IS Practices for SME Success Series

The Role of IS Assurance & Security Management

Edited by Rebecca Kestle & Richard Self
IT PRACTICES FOR SME SUCCESS SERIES

BOOK 1: THE ROLE OF IS ASSURANCE & SECURITY MANAGEMENT

1ST EDITION
2013

EDITED BY REBECCA KESTLE AND RICHARD SELF

Cover image courtesy of adamr at FreeDigitalPhotos.net
This book is the first of a 2 set series, composed of 35 articles and written by A grade students at the University of Derby. These students have been taught the technologies and practices that are at the cutting edge of enterprise systems.

This book has been written for all levels of management and members of staff or users working in small to medium enterprises where information systems have an impact, or are integral, to their business. The articles written have been done so with this in mind, and as such, any recommendations and statistics are centred around these types of businesses.

It aims to inform readers on many of the most applicable business practices that should be considered with regards to technology and information systems (IS), thus increasing awareness in the workforce, allowing optimisation of system practices and ultimately driving success in SME’s, delivering more of what they should, in the way that they should.

The main themes throughout this book include security (in many forms), online issues (implications and protection), governance and compliance, and insider / human issues. The book includes a host of other articles that are of particular interest to SME’s - current issues that can help increase proactive tendencies, competitive edge, efficiency and awareness.
<table>
<thead>
<tr>
<th>Title</th>
<th>Author</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Media Sites as a Security Risk to SMEs</td>
<td>Ademujimi, Adedeji</td>
<td>7</td>
</tr>
<tr>
<td>Information Security for SME’s</td>
<td>Anderson, Jermaine</td>
<td>11</td>
</tr>
<tr>
<td>Fighting Information Risk &amp; Security</td>
<td>Arthur, Joe</td>
<td>15</td>
</tr>
<tr>
<td>Considerations When Implementing a BYOD Strategy</td>
<td>Bell, Michael</td>
<td>19</td>
</tr>
<tr>
<td>How Secure is the Cloud</td>
<td>Benson, Andrew P</td>
<td>23</td>
</tr>
<tr>
<td>Information Assurance</td>
<td>Brevett, Adrian</td>
<td>27</td>
</tr>
<tr>
<td>BYOD: Can it Harm Your Business</td>
<td>Gladyng, Cal</td>
<td>31</td>
</tr>
<tr>
<td>The Threat From Inside</td>
<td>Hall, David</td>
<td>35</td>
</tr>
<tr>
<td>Bring Your Own Device: Employee &amp; Business Perspective</td>
<td>Hanify, James</td>
<td>39</td>
</tr>
<tr>
<td>Payment Card Data Security Standards</td>
<td>Harrison, Jack</td>
<td>43</td>
</tr>
<tr>
<td>Passwords and Post-its</td>
<td>Howden, Chris</td>
<td>47</td>
</tr>
<tr>
<td>Building Online Brand Trust for SME’s</td>
<td>Ikott, Mfon-obong Edwin</td>
<td>51</td>
</tr>
<tr>
<td>Title</td>
<td>Author</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-------</td>
</tr>
<tr>
<td>The Human Factors in Security</td>
<td>Shembi, Kirandip Kaur</td>
<td>107</td>
</tr>
<tr>
<td>What if Your Business was Held to Ransom?</td>
<td>Shillam, Richard</td>
<td>111</td>
</tr>
<tr>
<td>Your Business Identity: Just How Secure is it?</td>
<td>Smith, Joseph</td>
<td>115</td>
</tr>
<tr>
<td>Corporate Cyberstalking: A Guide for SME’s</td>
<td>Stewart, Charles</td>
<td>119</td>
</tr>
<tr>
<td>Free Wi-Fi: The Hidden Dangers</td>
<td>Straw, Kyle</td>
<td>123</td>
</tr>
<tr>
<td>Chip &amp; Pin Security for SME’s</td>
<td>Uddin, Ashraf</td>
<td>127</td>
</tr>
<tr>
<td>Social Networking: Employers are Watching!</td>
<td>Vaughan, Gerald</td>
<td>131</td>
</tr>
<tr>
<td>Cloud Computing: An SME Perspective</td>
<td>Welsh, Gareth</td>
<td>135</td>
</tr>
<tr>
<td>Storage Backup. Why is This Important for Small to Medium Enterprises?</td>
<td>Whittaker, Scott</td>
<td>139</td>
</tr>
<tr>
<td>Public Cloud Security: A Question of Trust</td>
<td>Whorrod, Andrew</td>
<td>143</td>
</tr>
<tr>
<td>Author Index</td>
<td></td>
<td>147</td>
</tr>
</tbody>
</table>
Social Media Sites as a Security Risk to SMEs
Scared Of The Social Media Frenzy? BEWARE!!!

Ademujimi, Adedeji
University of Derby,
Derbyshire, UK,
100280078@unimail.derby.ac.uk

Abstract - The purpose of this article is to identify and create awareness for SMEs (Small and Medium-Sized Enterprises) on the security implication and underlying threats involved in using online social media sites as marketing tools for generating income and brand awareness. This article posits that SMEs face serious challenges caused by lack of awareness about issues ranging from; Information leakage, advanced persistent threats (APT), identity theft, mobility, computer malware etc., affecting productivity and growth of businesses, which invariably results in loss of time, resources and reputation. To summarize this paper, SMEs need to invest more resources in training, awareness, research and development and IT security.

Keywords - SMEs, Internet, Social Media Sites, Business, Threats, Risks, Cyber criminals, Information Security.

I. INTRODUCTION

“Organisations and government are finding it difficult to accurately detect, identify, predict and prevent the malicious exploitation of social media” (Chandramouli, 2011). This article focuses on identifying the risk and consequences of using social media sites for business purposes by SMEs.

The internet has become so fundamental to businesses and all social media sites are dependent on the internet. According to Millar (2011), a major downtime on internet services is all it takes to cripple businesses the world over. The impact of this downtime could result in no network coverage, no phones, no email access, even client database and ordering systems would be affected. The Internet used to be associated with web search but over the years it has grown rapidly such that it is used not only for searching the web but for information dissemination, communication, social networking, micro blogging, etc. which are examples of services that are emerging technological trends in the computing world (Chandramouli, 2011). According to Kaplan and Haenlein (2010), social network is defined as “a group of internet based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User-Generated Content".

The proliferation of social media sites is having a major impact on businesses worldwide because organisations are opening up there systems to smart phones and portable devices without necessarily putting any security control in place to check this new technological advancement (PwC, 2012). A PwC (2013) survey report showed that security breaches has taken an astronomical increase costing firms in the UK billions of pounds yearly and small businesses were identified as being notably affected (PwC, 2013). SMEs have primarily become targets of cybercriminals because of the obvious weakness in their security programs which may not be as efficient as those of larger enterprises (Westin and Hoffman, 2006). Trust is a key concept in business and social media sites are built on trust. Organisations trust in their employees to protect confidential data whilst carrying out their job responsibilities using technology (social media) as a working tool (Shullich, 2011). Small businesses in comparison to large enterprises have the misconception they do not face as many content security risks (TrendsLab Primer, 2011). This fact is supported by the Council of Better Business Bureau’s study (Westin and Hoffman, 2006) which revealed that 7.4% of small business owners are victims of fraud.

A good example of the failure and security threats involved in using social media for business can be seen in the recent hacking of the Twitter account of the Associated Press, where hackers used the account of this firm to send out malicious messages which resulted in the Dow plunging 150 points within four minutes (Geary, 2013). This type of security breach highlights the consequences of integrating social media with business. According to Moore and Roberts (2013) the Dow Jones industrial average is an application that measures the financial performance of major companies in the United States of America and it also measures the strength of the wider stock market.

This article will take the following format: Section II discusses the kind of threats and the way they operate. Section III discusses some related business issues (business and IT security) followed by the main conclusions.

II. POTENTIAL THREATS AND RISKS

Stelzner (2012) stated that about 83% of marketers believed in the importance of running their businesses through social media. What kind of risks does social media portend to SMEs?

a) Identity Theft

Parmar and Hedges (2012) stated that over 60% of SMEs have identified cyber-attacks and data loss as a major threat due to the rise in cases of corporate identity theft. Identity theft is the process whereby a cyber-criminal fraudulently obtains very private information from an individual or business and in turn uses it to access confidential information for malicious purposes. Unfortunately, over 40% of SMEs are not aware of the existence of this type of threat and do not consider
their business at risk (Business Matters, 2013). Identity theft is carried out through the aid of pharming and phishing.

- **Phishing:** A process where cybercriminals through dubious means acquire financial details and information to scam their victim (Brody, 2007). Phishing can result in a hacker completely compromising the network of an organization.

- **Pharming:** This is an advanced form of ‘phishing’ where websites information from a legitimate site are redirected to a malicious site (Brody, 2007).

**b)** Advanced Persistent Threats (APT)

According to Rodgers (2011), “In March 2011, information about RSA’s SecurID authentication tokens – which are used by many of Australia’s largest banks and government agencies- was stolen in what the company described as an ‘extremely sophisticated cyber-attack’.”

The example above can best be described as a perfect case of APT. This process involves hackers sending malicious mail messages that look legitimate on the internet and in particular through the use of social media platforms. When the unsuspecting victim clicks the link it redirects the user to a website from where a hacker takes total control of the victims system from a remote location. This type of attack is common on websites like Facebook and Twitter. (McAfee, 2010). SMEs need to understand this challenge and fashion out a solution that could help detect this potential threat.

**c)** Mobility

With the adoption of modern technologies such as smart phones, tablet, etc. in the work place, a vast majority of professionals now use these devices as their primary working tool thereby integrating corporate data and personal data in the process (Kaspersky, 2012). This trend often referred to as BYOD (Bring Your Own Device), has become widespread amongst businesses worldwide as it allows for an effective and efficient way to conduct transactions thereby driving productivity, but it has also introduced new types of security risks to the workplace (Kaspersky, 2012). According to the same authors, more smartphones are being sold when compared to PCs and these devices are becoming more popular for both business and private use. There are over 5 billion mobile phones with internet access and various mobile applications that make users vulnerable to cyber-crimes (World Economic Forum, 2012). Smart phones are portable and this makes them easy to lose or steal which can result in data theft. Another reason why BYOD is a potential threat to SMEs on the social media platform is as a result of exposure to malwares. Most mobile devices are not as properly protected from malware as PC malware (Kaspersky, 2011)

**d)** Data Leakage

Gordon (2007) defined “Data Leakage, put simply, is the unauthorised transmission of data (or information) from within an organisation to an external destination or recipient.”

Making strategic decisions and effectively managing customers data plays a vital role in the outcome of a business concern. Most SMEs at some point would collect, store or share information, notwithstanding the type of transaction that might be taking place because businesses basically thrives on information (Westin & Hoffman, 2006). Small businesses are custodian of employee and customer information, making them prime cybercrime targets in every way (Trend Labs Primer, 2011). Cyber criminals have taken advantage of the importance of this keyword - data - to manipulate unsuspecting organisations. Data leakage on social media sites is on a continuous rise among businesses and users as a result of carelessness and lack of awareness.

According to Comsec Consulting (2010), data leakage occurs when cyber-criminals gather information about an organisation and its employees by running a quick search of social networking channels. According to a PWC (2012) survey “Data protection is no longer seen as an IT issue in isolation and the various data loss incidents have led to significant economic loss, impairment of the organisations reputation as well as serious legal lawsuits.”

**e)** Computer Malware

Malwares are applications that exploit system vulnerability to infect computers. Examples of malwares are computer viruses, spyware, Trojans and other malicious software. Spammers and hackers make effective use of lapses on social media sites to spread malwares (GFI, 2011). Findings of a survey carried out by Google (a firm well known for its effective search engine) on its website indicated that out of about a billion sites that were closely examined, about 450,000 had the capacity to install malicious codes, such as spyware, without a user’s knowledge (BBC, 2007). The increase in cases of malware attack was attributed to the internet and the surge in the reliance on social media sites where attackers have found security lapses. Attackers leverage on the personal information available at their disposal through social media (Weston & Hoffman, 2006). This type of threat has the capacity to destroy any SME that is not aware and prepared for this type of challenge.

### III. HOW SECURE IS YOUR BUSINESS?

As the world keeps evolving, the internet provides a platform for businesses to thrive. The strength of Business Information security is in the ability to protect customer data. Social media sites such as Facebook, Twitter, eBay etc. are good platforms that SMEs can use to develop a good customer base, build their company profile and also generate revenue.

The importance of IT security and social media to businesses cannot be understated. Majority of the attacks that have occurred through Social Media seem to be unidentified by SMEs, leading to attacks being not often reported. Interestingly, there has been a significant increase in the number of employees who use Social Media as companies continue to leverage on the popularity of Facebook and Twitter for marketing purposes which in turn as resulted in businesses becoming prone to attacks (Gonsalves, 2013). Consequently, there has been a steady increase in crimes against SMEs, over 15,000 small businesses admitted to have fallen victim of various cyber-crimes (Business Matters, 2011).

Viruses, Malwares and other types of cyber threats do not discriminate on the size of the business; rather for Cybercriminals what matters most is exploiting loopholes and
disrupting business, which results in economic loss. SMEs are failing to invest in information security and security awareness due to so many reasons, which include a limited budget, fewer compliance drivers etc. (Goucher, 2012). Criminals may attack SMEs as a result of lapses on their security platforms which may not be as effective as that of larger enterprises (Westin and Hoffman, 2006). Curiously, on the popular online social media sites Facebook, 83 million profile pages were reported to be fake (Guardian, 2012). The question remains who has created these profiles and for what purposes?

As earlier stated, Social Media sites are dependent on the internet and at a time when about 24% of UK SMEs currently conduct all or most of their day to day business on the internet, Parmar and Hedges (2012). It is disturbing to note that SMEs still do not consider investing so much on Information Security as a top priority. Information security is down the ‘pecking order’ when it comes to investment priorities of SMEs (Goucher, 2012). Findings of a survey report by, Parmar and Hedges (2012) indicated that, Cyber-attacks and Data leakage are the biggest threat to over 60% of SMEs due to a rapid surge in cases involving Identity theft. As a result of the sophistication cyber thieves adopt in carrying out their attack, 68% of businesses have problems identifying Fraudulent attacks and security breaches on the corporate network (Ayrapetov, 2013).

Most SMEs are not aware of compliance issues. Others are of the belief that they are compliant and have put the right security checks and balances in place. Sadly, close to a 1 million small businesses in the U.S have fallen victim of information security fraud (TrendsLab Primer, 2011). SMEs need to take into cognizance the fact that on Social Networks there are no checks and balances to enforce compliance or any rules guiding the way customers and attackers alike use the platform (Shullich, 2011).

Finding of a survey report by, Parmar and Hedges (2012) indicated that, Cyber-attacks and Data leakage are the biggest threat to over 60% of SMEs due to a rapid surge in cases involving Identity theft. As a result of the sophistication cyber thieves adopt in carrying out their attack, 68% of businesses have problems identifying Fraudulent attacks and security breaches on the corporate network (Ayrapetov, 2013).

Most SMEs are not aware of compliance issues. Others are of the belief that they are compliant and have put the right security checks and balances in place. Sadly, close to a 1 million small businesses in the U.S have fallen victim of information security fraud (TrendsLab Primer, 2011). SMEs need to take into cognizance the fact that on Social Networks there are no checks and balances to enforce compliance or any rules guiding the way customers and attackers alike use the platform (Shullich, 2011).

It has become imperative for SMEs to develop a strategy that can be used to identify and detect this type of threats. To effectively reduce security risks, SMEs ought to make employees aware of the prospect of becoming a potential target by way of social media (Gonsalves, 2013). They also need to educate employees and customers alike on the implication of negligence especially as it concerns information dissemination whilst using social media as a marketing tool. Consequently, Security awareness training should be a primary concern of all SMEs in tackling the issue of cyber-crimes on the Social Media platform.

**Figure 1.** The facts stated in the above diagram represents the gradual increase in cases of cyber-attack and also shows security threats which are having a direct impact on growth and productivity of Organisations (Kaspersky, 2012)

**IV. CONCLUSION**

SMEs and businesses in general, keep adopting new technologies without considering the security implications (Kaspersky, 2012). Not a few SMEs are prepared for the security challenges ahead which have provided incentives for the ever deceitful and sophisticated cyber criminals to keep exploiting and developing malwares, spywares and other harmful applications disrupting businesses. Anti-Viruses, anti-malware etc. are no longer as effective in dealing with the diversity and volume of threats businesses tends to face (Kaspersky, 2012). What may initially seem like business benefits can suddenly develop into IT security challenges such as loss of data, corporate identity theft, unauthorised access to systems or data, breach of data protection, laws or regulations, fraud, if the integration of social media and business is not properly managed. Interestingly, some of the most pressing issues in the field of cyber-crime and security as it relate to SMEs as to do with Failings in people, processes and technology (PWC, 2012). One of the major reasons why businesses and SMEs have suddenly become targets of attackers is because they lack and do not have good security measures and practices in place.

It has become imperative for SMEs to develop a strategy that can be used to identify and detect this type of threats. To effectively reduce security risks, SMEs ought to make employees aware of the prospect of becoming a potential target by way of social media (Gonsalves, 2013). They also need to educate employees and customers alike on the implication of negligence especially as it concerns information dissemination whilst using social media as a marketing tool. Consequently, Security awareness training should be a primary concern of all SMEs in tackling the issue of cyber-crimes on the Social Media platform.
REFERENCES


Information Security for SME’s

Jermaine Anderson
University of Derby
Derbyshire, UK
J.Anderson2@unimail.derby.ac.uk

Abstract - Information and technology are potential benefits to SME’s (Small to Medium Enterprises). A result of this drives SME’s towards maintaining protection over their information assets and technology. Both ISO 27001 and 27002 provide frameworks for this transition. With SME’s facing financial difficulties as well as a number of potential internal and external security risks, organisations need to determine solutions that will improve the security within their organisational structures. However, this is easier said than done. The purpose of this article is to analyse security threats and risk to identify potential failures within SME’s. In doing so, this paper will discuss ISO 27001 and 27002 principles to determine practices and procedures which are able to improve security within various organisations.

Keywords - SME, Security, Information, Governance, Threats, Risks

I. INTRODUCTION

Security is defined as “the safety of a state or organisation” (Hawker and Waite, 2009). However, information security refers to the protection of information assets (Upfold, 2005). These two statements conclude that in order for organisations to maintain security over their information assets, they must follow key security principles. With 76% of small organisations becoming victims of security breaches in 2011, statistics show there are concerns especially for SME’s (Potter and Waterfall, 2012). Various organisations have become victims as a result of failing to govern their organisations according to the principles of appropriate security frameworks such as ISO 27001 and 27002. Studies prove this as 75% of SME’s have poor understanding of security policies. In addition, 58% of small enterprises are failing to carry out adequate risk assessment (Potter and Waterfall, 2012; Upfold, 2005). As part of overcoming arising concerns, SME’s need to consider security risks and breaches, which often occur as a result of cyber-attacks and mishandled information (Whitman and Mattord 2011; Upfold, 2005). With 20% of SME’s breaching data protection act (DPA) laws by failing to protect information, security breaches are costing between £15k-30k (Potter and Waterfall, 2012). This makes evident that a solution is imperative (Potter and Waterfall, 2012; The Standish Group, 2004; Upfold, 2005).

As part of attempting to restore a level of control within the IT industry, this paper will identify different types of security failures within SME’s. This will be done by critically analysing the root of why failures occur. Also, the key factors of security failure that affect SME’s will be discussed in order to evaluate and determine how SME’s are going to strive towards making a change.

II. SECURITY FAILURES WITHIN SME’S

With risks concerning viruses rising from 20% to 73%, e-mail intrusion rising from 2% to 29% and theft of hardware rising from 23% to 46%, information security failures are a concern for SME’s (Calder and Watkins, 2008; The Standish Group, 2004). Although Baldin (2010) claims organisations are imposing strict policies, this is a controversial statement. Policies and procedure are important aspects of security but they are only a part of effective principles in terms of protecting information (Upfold, 2005). Also, SME’s need to be aware that in imposing policies and procedures that are two strict can restrict employees from operating effectively. Instead, organisations’ needs to consider security measures that are relevant and flexible to maintain security on a corporate level (Schneier, 2003; Upfold, 2005). According to Potter and Waterfall (2012), it is imperative that SME’s engage in information security processes as well as adequately understand and appreciate the purpose of addressing security threats as part of maintaining effective risk management. However, a failure many SME’s are facing is they are choosing to forget, ignore and move on from security failures. Instead they should take into consideration the risks and threats that have occurred in order to develop future solutions for information protection. The reason for this is because the issue may possibly be the same but the solution is different (Ashford, 2012). In addition, SME’s are known for relying purely on luck rather than appropriate security measures. This suggests that they are playing a game of trial and error as part of preventing threats (Calder and Watkins, 2008; Mardjono, 2005).

Threats are referred to as an object, person or an entity that represents a danger to an asset (Whitman and Mattord, 2011). While external threats posed by cyber criminals such as hackers, phishers and spammers are increasing, there are concerns about security in SME’s (Calder and Watkins, 2008; Upfold, 2005). Statistics show that 15% of SME’s suffered as a result of DOS attacks (denial of service attack), which is a common subset of cyber-attacks often aimed at high profile web servers (Potter and Waterfall, 2012). This shows that hardware, software and networks within SME’s are becoming exposed to cyber criminals as they pair up to launch attacks (Calder and Watkins, 2008). A perfect scenario of this is in relation to “PayPal” (Laville, 2012). As a result of cyber-attacks, “PayPal” lost £3.5 million, suffered from a damaged reputation and a loss of sales. This case involved a deliberate DoS attack, which was carried out by 4 males (Laville, 2012;
Whitman and Mattord 2011). Since then, Obama (2012), president of America, has stressed that organisations need to improve their cyber defence security, as a key measure of protecting their information assets (Ashford, 2012).

However, internal threats are also an issue. Vulnerable weaknesses in organisational structures are causing various SME’s to jeopardize their information assets. Incidents involving breached firewalls due to internal employees granting external hackers access to companies internal networks often occur (Calder and Watkins, 2008; Upfold, 2005). These incidents occur due to the lack of knowledge and failures to impose and comply with appropriate policies and procedures as well as failing to carry out adequate risk assessment (Calder and Watkins, 2008; Potter and Waterfall, 2012; Upfold, 2005). In addition, studies have found that 55% of employees are downloading software onto internal systems. These downloads have caused internal issues with IT help desk staff having to resolve the problems. Furthermore, 58% of employees have been involved in uploading confidential information on social media sites. With only 8% of SME’s monitoring information posted onto social media sites, there is a problem as such acts open gate ways for sensitive confidential information to be exposed to external threats (Baldin, 2010; Potter and Waterfall, 2012).

### III. Key Factors that Affect SME’s

A critical key factor that affects SME’s in maintaining good security is the war they face against banks (Duan et al 2009). Many SME’s are suffering financially. This is caused as banks are refusing to lend money to organisations’ as they believe it involves a high risk of unpaid repayments. This then affects SME’s in terms of staff capacity alongside in-house training opportunities, especially as 54% of organisations are lacking programmes that educate staff about security risks (Deschoolmeester et al 2008; Upfold, 2005; Potter and Waterfall, 2012). With SME’s lacking funds to employ in-house IT staff, they are forced to outsource information security services to external organisations. Although outsourcing can be cost effective in managing information security, there are tendencies that outsourcing poses risks (National Computing Centre, 2005). Outsourcing vital information and security measures to external organisations can have detrimental consequences as confidential information can be lost or even incriminated (Calder and Watkins, 2008; Deschoolmeester et al 2008; Whitman and Mattord, 2011). To add to this, financial difficulties also effect SME’s as they are unable to implement effective and modern hardware and software. In many cases, the installation costs are too much causing SME’s to settle for less (Upfold, 2005). Also with the IT industry rapidly developing, organisations are unable to keep up with the modern changes (Hilty, 2008; Pattinson, 2011).

With modern changes allowing many employees to bring personal mobile devices to a working environment, organisations internal networks are becoming vulnerable. A recent study proved that 60% of employees were accessing internal networks using personal mobile devices. 17% of these employees had previously accessed the internal network without detection. This is a concern as it shows that organisations are not considering policies that protect them from external intrusion (Ashford, 2012; Scott, 2012). Despite this, further analysis produced more damaging evidence. With 89% of organisations concerned about viruses intruding their internal networks whilst 91% believed their information is vulnerable to external attacks, SME’s are suffering, especially from the lack of in-house IT departments (Deschoolmeester et al 2012; Scott, 2012).

With SME’s lacking in-house IT expertise, there are complications in maintaining software updates and patches. This then causes weaknesses in the system providing hackers with vulnerable areas to gain access (Upfold, 2005; Whitman and Mattord 2011). Despite the strength of an organisations internal system, once a weakness has been identified, attackers will exploit various means in order to gain entry (Schneier, 2003). Schneier (2003) refers to this as the weakest link in a chain. Many SME’s are failing to acknowledge the importance of identifying their weaknesses, rather than focusing on various methods of protection. Regardless of the security measures imposed, SME’s will be unable to successfully protect themselves from external intrusion until they eliminate the open doors attackers are walking through (Schneier, 2003). This draws awareness that security is not about numerous countermeasures, but rather countermeasures that are able to function independently and in series as well as present various hurdles that slow and stop attack (Schneier, 2003). Furthermore, internal threats such as fires, floods and other natural disasters are also an issue (Calder and Watkins, 2008, Deschoolmeester et al 2008; Whitman and Mattord 2011). An incident involving BT where a fire destroyed underground cables affected various organisations in North West Manchester (BBC, 2004). Organisations were affected as they were unable to gain access to their networks because of this disaster (BBC, 2004; Goodwin, 2004). In addition, failures to impose and comply with effective business continuity plans caused many organisations to lose their information. From earthquakes to other natural disasters, organisations have been forced to learn the hard way. The 9/11 caused various organisations to suffer financially which in many cases led to bankruptcy. Organisations from data centers, universities and IT firms lost confidential information due to failing to produce consistent back-ups, damaged network infrastructures and even the positioning of their data centers (Cullen, 2011; Monaco, 2001; Savage, 2004). In such incidents, statistics show that an estimated 70% of SME’s fail to continue in business or close within 3 years of a major disaster (Anon, 2009; Gosling, 2008). This concludes that protecting information is crucial, especially as it is part of the key driving force within an organisation because of its value (Cole, 2012; Oppenheim et al 2001; Calder and Watkins, 2008).

### IV. Making a Change

Identifying, assessing, treating and managing information security risks are key procedures that need to be done if organisations intend to protect their information assets
(National Computing Centre, 2005; Lomas, 2010). As protecting information assets are vital, it is important SME’s comply with effective security principles from ISO 27001 and 27002 practices. ISO is a well-known framework that defines what should be done within an organisation to sustain information security (Calder and Watkins, 2008). ISO will ensure products and services are reliable, safe, and of high quality (Calder and Watkins, 2008). Furthermore, ISO 27002 will implement adequate procedures for managing and training employees, as part of allowing staff to receive appropriate updates on relevant policies and procedures in relation to security (Calder and Watkins, 2008; Gehrmann, 2012). This will ensure SME’s are able to diligently adapt to modern changes being made within the IT industry. It will also ensure employees gain relevant technological experience and knowledge, broadening their understanding of possible security risks, especially as skills and knowledge is vital in terms of protecting information (Paul, 2013). In combining practices from ISO 27001:2005 with ISO 27002:2005 security techniques as part of managing security is imperative, because of the mass of data as well as the risks of breaches including cyber-attacks, malicious code and other incidents like sabotage fires and floods that can affect software and hardware within SME’s (ISACA, 2009). In imposing and complying with control orders such as key security principles that relate to good governance will maintain confidentiality, integrity and accessibility in concern to information assets. This will help assess and prevent misuse of information by internal and external threats. It will also succeed in managing other possible risk that have potential to pose threats towards the state of information’s security (Calder and Watkins, 2008; Hardy, 2005).

With it known that SME’s face potential detrimental consequences in the event of disasters which may cause information assets to be jeopardized, it is crucial that appropriate business continuity plans are imposed (Anon, 2002; Monaco, 2001; Savage, 2004). Business continuity plans are designed to articulate the nature of internal and external risks and what can be done as part of preventing their effects. In having effective business continuity plans imposed, SME’s will reduce risks posed towards their information assets and technology (Herrick, 2011; Savage, 2004). Also, SME’s will be able to recover effectively whilst maintaining integrity of their systems. In addition, risk management must be incorporated into business continuity plans in order for it to be effective. This will be done by integrating a combination of practices from both ISO 27001 and 27002, which will provide a sustainable structure in managing developments, maintenance as well as analysing risk to reduce security threats (Calder and Watkins, 2008; Savage 2004).

As well as imposing and complying with information security frameworks as part of improving security, organisations need to consider important security skills. Maintaining good communication throughout an organisation and with outside contractors is extremely important. This will strengthen security within SME’s as there will be a clear understanding of possible risks and threats, allowing issues to be resolved much more effectively (Paul, 2013; Stackpole, 2012).

V. CONCLUSION

Security is becoming an issue for SME’s, especially as cyber criminals are fixating there attacks on small firms. Despite this, there are numerous information security principles available for SME’s to adopt as part of protecting themselves from these attacks. However, the main concern is that organisations’ need to comply with security principles in order for them to be effective. In addition, employees need to adequately understand the importance and process of security policies and procedures as well as risk management. This will nurture organisations in reducing the issues they are facing in terms of internal and external security threats. Implementing effective principle from ISO 27001 and 27002 will help resolve further issues organisations are confronted with, such as business continuity plans and in-house IT expertise. This will be done as it will provide a strong framework for SME’s to maintain good governance as part of sustaining security within their organisation. In a broader prescriptive, ISO principles will assist in reducing security risks, improving service delivery and ensuring compliance (Calder and Watkins, 2005).
REFERENCES


Abstract - This paper addresses the issues of Information Risk and how it can aid SMBs. Looking at Information Risk in the context of customers, managers and business decisions. The paper also analyses studies within the topic and how these can help businesses, along with views from Schneier and ISO27002.

Keywords - SMBs, Information, Risk, Security, ISO27002.

I. INTRODUCTION

Information is essential to modern society (HM Government, 2008). This article addresses the issue of Information Risk, and how it can affect every business, of any size.

II. WHAT IS INFORMATION RISK?

Information risk is about the probability of a hostile decision made on the basis of erroneous or ambiguous information, a critical factor in many key business decisions (Sinason, Webber & Nikitkov, 2009). Another paper describes Information Risk as covering all of the issues that are produced from an organisation’s need to protect and control its information (IAAC, ISAF, & BT, 2009). This second definition would be much more fitting, as it would include the issues involved in the first definition, drawing context to decision making. Overall, information risk could be defined as the control and protection of information to ensure best results.

III. WHY IS INFORMATION RISK IMPORTANT?

Research papers state that information is a key resource and asset in businesses (IAAC, ISAF, & BT, 2009; Ritchie & Brindley, 2001). Furthermore, it can be seen that information exists in not only financial business decisions, but further aspects such as outsource providers or growth decisions (Sinason, Webber & Nikitkov, 2009). It can easily be believed that if a person has the correct information at all times, then the best decisions can be made, meanwhile inaccurate information can lead to bad decisions and unsuitable directions for a company.

Kirmani and Rao (2000) talk about information asymmetry – whereby one party has more reputable information than the other. Further from this is the agency relationship problem, where one body (the principal) consigns work to another (the agent), who executes that work (Eisenhardt, 1989). The asymmetry becomes apparent in that the principal cannot monitor the agent and whether their objectives are being served (Adams, 1994). Information cannot be disregarded by any means, without the latest information businesses could not operate. Therefore information risk is an important topic, because it is about addressing the issues surrounding useful and accurate information within a business context. The wrong or improper use of information can lead to security breaches within an organisation.

IV. INFORMATION RISK AND THE CUSTOMER

In 2009, Webber, Sinason and Nikitkov put information risk into context in a rather strange study. They wanted to prove that information risk was a key issue, in that reliable information is a heavy requirement yet often unconsidered (Sinason, Webber & Nikitkov, 2009). The three researchers used eBay to prove the value customers place on third-party assurance services. Assurance services being services that reduce information risk for decision makers (Elliott, 1994).

The use of eBay was for access to a market with the implications of e-commerce, whereby anonymity means a lack of knowledge for buyers. This ambiguity brings a requirement for knowledge-acquisition, and this is where the assurance services and information risk comes in. The specific market chosen was baseball cards, because collectible items can be characterised on all aspects except quality, and assurance services (Professional Sports Authenticator) existed within the baseball card market (Sinason, Webber & Nikitkov, 2009).

The hypothesis for this study was simple, a seller would use the site to advertise their card, and usually try to cover up any defects in the images, and probably be biased in the description of condition. Meanwhile the quality assurance services would provide a rating on cards, which could also be added to the card seller’s description. What the researchers did was take a large number of sales on eBay that did not have quality assurance ratings, and a large number that did. This methodology then allowed the researchers to see how much more (or less) was paid depending on whether a card had a quality-assurance rating or not. The large market and data that could be taken meant that the same cards with the same perceived quality could be compared (Sinason, Webber & Nikitkov, 2009).

The researchers discovered that buyers were prepared to pay $39 to $141 more, dependent on grade, for cards that had been certified by assurance services. Furthermore, the seller’s reputation did not have an effect on price (Sinason, Webber & Nikitkov, 2009).

From this we can learn that if a company can find a way of assuring their customers, lowering the information risk shall increase reputation. This theory could be applied to a range of products, and means that companies can sell at a premium price if they are assuring quality for their customer. In context, customers are prepared to pay more
for popular products, because they have been assured, from the popularity, that they are getting a certain quality of product. This study shows that small or medium businesses could bypass the popularity assurance by finding methods to reduce customers’ information risk. So, information risk isn’t just about the security of a business, but it can apply to consumers too.

V. RISK

Before explaining the concepts of agency theory and other standings on information risk, it may be worth looking at the different definitions and some key concepts on risk. Risk is defined by the Oxford Dictionary of English (Oxford Dictionaries, 2010) as “a situation involving exposure to danger”. Meanwhile, with regard to the threats to assets and weaknesses in the organisation in terms of the business objectives and approach, a definition made by the International Standard 27002 (2005) offers more of an insight into the risk facing information technology. It can be taken that risk is about the probability of danger in next to anything.

The reason that risk needs mentioning is because of certain theories within the field. Namely, Bruce Schneier, who’s possibly largest literary offering is of there being no absolute security, and that it always involves some kind of trade (Schneier, 2008). This is a rather cynical claim by Schneier, yet conceding to this fact is more realistic and helpful. Schneier believes that a human brain does not assess risks mathematically; instead using different personal experience and bias, affecting our perception of risk (Schneier, 2008). Schneier’s concept of risk is very different, asking us to attempt to remove all bias and experience, and assess risk robotically so that we can calculate a better probability of what has more chance of happening and what doesn’t.

VI. THE AGENCY RELATIONSHIP PROBLEM

The idea of individual perceptions of risk brings the topic of the agency relationship problem about fittingly. To reflect, the agency relationship problem is about the relationship between the giver of work (the principle) and those who execute the work – the agent (Eisenhardt, 1989). Namely, the issues arise when the agent and principal have different views towards risk. The problem being that the agency and the principal may favour different approaches because of their preferences of risk (Eisenhardt, 1989). The problem also draws on the fact that both parties never know if their best interests are being served (Eisenhardt, 1989). Here is where information risk plays a part; both parties may make a decision and complete an action that may have a negative effect on the relationship, and this action may be on the basis of incorrect or inaccurate information. The action may then result in a larger affect across the organisation, and in turn negatively affect the company. For example, let’s say a manager of a small business, with only 25 employees, disciplines a member of staff with the information that they are not pulling their weight on a project. The manager decides to go very hard on the employee, making an example of them, before the employee can present some new work they have done on the project. The employee is consequently very angry about the unfairness and attitude of the manager. So from then on, the employee takes a negative stance towards the company, anonymously bad-mouthing it on the internet and to friends. Word gets around about the disciplinary and this negativity spreads to other employees, who also then share a dislike for the company. Subsequently, the company finds it very hard to get new employees, and morale is very low.

This is a rather basic example and a little over exaggerated. However, for a small or medium business, the probability of going bust at an early stage due to issues like this could be high. It can be seen that the manager has taken a rather large risk. The risk is with information and the example illustrates the agency relationship problem. The employee and employer are worried that their interests are not being served by the other party and so take information risks, thus bringing about a lower moral and lowered productivity in the workplace. While this could be dealt with in a larger company, small and medium businesses can find it harder to combat the issues, and there is higher threat of failure.

We have already seen how information risk can have an effect on the consumer; we can now see that if the information risk can be moderated, it can have a positive effect within the workplace too. If a company can find a way to control or alleviate information risk within the workplace, especially at an early stage, then they should find a better rate of productivity and morale around the workforce.

VII. A DIFFERENT VIEW

While the baseball card study found that lowering information risk can have a positive effect on market prices, a different study found the opposite. Ritchie and Brindley (2001) conducted an experiment on fifty managers whereby they asked for strategic analysis and decisions. In this study the managers were allowed access to databases of information for assistance.

Ritchie and Brindley (2001) found in this study that the decision makers often use selective information to support their preliminary opinions on a decision. Therefore what the study found was that users with information will just use this information to go with their initial gut feeling about the decision, to ‘back up’ their opinion. The researchers reinforced this selectiveness by providing information that should change initial perceptions.

On a sceptical side, these are managers and the other study looked at customers. There is a difference; this study outlines that the managers had taken some form of graduate degree and were aware of the business decision processes to be taken, whereas we were never made aware of the type of customer being looked at in the previous study, due to anonymity. This research has taken a particular demographic and applied this test. What if we had taken a
certain experienced manager that had no degree and wasn’t aware of business decision processes? Would there be a different result? Would they then use the information available to change their preliminary decision? This is subject to further research in the future.

Schneier (2009) depicts how we should try to conduct risk assessments mathematically, so if these managers had used more logic and maths rather than gut-feeling they may have reached different outcomes.

While this study isn’t a great advert for addressing information risk for better decision making, it could still be said that a manager does need the additional information. Executives should ask themselves if they rely too much on their manager’s gut feelings, and if it is time to apply information risk concepts in a more logical, mathematical way.

VIII. ISO 27002

International Standard ISO 27002 (2005) depicts a code of practice for security information management. It can be used as a risk assessment or a general guide on implementing information security for an organisation. While ITIL and COBIT look at information technology management and services, ISO 27002 addresses the practical aspects - the actual implementation and control of information systems.

So what does ISO 27002 say about information risk? Well the document mainly refers to Information Security as a whole, with sections on policy, co-ordination, back-up, leakage and exchange. The most relevant section for information risk is 7.2.1 - information classification. This section suggests controls to ensure information is classified in such ways as sensitivity, criticality, value and legal requirements (ISO 27002, 2005). In short, the standard is suggesting that classification is a good way of determining quickly and easily how the information should be handled.

If the executives of a company can implement these concepts into their business, they should be on their way to minimising information risk. By classifying information in the most efficient and appropriate manner, an organisation’s decision makers should then have the most valued and relevant information available to them. Meaning a company’s business decision making becomes beneficial financially and sustainably.

IX. SECURITY CULTURE

Finally security culture, words need applying to this aspect of information risk and assurance because it is key to survival. Calder and Watkins (2012) suggest how often information security is perceived as only an issue for the IT sector of a company, and how this just is not true. It needs recognising and reiterating that information security is not just for the IT department, this report has shown that information is a company-wide concern. Information security is a critical part of managing information risk (HM Government, 2008).

ISO 27002 (2005) has a specific section regarding awareness. This section suggests that the education and training for security awareness should be appropriate to the employee’s roles and responsibilities. However, it would be better advised to produce at least a standard level of education and training for information security awareness across a company so that all employees are at least aware to a suitable level of how information security and risk has a large impact on a business.

Schneier (2009) talks about how he believes that in some companies the average employee understands risk better than those actually concerned. He suggests that we as humans all understand risk very well and that before assuming somebody does not know the risks, one must assess the risks themselves. Schneier’s comments in some way agree with the standard level of awareness, because if everybody is given this standard awareness then there is an accepted level of staff knowing what is correct and what is not. It would also be well suggested that information security staff revise and update their knowledge of information security at regular intervals, to ensure their knowledge is ahead of those being educated, and to allow additional education where necessary to company employees.

While there is no evidence here that standard levels of information security education is useful, the concept cannot be dismissed. As a manager or executive of a company, is it not common sense to bring as much education to your staff members as possible? This report has even suggested ways in which this process can be cut down and made manageable, allowing all staff to be up to date and aware of the impact information security can bring, and ways to aid its implementation.

X. CONCLUSION

Over the course of this report, we have established the impact information risk can have on a business, as well as customers. It has also been established that through a few simple steps a company can become completely aware and able to tackle the issues that information risk can bring. For further information on how to tackle information security, it would be highly recommended to read and implement the key concepts of ISO 27002 (2005).
REFERENCES

Considerations When Implementing a BYOD Strategy

Michael Bell
University of Derby
Derbyshire, UK
100164250@unimail.derby.ac.uk

Abstract - If your company is planning to jump on the BYOD bandwagon or already happen to have a BYOD scheme in place; have the security risks, potential legal consequences and a recovery plan been considered? This article offers advice on what considerations should be made before embarking on the BYOD journey, ensuring your SME gets the most out of the scheme and more importantly, your company doesn’t suffer any consequences of the scheme being insufficiently managed and/or applied.

Keywords - BYOD, Corporate software applications, Electronic mobile device, IT Security, Security policy.

I. INTRODUCTION

There are many aspects to consider when implementing a Bring Your Own Device (BYOD) scheme including financial costs, security, legislation and the very reason for which most organisations embark on the BYOD journey; employee satisfaction leading to increased productivity (Rege, 2011). David A. Willis of Gartner (2013) stated recently that “Bring-your-own-device strategies are the most radical change to the economics and the culture of client computing in business in decades”. However, many organisations, particularly Small to Medium Enterprises (SMEs) are guilty of underestimating the potential either by ignoring it or by taking insufficient measures to incorporate it correctly.

A common misconception amongst SME’s is that their pre-existing security measures are sufficiently armed to protect their network when personal electronic mobile devices are brought into the workplace and connected to it. However, in reality an amalgamation of aging network security, insufficient knowledge, and the failure to ensure anti-malware programs are regularly updated or sometimes even installed on mobile devices all lead towards an extremely vulnerable BYOD system. The consequences of which could potentially lead to the demise of not just an employee’s career but also, in extreme cases the company’s status.

Privacy and security policies are also overlooked or insufficiently designed to accommodate BYOD. This article will look closely at both the security and legislative aspects, amongst others that your SME must take into consideration.

II. AN INSIGHT INTO BYOD

BYOD is an acronym of ‘Bring Your Own Device’, a phrase used to front a scheme based on the idea of allowing employees to take their own mobile communication device into the workplace and use it in place of or, in some cases in addition to their work PC and/or phone, tablet or smartphone, etc. (Scarfò, 2012). The scheme is primarily driven by consumer preference rather than corporate initiative (Rege, 2011). However, BYOD has potential benefits for both parties. A SME may consider implementing or may have already adopted a BYOD scheme for many reasons. Primarily however, it is utilised to increase mobility, flexibility (Citrix, 2012) and general employee satisfaction, theoretically leading to increased productivity (Rege, 2011).

Whether this theory works in practice depends on a number of factors but like all schemes, the way it is managed and applied generally dictates the level of success a SME will experience. Never-the-less, this is a scheme that more and more organisations of varying sizes are adopting and allocating a substantial amount of their budget and resources towards. In fact on average, 61% of global organisations now claim that the majority of their employees use their own personal electronic mobile device(s) in the workplace (Qing, 2013). Ponemon reported that over the last four years the growth in organisations adopting a BYOD strategy has increased by 73% (Ponemon Institute, 2012) and it is predicted that up to 90% of organisations will be encouraging employees to use their own electronic mobile devices and supporting the use of corporate software applications on those devices by 2014 (Rege, 2011).

One employee based in Singapore recently confessed that his SME is embracing the BYOD strategy and have moved their e-mail and other online services to the cloud using Google Apps, benefiting both employees and the company as only one device per employee is required to access both corporate and personal apps (Qing, 2013). This is just one of many positive effects experienced by SMEs and larger corporations alike (Qing, 2013) with profit increase and employee satisfaction, the two primary goals of BYOD being recorded by the majority of companies surveyed (Qing, 2013).

III. CONSIDERATIONS - IMPLEMENTING A BYOD SCHEME

As mentioned previously, there are many factors that contribute towards a BYOD scheme being implemented successfully and each of these possesses their own complex and sometimes hidden implications for which a SME must define a strategy to overcome (Rege, 2011). As with any business decision, financial cost is at the forefront of any consideration and this can have a huge effect on the sophistication of an organisation’s IT security capabilities which change dramatically when BYOD is introduced, as discussed later on in the article. It is important therefore that such costs are accounted for in the company’s budget. On the flip-side however, it is also necessary to point out that
hardware costs must also be incorporated into this budget (Lo, 2013), as these would decrease somewhat if the SME is not required to purchase devices such as laptops, PCs, mobile phones and mobile data plans. The legal aspects, application management and employer moral should also be considered.

One stumbling block with regards to the introduction of corporate software applications for use on mobile devices is that it can pose its own security and supportability issues for IT departments (Rege, 2011). The trend of employees using their own mobile phones and smart phones in particular is unstoppable and the user is essentially taking control of the company’s security program (Martin, 2012), a situation that should be addressed by developing relevant security policies and/or updating existing company policies (Navetta, 2012a) to help protect both the company’s network and legal rights. Even with such policies in place however, the IT department is faced with the task of ensuring company software applications work with multiple operating systems on a range of device models (Qing, 2013) as employees will inevitably choose a device they are familiar with but not necessarily what the company’s IT department have come across before (Lev-Ram, 2011). Companies such as Mobile Iron have developed software offering assistance to IT departments plagued with such security issues which allows them to manage, secure and track a range of wireless devices across all the major operating systems (Lev-Ram, 2011).

A. Legislation & Corporate Policy

Information security is acquiring more and more legislative risks (Kassner, 2013) and is an aspect that will only continue to increase at an arguably more rapid rate with the introduction of BYOD. Unfortunately for security professionals, this signals a requirement to defend their security decisions legally if required (Kassner, 2013) and so it is vital that SMEs analyze their existing security and privacy policies and if required, devise and apply new policies in order to reduce legal and liability risks (Navetta, 2012a).

A major concern for SMEs is the consistency between new BYOD policies and existing security and privacy policies (Navetta, 2012b). A mobile device security policy for example would normally include detailed requirements with regards to the security and configuration of a device (Navetta, 2012b). However, the standards required may not be achievable on personal devices (Navetta, 2012b) due to numerous reasons; device software and employee privacy to name a few. In this instance, a policy encompassing the requirements and expectations in relation to responding to security incidents and resulting investigations should be drawn up (Navetta, 2012b), allowing for prompt access to non-company owned devices in the event of a security breach (Navetta, 2012b) and setting out privacy guidelines depicting the type of instances that may require employees to hand over their personal device for investigation, examples may include audits, security incident response, forensic analysis and court orders (Navetta, 2012b).

Figure 1. SANS Mobility/BYOD Security Survey, March 2012

For a forensic analysis of a device, a full image of the entire device is taken and it would be extremely difficult, if not impossible to distinguish between the employee’s personal information and the company data requiring analysis (Navetta, 2012b). Therefore, the policy should incorporate the requirement of employees to provide all passwords and decrypt any stored data on their device if required (Navetta, 2012b). There is also a need for employee’s to be made aware that they may not have access to and therefore will not be able to use their device for the duration of the investigation (Navetta, 2012b). For such an incident to occur without prior warning of the consequences the SME would have no legal right to perform the investigation leaving the company vulnerable to further breaches.

Similar issues arise in the event that a personal mobile device containing company data is lost, stolen, retired, re-allocated, sold on or disposed of (Navetta, 2012b). An employer must be advised and agree to the policy declaring that, in such an event the organisation can lock, disable or completely wipe all data from their device, risking loss or corruption of their personal data (Navetta, 2012b).

Many SMEs find it difficult to implement policies to govern employee-owned devices (Qing, 2013) citing a lack of clarity and uneven application of existing, sometimes outdated policies as the main cause (Willis, 2013). Some even claim that employees are often unaware of relevant policies and openly violate them (Willis, 2013).

It is important that the policy drawn up by the SME states clearly that the use of their own device is voluntary and at their own risk (Navetta, 2012b). Their organisation are in no way responsible for any damage, data costs, data loss or corruption, contained software and loss of use or liability associated (Navetta, 2012b). It is also vital that any such policy includes a signed waiver/consent (Navetta, 2012b) evidencing the employee’s knowledge, understanding and acceptance of the terms set out clearly in the policy wording.

B. Security

The increase in use of personal electronic mobile devices
creates entirely new issues in respect to a SME’s IT security (Ayrapetov, 2013) adding to and in some cases, increasing the probability of existing security issues, such as malware attacks.

Generally, malware does not differ between small, medium and large organisations, posing the same risk regardless of the financial budget the company allocates to its network security infrastructure (Ayrapetov, 2013). One thing is for certain though, and that is attacks on company networks via mobile devices connected to them will become more sophisticated and executed more frequently in 2013 (Ayrapetov, 2013). The predominant reason for this being organisations adopting the use of social media applications such as, Facebook, Skype and Twitter (Ayrapetov, 2013). It is therefore important for companies to not only monitor and limit network use but also to do their utmost to eradicate other human elements of security. For example, setting up a 'sandbox' on personal devices ensuring company information on those devices is secluded from non-corporate data (Navetta, 2012b).

Bear in mind that not all implementers of the BYOD strategy will have to go to such lengths to protect their data. However, it is important for each company adopting the scheme to at least consider what data will be stored and transmitted on personal electronic mobile devices, how they will connect to the company’s internal network system (Navetta, 2012b) and also what the device or applications on it are permitted to do whilst connected (Martin, 2012). A decision can then be reached as to the level of security required for each device or all mobile devices across the board. This combination of Mobile Device Management (MDM) and Mobile Application Management (MAM) can then be incorporated into the SME’s main network security policy which should also be sufficiently designed to deal with today’s threats. Provided both MAM and MDM are executed efficiently, as per the policy your organisation create at the outset, secure access to relevant resources from secured devices at any location can be achieved (Martin, 2012).

An advantage SMEs have over larger corporations is that the more personnel an organisation employs, the more vulnerable their network is (Ayrapetov, 2013). However, it is also more likely that a SME do not have the IT infrastructure and budget that a large corporation has access to and may therefore be more susceptible to malware attacks (Ayrapetov, 2013). These very SMEs are also more likely to convince themselves that their current firewall setup is sufficient enough to protect them against today’s threats whereas, in reality old firewalls can leave a company’s network open to serious security threats (Ayrapetov, 2013). It is for this reason that your SME must develop an incident response plan to ensure that, if and when a security breach occurs sufficient measures are in place to tackle the consequences of the breach minimizing its overall impact. A recent poll taken by InfoSecurity Europe indicated that 64% of organisations do have an incident response plan in place (2013).

IV. CONCLUSION - A BYOD IMPLEMENTATION CHECKLIST

According to Dell SonicWALL customers, 68% of all businesses recently reported that their employees were unable to identify fraudulent attacks on their company’s network (Ayrapetov, 2013). In order for a BYOD strategy to be implemented successfully it is paramount that all employees are educated sufficiently so that they can recognize all types of potential threats (Ayrapetov, 2013). It is also important to make them aware of the potential repercussions of a security breach as, regardless of the size of your business these attacks could lead to not only loss of data but also loss of financial assets, productivity, profitability and even business continuity (Ayrapetov, 2013).

Employees should also be fully aware of company policies covering security, privacy and data protection amongst others. Making it compulsory for them to sign a waiver giving their consent for each policy would be an effective way to do this (Navetta, 2012b) and/or even incorporating it into their employment contract stating if policies are not adhered to disciplinary action could ensue if required. This ensures the company is covered legally, as any encroachment on privacy that could potentially ensue, for example in the forensic investigation scenario mentioned earlier in the article, would have been planned for and the plan would have been pre-agreed by all parties involved.

Having BYOD policies in place will only be beneficial if your SME can ensure the right applications are made available to their workforce (Qing, 2013). Software compatibility is also vital across a wide range of mobile devices in order for the BYOD theory to succeed in practice (Qing, 2013). A clear, well thought out MAM and MDM strategy executed by your IT department should remedy this, including setting up a ‘sandbox’ on personal devices ensuring company information on those devices is secluded from non-corporate data (Navetta, 2012b) and authentication management for each device, ensuring any device on the company network is indeed being controlled by the registered owner of that device (Martin, 2012). A log of IMEI, MAC or equivalent device identification would help to implement this (Martin, 2012).

If these suggested measures are put into practice there should be no reason why a SME can reap the benefits of BYOD ensuring employee satisfaction and increasing productivity as a result (Rege, 2011).
REFERENCES


How Secure is the Cloud?
Are SME’s reaching for the Cloud too quickly?

Andrew P Benson
University of Derby
Derbyshire, UK
A.benson1@unimail.derby.ac.uk

Abstract – As cloud computing becomes a major consideration for many SME’s in the 21st century; they should be asking one essential question, “What are the security risks involved with cloud computing?” This article looks at the growth of cloud computing usage and the failures of major cloud providers, over recent years. Whilst also informing the reader about the risks that SME’s should be aware of, and consider before venturing into the cloud.

Keywords – Cloud computing, security, risk, failures.

I. INTRODUCTION

Cloud computing in its simplest form as described by Lawlor (2012) is the facility to purchase computing power and data storage services via the internet, from third party providers. Which intern allows them to expand or contract as needed, rather than investing in their own data centres, servers or software.

Cloud computing has now been around for a number of years, with its underline concept being traced back to the 1950’s, when academia and some large corporations needed several clients to access the information on separate terminals. However it was not until 1999 when Salesforce.com became the first merchant to deliver applications and software over the Internet for client use (Prakash, 2012). Although other merchants were constantly launching their own cloud service it wasn’t until 2006 when Google launched Docs & Spreadsheets at docs.google.com, that cloud computing was really brought to the forefront of public consciousness (Biswas, 2010). This was further followed by other platforms such as Eucalyptus, OpenNebula and Windows Azure to name but a few.

II. BENEFITS OF THE CLOUD

It is understandable why the cloud computing business model offers many benefits to organisations; among the most attractive being lower upfront costs and increased agility. Also as an organisations growth exceeds their expectations they no longer have to predict server capacity; this can now be implemented in minutes rather than weeks (Lawlor, 2012). Salesforce (2013) believes the reason that so many businesses are now moving to cloud computing is to increases efficiency, can help them to improve cash flow, and offers many more benefits such as the following 10:

- Flexibility – more bandwidth & resources available upon demand.
- Disaster recovery – no longer need complex disaster recovery plans.
- Automatic software updates – suppliers do the server maintenance.
- Capital Expenditure Free – pay as you go, so there’s no need for capital expenditure at all.
- Increased collaboration – allow all employees wherever they are to sync and receive critical updates in real time.
- Work from anywhere – as long as employees have internet access.
- Document control – cloud computing keeps all the files in one central location.
- Security – data can still be accessed no matter what happens to a machine.
- Competitiveness – the cloud grants SMEs access to enterprise-class technology.
- Environmentally friendly – only use the server space they need, which decreases their carbon footprint.

Essers (2012) says as more and more government agencies and global businesses are starting to see the appeal in cloud services, the reliability of the provided services as never been as important, especially when the systems are mission critical.

III. CLOUD USAGE GROWTH

The number of businesses looking to cloud solutions has not only seen an increase over the last 12 months, but those making the switch are also a variety of different organisations. This can be clearly seen as a sign that cloud computing is now firmly hitting the mainstream, and that is no longer the mainstay of just technologically minded businesses (Kaderer, 2013). And as Dwight Klappich Vice President at Gartner Research explains that cloud services are now becoming more central to the running of business operations, much of this increase is due to trust that mangers are having in the cloud. Klappich also states that decision makers within business are beginning to see the benefits and consistent service such systems could offer, and that security and downtime are becoming less pronounced. “Two or three years ago when we talked to shippers about software, the cloud was just one option,” Klappich told onlinetech.com. “In many cases, cloud has now become a preference for companies.”
Cisco (2012) in a recent report of global data centre and cloud-based IP traffic, forecasted that there will be a significant increase in the usage of cloud data centre workload, compared to the increase in traditional data centre workload over the coming years. This growth of workloads in cloud data centres will be five and a half times that of the growth in traditional workloads between 2011 and 2016 (Figure 1.).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional data centre workloads</td>
<td>49.8</td>
<td>53.1</td>
<td>58.3</td>
<td>63.7</td>
<td>66.7</td>
<td>68.5</td>
<td>7%</td>
</tr>
<tr>
<td>Cloud data centre workloads</td>
<td>21.3</td>
<td>33.5</td>
<td>49.7</td>
<td>67.9</td>
<td>88.4</td>
<td>112.1</td>
<td>39%</td>
</tr>
<tr>
<td>Total data centre workloads</td>
<td>71.1</td>
<td>86.6</td>
<td>108.0</td>
<td>131.6</td>
<td>155.1</td>
<td>180.6</td>
<td>20%</td>
</tr>
<tr>
<td>Cloud workloads % of total data centre workloads</td>
<td>30%</td>
<td>39%</td>
<td>46%</td>
<td>52%</td>
<td>57%</td>
<td>62%</td>
<td>NA</td>
</tr>
<tr>
<td>Traditional workloads % of total data centre workloads</td>
<td>70%</td>
<td>61%</td>
<td>54%</td>
<td>48%</td>
<td>43%</td>
<td>38%</td>
<td>NA</td>
</tr>
</tbody>
</table>

Figure 1. Workload Shift from Traditional Data Centre to Cloud Data

According to a recent Gartner report (Gales, 2013) the market for public cloud services is expected to grow to $131 billion worldwide in 2013, a rise of $20 billion from the 2012 figure of $111 billion. Gartner also predicts that $677 billion being spent between 2013 and 2016 on worldwide cloud services. Ed Anderson, research director at Gartner said "The continued growth of the cloud-services market will result from the adoption of cloud services for production systems and workloads, in addition to the development and testing scenarios that have led as the most prominent use case for public cloud services to date.”

IV. CLOUD COMPUTING RISKS

Cloud based hosted services can save on the expensive outlay for servers, licences, and maintenance, particularly for small businesses, however it is imperative that SME’s are aware of the possible risk when utilising the cloud. It is essential that organisations take an active approach to security and that all staff should know how to handle data appropriately; and what kind of risks to look out for and what to do if a breach does occur.

The Cloud Security Alliance’s (2013) notes that among the most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers, with their top nine threats to Cloud Computing in 2013 being:

Data Breaches – An organisation’s sensitive internal data falls into the hands of hackers or their competitors, breaches can happen if there are flaws in client applications or if a multitenant cloud service database is not properly designed.

Data Loss – There are numerous ways in which data stored in the cloud can be lost, and the prospect of permanently losing an organisation’s data is a terrifying thought. Malicious attackers, accidental deletion by the provider and natural disasters are all causes of possible loss of customer data.

Account or Service Traffic Hijacking – This can usually happen with the credentials and passwords being reused. If access is gained, attackers can manipulate data, return falsified information, and redirect your clients to illegitimate sites all by eavesdropping on your activities and transactions.

Insecure Interfaces and APIs – The security and availability of general cloud services are dependent upon the vendor providing security of these basic APIs. The design of these interfaces must be in a way that protects against both accidental and malicious attempts to circumvent policy, being fully encrypted for authentication and access control.

Denial of Service – User are prevented from using their cloud service has it is forced to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth by the attacker.

Malicious Insiders – These threats to an organisation can come from anyone who has or had authorised access to the network, system, or data, such as a current or former employee, contractor, or other business partner. This is normally undertaken by intentionally exceeding or misusing access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.”

Abuse of Cloud Services – This does not normally affect the cloud consumer, but is more of an issue to the cloud service provider. The processing power of the numerous cloud servers could be used in criminal activity, thus possibly raising a number of serious implications for those providers.

Insufficient Due Diligence – Organisations can sometimes rust into the promise of cost reductions, operational efficiencies and improved security, without having a complete understanding of the cloud service provider environment, applications or services being pushed to the cloud.

Shared Technology Vulnerabilities – When a piece of shared technology, such as a shared platform component is compromised, it exposes more than just the compromised customer -- it exposes the entire environment as the threat of shared vulnerabilities exists in all cloud delivery models.
V. CLOUD FAILURES

According to Bonderud (2012) the stalwart benefit of cloud technology is supposedly reliability, the ability to offer always-on service for SME’s. Cloud services have an average downtime of 7.5 hours per year, according to their own data, which amounts to an uptime of 99.9%. But whilst having a cloud uptime of 99.9% sounds like a great number, the costs associated with the 0.1% downtime, as shown in recent studies, are far higher than many administrators realise.

The International Working Group on Cloud Resiliency (IWGCR, 2012) showed in a recent report that between 2007 and 2012 there was a total of 568 hours of downtime across 13 well-known cloud services, which in turn had an economic impact of more than US$71.7 million dollars.

VI. DATA RESPONSIBILITY

Under the new EU data protection rules, data destruction and corruption of personal data are considered forms of data breaches and would require appropriate notifications.

Additionally, many of the compliance policies require organizations to retain audit records or other documentation. If an organization stores this data in the cloud, loss of that data could jeopardize the organization’s compliance status.

When it comes to Data Protection ENISA (2009) states that attention should be paid to choosing a processor that provides sufficient technical, security measures and organisational measures governing the processing to be carried out, and ensuring compliance with those measures.

ICO (2011) states that it is good practice for a senior, experienced person in each organisation to take overall responsibility for information governance.

It must be emphasised that the ultimate responsibility for data protection falls to holder of the information, and not the service provider.

VII. CONCLUSION

Stuart McClure has simple advice for companies that want to put their data in the cloud: Don’t do it. When it comes to security, the former chief technology officer of McAfee said choosing a safe service can be like “picking a dog with the least fleas.” (Robertson, 2013).

We must however remember that in some respects the cloud is still a maturing technology, but the impact it is having throughout the business world looks unstoppable.

There are plenty of issues associated with the cloud; downtime may stop a business from accessing critical files in time, thus forcing it to cease trading, but there are also great advantages to be taken; staff no longer need to be in the office to retrieve work-related documents, as this can all be done over the internet.

It seems there could always be continued problems in the cloud, but we should also expect to receive continued progress. As previously stated the cloud is still in its infancy, realistic expectations of trouble free cloud surfing may not be available in the near future.

So what is the solution to moving forward with the cloud? Whilst it may not be the answer that some people want to hear, the solution is to simply accept that it is here to stay. It is not being said that we should just accept anything, but that as anything in life, it is your responsible to make sure you understand the risk. This is the price of doing business in the cloud!
REFERENCES


Information Assurance

Pothole Detection

Adrian Brevett
University of Derby
Derbyshire, UK
100146498@unimail.derby.ac.uk

Abstract - Each year potholes have become an increasing problem for road users. The damage caused to vehicles that encounter these obstructions in the road will cost road users hundreds of pounds in repair bills, and will cost the Highway Departments in England and Wales millions of pounds in claims. Although a few software development companies have developed free downloadable applications (apps) for smart phone’s, in the attempt to crowd source data to allow local authorities to locate and repair potholes at a faster rate, these apps encourage users to hit the potholes in order to detect the location on the smart phone using accelerometers and global positioning system (GPS) sensors. This approach could potentially increase the amount of claims received by the local authorities as users of the application will attempt to hit as many potholes as possible. Therefore it is recommended that an improvement of the apps would be to allow road users to identify a pothole by using their voice, by saying a command such as ‘pothole’ to the smart phone, which will then allow road users to bypass the pothole but will still help authorities such as the Highway Departments in repairing the problem. The proposed improvements were critically analysed which lead to a conclusion that further tests would need to be conducted to insure the provided data was accurate.

Keywords - Potholes, GPS, accelerometers, crowd sourcing, voice recognition.

I. INTRODUCTION

A pothole is the result of water on the road which goes through a continuous cycle of freezing and thawing, which eventually causes the road surface to break up (Midlands Business News, 2013). The world’s population is always on the increase, which means there is an increasing load on the road infrastructure that will worsen the state of potholes (Rode, 2008). In 2012 there was an emergence of pothole detecting applications available for smart phone’s, which use the phone’s accelerometer to detect the hazard when the phone has been mounted in a vehicle. When a detection is achieved, the phone’s GPS (Global Positioning System) will locate the position of the pothole. This information can then be sent to local authorities to help them locate and repair the hazard with increased effectiveness. There are two areas in which pothole detecting apps such as Street Bump and Pothole Season could be improved which are to, 1) Allow users to detect a pothole using voice recognition. Currently the apps encourage users to hit a pothole which in turn could cause damage to the vehicle, as well as cause a number of serious accidents. 2) Provide visual feedback on the phone’s display in the form of a map, which shows previously detected potholes from users of the app. This feature will then act as an early warning system, in the same way a satellite navigation system displays an overlay of speed cameras on map. Currently pothole detecting apps show no more than a number count of the amount of potholes detected. If these two suggestions were to be put in place, road users will save money on repairing their vehicle from pothole damage, which has cost British motorists in the last year around £1 billion pound (Groves, 2013). The early warning system of displaying detected potholes on a map in the app, could reduce the number of accidents caused by hitting the pothole which could swiftly change the direction the vehicle was heading to, and could also prevent road user suddenly breaking or swerving to avoid the hazard which could also lead to a number of accidents. This paper will analyse possible implications that the suggestions may cause when using the crowd sourced data.

II. CURRENT POTHOLE DETECTION

The technology that smart phone’s now provide has allowed developers to develop apps (applications) that can detect potholes and there location. The apps such as Street Bump require the user to open the app before the journey and mount the smart phone in their vehicle; the app will then begin detection for the journey. The phone’s built in accelerometer algorithms are programmed to differentiate potholes from other road hazards such as manhole covers, speed bumps and rain drains (Doughty, 2011). The built in GPS (global positioning system) will then locate the detection that the accelerometer has made. This valuable information can then be sent to the local authorities’ central server, who will then be able to repair the potholes at a faster rate with increased efficiency and prevents the authorities from trawling miles of roads to find the hazards (Hardy, 2012). Although this information is then sent to local authorities, they will not take the bump seriously unless three separate detections are reported by three different users (Broviak, 2013).

III. IMPROVEMENTS

The two improvements suggested for the current pothole detecting apps are:

- Allow users to detect a pothole using their voice.
- Display previously detected potholes on a map.

This will prevent the need for the users of the app to deliberately hit a pothole which increases the chance of accidents and damage to the vehicle (Bertuca, 2000), and a
display of previous detected potholes on a map for the users to view as they drive will prevent any sudden braking or swerving due to identifying a pothole late which is potentially dangerous. Street Bump already uses this information on their website (see figure 1-1) which will be more useful if the users of the app had access to the information within the app, in the form of a satellite navigation map UI (user interface).

![Figure 1-1. The Street Bump webpage displays pothole location information.](image)

The data provided from these added features will need to be as accurate as the current detection methods or the information provided will be deemed as useless. Although the algorithms of the accelerometer are programmed to only detect potholes, the developers of the Street Bump app have found that of the first one hundred thousand bumps registered by the app “traditional potholes accounted for a stunningly small percentage. They were vastly outnumbered by misaligned castings” (Moskowitz, 2012) shown in figure 1-2.

![Figure 1-2. Sunk casting.](image)

Even though the location of the detection will be accurate, the detection may not always be a pothole which can also depend on the vehicles tire pressure and the stiffness of the suspension. Castings rarely damage a vehicle but they can often move several inches which leads to them being surrounded by cracks, and causing road users’ problems (Moskowitz, 2012). This has lead to some road maintenance services repairing castings thanks to the Street Bump app, which in this case the false information has lead to the problem of castings, which has been overlooked for years, now being identified and repaired. Using the voice recognition method increases the chances of providing false information to local authorities. If a road user identifies a pothole and the system doesn’t recognise the command, it could mean the user will have to repeat the command until the system recognises it and plots the position on the map. The more attempts for the system to recognise the command, the less accurate the data. The same inaccurate data could also be provided if the voice recognition system takes too long to process the command. A comparison of two systems were compared (see graph 1) on the accuracy of the data which could be provided if one system took two seconds to process a command, and the other took eight seconds.

![A graph to show how many feet are travelled at various speeds](image)

If the system was to take eight seconds to process the location of the user, the accuracy of the identified hazard could be as much as eight hundred feet away from the actual pothole, assuming that the vehicle is travelling at the national speed limit in Britain of seventy miles per an hour. The accuracy of a system that processes the users location within two seconds of the voice command, considerably improves the accuracy and reliability of the information provided. The users’ location pinpoint will be processed within two hundred feet of the command being spoken when travelling at seventy miles per an hour. Ideally the voice controlled system will process the voice command at the same speed that the location is marked using the accelerometer method.

**IV. GPS Accuracy**

The method of using accelerometers to detect a pothole is a quick process due to the fact that the sensor is tightly linked to the GPS (global positioning system); the process from the accelerometer detecting the pothole to the GPS locating the incident is almost immediate. Although the process is fast it is not guaranteed that the location of the incident will be accurately portrayed when it is shown on a digital map. Satellite navigation systems are usually accurate to ten meters or so in good conditions, but that accuracy decreases in other conditions such as urban settings where there are buildings that block and reflect signals, which can lead to GPS accuracy being off by over fifty meters (Ray, 2013). Users of satellite...
navigation systems could have passed their next turning or when relying on the overlay of speed cameras could potentially have already passed the camera if the conditions are not optimal, which could have the same effect with the pothole detecting apps using either the accelerometer or the voice recognition method. Researchers have recently developed a navigation system which improves accuracy of GPS location down to two meters, and they plan to use the technology in smartphones by taking advantage of the sensors already built in to the phone such as accelerometers, a gyroscope, a magnetometer, GPS, cameras, Wi-Fi, Bluetooth or GSM (Global System for Mobile) communications (Osborne, 2013).

V. Threshold

An advantage with the voice recognition system compared to the accelerometer detection method is that the voice system can detect a pothole at any speed, which includes when the vehicle is stationary. Currently Street Bump specifies that their app has a threshold of five miles per an hour to prevent false data being recorded (City of Boston, 2013), anything recorded whilst travelling below the threshold speed will not be taken as a serious detection by the authorities in case a user manages to falsely detect a pothole. An example scenario is if the Street Bump app has been left running after a journey and the user drops their Smartphone, which could trigger the accelerometer to make a false detection. It is also unlikely that the accelerometers will detect a pothole below the threshold speed.

Although the voice recognition can detect a pothole at any speed, the authentication of the detection will be difficult to analyse. The voice detection method will not restrict potential detections to just being on the road, as it would not be difficult for users of the system to run the app in any location and provide false detections. Therefore a detection should not be taken seriously by the authorities unless a certain amount of detections are identified in the same area, by different users of the app (Schwartz, 2012). If the threshold was not put in place, the authorities would waste masses of time travelling to repair the false detections; and if the suggested early warning system plotted a pinpoint on a map for the detections that did not have a threshold in place, the data will be deemed as useless.

VI. Prioritise Repair

The pothole data provided by the app regardless of being the voice recognition or accelerometer method could also be prioritised for repair. If a date and time stamp was to be provided with each detection made, the authorities will be able to see which detections are more popular. If a detection of the same area is being made once a day compared to once a week, then it is logical that there will need to be priority in repairing the detection that is being provided daily. The accelerometer method can have further information tagged to its detections which will make the data more authentic, which is a graph that provides detail of a users’ journey (shown in figure 1-3).

When the Street Bump app was in beta, the data it provided was a graph which shows the user’s trip (Toor, 2011). The developers were able to identify the severity of each detection from using the information provided. Whereas the voice recognition method would only be able to use the date and time stamp for help with prioritisation.

VII. Conclusion

The current method of detecting a pothole using accelerometers and GPS will increasingly damage the users’ vehicle, which will not only lead to expensive repair bills, but could also provide the already cash strapped local authorities with a problem in the form of compensation claims (Birch, 2010). The voice recognition method could be an improvement on the current app to provide users’ with the option of detecting the pothole, and reducing vehicle damage which will then lower the amount of compensation claims being applied for to the local authorities. The assurance of information provided to the authorities needs to be as accurate as possible, particularly if the data is to be overlaid on to a map within the app as an early warning system for users. There is a danger that the voice recognition method could provide useless information as there is no restriction to when a user could falsely detect a pothole, which could include using the app in buildings, which is why a threshold would be an important feature. The voice recognition process will need to be as quick as the process of the accelerometer detecting a hit and locating the position, but with GPS accuracy being accurate from ten meters in good conditions to over fifty meters in poor conditions (Ray, 2013), users of the app will need to be aware not to be fully reliant on the data provided.
REFERENCES


BYOD: Can It Harm Your Business?
A Mobile Device Based Study
Cal Gladyng
University of Derby
Derbyshire, UK
100108955@unimail.derby.ac.uk

Abstract - With 77% of companies stating that mobile devices are a critical part of their business and with the rise of “Bring Your Own Device” (BYOD) in the workplace, securing a company network has never been tougher. So much so that 41% of data loss is due to insecure mobile devices. Though, by implementing well thought-out policies and rules that limit the use of a BYOD device in the workplace and offer staff training on how and why policies are important, you can better protect your company from such threats.

Keywords - Bring Your Own Device, BYOD, Security

I. INTRODUCTION

This paper will delve into several sections surrounding the topic of the ‘Bring your own device’ (BYOD) trend that is being seen more and more in Small to Medium Enterprises (SMEs). It will look into what BYOD is, why it is so popular with companies in this modern era and the rise it has taken in the past few years. It will then move on to discuss the security issues surrounding companies that employ the use of BYOD, looking into the types of threats it can open up as well as how many companies are being affected. Possible solutions will then be considered to help secure a company from the types of issues raised.

II. WHAT IS BYOD?

BYOD is a scheme that a company adopts, allowing its employees to bring in and use their own private mobile devices for their job (Scarfo, 2012). What this means is that, this one device would not only carry the individuals personal data but also their work data (Scarfo, 2012).

77% of companies surveyed by Ponemon (2012) stated that a mobile phone is critical in its ability to accomplish its everyday business needs (Ponemon, 2012).

A. The Rise Of BYOD

Looking at figure 1 it can be seen that there has been a steady rise in businesses allowing BYOD in the workplace (Aberdeen, 2012). With the growth from 10% to 83% in just four years, it is clear to see that BYOD is on the increase (Aberdeen, 2012).

![Fig. 1. The permittance of BYOD from 2008 – 2012 (Aberdeen, 2012)](image)

B. Why Has It Risen?

From statistics shown in Figure 2 it can be seen that BYOD has a firm foot in the door. Yet why has this trend risen and why so fast?

One of the highest contributing factors is that employees are calling out for it (Afshar, 2013). This is because they do not have to learn how to use the latest mobile operating system as they are just using a familiar system on their own phones (Miller, 2013). Considering that they have undoubtedly invested a lot of time and research into picking the right device for themselves. Being forced to use a phone that is foreign to them could build up reluctance to use it (Miller, 2013). Since they would have to invest more time into learning the new device’s system (Miller, 2013).

Another reason is that it means that the employee does not have to carry around two devices, their work and personal phone (Weber, 2013). Since this would become one phone when using a BYOD approach, meaning that they only have to remember to pick up one phone when they leave the house and give out only one phone number when required (Weber, 2013).

Another factor from the company side and not the employee is that with using the BYOD scheme, companies do not have to front the cost of the device or the data plan (Miller, 2013). It also frees up time for management as they do not have to spend valuable time pushing permitted devices on their employees (Miller, 2013).

![Fig. 2. “Is BYOD use Allowed” (SANS, 2012)](image)
III. THE ISSUES SURROUNDING BYOD

With the rise in BYOD, the precaution to make sure that the company’s data is kept safe has never been trickier (Smith, 2013). Furthermore, with 41% of data losses being due to insecure mobile devices it can be agreed that companies need to secure their networks when implementing BYOD (Ponemon, 2012).

Looking at figure 3, which was produced by Ponemon (2012), it shows a breakdown of what type of security issues arise due to insecure mobile devices.

![Fig. 3. Consequences of a mobile device data breach (Ponemon, 2012)](image)

From these statistics it can be seen that the most common consequence due to a mobile device data breach is the theft, removal or loss of information and/or resources (Ponemon, 2012).

Another takeaway from this graph is that mobile data breaches are a real and serious threat that can have grave consequences (Ponemon, 2012). A further survey undertaken by F-Secure (2012) helped show that the largest mobile threat by type, in the 4th quarter of 2012 was a Trojan attack, accounting for 53% of all cases (F-Secure, 2012).

The types of data that can be retrieved through access to an insecure device that is being used in a BYOD scheme is as follows:

<table>
<thead>
<tr>
<th>Types of data</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic information</td>
<td>• Mergers</td>
</tr>
<tr>
<td></td>
<td>• New product</td>
</tr>
<tr>
<td>Tactical information</td>
<td>• Plan for organisation change</td>
</tr>
<tr>
<td></td>
<td>• Proposal to client</td>
</tr>
<tr>
<td>Network or computing infrastructure information</td>
<td>• IP address scheme</td>
</tr>
<tr>
<td></td>
<td>• Primary mail servers</td>
</tr>
<tr>
<td>Personal information</td>
<td>• Credit card numbers</td>
</tr>
<tr>
<td></td>
<td>• Passwords</td>
</tr>
</tbody>
</table>

*Table A. Types of data that can be stolen from an insecure mobile device (Course Technology, 2011)*

From Table A, it is possible to see that very important and private data can be retrieved from an insecure mobile device (Course Technology, 2011). This paper will now take a deeper look into what way breaches like this can occur and how much it could cost your business.

A. A Lost Or Stolen Device

If a mobile device was stolen or lost, which was part of a BYOD scheme, not only the personal data stored on the device could be compromised but also any work secrets or proprietary information.

If the lost/stolen device uses a weak or does not implement the use of a password, this could assist in the (Perakovic, 2012):
- Possibility of a data breach (Perakovic, 2012)
- Loss of the company's intellectual property and/or other secrets (Perakovic, 2012)
- Loss of the employee's personal data. (Perakovic, 2012)

B. Malware

Malware is a program purposely built to install hidden files, damage/steal data stored on the device and/or retrieve access credentials (which the user uses to gain access to confidential systems) (F-Secure, 2012).

If the infected device is then connected to the company infrastructure, say via a wireless connection, the malware could move from the infected device to the corporate network, where it can wreak havoc on the company's computer systems (Miller, 2013).

C. Not Having Policies In Place To Handle BYOD

With 31% of the companies surveyed by SANS (SANS, 2012) saying that they do not have policies in place to handle BYOD and a further 26% stating that they only “sort of” have policies, it is possible to see how unsecure mobile devices are infiltrating corporate networks.

With only 14% of companies feeling that the policies that they do have in place are very thorough (SANS, 2012) and 49% feeling that their policies catch some basic threats or none at all (SANS, 2012). It can be seen that policies are a large issue that companies need to be addressing.

With regards to implementing policies, there are many challenging questions facing a company, as they do not actually own the mobile device, for example: If the device is compromised what is the company legally allowed to do with the phone? (SANS, 2012) Is it right for a company to image a personal device? (SANS, 2012) Or determine what applications can and cannot be installed on a personal phone? (SANS, 2012) If a phone were to be imaged, what would be the procedure with regards to looking at the personal data that could be discovered? (SANS, 2012)

With all these complex issues it is easy to see why so few companies have policies in place.

D. The cost of a Breach

This paper has discussed what possible breaches could happen if an insecure mobile device was to enter a company network but how much could it cost your company financially if you were to have a breach?
During 2010 in the UK the average cost of a lost or stolen record was £71, which rose to £79 in 2011 (Ponemon, 2011). The cost would not be just financial, as time and research would be required to fix the breach. As well if the breach was to be revealed to the public your company’s reputation would be hurt (Thomson, 2012).

IV. WAYS TO SECURE YOUR BUSINESS WHEN USING BYOD

This section will look into ways to protect your company against possible exploitation via insecure mobile devices when implementing a BYOD scheme.

A. Building Dedicated Policies

Dedicated mobile device policies should be devised and implemented across the corporate network (British Standards Institution, 2005). They should cover; access controls, physical protection, encryption, backups, and use of anti-virus software (British Standards Institution, 2005).

They should also fully cover rules in addition to giving advice as to how the user can connect their mobile devices to the corporate network (British Standards Institution, 2005), together with how the device should be used in public places (British Standards Institution, 2005).

The employees should also be involved in designing such policies so that they understand the reasoning behind them (Bradford Networks, 2012).

These policies should then be broken up to serve the employees in different roles of the company. For example, one set of policies for a group that does not deal with confidential information and another for those that do. This can then determine what is allowed on one device and not on another (Bradford Networks, 2012).

B. Knowing Who And What Is On Your Network

A system should be put in place in which a user must register their device with the company’s IT department before it can access the corporate network (Bradford Networks, 2012).

They should not only register their name, make and model of their device but also its unique identifier, such as its MAC address (Bradford Networks, 2012). This can then be used to grant access to the network (Bradford Networks, 2012).

The mobile device should then only be allowed to access the network during that particular employee’s time of work (Bradford Networks, 2012). For example, if an employee works from 9am to 5pm, the device should be allowed on the network from 8am to 6pm and disallowed any time before or after that.

C. Knowing What Is Installed On The Device

A list of authorised and unauthorised applications that can be used on the device should be drawn up (Bradford Networks, 2012). This will help keep unsecure devices from accessing the network (Bradford Networks, 2012).

The company’s IT department should also implement a Mobile Device Management (MDM) tool (Bradford Networks, 2012). This tool can then be used to enable access to certain applications on the device when on the corporate network (Bradford Networks, 2012).

It should also be used to show if a device has been tampered with e.g. jail broken or rooted. Depending on what policies have been chosen, the tampered-with device can then be revoked access to the network (Bradford Networks, 2012). This helps to protect from a phone that has privileges to access the network but could now contain malware since it had been tampered with and so should not be allowed access to the network.

D. Rules For Use In Public Places

Protection should be put in place to help protect a mobile device in a public place; this should help avoid unauthorised access to the information stored on the device (British Standards Institution, 2005).

This can be achieved by encrypting the data through a VPN or SSH tunnel (Dasgupta, 2004).

E. Keep The Device Backups Safe

Any backups of the device should be encrypted to help ensure that they have protection if the backup is lost and/or stolen (British Standards Institution, 2005).

F. Train Your Staff

Compulsory training should be developed and implemented, in which the main goal is to raise awareness of the risks and issues regarding the use of mobile devices. (British Standards Institution, 2005). Teaching, not only the rules of the BYOD scheme within the company but also best practices to stay safe when away from work.

G. Rules About Who Has Access To The Device

Rules about who else has access to the mobile device should additionally be created. They should state that any mobile device that carries sensitive and or confidential company information should not be left unattended and locked away if need be (British Standards Institution, 2005).

Rules that take family and visitor access to the device into consideration should also be developed (British Standards Institution, 2005).

V. CONCLUSION

This paper has shown that there has been a big rise in the acceptance of BYOD schemes in companies and that with this rise there is now serious security concerns surrounding the scheme. From the loss or theft of company data via a lost or stolen device to companies not implementing mobile policies to help secure against such threats. By following the seven ways laid out in section IV “Ways To Secure Your Business When Using BYOD”, you can better protect your company from any unwanted attacks, saving you time, money and your reputation.
REFERENCES


The Threat From Inside

David Hall
University of Derby
Derbyshire, UK
D.Hall5@unimail.derby.ac.uk

Abstract—Insider attacks are those carried out by employees, students or contractors who use their position on the inside of a business as an advantage in compromising. This paper identifies the different type of insider attacks, gives a background on their prevalence, and outlines a method, based on the International Standards Office (ISO, 2007) 27001 series of best practices, that small to medium-sized businesses can use to protect themselves against them.

Keywords - Security, Business, Malicious Insider, ISO217001.

I. INTRODUCTION

Small and medium-sized enterprises (SME’s) go to a great deal of trouble to protect their perimeter; they employ firewalls, anti-virus software and, in some cases, even intrusion detection systems (IED’s), but according to a white paper by CISCO (2008) they may be leaving themselves vulnerable from the inside. It described protecting the perimeter as a ‘good start, but not enough,’ then went on to highlight the fact that ‘many information thefts’ are assisted by a ‘trusted insider, such as an employee or contractor.’ The paper also revealed worrying statistics to suggested that, despite being somewhat concerned about the insider threat (with ‘thirty-nine percent’ of IT professionals more concerned about the threat from their own employees than outside hackers), many businesses aren’t taking the necessary steps to actively protect themselves against the threat from inside. Ruppert (2009) described how many companies ‘still tend to rely on audit logs after the insider attack has occurred instead of focusing on developing tools and techniques for analysing and solving the actual problem.’ This paper defines the different types of insider threats currently known within the security industry, reports on their prevalence and identifies ways in which small to medium size businesses can protect themselves against them.

II. BACKGROUND

In order to protect themselves adequately against them, it is imperative for SME’s to know what an insider attack actually is, including the different variations within the scope of the insider threat.

Initially, Stoflo, Bellovin and Hershkop (2008) give the definition of an insider as a trusted employee, student or contractor that is given a higher level of trust than an outsider; this trust is usually established through ‘some means of authentication followed by authorization to internal assets.’ This definition of an insider is widely enduring, with CISCO (2008), IBM (2006) and Maybury, et al (2005) all giving similar definitions. What separates the different types of insider attacks, Ruppert (2009) argues, is the motivation of the insider.

A. The Motives of an Insider Attack

There are various motivations that drive an insider to become a threat to a business, however not all of them are criminal. Ruppert (2009) identifies motivations that arise from innocent intentions, such as an employee sending a confidential e-mail to the wrong person, or an employee trying to accomplish a needed task: ‘for example, in a case in which the system does not support a particular action or the insider is blocked from accessing certain data, the insider may try workarounds to accomplish the same thing.’ These incidents are relatively innocent, however they could still leave the business vulnerable to attack. Other, similarly innocent, motivations include insiders trying to experiment with a system to improve it, or checking the system for errors and vulnerabilities with the aim of reporting them once they have been discovered so that they can be fixed.

Despite the chance of inside threats arising from innocent intentions, the large majority occur through malicious motivations; according to Randazzo, et al. (2004), eighty-one percent of insiders were motivated by financial gain, for example, while CISCO (2008) discovered that an alarming ‘eleven percent’ of employees had ‘accessed unauthorized information and sold it for profit, or stole computers.’ These kind of attacks can be defined as malicious insiders, as their intentions are to inflict harm on a business or organisation for some kind of personal gain. Another prevailing motivation is sabotage; Cheung (2011) outlines the issue of employees who have been recently ‘demoted, fired or formally reprimanded,’ and then attack after they have left the company. These malicious insiders can be further defined as disgruntled employees, and Silowash, et al (2012) described the insider threat field as being ‘increasingly dominated’ by professionals who steal information for sale and disgruntled employees who damage systems or steal information for revenge.

B. The Prevalence of Insider Attacks

The Ponemon Institute (2011) discovered that criminal insiders were the second most common type of malicious attack to businesses during the year, second only to the viruses, malware, worms and trojans group. Their study found that malicious insiders caused thirty-three percent of the attacks experienced by the eighteen companies they surveyed. A CyberSecurity Watch Survey (2011), meanwhile, on a larger scale, found that two-hundred and twenty four companies,
fourty-three percent of their respondents, had ‘experienced at least one malicious, deliberate insider incident in the previous year.’ These statistics suggest that insider attacks are a real threat to businesses, and the large sample sizes used in the surveys, including both small and large businesses, highlight the fact that small businesses are not immune from the threat. Indeed, a report by TrendLabs (2012), specifically on threats to small and medium-sized businesses, comments on the negligence shown by small businesses (usually because they do not think the threat applies to them): ‘this negligence puts critical business data at risk from data-stealing cybercriminals and malicious insiders.’ The numbers given so far may also be higher than reported, as the methodology used in these studies were surveys, and businesses may not have wanted to report an attack in fear of damaging their reputation, or because they wanted to keep it internal; another CyberSecurity (2010) survey, for example, found that seventy-two percent of insider incidents are ‘handled internally without legal action or the involvement of law enforcement,’ which suggests that the extent of criminal insider attacks may actually be higher than the public perceives.

Despite the tendency for businesses to keep information on insider attacks private and choosing to deal with them completely internally, as already identified, there have been many malicious insider incidents reported in the press. Kerr (2012), for example, reports on an incident where Alan Patsmore, the general manager of Zynga – a successful social-gaming company – stepped down from his position, but ‘nabbed data files, financial information, unreleased game design documents, and more’ before he did so, by transferring them all to his own personal Dropbox account. Zynga then filed a complaint to try and stop him from giving the information to other, rival companies. Another example is given by Thomson (2011), who described an investigation into Indian call-centre staff which discovered that some of them were selling UK broadband customer’s financial data, ‘including credit card numbers and security codes’, for as little as ‘twenty-five pence’ each for bulk purchases.

As well as being a highly common form of attack, research also suggests that insider attacks are, on average, more expensive and take the longest time to recover from; the Ponemon (2012) report found that insider attacks had an average recovery time of 57.1 days, longer than malicious code, denial of service, viruses or any other type of attack. Silowash, et al (2009) argues that this increased recovery time is because insiders ‘have a significant advantage over others’ because insiders are not only ‘aware of their organization’s policies, procedures, and technology,’ but also ‘aware of their vulnerabilities or exploitable technical flaws,’ which effectively means that they can penetrate deeper and afflict more damage to the system.

III. PROTECTING AGAINST INSIDER ATTACKS

There are many suggestions within the security industry as to how small to medium-sized businesses can protect themselves against the threat of an insider attack; suggestions such as Silowash, et al (2009), IBM (2006), Ruppert (2009), and Stolfo, et al (2008). Although there are some differences between them, with each of those identified offering differing perspectives, there is a common theme amongst them: the theme that, in order to properly protect themselves from the threat of insider attacks, small to medium-sized businesses need to implement a layered defence strategy, consisting of multiple policies, procedures and technical controls. As highlighted by Ruppert (2009), this means that there is no quick fix for businesses defending themselves from the threat of an insider attack.

A. The ISO 27001 Standard

Interestingly, many of the policies, procedures and technological controls identified by experts within the industry fall in line with the International Standards Office (2007) 27001 standards; the ISO/IEC 27000 series provide sets of best practices for developing and maintaining security standards and management practices within an organization.

The first step in protecting against malicious insiders, for example, is given by Ruppert (2009) and Silowash, et al (2009) as identifying and classifying assets within the organisation. This is also the third code of practice within the ISO 27001 standards: ‘Assets clarification and control.’ This process involves categorizing assets and maintaining an inventory of them, then ensuring that every asset receives an appropriate level of protection. Ruppert (2009) highlights the importance of ensuring that the only employees who have access to each asset are the employees that absolutely need to. Silowash, et al (2009) also identify another practice as ‘Beginning with the hiring process, monitor and respond to suspicious behaviour,’ and this practice also comes under the ISO 27001 policy of ‘Personnel security.’ The ISO standard describes policies such as ‘pre-employment screening,’ that help to ensure any new employees or contractors are suitable for their job, and Silowash, et al (2009) concurs with this. They noted a case study in which an organisation employed a contractor, the contractor’s company told the hiring organisation that a background check had been performed on him, and the contractor later ‘compromised the organisation’s systems and obtained confidential data on millions of its customers.’ It then emerged that the contractor had a ‘criminal history of illegally accessing protected computers,’ thus emphasizing the importance of proper background checks by the hiring organisation themselves.

These were just two examples of the similarities between the ISO 27001 series and the suggested methods of protection within the security industry. Other examples include Cappeli, et al (2009) suggesting a practice of ‘clearly documenting and consistently enforcing policy controls,’ alongside the similar ISO practice – ‘Information Security Policy,’ and Stolfo, et al (2008) outlines more technical methods of protection such as restrictions on access, which falls in line with the ‘Access control’ section of the ISO standard. All in all, the clear similarities between preventative measures recommended within the industry and the policies and procedures set out by the ISO standards, suggests that in order to protect themselves properly, an SME should implement the ISO standards as fully as they can.
The full set of ISO 27001 standards include:

1) Information Security Policy
   This ensures that the management of a business enforces a proper security policy, which is regularly assessed and updated. It should contain: the overall objective and scope of information security, including goals and principles, as well as defining responsibilities and an explanation of the process for reporting security incidents.

2) Security Organization
   This involves properly assigning responsibilities to the right members of staff, maintaining the security of assets accessed by third-parties and establishing a management approval process for new IT facilities.

3) Assets Clarification and Control
   The first stage of this is collecting an inventory of all business assets. These assets should then be classified; in terms of physical or information assets, for example, and appropriate levels of security assigned to them, depending on how crucial they are to the business’s system.

4) Personnel Security
   One of the main aims of this process is ensuring all employees are suitably aware of their security responsibilities. Another important aspect of it is the ‘Responding to Incidents Objective’ (ISO, 2007), which includes establishing a proper reporting and discipline process for security incidents.

5) Physical and Environmental Security
   This involves the physical security of the business, such as the security of data centres and computer rooms, the physical perimeter, and the handling of business data and software.

6) Computer and Network Management
   The aim of this process is to ensure the correct and secure operation of computer and network facilities. This includes segregation of duties, documented operating procedures and incident management procedures.

7) System Access Control
   This standard centres around controlling access, implementing technical restraints such as privilege management and user registration, as well as monitoring techniques such as event logging and clock synchronisation.

8) System Development and Maintenance
   This standard ensures that security is built in to any business IT systems. It outlines security requirements analysis and specification, as well as validation and authentication of any data used by the business. It also overviews the security of any IT projects and the security of application systems software and data.

9) Business Continuity Planning
   The main objective of this standard is to ensure the business has a system in place to keep the business going if anything goes wrong; it aims to back up the essential systems and processes of the business, maintain its resilience and flexibility in the process.

10) Compliance.
    The final standard is compliance. This ensures that the business avoids breaches of any legal obligations it may have to adhere to, as well as reviewing systems within the business, ensuring that they comply with the security policy of the business and technical compliance checking.

Cappeli, et al (2009) also describe how this defence strategy should be implemented in line with an appropriate corporate culture, one that remains vigilant to the threat of an insider attack: ‘Management must look beyond information technology, to the organisation’s overall processes and the interplay between those processes and the technologies used.’ This suggests that if a small or medium sized business wants to be truly protected against the threat of an insider attack, they should not just implement some areas of the ISO 27001 code of best practices, but all of them, as part of an overarching corporate culture that ensures both awareness and vigilance to the threat of an insider attack.

IV. CONCLUSION

Initially, this paper defined an insider attack before providing a background to its prevalence and motives. It then identified the best way in which small or medium sized enterprises can protect themselves against them. Although Cheung (2011) suggests that a business can never be completely secure from the threat of an insider attack, the defence strategy identified in this paper – namely a full implementation of the ISO 27001 standards – can help to guarantee that a business reduces the chances of an insider attack to an absolute minimum, while ensuring that if it does fall victim to one, it is in a suitable position to recover quickly and efficiently with a minimal cost to its system and processes.
Bring Your Own Device

The Employee and Business Perspective

James Hanify
University of Derby
Derbyshire, UK
100200810@unimail.derby.ac.uk

Abstract - Bring your own device is a result of consumerization of IT and the result is the increasing use of our personal mobile devices for both business and private use. Businesses are in a delicate situation where employees are embracing technology and want to use their own device to work and use but must keep data safe for compliance reasons. This will ultimately lead to some conflict between both sides with each having their own valid reasons for wanting to use their device in a particular way. This paper proposes and explores some of the issues in the two-sided debate to show the concerns, and some suggestions as to not only ensure that organisations can bring in the new generation of talent but by taking advantage of BYOD, it will reduce the overall risks for the business and be able to take advantage of new-found knowledge in the form of their employees.

Keywords - BYOD, Compliance, IT, Security

I. WHAT IS BYOD?

Bring your own device or better known as the acronym, BYOD, is used to describe mobile workers bringing in their own mobile devices e.g. tablets and tablets with their own applications and data into the workplace for both personal and business use (Scarfo, 2012). It is a trend, which has come about due to the power and flexibility of our handheld smart devices, allowing us to have access to corporate information as well as our own (ICO, 2013).

This creates a problem since the device has not been configured by the company’s IT department (Mansfield-Devine, 2012) and therefore will vary in their security. This could potentially cause an issue when complying with data protection obligations (ICO, 2013) since mobile devices connected to the organization’s network, poses a significant threat to the accessing of sensitive data (Morrow, 2012). Likewise, it is possible for sensitive data to be transferred to personal devices and once that happens, the company loses its ability to control that data (Miller et al, 2012).

II. IN THE WORKPLACE

BYOD is nothing new and is currently in place in 76% of enterprises in a survey conducted by Good Technology in 2012, following a 4% rise from the previous year (McCallan, 2013). Despite its relatively low number of participants only being 100, other surveys suggest the same such as in a survey conducted by ZDNet, which had 1000 participates, found that 44.1% of organisations already allow BYOD with a further 18.2% planning to do so in the next 12 months (Hammond, 2013).

However, a survey conducted in New Zealand found small to medium businesses (SMBs) felt slightly differently, with 43% concluding that mobility of BYOD outweighed the risks (Eskow, 2013). This is likely due to the relatively low operational capability that a SMB can achieve in comparison to a bigger corporation. A SMB is unlikely to achieve the same benefits from avoiding the cost of corporate-issued devices since many of them simply may not be able to afford it thereby creating the extra costs to IT department in terms of security controls and support (Ranger, 2013) with no balance of cost savings in other areas.

A. Security Policies and Compliance

Businesses face a troubling dilemma with BYOD, the amount of personal devices now outnumber laptops in offices and since security policies are less likely to be enforced on personal devices, the risk of confidential data falling into the wrong hands is high (Miller et al, 2012). On one hand businesses want to motivate their employees by allowing them to use their personal devices in a secure environment (McCallan, 2013) and on the other, they need to comply with data compliance.

This issue is only heightened when you consider that in a survey conducted by Infonetics found that 64% of enterprise respondents had devices that contained sensitive or personal data that has been lost or stolen but few had ways to protect those devices (Morrow, 2012). Such cases can only make businesses nervous of legal action and the potential for corporate espionage to exist (Fick, 2013). This ultimately lead to the US in April 2012 creating the national government registry in conjunction with the four major phone networks to remotely disable mobile phones and tablets when reported missing (Miller et al, 2012) thereby helping mitigate at least some of the risks for businesses.

Furthermore, it was only in May 2012 that IBM banned its 400,000 employees from using the cloud storage, Dropbox and Apple assistant Siri over concerns of security (Sophos, 2013). However, this does not need to be the case. The UK’s information commissioner’s office (ICO) responsible for independent advice on data protection advises that the regular auditing of the types of personal data and deciding whether to place them in a more restrictive environment is key to keeping compliance. Adding that restricting these data types to only be
transferable to devices that offer a high level of encryption as one way to combat this risk (ICO, 2013).

Additionally, Sophos (2013) advises that protecting devices with strong passwords make it particular difficult to steal data and if, somehow the device becomes compromised; further encrypting the data itself provides a secondary layer of security.

B. Operational Demands

BYOD has made the IT department’s role of ‘enterprise data protector’ slightly redundant (Ranger, 2013) since presumably prior to BYOD, anything that was connected was approved and installed by them (Mansfield-Devine, 2012). Therefore creating a standard level of security, but when it comes to consumer devices, the problem becomes difficult with the focus from Management moving from platforms to operations (Scarfo, 2012). Thereby making Businesses implementing technologies to restrict users to a limited amount of apps such as using mobile device management (MDM) to enforce encryption of corporate data (McLellan, 2013) but where do you set the balance. If it is too little, you risk losing control of data and too much, you undermine the reason for BYOD to begin with (Mansfield-Devine, 2012).

Perhaps a little worryingly, a RSA conference 2012 study found that 68% of organisations had no way of identifying known mobile device vulnerabilities affecting their network (Morrow, 2012). This will only create problems in the long term and therefore needs a solution by software vendors such as Google and Apple to tighten the security measures on their mobile operating systems or some kind of enterprise edition, which can have better security built in and specific apps to aid businesspersons.

Additionally, it is essential that the network infrastructure can cope with the extra demand (Oliver, 2012). You may see a person with at least two devices, which in turn affect the available network addresses and typically will continue to connect automatically each time that person enters the building with that device (Mansfield-Devine, 2012). This problem is only going to become worse and since we live in an age where technology is incredibly cheap, it means that people will have different pieces of technology to perform different tasks based on their preference. Therefore the need for a dynamic network addressing system where there are more than one Wi-Fi for business and personal use will not only help mitigate security risks (ICO, 2013) but also aid in managing congestion.

C. Cost Saving Benefits

Cisco estimates that employees pay $600 on average for their devices (Scarfo, 2012). In their eyes, this is likely to reduce costs associated with buying and managing devices for their employees (Morrow, 2012) since presumably, a technology corporation like Cisco would have some kind of corporate issued device scheme.

Other than the benefits of employees enjoying the device that they have paid for, it reduces the costs associated with training them on how to use it (Miller et al, 2012). Thereby creating a win-win situation, with employee feeling motivated that they can use the devices they prefer and businesses being able to allow their workforce to work wherever they want.

III. THE WORKFORCE

Apple CEO, Tom Cook called this the “post-PC era” (Sophos, 2013), what he means by this was the decreasing importance of the PC in the work and home environment. BYOD is one outcome from the post-PC or perhaps better-worded, post-Desktop era with our mobile devices becoming increasing important. This in turn has made working and personal life increasingly blurred (Scarfo, 2012) since people will be using the same device for both personal and work and even working at home and vice versa.

Bringing your device to work typically seems to be a trend, in a survey conducted by Cisco involving 600 IT leaders found that 78% of employees bring a mobile device to work (Scarfo, 2012). Additionally, Shell believes that in a few years, less than 10% of its users will be using company-provided IT equipment (Bennett, 2013) thereby creating a lot of potential problems such as lack of privacy.

A. Privacy Concerns

BYOD security policies typically uses MDM, which works by enforcing numeric or alphanumeric passwords for accessing their mobile devices, encryption of corporate data along with remote locking and wiping for lost or stolen devices (McLellan, 2013).

Leading to employees to be concerned at the ability for their employer to be able to remotely wipe their phone in an instant. A case has existed where a Woman’s iPhone was mistakenly wiped, resulting in lost contacts and photos. A fix has since been made (Kaneshige, 2013) but it is an issue that organisations are facing, BT being one of them and wondering at what time is it reasonable to wipe devices (Preez, 2013). Part of this does include trust, but the balance between a user’s freedom and restriction of corporation data is the hardest part to get right (Ranger, 2013).

However, take a situation where you have an app, which is paid by the corporation but has private data too, once the employee leaves, this app has to be wiped and uninstalled but the question of who is liable for this lost data still exists. Additionally, the intrusion of these apps on their whereabouts brings up some insecurity with employees, who some also believe they are trying to exploit free work time from them (Kaneshige, 2013).

A lawsuit in the US is currently underway for this very reason, Police officers in Chicago are owed millions of dollars in overtime when they forced upon them department issued Blackberrys to respond to e-mails and calls (Kaneshige, 2013). Despite this, BYOD continues to be extremely enticing to the younger generation.

B. Young Talent

BT’s head of security told Computerworld UK that the conservative culture in the organisation in employing BYOD is already affecting their ability to bring in new young talent (Preez, 2013). This is perhaps no surprise since as of January 2012, 71% of users aged between 25-34 in the US own a
smartphone. In contrast, only 17% over 65’s have a smartphone. Additionally, Bill Gates, famous from his Microsoft era, has embraced the advantages of BYOD as an anytime, anywhere education system (Miller et al, 2012) thereby making a number of young people knowing nothing other than using their own devices for personal and work purposes.

Interestingly, in another survey, 66% of college students in the US expect to be able to access their corporate network using their home computers with around 50% of those expecting the same with mobile devices. Meanwhile, 30% of young professionals admit the absence of remote access would influence their job decisions (Thomson, 2012). Therefore, it is likely that young people do not want to be locked into a corporate environment (Bennett, 2013).

In contrast, Shell plans to fully embrace BYOD by planning to move 135,000 staff to BYOD. This is most likely in part due to estimates that within 10 years, 50% of their workforce will retire (Bennett, 2013) and therefore do not want to be in the same position BT find themselves in and advertise that they embrace the new culture of working in the hope that they get applications from the best of the young talent.

C. Education and Experience

Employees are becoming more informed, sometimes knowing even more about the devices than the IT staff (Mansfield-Devine, 2012). Therefore businesses should be utilising them rather than dictating what devices to use, allowing people to ditch those corporate issued Blackberrys (Kaneshige, 2013).

Doctors were one of those who were forced to use Blackberrys due to the perception of being more secure, when they refused to use them for their iPads, there was a legitimate reason for it. Doctors argued that between patients they could wipe the screen with sanitizer, which they could not do with a keyboard (Mansfield-Devine, 2012).

Therefore, by both sides working together, they should be able to meet somewhere in the middle. For example, certain devices are inherently more secure than others (Mansfield-Devine, 2012), but simply telling someone they cannot use their device, will only cause a higher risk since they will most likely use tools to bypass them anyway (Preez, 2013). In addition, it may help sway their choice when they decide to upgrade next and what device themselves or their family gets for them. The initial solution is that for Android as an example, downloading from Google’s app store is somewhat safer than a third party (Mansfield-Devine, 2012).

IV. CONCLUSION

Despite some initial resistance by organisations, even the most conservative organisations are deciding to drop many of their initial reservations and become in favor of BYOD and this is in large part due to a changing culture of the younger generations. They realise how important bringing mobile devices are into the workplace, not only for personal use but for work too since it is what many younger people now are accustomed to. Whilst there are some costs associated to operations by keeping these different types of devices encrypted and safe, a large organisation will largely offset these costs because of no longer needing to provide corporation-issued devices, which in turn employees like because they are more familiar with them and may motivate them to work harder.

That is not only to say that there are not any issues still remaining, privacy is still a major concern for both sides and the balance has not reached a point where it is suitable for either needs. It is likely that in order to do this, software vendors will need to work together with businesses to construct mobile operating systems to provide better security and clearly separate the personal from the business part of the phone. Therefore, when employees leave companies, which ultimately happens eventually, the organisation can be certain that the device has been wiped sufficiently of corporate data and that their own personal data is intact.
REFERENCES


Payment Card Data, Security Standards

The Loopholes

Jack Harrison
The University of Derby
Derbyshire, UK
100127967@unimail.derby.ac.uk

Abstract - Organisations are quick to confirm their compliance with the payment card security standards. More often than not, organisations genuinely believe they are compliant. This paper aims to highlight common areas that are missed during the assessment of compliance. The overall aim of this paper is to aid with the creation of an effective security planning team, who will create successful security policies and procedures.

Keywords - Information, Security, Standards, Payment, Card.

I. INTRODUCTION

Any organisation that is required to keep a record of the payment card details of their clients, are now also required to be PCI DSS (Payment Card Industry Data Security Standard) compliant. Although compliance is not yet a legal requirement, VISA and Mastercard can issue fines of more than £10,000 for failure to meet the standards. When discussing commitment to PCI DSS Bonner, et al (2011) claim Mastercard issued fines of up to $375,000 a year for non-compliance. Most organisations meet most of the criteria to become compliant, and most claim to meet all the criteria. There are a few loopholes that many organisations are overlooking when analysing their compliance. In this paper I will demonstrate how simple errors can prevent an organisation from meeting three of the twelve requirements for PCI DSS compliance:

2. Requirement 7: Restrict access to cardholder data by business need-to-know.
3. Requirement 9: Restrict physical access to cardholder data.

II. OVERVIEW OF PCI DSS

The PCI Security Standards Council (2010) outline 12 requirements needed to meet their outlined objectives, and therefore become PCI DSS compliant (see table 1). The following discussion of PCI DSS is based solely on version 2.0 of the security standard.

Table 1. PCI DSS requirements (PCI security standards council, 2010)

<table>
<thead>
<tr>
<th>Objective</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data.</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters.</td>
</tr>
<tr>
<td>Maintain a vulnerability management program</td>
<td>3. Protect stored cardholder data.</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>5. Use and regularly update anti-virus software or programs.</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>6. Develop and maintain secure systems and applications.</td>
</tr>
<tr>
<td>7. Restrict access to cardholder data by business need-to-know.</td>
<td></td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access.</td>
<td></td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data.</td>
<td></td>
</tr>
<tr>
<td>10. Track and monitor all access to network resources and cardholder data.</td>
<td></td>
</tr>
<tr>
<td>11. Regularly test security systems and processes.</td>
<td></td>
</tr>
<tr>
<td>12. Maintain a policy that addresses information security for all personnel.</td>
<td></td>
</tr>
</tbody>
</table>

Within their report on data breach investigations Baker, et al. (2011), claim that 89% of those organisations who suffered payment card breaches in the past year, were not PCI DSS compliant. We can deduce from this that 11% were compliant when they suffered a payment card breach. I strongly believe this is due to a poor assessment of the organisations, during their PCI DSS assessment. In my professional opinion there are a number of loopholes in security, which organisations quite commonly miss when assessing their information security.

III. TRANSMISSION OF CARDHOLDER DATA

One question any information security officer must ask themselves when evaluating security within their organisation is: How is data transmitted within the organisation? Typical answers to this question include: email, internal mail and shared drives. Requirement 4 of PCI DSS compliance requires that strong cryptography is utilised during the transmission of cardholder data.
A. Outsourcing and Unsecure Email

The most common way of capturing client’s card details is via a customer webpage. The client accesses the secure webpage and manually inputs their card data. Once these card details are entered the information is stored securely on a web server before being transmitted to the relevant finance department for processing. When discussing the method of small and medium enterprises capturing their clients card details Williams (2001) suggests that these web pages are usually hosted externally. This academic goes on to highlight the problem of transferring the data from the external host into the organisation, and suggests a common method is unsecure email. The transmission of card data via unsecure email is a clear violation of requirement 4 of the standards. It is highly possible for small and medium enterprises to outsource many of their processes to save on cost. The main problem with outsourcing resources is that the organisation has a responsibility to their clients to ensure that the information is secure when being processed by these external resources. When discussing the outsourcing of accounting functions Jayabalan, et al. (2009) suggest, data security and client privacy issues are a main concern when outsourcing resources.

B. Internal Mailing Systems

Another common method for transmitting information within an organisation is via internal mailing systems. Paper documentation is often transferred within an organisation via their internal mailing systems. When discussing the protection of confidential information, the centre for management and organisation development (2008) explores the security of internal mailing systems. They suggest that the majority of organisations internal mailing systems feed directly into their external mailing, which causes a security concern for the exchange of financial data. Unsecure, external transmission of card holder data is a breach of requirement 4 of the standards. One of the responsibilities of the information commissioner’s office (2012) is the enforcement of the Data Protection Act 1998. In 2012 the information commissioner’s office (2012) issued a monetary penalty notice to Leeds city council, due to a data breach they had experienced via their internal mailing system. Confidential data was transmitted via their internal mailing system; however the data was accidently transmitted externally. This happened due to the internal and external mail utilising the same system. An internal investigation resulted in two separate mailing systems being established within this organisation. One could argue that the transmission of card holder data should never be transmitted via the internal mail irrespective of the security measures in place. The payment card standards actually state that all paper documentation of card holder data should be physically secured. One could argue that a sealed envelope is not physically securing the data within. In my professional opinion any paper documentation that needs to be transmitted should be scanned and transmitted via secure email. The paper documentation should then be securely stored.

C. Shared Network Drives

The final method of transmitting this confidential data, I will explore in this paper, is the use of shared network drives.

One of the most crucial requirements for compliance with the standards is network security. I suggest any organisation aiming for compliance will already have a unique ID for each of their users and their network access will be set up based on business need-to-know. If this is the case any network access to card data will meet the business need-to-know requirement of the standards. During my own industry experience I have noticed that, end users have a habit of copying and pasting files to different areas on a drive to provide access to different users. For example, a user may be having technical difficulty with a database which contains card data. To provide a more technically minded individual access to fix their database they copy it to an area of the drive that the technical user has access to. No consideration is taken for the number of other users who have now gained access to this confidential information. The correct process for this scenario would be the user replacing all confidential data with “dummy” data and saving this as a version for the technical user to fix.

To meet requirement 4 of the standards any transfer of card holder data should be securely transmitted using encryption. Within this section I have highlighted three common loopholes in the secure transmission of card holder data.

IV. VIRTUAL ACCESS TO CARDHOLDER DATA

Within the previous section of this paper I highlighted the end user’s habit of moving files on a network drive to transmit data, resulting in unauthorised, virtual access to card holder data. In this section I will discuss the need for strong and understandable system security policies to protect card holder data. I will conclude this section by highlighting that the need for an effective system policy is crucial for meeting requirement 7 of the standards.

A. Least Privilege Principle

The foundation of any system policy is to provide users only with the access they require to perform their job. Saltzer and Schroeder (1975) explain the principle of least privilege while discussing the principles of information protection. The least privilege principle basically suggests that both programs and users should only be given the access that is required to complete their functions. Any additional access is producing unrequired risk to both the system and the information within. As I have previously stated within this paper, all organisations should have unique IDs for each user; however can one be sure that each user is set up using the least privilege principle? The only way to be sure is to have an effective system security policy.

B. System Security Policies

The security access to a system and the information within is usually approved by a member of management. One could argue that not all members of management understand system security access. Therefore when they approve security access they may not realise what information they have provided the user with. Sandhu and Samarati (1994) explain the use of three different system security policies within their academic paper. First they describe the discretionary policy. This policy works with users requesting access to information, the access is then
granted as soon as they receive the correct authorisation. One could suggest that this policy provides no real assurance about the security of the information. One could also argue that this type of policy makes it very easy for a user to be granted more access than they require and it is also very easy for users to share information. In conclusion of their paper they offer two alternatives to this policy; the mandatory policy and; the role based policy. The mandatory policy is the concept of assigning security, not only to the users, but to the information also. This policy states that a user’s assigned security must dominate the information’s security; otherwise access will be either limited or denied. The role based policy is based on the creation of security roles. The roles only provide access to information to perform a specific function. Both the mandatory and role based policies have their positives. For systems that are not required to continuously update their user’s security, a mandatory policy may be suitable; otherwise I suggest a role based policy. Role based policies only provide information access to perform specific functions within the system. Using these functions management can easily highlight the roles each user requires to perform their job. The role based policy is a good policy for achieving the least privilege principle. The role based policy is very easy for management to understand; therefore ensures they understand exactly what access they are approving. It is crucial that any user or administrator authorising access to a system understands the full extent of the information they are providing a user. It is also crucial that end users understand the responsibility they have to ensure the protection of the data they have access to. I suggest there are many organisations, which have both users and administrators, who do not have a full understanding of the information they are dealing with when access requests are processed. One could argue this is due to the system security policy not being fit for purpose. If due to this lack of understanding, users are provided with unrequired virtual access to card the organisation fails requirement 7 of the standards.

V. PHYSICAL ACCESS TO CARDHOLDER DATA

Within a previous section of this paper I highlighted the unsecure method of transmitting payment card data via internal mailing systems. This could result in unauthorised, physical access to card data. In this section I will discuss the security risks of unsecure paper documents and how this can violate requirement 9 of the standards.

A. Clean Desk Policy

One of the most common policies organisations now have is a clean desk policy. The clean desk policy has been proven as one of the hardest to enforce within organisations. In the payment card industry it is common for finance departments to be dealing with hard copies of their client’s card data. One might also suggest that it is quite common for an employee to go to lunch without securing the physical documents on their desk. If any documents containing card information are left unsecure on a desk, the information could be available to unauthorised personnel. This is a violation of requirement 9 of the standards. The clean desk policy basically requires all employees to clean their desks before they leave. All sensitive documents should be locked away and any that are no longer required should be shredded. When discussing human factors in security Parson, et al. (2010), outline the importance of shredding confidential information to prevent unauthorised access. During my own industry experience I have learnt that the clean desk policy is one of the hardest for management to enforce. Whitman and Mattord (2011) and Calder and Watking (2005), both highlight the importance of the clean desk policy but do suggest that management have to be persistent with their attempts to enforce it. Failure to enforce this policy could leave organisations in violation of requirement 9 of the standards.

B. Shared Printers

As well as leaving hard copies of card data unsecure on desks, users can often leave them unsecure at a printer. Most offices within organisations utilise shared printers. Sending an unsecure document to a shared printer could allow unauthorised personnel physical access to card data. During his discussion of the information security chain in a company, Finne (1996) suggests, employees should not be printing highly private information on a shared printer. I agree with this academic, and suggest that card data should not be insecurely printed to a shared printer. However the majority of modern printers and print drivers now offer the functionality of locked printing. This functionality allows users to send their documents to a printer; however it will not begin printing until they are physically stood at the printer and input their security code. The unsecure printing of card data could make an organisation fail requirement 9 of the standards.

Within this section I have revealed how common mistakes made by a user can allow unauthorised, physical access to card data. I have also highlighted the importance of management being persistent with the enforcement of their policies. It is vital to understand that just because a policy is in place does not mean users are meeting the requirements.

VI. RECOMMENDATIONS

This paper is the foundation for the creation of a security plan or risk assessment. I argue that not having a sufficient team setting up an organisations security plan or risk assessment is the main cause of overlooking information security weaknesses. Pfleeger and Pfleeger (2010) suggest, a security planning team for organisations which includes representative users. It is only the end users of a financial system that will have the true knowledge of how card data is stored and shared. Taking into consideration the loopholes I have highlighted, the security planning team should explore all areas of their card information processes and all concerns should be considered. The most important point to take into consideration is to ensure the security team’s main objective is to make the organisation’s processes fit the standards, and not make the standards fit the organisations processes.
REFERENCES


Abstract - Computer logon and passwords form a necessary part of the controls used to access information systems, yet remain universally considered one of the weaker parts of the information security chain. They are issued to an end user who is the most fragile of the links. This makes for, and often results in, a highly combustible combination.

Information systems users are negligent and forgetful, often resulting in rogue access to highly confidential data, whether intentionally sought and not. The logon combinations themselves can be easily manipulated. Unless systems and processes are implemented to address these concerns it will continue to be an area of failure for small and medium enterprises. The repercussions for failing adequately to address these are wide-ranging and can have such an impact that a business may potentially never recover.

Understanding in the subject area is crucial as approaches are readily transferable. The concepts must remain an integral part of the promotion and enforcement of best information security risk mitigation, practice and ethos in the workplace.

Keywords - Access, Security, Password, Information systems, End Users.

I. INTRODUCTION

The modern, developed world inherently relies on information systems, digital devices and the internet (Vu et al., 2007), forming an essential element of our personal and professional lives. Methods of control are almost universally innate, so as to restrict access to only those that require it. They are characteristically enforced with unique logon and password credential combinations. These systems can record customer data, financial transactions, profit and loss. The sensitive information contained within is not commonly afforded to all.

The average cost to a UK business for a typical information system security breach is just over £2 million (Ponemon Institute LLC, 2012). For a small or medium sized business this may seem to have little or no bearing and may not even equate to many years of turnover or profit. But converted to a cost per customer record and the annual trend examined, the average cost per record has risen year on year from £47 in 2007 to a high of £79 in 2012 (Ponemon Institute LLC, 2012). This is a rise of 68% in just five years, well above any inflation figure or interest rate. For a business with a customer base in the low thousands or even less the effect can be devastating.

These breaches can and will affect all manner and size of enterprise. Their impact and cost continues to grow. 90% of these successful security breaches resulted from a weak, stolen re-used or default password; a third of these brought about through user negligence (Ponemon Institute LLC, 2012). This statistical combination must give cause for concern.

II. THE THREE STRANDS OF CREDENCE

An information system consists of technology, people and processes, all should be considered of equal importance (Tarwireyi et al., 2011) and are interdependent. Unauthorised and casual authorised access, unintentional leaks and negligence are unwanted tenets of an information system and every effort should be made to remove them. By securing a system, the confidentiality, integrity and availability will be protected (Gordon & Loeb, 2002). To access a protected system, a text based authentication procedure is the convention (Bafna & Kumar, 2012). This typically has two stages; first the identification of the user, usually in the form of a user ID, then authentication with a password. This confirms that the user is the genuine owner of the ID (Vu et al., 2007). Different levels of access can be afforded to the end user. An entirely open system, with no control will result in little or no delay to the user, but leaves the potential for unauthorised or rogue access. Therefore, when designing, building and maintaining an information system; the amount of security imposed should be proportional to the value of the data being secured (Gordon & Loeb, 2002).

III. UNDERSTANDING THE USER

Any information system is only useful if people use it (Mathieson, 1991). The perceived ease of use and usefulness are major factors in the likelihood of use and the overall success of the system (Davis, 1985). By removing all known constraints and objections by the user, the system can be used to its maximum capabilities. Accessing information systems and logon techniques are known to cause frustration to the end user (Adams & Sasse, 1999). Users are the weakest link in information security (Schneier, 2000). Systems can be placed under acute risk through flawed actions and unwanted behaviour (Thomson et al., 2006), which can be difficult to predict and control. The human memory has only a short term capacity to recall approximately seven items (Miller, 1956) and a maximum of three passwords. It is perhaps unsurprising that credentials are forgotten and manually recorded. Sticky notes attached to the side of screens are not uncommon sights in an office, with passwords often written onto them.
A user is likely to have an average total of twenty-five password protected accounts and typically six or seven passwords in total (Florencio & Herley, 2007). Logon combinations are known to be replicated across multiple accounts (Ives et al., 2004) (Bang et al., 2012), yet when questioned two thirds of people insist they memorise all their passwords (Tarwireyi et al., 2011). Proven cognitively impossible, the majority of those interviewed are delusional.

There is a temporal limit for recalling items and the sequence in which they should appear. When recalled correctly there is an increased likelihood of them being familiar words, symbols or items of self-reference (Nelson & Kim-Phuong, 2010). Some 18% of system users will include a pet’s name, 12% a birthday, 10% their child’s name and 9% their mother’s maiden name in a password (CPP, 2009). To better assist with recollection of an object or sequence redundancy is usually required, using a combination of the five senses. Different formats and using different cues increase recall ability. Memorising a set of logon credentials is not as simple as it seems.

Outside of the working environment a user is not subject to policy. As social norms evolve they are willing to share more confidential information online, resulting in a decrease in their level of online privacy. Habits will transfer across to the working environment, like password replication, a common factor in most social engineering attacks. The act of targeting legitimate users into revealing their logon credentials, it is reliant on password disclosure and a lack of motivation and awareness of information security issues to break security controls (Adams & Sasse, 1999). It can lead to a ‘domino effect’ where all of an individual’s accounts are hacked (Nelson & Kim-Phuong, 2010).

In studies, up to half of the sample will admit to sharing their logons and passwords with another individual, despite knowing it to be wrong (Tarwireyi et al., 2011). This credential sharing will result in a scheme failing to accurately identify the user (Jain et al., 2006). In an enterprise environment, plausible deniability by the original owner of logon combination as a defence would be difficult to maintain. It should result in both parties being charged, if none were to admit guilt.

There are typically three types of authentication available: ‘what you know’, ‘what you are’ and ‘what you have’; the latter may be a token or smart card access (Almuairfi et al., 2012). Biometric authorisation is the establishing of identity based on physical or behavioural qualities: ‘what you are’. More reliable than ‘what you know’ logon and password combinations, they are difficult to replicate and are typically not lost or forgotten (Jain et al., 2006). The owner is required to be present at the time of access; fingerprint, facial or iris keystroke, signature and voice recognition may be used.

Manufacturers of portable smart devices and mobile phones are now deploying facial recognition and fingerprint logon techniques. A modern laptop often has fingerprint recognition technology installed. On Microsoft machines operating in an Active Directory environment and running Windows 7 and above, fingerprint logon techniques are now supported, with biometric data stored locally and the responsibility of the user (Microsoft, 2012). If laptops were issued to users by default it would also benefit business continuity. An applied policy of device removal at the end of the working day could minimise the impact of fire, burglary, even acts of god on the premises.

All of these techniques are likely to require infrastructure investment, which may not be particularly necessary or catered for in an operating budget (Conkling & Hamilton, 2008). It must be reiterated that the level of protection should be appropriate to the sensitivity of the information being cared for. By combining several forms of access control, the risk of unauthorised access can be decreased and overall security can be increased. The cost, time and technical prowess require to implement, maintain and service these levels of control should be factored into any business decision. A reliance on technology without considering other factors has been demonstrated to cause failure (Thomson et al., 2006). Whilst a permanent shift away from a combination of logon and password may seem not be far off, there are situations where alternative methods of access control cannot be used such as web sites (Vu et al., 2007) and the traditional is therefore likely to remain pragmatically persistent.

IV. UNDERSTANDING THE PROCESS

Security awareness is the knowledge and attitude that an organisational member has about the protection of their business’s information assets (Thomson et al., 2006). In a perfect world there would be an inherent, consistent and tireless understanding and appreciation at an organisational level for the concept of information security, together with idyllically committed users to a company’s overall security mission.

Simply providing a user with cutting edge technology and tools (or not as a business decision may dictate) to protect company issued assets and information is not a solution. Persuading and ensuring the appropriate use is dual-faceted. Without vision and direction from the senior hierarchy and policy driving it, it will fail. Any security mission itself should ultimately be expressed in end-user security guidelines (Thomson et al., 2006). This awareness can be either systematically taught as an inherent part of the culture or by adopting a framework (Siponen, 2000), such as ISO 27002.

Research has shown that performance, ability, motivation and the employees working conditions are in constant interaction with each other (Siponen, 2000). An employee’s motivation is archetypically short term, from days to weeks and varies between individuals in terms of quantity and kind (Ryan & Deci, 2000). Multiple techniques and approaches should therefore be used to inspire employees. Inciting excitement and issuing challenge to the user through short term campaigns, competition and persuasion will promote, remind and increase overall security. The threat of user culpability will at worst be minimised and theoretically be quashed.

A lack of communication and discussion will fail to place the user at the centre of any design process (Adams & Sasse, 1999). By making the user feel respected, part of the process
and providing impetus, motivation towards a subject can be inferred (Ryan & Deci, 2000). However the message is communicated, it should be continuously maintained. By forming an unremitting positive attitude to this imperative part of the information chain a long lasting ethos can be developed. Properly trained and information security aware employees can actually become the most robust part of a business’s security structure (Henry, 2004 as quoted by (Thomson et al., 2006)). A user should learn to treat their logon credentials with a suitable level of care and respect, like their own finances: essential and expensive to replace.

A. Applying Technique

If an alternative to the conventional is not realised then a system generated random password is secure (Bafna & Kumar, 2012), but allowing the user to generate their own is less likely to lead to disclosure (Adams & Sasse, 1999) and easier to remember (Vu et al., 2007). The user may not have enough information to make an informed choice, choosing a single word in their own natural language can be susceptible to a brute force dictionary attack, where an attacker tries all the words in the dictionary (Horcher & Tejay, 2009).

Password effectiveness can be improved through clearly communicated policy, although too complicated and the user will attempt to circumvent the procedure altogether (Bensnard & Arief, 2004). The simplest system restricts certain password structures and words, by imposing a minimum and maximum number of characters and a combination of letters and numbers security will increase (Burr et al., 1992). Microsoft’s Windows Server is currently the most commonly used network service operating in the enterprise environment today (IDC, 2012) and such restrictions can be universally enforced within their schema for all users (Microsoft, 2012). Smaller sized businesses with fewer devices may use alternative software from Microsoft, another vendor or perhaps no networking software at all. Regardless of the situation a system of password complexity is recommended.

A user is unlikely to change a password once selected until it has been compromised (DeAlvare, 1988). Enforcing a frequent password change will reduce the risk of a compromised password staying undetected. This can result in previous passwords interfering during recall (Vu et al., 2007). Increased frustration and lockouts can be reduced by increasing the number of logon attempts available to the user. Using favourite foods, film stars and television characters can limit the effectiveness of a dictionary attack and using a pass-phrase increases the randomness and chance of memorisation (Horcher & Tejay, 2009) (Vu et al., 2007) and makes them harder to crack (Kuo et al., 2006). The first or final letter of each word of a phrase could make up the password. This could then be padded out at the end with non-alphanumeric characters such as exclamation or question marks in a sequential and meaningful fashion up to any character limit.

V. RECENT ADVANCES

As many as 90% of passwords are now vulnerable to attack (Deloitte, 2013). Users will trade productivity and practicality against risk (Bensnard & Arief, 2004) and deem this rational behaviour (Duggan et al., 2012). The recording and sharing of passwords will continue to result in an overall decline in security.

Information systems are now distributed across multiple devices: from desktop computers, to laptops, smart mobile phones and tablets and exist in unseen and often unfathomable cloud infrastructures. Using this technology a password manager can be accessed through one master password. It can synchronize encrypted data to a cloud storage solution and can be installed and used across multiple devices (Information Week, 2012). The password could be changed regularly and recalled efficiently, although data is placed in trust with in a third party.

Dual-factor techniques are increasingly common and one-time pass-codes are being sent to mobile devices to confirm authenticity where additional levels of security are required (Huang et al., 2011), but additional time has to be factored in for their use. Single sign on techniques can be investigated with these limiting the number of logon and passwords combinations an employee must remember, but can expose a complete infrastructure. Graphical password systems have increased levels of accuracy (Wiedenbeck et al., 2005) but can be subject to shoulder surfing and screen dump attacks (Almairfi et al., 2012).

VI. CONCLUSION

Information systems have three key elements: processes, people and technology and are intrinsically intertwined. Past, present and future; there has, is and always will be a reliance on controls to protect what is stored inside them. When breached, it can clearly cost a business. The vast majority of breaches result from poor password management and policy and more often as a direct result of user negligence. The user is the weak link and their actions can be disastrous, but this must be reasoned against temporal ability and behaviour transferral.

The conventional method of ‘logging on’ is unlikely to disappear, despite frustration and attempts at evasion and circumvention by the user. Technologically advanced solutions will undoubtedly assist and some are now more affordable to small and medium enterprises. Rather than what you know, it can be something you have, or are. Like the techniques available to improve password recall these have side-effects, some welcome, some not so. As important is ensuring that process and policy is in place. It should be discussed, communicated and enforced and considered both long and short-term.

An intricate and incredibly complex conundrum; the subject will require great thought. There is no universal solution; one size does not fit all. Yet it is the most crucial element of information security. Getting it right will almost certainly result in secure, reliable systems. Positive attitudes will spill over from the working environment into our everyday lives and the people we interact with. The thought and consequences of getting it wrong should not even be entertained.
REFERENCES

Building Online Brand Trust for SMEs
Can SMEs Gain Trust Online?

Mfon-obong Edwin Ikott
University of Derby
Derbyshire, UK
M.Ikott1@unimail.derby.ac.uk

Abstract - Trust has been regarded as a major obstacle in e-commerce and is identified as the key to building a relationship between enterprises and consumer online. With Small and Medium-sized Enterprises being no exception, e-commerce gives SMEs the prospect to grow its business. As great as the possibility of this opportunity sounds, these SMEs encounter many challenges in business relationships online and building online brand trust is one of them. Online trust building is vital for SMEs to build and preserve business relationships with consumers online. This paper looks at the factors affecting online trust in SMEs and the trust enhancing processes which also highlights the compliance and governance strategies for SMEs to incorporate in order to gain online brand trust.

Keywords - E-commerce, SMEs, Trust, Trust building, Governance.

I. INTRODUCTION

SMEs are the spine of the European market. According to the federation of small businesses, SMEs account for 99% of 4.8 million businesses in the UK and 96% of the Australian businesses of which only 26% had some sort of online presence as at 2009 (Gligorijevic & Leong, 2011). The rapid development in electronic commerce over the last decade has enabled SMEs to exploit the possibilities of e-commerce by expanding its geographical reach as a result of the internet (Kamari & Kamari, 2012). Electronic business could easily be defined as the trade of goods and services using information and communication technology as a platform. This has made it possible for SMEs to use the web as a trading and marketing medium to reach a greater audience and customers for many businesses (Ranganathan & Ganapathy, 2002). However, as with every form of business there is perceived risk making trust online essential for SMEs to build and maintain relationships with consumers. This is often the case as the absence of direct interaction or communication is an issue for SMEs unlike the traditional form of business where direct contact is established for transactions to occur (Kamari & Kamari, 2012). In the case of e-business, in order to establish transactions between SMEs and consumers trust is essential (Thomas Deelmann, 2002). Despite the technological advancements in online security, there tends to be an opinion that trade via online transactions may be unreliable and unsafe as a result of several factors especially for SMEs that are susceptible to foreign threats as compared to bigger firms (Ren, et al., 2005).

Trust has been recognized as the main hurdle discouraging consumers to engage in online transactions. Although extensive studies have been carried over the years on online trust in e-business, there is no sign that an acceptable answer for online trust with regards to e-business has been attainable (Pittayachawan, et al., 2008). This paper looks to offer an understanding of the factors affecting online brand trust in SMEs. Trust is alleged to be complex and can be addressed in different dimensions (McKnight & Chervany, 2001), and as a result it involves variables which SMEs should be attentive to in order to build and maintain online brand trust (Pittayachawan, et al., 2008). This paper also covers a review of literature on trust issues such as security, privacy and website factors. While trust is cited as an important factor affecting online trading due to its influence on consumers’ decisions to oblige to an online purchase (McKnight & Chervany, 2001), trust on the other hand plays a vital function in e-business because it allows consumers to engage in online purchases confidently when the online retailer or SMEs are not well-known or recognized brand wise (Akhter, et al., 2004; Jutla, et al., 2004; Pittayachawan, et al., 2008). Trust can be a success factors for SMEs or e-vendors if implemented adequately (Stockdale & Standing, 2003). Trust is vital for SMEs to develop a relationship with consumers, consumers who trust the Brand of an SME is more willing to engage in e-transactions and is more likely to remain loyal and committed to the brand for future services (Alam & Yasin, 2010).

II. FACTORS AFFECTING ONLINE BRAND TRUST IN SMEs

Brand trust can be defined as the “willingness of the average consumer to rely on the ability of the brand to perform its stated function” (Chaudhuri & Holbrook, 2001). Therefore with regards to this paper, online brand trust can be referred to as the self-assurance an individual has in the brand of a specific SME in order to participate in e-business. Without brand trust, a consumer is likely to be unwilling to engage in an online transaction. Hence it is essential for SMEs to build an online brand trust with consumers. Trust is also centered on the belief of the consumer that the brand of a specific SME has qualities that makes competent, responsible and honest in its business (Alam & Yasin, 2010).

There are several factors affecting online trust and can be categorized into internal and external factors (Salo & Karjaluoto, 2007). The consumers’ perception of risk, past experiences with online transactions makes up the external factors while internal factors include the online or web-based security which covers the aspect of privacy and third party policy, web interface and acceptance of the information.
This paper focuses on the factors affecting online brand trust. Brand trust can be classified into two dimensions with the first being technical and competence based which relies on a SMEs ability to satisfy consumers’ need (Alam & Yasin, 2010). Secondly, it involves the acknowledgement of respectable intention to the brand with regards to the consumers’ benefits (Alam & Yasin, 2010). According to Ha (2004) in his study of factors affecting customers’ notion of brand trust online, defined these factors as web-purchased related. These factors include; security, privacy and third party, brand recognition, word-of-mouth, quality of information and online experiences (Ha, 2004). A survey about consumers’ issues online shows that if privacy was addressed properly, 78% of online users would use the internet more and 61% non-users will use the internet (Mahadevan & Venkatesh, 2000).

Security and online trust go in tandem and it is critical that the security of online transactions and trust are the most important aspects that affect the success of SMEs in e-business (Papadopoulou, et al., 2000; Chong, et al., 2011).

### Table 1: Factors Affecting Online Brand Trust (Alam & Yasin, 2010).

<table>
<thead>
<tr>
<th>Reference</th>
<th>Factors Influencing Online Brand Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Ha, 2004)</td>
<td>Web purchase-related factors: security, privacy, brand name, word-of-mouth, good online experience</td>
</tr>
<tr>
<td>(Srivivasan, 2004)</td>
<td>Security, past experience and third party recommendations</td>
</tr>
<tr>
<td>(Sultan, et al., 2002)</td>
<td>Website factors: navigation, advice, no error, fulfillment, community, privacy/security, trust seals, brand and presentation. Consumer factors: self-confidence, Internet savvy, past behaviour, Internet shopping experience, and entertainment experience</td>
</tr>
<tr>
<td>(Lee &amp; Turban, 2001)</td>
<td>Trustworthiness of Internet merchant, trustworthiness of Internet shopping medium and contextual factors</td>
</tr>
<tr>
<td>(Salo &amp; Karajaluoto, 2007)</td>
<td>Consumer characteristics, product/service characteristics, different markets/cultures/countries, perception of risk and past experience</td>
</tr>
<tr>
<td>(Dayal, et al., 1999)</td>
<td>Security, merchant legitimacy, fulfillment</td>
</tr>
</tbody>
</table>

Table 1 summarizes the factors affecting online brand trust in SMEs that have been studied in previous research. These factors can be categorized into consumer factors and website factors. Studies suggest that customer’s perception of trust is based on the website and customer’s attributes and trust facilitates the relationship between the website attributes and the consumer’s action (Sultan et al., 2002).

### III. TRUST BUILDING PROCESS

For SMEs to build online brand trust it is essential to develop strategies to tackle the above discussed factors affecting brand trust in SMEs (Mahadevan & Venkatesh, 2000). Research on online business have indicated privacy and trust concerns as important factors that determine the likelihood of consumers’ engaging in online business, mainly SMEs without a recognized brand (Suh & Han, 2003; Teo & Liu, 2007). According to Ren, et al., (2011) trust in e-Commerce can be looked at from three different standpoints: interpersonal/organizational trust, website security mechanisms in e-Business, and external governance/Legal trust (Ren, et al., 2005).

The trust building process begins with the consumer is willing to trust thereby checking if the SME is trustworthy. If all the key factors affecting online brand trust such as security, privacy, web factors and online experiences checks out positively with the consumer’s perception and is satisfactory, The risk of engaging in such transaction is assessed and if it’s not too high then trust would be established between the consumer and the SMEs for a particular transaction (Thomas Deelmann, 2002). A Repeated success of this can be referred to as a Trust cycle as shown in the figure below.

![Figure 1: Trust cycle (Thomas Deelmann, 2002).](image)

From the above figure it is clear that trust has to be developed and maintained for SMEs increase online brand trust. For SMEs to be able to create and increase brand trust, instruments and processes that tackle and address the major factors affecting online brand trust must be implemented. They include; Trust signals/trustmarks, communities, security and privacy strategies, reputation renting, data ownership, product testing and warranty. In order to gain consumer and brand trust, SMEs have to convince consumers on the security of their personal information obtained via e-transactions. As a result of this, SMEs have implemented a range of security processes and instruments to boost perceived trust which includes trustmark logos on websites, quality of web design, customers’ ratings (Peterson, et al., 2007; Sun & Han, 2003). Trustmark logos help engender trust between consumers and SMEs as it is certification that an SME has met the security criteria standard of a trusted third party agency. It is also suggested that trustmarks has a positive influence on consumers and propels them to engage in online transactions with unknown websites (Thomas Deelmann, 2002; Hu et al., 2004). SMEs need to improve key areas of security such as; authenticating online transactions, non-denial of transactions. A high level of security during online transactions influences
the consumers trust positively and this helps an SME gain online brand trust (Kamari & Kamari, 2012)

Reputation renting is also a trust building process for SMEs not willing to develop a steady or well recognized brand can buy into the reputation of another firm. This strategy is viable for short-term SMEs that do not need to build a reputation for the long run (Choi, et al., 1997). SMEs that trade information based products tend to experience difficulty in describing such products to meet the information needs of potential consumers. Product testing and warranty can be a possible solution where by testing the product decreases the consumers’ perceived risk and improves the consumers’ willingness to pay which in turn leads to a level of higher trust and reputation for the SMEs (Hoffman, et al., 1999). A potential consumer could be more willing to be a customer there is an incentive of a warranty and a right to return the product within a certain period, this could help build online brand trust for SMEs (Thomas Deelmann, 2002)

Apart from the various process of addressing security and privacy issues, this paper has described various ways to gain online brand trust. Although the above described means is quite attainable for SMEs, other means like the governance strategies and actions to help build trust would be further discussed in this paper.

IV. COMPLIANCE & GOVERNANCE

In addition to the various means of trust building in SMEs, there is the need for these processes to be supported by a legal environment, compliance, industry self-regulation and personal and organizational relationships (European Commission, 1997). Since privacy and legal protection for online purchases are important for both SMEs and consumers, the legal uncertainties regarding these issues may affect SMEs brand trust. Therefore, it is vital for SMEs to comply with the legal framework and policies developed by the Government addressing the various factors affecting online brand trust in SMEs. The Korean republic government created the Korean Market Place website that showcases products of Korean SMEs to potential customers globally and hosts over 20,000 SMEs and e-catalogues of over 120,000 products (United Nations, 2007). This initiative not only provides SMEs with a wide range of customers globally, it builds and maintains the online brand trust of SMEs whose websites are hosted on the website.

SMEs should adhere to rules, guidelines and e-government policies in order to alleviate the consumers’ perception of risk and also promoting ethical e-transactions. The OECD’s guidelines for consumer protection should be taken into consideration by SMEs. This guideline features eight principles which include: transparent and effective protection, clear online disclosures, confirmation process, privacy, easy and secure payment systems, dispute resolution, and adequate information (United Nations, 2007). Adherence to the above mentioned principles would enable SMEs to build a trustworthy relationship with customers thereby enhancing its brand trust. Business ethics of SMEs play a vital role in building brand trust; ethical practices should be carried out by employees of SMEs and this practices help build consumer trust in relation to future online purchases (SME World, 2011)

SMEs should also refer and comply with governance standards to tackle factors affecting online brand trust. ISO 27002 sections 6.2.3, 10.2.3, and 15.1.4 all provides guidelines to enable SMEs address security in third-party agreements, data protection and privacy of information (ISACA, 2008).

The OECD also has eight privacy guidelines which SMEs could strictly implement. They include; collection limitation principles, data quality principle, use limitation principle, security safeguard principles, accountability principle, openness principle, individual participation principle and purpose specification. These guidelines summarises the need for SMEs to obtain and use personal data of customers only relevant to a given online transaction and effective security of data to avoid unauthorized access (OECD, 1980).

V. CONCLUSION

This paper has reviewed the importance of online brand trust in SMEs and the need for SMEs to build and maintain brand trust albeit the various issues affecting online brand trust in SMEs which were discussed in this paper highlighting security, privacy, third party and consumer characteristics as the main factors. As a result of these hindering factors, various ways of building and ensuring online brand trust in SMEs were elaborated showing its importance to SMEs and its effectiveness towards influencing a consumer’s willingness to engage in online purchases. Additionally, this paper presented some legal and governance policies to guide SMEs in tackling and addressing the various factors hindering trust in order to establish and maintain online brand trust.

Although there is indication of common agreement about the significance of trust for the success of e-Business, various research only discuss the role of trust for e-business adoption and trust building processes (Papadopoulou, et al., 2001). Many do not provide an insight of the trust building process SMEs could implement alongside compliance and governance policies to effectively develop and maintain online brand trust in SMEs.
REFERENCES


The Insider Threat - Are You Secure?

Daniel Jones
University of Derby
Derbyshire, UK
100100061@unimail.derby.ac.uk

Abstract - The insider threat can take many forms and can have a damaging effect on a business. The global economic recession has shown to have had a direct link to inside network attacks; criminals obtain sensitive data by either coaxing employees to steal the information for financial gain. Business management decisions such as outsourcing and redundancy have also shown to have a direct link to provoke internal threats. By ensuring that a robust security policy is in place along with adequate security systems, the damaged caused by inside network attacks can be severely reduced or completely removed in some instances.

Keywords - Security, Insider, Networks, Employees, ISO27002.

I. INTRODUCTION

Today the majority of security concerns focus on issues in relation to corporate networks being exploited externally; be it through intrusion via hackers or malicious viruses designed to steal or manipulate data. As technology continues to advance, perpetrators are increasingly finding new means to sabotage or disrupt the operation of businesses across the country. Various groups behind these types of attacks also appear to be on the increase; the likes of ‘Hacktivism’ groups are continuously disrupting target systems. The complexity behind viruses and worms are also on the increase; the ‘Stuxnet’ worm from 2010 which was found implanted in infrastructure systems throughout Iran which had the potential to cause major disruptions.

Many businesses fail to identify internal disruptions as a realistic threat with current security implementations in place failing to meet an acceptable standard.

II. THE INSIDER THREAT

Inside network attacks have the potential to cause significant disruptions to a business due to the physical access an individual may have to critical systems. Delahunty (n.d) suggests that insiders have a decisive advantage due to being familiar to the systems that they have worked with, as opposed to an outsider perpetrator who has identified target systems through various other means. Krau et al. (2008) also suggests that some insider attacks are difficult or even impossible to prevent. This is particularly evident in wireless networking and a business can merely limit the damage caused as opposed to eradicating the issue permanently.

Security incidents which resulted in the breach of a business’s network hit 45% for SME’s throughout the UK for 2012; 33% of these accounting for the misuse of Internet access and a further 25% for misuse of email communications. (PWC, 2012). Figure 1 Shows various other security incidents which have been caused internally by staff throughout the last working year.

![Figure 1: Staff-related security Incidents. (PWC, 2012).](image)

Kotsev (2011) also provides a list of concerns for businesses related to internal security gathered from the SANS institute. These include areas such as access rights to critical systems for untrained employees and relying primarily on network security systems (such as firewalls) without adequate physical security in place. It is also common for businesses to authorize short term fixes for problems which have been discovered but are then forgotten about until the issue reoccurs to cause further disruption. By identifying potential areas within the business which could be targeted for an attack, reducing or eliminating the threat to a particular system or area of the business may be possible.

III. WHO ARE THEY

Brancik (2008) describes an insider as anyone who has access rights into a network, system or application and can vary from current or former employees, software vendors and external contractors. Schultz (2002) defines an internal attacker as someone entrusted with authorized access who instead of fulfilling assigned responsibilities, manipulates access to a system to exploit it. This could be to either intentionally sabotage a specific system known to be critical to the business or manipulate valuable data which the business may hold.
Many organizations focus their attention protecting their assets from outside of the business, be it from thieves trying to physically steal equipment or hackers trying to steal confidential information to sell to the highest bidder. As the above statistics show, an inside attack can be just as devastating as an external unauthorized breach due to the physical access or knowledge of a system that an attacker may have.

IV. INSIDER MOTIVATION FOR ATTACKS

There could be a number of reasons which may have provoked an insider attack on an organization. Colwill (2009) provides an insight into why employees may decide to implement an attack throughout various different factors associated with the business; some of which may be out of reach for a particular business to resolve independently. Business, economic and cultural factors can all have a bearing on an employee which may provoke them to carry out malicious attacks. Colwill (2009) suggests that both organizational and cultural differences can cause fear, uncertainty and doubt in employees. This can impact attitudes towards current working practices in relation to information security. Outsourcing has also shown to have a negative effect on employee morale; with over 50 percent of UK businesses suggesting that they outsource their IT solutions throughout 2012 (UK IT Outsourcing Intelligence Report 2012) this may cause concern for many businesses. Outsourcing may also cause further problems in terms of language barriers when security requirements and third party contracts are constructed within these agreements. Various other issues are likely to occur which could include misinterpretation of rules or contract requirements. Employees from the third-party vendor could breach contract agreements and further increase security concerns in terms of systems access and information confidentiality.

The current economical climate and the pressures of the global recession have and are continuing to affect employee motivation; reducing costs whilst still maintaining a high level of efficiency can prove to be a difficult challenge for many businesses. Mohamed (2009) suggests that there is a direct link between falling national prosperity and increased criminal activities, with more people likely to turn to illegal activities in order to ensure they maintain an acceptable standard of living. With many businesses across the world struggling with the current economic climate, reducing costs is likely to be a high priority in order to avoid financial difficulties. A solution to reduce costs may involve reducing the size of the workforce, which may have a direct impact on employees by causing fear of redundancies. Motivation to continue operating efficiently may be more likely to be reduced. The McAfee Virtual Criminology Report (2008) suggests that there is also a direct correlation between cybercriminals and employees within a business in the current economic climate revealing sensitive information for financial gain which provides another factor for small businesses to consider.

V. INDICATORS OF AN INSIDE ATTACK

Stolfo et al. (2008) suggests that in order to understand how to detect malicious insider actions, it is important to understand the different forms of attack which may be undertaken from an inside perpetrator. These attacks can range from unauthorized extraction or manipulation of data, destruction of assets, and the use of unauthorized, third-party software within the business environment (may contain harmful viruses). Forms of social engineering attacks are also considered forms of insider threats which contain acts such as spoofing or impersonating other users in order to gain access to previously restricted data or systems. From this point, many frameworks have been developed within the computing community in order to aid law enforcement agencies for catching the perpetrator and preventing similar attacks in the future. Brannick (2008) describes a framework in which various indicators and behaviors from an individual are monitored to determine whether harmful actions have been committed or not. These indicators include behaviors such as correlated system usage patterns, verbal behavior, personality traits, meaningful errors and preparatory behaviors such as gathering unusual system information to exploit known system weaknesses.

As well as intentional attacks, UK businesses are vulnerable to unintentional attacks such as accidental deletion of sensitive data or policy violations in terms of computer usage which could result in a system breach from an unknown source. Fyffe (2008) suggests that it is also important for a business to have an idea of exactly who has access to company data, what access rights they have been granted and what systems they use in order to access this. By knowing who has access to which systems, assistance can therefore be provided when designing or updating policies by authorizing relevant access to the right people.

VI. PREVENTING AN INSIDE ATTACK

In order to limit the effects of insider attacks there are many pro-active measures which a business can undertake. Jones (2008) provides a list of technical and non-technical measures which a business could implement in order to reduce or eliminate the effects of certain types of insider attacks. Walton (2006) suggests that the role of technical counter-measures ensure two things; damage limitation and early eradication of potential vulnerable security threats. Physical security plays a vital role in protecting an organization’s assets from both inside and outside attacks. By restricting access to core systems businesses are able to limit (or in some cases completely remove) damage to critical systems and maintain some form of functionality. Bernard (2007) suggests that by implementing an Information Lifecycle Security Risk Assessment a business will be able to determine the effectiveness of any security measures put in place. It will also be possible to detect what corporate policies exist and how effective they are, the physical locations of critical systems.
and the full lifecycle of critical data (i.e. from creation to the secure destruction of the data).

VII. PHYSICAL SECURITY

Delahunty (n.d.) states that physical security is one of the most important areas in relation to Information security and is often overlooked. Critical systems and main system servers should not be easily accessible, and non-IT staff should have very limited access (if any). They should be securely locked away so that only authorized staff can physically access these systems for maintenance purposes. Various safety features are often overlooked to prevent further damage to IT equipment; climate and environmental hazards can cause severe damage to equipment where for example it may overheat or become damaged from smoke caused by fires. A Backup power supply or UPS should also be considered to ensure the continuity of power, which may also prevent system down time and security systems are maintained throughout the site. It is also critical that regular backups are taken for business information and current systems in place; ideally this will be stored offsite in a secure location to avoid accidental or intentional destruction. A disaster recovery and business continuity plan should also be implemented to ensure that there is a clear plan in place should a natural disaster occur. Delahunty (n.d.) also recommends that external audits will benefit a business as impartial views can identify any potential security ‘holes’ which may have been missed by previous internal audits.

VIII. SECURITY POLICY

The protection of information systems is a major problem faced by modern businesses, with criminals discovering new threats as technological advancements continue to rise. Kardya et al. (2005) suggests that the application of a robust security policy is essential to the management of security within information systems. An IS security policy should include the intentions regarding the protection of IT systems with details describing how this will be achieved. Many businesses however fail to recognize the importance of this. Colwill (2009) shows that 35% of IT workers admit to accessing corporate information without authorisation and 74% of respondents stated that they could circumvent current security controls to prevent access to internal information. 75% of organisations with a security policy believe their staff had a poor understanding of current practices and 54% of SME’s in the UK do not have a programme to educate staff about security risks (PWC, 2012). If staff do not understand how systems are to be used within the business, they are unlikely to be aware that they are breaching the security policy or potentially leaving the business open to a security breach. It is therefore vital that staff fully understand what is expected of them and what they should or should not be doing in relation to the use of computers.

A robust security policy should address the following areas: Password management and computer acceptable usage, confidentiality of company data (non-disclosure agreements), physical security, administrative matters (such as computer privacy, copyright infringement, disposal of sensitive data) computer privacy and external communications with third party businesses. This is not an exhaustive list but should be a minimum requirement when designing a similar policy to ensure all aspects of computer usage and privacy are covered and that all employees fully understand what is being requested of them.

The ISO27002 standard is a good place to start for any business. This working practice provides guidance on many aspects of information security management including physical and environmental security, human resource security, access control, risk assessments and the acquisition, development and maintenance of Information systems. Many practitioners suggest that by adopting the ISO27001/27002 standards and becoming certified provides improved information security controls, greater security awareness, business alignment and management assurance (ISO27000 News, 2013).

IX. CONCLUSION

It is clear to see that inside network attacks are as damaging as external attacks for a business, and can have the potential to severely damage a business’s reputation. An insider attack can take many forms ranging from social engineering attacks to corporate espionage and are a constant threat for all sizes of businesses. There are various indicators that an attack may be imminent or have already been implemented. A perpetrator may have various motives for conducting these attacks which a business should be aware of. By ensuring that a detailed security policy is in place with adequate physical security systems many inside attacks can either be severely reduced in terms of their effect or erased completely in some instances.
REFERENCES


Getting On-line Security and Privacy Right for SME’s
How These Factors can Influence Trust and Benefit a Business

Rebecca Kestle
University of Derby
Derbyshire, UK
R.kestle1@unimail.derby.ac.uk

Abstract - Many organisations may wonder how trust can affect or be relevant to security and privacy concerns in the online world - but much research has proven it to be very important - not just for the customer but everyone “trust is not only important to customers, but also employees, suppliers, distributors, partners, stockholders and regulators.”(Shankar, Urban & Sultan, 2002). Most SMEs nowadays will be using some sort of online resource to carry out their work and we discover that there are many things to help improve privacy and security concerns in this environment, and that these remedies can in fact directly impact on a users trust level which in turn leads to increased online business allowing your company to work better. It is also apparent that whilst there are many dangers posed in this area, there are many simple things that you can do to combat them.

Keywords - Trust, Security, Privacy, E-commerce, SME’s.

I. INTRODUCTION

One of the most important issues facing businesses within cybercrime and security are based around human engagement as indicated by Ayrapetov (2013) which means that trust in systems, especially with regards to security and privacy are of important consideration as it could dramatically help organisations with both their understanding of security, privacy and trust concerns in an online setting and how these relate, as well as contingencies and practices that should be put into place to reduce the amount of security flaws and therefore increase employee and consumer trust and promote continued use in such environments.

With the amount of threats posed online these days - from viruses and malware to ID theft and phishing, it can be perceived that trust is becoming ever increasingly difficult to generate as users either become all too wary of the threats or have too little knowledge about them to use the internet, so it is vital that trust can be understood, built and maintained in order to keep businesses going, customers returning and to gain that competitive edge that all companies seek. Numerous studies highlight the importance of online trust and how central security and privacy concerns are to building and maintaining those trust levels(Dinev & Hart, 2006; Aiken & Bousch, 2006; Urban et al. 2009; Midha, 2012), and with retail moving evermore into the online environment as traditional retail problems become more apparent; such as loss of sales, increased costs for brick-and-mortar shops, higher inconvenience to shoppers (Colao, 2012)- it makes this topic all the more pertinent to SMEs working in this setting. In addition - it is said that these security related risks are just as prevalent in small businesses as they are in large companies (Ayrapetov, 2013).

Trust can influence and impact on many different things - including a user’s willingness to participate in business online, and a lot can be learnt about how it relates to the security and privacy of online services. Most organisations nowadays (even very small enterprises) have an online presence or use the internet for a vast number of reasons and they all want to ensure that they are providing the best security and privacy measures possible to suit legal requirements, allow their employees to reach maximum potential with the technology they have and to make customers comfortable in using their service and if possible return in the future. The subsequent sections should help in achieving this.

II. PRIVACY, SECURITY & TRUST: WHAT ARE THE ISSUES?

Privacy issues include spamming, usage tracking and data collection and the sharing of information with third parties (Belanger, Hiller & Smith, 2002). Security issues can range from hacking, viruses and DoS (Denial of service) attacks to ID theft and fraud, theft of information or property and other kinds of malicious attacks through flaws in a system / website. Trust in an online context can be seen as “The belief that allows consumers to willingly become vulnerable to web retailers after having taken the retailers’ characteristics into consideration” (Pavlou, 2003) and this is therefore directly impacted upon by the amount of security and privacy flaws perceived or visible within a website, suggesting these 3 components to be very much interwoven with one another; if the security and privacy features are very robust, this inherently increases a user’s level of trust - driving a user towards further use and creating more business, and this will work conversely too; a users trust will depreciate if there are too many security and privacy flaws, which again, will reduce a users participation with a website. Many studies agree upon the importance of security and privacy online (Urban, 2009; Midha, 2012; Aiken & Bousch, 2006; Koufaris & Hampton-Sosa, 2004) and the relationship between these and trust (Chellappa & Pavlou, 2002). Urban et al (2009) argues that “Privacy and security have become the new baseline from
which one evaluates trustworthiness”. But for SME’s it can sometimes be difficult to build and maintain a secure, trusting environment due to the tighter budgets available to these companies (Cisco, 2006). Interestingly, a study undertaken by Prince & King (2012) showed that out of 98 SME’s, protecting customer data was the highest driver of IT expenditure, which one could assume included implementing security measures throughout systems, but this does not correlate with their results for SME’s security budgets; 47% of companies spent less than 5% of their budget on security. This is a very small amount and indicates that companies are not spending their money and focusing their attention on the most critical areas.

In addition to this, several hundreds of thousands of infected websites are said to be found on a monthly basis by Google (Schwartz, 2012) and figure 1 and 2 show the fluctuations year on year between these infected sites found and attack sites found. It is this kind of information that is very alarming for consumers and can deter them from using your online services as they perceive too much risk. Information such as this also highlights the necessity for security to be in place online and the need for more of a company’s budget to be allocated to security and privacy solutions. These “infected” or “attack” sites could potentially lead to loss of business and customer faith, fraudulent activity, theft of sensitive customer and company information or theft of money, and as you can see the numbers are not small - these issues are affecting thousands of sites, and potentially thousands of people.

III. HOW DO WE GET IT RIGHT?

With regards to enhancing trust through privacy and security measures online - there are many relatively simple things that you can do with your website that will not cost much, or be that difficult to implement. Some however, are quite timely. The following details such solutions;

It is important to include security and privacy policies; Lee et al (2005) found that the mere presence of such policies increases the probability of further participation in e-commerce. Having said that, many privacy statements that businesses employ are often quite off-putting to users - they can be regarded as “trust busters” due to many of their unappealing characteristics; They are often very lengthy, use language that most users find confusing or difficult to understand (which can make a user feel as though you are trying to disparage them) and all of this leads to an uncertain feeling on the users behalf and can sometimes deter them from participating. Therefore, you should do as much as possible to ensure that any security policies and privacy statements you have are user friendly; Use clear and understandable language - this will make a user feel as though you understand them and that you are communicating through a common framework (Urban et al., 2009), make sure policies are not too complex or lengthy - simplicity is key, and try to update them regularly - in the online environment, one can never be too up-to-date with security and privacy contingencies (Pollach, 2005).

Customers regard transparency as a very important issue - it shows benevolence on the company’s behalf and tells them everything they want and need to know about a company, and its processes. Some organisations omit information in order to keep customers coming back to their business and to essentially steal customers regardless of whether they offer the right product or service, but contrary to what most SME’s may believe, disclosing clear details on what you offer and how
you function, as well complete and unbiased competitor offerings - with possible advocacy features to help the user decide, can actually increase a user’s likelihood to continue to do business with you - it shows goodwill and trustworthiness (Urban et al., 2000).

Customer empowerment and control features are becoming more important (Midha, 2012) - such as opt in / out preferences for cookie control and targeted ads. People are also more inclined to do business if they can tailor the site to their individual preferences - from simple background colour selections to more complex morphing algorithms that are based upon a user’s cognitive decision style (analytic, compulsive, holistic). The goal with this kind of technology is to communicate more efficiently with each individual - a site’s appearance and content can be confusing and difficult to use for some people, which does not help to foster trust, or promote further use. This idea therefore tracks a user’s clicks and uses Gotten’s algorithms and machine learning theory to display the most appropriate morph for an individual, and this should help consumers to feel like the website understands their needs and provides a level of empathy (Urban et al. 2009).

For transacting businesses, you need to make your security and reliability tangible to a customer, so evidencing things such as third party assurances and seals of approval from neutral sources (Verisign, TRUSTe, Norton, etc.) and displaying them in clear view on your website is vital. This will assure consumers of several things depending on what seals you have in place; firstly, that the technology you have in place is capable of handling payments successfully and securely, secondly, that your company is compliant with privacy regulations (Beldad et al., 2010).

System and transaction security has been cited as more important than privacy concerns (Belanger, Hiller, & Smith, 2002) especially for new businesses in particular as customers will only engage in what they deem to be secure and trustworthy. So, it is important to regularly check and update the security of your system / website. This could include ensuring you have the most appropriate encryption in use for your particular infrastructure, added security plug-ins, and advanced, robust programming features that stop hacking - simple things such as SQL injection for obtaining information from a database through a website sometimes get overlooked by smaller companies, and if you do not understand how to implement any of these features, it is important that you hire a specialist to thoroughly investigate and improve your system’s security.

Studies highlight how higher levels of online proficiency and experience can increase trust levels (Liao et al., 2006; Gefan, 2003) - which consequently increases their inclination to use a system / website. This shows how getting customers and employees more involved and on a regular basis can help a business to do well; people are more comfortable using it, they gain more knowledge around it, and this could lead to further technical use and perhaps ideas for better, more secure ways of working too. But to begin increasing online proficiency and encourage extended use of systems for all kinds of users, trust in the system must first be built through the aforementioned security and privacy mechanisms.

Educating, guiding and training both staff and customers are all good ways of trying to foster trust as it has been evident in studies that user knowledge and experience increases interest and willingness to participate (Corbitt et al., 2003; Gefan, 2003). It will also allow employees to make safer, more intelligent decisions based on security. It is advisable to create an in house security team that have been specially trained and educated in online security and how staff and users access and use the website and its information - Pfleeger & Pfleeger (2010) also recommend this. A report by Prince & King (2012) reports that out of 98 SME’s surveyed, only 45% of SMEs have ongoing security training, and 20% after the initial induction phase never train their employees again. These results are in alignment with PricewaterhouseCooper’s annual report (2012) showing 54% of SME’s to not have any training or educational program at all for their staff on security related issues. This data suggests something interesting; that despite the stream of published security issues we see in media, companies still overlook this topic and choose not to spend their time training their staff on important matters that can help push a business forward. Whether this is out of ignorance, the perception of wasting time, money or whatever reason - it is clearly the wrong attitude to hold, as it can affect your business and your customers.

IV. CONCLUSION

The online setting is one of uncertainty with many threats and hindrances, but it is also one in which growth is still taking place, and business is becoming ever more common, so this article has looked at some of the key issues surrounding security and privacy in this context, and how they affect trust levels in users. It is clear that these trust levels are important in retaining customers and improving business for SME’s. It has also been shown that the potential consequences are high if these areas are overlooked. We can deduce from this article that whilst these suggestions will work much better together, the most vital solutions include educating, training and developing an appropriate security team as well as ensuring your infrastructure has the right security and privacy features in place to begin with - assurances & privacy policies, encryption, secure and reliable transaction processing, etc. This will help to make new customers feel safe, whilst at the same time retaining your existing customers. Through integration of these suggestions you can also increase the knowledge and understanding that your staff have on these topics - reducing the chance of human error from inside the company.
REFERENCES


Abstract - This article aims to address the impact that revealing too much information on social networks can have on small and medium businesses. First, the size of the problem is assessed, providing relevant statistics as to how social engineering effects businesses. Different types of social engineering relevant to businesses are then defined. We will then look at the potential consequences of falling victim to a social engineering scam, and most importantly, how to prevent yourself, and your employees, becoming victims.

Keywords - Information Security, Risk Management, Security Assurance, Social Engineering, Social Networking.

I. INTRODUCTION

Facebook: The social networking giant with over one billion active users, of which 680 million sign-in each day (Facebook, 2013). Studies have shown that 77% of Facebook users browse the social networking site at work at least once a day on either their personal or work-provided device (Gaudin, 2009). The use of social networking websites has started to appear more and more throughout businesses, with an increasing number of companies using Facebook and Twitter to advertise and promote offers and giveaways. 97% of IT professionals realise that social engineering in the work place is a problem, so why are 74% of businesses not providing training for their employees in order to prevent against it (Dimensional Research, 2011).

II. TYPES OF SOCIAL ENGINEERING

There are many different types of social engineering, and many that are used over social networks. The following types are those that are common in business environment.

A. Spear Phishing

Phishing is when an attacker sends out thousands of emails at a time pretending to be from a legitimate organisation such as a bank, typically explaining how there has been a problem and the recipient needs to log into the website using the including link and re-enter their personal information and bank details (TrendLabs, 2012). The user is then redirected to a fraudulent website replicating the website it is representing, and once the user enters their details they are stored by the attacker (TrendLabs, 2012). Whilst regular phishing attacks attempt to broadcast to as wide an audience as possible, spear phishing attacks are more targeted, often aimed at those in a particular role with a company (TrendLabs, 2012). Attacks of this nature often include intimate details about the recipient to make the communication feel more personal, and genuine. A spear phishing attack in 2008 involved roughly ten thousand LinkedIn users receiving a targeted email that when opened, installed malware onto the victims computer that gathered information such as usernames and passwords (Krebs, 2008).

B. USB Baiting

How much damage can a memory stick do? USB baiting is purposely losing a memory stick baited with malicious software (Wagenaar et al). The memory stick is placed in a location that the attacker knows it will definitely be seen and picked up by an unsuspecting employee. The idea behind USB baiting is to exploit a curiosity trait in human nature, whereby a memory stick found on the floor will inevitable be inserted into a computer, where the user can either snoop through the contents or attempt to find information that will lead to the safe return of the memory stick to its owner (Wagenaar et al). Once the memory stick is inserted into the victims computer, the malicious software is installed onto the host PC, unbeknownst to the victim. A new tool in the attacker's arsenal is the USB Rubber Ducky, a device that masquerades as a memory stick, but hides a memory card and a processor that allows the attacker to execute scripts on command (Hak5, 2013). Fooling the computer into thinking these devices are keyboards or other input devices, the attacker can deliver powerful payloads, given access to the victim's computer. These devices are particularly dangerous, since there is no defense against them, short of disallowing the use of keyboards and other input devices (Hak5 Ep. 709, 2013).

III. HOW BIG IS THE PROBLEM?

Aside from the obvious exceptions of not focusing on tasks and cutting productivity, using social networking websites like Facebook at work may not seem like it can cause a lot of harm to your business, but you would be surprised; Facebook now reports that over 83 million of its users’ accounts are fraudulent (Mashable, 2012).

According to GetCyberSafe.CA, 156 million phishing emails are sent every single day, 90% of which are caught by spam filters and a further 50% go on to be read (GetCyberSafe, 2012). A survey by WebSense in 2012 revealed that most successful phishing emails are sent on Friday, accounting for 38.5%, followed by Monday, (30%) and Sunday (10.9%) (Websense, 2012). In fact, only 16% of businesses have said that they were confident they had not been targeted by social...
engineering attacks, and 41% were unsure whether they had been targeted or not (Dimensional Research, 2011). Even more alarmingly, 33% reported over 50 social engineering attempts over the past two years (Dimensional Research, 2011). Figure 1 shows the most common factors behind social engineering attacks. The top motivation is for financial gain, account for 51% of all social engineering cases.

Figure 1. Motivations for Social Engineering Attacks.

IV. UNDERSTANDING THE CONSEQUENCES

A study into social engineering on information security by Dimensional research revealed that use of social networks was the second most common vector of social engineering, accounting for 39% of all incidents, with phishing e-mails being the most common, accounting for 47% (Dimensional Research, 2011). This can be shown in Figure 2. The same survey also revealed that 30% of each social engineering incident that took place at work costs the company over $100,000 (Dimensional Research, 2011).

Figure 2. Most Common Sources of Social Engineering.

A. Corporate Espionage

What if someone from a rival business managed to get a corporate spy on the inside of your company? What access to your files would they have? Client lists and financial records, trade secrets, and expansion plans are just some of the confidential information that can be shared with your competitors. It is estimated that the total amount lost to the theft of trade secrets and other corporate data is somewhere in the region of $45 billion per year (Robinson, 2007). From Figure 1 we can see that getting the competitive advantage accounts for 40% of all social engineering attacks.

B. Identity Theft

Information gained by an attacker on a victim can be put towards a profile to either further refine attacks to increase the probability of success, or even more likely to be used to impersonate the victim, or steal their identity. In 2011, two thirds of organisations experienced attempted or actual fraudulent payments, and the total cost of fraud amounted to $18 billion (ID Theft Center, 2012).

C. Corporate Identity Fraud

Corporate identity fraud is defined as the abuse of corporate identity assets with the intention of deceiving or defrauding customers (Fite, 2006). These identity assets can include logos, brands, website domains or email addresses, and trademarks. A common partner to corporate identity fraud is IP spoofing. This involves the attacker sending the victim a link to a website, where the attacker has replicated the organisation’s website (such as Facebook) and altered the username and password fields so that they send the information to the attacker. Since the victim believes they are on the alleged website, they will attempt to enter their details without suspecting that the website they have been linked to is fake.

D. Malicious Software

Once an attacker has become acquainted with a victim on a social networking site, it becomes a lot easier to coerce them to a particular link. On Facebook or LinkedIn for example, once the victim has accepted the attackers friend request a certain level of automated trust is assumed, otherwise the victim will simply deny the friend request. This trust can then be exploited to send the victim private messages containing links to malicious software. Malicious software can also be installed directly onto the victims computer, as mentioned in the previous section about USB baiting.

E. Case Study Example

One commonly used example of social engineering in the workplace is how an attacker managed to get the confidential information of over 200 customer’s accounts (Granger, 2001). The attacker contacted AOL’s tech support and spoke with an employee for over an hour on the phone. During the conversation the attacker mentioned that he had a car for sale at a great price, and the employee was interested, and gave the attacker their personal email address in order to receive details of the car and for the attacker to send photos of the car (Social-Engineer.org, 2009). The attacker emailed the AOL employee but did not include pictures of a car, but instead attached a malicious software application that opened up a backdoor into the AOL system’s firewall (since the employee was still at work when he read the message). Using this backdoor, the attacker was able to gain access to the accounts of AOL customers (Granger, 2001).

V. HOW TO PREVENT BECOMING A VICTIM

Denying access to social networking sites may seem like a drastic step for some businesses, as there are many legitimate reasons for allow their use, but there are many alternatives to ensuring that your employees stay safe and protect your business in the process.
A. Security Awareness

Brodie says that when a business is compromised from the inside, it is not always a disgruntled employee or corporate spies that are the cause of the breach, and that often it is uninformed employee ignorant how security awareness (Brodie, 2008). This can be supported by a survey conducted by Dimensional Research, where it was discovered that the highest group of employees most susceptible to social engineering attacks are new employees, accounting for a majority of 60% of attacks (Dimensional Research, 2011). One in five employees let their friends and family use their company issued laptop and computers to access the internet without realising the consequences (Schneier, 2005). Raising staff awareness to threats such as social engineering (but not limited to - awareness to all different types of threats should be taught) is best taught in ongoing staff training sessions.

B. Staff Training

Staff training is probably the most important step to take in the proactive defence against social engineering attacks. Educating staff to recognise and avoid the actions of a social engineer is crucial. A study of IT professionals showed that 34% of companies make no attempt whatsoever at educating their staff on social engineering threats, and only 26% of businesses give ongoing training (Dimensional Research, 2011). The remaining 40% offer guidelines to social engineering-based threats in their security policy, however the onus is on the employee to read and understand the information (Dimensional Research, 2011). These results can be seen in Figure 3.

C. Usage Policies

Your usage policy should already dictate what users can and cannot do. By including a section on the guidelines of handling information and appropriate usage of information over social networking sites. One suggested would be to allow general use of social networking sites on personal mobile devices whilst at work, but not on the company systems or network, cutting down the risk of malicious software. Another suggestion would be to disallow users talking about work on social networking sites. This would hinder an attackers chances of gaining information about the business if they managed to 'friend' one of your employees.

VI. CONCLUSION

The human element is always the weakest link in any security system, and social engineering will also remain a popular vector of attack as long as the human element is still present to exploit and take advantage of. Social engineering poses a consequential threat to information security as there is no way of stopping it - only steps you can take to ensure that the chance of such attacks succeeding on your business is minimal. It cannot be stressed enough the importance of staff training in how to spot and avoid social engineering tactics, as well as general information security guidelines put into a usage policy to ensure that your employees are staying safe whilst on social networking sites.
REFERENCES


The Issue of Paper Data in a Digital World: 

Is Paper Data Still Relevant?

Jon Maisey
University Of Derby
Derbyshire, UK
1001271119@unimail.derby.ac.uk

Abstract - The issues surrounding data protection are as prevalent now as they were 20 years ago, however how we collate and use data has changed, yet companies still struggle to protect customers and themselves, and in a rapidly growing digital world is there a place for paper data, this article outlines numerous opinions as well as firsthand experience to show the issues around data protection.

Keywords - Data Protection, digital data, physical data, data destruction, DPA laws.

I. INTRODUCTION

The Data Protection Act (1998) has been a significant consideration for businesses and organisations since its implementation, even considering its predecessor, the Data Protection Act 1984, you can understand that its wording is designed in a way to be somewhat flexible but at the same time distinctly clear in meaning. The idea is not just to protect the organisation but also the person the data relates to. Considering the current state of data handling, where an increasing number of companies have personal data, and the ease of access to both companies and users through the internet, it means we are in a situation where personal data is no longer personal, it’s free.

Consider this, you wish to get an insurance quote on your car, house and life. For any company to provide this they need to know a huge amount of information about you, and more importantly they need to store it. This is where considerable issues arise, especially when it comes to more personal data; at some point a client will often find themselves filling in a paper form and this can create issues when it comes to the storage and destruction of these documents. When you consider digital data there are steps you can take to maintain its integrity, for example using high level encryption or network firewalls.

II. PAPER DATA AND THE FACTS.

However, the issue of paper data use is almost a forgotten task, for example a report from CIFAS (2013) showed that 20% of fraud cases did not involve the internet, meaning that of 248,000 cases at least 49,000 involved either physical or social interaction. One of the most incredible cases relating to security in Pakistan and Iraq, on a train. These were then found by a third party (Strucke, 2008). This case was particularly concerning as it involved a senior intelligence officer, who should have known how to treat such documents.

When you consider this fact what would be the case for less trained employees?

In 2012 the IDC reported that in 24.9% of document loss cases, major customers were lost as a result of bad practices, and 20.4% where pulled into a major audit. It also states that between 31% and 39% relied on paper processes, which they believe are more efficient that electronic (Boyd, et al., 2012).

To support the thought that paper documentation is superior to electronic, consider the number of cases relating to electronic data loss. KPMG released a report showing that 681 million records had been affected by hacking, that is 1 in every 10 people on the planet, 67.2% of data loss was caused by hacking whereas only 4.6% was caused by hard copy theft/loss, which accounted for 76% and 0.7% of number of records respectively. This means that 6 million paper records were stolen, just 1/10th of the amount of digital data (KPMG, 2012).

In 2008 Price Waterhouse Cooper went undercover assessing security of data, in one case in the retail sector; they posed as members of the data management team and were given original copies of personal information of staff, customers and potential recruits, however they too found that the majority of data theft was conducted via computer (PricewaterhouseCoopers, 2010).

Interestingly another PWC document specifically looking at companies Information Security, has little information on physical data thefts from paper documentation but supports the IDC, CIFAS and KPMG by showing the most common form of security breach was from hacking, with 73% of large organisations suffering that type of attack, with a median number of attacks of 54, and a low of 28 in a year. Data theft or fraud involving computers only had a median of 5 incidents in 2012 and a low of 4 (PricewaterhouseCoopers, 2012). They do not specify any details regarding paper documentation and this is likely due to the nature of large business as they also found in their Global State of Information Security Survey that 100% of large business leaders (which are only 8% of the total number of respondents) had measured and reviewed security over the past year (PricewaterhouseCoopers, 2013).

One issue with paper is storage. A company holding 50,000 customer details on paper documents with the assumption of each customer requiring 4 sheets of paper, the total weight for that paper would be around 1 tonne, this excludes the weight of separators, organisers, or filing cabinets. One Tonne is a considerable weight, considering BS6399-1:1996 (2007), the standard for load tolerances of buildings, defines a uniform office buildings load as 2.5 kN/m². A simple calculation of
2.5x1000=M*9.81 tells us that the uniform mass allowance would be 254.8kg per meter squared. Assuming filling cabinets and additional materials way another 400kg, it would mean a total requirement of 1400kg, and a room area of 1400/254.8=5.49m² which is approximately a 2.3x2.3 meter room, however this would be for a uniform load, and with no physical space to move, if the room becomes larger, the overall uniform load increases but the point load stays the same, the requirements for pointloads are similar but slightly more demanding no more than 275kg per placed on any meter square, this would mean one full four draw filling cabinet per meter square, an average four draw filling cabinet can handle 17,600 pages (Precision Data Imaging, Inc., 1997) meaning you would need 60 cabinets, requiring a room at least 10mx6m. A size many companies simply could not support. This excludes the physical usage of the paper, which requires an incredible amount of work in comparison to a multi-user database. It is simply not practical for a SME to hold this amount of paper, a large organization could potentially

III. IS PHYSICAL DATA RELEVANT?

Clearly it would seem that even though physical data security is a concern, it is minimal compared to the threat of cyber security. This implies up to three things:

- That physical security is easier and cheaper to provide.
- Physical data policies are in place and to a high standard.
- Physical data is, on the whole, harder and less reliably available.

If for example, a company gets a huge quantity of paper data, they will be able to secure the documents in a central location, in locked rooms and vaults, and even if a theft were to take place security would be in place to hopefully lead to the recovery of the information.

Considering the Joint Intelligence Committee’s incident, it happened by chance, and by accident, even if the Security Officer was fully aware of the rules and regulations in place, it was by sheer accident that they left the document on the train, as a result it was an un-predictable mistake, it would have been impossible for a thief to have planned such an incident.

In 2007 a similar incident occurred within the HM Revenue and Customs, in this incident a junior worker at HMRC sent a disk containing 25million individual’s records, to the National Audit Office, however the package was not recorded and was lost on its way. In this case it was one person’s mistake that resulted in a huge loss of data. Again an unpredictable, accidental loss, however this was not the first time the situation had occurred, earlier in the year in March, another member of staff had sent child benefit data to the NAO, and did not follow the data loss prevention policies in place, and all data was returned. (BBC News, 2007)

These incidents show how important a standard policy on data protection and security is required, and there are numerous policies that can be followed to meet these requirements.

IV. METHODS OF PROTECTION

Having a standard method to protect data is a very difficult task; large companies have almost infinite resources to be able to meet requirements for large standards such as ISO 27001.

Information security to some is just the accumulation of knowledge over previous years, and applying best practice which to some are the basis of ISO 27001 (Humphreys, 2008).

It can also be said that many, particularly SMES’s, consider data security an issue of IT and therefore out of the scope of most CEO’s, however she argues that it is a business issue, it is not simply about improving the computing infrastructure in place, but teaching people and protecting the processes involved in the organization (Everett, 2011). This belief is somewhat supported by PCW research finding that only 63% of small businesses have a formally documented information security policy, this is still a surprisingly low figure as any business which has information on clients, or even sellers could be a potential target for information theft (PricewaterhouseCoopers, 2012). There is however an argument that even if a company does not adopt an ISO standard still legally have to adopt some form of information management, particularly in Europe with European Directive 95/46/EC Article 17 (1995), this is also supported by Otto (2009), who feels laws and regulations tell companies exactly what they need to do, and what basic requirements must be taken.

Other methods of protection can in fact vary, dependent on industry, for example the US has the Health Insurance Portability and Accountability (1996) act, which, when compared to ISO 27001 is somewhat more limited but meets requirements of the health insurance industry, similarly the Payment Card Industry Data Security Standard (2004) had nearly double the security considerations of ISO 27001 (Gikas, 2010).

Other considerations would be generic management and control systems such as COBIT 4.1 with many saying that a generic system can help smaller businesses head towards basic data protection responsibilities and acts as a building block towards a more in depth standard such as ISO 27001 (Simonsson & Johnson, 2007).

A generic data protection system can also be created by those within a company but utilising other common features of larger standards; having rules such as:

- No personal data may be taken off site for any reason
- All laptops and personal devices must meet a certain security level.
- All personal documentation will be stored in one location only and is not available for copy or modification, except by those with explicit access.

By starting off with some basic fundamentals a company or organisation can progress and adapt over time, making sure to get staff opinions on data matters. Additionally using existing legislation, such as the Data Protection Act can give a company a check list of things they must cover, again reiterating the need of some form of policy.

68
V. CONCLUSIONS: DOES PAPER STILL HAVE A PLACE?

Based on the overwhelming lack of statistics regarding paper data, it would significantly imply that it is simply a no-factor in the modern world, where electronic data is more used and more discussed. This is not to say it is not an issue, as shown in KMPG’s report, which shows only a small sample of the worldwide issue, 6 million records is still a huge amount of lost data, but it is merely a drop in the ocean in comparison to computer crime.

As previously discussed, paper to some is in fact more secure, as it is stored in one place (maybe two or three if copies are made), however this obviously leads to issues of how the documentation is worked with, having potentially millions of customers details on paper would make it inefficient for employees to work with - it would require a considerable cost, which is why when you send in a form it is usually transferred to some form of computer system or database, that way employees can easily access, search and sort data they need there and then. Ultimately paper will likely always have a place until the use of portable tablets and computers becomes cheap and easy enough to allow all users on a system to use them for completing forms, and accessing a central database.

To improve validity of this argument, it would be suitable for further research to take place into the area of paper data. If we could gain an accurate idea of how paper was stored, managed and used within both SME’s and Large organisations, it would either validate or invalidate my argument that paper is incredibly secure but impractical.
REFERENCES


Governance Frameworks: Are Company’s Giving Them Much Consideration? If not, Should They?  
An Evaluation of Governance Frameworks

Liam Mander  
University of Derby  
Derbyshire, UK  
100172396@unimail.derby.ac.uk

Abstract - It’s well documented in the media when an organisation has a problem that causes serious consequences, but not many people realise that there could be a potential solution to prevent them from happening. This article looks into a resolution which is governance frameworks; an evaluation of possible frameworks has been conducted to see how each one can affect an organisation. An assessment of the current circumstances has been undertaken just to prove how bad the situation is and how much a solution is required. An extensive look into past failures will facilitate how these frameworks discussed could have helped and possibly even prevented it from happening. Overall this paper provides an insight into governance frameworks and proves why some people hold them in high regard.

Keywords - Frameworks, Information, Governance, Security, failure

I. INTRODUCTION

The governance of organisations has become a big topic in recent years due to the rapid growth in technology. We continue to read reports on organisations that have encountered a failure of some sort, hence the reason why frameworks are becoming an integral part of all companies regardless of size.

This paper will look into how big the problem actually is by looking at statistics from the Standish group reports and other sources to demonstrate exactly how severe the problem is. Furthermore the paper will look into how we can prevent these complications by simply evaluating potential frameworks to see how each one can assist an organisation. It will also be looking into some of the features that the frameworks focus on such as risk assessments, continuity and compliance.

The overall idea of this paper is to simply inform not only SME’s but all size company’s how important and beneficial a governance framework can be to ensure their survival. Examples of failures will also be assessed to see if these governance failures could have been prevented in the first place.

II. REASONS FOR THIS STUDY…

The technical report from PwC (2012) discusses security breaches with organisations and from this we get a great perspective of how significant security is via statistics. These statistics will be looked into more depth further into the paper but we can safely say it can cost businesses millions and sometimes their existence if something fails or goes wrong.

Due to these shocking statistics and damning consequences something drastic needs to be done and this is a big enough reason to research governance frameworks as a possible answer.

III. HOW BIG IS THE PROBLEM?

Before we begin to solve the issue we need to understand how bad the current situation is within the IT industry and also the business sectors. IT projects are being implemented constantly and even before a system is fulfilled a failure can occur. In 2001 when these figures were published, research showed an astounding 31.1% of all IT projects in America were cancelled before they were completed and 52.7% of projects came in over budget in as much as 189% of the original estimate (The Standish Group, 2001). The situation hasn’t got any better from then, as the Chaos Summary Report 2009 displays similar figures for project failures. For example the failure rates have slowly increase from 2002 to 2008 (15%-24%), which is very worrying as it demonstrates that people aren’t learning from mistakes made previously (The Standish Group, 2009).

Once a system has been put in place there are a whole set of other issues such as maintenance and prevention of intruders. Although it doesn’t appeal to SME’s 93% of large organisations had experienced a security breach compared to 76% of small organisations, either way you look at it these are shocking statistics (PwC, 2012). Another reason for the study but something that also highlights how big the problem currently is are the total figures security breaches cost organisations; the total isn’t in the millions but in fact the billions which shows how significant not only security is but also the area of research (PwC, 2012). This proves that governance frameworks should be researched fully as a strong possibility of reducing these figures. Some companies may have already implemented a framework but this still doesn’t make them exempt to a failure. Figure one below shows how the situation has progressively become worse over the years which is an additional reason to investigate.
It's acceptable to vice quality and, rather than offering set procedures on how to prevent Clinch, 2009) actually leads to the organisation, s eradicated by the creation of we. Tsohou et al, 2010) ‘t ternance framework allows the protection of n organisation would be that it’s a ll Calder and Watkins, 2012). The auditing aspect of it functioning in the approved manner. The auditing aspect of it worldwide respected ISO that provides evidence of a company have alongside an additional framework. The benefits of security breaches it looks on how to maintain and build upon what is already in place, this would be an ideal framework to carry out an audit to safeguard certification organisation such as ISOQAR can be requested to demonstrate that the company is ensuring the integrity of its information and assets. Once it has been applied an external certification organisation such as ISOQAR can be requested to carry out an audit to safeguard and improve all information/procedures (ISOQAR, 2003).

ISO 27001 focuses on several topics and provides a model that covers all areas regarding information security management systems such as maintenance, improvement, monitoring, etc. (British Standard ISO27001, 2005). As you can see rather than offering set procedures on how to prevent security breaches it looks on how to maintain and build upon what is already in place, this would be an ideal framework to have alongside an additional framework. The benefits of implementing this into an organisation would be that it’s a worldwide respected ISO that provides evidence of a company functioning in the approved manner. The auditing aspect of it allows a constant review of all procedures to ensure a strong and sustained governance strategy is in place throughout.

ISO 27002

ISO 27002 mainly focuses on security issues regarding information technology however it offers much more than just that. The ISO initially provides the organisation implementing it 11 clauses in which to consider, these clauses include objectives and controls in how to govern that particular area of an IT system (Tsohou et al, 2010). Although it does mainly provide guidance on security issues it does outline a set of strategies in each area for example compliance, continuity, maintenance and others (Clinch, 2009). Businesses are becoming more interconnected and because of this it creates more threats and exposures within a system (British Standard ISO27002, 2005), this is why a framework such as this is essential due to it being able to limit/eliminate those threats.

Although the paper has only mentioned the good aspects of ISO 27002 there is a slight downside to it however this can apply to most security based frameworks. Due to the constant evolution of technology people are identifying newly recognised threats and vulnerabilities; this then causes the framework to be outdated as it offers no guidance on these newly established dangers (Calder and Watkins, 2012). Even though frameworks get re-written every so often there isn’t anything anybody can do about people creating brand new threats.

ITIL

ITIL is a widely known governance framework for IT service management and is more focused on the business operations of an organisation. ITIL is known for, and adopted because of, its methodical approach for providing and handling IT services. It also focuses on the service lifecycle connected with any type of project (Cervone, 2008). The service lifecycle is an interesting one as this will enable organisations to integrate IT services/projects much easier with this framework in place. At the beginning of the article the amount of project failures was revealed and this could well be the resolution to that problematic area. Gale (2011) believes that the implementation of ITIL eventually leads to the organisation being more competitive by utilising resources to its maximum and this is what makes it different to other frameworks (Gale, 2011). Mohamed et al (2008) also backs this up by describing it as having two goals, increasing IT service quality and decreasing IT costs (Mohamed et al, 2008). It’s very important to understand that it’s not only the security aspect that causes failures but also the business side of things so the more organisations realising this fact the better. From Mohamed et al and gales comments they demonstrate that ITIL is similar to other frameworks in the way it’s process orientated but offers different advantages e.g. a more efficient approach.

A clear observation from this framework and what it offers is that it could easily teamed up with a framework that is more technical based such as ISO 27002, this way organisations can have a well-rounded governance structure. Integrating two frameworks can only help and benefit a company especially
one that is IT based. For example ITIL would take care of the business aspect of things whereas ISO 27002 could ensure the integrity of the information is intact.

**COBIT**

COBIT is a self-audited framework that again mixes the business and IT side of the organisation and tries to combine the two together similar to ITIL. With COBIT being self-audited it is essential that employees are trained to the highest level as they will be responsible, if training values aren’t taken seriously poor governance can be a result of that and subsequently failures occurring. Morwood (1998) who looks into business continuity and whether it’s important to implement training alongside the continuity plan itself, goes onto to state that a plan is only as good as the company’s capability to actually implement it (Morwood, 1998).

Simonsson and Johnson (2006) have looked into the governance topic area and conducted a case study based around the Cobit framework. The authors have divided the framework up into different sections and these are: Plan & Organise, acquire & Implement, Delivery & Support and finally Monitor and Evaluate (Simonsson and Johnson, 2006). Each of these sections has control objectives which are the results that should be achieved via the processes via the Cobit framework; this is a useful way to check whether the framework has had a positive effect on the organisation.

**V. EXAMPLE OF AN ORGANISATION FAILURE**

To show how devastating a disaster can be to an organisation an investigation into some previous failures that have materialised due to poor governance. One of the most notable and well known failures relating to SME’s is the Knight Capital situation. Knight Capital lost around $440 million in approximately 30-45 minutes due to something that they called a ‘trading glitch’. This glitch caused by a software update managed to interfere with the algorithm concerning its shares (Heusser, 2012). From this malfunction there were several consequences for the company even without mentioning the $440m which was three times their annual revenue. Shares plunged 80% in two days which resulted in the loss of clients and most importantly their reputation being severely damaged.

When reading a failure such as this it makes you wonder was there anything that could have prevented this or something to halt it from escalating as it did? ISO 27002 has a section dedicated to risk assessment with three categories: identify, quantify and prioritise. Having researched the failure it seems that this scenario hadn’t been thought of by directors as they had no answer to it once it had occurred. If the scenario had been considered and gone through the three stages then the company would have had a much larger chance of surviving the failure and more likely to halt it.

**VI. DO THEY ACTUALLY WORK??**

It’s all well and good suggesting these as solutions but do they actually work and provide sufficient governance to end/reduce these failures from happening. Although there hasn’t been any direct research into frameworks and their effectiveness within organisations, there are some statistics provided by PwC (2012) that deliver a great perception of frameworks.

![Figure 2. (PwC, 2012)](image)

Figure two demonstrates how many respondents from the survey have actually implemented the ISO 27001 framework, surprisingly 42% of small organisations haven’t even thought about implementing the framework. Although figures for other frameworks haven’t been published it’s likely to be the same across the rest of them, and this is probably the reason for companies still experiencing failures. Therefore these statistics confirm that if everybody applied some sort of framework to their company they would have a much better chance of surviving anything that was thrown at them.

**VII. CONCLUSION**

From the research done in this paper it’s evident that this is a problematic area via the statistics provided, these show that nearly all businesses encounter a security breach at some point. Having looked at the areas in which organisations are failing the appropriate frameworks have been investigated into to see how they could help them not becoming a victim of poor governance. From the PwC figures about ISO 27001 it shows that companies aren’t taking governance frameworks seriously which is extremely worrying. Studying the frameworks has shown that they provide a systematic approach to their respective fields e.g. security or business continuity. These approaches enable companies to create a clear strategy of how to run/protect aspects of their organisation resulting in good information governance. From this good governance it delivers good efficiency throughout the company allowing it to function more proficiently.

To answer the article title of whether companies should be considering governance frameworks it clearly evident they should be. Failures are going to continue to happen until companies realise how important governance frameworks are and the positive effect they can have on an organisation.
REFERENCES


Are you Aware of the Causes and Consequences of Technology Induced Stress in the Workplace?

A Message to Corporate Managers of Small to Medium Enterprises

Natsayi Mlotshwa
University of Derby
Derbyshire, UK
n.mlotshwa1@unimail.derby.ac.uk

Abstract - Following a range of surveys conducted by Rosen and Weil between 1987 and 1989, the researchers revealed that between 33% and 50% of teachers exhibited some degree of technophobia. In his study in 2010/2011, Aquilina identified that 56% of the respondents in the Maltese government exhibited some degree of technophobia. This suggests that nothing much has changed in reducing technostress levels in the last 20 years which coincides with the recent study in 2012/2013 which revealed that 70% of ICT users within the Derbyshire Healthcare Foundation Trust experienced some degree of technophobia. The information highlighted in this article is aimed at helping employers, especially Corporate Managers of Small to Medium Enterprises, to root out the key issues which are generating stress amongst their employees so as to strive higher satisfaction levels and improved productivity, as well as sustain high levels of commitment amongst employees.

Keywords - IT, Technology, Technostress, Technophobia, Stress, Workplace, SMEs.

I. INTRODUCTION

Speedy access to information and simplicity of communication are the short-term benefits of IT. However, research has revealed prevalence of IT-related stress (technostress) and its associated risk in the workplace (Rosen and Weil, 1995; Kupersmith, 2003; Ragu-Nathan et al., 2008; Tarafdar et al., 2011) due to technology’s rapid change.

In the context of this article, Huwe (2005) defines technostress as the challenge of keeping up with the rapidly changing technologies. so, is it the technology or stress which must be managed or both? Following a survey by Kupersmith (2005), it was revealed that 73% of the 92 respondents regarded technostress as a serious problem. In a survey by the Health and Safety Executive, there were 428 000 out of 1 073 000 of work-related illnesses highlighted with work pressure and the lack of managerial support cited as the leading stress factors (HSE, 2012). In October 2011, Prevent conducted a survey comprised of over 600 Swedish workers. The results suggested that as many as one in four workers had a negative experience whilst using IT at work. Tarafdar et al. (2011) conducted a study on 233 Information System (IS) users, in which it was revealed that 80% of the respondents felt IS had made their work even more stressful as a result of higher technological use.

Literature suggests that work stress can negatively affect an employee’s work performance which can then have undesirable effects on the organisation (Ragu-Nathan et al., 2008; Tarafdar et al., 2011). This is a huge challenge faced by corporate managers of SMEs. It would therefore help the managers if they understood the risk factors. This, in combination with detailed knowledge about the needs and habits of personnel, can go a long way to allow the development of best practice in order to withstand the pressures of technology induced stress as well as avoid detrimental effects to both the employer and the organisation as a whole and ensure that staff are happy, and healthy and that high levels of satisfaction are maintained amongst employees.

A. Background

The reason for this study is to highlight the causes and consequences of technostress on SMEs. This is important because many of the Corporate Managers of these SMEs may not be aware of their existence which gives them something to think about as they have a duty of care and responsibility to their employees. Additionally, knowing how technostress affects employees will enable SMEs to devise appropriate mechanisms to handle it and help increase productivity and sustain a high level of obligation among the employees.

II. HOW DOES TECHNOLOGY CAUSE STRESS?

ICT stress can arise when the volume of information and demands on communication become too great to deal with (Prevent, 2012). Technology can generate stress as a result of numerous aspects.

A. Techno-overload

Though technology is perceived as a tool for improving productivity and efficiency, it escalates the pace at which employees work and thereby producing more work in shorter periods. However, this can result in increased workload and thereby leaving the employee feeling pressured to work quicker (Ragu-Nathan, 2008). A good example is the uninterrupted flow of emails at work that necessitate answers. Imagine being interrupted consistently when performing a particular task to respond to emails as this will take some time to refocus one’s full attention back to the task before another message comes in and the cycle starts again.
B. Techno-invasion

The capability of technology to keep employees continuously connected to their work wherever they are, at any given time, has resulted in employees feeling that technology is intruding on their personal lives (Ragu-Nathan, 2008). As a result, there is a work-home conflict and employees may be left feeling having to sacrifice their personal commitments whilst dwelling more on their work, at times, even out-of-hours. The constant access to the internet may mean being in touch with one’s work even after working hours.

C. Techno-insecurity

Technological implementation in the work environment has generated job uncertainty amongst employees which emerges when a user may feel threatened about losing their job to someone else who seems to understand the new technology better. It is not uncommon to find fresh, usually younger, workers who come well equipped with a greater comfort level which may lead to insecurity and stress amongst existing workers (Melchionda, 2007; Ragu-Nathan, 2008).

D. Techno-uncertainty

This phenomenon induces fear in that computers are taking over employee roles as a result of the constant and rapid changes in technology causing a great deal of stress amongst ICT end users. This rapid change does not give employees the opportunity to develop a base of experience for a particular system which they might find unsettling because it means their knowledge becomes rapidly obsolescent (Ragu-Nathan, 2008).

E. Techno-complexity

Due to the fast changing technologies, end users may feel incompetent and inadequate, always finding themselves in need of learning new things and upgrading their skills. To this end, users could find this intimidating and thereby consequently feel stressed (Harper, 2000; Ragu-Nathan, 2008).

In her study, Ennis (2005) also established lack of standardisation, lack of or poor training and documentation, increased workload, changing roles and rate of technological change as the six main causes of technostress amongst Librarians in the United States of America.

III. CONSEQUENCES OF STRESS CAUSED BY THE USE OF TECHNOLOGY IN THE WORKPLACE

Brod (1984) reckons that if technostress is not managed efficiently, it can be detrimental both to the individual and the organisation. Although some individuals may be easily receptive to the technological changes, others may be resistant.

First and foremost, Brillhart (2004) states that stress can affect physical health which is usually made worse by increased heart frequency, high blood pressure, muscular tension, frustration as well as depression. According to the survey by Prevent (2011), IT-related stress can lead to health problems for individuals such as insomnia, memory disorders, depression and an increased burden on the cardiovascular system which ultimately results in a lower output and efficiency in their workplace. The survey also highlights that the brain goes on autopilot when under ICT related stress, which can lead to big and costly mistakes.

Since the internet explosion, most SMEs became the first adopters of this tool in a bid to educate its users of the benefits of the internet and to guard against their precarious existence. Saunders (1999) describes more end-users experiencing physical and emotional stress when adapting to the fast increasing complex technologies, causing greater levels of absence and turnover, escalating costs of training new recruits and increased litigation costs associated with stress at work.

When an employee perceives their work to be too much forcing them to do more in less time, they may experience role related work overload. This can cause anxiety on the part of the employee and hence they become unhappy and frustrated when they feel they are not coping with the demands of their work which, in turn, can lead to job dissatisfaction reduced productivity (Harper, 2000).

Due to uncertainty in the employment field resulting from technostress, employees may be left feeling trapped in jobs they do not enjoy doing, leading to reduced psychological wellbeing (Sunderland and Cooper, 1986).

Whilst an employee experiences job insecurity, this can lead to diminished morale (Luthans and Sommer, 1999) and this spells disaster for the organisation because it means the employee is no longer performing to the best of their ability.

Low productivity is another serious consequence of technostress which can be detrimental to the organisation as a whole (Tarafdar et al, 2007). This is because employees are constantly trying to unsuccessfully learn and adapt to new technologies (techno-complexity) whilst productivity suffers. Valuable time is therefore wasted whilst seeking technical assistance and sifting through an overabundance of unnecessary information (techno-overload). Imagine coming into work after a week’s leave, and being inundated by a pool of emails which means probably spending half a day sifting through them and responding to those that matter. This is half a day gone which could have been used productively.

Research reveals that individuals who engage in excessive multi-tasking have exhibited increased tension, reduced perceived control and job dissatisfaction which has adverse effects of productivity (Brillhart, 2004; Rosen and Weil, 1997).

When employees are stressed and not in the right frame of mind due to the causes of technostress mentioned in (II) above, there is the increased risk of errors or mistakes which can lead to a serious risk of litigation which carries significant accountabilities for damages, negative publicity and bad a reputation for the organisation. Moreover, the costs to the organisation are high as a result of reduced productivity, absenteeism, presenteeism, high staff turnover and, potentially, legal fees resulting from stress related claims.

Poor role characteristics namely restricted variety in tasks; little or no job control, increased role conflict and lack of clarity in one’s role are some of the hazards associated with the introduction of new technologies. To this end, employees may find themselves stuck with monotony, experiencing contradictory demands from managers or unsure of what they are expected to do leading to frustration. Terry and Jimmieson
(1999) point out that those employees with restricted task variability exhibit much greater stress than those with greater job control who report greater job satisfaction. High monotonous work can be detrimental in many ways because a worker can become bored with role under-load and thereby fail to give full attention to their work and this, consequently, increases the risk of poor quality work and errors HSE (2003).

IV. KEY CHALLENGES FACED BY CORPORATE MANAGERS OF SMEs

Employees are having to learn new technologies all the time due to the rapid technological changes as organisations thrive to measure up to the competition to continue to surviving. The fast changing technology also puts pressure on the Corporate Managers in that they are required to sustain organisational commitment at higher levels among workers and, at the same time, have a responsibility to these workers. The doctor will usually treat a common mental health issue by administering treatment. However, SMEs and their managers have a duty of care and responsibility to their employees by making adjustments and helping employees to manage the stress caused by the use of technology. But how can this be achieved?

V. GUIDANCE FOR CORPORATE MANAGERS IN MANAGING TECHNOSTRESS

Prevention is definitely better than cure. Corporate Managers can play an important role in addressing issues relating to stress induced by technology to alleviate its adverse effects on both the employee and the organisation as a whole. Previous technostress studies have identified some organisational mechanisms that can offset the intensity and outcomes of technostress creating conditions.

Studies have corroborated a strong relationship with regards to work design features and employee efficiency (Parker and Wall, 1998). Parker et al., (1998) stress the importance of work redesign in preventing stress and expediting organisational efficiency. Corporate Managers therefore need to intervene in improving the nature of work redesign as this would ensure enhanced employee well-being and performance. Moreover, this can help reduce the risk hazards of technology induced stress in the workplace.

Managers must be clear of what the requirements are from employees and must also apply consistent criteria to judge work standards as failure to adhere to this could lead to diminished employee morale as well as destruction of management trust (HSL, 2003).

Indeed, it would be beneficial to involve ICT end users in the implementation decision making process, informing them why new applications are implemented; involve them in the implementation planning processes, keep them informed as to how this might change workflows and encouraging them to utilise the new systems. When users feel they have some measure of influence over new ICT implementation, they will not perceive the associated changes as disruptive and may experience less techno-uncertainty. Since they would have also provided input regarding desirable system features, this gives them a sense of satisfaction and value. Involving employees in the strategy formulation process has been revealed to increase their obligation in attaining their goals towards their work (Korunka and Vitouch, 1999; Ahmad et al., 2009, Tarafdar et al., 2011).

Educate employees which includes mechanisms that educate through sharing of ICT related knowledge, and providing training and clear documentation on applications and systems to end-users before their introduction in order to increase ICT related awareness. This practice would reduce the intensity of techno-complexity, for example, by helping end users cope with the demands of learning about new ICT technologies. Moreover, this could offset the productivity reducing effects of technostress by speeding up learning and decreasing users’ mistakes in the context of ICT usage (Tarafdar et al., 2011).

Provide readily available technical support by having an easily accessible end-user help desk which is well manned by experienced persons who are responsive to end-user requests. This can reduce techno-complexity and techno-uncertainty where ICT related issues and queries can be addressed, thereby increasing end-user satisfaction. Technical support is key to reducing interruptions when dealing with workflow applications and transaction processing which, in turn, offsets the effects of decreased productivity (Tarafdar et al., 2011).

Provide innovation support, a mechanism which encourages ICT users to experiment and learn. This would include creating a general climate that promotes supportive relationships among employees, facilitates communication in which experimentation and learning can thrive. End users can be rewarded for using new technologies (Tarafdar et al., 2011).

Adopt an open communications work culture and, in addition, policies to limit unnecessary email distribution can be enacted Tarafdar et al., 2011).

VI. CONCLUSION

ICT is changing the rhythm and pace of organisational life in unexpected ways. Emerging research has only begun to explore various aspects of these changes. This article highlights that technostress is a manifestation of undesirable phenomenon created by the use of ICT in the workplace. In recognising the causes of technostress and their consequences, the article draws an urgent awareness to Corporate Managers of SMEs. Finally, in proposing inhibiting mechanisms and strategies, the article demonstrates ways for reducing and alleviating the causes and effects of technostress in order to maintain high levels of organisational commitment on the employee’s part and also to ensure the system runs smoothly and efficiently.
REFERENCES


Abstract - Ensuring user awareness of the key issues relating to information security is vital to improving and maintaining the overall level of security within an organization. This, however, is often overlooked in favour of implementing technical security methods such as anti-virus software and intrusion detection systems. This article outlines the importance of user awareness, and discusses key considerations in relation to user awareness which can help to increase the overall effectiveness of the security program.

Keywords- Information, Security, Awareness, User Training.

I. INTRODUCTION

There are numerous different methods which an organisation can employ to protect its information from unauthorised access, such as the implementation of firewalls, virus detection software and intrusion detection systems. While technical solutions such as these are necessary to avoid system vulnerabilities, the importance of user activity cannot be underestimated (Kruger et al. 2008). It is generally accepted that around 30-50% of information security incidents originate from internal sources, either by intentional attacks or accidental misuse of equipment (Johnson, 2006). This idea is confirmed in the PWC report which outlined, among other things, the percentage of security incidents which were linked directly to the actions of a staff member or other user within the organisation.

As such any information security program which is going to be implemented successfully will need to place a high importance on the human aspects, and how best to communicate the information to people of differing roles and technical backgrounds.

Despite these statistics, however, the human factor in information security generally receives much less attention and investment than the traditional technical and physical security solutions (Kruger et al. 2006). This article aims to outline the key issues relating to this subject and to provide the reader with an understanding of why users play such a central role in determining the success or failure of an information security program. It will also provide the reader with a general understanding of how best to take advantage of these user-related issues to ensure that any security programs are implemented as effectively and successfully as possible.

II. DEFINITIONS

For a clear understanding of this article a differentiation needs to be made between information security, an information security program, an information security training program and finally an information security awareness program.

The ISO 27002 standard (2005 cited in Murane 2008, p.1) defines information security as a tool to assist with the “preservation of confidentiality, integrity and availability of information”. As such, and for the purposes of this article, an information security program should be considered as the amalgamation of all processes, procedures and policies which serve the purpose of improving the information security within a specific company.

The information security training program and the information security awareness program both fall within the umbrella of this program, and each have their own specific focus. The focus of the information security awareness program is to promote a heightened importance of information security and the possible negative effects which would result from a security breach (Hansche, 2001), whereas the information security training program is generally much more in-depth and focussed on the relevant skills and issues (Wilson et al., 2003).

III. THE PROBLEM

There are numerous examples available where a company or government department has, though policy failure or human
error, lost large amounts of data. Most recently, in March 2013, the Department of Health and Human Services in North Carolina lost up to 50,000 records containing information such as social security numbers, date of births and addresses, when a contractor misplaced a USB pen containing the data (Colon, 2013; Binker, 2013). This is not a new failing, and it is by no means limited to the USA either - it was revealed in 2008 that numerous government departments in the UK, including the Ministry of Defence, had lost around 500 laptops in the preceding decade either by theft or human error (Sturcke, 2008). Most worryingly in the case of the Ministry of Defence, many of these lost laptops contained top-secret documents relating to Al-Qaeda and Iraq.

In these types of situation the loss of the data is not only damaging to the company’s ability to function - if the data lost was critical it may be difficult, if not impossible, to replace - but it can also severely damage the organisation’s reputation and trust within the general public. An information security program can have a great positive effect on reducing the chances of these types of incident occurring, and minimising the losses when they do.

These programs should cover general topics such as the implementation and maintenance of physical security methods such as firewalls, anti-virus products, and encryption systems. Solely focussing on physical measures, however, is generally considered to be a naive approach, and for such a program to be effective it is critical that the importance of information security awareness throughout all levels of the organisation is not underestimated.

In light of these issues, one suggestion to counteract them is the implementation of a specific information security awareness program as a part of the organisation’s general security policies and procedures (Kruger et al., 2006). The general purpose of these awareness programs is outlined in BS7799-1 (2000, cited in Kruker et al. 2006, p. 1), as being to ensure that all users within an organisation are both aware of the potential security risks within their working environment, and have the relevant skills and training to help reduce these risks and promote the general security within the organisation.

IV. THE USER FACTOR

Numerous methods have been outlined by researchers by which an effective program can be created and implemented. These, in general, focus on the types of information which should be considered during the design stages, what information should be presented to different groups of users, and how best to judge how successful the program is once it has been implemented.

The three main phases to implementing an information security awareness program were identified as the assessment, identification and education phase (Valentine, 2006), however the specific methods and details tend to vary from method to method. Despite this variation, however, one key principle is outlined in the majority of these methods - that there is no ‘one-size-fits-all’ solution (Wilson et al., 2003; Hansche, 2001; Valentine, 2006). Attempting to implement such a generic ‘blanket’ program is generally much less efficient and cost-effective than if the program was specifically tailored to suit the organisation (Valentine, 2006). As such, any development of security programs needs to pay very close attention to the users within the organisation, in order to ensure that the program is relevant and applicable to the working environment - it is the users within the company that will be most affected by the policy changes, and it is also these users who can, willingly or otherwise, pose the greatest risk to the security of the organisation’s IT infrastructure.

Just as there are numerous methods available for implementing such a program, there are many possible barriers which have been identified to increasing awareness and improving the behaviour of users towards information security. One such barrier is the idea that most employees either don’t want, or have the time to read through documentation on security policies, standards and procedures (Peltier, 2005).

Another consideration is that, for most users, there will always be a trade-off between applying the strict security processes, and working in a manner which, at least for the user, is more efficient and simplistic. This trade-off can be outlined using the example of a fairly standard password policy, where instructions are to use a complex password consisting of letters numbers and symbols, which then should not be written down or shared with other people.

While this is clearly a secure way of working, it can put users in the position of choosing between choosing a complex password which they are likely to forget, and creating a simplistic password which would be much easier to guess. As such, to achieve a better balance, it could be better for both the user, and the overall security of the organisation, if the user was to create a strong password which was written down and stored in a safe place (Murane, 2008).

Furthermore, one additional issue is that of maintaining a user’s attention and ensuring that they actually see the information provided to them as being useful, and relevant to their work. All too often, information is generalised to meet a wide variety of audiences, but this just leads to employees viewing the information as being ‘canned’ and as a result, they will see it as just being “something they have to do” as opposed to something which is actually relevant to them (Wilson et al., 2003).

From the examples outlined above, the barriers to successfully implementing an information security awareness program within an organisation could be summarised as follows;

- Ensuring that users have an incentive/willingness to familiarise themselves with procedures and best-practices relating to security
- Ensuring adherence to the outlined procedures and policies instead of taking the ‘easier’ workflow
- Maintaining interest in the program, and the information it is providing

It is clear that all of these points would have a severe impact on the effectiveness of the program, and as such, the best way to mitigate these factors must be carefully considered during the design and implementation of any information
security awareness program. As a result of these observations there have been a number of suggestions made as to how an organisation can use this knowledge to better tailor their awareness program, and to ensure that it is as effective as possible.

The issue of ensuring that users have the incentive and willingness to pay attention to procedures, documentation and awareness group sessions are both interlinked, in that they both require similar considerations to ensure the overall effectiveness of the program. One suggestion is to ensure that the information is easily accessible, and is clear and easy to understand (Hansche, 2001). This may seem like an obvious statement, but with a subject as nebulous and detailed as information security, it can be easy to fall into the trap of trying to give users all of the information relevant to the subject, as opposed to just focussing on the information that is actually relevant to them.

Awareness material should be regularly distributed and kept up-to-date, perhaps using examples which are either directly affecting the organisation at that time, or that are currently in the media (Hanshe, 2001). While this type of material would usually be more generalised in order to simply portray the main points of importance, awareness group sessions should be designed in a more targeted manner.

The sessions should focus specifically on the needs and knowledge level of the users, and should directly address issues which the users actually want and need to know about to help them support the organisation as a whole (Peltier, 2005). These sessions are considered to be most effective when they are kept relatively short, and with smalls groups of users in each session (Albrechtsen et al., 2010) - this can, in turn, help to ensure that the information provided is more concise, and will help to ensure maintain the users’ interest in the information being provided. These considerations can also help to ensure user adherence to the relevant policies and procedures, as it has been found that where the information provided seems to have been specially designed for that user or group of users, it is much more likely that the message will actually be incorporated into their workflow (Wilson et al., 2003).

V. CONCLUSION

The implementation of an information security training and awareness program within an organisation can result in great improvements to user attitude and behaviour towards security in general, providing it is implemented effectively. All too often, however, information security programs tend to focus on technical security measures such as anti-virus programs, firewalls and intrusion detection systems.

This technical approach, while completely necessary, is a very limited approach. If the program is to be effective it is important to give serious consideration to the users themselves. This means that the program must be carefully designed and tailored to focus on the different groups of users within the organisation, and their specific training and awareness needs (Thomson et al., 1998).

Focussing on groups of users in this way will help to reduce the time required for awareness group sessions, and will ensure that the information provided in the sessions can be specifically focussed towards the working roles and requirements of the group. This is particularly important, because if there is any confusion about how the information and instruction should be applied, then the level of insecurity within the group or individual will be decreased - especially if the user already lacks confidence in relation to IT and security in general (Murane, 2008).

Finally, from the range of research available on this subject, it is clear that while there are a number of differing opinions and methods being put forwards, they are just that – opinions and suggestions. The information in this area needs to be seriously considered to improve the overall quality and effectiveness of awareness programs and materials, however they should not be considered as direct instruction or requirements. The most important thing when designing and implementing an information awareness program is to ensure that it is designed and specifically tailored towards the culture and working environment where it is to be implemented.
REFERENCES


Social Engineering and how it Affects Your Business

Discover the Tactics Used by Social Engineers and how to Protect Your Business and Data

Greg Mott
University of Derby
Derbyshire, UK
100124071@derby.ac.uk

Abstract - This article looks at a very prominent threat to information security for SME’s, social engineering attacks. It will look closely at the types of attacks that are used, how they work and most importantly, how you and your business can effectively defend against them. It will also cover current issues and weakness within current social engineering defenses and how to strengthen them.


I. INTRODUCTION

Threats to small and medium sized enterprises (SMEs) are great and varied. From natural events such as fires and flooding’s to digital threats to a company’s network infrastructure and data, even corporate espionage, disaster recovery, business continuity plans and digital security all help to protect and recover from such events, but one type of attack that is often overlooked by businesses, left unprotected against, is social engineering. Motives for digital attacks or hacks have many reasons, from ‘hacktivism’ for some cause or ideal, but the most common reason is financial gain; as information such as login details, e-mail address and DOB all have a price and someone willing to pay for it on the black market. With this sensitive company data being the life blood of many business operations, the amount of outside attacks targeting it increases and simultaneously the need for a defence increases (Sarkar, 2010).

Social engineering is the use of social, cultural and technical tactics to deceive and manipulate a human into giving the attacker access to the network or confidential data, which they are not authorized to access (Peltier, 2007). SANS identify social engineering as a formidable threat to most secured networks and how the danger is very real and not easily defendable (Gragg, 2002).

This paper will inform readers about the types of tactics used by this specific type of hacker, how attacks can be identified and defensive measures that can be taken to deal with the danger posed by the social engineer. To build an understanding of social engineering, it is important to understand that it is not one specific type of attack; the term encompasses a large and varied range of attacks all with a founding on a social element, but can contain very sophisticated technical elements also.

II. IDENTIFYING THE RISK / TACTICS

Social engineers works as it focus on what is commonly accepted as the weakest point in computer and information security, the human aspect (Mitnick, 2002). A traditional hacker may spend hours, days even weeks trying to crack usernames and passwords, where as a social engineer will simply ask for it. This may sound so simple that it could never work, but the unfortunate truth is that it does, with a study being conducted in which just over 70% of commuters approached in London’s Liverpool Street station shared their password for a bar of chocolate (Furnell and Zekri, 2006). These types of attacks work, as the social engineer creates situations in which they can control to extract the data they want; by learning key staff member names and company jargon and having a key understanding of how cognitive bias work (Raman, 2008), they can effectively manipulate the victim. This can be used by impersonating a high level member of staff; creating a high pressure situation with a more junior member of staff to manipulate to releasing confidential data as they do not want to go against a higher level member of staff.

Social engineering is a very different type of computer attack, as so many of the techniques and types of attacks do not require any hacking tools or even a computer. It has been likened to simple cases of fraud (Gragg, 2002), quid pro quo is a term often associated with social engineers, by offering something for something in return. This is taken further with a type of attack known as reverse social engineering; this is when the attacker creates a technical problem intentionally, and then ensures they are in a position to fix the problem once it has been detected. This then gives them an air of credibility trustworthiness which they can then use to gain access to the secured network.

Social engineering threat does not only come from external sources over a telephone or computer, in fact, some very bold social engineers will walk right in to the building of the business they are trying to attack to look for information. This tactic detail by one of the most famous social engineers, Kevin Mitnick (Mitnick and Simon, 2011) as they see how far the can get before getting caught or spotted. Alternatively, a job can be taken as a cover providing a legitimate reason to gain access to the building. A famous example of this is a group of thieves masquerading as cleaning staff gained access to computers within the London branch of a Japanese bank and successfully
install key logger and was on target to steal £220m but the attack was shut down by the National High Tech Crime Unit (Sarkar, 2010).

Not all attacks are dependent on interacting with another individual, instead just capitalising on their actions and mistakes. With data being so precious, how it is disposed of and displayed is of vital importance but can often be over looked. Dumpster diving is a common oversight, as often office waste can hold a great deal of valuable information such as memos, work orders and confidential data. Identification documents can also be to easily accessible, with many organisations requiring ID to be worn these badges can often be attached to clothing or worn around the neck. The problem occurs when they are worn outside of the working environment, for example if displayed when on lunch as a local restaurant they employee becomes a target for several reason (Mitnick, 2002). Firstly, a social engineer can gather information from the ID to engage the employee in conversation which they may release some information. Secondly they are able to view the ID, which can allow them to create forgeries, extract data from magnetic strips and even steal them from the person and try gain access to the building before it is reported missing.

Email is a very common delivery method used by social engineers. As nearly all business will have email addresses it is easy to target a large audience, as well as a very cheap and time effective method. How the email can be used also varies, phishing emails are common, in which they mimic reputable companies (such as PayPal, banks, ecommerce websites) and attempt to trick the recipient to enter in credentials. Alternatively they can have malware attached which they will aim to get the recipient to download often with the lure of a prize or free gift. Phishing attacks are growing but more importantly, it is who they are targeting that attention needs to be focused upon. SME’s make up 28% of target as shown by fig. 1, so is a real threat to them, especially when you consider that 1 in 358.1 emails is a phishing email (Goldman, 2012). Furthermore SME’s (up to 250 employees) is the second most target business; it has been suggest by Goldman (2012) this increase in phishing attacks on SME’s from 2011 to 2012 is due the fact that typically the smaller businesses have weaker security than larger competitors.

The increase of social media has also been noticed by social engineers are now use this as a platform to launch attacks from so use of social media in the professional environment should be carefully considered, KPMG e-Crime report 2011 discusses how the future of malware delivery and social networking are inextricably linked (KPMG, 2011); so websites such a Twitter are more dangerous to information security than they initially seem.

III. DEFENCE OPTIONS

To be able to effectively defend against the social engineering threat, it is important to not only understand the types of attacks that have been discussed but also the underpinning tactics used by social engineers which make them so effective. Also digital defence strategies typically consist of large amounts of software and hardware, however technology cannot fully protect you from social engineering because the firewall, Web server or database is not the target (Barber, 2001). A study carried out by Verizon in 2012 found that “97 % of breaches were avoidable through simple or intermediate controls” (Verizon, 2012) highlighting how social engineers will capitalse on the weakest point, which is often manipulated through the use of social engineering tactics.

The most widely recognised defence, and considered as the most effective defence is education; as it is the human they are attacking, it is the human element that must be strengthened. By educating staff with the tactics used, they are able to spot the attacks much more easily, as many are unaware of the threat and risks; and in their overzealousness to do a good job, they can compromise security in the process (Sarkar, 2010). Policy is also key, policies vary depending on each business needs but should a wide range including:

- Physical security – should cover ID badges and access to building and how to treat visitors. Locks on secure rooms, server racks, CCTV
- Password management – should implement complex passwords that must be changed at regular intervals. Also include the reset password process so that it is secure, could include security questions.
- BYOD policy – Policy that covers staff using their own device at work, including laptop smart phones and tablets, and if they do use them, what standards they must adhere to.
- Acceptable usage policy – clearly define what is allowed in term of use of internet and particularly social media with it fast becoming a popular avenue of attack by social engineers (Boshmaf et al., 2013).
- Sensitive data – Define the classification of data and the authentication process of how to gain access to such data.

Hardware and software have their part to play in a social engineering, as although the primary attack will focus on the human, it has to be considered that if they are successful in penetrating the first layer of the defence plan, they will then be stopped by the second, hardware and software solutions. There is very sophisticated social engineering toolkit (SET), that enables users carry out technical social engineering attacks.

![Figure 1. Distribution of phishing attacks (Goldman, 2012).](image)
(Pavkovic and Perkov, 2011). This allows even inexperienced social engineers to carry out complex attacks with very little understanding, making the risk of complex attacks greater as these tools become more widely available and complete in terms of the range of attacks SET can perform. This is why hardware and software still play a vital role, the expected defences of firewalls and antivirus are typically installed by default, but there are some further points that can sometimes be over looked. SET takes advantage of out of date and unpatched security flaws in browsers and operating systems, which can be easily defended against by keeping up to date, making you protected by many attacks. Another key attack SET is used for in carrying out man in the middle attacks in web browsers, getting victims to give away personal and sensitive data, which can be defended against in two ways. The first being education that has been previously mentioned, but corrected configured webservers with appropriate security measures that detect this form of attack and automatically shut it down before any damage can be done. This is done as by performing a man in the middle attack will remove the security certificate from the website which can be easily detected (Pavkovic and Perkov, 2011).

If an attacker in within the network or system they can begin with their desired tasks, downloading data, infecting systems and installing backdoors so can have remote access to the system (Mitnick and Simon, 2011). As after spending the time and effort into getting to this point in the attack, they don’t want to be locked out by something as simple as changing the password on the account they hijacked (Mitnick and Simon, 2011). This is why defences such as intruder detection systems (IDS) can be so valuable in tracking down attacks who have managed to bypass all the security in place to get to this point.

IV. INCIDENCE RESPONSE

Very few system anywhere are 100% secure and at no risk from some sort of attack, and this is the reason why preparation is needed to be made if the circumstance in which a data breech is suffered. As detailed in SANS multi-layered defence plan against social engineering, incidence response policy is key to shutting down attacks is very time critical (Gragg, 2002).

A system needs to be in place in which employees can report suspiscious events, so that the attacker can be actively located and hacks terminated. Also to hinder the attacker’s process, proactively informs other members of staff that are more likely to be victims so they are mindful of what’s on going and what to expect if they come in contact with the attacker. Gragg (2002) goes on further to explain how instances should be dealt with by one person or team so that they can be more effectivly monitored and recorded.

V. CURRENT DEFENCE ISSUES

The main issue with current social engineering is not the defence strategies, is not the defence methods, but the implementation of them. It is not enough to simply create a security policy to defend against social engineering; it must actively be enforced by all colleagues at all levels (Barrett, 2003). All it takes is one member of staff to fall for social engineers attacks to comprise the system security as social engineers will always focus on the weakest point.

Many issues arise when security procedures are not fully implemented by every member of staff as this allows greater success from the social engineers point of view. A key example of this is tail gating, when security door are put in place, they only work if every person, with no exception uses authentication method in place to gain access; whether that be a smart card or pin code. When someone asks you to hold the door as they run up behind you, it is human nature to be polite and hold the door, but it is this trait that the social engineer relies on and takes advantage of. Whereas if the policy of checking ID upon entry is fulfilled by everyone this can be avoided and attacks can be prevented.

A key area that can be overlooked when implementing new security policy is actually defining what information is confidential and who is allowed access what (Mitnick and Simon, 2009). If this key point is not very clearly defined to all personnel then data leaks are more likely to happen. It should not be expected for employees to make these decisions for themselves, in the majority of cases, as these are the types of situations and weak points that a good social engineer will take full advantage of.

The issues so far discussed in this paper can be linked to one overriding issue; education. Implementing the correct policies, installing required hardware and software is the first step, but if the employees of the SME do not understand why they are in place, and the real dangers, they are not going to actively fulfil them or be aware of the dangers in not sticking to the policies in place. Members of staff do not typically make the connection between letting someone use their PC, opening a door or sharing a file to the huge security risk that the action could have. This is not to say it is because they do not care or have no interest in security and keeping the company safe, but simply because they are unaware of the present danger and what a social engineer can do in that situation (Barber, 2001). Nor are they aware of the costs and negative implications it can have for the business. The following analogy seems fitting; you can have a top level burglary alarm system at home, with high tech sensors and bars on the windows to keep burglars out. But all the security in the world will prove ineffective if you open the front door and let the burglar in. Education is the key to removing this ignorance, this lack of knowledge towards key security principles within the professional environment.

VI. CONCLUSION

It is clear that social engineering is not only a very real threat to information security, but to SME’s as a whole; as they become more priority targets for attacks. However, as shown that a well-structured, implemented and maintained security defence plan can stop social engineers and ensure the safety of your business and data. Ensuring employees understand the true costs of their actions and how they conduct themselves has an overwhelming effect on your company’s information security.
REFERENCES

Social Engineering and Business Practice
A Study into the Threat that is Social Engineering and the Implications and Consequences that it can have for Businesses.

Max Orzeszek
University of Derby
Derbyshire, UK
M.Orzeszek1@unimail.derby.ac.uk

Abstract - The purpose of this article is to identify the presence of social engineering and its effects on businesses. Initially the concepts are outlined and the scale and extent of the problem is assessed. The consequences of falling victim to a social engineering attack are defined and some of the methods for such an attack are covered. Preventative measures are discussed as to how a business can look to protect itself.

Keywords - Attack, Community, Phishing, Social Engineering, Social Networks, Spam.

I. INTRODUCTION

Social engineering is a term that encompasses a variety of different methods for the purposes of obtaining information, usually this information is of a nature such that it can be considered sensitive, the perpetrator of the attack can then go on to use this information for their own personal gain.

One such medium that these attacks are directed towards are social networks, this is the primary focus of this paper however it will also cover a few other methods that can be considered to be common such as phishing.

The leading, largest and most well-known social network is Facebook, with its reported 1 billion users (Facebook, 2013) it may come as no surprise, or even a shock, to hear that statistically speaking, 1 in 12 people browse Facebook while they are at work, whether that be from their own private devices or company computers (Schawbel, 2012) (Gaudin, 2009), it is also of note that 1 in 14 total (inclusive of employees that do not own a Facebook account) internet excursions resulted in the accessing and browsing of Facebook (Wee, 2010).

II. WHAT EXACTLY IS SOCIAL ENGINEERING

As said previously social engineering is a broad term used to describe a variety of attacks meant to result in the procuring of information. 97% of security professionals report that they are aware of social engineering presenting a threat with 43% of businesses acknowledging that they have been on the receiving end of such an attack (Dimensional Research, 2011). The following are some of the primary applications of social engineering that businesses may face:

A. Spear Phishing

What harm could an e-mail do? Quite a bit depending on the nature of the e-mail in question. Phishing is the act of tricking users into providing personal information through the use of an e-mail that appears to be from a legitimate source. Surprisingly, phishing remains one of the biggest threats that you can encounter online and is costing millions for businesses worldwide (Dawes, 2012). However phishing is not limited to email, it can be performed across any medium of electronic communication such as private messages or statuses on a social network.

Spear phishing is the act of targeting a specific group of people or an individual for the attack as opposed to a general populous. To place context onto the situation the target of the attack may be a single company. If the perpetrators are aware of which individuals work for the company and have a method of contacting them online then an attack can be attempted. The employee(s) of that company may receive a message, email or see a status from the perpetrator that is masquerading as co-worker or the company itself. The context of the message is of no relevance to us but it would be to the recipients. The contents however would include a link or attachment that appears genuine but is actually malicious in nature.

If such a link (or attachment) were to be opened by the recipient it is more than likely that the attacker will be successful in placing some form of malware on the victims (recipients) machine that can then collect, read and write data from and to the machine and, if it were a company machine, ideally spread itself throughout the company system and infect the entire network (Schwartz, 2011). An example of the potential consequences of spear phishing can be found in section IV.

B. Quid Pro Quid (Something for Something)

Would you give away your password for a free gift? According to a survey conducted by InfoSecurity Europe in 2003, 90% of office workers relinquished their password in exchange for a simple pen (Leyden, 2003). That is, quite frankly, a scary example of just how easily people are willing to disclose information if they receive something in return.

An attack of a similar nature is placing a phone call to an individual (or business) and claiming to be ‘calling back from technical support’ or similar, for example, a current method is being used throughout the UK with the caller claiming to be ‘from Windows’, this particular method is aimed at
individuals that are not proficient in the use of technology (Egan, 2012), I can personally say that I have received two such calls and proceeded to enjoy a sarcastically passive aggressive conversation with the person who was from ‘Windows’ and not ‘Microsoft’. But to return back and place context to the situation for a business it would not be strange to have an employee receive a phone call from the supposed ‘IT department’ regarding the problem they had, if the perpetrator is lucky and the recipient does indeed have a problem they can then be tricked into installing various malware to ‘fix’ whatever problem it was they were having or even give the attacker remote access into their system. (Criddle, 2012).

C. Too Good to be True (Baiting)

Baiting is the act of offering a piece of software, or presenting a piece of media, that appears to be something harmless or genuine – akin to phishing schemes. (Criddle, 2012) However what makes the concept of Baiting unique is that it can be applied to physical media, for example an individual (or employee) comes across a USB device that caught their eye lying in the corridor, and because curiosity has gotten the better of them they proceed to plug the device into their computer. No matter their intentions, whether to see if any information relating to the owner is present or they were simply curious what they could ‘gain’ from the device upon plugging it in and running it (or via auto run) their machine has potentially just been infected. (DarkReading, 2006)

III. WHAT ABOUT THE SCALE AND CONSEQUENCES

In the fourth quarter of 2012 the amount of spam transmitted globally per day was, on average, 90 billion messages. This spam accounts for roughly 75% of emails sent and is synonymous with phishing attempts. (Commtouch, 2013) To add another sense of scale a single phishing attack peaked at an astonishing 167 million emails being sent in a single day (Boscovich, 2012). Dimensional Research conducted a survey in which they asked IT professionals what they believed to be the driving force of social engineering attacks that they had been victim to, whether successful or not. The following displays their answers.

The prime application of social engineering is phishing, resulting in either manipulating an individual into disclosing sensitive information or tricking them such that malicious software is placed on the machine they are using. Following closely behind is social engineering applied to social networks, again this research was performed by Dimensional Research in the same survey and the results can be seen in Figure 2 below.

From the very same survey it can be seen that 48% of companies have been the victims of social engineering attacks and subsequently face a loss of, on average, $62,500 because of it (Dimensional Research, 2011). A. Identity Theft

Once the attacker has obtained a sufficient level of information regarding their victim they can potentially use this to perform a similar, and more personalised, attack on the initial victims friends which is even more likely to succeed compared to the initial one. B. Corporate Espionage

Corporate espionage is the act of information theft for purposes of, generally, gaining a competitive advantage over other competition in the market. If a business’s employee happens to be a victim of a successful social engineering attack, that infects the company systems and subsequently sensitive company data is leaked to the attacker (a rival company). C. Fraud

At its basics fraud is the use of deceptive information for personal gain, for a business this is a very prominent threat as if information regarding their customers is leaked, depending on the nature and contents of that information, it could put every single one of their customers at risk of fraud.

IV. HOW CAN A BUSINESS PROTECT ITSELF

The simplest method to securing the integrity of your business and protection of your information is to ensure that your employees understand what they are doing and what they represent. A. Employee Training
Training can be seen as implying that there is a correct method of conduct in regards to the going about of your work day. After all I doubt there are many, if any, jobs whereby new employees are simply left alone to suddenly work for the company and are expected to know what to do without them being told to. The point here is to ensure that a sufficient level of training is given to employees such that they understand the existence of social engineering, how it is performed and what to be wary of. (Schawbel, 2012) It is imperative to make sure that the employees understand the potential consequences of their actions and that it is not simply left up to them to learn and understand (Wengroff, 2012; Dimensional Research, 2011). This may of course cost the company money but if it is to ensure that they do not lose a larger amount of money in the future for the mistake of a single employee then sure it can be considered worth it.

B. Usage Policy

It is unlikely for a business not to have a usage policy already in place in regards to the use of the internet at work, however obviously it is something that is, to some extent, going to differ between companies. There are systems out there available to purchase to enforce a specific set of policies and internet usage such as GFIWebMonitor, the implementations of guidelines may also be sufficient if trust is present. It is important to note that some form of internet usage policy should be in place, and it should be of sufficient detail so that employees are not confused in any way. One suggested method for handling employees that wish to use social networks may be that they do it on their own private device and not using the company network, another suggestion could be that they have separate accounts for within work and for personal use. Restricting the read-write functions of employees based on their position within the company may also be one such solution to the problem. Regardless, usage policies are never a bad idea and there are more than enough resources available on the internet for creating them and complying with standards for business practices.

V. SHOULD BUSINESSES THEREFORE SHY AWAY FROM SOCIAL NETWORKS?

Quite the opposite in fact, a business should encourage its employees to take part in social networking, but ideally, not for extensive personal use. Social networking can be an excellent method of promoting a business – after all it is the cheapest form of advertising as it can effectively be considered word of mouth. A company that widely uses a variety of social networks can be seen to be one that is quite close to its audience, it presents the opportunity for a strong market presence if they are known to be vocal about upcoming products, events or active with their customers, obviously it all depends on what type of company it happens to be but the principles are there. (Schawbel, 2012)

VI. CONCLUSION

Within any system that involves some form of human input, it is generally that individual or group that is the easiest to manipulate or coerce into being the victim of social engineering. That is because they will generally always be present in some form or another, even if it is a fully automated system there will be a time when user input is needed (such as maintenance) and as such they may make the mistake of falling for a social engineering trap. The hint to why it is always the human lies in the name: Social. Every single type of social engineering attack hinges on the fact that communication is required between at least two parties (the social aspect) and so although there is no guarantee of being completely protected from attacks the best method of prevention is simply being aware of the possibility of it, and that would be through training.
REFERENCES


The Trade Offs for Bring Your Own Devices
Investigating the Issues and Benefits Behind the new Business Trend

Luka Page
University of Derby
Derbyshire, UK
Luka.page@ntlworld.com

Abstract—Consumerisation in IT is on the rise and with it comes the opportunities for companies to capitalize on the trends that occur. This paper presents factors to consider when adopting a Bring Your Own Device program within a small to medium enterprise, focusing, but not limiting the research to, malware attacks and issues. The paper will also touch on what exactly BYOD is, how it can beneficial to a company and why it is so popular among businesses today. Furthermore methods of mitigation for the previously discussed issues are suggested and discussed with the implementation of a robust security policy supported by the ISO standards and security software for smart devices being considered and recommended.

Keywords - BYOD, Corporate Network, Smart Devices, SMEs, Security.

I. INTRODUCTION

Small to medium enterprises have always benefited from capitalizing on technological trends and with the rise of the ‘Bring Your Own Devices’ trend SME’s need to be fully aware of the risks in allowing their employees use personal mobile devices within the workplace. This paper will focus on the security dangers in allowing an employee to use their mobile device (tablet, smart-phone, etc.) for work purposes, as opposed to supplying the employee with a secured work smart device.

The aim of this paper is to raise awareness within SME’s of the security issues of BYOD focusing on the access of a corporate network, in support of this the objectives are to suggest methods of mitigation against the threats and issues raised by adopting such a trend with a small to medium sized business, the focus of the mitigation will be on a security policy which will allow for a more secure work environment whilst still allowing users the freedom of using their own smart devices.

II. WHAT IS BYOD?

In today’s markets there are countless numbers of smart devices being adopted by consumers from smart-phones to tablets, with the majority of these consumers being employees of companies, it is growing increasingly hard to not accommodate for personal smart-devices within the work place (Burt, 2011). This new and emerging trend within the workplace is called Bring Your Own Devices or BYOD, it is a business trend adopted by the management teams to allow the use of personally owned smart devices within the work place, to perform such tasks as access corporate data, emails or other important assets (Singh, 2012).

The biggest benefit posed by the BYOD trend is that the business can save money by allowing their employees to use their own devices but first the business must establish sufficient security protocols for allowing employees to gain access to their network (Burt, 2011), from previous case studies it has shown that those companies that have transferred the cost of devices to their employees in terms of mobile devices have found the employees are happy to take on the costs in exchange for using their own devices (Hawkins et al, 2012).

Continuing on from the previous benefit research conducted has found that 80% those companies that allow a BYOD program have seen an increase in worker productivity (Trend Micro, 2012), this is due to the employees using their personal devices to communicate with other workers at any place or time as they always have their personal devices at their disposal and are more willing to use them.

A major benefit that a business’ IT department needs to consider is that in implementing BYOD staff require less training as they already have sufficient knowledge about the devices they are using, this will result in less reliance on the IT staff to support and train these users (Brooks, 2012), which in turn will free up their time to focus on other projects/programs that may benefit the business. However in not supplying training, methods of best practice will become difficult to communicate with the employees due to a lack of a physical training program placing the company at risk.

III. WHY BYOD?

The rise in companies implementing the BYOD trend is not a coincidence, there are many factors that are driving the use of BYOD programs, and this section will discuss these driving factors in terms of small to medium businesses.

The first factor that is a huge driving force behind BYOD programs in businesses is the consumerisation of IT and IT products. The consumerisation of IT is the recent development of more people acquiring their own personal computing devices such as laptops, tablets and smart-phones (Moscchella, et al, 2004) the market for mobile devices alone has grown 46% since 2011 (Ahonen, 2013); with this rise in acquisitions, comes the expectation that the users can use these devices freely within the workplace due to them being unaware of the repercussions.
Another driving factor for businesses is that with BYOD comes the benefits of ‘Green Computing’, this is the idea of IT trends that provide environmental benefits creating a better image for the company. BYOD does this by encouraging the use of personal devices reducing the number of devices the organization has under its roof at one time, in turn reducing the companies ‘carbon footprint’.

IV. THE PROBLEM

With the increased use of personal smart devices within businesses comes the rise of new cyber security threats, including loss of company data, issues of non-compliance and financial threat, with many more issues becoming apparent every quarter (Ayrapatov, 2013). Security reports state that only five percent of smartphones and tablets across the world have security software installed (Goldman, 2012), this and employee negligence when browsing the internet via these smart devices, are the main reasons for the issues of BYOD.

Studies show that 89% of employee’s mobile devices are connected to a company network with only 10% of these companies aware that these devices are even accessing their network (Fieldman, 2012), a cause for concern when such vital and confidential data is stored here. Furthermore recent surveys report that 34% of mobile device users store sensitive data on their devices, this figure effects businesses as a company cannot be certain that this sensitive data is not related directly to their company, a huge cause for concern when there is hardly any security features posed by many of today’s smart devices.

Research on a group of small to medium sized businesses found that nearly half (46.5%) that allowed for BYOD experienced a security breach due to an employee-owned device accessing their corporate network (Harris, 2012). The access of the corporate network is the biggest and most concerning issue faced by companies when considering BYOD, this is due to the large amount of confidential data stored here, such data that if exploited could damage the company.

Another issue raised by having BYOD implemented in the workplace is the idea of who actually owns the data and who is liable for said data (Hawkins et al, 2012), when establishing a BYOD policy it will be important for the company to outline that despite the data being present on an employee’s device it is still owned by the company and any other data related to that company is owned by them as well, therefore they are liable for whatever happens to the data, if something does happen to their device and the data is lost they will have to suffer the consequences be it disciplinary or other actions. This can be seen as off-putting by the user and may not motivate them to use their personal devices in fear of the repercussions.

Finally an issue that relates back to the previous issue is the loss and/or theft of smart devices (Juniper, 2011), this is a major issue for businesses as stated previously over 30% of mobile devices can contain sensitive data. The portability of these smart devices means that loss and theft are not uncommon especially due to the constant developments in the size and weight of these devices. The loss of devices can present a business with devastating consequences such as the loss of intellectual property and the loss of sensitive customer/employees information.

V. SMART DEVICE SECURITY THREATS

Smart devices left without security software or protocols are vulnerable to various cyber security threats, this section will discuss some of the most popular and biggest security threats to a mobile device, defining and discussing how they occur.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Software that is installed without the user’s consent, downloaded through fake apps in an attempt to steal personal data (Microsoft, 2012). Malware can attach to a smart device from any public network, and then spread onto the corporate network once the device connects, removing the need to bypass security measurements (Mohling, 2010).</td>
</tr>
<tr>
<td>Drive-by-downloads</td>
<td>An extension of the malware threat is the increasing vulnerability of mobile platforms to drive-by-downloads, this is the downloading of applications to the device without the person’s knowledge (Tode, 2013), downloads can include viruses, spyware and malware which as stated earlier can not only be transferred onto the corporate network, but also exploit the data already existing on the device.</td>
</tr>
<tr>
<td>Phishing</td>
<td>This is a method of acquiring a user’s passwords, credit card details and other sensitive information by masquerading as a trustworthy source, most notably this method has been implemented via Bluetooth. Attackers search for devices with the Bluetooth enabled and ‘fish’ for sensitive information, through this method an attacker can access almost all of the devices information then send the data back to their own device via the Bluetooth (Dunham, 2009, pp-131). This is a danger for businesses as the data retrieved via the attack could be the company’s property.</td>
</tr>
</tbody>
</table>

Fig. 4. A table of security attacks to smart device

The attacks above are just a few of the attacks that an unsecured mobile device is vulnerable to, methods to prevent these attacks must be undertaken by a business if they truly want their BYOD program to be a success and to financially benefit them, these methods will be discussed later in the article.

VI. BYOD AND RISK

Risk is a major factor that contributes to the Bring Your Own Devices trend, especially when considering whether to trust the user with the company’s private data on their
personal devices, as there are many environments that the users can visit using their devices where in its validity is uncertain.

Schneier (2008) discusses a user’s perception of risk and how users are often incompetent in evaluating risks appropriately due to how they distinguish them. Schneier (2008) believes that users react to risks as they occur and are not proactive in their recognition of risks.

If Schneier’s theory is proven to be true it shows that entrusting the employees of the company with safe guarding company data on their mobile devices is not an appropriate action to reduce the problem as different employees may judge the risk of visiting a website differently to others, meaning every employee in the company must have the same security measures in place, it is not good practice to grant certain employees special privileges as those employees may fail to assess risks as well as others.

VII. THE SOLUTION

The first step an enterprise should perform in order to solve the problems that arise with enabling BYOD is the adoption of a companywide security policy to mitigate the exploitation and misuse of company data from theft and loss by cyber criminals or careless employees. The security policy should be supported by and consider security frameworks provided by the British Standards Institute, more specifically ISO 27000 series of frameworks.

This specific series of standards is a set of security frameworks which when applied correctly become the backbone of a company’s security policy (Digital Curation Centre, 2009). This set of standards will be a good support for the policy as they cover a large domain from physical security which can be applied to the smart devices, to the principles of implementation that they outline, which aid the enterprise in applying and maintaining policies (ITGI, 2005).

Implementing a comprehensive information security policy can be difficult however performing a thorough risk assessment as suggested by the ISO frameworks will help determine areas of focus, a risk assessment will ask questions such as the following:

- What business assets need protecting?
- Are these assets physical or digital?
- What specific threats exist that target these assets?
- What damage can be caused if these threats occurred?

The main focus of a risk assessment is to prioritise which information assets need immediate attention and protection, as well as analysing whether these ‘safe-guards’ will be cost effective for the enterprise (Mitnick & Simon, 2011, pp-260-262).

The application of the ISO 27000 standards will guarantee the probability of risks is reduced or removed completely through the agreement of a security framework which will be applied companywide (Digital Curation Centre, 2009). Another benefit to using the standard is that it also offers appropriate actions for the administration of digital and physical data, maintaining its integrity, accessibility and confidentiality through methods such as training, identifying and restricting the employees were deemed necessary. It also provides procedural context for keeping a constant list of physical and digital assets to aid the monitoring process (Digital Curation Centre, 2009).

As mentioned in section IV the loss and theft of devices can create devastating repercussions for a business, the solution for this issue can be found in the implementation of the aforementioned security protocol, when creating the policy ensure that you allow the data management team to be able to remotely access and disable a employees smart devices, for this the employees permission is needed so it must be highlighted in the policy that in the case of loss/theft a remote wipe will be implemented (Chickowski, 2009).

To further solve the issues generated by BYOD a business can choose to purchase and implement a third-party security product, these products focus on adding robust security functionality to smart devices (Dunham, 2009, pp-373) such as malware protection. The implementation of a third-party security product can help support the company’s security policy by making the user more aware of the security issues they face when using their personal mobile devices.

VIII. CONCLUSION

This study set out to find and solve the issues faced by a small to medium business when implementing the current trend of Bring Your Own Devices. From the research conducted and discussions made it can be determined that the major issues faced when implementing such a program within a business can be mitigated through the creation of a versatile information security strategy that focuses on the use of personal devices by employees and the importance of assets within the company.

This paper has also discussed without bias that in regards to a small to medium business a BYOD program can be beneficial if the correct security procedures are put into place, research in section II has shown that a company can not only benefit financially but will also see an increase in employee productivity due to morale being high.

It can be concluded that the findings and discussions made support the revelation that whilst it being a venture filled with risks (See section IV/VI) BYOD can still be a profitable and beneficial venture if the issues are mitigated correctly through a robust and detailed security strategy that will protect a business’s physical and digital assets.
REFERENCES


BYOD: Implementing the Right Policy

Pell, Luke C.
University of Derby
Derbyshire, UK
chukpell@gmail.com

Abstract - With the growing number of data endpoints connecting to an organisation's network, the need for a robust, secure policy is more relevant than ever. BYOD and the general consumerization of IT are presenting IT professionals with unique challenges. Is there a way to reap the benefits of BYOD whilst maintaining a rock solid data protection plan? This paper highlights the key areas that should be approached when considering the implementation of BYOD in your business.

Keywords - BYOD, Bring Your Own Device, mobile computing, IT policies, consumerization.

I. INTRODUCTION

When researching implementation strategies on corporate mobile management, it is likely you will come across the acronyms 'BYOD' and 'CYOD'. BYOD stands for Bring Your Own Device whilst its sister strategy CYOD stands for Choose Your Own Device. Both are mobile strategies that define how mobile devices should be implemented into a corporate eco system. BYOD is a system that allows employees to bring their own personal devices into the workplace and use such respective devices to access corporate data. Scarfo (2012) believes that BYOD comes from the concept of 'consumerization'. He cites the growing tendencies of new technologies appearing in the consumer market having a large impact on the scale of devices being used in the corporate arena. A well implemented BYOD plan can lead to:

- Cost Savings – The device and hardware costs are transferred onto the employee.
- Employee Satisfaction – The employee has the flexibility to work where and when he/she is needed.
- Less device support – As the ownership of the device is transferred to the employee, the IT team can spend less time providing end user support.

CYOD is a strategy, that while still embraces the core aspects of 'consumerization', reduces the amount of devices an employee can choose from to access corporate data. Conversely to BYOD, all aspects of purchasing and maintaining the device are assigned to the employer and not the employee.

This paper will highlight the key areas of an efficient BYOD plan and offer guidance in areas that can seem challenging to IT professionals. The benefits of a reduced mobile spending budget and a more comprehensive out-of-office working environment can see tempting to an employer; however one has to consider the security implications of a BYOD based approach. Whilst in general, this paper analyses the core aspects of a BYOD implementation plan, the majority of advice can be replicated to CYOD based policies.

II. BYOD – WHAT CONSTITUTES A 'DEVICE'

One of the biggest transitional issues when adopting a BYOD policy, is the acceptability that data will be delivered to devices that are not directly managed by the organisation's IT department. Marrow (2012) identifies that organisations have less control and 'fewer mitigation options' in terms of regulatory compliance. The threats of data theft and data leakage fundamentally increase with the introduction of unmanaged devices. Morrow also highlights that the 'D' in BYOD isn't limited to just smartphones. The identification of devices within a BYOD policy is fundamental in ensuring that potential data leaks are plugged. With the growth of cloud computing and mobile technology; anything from web applications such as 'Dropbox', to physical devices like tablets, should be considered as a viable 'device' (Morrow, 2012).

Cisco (2012) concluded from its IBSG horizons Study, that by 2014 it is expected that the average number of connected devices per worker will reach 3.3. Each endpoint will consequently have its own associated weaknesses and thus it is important that an efficient policy identifies and mitigates each risk individually. Having technical measures in place to identify the type of device connected to a corporate network is essential in ensuring unidentified devices have limited access. It is the opinion of this paper that any device undefined in the scope of the BYOD policy has very limited access to corporate resources.

To ensure that risk is kept to a minimum, each defined device in the respective policy should undergo a generic risk assessment. An assessment could cover features such as: update schedule, encryption abilities and its ability to jail break.

III. DEVICE VARIATION

With Android (2013) alone defining over 1500 officially recognised devices from 50 different original equipment manufacturers (OEMs); it is important to understand the risks of opening up a corporate network to a potentially unlimited amount of different operating platforms. The table below illustrates the growing number of smartphone platforms that are occupying the current consumer market. It is clear from the figures that the two dominating forces on the market are the operating systems: Android and iOS. With a consumer market share of nearly 90%, an efficient implementation plan should identify and initially target these two platforms. Priority to
Android and iOS should be given in terms of support and training to both IT support staff and network administrators.

<p>| Worldwide Smartphone Sales to End Users by Operating System in 4Q12 (Thousands of Units) |
|-----------------------------------------------|-----------------------------------------------|</p>
<table>
<thead>
<tr>
<th>Operating System</th>
<th>4Q12 Units</th>
<th>4Q12 Market Share (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>133,720.3</td>
<td>69.7</td>
</tr>
<tr>
<td>iOS</td>
<td>43,457.4</td>
<td>20.9</td>
</tr>
<tr>
<td>Research in Motion</td>
<td>7,333.0</td>
<td>3.5</td>
</tr>
<tr>
<td>Microsoft</td>
<td>6,185.5</td>
<td>3.0</td>
</tr>
<tr>
<td>Bada</td>
<td>2,684.0</td>
<td>1.3</td>
</tr>
<tr>
<td>Symbian</td>
<td>2,569.1</td>
<td>1.2</td>
</tr>
<tr>
<td>Others</td>
<td>713.1</td>
<td>0.3</td>
</tr>
</tbody>
</table>

Taking Android as an example, since its conception in 2009, Android has had over 9 main software updates. Each one of these software updates has fixed critical bugs and added newer functionality. The problem lies that the main core updates only instantly go to one range of devices, the ‘Nexus’ range. All other devices, such as those designed by Samsung, HTC, Motorola and Sony, each implement their updates according to their own schedules. Nilsson (2011) from Sony’s developer team highlights the key difficulties in adopting Android for each device. As the original source code of Android is designed to work only on reference devices found in the Nexus range, every other manufacturer have to create proprietary drivers and HALs (Hardware Abstraction Layers) to achieve a fully functional device (Android, 2013). The time this takes varies between manufactures as thus an ecosystem of Android devices with different software versions is created (Nilsson, 2011).

Why should you care about this? When considering allowing one Android device access to your corporate ecosystem, it is important to understand that this device may be running out-dated (and vulnerable) software. Whilst this problem isn’t as prevalent in other operating systems, the underlying point is that out-dated software poses a big risk to the security of your corporate network. As mentioned earlier in this report, it is key that your plan has measures in place to identify both hardware and software specifications of every device in your network. This could be implemented in the form of a native application that reports back to a central server or simply by requiring each employee to fill out documentation defining their device.

IV. RESPONSIBILITY

In response to the surge of personal devices entering the corporate workspace, the Information Commissioner’s Office (2012) produced a report outlining the legal responsibilities associated with BYOD. A survey found in this report concluded that 40% of employees use personal owned device for work purposes, without any guidance from their employers. The levels of responsibility on both the employee and the business will vary according to implementation. However the key areas that should always be approached are: data loss, loss of the device, remote deletion, employment termination procedures and backup retention (Wong, 2012). While this area of policy management, on the surface, seems more ‘office politics’ than risk management, ensuring that both the employee and employer are aware of each other’s responsibility is important in alleviating potential risks.

Using employment termination procedures as an example, without adequate policies in place, it would be extremely difficult for a company to ensure data security. The employee’s device would most likely contain key information about the company that could be maliciously abused or lost. The business has both legal and financial responsibility to ensure that the device can be wiped of all corporate information. Without technical measures in place to allow remote wiping, this would be extremely difficult to implement if the employee has left in unfavourable circumstances.

While the ICO hasn’t directly fined anyone for the loss of personal data, the Nursing and Midwifery Council were fined £150,000 for the loss of two DVD’s (Wilson, 2013). A DVD can hold significantly less data than most modern smartphones and thus the potential for very expensive fines are high for data security failures.

“Appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data” (DPA Seventh Principle)

Under the Data Protection Act (1998), responsibility in terms of data security, will always lie with the employer. Consequently it is important, that businesses have strong rigid policies in place, to ensure that employees are made fully aware of their responsibilities. Employees should be made aware that remote deletions, among other policies, have to be applied to personal devices. An important component of this policy will be the audit and on-going monitoring of compliance. (Information Commissioner’s Office, 2012)

It is also important to consider ISO standards when implementing a mobile policy. The original standard ISO 27001/BS7799 failed to address the use of mobile devices in the corporate environment. However with the release of ISO27002, the standard now addresses the issue of mobile devices in the corporate arena. The standard doesn’t go into great detail into how it expects mobile devices to be secured, however it expects the use of mobile “cryptographic techniques”, “backups” and “virus protection”.

V. AUDIT AND ON-GOING MONITORING

As outlined above, the Data Protection Act (1998) places the burden of responsibility on the employer and not the employee. It is the employer’s job to prove in the event of a data leak that they have completed all possible steps to ensure the principles outlined in the DPA are being abided. However the employment practices code conceived by the ISO also highlight “that employees have legitimate expectations that they can keep their personal lives private”. How can you as an employer ensure your corporate data stays safe whilst not crossing the boundary of your employees’ personal lives?

Technical measures have to be put in place to ensure that all devices allowed access to corporate data are abiding by your standard data protection measures. The key is to be clear with
your employees; you should outline every form of technical measure you are using to monitor device usage. By definition, it is clear that some use of the employee’s device will be personal in nature and thus it is important that the data monitoring techniques are non-invasive. The ICO (2012) highlight several key tips to consider when drafting a BYOD Acceptable Use Policy, including guidance outlined in the ICO’s Employment Practices Code. Drafting an acceptable use policy is outside the scope of this paper however we will analyse some of the technical techniques you can implement to control mobile endpoints.

**Digital Rights Management (DRM)** – is generally seen to protect digital media from copyright. However this paper believes DRM has a place inside the corporate security model. The foundation of DRM technology prevents unauthorised copying and generally makes it very difficult to steal digital content. DRM can be applied to company assets (data) and designed to only work on approved corporate devices. Whilst this wouldn’t protect against device loss, it allows an organisation to control the flow of information to unauthorised devices.

**Extra Points to consider:** Data can be categorised into the level of corporate importance. If data is considered ‘High Risk’, device-specific DRM can be implemented. Using unique device ID’s, an organisation can limit certain documents to devices owned by management.

**Network Access Controls (NAC)** – A NAC allows an organisation to see who exactly is on the corporate network. The biggest issue with BYOD is the lack of visibility in terms of who is accessing corporate resources. An NAC helps establish who and what is connecting to a corporate network. (Bbosa, 2012) By logging and monitoring all devices that have access, you are identifying to the ICO that you are taking all possible steps to prevent data leakage. Plus NAC solutions help you dynamically block devices you don’t want in your network.

**Extra Points to Consider:** NAC solutions can be used alongside client side apps to detect mobile devices that are breaching the acceptable use policy. For example if a device is rooted or jail broken, the application could identify this and report back to a backend server. This server could then report to the NAC and request that this device is blocked access to corporate resources.

**Application Access Control (AAC)** – As described above, a client side application can be installed on the employee’s device to monitor certain use. A complete solution could identify all applications that are running on the device and block access to applications deemed to be inappropriate for the workplace. The application could also report back all the devices specifications to ensure that the IT team is aware of all possible vulnerabilities for that version of software. If it is deemed a ‘high risk’ device, the IT support team can step in to minimise risks or block access completely. It is important to note however that AAC is an intrusive form of device monitoring. Employees would have to be made aware of all the applications functions and agree to such application running on the device.

**Extra Points to consider:** The intrusive nature of an AAC would be deemed acceptable during office hours (9-5, Monday – Friday). However the ICO may consider the use of an AAC based application outside of office hours as a step into the employee’s personal life. Technical measures would have to be implemented to ensure that active protection is only used during office hours. This could include using the devices geo-location to detect out of work activity or simply enforcing polices during certain times.

### VI. IS A BYOD POLICY RIGHT FOR YOU?

Being able to successfully create a mobile management plan for BYOD without hindering some section of users, is an extremely difficult task. You will most likely as an employer have to spend more money to support multiple devices and imposed rules will inevitably limit the amount of freedom an employee has with their device. As an employer you have to ask yourself 3 main questions when considering transitioning into a BYOD environment:

- Will it help my employees do their job better?
- What will make them most productive?
- Is the extra cost and IT support necessary to fulfil your employees desire to use their own device?

The reality is that a BYOD policy is an intrusive policy that unfortunately hinders employee productivity. In the ideal world, every employee should be able to use their device without limitations or rigorous policies. As with any data protection policy, the key is creating a framework that reduces the risk of data leakage whilst limiting the impact on staff in terms of the freedom they get from using a personal device.

Can your business improve productivity to a similar level by implementing a CYOD or COPE (Corporate Owned, Personally Enabled) plan? This will enable tighter controls whilst still encompassing the traits a millennial worker would expect. Katz (2012) works under the assumption that the art of mobile management is defined by three aspects:

- The User
- The User has a Need
- An efficient solution should fulfil that need

Now whilst this sounds incredibly obvious, it is important to understand that your end users are your employees. To completely understand whether or not a BYOD plan is needed in your enterprise, you should first consult your employees. If your employees are happy with the current system, tighten controls and improve your current policies. Undertaking the transition into a BYOD environment is a long and costly process, however if you improve the satisfaction of your employees, ultimately that process is worthwhile. If you believe that a BYOD policy would hinder more than benefit your organisation, then BYOD – *Is not the right policy for you.*
REFERENCES


The Impact of Phishing on SME’s

Luke Presland
University of Derby
Derbyshire, UK
100103886@unimail.derby.ac.uk

Abstract - Phishing has become one of the biggest threats to small to medium sized enterprises over the years. With multiple threats to company networks, the ability to adequately protect against such threats is no longer a single point solution. Software solutions have become more useful in detecting phishing attacks, but are yet to provide a suitable, economic solution. This paper discusses the need for a user focused education policy to become the main tool in a combination of multiple strategies to tackle phishing attacks.

Keywords - Phishing, Social Engineering, IT, Security, Education.

I. INTRODUCTION

IT security across all sized businesses is something to be taken very seriously. Small to medium sized enterprises (SMEs) on the other hand have a harder job, as the threats and repercussions are the same as bigger businesses, but the budget available for IT security is considerable less.

When business owners think about IT security, the big hitters that tend to be at the forefront of budget allocation are usually attacks on physical systems, authentication and privileged, attacks, denial of service and malicious content. What’s often overlooked however is that there is one common denominator between all of those risks yet is not at the top of a budget list, and that is Social Engineering.

Social engineering is the cheapest and easiest technique for attackers to gain access to physical systems, commit privileged attacks, produce a denial of service and spread malicious content. Social engineering consists of multiple techniques used to deceive unsuspecting users into providing privileged information for the use in a myriad of crimes. Phishing, as a method, is one of the most challenging security threats in a social engineers arsenal, with phishing costing brands and corporations over 200 billion dollars a year according to Cisco (Cisco, 2011).

If you have ever received an email from someone you don’t know, asking you to click a link, or a bank you have no connection to, this may be your first exposure to phishing. In reality, this won’t be your first exposure, with an average 150 million phishing emails being sent every single day, you may have been a target on several occasion before (APWG, 2005). The definition of Phishing is the act of acquiring sensitive information, such as email addresses, passwords or credit card details, by pretending to be a trustworthy online communication (Furnell, 2004).

Phishing doesn’t just affect the unfortunate victim though. Phishing is involved in multiple IT security threats a business may face, including:

• Malware
• Drive by downloads
• Web Application attacks
• Targeted Denial of Service
• Data loss and theft

Covering all aspects of IT security that are important to any SME’s.

With half of Fortune 100 companies already being hit by phishing attacks, with 30% of the companies having experienced more than 20 attacks, there is a misconception that SME’s are not the target for cyber attackers (Anon, 2005). But with a recent PwC (2012) report showing that 76% of small businesses in the UK have suffered a security breach in 2011, with the average cost of the worst incident being £15,000-20,000, it is time for SME’s to realise that they are the new target.

It is obvious then that SME’s are inherently easier targets for social engineers, however linked with a study by The Hanford, finding that 85% of small business owners believe that data breach is unlikely, is a dangerous concoction of blind sidedness and naivety (Nachreiner, 2013).

II. BACKGROUND

Phishing works on the cognitive basis that people are gullible, and take things at face value. A survey conducted in 2007 shows this human nature in a non-technical situation via a survey on the streets of London. 100% of the people that were surveyed happily provided their full name to a complete stranger. More worryingly, 94% provided their pets names and mother’s maiden names, two very widely used security ploys however aims only to increase the likelihood of gaining such information when users are put in such a situation.
With not much more needed to gain access to multiple online accounts, this shows how the gathering of information can leave SME’s open to unauthorised access. This coupled with the Radicati Technology Market Research Groups estimation that in 2007 there were 1.3 billion email users, rising to 1.6 billion by 2011, opens the population to such social engineering attacks via electronic communication (Abraham and Chengalur-Smith, 2010).

III. Threats

The usual implementation of phishing begins with a fraudulent email message, purporting to be from a trust worthy source, directing users to click a link within the email to take them to an equally fraudulent website. Such a website is specifically designed by the phisher to collect the desired information, while making the user believe they are providing information to a legitimate source.

The threat of Phishing has been around for years and the reason it still continue to wreak havoc is because it still works. With Anti-Phishing.org suggesting that up to 5% of recipients of phishing emails tend to respond. If your business is around 1 – 500 employees, that’s a possible 25 staff members that will fall for this scam and respond, opening up your network for attack.

A test of employees conducted by the IRS found that 60% complied with the request from a scammer purporting to be a member of staff to change their company password. A similar test in 2004 caught 35% and in 2001, 71% changed their passwords upon request (Forte and Power, 2007). This would allow an attacker unrestricted access to the company network. The attacker could then start accessing sensitive information, taking down systems or even using networked computers as a bot net. An attacker gaining access to sensitive data won’t just affect the company; the data is often stolen to be used in fraud which will directly affect customers.

The threat from phishing is often instigated by the staff and insiders of any business. It is said that human error is the most significant cause of IT security breaches, with 70% of all security incidents originating from inside the organisation (Philpott, 2006).

What large businesses and enterprises are fully aware of, and SME’s must begin to appreciate is that these phishing attacks are not designed to access staff email accounts and send out the standard advertising emails you see in your spam folder. Phishing has in fact developed into becoming a tool to gather enough information, to give attackers access to business networks, where the real danger is.

The following graph shows the responses from The GFI Software SME Security Report, 2009. Question 8 asked the 269 IT Directors, managers and security professionals from SME’s which of the threats are you most concerned about. The graph above shows that Phishing came as the 5th most worrying IT security threat. However looking at the other threats, eg. “Spam clogging inboxes” and “Virus attacks via email”, with these being specific classifications of Phishing, in actual fact Phishing came 2nd, 3rd and 5th (GFI, 2009).

![Graph 1: Security Threat distribution (GFI, 2009)](image)

But the threat of phishing is not just felt by the organisation. Many phishing scams can impact individual users, or customers. Not only causing problems for the individual users who is tricked into divulging personal information, there is also a possibility of damaging the wider consumer trust in the brand (Furnell, 2004). SME’s who find phishing scams being committed in their name ought to take a responsible stance, and do their utmost to warn and inform potential victims (Furnell, 2004).

IV. Defence

When it comes to protecting your business from phishing attacks, there are usually 3 different paths that are taken; user education, client-side protection and network gateway systems.

Client-side protection such as the netcraft and Google phishing toolbars, are largely a wasted effort. Such toolbars rely on the user to already be cognizant of the phishing problem, along with that fact that these systems only work once the user has been redirected to a fraudulent website. If the phishing email requests information via email, these toolbars may as well have not been installed (Tipping Point, 2005).

Network gateways on the other hand do have a legitimate reason for being a suggested defence strategy; however this solution will expect you to have an unlimited budget when it comes to IT security. The idea is that you have a system installed at the gateway of your business network, scanning different types of connections, filtering known suspicious connections to attempt to block such scams before the user is able to be duped (Tipping Point, 2005).

![Graph 2: Phishing disturbance (GFI, 2009)](image)
The above table shows how anti-phishing applications are the least adopted countermeasure and least planned for addition to security setups. Figure 1 from the same report shows that phishing is one of the most worrying threats; however this graph shows that SME’s are the least prepared for phishing.

Figure 1

Software solutions therefore are not being widely adopted into SME’s security plans. If this is the case, why then must we assume that staff must stay uneducated and rely on software to do all the work? Business owners must remember that staff are the life blood of businesses and that you rely on them to do their job correctly. If you enable them to learn the fundamentals of IT security and the risks of phishing, this would in fact be the most effective and economic method for the prevention of such scams (Power and Forte, 2006).

Technology cannot protect your business from phishing because your database, firewall or webserver is not the initial target. These scams target your employees, offering a window into the business and a path to your system (Barber, 2001).

Most organisations that are aware of phishing acknowledge the problem, but treat is a nuisance rather than a serious problem. Consequently most organisations do not invest enough in the one real countermeasure; effective and empowering security awareness and education (Power and Forte, 2006).

Ultimately, phishing attacks can be prevented by educating your employees. People do not have to be obsessive or paranoid to protect themselves and their company’s assets. They simply need to be successfully educated and aware of the potential risks (Barber, 2001).

The lack of effective phishing education and awareness in IT security is a chronic problem across SME’s. A common misconception is that IT security is inherently expensive. In actual fact, awareness and education is economical. If a successful, robust program and strategy is developed, the total cost will not be much more than two to three pounds per employee, per year. Also if done correctly “i.e. if it is current, topical, hip, psychologically clever and customised to be relevant to the business environment of the work force” – awareness and education can mitigate risk (Forte and Power, 2007).

Many still believe that software will one day prove to be a useful defence for phishing, especially if email clients are able to incorporate a strong anti-phishing strategy. Until this is the case, user education will still be the most efficient and economic solutions (Forte and Power, 2007).

V. RECOMMENDATIONS

At this point, it should have become apparent that phishing is a real threat to small and medium sized enterprises. The complete solution to which though may be less clear. Currently there is no complete solution to phishing, which is why a combination of multiple strategies must be implemented.

Suitable firewalls and anti-viruses are a staple ingredient in a secure network, so the need for this is really a given. Developing a user focused education policy is the way forward. Put the security of your network in the hands of your staff. These are people you employ and trust to do a job. After suitable training and education in the ways of IT security, they can also be trusted to safe guard the sensitive information targeted by phishing attacks. Of course having technical backups and software systems to pick up the slack is suggested, after all, no matter how many training sessions and security audits staff undergo, they are still likely to act like a human being from time to time (Barber, 2001).

VI. CONCLUSIONS

In conclusion, the impact of phishing on SME’s is going unnoticed, yet is becoming one of the most important and costly threats businesses are facing on a daily basis.

The current state of affairs on social engineering, specifically phishing, is that the employees of small and medium sized enterprises are severely unprepared and unequipped to deal with such scams.

While the needs of businesses differ, the obvious need when tackling an IT security threat such as this is that the risk is minimalized, with suitable solutions in place to deal with developing attacks.

The debate on which solution is in fact the best will continue to go on, however what is obvious is that user education can be the most thorough, economic and successful tactic in the detection and prevention of phishing scams in small and medium sized enterprises.
REFERENCES


Cryptography in the Workplace
Organisational Use of Encryption

Iayesha Reid
University of Derby
Derbyshire, UK
100136584@unimail.derby.ac.uk

Abstract - Cryptography can aid organisations to maintain the confidentiality and authentication of digitally-held information assets. This paper facilitates awareness of SME’s regarding the issues, implementation and the ever changing controls surrounding the use of cryptography in the workplace.

Keywords - BYOD, Compliance, Cryptography, Data, Information, Organisation, Security.

I. INTRODUCTION

Security threats are found to be on the rise which has supposedly increased the use of information security regulations in the workplace (Webb 2013, p.18). This has influenced many organisations to implement the use of cryptographic products in order to protect their information assets against potential threats (Webb 2013, p.18).

According to the National Archives (2013, p. 1), an information asset is a set of information held by a single unit, for example an organisation. They are recognisable as being of value to organisations therefore risk of damage, loss and exploitation should be kept to a minimum. Information assets are either logically (i.e. binary 1’s and 0’s) or physically (i.e. paper) based (Blyth & Kovacich 2006, p. 4). In this paper, logical-based or digital information assets are discussed.

Although many organisations are found to be using cryptography as a precautionary measure, little legislative emphasis is put on to organisations to employ encryption technologies to protect information assets from security threats.

This paper will discuss the changes made in cryptography over the years, with focus on its importance in today’s information security and assurance procedures.

II. CRYPTOGRAPHY OVERVIEW

Cryptography is also known as encryption and is found to be an effective and commonly used security mechanism in both personal and organisational settings (Emam 2013, p. 75). Other terms are also used in reference to cryptography such as ciphers and crypto systems (Tsou et al. 2010, p. 360).

There is a wide variety of encryption protocols to choose from upon selecting a desired crypto system, however they all possess the same objective and that is to protect the confidentiality and authenticity of data, whether stored on a digital device or transmitted via a computer network (BSI 2005, p. 5). This is accomplished by converting readable data into unreadable data (ACPO 2011, p. 43). This means that if a connection or computer is accessed by a third party through overcoming other security measures, information assets that are encrypted are secure as they cannot be understood. The level of security encrypted data has, effectively depends on the strength of the encryption algorithm used.

Encryption systems fall into either one of two categories, symmetric key or asymmetric key (Sideridis & Patrikakis 2010 p. 242). Symmetric key encryption is where each computer is given a secret key that is used to encipher a packet of data in plaintext form, before it is transmitted via the company’s computer network. The same key is used to encrypt and decrypt data packets in this context. Asymmetric key on the other hand provides each computer with a unique private key which is used to decipher data and is secret to that single computer. Asymmetric differs from the symmetric key alternative because a public key is also used in the algorithm. This key is made available to any computer communicating with the transmitter securely and is used by the receiver to decrypt the enciphered data packets (Sideridis & Patrikakis 2010, p. 242).

Digital signatures are also supported by cryptographic methods but this topic is beyond the scope of this paper.

III. CRYPTOGRAPHY HISTORY & BACKGROUND

Controls on cryptography have changed over the last 20 years according to Sundt (2010, p. 2). In 1987, Fak (p. 36) reported that encryption played a significant role in data protection. Many large organisations were made security conscious in the 1980’s but practical problems inhibited the implementation of cryptography in complex working environments (Fak 1987, p.36). According to Fak (1987, p. 36) the installation and maintenance of these products created problems for systems administrators, however we are now in technological-driven era whereby advancements in technology have made encryption implementation easier; at least that is what is assumed.

As encryption became more desirable and adaptable in the 1990’s on a commercial scale, controversy heightened as debates were established in regards to cryptography and the strict controls on its use (Sundt 2010, p. 2). Denning and Baugh (Denning & Baugh 1997, p. 84) reported that the majority of computer intrusions were the result of authentication failures which cryptographic techniques would have been able to overcome.
Regulations and compliance to best practices are distinctive influences in the choice made by security administrators to implement crypto systems in today’s enterprises (Webb 2013, p. 18). Standards aim to provide a framework for best practices within organisations. Each and every enterprise should adhere to those standards applicable to them, when providing products or services to the population but are not necessarily required to do so (Tsouhou et al. 2010, p. 351).

Specific security standards facilitating the use of encryption systems are found in the ISO/IEC 18033 collection facilitated by the British Standards Institution (BSI) (BSI 2005). However, Tsouhou et al (2010, p. 360) goes on further to suggest that any organisation that facilitates password storage or the transmission of data are specifically required to adopt encryption systems. This should include adherence to the ISO/IEC 18033 standard however they are not legally obliged to do so. Being certified by the BSI persuades clients that they conform to best practices, which is a compelling reason for adopting changes within organisations but leniency towards information security and encryption can prove detrimental to the safety of information assets.

The BSI is the national standards body for the UK, similar to the National Institute of Standards and Technology (NIST) supporting the US. The ISO/IEC 18033 standard reports to provide recommendations on the most effective encryption techniques, but how many organisations are found to fully implement professional security advice given by the BSI? It had been recognised by Tsouhou et al (2010, p. 350) that the majority of organisations fail to be aware of security standards. If many are unaware, it can be assumed that they fail to meet crucial security guidelines making these enterprises vulnerable to threats.

Controls have however strengthened towards compliance with encryption standards. For instance, the Payment Card Industry (PCI) issues its own Data Security Standard (PCI DSS) supporting the protection of customer-based data collected from card transactions (PGP Corporation 2009, p. 9). Macleod (2012, p. 11) describes a new incentive for organisations to follow, that being to encourage businesses to integrate encryption in to each stage of a card transaction, from start to finish. Macleod (2011) goes on further to explain that this will soon become a mandatory requirement rather than an option. Questions are however raised to why this is not already a requirement for businesses to adhere to.

Pricewaterhouse Coopers (PwC) (PwC 2012, p. 3) argues that controls are failing to keep pace with the developing business world.

Now outsourcing a lot of their business processes to external providers. If encryption was made a mandatory security measure through legislation or otherwise, customers and businesses would have less to worry about concerning the security of their data.

Although it appears that some enterprises fail to recognise the benefits of crypto systems, many have made great efforts over the years to integrate encryption technologies in to their computer systems framework. Webb (2013, p. 18) stated that there are now tens of thousands of encryption keys deployed enterprise-wide.

Legislative developments have also taken place over the years in support of legal practices surrounding encryption technologies. Law enforcement agencies such as the police have the ability to force the retrieval of encryption passwords from perpetrators. Where suspects fail to disclose this information, they can be prosecuted under the Regulatory of Investigatory Powers Act (RIPA), section 3 and jailed for up to 5 years (RIPA 2000, p. 55).

V. ISSUES

Adopting cryptographic techniques is important to the majority of organisations today as services and products are being moved from the high street to online web utilities, yet some argue cryptography algorithms result in more harm than good. Gasper et al (2010, p. 280) reported in their respective article, that systems can become vulnerable and unstable once encryption protocols are utilised.

Another distinctive problem concerning cryptography is that various encryption algorithms are not entirely faultless, some are easily cracked and other, more complex algorithms have the potential to be broken also depending on resources. Where less secure protocols are used, data is at greater risk of being compromised as they fail to be 100 percent secure (Emam 2013, p. 75). Providing recommendations made by BSI on the use of encryption, it can be assumed that any organisation complying to such standards have an effective cryptographic design in place.

The objective of creating a good cryptographic design is to have a maintainable crypto key management system in place. This should support secure storage of encryption keys which hardware and software can be entrusted to manage, however the installation and maintenance of these systems can be difficult to adapt in complex working environments (Menezes, Oorschot & Vanstone 2010, p. 545).

Hardware cryptography concerns the physical installation of specialist computer chips. They contain built-in encryption protocols which are able to protect mass amounts of data from security threats. Where hard-disk encryption is utilised, the impact of security breaches is proven to be reduced according to PwC (2012, p. 13), particularly those incidents concerning the physical theft of computers.

VI. CRYPTOGRAPHY LIMITATIONS

The objective of Information Assurance (IA) is to protect information from manipulation, degradation, destruction and exploitation from an unauthorised third party (Blyth & Kovacich 2006, p. 3). In order to do this effectively, Information Security (IS) methodologies can be adapted. This is defined by BS7799/ISO1779 (BSI 2006, p. 2) as the
availability, confidentiality, integrity and lastly, the preservation of information.

Encryption is a useful measure in maintaining both the confidentiality and authentication of information assets but there are particular elements of IS which cryptographic methods are unable to support such as availability and integrity.

Nonetheless where encryption technologies are not adapted, organisations allow themselves to be at greater risk of exposure which in relation to information security means, leaving information assets exposed to possible harm or loss (Blyth & Kovacich 2006, p. 4). Emam (2013, p. 75) agrees that encryption does not provide a complete solution for securing information assets however it should not be ruled out of being a useful measure to employ.

VII. HUMAN INTERACTION

A key vulnerability has been recognised but is very difficult to manage, that is people and their actions. According to Ayrapetov (2013), human engagement is often found to be the cause of vulnerabilities and even so, those involved are usually unaware of the impact. Where information technology (IT) dominates an organisation, there will always be risks related to human error or criminal acts deliberately carried out with malicious intent (Emam 2013, p. 75).

Trivial errors can be made by employees who are unaware of the risks they pose to an organisation’s information assets. For example, people may record their encryption passwords on pieces of paper as they can often be complex and difficult to memorise. If the written password is readily available which is often the case, being stored within close proximity to the computer in question, this can lead to unauthorised exposure of what should be secure, information assets. Emam (2013, p. 76) points out one particular incident where a health service employee had their work laptop stolen from home, alongside a piece of paper containing an encryption password. The paper was collected during the robbery having been kept next to the laptop, and would ultimately allow the perpetrator access to sensitive documentation stored on the machine. The encryption protocols used at that time had proven to be entirely ineffective due to a single error made by a member of staff.

VIII. BYOD

Bring Your Own Device (BYOD) concerns the use of personal devices in the workplace. It is a new concept that has been rolled out across many organisations as smart devices have become more and more business-friendly (Kaspersky Lab 2012, p. 18).

BYOD has increased the threat of particular cyber security incidents such as the loss or unauthorised access to sensitive company data to name a few (Ayrapetov 2013). The risk of such an incident occurring is increased dramatically where sensitive information is not encrypted whether they be financial files, passwords or customer data. Where information is effectively encrypted, access is limited to key holders only, eliminating the possibility of unauthorised access. Encryption however cannot prevent the loss of information therefore the BYOD strategy is still vulnerable where cryptography has been adapted on personal devices.

Kaspersky Lab (2012) conducted research last year to better understand the concept of BYOD and the affects it has on organisations. An element of this research was targeted at 3,300 senior IT professionals who were required to give feedback on the use of BYOD within their respective enterprise. Given the knowledge Kaspersky had gained from their research, it had been established that companies were creating large security risks for themselves as they allow the BYOD concept to be adapted by employees. Companies appear to be aware of the risks but 36% of those responding to the survey continue to proceed which may be due to the positive affect BYOD has on their organisation (Kaspersky Lab 2012, p. 2).

IX. CONCLUSION

An organisation must understand their risk profile with consideration to all possible security threats. They themselves have to provide a model which groups together information assets for an effective and targeted risk assessment to take place (Lillywhite 2004, p. 7).

Where electronic information assets are concerned, targeted areas for risk assessment should be to analyse how well the organisation maintains the availability, confidentiality, integrity and preservation of data. These are elements belonging to the concept of Information Security, which would ultimately verify how well an organisation is protecting its electronically-held information assets. Satisfying all four areas successfully will reduce the threat of assets being; exploited, manipulated, degraded, destructed or exploited which occupy proprietary elements of Information Assurance.

Encryption was and still is an important information security and assurance measure in both personal and organisational contexts; however enterprises are often found to be discouraged in the implementation of encryption products due to the complexity of some crypto systems. In addition to this, encryption provides limited security of information assets which is variable dependant on the cryptographic algorithm used.

The Association of Chief Police Officers (ACPO 2011, p. 43), state that the purpose of encryption is to guarantee that only the targeted recipient can decrypt and read the supposed message, however this is not always the case as there are a variety of factors that affect how well cryptographic algorithms secure information assets i.e. human error, incorrect installation or the encryption algorithm itself.

Encryption does not provide a complete solution to securing and assuring electronically-held information assets, however it acts as a beneficial component in maintaining the authentication and confidentiality of data.
REFERENCES


The Human Factors in Security
Are You Aware?

Kirandip Kaur Sehmbi
University of Derby
Derbyshire, UK
100091639@unimail.derby.ac.uk

Abstract - Information Technology has become one of the fundamental aspects within an organisation and it is mostly implemented by the employees of the business. It has been found that a large percentage of security breaches which occur within an organisation are due to staff negligence and disregard for company policies. However extended research has found that initially it is not the employees who are to blame but the lack of awareness, training and education of security risks to an organisation. With this investigated and the necessary policies highlighted this paper gives a brief outline of potential steps which managers of organisations can take to reduce the level of security breaches occurring due to the human or “people” factor.

Keywords - Human Factors, Security Breaches, BS7999, ISO17799, ISO/IEC 27001, Awareness, Training.

I. INTRODUCTION

Businesses today rely highly on Information Systems (IS) and technology, and consider it as an integral part of the organisation structure. Without this underlying technology businesses today will not be able to compete with the competitive society that exists today. With technology however, comes risks and with risks comes the need for effective security measures and policies. One variable which has begun to raise concerns within businesses is their employees. This paper is going to look further into the issues related with staff and security. It is going to address the potential risks which employees can cause to the business structure, but alongside this the paper is going to investigate the reasons why staff related issues cause such risks to the business. Further the paper will discuss areas which are lacking attention by business manager such as security awareness, policy enforcement and education for their staff. In conclusions to this paper, suggestions are made into what procedures can be taken to reduce the risk of security breaches, such as pre-employment checks, enforcement of security policies within the work culture and continuous training to raise awareness.

II. ISSUES OF SECURITY BREACHES

Today’s society and business environment is increasingly becoming more and more IT dominated with 84% of organisations being highly reliant on IT systems (PWC, 2008). But where there is IT in an organisation there is always the underlying issue of security and security breaches. According to the PWC report (2012a) 93% of organisations suffered from security breaches which as a result has cost UK plc., £Billions over the years. When it comes to security breaches, there has to be a fundamental aspect which is causing them. While being an organisation’s biggest asset the staff on the contrary can also be the biggest weakness to an organisation as well (PWC, 2008).

III. STAFF AND SECURITY

It is a fact that for any large organisation to function and run, there is a need for employees and staff. It is important for the organisation to know that the potential security breaches and risks could be coming from their employees (Susanto, Almunawar & Kang, 2012). It is the employees who are using the Information Systems on a regular basis in the organisation and, not only the Information Systems, but are also using the business network. The PWC report (2012b) further acknowledges that 82% of security breaches which occur in businesses were staff related. We look further into the types of Security breaches mostly caused by staff and the possible reasons of their occurrence.

A. Human Factors and Security Breaches

According to Lacey (2009) security breaches to an organisation in terms of human factors can be caused by many variables, such as stress, carelessness, criminal intent and inattention to name a few. It has been reported that without specifics 82% of security breaches within an organisation are staff related and of these the highest ranked breaches include misuse of web access at 78% and misuse of email access at 73% (PWC, 2012b). Fig. 1 also shows other types of security breaches caused by staff within an organisation. With the majority of organisations having internet access, it has become easier for security breaches to occur at the hands of staff, and in most cases the occurrence is unintentional.

B. Reasons for these Breaches

There are three main causes for the high levels of security breaches in businesses today, which are, Lack of Training, Lack of Education and Lack of Awareness for employees (Sasse et al., n/a) For an organisation it is vital that security awareness is implemented as much as possible (Susanto, Almunawar & Kang, 2012) to ensure employees are alert of security threats and the effects they can have on a business. Another factor is the lack of education about security risk and threats. It was found that 54% of businesses had no program in place to educate staff about security and in terms of training...
44% of organisation conducted extra staff training however this was after they suffered from their worst breach recorded (PWC, 2012a).

Fig. 5. Types of Staff Related incidents (PWC, 2012b).

IV. SECURITY POLICIES

For organisations to take control of the occurrences of security breaches it is important for them to understand the essential security policies which by law must be implemented in every organisation. The main policies stand as the BS7799 standard and the ISO 17799 standard. BS7799 is an internationally recognised standard which is a part of implementing an Information Security Management System. There are two parts to this standard; Part 1) this section states the “best practices” for information security and Part 2) states the 127 controls which an organisation can put into practice to accomplish the standards stated in part 1 (BH Consulting, 2005). The ISO 17799 Standard is the updated standard of BS7799. This standard looks at information as a quality which adds significance to an organisation. In addition, the standard states 3 ideals which characterise information security (Carlson, 2011):
- Confidentiality
- Integrity
- Availability

These standards create a foundation for an effective contingency plan for an organisation however statistics show that 79% of organisations are not even aware of the BS7799 and ISO 17799 standards (PWC, 2008). Again there is the issue of awareness and this time relating to high authorities of an organisation. If management level is not recognising these vital components of security, then the employees are bound to come under pressure which is why it was found in PWC (2012a) that only 26% of staff in an organisation had a good understanding of the security policy in place, compared to 75% who did not understand the policy in place. One important fact which should be remember is that policies shouldn’t be looked at as a set of rules which confine the efficiency of an organisation but more as key enablers (Sustanto and Almunawar, 2012).

A. One Standard Fits All

For today’s businesses however there is one complete standard which should or needs to be implemented to reassure both clients and employees that security is one of the most prioritised factors in the organisation; this is the ISO/IEC 27001 standard for Information Security Management (BSI, 2013d). The ISO/IEC 27001 standard will help the organisation to comply with legislation regarding information security and meet strenuous industry requirements (BSI, 2013a). In a study conducted by the British Standards Institute (2013a) management reported a 60% increase in client assurance and productivity. Fig. 2 shows the reported improvements in IT and Operations when this standard was adopted:

<table>
<thead>
<tr>
<th>IT &amp; Operations</th>
<th>Percentage with ISO/IEC 27001 implemented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>48% - reduced level of Risk</td>
</tr>
<tr>
<td>Information Security Processes</td>
<td>82% - Increase in the quality of the processes</td>
</tr>
<tr>
<td>Confidence and Security</td>
<td>100% - increase in the overall organisation</td>
</tr>
</tbody>
</table>

Fig. 6. Reported Improvements in IT & Operations (BSI, 2013a).

V. REDUCING THE RISKS

From the stated risks it can be collated that the best way to overcome current security issues and prevent new ones from occurring is to educate and train staff of the potential risks an organisation must fight and overcome. This role must be undertaken by the managers of the organisation. There are many ways in which managers can achieve the desired security prevention they need with methods such as conducting pre-employment checks, having a good security awareness program in place and having a business continuity plan.

A. Security Awareness Programs

Making users aware of the threats and issues surrounding them has become a vital part in an organisation structure. In general practice employees and staff should sub-consciously be carrying out their daily task in a secure way, such as locking computer whenever they leave their desk and saving work on a regular basis. To make sure employees are working in this way, an effective security awareness program is necessary (Thomson and Solms, 1998). This type of program allows both the employees and managers to see the level of understanding they have about the significance of information security. Also it allows them to review and reflect upon their responsibilities and acts to ensure there are substantial levels of information security control (Shaw, Chen, Harris & Huang, 2009). Within these programs it is good to look at the current situation first which will allow a basis to be formed for the initial program. Questions such as, what do people already know, what they think about the current situation and their behavior towards it (Lacey 2009). From here methods such as...
questionnaires can be devised and handed out to staff, however with this type of method even the questions must be complied and thought up carefully in order to gain the highest amount of details from them. If an awareness program is designed and implemented properly, the results can be very fruitful.

B. Risk Assessments

Pre-employment checks may sound like the obvious but it is amazing how many organisations skip/avoid this crucial step when employing new staff. It was found in the PWC report (2008) only 59% of organisations carry out background checks and assessments of potential candidates before employing them. This in itself speaks out as a security breach waiting to happen for the organisation. If not the extensive checks then basic background checks such as CRB (Criminal Record Bureau) will allow managers to gain a basic idea of whom they are about to give access into their organisations assets. It has been found that around one in ten candidates will fail a CRB check (Lacey, 2009).

The downside to such checks is that they are not 100% infallible, and can at best reassure managers that the potential candidate has a clear background, as well as being quite time consuming and costly (Lacey, 2009). But in comparison to the cost of the assets being handled in the organisation, it is worth carrying out these checks for the long term.

C. Business Continuity Planning

Business continuity planning is a concept which allows the managerial commission of an organisation to show that is has implemented thoroughness in relation to information processing. With such a plan in place it allows managers to show their employees that the security of it organisations assets is of number one priority and is taken seriously (Peltier, 2005). Even for business continuity there are standard which can be adopted to ensure a secure and resilient plan is in place; this is the ISO 22301 standard. The original standard which was used to identify Business Continuity was the BS 25999, however major improvements have been made over the year due to the change in technology and business operations. So the old BS25999 is now widely known as the internationally recognised ISO 22301 standard (BSI, 2013c). This standard outlines all of the major components required for a good and robust business continuity plan. In a report by the British Standards Institution (2013d) it was found that 81% of managers who had to use their business continuity plans affirm that it was effective and reduced the level of disruption caused to the organisation.

VI. CONCLUSION

All in all this paper has looked into the aspect of the human factors when it comes to security within an organisation. It is a common occurrence in most organisations where top of range security features for the IT systems are implemented as they become available however the human contribution to protect the company’s resources is elapsed (Ashraf, 2005). Simply having a security policy in place does NOT mean that the staff awareness will increase (PWC, 2008).

Awareness plans should be integrated with training and education so that a better result can be obtained. It has been acknowledged through this paper that one cannot solely blame employees for the occurrence of security breaches. Managers need to take responsibility for ensuring that an adequate policy is in place so that employees have a guide to follow. It is a point needed to be considered by management, to make employee training compulsory (Susanto & Almunawar, 2012) so that continually as IT and technology develops so does their understanding. In research conducted by Schneier (2013) it was found that it is not essential the fault of the employees of the organisation but of the IT systems which they are using, not being secure enough to handle the evolution of technology and the threats it poses with it. The study further states that if computer systems were designed in such a way that, users cannot commit a mistake even if they wanted to then managers would spend less money on training their employees and more on adapting to a secure IT System. Therefore it can be a thought to managers to implement more security features to their systems and then talk to the employees about how mush secures the system has become, rather than trying to make the staff into the experts (Schneier, 2013).

It has been acknowledged that one successful way for higher management to ensure preventions methods of security breaches is to conduct pre-employment checks and have their employees and staffs undertake a risk assessment. With pre-employment checks, although there is not a guarantee with end result, it allows a reassurance perspective for managers that they know they are employing the right person for the job so in conclusive CRB checks can prove a valuable investment. Risk assessments however are a fundamental way in allowing managers to gain an insight of what they can do to improve the current security procedures and practices. As well as staff and employees it allows managers to also reflect and gain knowledge about preceding security problems as well as new ones at that. In a study conducted by Desman (2003) ten potential areas were discovered which can be used as a basis for a successful risk assessment program. It was concluded that so long as the information was reaching everyone in a timely fashion and understandable format a risk assessment proves quite successful.

As rightfully stated by Ashraf (2005) there is no way an organisation can be 100% protected from security breaches however through methods such as security awareness ,the full potential of securing an organisation can be achieved. It can be gathered from our developing society today that more emphasis has to be placed on general IT skills and knowledge.
REFERENCES


Abstract - Ransomware is a type of malware that can be downloaded by employees of SME’s just like any other malware, however, ransomware can be much more dangerous than other types of malware. Once ransomware has been downloaded onto a business’s PC, it will seek out (or be remotely guided to) important data within the business, such as customer records, staff records, HR files and accountancy records. It will then encrypt this data using the same encryption standard as military and governments all around the world (known as the Advanced Encryption Standard). The business is then given notice that this data will only be released once a ransom has been paid, and may be destroyed after a certain period of time. The real deviousness of these attacks is that the police will rarely be able to track the source of the malware, and only in circumstances of extreme sloppiness of the criminal will they be able to crack the encryption. There is nothing that the business can do. They have to make the choice of whether to pay a hefty ransom, or face losing all of the important data from the business. Paying the money can be a hefty financial blow, but losing the data is likely to result in the business failing.

Keywords - Ransomware, Malware, Virus, Data, Cybercrime.

I. INTRODUCTION

Malware (short for malicious software) is a massive problem for businesses. Cybercrime such as malware and web attacks costs the average US business $8.9 Million per year and the average UK business $3.3 Million per year. It is also evident that small to medium sized businesses suffer more per capita than larger businesses do based on enterprise seats (Ponemon Institute, 2012). It is very easy for a single employee to click on a bad link, and a piece of malware could start downloading in the background. A substantial network security system including a firewall and an antivirus will usually detect and destroy most this malware, but new malware such as the recent development of ransomware and cryptoviruses may slip through these safeguards, especially if they are not updated and upgraded regularly.

For a long time people have been hacking networks and inventing new malware as a hobby; for the credibility they would receive from their peers; or simply for the havoc they knew they could cause. Before long there were scams such as phishing and URL redirection attacks, which could earn money for the criminal from any victim that was not on their guard.

Ransomware has taken this moneymaking to a whole new level, in the past with phishing scams for example, you could always close your browser window once you realized it was a phishing scam, or for example, if you downloaded a piece of malware, most of the time if you (or an anti-virus) could track it down, and could contain or destroy it, but with many ransomware attacks, as soon as you download it, it will start to execute itself, and a large amount of your personal data is at risk.

II. HISTORY OF RANSOMWARE

The first recognised piece of ransomware was the PC Cyborg Trojan, also known as the AIDS Trojan written by Joseph Popp in 1989. This Trojan was mass mailed by floppy diskette to thousands of individuals and businesses subscribed to the PC Business World magazine. After it installed itself to the PC, it replaced the AUTOEXEC.BAT file to allow itself to count the number of times the PC rebooted. It would tell the user after x number of reboots (usually around 90) it would expect payment for some software or another, and that if payment wasn’t forthcoming, it would render the computer useless, and none of the files would be accessible. Sure enough after that number of reboots (or on a different version of the Trojan straight away on a single reboot) it would encrypt all of the files on drive C and demand payment again (Aycock, 2006).

Luckily in Popp’s attack, a symmetric encryption method was used (the same key is used to encrypt and decrypt the data) which meant that somewhere within the Trojan must have been the key that encrypted (and therefore would decrypt) the files.

The notion of using a public key encryption was conceived in 1996 by Adam Young and Moti Yung in their proof of concept attack against a Macintosh SE/30. This meant that the Trojan only possessed a public encryption key. The only one who knew the decryption key was the attacker themselves and there could be no evidence of it on the victim’s computer. This was really the birth of the cryptoviral attack as it is known today. (Young and Moti, 1996)

III. ENCRYPTING VS NON-ENCRYPTING RANSOMWARE

Between 1996 and 2004 there was limited activity in the field of ransomware. It is believed that this was due to the time and complexity involved in creating a cryptovirus. It is also speculated that many computer hobbyists had not truly understood the potential of a piece of ransomware as a moneymaking tool. This was up until the GPcode, TROI.RANSOM.A, Archiveus, Krotten and Cryzip malware all surfaced around the mid-2000’s, using more and more complex RSA public key encryption schemes. The RSA
(Rivest-Shamir-Adleman) algorithm is an encryption scheme based on multiplying two large prime numbers together and performing other operations to receive two keys (one public and one private key). Anyone can encrypt messages using the public key, but only the owner of the private key can decrypt the messages. (Rouse, 2005)

If implemented correctly, these RSA Encryption schemes can be practically unbreakable. For example, the most dangerous recent ransomware generates its own AES-256 key (the encryption used by military and governments across the globe), and then uses the criminals public RSA key to encrypt it. (Brulez, 2011)

One example of a recent ransomware that has been causing a lot of disruption is a worm known as Reveton. The malware, found in 2011, has been nicknamed the “police Trojan” and as well as being a complex technical piece of malware, it is a sophisticated social manipulation scam. According to Ducklin (2012) “Reveton pretends to be a warning from your country’s national police service, locks you out of your PC, and threatens criminal proceedings within 48 hours - usually for unspecified copyright offence. … you can bypass the prosecution if you pay a “fine” to the cybercriminals. The amount they extort is typically about $200.”

Many victims are tempted by the Reveton ransomware just to pay the fine in the hope that they will get all their files, and control of their PC back, but even if they do pay the fine, they are still dealing with criminals, and are unlikely to ever get their files back without a restoring from a backup.

As explained in the video accompanying the Ducklin article, the Reveton ransomware scares the user by posing as a law enforcement agency, displaying the user’s IP address and activating the computer’s webcam so that the victim will think they are under surveillance. What the video doesn’t explain is that even though the victim will be able to clear the malware relatively easily by using anti-virus software, the likelihood is that all the victims’ files have already been encrypted, and the only way to restore those will be from backups.

There are other non-encrypting types of ransomware that are also very dangerous to users such as WinLock. This was a piece of ransomware discovered in 2010 that would not encrypt any data on the PC at all, but would disable many of the Windows components, and would lock the screen, displaying a series of pornographic images until the victim sent a premium rate text message that would cost between around $10 - $30.

The victim would then (according to the scammers) be sent a password to unlock their computers. No data was encrypted by this ransomware, it was a simple case of locking the screen with a password unknown to the victim, but nonetheless, for the victim with pornographic images cycling on their screen, it can be very scary and embarrassing. (McMillan, 2010)

Another very clever social manipulation scam that held the victims computer to ransom without any encryption was found in 2011. A worm that imitated the windows product activation surfaced, it would tell the users that they needed to re-activate their system because they had been a victim to fraud, or a system error, but re-assured them that it would not cost them anything, and no personal details would have to be handed over. It had an option to activate windows online, but this option would never work, leaving the victim forced into calling a telephone number. This telephone number was in fact a high-cost premium rate international number. (Keizer, 2011)

As well as the ransomware and cryptoviruses we have been looking at thus far there is another category of malware called scareware. These are not ransomware in the classic sense that the victims computer is never really in danger of being held to ransom, but to an inexperienced user it may seem that way. The Winwebsec Malware is a classic example of a piece of scareware. It poses as a piece of anti-virus or anti-malware software that will alert the user (by means of pop-ups and fake detections) that there are lots of viruses and malware on the user’s computer that need to be cleaned up, where in reality the only malware present may the Winwebsec software itself. Winwebsec will then ask the victim to purchase the “full version” of the software in order to clear these viruses. Winwebsec often uses logos of popular anti-virus software to make the virus detections look legitimate in order to scare the user enough to make them pay the money. (O’Dea, 2009)

IV. GPCode

The most worrying of all the different ransomware is the GPCode malware. First seen in 2006, this Malware has evolved and changed into something that can be very difficult to deal with for the average computer user. The original GPCode, released in late 2004, tricked analysts by giving the name a reference to PGP “PGPcoder”, which became shortened to “GPCode” nonetheless, the cryptography it used was relatively weak, and so anti-virus and decryption specialists were able to decrypt it rather easily. There is no doubt though that people still will have paid up for fear of their files. (Emelyanova & Nazarov, 2006)

A number of variations of GPCode followed, each with strengthened encryption, using better RSA public keys, until 2008 when GPcode.ak was released. This has excellent cryptography which at the time was thought unbreakable. It did have a flaw though, in that when it encrypted the files, it deleted the old unencrypted files through the windows file system. This meant that certain programs such as PhotoRec could still recover some or all of the deleted files, without needing to decrypt anything at all.

Then the most recent incantation, GPCode.ax appeared in 2010 after a relatively long period of silence (speculatively due to the money that the author made from GPCode.ak) Unlike GPCode.ak before it, instead of deleting the old unencrypted files, it actually overwrites them on the disk, meaning that it is very unlikely that any files could be recovered without cracking the encryption, and that certainly wouldn’t be easy either. It uses an AES 256 encryption key encrypted with the author’s RSA 1024 encryption algorithm. (Kamluk, 2010)

Arora (2012) described the process of cracking AES128 encryption (which has half the key length of AES 256) with the Fujitsu K computer (at the time the faster supercomputer in the world) using a brute force (every possible combination) attack.
Arora showed that with the K computer running at its full theoretical speed of $10.51 \times 10^{15}$ flops per second, and with 1000 Flops required per combination check, it would carry out $10.51 \times 10^{15}$ combination checks per second. And because there are 31536000 seconds in one Year - 365 x 24 x 60 x 60, it would take 1 billion billion years to go through every possible bit combination in AES 128 - $(3.4 \times 10^{38}) / [(10.51 \times 10^{15}) \times 31536000] = (0.323 \times 10^{25})/31536000 = 1.02 \times 10^{18}$.

Obviously, if the author was caught, then the authorities could demand the keys to all reported cases of the ransomware using RIPA 2000 (the Regulation of Investigatory Powers Act) and if disclosed, the victims would be able to get their files back within hours (depending on the amount of data) but as of this report being written, the identity of the author of GPCode.ax and all of its predecessors, is still unknown.

Kaspersky had reportedly been able to make contact with the author in 2008, and were able to verify that the contact was the real author of GPCode (most likely they were provided with a key to decrypt the ransomware on a test machine.) (Dunn, 2008) Regardless of this contact they have no idea of his real world identity, and with the amount of money that the author has most likely made off of these scams, they are unlikely to ever find them.

V. Impact on SME’s and Case Studies

The use of ransomware has been particularly prevalent in the Asia and Eastern Europe, especially in regards to attacks on businesses. They started causing real disruption in the UK late 2012 and early this year. This is a very worrying trend as businesses are woefully unprepared. Most businesses computer networks are penetrated by hundreds if not thousands of viruses and malware per year, but most of the time they can either quarantine them before any damage is done or can remove them easily and automatically. If even a single GPCode.ax were to infect a business and their antivirus not completely alert and up to date, there could be disastrous consequences as the virus gets to work encrypting millions of files.

Infection from ransomware can be very costly for business in monetary terms. The suspected authors of the Reveton ransomware described in section 3 were arrested in 2013, on the Costa del Sol in Spain, while the gang leader was arrested late in 2012 while holidaying in Dubai UAE. It was estimated that the Reveton ransomware had made at least 1 million Euros a year (and presumably continues to make money to this day.) (BBC, 2013)

It has been demonstrated in a number of cases in Australia how devastating this can be for businesses, especially those with a lot of client data. Only last year a primary school in Byron Bay was hit with a piece of ransomware that could have cost them $5000. Luckily for the school, the criminals attacking them were not sophisticated at all. Presumably they were using an attack similar to the older GPCode.ak, allowing a technology expert to recover much of the data (Pauli, 2012)

As seen in the Pauli’s article, there were businesses that were not so lucky; Deane’s transit group paid around $3000 to the attackers to recover the sensitive data that they keep about the children they transport around.

Even with an antivirus in place, it may be difficult to keep out a determined attacker, as in the case of a Queensland medical centre, whose attackers demanded $4000. Luckily, the medical centre had backups of patient records and refused to pay out to the criminals. (Ragan, 2012)

There are more potential costs to businesses, if for example after the business pays the ransom fee, the attacker then decides not to send them the key to release their data, or if the company simply decide not to pay up they will lose so much valuable data. Research shows that 70% of businesses that experience a major data loss go bankrupt within one year (DTI/Pwc, 2004)

VI. Protecting Against Ransomware

It is extremely important for businesses to secure their data against this kind of attack, and all other malware attacks, which can be done with relatively little cost. It can be a source of pride and comfort for the business and their clients. A combination of a strong firewall, an up to date trusted antivirus and a well implemented, well maintained intrusion detection system can prevent so much hassle and so much embarrassment. Closing down TCP and UDP ports that are not being used is also extremely important, as this is one of the main ways that hackers can gain entry to computer networks to inject malware. These are all known as technical factors in a network.

Another consideration to any business should be the Human factors in network security, such as staff training and knowledge of good information security practice. All staff in any business should know how create and remember a secure password for their user accounts. They should also know the types of websites they are accessing, and those they should avoid, in order to avoid downloading any viruses. It should also be taken into account that malware can easily be brought from outside the network on removable media such as USB Memory sticks and CD’s (with or without the owner’s knowledge).

VII. Conclusion

Ransomware can be very lucrative for cybercriminals and can be very dangerous for businesses – particularly small to medium size enterprises. It is believed that in years to come, it will take over as the prominent force in malware, as it is more profitable for criminals than other forms of malware.

Antivirus and computer security firm Sophos predict ransomware to rise massively in 2013 and if they are to believed then businesses, in particular those with high value or sensitive personal data, should certainly be very wary of the threat. (Raywood, 2012)
REFERENCES


Your Business Identity: Just How Secure is it?

Joseph Smith
University Of Derby
Derbyshire, UK
J.Smith20@unimail.derby.ac.uk

Abstract - Business identity theft is an issue that many businesses simply ignore. Having affected around 100,000 small and medium sized enterprises in the UK with an average cost of £13,500, it is an issue that should not be ignored. There are a number of simple steps business's should take to protect themselves, particularly with regard to managing employees.

Keywords - Identity, Information, Businesses, SMEs, Theft.

I. INTRODUCTION

Identity theft is a well known crime and is considered by many to be the crime of the 21st century (Collins, 2003), however, less well known is business identity theft. Business identity theft affects many businesses each year, damaging their reputation, causing significant financial loss and ruining their credit rating. This paper looks into what business identity theft is, the different ways a criminal will use a business's identity and, perhaps most importantly, looks into the ways businesses can protect themselves from business identity theft.

II. WHAT IS BUSINESS IDENTITY THEFT?

Sproule and Archer (2007) define identity theft as:
"The unauthorized collection, possession, transfer, replication or other manipulation of another person's personal information for the purpose of committing fraud or other crimes that involve the use of a false identity."

Collins (2003) defines business identity theft as:
"Business identity theft is the unauthorized use of a business's business identifying information to obtain credit, goods, services, money or property; or to commit a felony or misdemeanor."

These definitions will be used throughout this paper.

III. THE EXTENT OF THE ISSUE AND IMPACT ON BUSINESSES

According to Lynch (2010), business identity theft now costs UK businesses £1.3billion. 100,000 SMEs in the UK have been a victim of business identity theft, with an average cost of £13,500 to each business; some cases were as high as £30,000. According to CPP (2011), a loss of £13,500 would put 20% of SMEs out of business, while a £30,000 loss would put as much as 76% of SMEs out of business. Campana (2006) explains that a leading American commercial insurer projected a 1300% future growth in losses due to identity theft. While this figure was based on American statistics, identity theft is a worldwide issue (Fraud Advisory Panel, 2003).

While there have been 100,000 reported cases of business identity theft, there is likely to be many more cases, where businesses have either not reported the crime, perhaps because they don't want bad publicity, or they may not even know about it. CPP (2011) reports that ex-employees are to blame for as much as 67% of all business identity thefts, employees may use their business's credentials to obtain goods and services for personal use, which could remain undetected. This makes it difficult to understand the full extent of the problem.

IV. LACK OF AWARENESS

Worryingly, a recent study by CPP (2011) showed that 42% of UK SMEs were not aware of business identity theft. Business identity theft is a problem that can affect any business in the UK, yet only 34% of SMEs thought they were at risk. The study also found 68% of SMEs trusted Companies House to check documents; there was limited compliance with the Data Protection Act 1998; and few had insurance against business identity theft. These statistics show that SMEs in the UK are not aware of the dangers of business identity theft and do very little to protect themselves against it.

V. HOW BUSINESS IDENTITY THEFT HAPPENS

A fraudster will steal or acquire information about the business, such as the company's name; company number; information about employees; domain names; phone numbers; bank details; supplier details; customer details etc. This information could then be used to gain finance; obtain goods; make VAT claims; deceive customers; obtain assets etc. all in the victim business's name (Fraud Advisory Panel, 2011).

VI. TYPES OF BUSINESS IDENTITY THEFT

While there are no explicitly defined types of business identity theft as such, there are various different ways a criminal could make use of a business identity. This article looks into a number of ways a business's identity could be used and splits the different ways into 5 main types: application fraud; account takeover fraud; customer targeted fraud; supplier fraud; and online impersonation.

A. Application Fraud

This type of identity theft involves the fraudster applying for financial products, such as payment cards, loans, bank accounts etc., all in the victim's name (Fraud Advisory Panel, 2003). Fraudsters will often take as much credit as they can from any credit they can get, which can severely damage the victim business's credit rating and put the business into a lot of debt (Lynch, 2010).

B. Account Takeover Fraud

Account takeover fraud is where a pre-existing account is taken over by a fraudster. For example a business's bank account may be taken over and the funds accessed by a fraudster, business credit cards could be stolen and used to purchase goods and services etc. This could be very costly to
the business, as well as damaging it's credit rating (Fraud Advisory Panel, 2003).

C. Customer Targeted Fraud

Fraudsters may target a business's customers by pretending to be the business. Below are a few ways they may do this.

1) Phishing Attacks & Cloned Websites

Phishing attacks are very common, most of us have received phishing emails and most people realise they are phishing attacks and delete them straight away. However, there are still many people who reply to phishing emails, and with most phishing emails claiming to be from a genuine business, it can be damaging those businesses. Cloned websites are a huge issue that affects many businesses, in particular, banks and online retailers. Criminals will set up a website which looks the same as another business's website, such as a bank's website, and customers of the genuine website are directed to the fake website, often through phishing emails, and asked to enter in various pieces of information, such as bank details, personal information, card details etc. This is then used by the criminals to commit other fraud. While this does not usually directly impact the business, their customers can lose confidence in the business or the use of websites, which can mean a loss of business. An example of such phishing emails and cloned websites is an email claiming to be from the online retailer very.co.uk, the email asks customers to update their information online, and provides a link to do so; however, this link takes the user to a cloned website designed to harvest personal information and passwords (FraudWatch International, 2011).

2) Customer billing

A fraudster may try obtaining customer records from a company, then send out fake invoices to these customers, claiming to be from the genuine company they have used before. The customer may be expecting this invoice and payout to the fraudsters. Once the customer gets the real invoice, they may refuse to pay, explaining that they have already paid. The matter could be escalated to court and the business could suffer a huge financial loss and a damaged reputation (Fraud Advisory Panel, 2011). Collins (2003) highlights a case where a fraudster advertised loans using the Omega Financial name, the customer would apply for the loan, paying the fee, then contact the genuine company asking why their loans hadn't been paid.

D. Supply fraud

A fraudster may obtain company information and use this to obtain goods and services from suppliers by using the company's name and information, this information could include things like VAT and company numbers, they may also obtain pieces of the victim company's property such as stationary with the company's name on it to convince the supplier that it is the company they are pretending to be. This could damage relations between the supplier and the company. The Fraud Advisory Panel (2003) describes a situation where fraudsters obtained company documentation and used it to convince a supplier they were a business and obtained £100,000 worth of goods from the supplier.

E. Online Impersonation

While it can be considered a less costly form of identity theft, online impersonation can still damage a business's reputation. This is a newer form of identity theft which exploits the fact that as online social media has increased, business's presence on social media has also increased. Many businesses have Facebook or Twitter profiles, which can help promote their business, however, there have been a number of cases where these accounts have been hacked or misused by employees. Recent notable cases include Burger King whose Twitter account was hacked, the profile picture was changed to the logo of competitor McDonald's and a number of posts were made about its competitors (BBC News, 2013); and HMV, where disgruntled employees hijacked the HMV twitter account after finding out they were being made redundant (Rudd, 2013).

F. Other uses of a fake business identity

The business's name may also be used to advertise jobs for the purposes of identity theft. An advert may be placed online or in a paper, advertising a job at a business, however, the responses to the job don't go to the business but to a fraudster harvesting personal information (BusinessIDtheft.org, 2013).

VII. PREVENTING BUSINESS IDENTITY THEFT

It is important that businesses take a number of steps in order to prevent their business identity from being stolen. While it is never possible to completely remove the threat of business identity theft, it's always a good idea to try to stay one step ahead of the criminals.

A. Plan

It is important for businesses to have a plan to deal with and prevent fraud. A risk assessment should be completed and a policy should be written with regard to business identity theft. The policy should be published such that all staff read the policy (Fraud Advisory Panel, 2003).

B. Managing Employees

CPP (2011) states that 67% of businesses affected by business identity theft believe that ex-employees were to blame. Campana (2006) states that "as much as 70% of all identity fraud and identity theft comes from a place of business, an employer, or other entity." Siciliano reports that most perpetrators who commit identity theft are current or ex-employees. It is therefore important to have strong policies in place for managing employees.

1) Recruitment

It is important that, when recruiting new employees, appropriate vetting is carried out, including on temporary and part time staff (Fraud Advisory Panel, 2003). The amount of information provided on recruitment advertisements should be limited to prevent fraudsters from abusing it (NatWest, 2013).

2) Training

Employees should be appropriately trained to enable them to detect and report any signs on identity theft (Fraud Advisory Panel, 2003). Employees also should be trained on current information security practises regularly (Shredit, 2012).
3) Job Rotation
Where feasible, jobs should be rotated, as this could help increase the chance of fraud being spotted, as if one employee misses something suspicious, when the jobs rotate another employee may notice it (Fraud Advisory Panel, 2003).

4) Monitor
Records of what information employees have access to should be kept. An auditing system should be used to record what employees are accessing and when (Fraud Advisory Panel, 2003).
Employees should also be monitored to ensure that they are not committing any fraud or stealing any sensitive or personal information (Fraud Advisory Panel, 2003).

5) Multi-level Security
Where appropriate, a multi-level security setup could be used so that different employees have different levels of access to information depending on what information they need to complete their role at the company. When an employee leaves or is transferred, it is important that their access is removed or adjusted, as appropriate (Fraud Advisory Panel, 2003).

C. Data Handling
Most businesses hold a vast amount of data about their business, their customers, and their suppliers. It is therefore important to have policies in place to protect this data. Policies and protocols should be developed that control how and where documents are stored and disposed of.
Physical documents should be shredded on a regular basis when they are no longer needed (Shredit, 2012). Hard copies of documents containing personal, sensitive or non-public business information should be stored in a secure locked place (Fraud Advisory Panel, 2003), an inventory of all documents held should be kept (Gessler, 2012).

Electronically stored information should be stored with strong encryption on secure computers on secure networks. Disposal of data on disk drives should be done using appropriate measures, such as forensically wiping hard drives (Shredit, 2012 & Fraud Advisory Panel, 2003).

D. Data Transmission
It is important that there are appropriate procedures in place for transmitting data, whether sending customers bills, communicating with a bank, or ordering from a supplier. Sensitive information, such as financial information or personal information, should only be sent if the recipient's identity has been confirmed (Gessler, 2012).

E. Business Details
It is important that the details with Companies House is checked to be accurate regularly. Companies House for Protected Online Filing is service that can help protect companies against identity theft by preventing filing from certain paper forms (Companies House, 2013a), and the Monitor Service is a service that will notify the business for any changes to documents set to be monitored (Companies House, 2013b), therefore registering with these services is recommended (NatWest, 2013). Business credit reports, accounts and bills should all be monitored carefully. If there are any discrepancies, it should be investigated and checked with the appropriate person or organization (Gessler, 2012).

F. Online Presence
If a business has a website, it is important to protect that website. Steps should be taken to prevent the website from being cloned, for example, using a product that encrypts webpages, prevents the source code from being visible etc. (RightFiles, 2013), while constantly checking to make sure the website hasn't been cloned by using search engines and reverse image searches to check for cloned content. Sensitive information should not be shared online (Gessler, 2012).

G. Data Sharing
Businesses could consider creating databases of frauds which have, or which they suspect have, been carried out against it; known fraudsters including names and address; and the indicators of various frauds. These databases could be used to help prevent future frauds by using the information to find patterns and detect frauds, but could also be shared with other businesses to create a comprehensive database which businesses could use to protect themselves. Clear reporting procedures should be carried out to maximize the effectiveness of the databases (Fraud Advisory Panel, 2003).

VIII. IF A BUSINESS BECOMES A VICTIM OF IDENTITY THEFT
All fraudulent activity should be reported to the police and/or other relevant authorities (Fraud Advisory Panel, 2003). The business should contact their financial organisations, banks, credit card providers etc., and credit rating agencies to alert them of the fraud. All contact with these organisations should be documented, requesting names and departments (Gessler, 2012). It may be possible to recover some losses through civil proceedings, hence legal advice should be sought (Fraud Advisory Panel, 2011).

Customers that could be affected by the fraud should be contacted, alerting them of the situation. If a customer became a victim of a fraud because of a failure by a business to deal with the situation appropriately, the reputation of the business could be severely damaged.

IX. CONCLUSION
Business identity theft is a crime that affects many businesses worldwide and it doesn't get the attention it needs. Often staff are to blame, there is limited awareness and little is done for protection. Businesses need to be aware of the threat of business identity theft and how they can protect themselves. Businesses should put policies and procedures in place to protect themselves and limit the potential damage of business identity theft.

117
REFERENCES


Corporate Cyberstalking
A Guide for SMEs

Charles Stewart
University of Derby
Derbyshire, UK
100134309@unimail.derby.ac.uk

Abstract - Corporate cyberstalking is an extension of cyberstalking that has become widespread within the corporate world. This paper defines cyberstalking, explains the increasing problem within the corporate world and gives guidance for SMEs.

Keywords - Corporate Cyberstalking, Stalking, Online Harassment, Network Security, BYOD.

I. INTRODUCTION

Cybercrime is an increasing concern, not just in the UK, but worldwide. It is estimated to cost £27bn to the UK economy in lost cash and lost business (BBC News, 2011). The increasing use and interconnectivity of portable devices and computers facilitates cybercriminals to accomplish an assorted amount of cybercrimes. One such crime is cyberstalking.

Cyberstalking is a relatively new term that has formed through the relative ease of obtaining personal information through online content. Chatrooms, email, social networking, instant messaging and the emergence of portable devices have all contributed to the advent of cyberstalking.

A sub-group of cyberstalking is that of corporate cyberstalking where companies and organisations become the target or perpetrator of online stalking. Corporate cyberstalking encompasses many different approaches, including, the silencing of critics, the theft of data, causing loss of business and the distribution of negative material of rivals.

II. CYBERSTALKING

This form of stalking is different to conventional face-to-face or ‘offline’ stalking, where traditional methods of monitoring a person through following, making abusive and threatening phone calls and sending abusive and threatening letters are associated with people with social and psychological problems. The ease and anonymity of stalking over the internet means that anyone with a grudge and an IP address can cause harassment with minimum time and effort.

Cyberstalking encompasses a wide range of behaviours, some of which are not associated with offline stalking. Bocij, 2003), including, but not limited to, the activities of paedophiles, political intimidation, school bullying and corporate cyberstalking.

Bocij and McFarlane (2003) offer their cyberstalking definition as:

“A group of behaviours in which an individual, group of individuals or organisation, uses information and communications technology (ICT) to harass one or more individuals. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual purposes and confrontation. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress.”

The ascension of social networking has seen it become the dominant medium in cyberstalking (Read, 2011). Current Facebook accounts stand at over 1 billion (Yung Hui, 2011) and current Twitter accounts stand at over 500 million (Barnett, 2012). The amount of personal information stored on these websites makes it an attractive medium for cyberstalkers to utilise.

Cyberstalking is now more common than offline stalking (McVeigh, 2011). Working to Halt Online Abuse, an organisation set up by a victim of corporate cyberstalking, receive requests for help from in to 4000 cases per year (WHOA, 2012). McVeigh (2011) states that according to the British Crime Survey 2006, it is estimated that up to 5 million people experience stalking each year, although there were no official statistics on how many that includes of cyberstalking at that time. According to figures from the Crown Prosecution Service, cited in the University of Bedfordshire’s analysis of the ECHO Pilot Survey 2011 (Maple, Short and Brown, 2011), 33% of all stalking incidents occurred by email, 32% by text message and 8.4% through various social networking sites. This is contradictory to recent news articles, which may come from basing figures on different sample groups. However, the problem remains regardless of statistics.

There is a wealth of statistics on cyberstalking pertaining to that of age, gender, race, etc., which the mode average suggests that caucasian females in the 31-40 age bracket are most affected (Bocij, 2003; Bocij and McFarlane, 2003; WHOA, 2012), but this does not necessarily correspond to that of corporate cyberstalking.

A. Classification of Cyberstalkers

Researchers have attempted to classify stalkers for the last 40 years with no definitive standard typology universally acknowledged. However, Mullen et al’s (2000) multi-axial study is considered in the field to be as complete to a classification as there is today. This work was essential in helping Bocij and McFarlane (2003) to create their own classification on cyberstalkers. It was revealed that there are
many differences between that of stalkers in the physical world and that of online stalking.

This research revealed four general types of cyberstalkers. These were the vindictive, composed, intimate and collective cyberstalkers. Whereas Mullen’s study revealed most types of offline stalkers had some form of psychological, mental or social disorder, Bocij and McFarlane revealed there to be only one type of cyberstalker to have such problems. Another glaring difference is that of the collective cyberstalkers. These stalkers operate in a group of two or more and usually have a very high computer literacy rate. They often utilise a wide variety of ICT methods to harass their target. A sub-group of the collective cyberstalkers is that of corporate cyberstalkers. This group is actually categorised within this cyberstalking classification, highlighting the dangers of such an offender.

III. CORPORATE CYBERSTALKING

The term corporate cyberstalking is often used to describe cyberstalking incidents that involve companies or other organisations (Bocij, 2002). Statistics and figures on corporate cyberstalking are not freely available, but already it is estimated that corporate cyberstalking amounts to one in four of all cyberstalking cases (Megias, 2013).

Bocij and McFarlane’s cyberstalking classification state that corporate cyberstalkers usually cause harassment to discredit or silence their victims. They employ the use of identity theft and a wide variety of other computational means of harassment. They feel they have been wronged in the past and wish to punish their victim. Corporate cyberstalkers are often found to recruit others to carry out their cause.

Corporate cyberstalking can involve the organisation either as the victim or the perpetrator and in many cases may be an unwitting accomplice rather than a willing participant (Bocij, 2002). The use of company resources, such as email, to attack an individual or organisation can constitute corporate cyberstalking. Therefore, in many instances it may be the role of just one person carrying out such attacks without the knowledge of the organisation. To many this may simply constitute cyberstalking and not necessarily the fault of the organisation. However, it is argued that it is the organisation’s duty to ensure that company resources are used appropriately (Bocij, 2002).

There are several ways in which corporate cyberstalking is committed. One such example is when a company pursues the author of negative comments made about the company online. One such case is that of Mark Zeman, who alleges that Geocities, a free web space provider, actively pursues those who criticise the company on their websites (Bocij, 2002). He claims to have been tracked around the internet, threatened and harassed. This, he claims, makes it difficult to exercise free speech on the internet.

Another example, although legal, contains the use of SLAPPS (Strategic Lawsuits Against Public Participation). This enables companies to prevent the public from publishing various online material, such as complaints and slanderous comments. This is in an effort “…to intimidate activists into silence by filing meritless lawsuits against them…for such torts as slander or intentional interference with business advantage” (Bocij, 2002). This can be argued as a form of cyberstalking, as organisations can use SLAPPS to control information on the Internet.

These first two examples are that of an organisation clashing against individuals, but two organisations can become involved against each other. Lopez, cited in Bocij (2002), describes an incident involving Amway, the world’s largest direct selling company, and Proctor & Gamble. It was alleged that Proctor & Gamble sponsored a website that encouraged negative comments about their rivals. This website contained negative news stories about Amway and even confidential documents. There has also recently been a claim of Samsung paying students to post negative online reviews of their rival HTC’s new phone (Sky News, 2013).

Organisations also become the victim of individuals, both internally and externally. Most instances of corporate cyberstalking concerning individuals as the perpetrator are, as Bocij and McFarlane’s cyberstalking typology states, for financial gain or to exact revenge against a former employer. Organisations can also become targets of political and social activists, which often result in a targeted and sustained cyberattack, such as a denial of service attack or other form of hacking.

Hacktivists is a term given to that of a group of individuals that hack into the networks of organisations in order to cause disruption. They usually justify their actions as remuneration for online injustices and to exercise free speech. Hacktivism is a form of corporate cyberstalking and can be very costly to an organisation if it interrupts their online business. In December 2010 the Hacktivist group Anonymous caused huge disruption to that of Mastercard’s online service in response to them ceasing the process of donations to Wikileaks (Addley and Halliday, 2010). Visa and PayPal were also targeted, which cost the companies a combined total running into the millions. The disruption was caused by running a distributed denial of service (DDoS) attack, which prevented customers from using their services. Two of the group were recently found guilty of launching DDoS attacks from their home computers and sentenced to 18 months and 7 months prison sentences (BBC News, 2013).

A. The First Internationally Headlined Case

The first internationally recognised case of corporate cyberstalking involved Jayne Hitchcock in 1996, who was using the Usenet newsgroup *misc.writing* (Hitchcock, 1996). She responded to an advertisement representing a literary agent, contacted the company Woodside and sent in a book proposal. She was replied to within a week commending her ‘professional’ proposal and was asked for a $75 reading fee. Knowing that this was not the normal conduct of a literary agent she queried it with the Woodside Literary Agency. At the same time negative posts were appearing about this agency and it had transpired that other people were asked for reading fees. After occasional dialogue with the company about the subject and refusing to hand over any money, she alleges she became the subject of forged posts on the newsgroup from an email account claiming to be that of herself. The worst forgery
is alleged to have contained Jayne’s home address and phone number and claimed she was interested in sado-masochistic sexual fantasies. She also claims she was the victim of mail bombing where an enormous amount of emails are sent to an account in an attempt to render the email facility useless. The company were kicked off dozens of different Internet Service Providers. The legal case brought against them by Jayne Hitchcock is still ongoing. She has since become a spokeswoman for cyberstalking and championed the need for tougher laws on the subject.

IV. IMPLEMENTATION OF NETWORK SECURITY

According to PriceWaterhouseCooper’s (PWC) 2012 statistics on security breaches, 54% of small businesses do not have any programme in place for educating their staff on security risks. The use of staff’s own devices connected to the company network can pose many security dilemmas. PWC’s statistics show that 34% of small businesses allow smart phones and tablets to connect to their systems without doing anything to mitigate the security risks (PWC, 2012). This can prove useful to a perpetrator of corporate cyberstalking, as it could prove substantially easier to sidestep security protocols that are already in place on the company network.

A. BYOD

BYOD (bring your own devices) is an increasing problem within the corporate structure. Its accessibility and convenience makes it very useful in the workplace, but unless the security implications are addressed, potential problems may arise. If the security of BYOD is not managed, these devices can be much more easily used in an instance of cyberstalking. Devices can be used to instigate the theft of data.

In May 2012, IBM banned its employees from using Dropbox and Apple’s Siri over concerns for data security on staff’s own devices (Eschelbeck and Schwartzberg, 2012). Concerns such as this can hinder security within an organisation, but steps can be taken to minimise the risk. Sophos’ guide to BYOD security suggests the following security measures be implemented;

- Enforcing strong passcodes on all devices
- Antivirus protection and data loss prevention
- Full-disk encryption for disk, removable media and cloud storage
- Mobile device management (MDM) to wipe sensitive data when devices are lost or stolen
- Application control

(Schertz and Schwartzberg, 2012)

Small companies may find it excessive to implement all these measures, but they are there to provide maximum security. It is up to individual organisations to apply what they feel is necessary. They should note that whatever the cost of implementing such measures, it may prevent them from losing much more in the future in lost business.

B. Network Policies

Strict company policies should be implemented to deter organisational employees from abusing company resources. These policies should include a social networking policy. Whether social networking should be used at all in the workplace is debatable and will vary from job to job. However, if it is allowed, strict instructions should be made to both educate staff and to deter staff from abusing such websites. Not only does it help protect the company from libellous comments, it also protects staff’s own interests.

A general internet usage policy should also be implemented. This should include avoidable websites, appropriate comments to post online and appropriate content of emails. All policies should always remain easily available and accessible to staff and a dedicated person available to discuss with staff any queries about such policies they may have.

It would be advisable to include web filters to prevent staff from using sites that could embroil the company in a corporate cyberstalking case. Also, network monitoring software should be installed. This can be used to track websites that have been used by staff, which is vital if claims of cyberstalking arise within the company, as it can act as a form of evidence. A form of monitoring software that detects words and phrases being typed on the network by staff could be useful. If staff are aware of such policies and monitoring software, it should deter them from using resources inappropriately and protect the professionalism of the company.

The BS ISO/IEC 27002:2005 is a British Standard for code of practice for information security management. This document doesn’t specify details on how to deal with cyberstalking, but it does give a wealth of information on how to manage an organisation’s network resources in an appropriate, responsible and security-minded way. This will help a company to pre-empt, or at the very least minimise, any cyberstalking or harassment attempts from both company personnel and external parties. The BS ISO/IEC 27005:2011 is a British Standard of information security risk management and may also be of value in the identification of security risks and threats.

V. CONCLUSION

Corporate cyberstalking has become a major problem within the corporate world. Statistics on the issue continue to rise, as more and more people are connected worldwide through technological devices. The ease of access to the internet and the ability to anonymously stalk someone online means serious security implementations must be considered.

Sound network security measures are essential in a corporate cyberstalking environment, as data theft is one of the largest issues in corporate cyberstalking. However, increased hardware and software security is not the only remedy to this problem, the education of the company workforce is also essential. If staff maintain vigilance to such activity and preserve the company’s and their personal information as much as they can, needless acts of cyberstalking may be prevented.
REFERENCES


Free Wi-Fi: The Hidden Dangers
An Independent Study

Kyle Straw
University of Derby
Derbyshire, UK
100167172@unimail.derby.ac.uk

Abstract - Free Wi-Fi is a vastly dangerous method to connect to the Internet, however the need to be connected to the internet is ever increasing. How secure is your data when browsing the Internet over Wi-Fi, do you trust the data that your receiving, has somebody captured your passwords and user names. This document provides a best practice guideline on how to stay secure online as well as highlighting the common attack that hackers used to gain access to your data.

Keywords - Computer security, Data security, Wireless LAN, Wireless Roaming.

I. INTRODUCTION

Living in an increasingly technology-reliant world with connectivity at the heart of it all, whether accessing Facebook or browsing the latest emails, we rely on the Internet to conduct our day-to-day activities. A number of industries have come to realize this, with Free Wi-Fi now offered by vendors such as Starbucks, McDonalds, Airports, and a plethora of others.

The daunting fact is that the average smart-phone usage grew 81% in 2012 and is still rapidly growing, with the number of mobile-connected devices exceeding the world’s population in 2013. By 2016, one in four users will use more than one device with 90% of all tablets being Wi-Fi only. 70% of iPhone users and 32% of Android users will be exclusively using Wi-Fi (Chetan Sharma, 2011) for Internet browsing. This comes at a time when, within the UK last year 93% of large organisations reported a cyber-breach with 76% of smaller organisations reporting a breach. In addition, 33,000 malicious emails were blocked by the government’s secure intranet gateway each month. The total cost of a breach is estimated at between £110,000 and £250,000 for larger organisations and £15,000 to £30,000 for smaller organisations. (Cisco, 2013) The need to be secure is ever more paramount.

This article intends to look into the dangers that are associated with free Wi-Fi and how we can help protect ourselves against some of the more common attacks, providing a best practice guideline to stay safe when utilising free Wi-Fi.

II. WHAT ARE THE DANGERS I FACE?

Free Wi-Fi comes with a number of different associated dangers, these can be broken down into the following sections: Sniffing, hijacking and Malicious Access Point (MAP). Each has its own way of intruding on your connection.

A. Sniffing

Wi-Fi Sniffing is a method of recording all data that is transmitted across an open wireless network and works in a similar fashion to eavesdropping in on a conversation. If you are stood chatting to a work college about sensitive information and the person behind you is able to hear you without you realizing. Wi-Fi sniffing is exactly the same but rather than a conversation being heard it is the data being transmitted that is recorded.

This is a relatively easy skill to master and is surprisingly widely used in public places. Sniffing is almost impossible to detect, untraceable and often results in criminals gaining a vast amount of private information they are able to use. The equipment required to ‘sniff’ is no more than a laptop or a smart phone in somebody’s pocket.

The danger of a sniffing attack is that, unbeknown to the victim the ‘sniffer’ is able to read all emails sent and received, passwords typed into websites and any unencrypted web browsing but to name a few.

B. Hijacking

Hijacking (Owasp.org,2011) is where an attacker clones your current Internet session in order to imitate you online; this can also be referred to as session hijacking. A hijacking attack normally involves a hacker performing some form of attack to gain access to the session; some example attacks could include Java Script codes, Trojans, Cross Site Scripting (Xss) but to name a few.

While this is an advanced skill to learn and perfect, the results are often worth the time invested in learning it. It is more detectible than sniffing but provides greater control if successful, allowing the reading of encrypted website data such as online banking details.

There are a number of tools that are available to automate the process of collecting the session keys from a user’s web session and to replay them on the attackers device, one such tool is fire sheep (Codebutler.com, 2011) This allowed hackers to clone any local encrypted social media sites and replay them in order to gain access to the relevant sites. It is still a highly effective tool in the attackers arsenal today.

Again, these attacks occur unbeknown to the victim with the hacker being able to read all of their incoming and outgoing emails, passwords typed into websites as well as all websites visited including, as previously mentioned, online banking details. This also provides the hacker with more
control than the sniffing attacks as it is almost the next escalation of an attack on the victim.

C. Malicious Access Point (MAP)

A Malicious Access Point is, as it states in the name, an access point that allows you to connect to the Internet. It is however, controlled solely by the hacker and not by the establishment offering the free Wi-Fi service.

To understand how dangerous this is we need to know about how a device looks for an access point. A device with Wi-Fi turned on will constantly probe for known access points, i.e. your home Wi-Fi or work Wi-Fi. If this is found it will then connect, if not it will very often just go idle until the next probe is sent looking for Wi-Fi. This probe contains a list of access points that your device will automatically connect to and can be used by a hacker to act as a known access point that will be connected to automatically, connecting you to the hacker’s device.

Once on the hacker’s network there are a number of different attacks he/she could perform. The standard attacks; reading any email, password and website the user connects to, manipulating the data that is sent and received. To explain the full severity of unknowingly connecting to the hacker’s access point a typical coffee shop scenario shall be used:-

Typically, in a coffee shop you would browse the Internet, perhaps looking at the Financial Times or the stock market to catch up with current affairs. The hacker could manipulate the data you see on screen, changing stocks from 2.22p a share to 200p a share simulating a massive growth in the share price. Alternatively, he/she could do the adverse and make share prices look like they have plummeted. Likewise, he/she could provide false news articles or populate your Facebook account with false information. Not only would they have full control over everything you see and do online but also they could manipulate what you see without you having any suspicion of being attacked.

After checking the stock prices you decide to watch the highlights of last night’s football match but require Adobe Flash Player to view the footage. The attacker is incredibly helpful in the fact that he has redirected you to his Flash Player, a disguised virus enabling you to play the video. However, not only will the hacker now have full control of your web activity but he/she would also have control of the device.

This is by far the most advanced attack that can be performed on Wi-Fi but with the greatest results, including full access to everything and anything on the victims device as well as providing a platform to exploit the computer.

III. HOW WOULD ALL THIS AFFECT ME?

There are a number of different ways in which one or multiple attacks would have affected you, the first of which is that all the attacks listed would be able to gain access to all unencrypted communications that were transmitted across the network. (Lucidlink.com, 2007) with the latter two being able to circumnavigate the encryption provided. Some of the associated risks are that the attacker then has full access to email accounts, social network accounts, any client information viewed, anything on the web viewed and in short, full access to anything that was visited in the time using open Wi-Fi. All this information could be used to tarnish the reputation of and/or blackmail the individual and their corporation or the information could be sold on to competitors for a profit.

The highest risk lies within the Malicious Access Point attack as the hacker then has access to not only everything you do whilst online but also without too much knowledge or effort, gain full remote access to all the files on the device as well as gain accesses to credit card information. (Creditcards, 2013)

IV. WHAT CAN I DO TO PROTECT MYSELF?

There are a number of different methods to protect yourself from the attacks and exploits discussed. It will not guarantee that you are completely safe but will aid you in securing your connection to the internet. One of the most important things to do to protect yourself is to move your end point; the point you connect to the Internet. There are a number of ways to do this, the most common being SSH tunnels and Virtual Privet Network (VPN) Connections, (Ikeepsafe.org, 2011)

Both methods have a similar outcome but in moving the location of where the traffic you generate gains access to the Internet, by moving this to a location you trust for example your work, you prevent the hacker from gaining access to any information. A hacker will only be able to pick up the encrypted data to and from the wireless device and not the data itself.

There are a number of solutions involving using Virtual Private Network (VPN) to control network traffic. Some are freely available commercially but capped by data use, others are based on monthly payment plans. Another alternative is to host your own VPN; this can be achieved using a number of different methods.

Two-Factor Authentication is a method of using two pieces of information to log into a website. It requires something you know, such as a password and something you have, such as a security key on your phone. A large number of online social media networks and email services now offer this in order to keep you secure online.

Ensure that your device is protected with a firewall guaranteeing that you have file sharing deactivated. These are relatively trivial tasks but can make a huge difference when browsing via public Wi-Fi and protecting your data. It will not only make the computer safer for browsing online but will also make it harder for an attacker to gain access to information stored on the device.

An up-to-date antivirus software tool is crucial to online security and will help provide a second line of defense alongside the firewall, alerting the user to any malicious activity on the device. Depending on the vendor, this will usually bring to the users attention that they are currently on an unsecure network.

Avoiding automatically connecting to Wi-Fi hotspots is a good way of helping to prevent your network from becoming
compromised. Connecting automatically could dramatically increase the probability of connecting to a malicious network designed to steal your information. Most devices have auto connect function enabled by default.

The use of https will always deter an attacker due to the time and effort involved to circumnavigate it and it should be used whenever possible on websites, most social media websites have an option to turn on by defaults as well as there being several useful browser plug-ins that request https sites.

One of the easiest method to ensure that you are safe it to check the Wi-Fi name that you are connected to. Now this might not help every time but it can sometimes give an indication if you are connected to your home network, while sat in Starbucks. (Norton Security, 2013)

The final tip for staying protected is to assume that a hacker has always got access to your information on free Wi-Fi. Try to avoid any sensitive or private information whilst online, such as online banking and corporate secrets.

It is not always possible to perform the above but some best practice guidelines should be followed when connecting to open Wi-Fi in order to try and minimalize your risk of a successful attack.

V. BEST PRACTICE GUIDELINES

- **Turn Off File sharing** – This can be one of the simplest things to prevent access to your files and data, and should be turn off when using Free or untrusted Wi-Fi.

- **Use a VPN** – As stated above, move the end point to the Internet to a trusted location.

- **Avoid automatically connecting to networks** – This will prevent you from accidently accessing an unsecure network and transmitting data.

- **Confirm the network name** – Check the name of the Wi-Fi connection, likelihood is that if you are connected to your home Wi-Fi it’s a malicious connection.

- **Use https** – This will not make you impervious to attackers but will help in you favor.

- **Use Two-Factor Authentication** – This makes it increasingly difficult for a hacker to gain access as you now need access to pieces of information to log into the account.

- **Protect your passwords** – Unique passwords for each site makes it harder for an attacker to guess password for other websites.

- **Turn on the Firewall** – An added layer of protection against inbound attacks.

- **Assume everything is monitored** – Make the assumption that anything you do online is monitored, and therefore do not access confidential information or online banking. (ZDNet, 2006)

VI. SUMMATIVE CONCLUSION

In short there are a number of precautions that should be taken to ensure that safe browsing is achieved when using free Wi-Fi and by following the best practice guidelines you should minimalize the chance of attack.

Common sense is a good indication when browsing online and should be followed. If you can see it there is a high probability that somebody can also see it by looking over your shoulder, whilst not a technical issue it is something that should be brought to attention.

If in doubt about still using free Wi-Fi there is always a mobile 3g-dongle, which will provide a more secure Internet connection whilst travelling, however best practice guidelines should still be applied when using this approach.
REFERENCES


Chip and Pin Security for SME’s
Is it Out There to Get You? What You Need to Know

Ashraf Uddin
University of Derby
Derbyshire, UK
100244848@unimail.derby.ac.uk

Abstract - The concept of chip and pin is nothing new to the business world, although there is some research that can testify it is a very effective type of payment system, it is not foolproof regarding security, this paper will critically analyse whether this technology should be of assurance to the consumer and retailer, and whether emerging technologies should be considered to replace or be used in addition to present systems that we have been relying on at the dawn of the 21st century.

Keywords - Chip and Pin, Card Fraud, Security, EMV, PIN.

I. INTRODUCTION

Ever since “Chip and PIN” technology was rolled out to businesses and made more widespread from 2004, and made compulsory two years later (Chip and Pin, 2006), the business and consumer world saw a revolutionary method of how payments are handled, although this technology has not been implemented in every country worldwide, this initiative is not being overlooked, as the results in France have seen an 80% reduction in fraud ever since introducing it at a much earlier time in 1992 (Chip and Pin, 2004). As a result other countries including UK saw similar successes.

However seeing great results does not mean you should assume your chances of being a victim of fraud is remote. It is argued by some that this technology is far worse than the traditional magnetic strip or fundamentally broken. In addition any consumer, who happens to be a victim of fraud, is nowadays considered the negligent element of why it happened in the first place (Lythe, 2012). Is this justified? This could happen to one of your clients and you may have to bear the chargebacks of unauthorised transactions. (Streamline, 2011).

The creators of Chip and Pin have declared this initiative as the best solution towards fraud security. But is it really? Is it a sustainable solution for the distant future and beyond? Are there other solutions available to achieve assurance and satisfaction?

II. THE JUSTIFICATION OF EMV SYSTEMS

EMV (known as Europay, MasterCard and Visa) is the technology that is present on cards that carry a small chip, for making present day payments electronically, that most often involves identification through PIN (personal identification number) . (Herron, 2012).

Chances are if you are running a small or medium business in Europe or in America you will have a payment terminal that accepts this smart card. However if you have a online store alongside your business, or operate solely on the internet, then the current EMV smart cards cannot protect the interests of your customers, as this in turn becomes a ‘cardholder not present’ situation. The following graph will illustrate the amount of losses that took place and the steady decline of fraud over the years building up to the year 2011; this includes fraud that did not require EMV identification (the physical aspect broadly speaking).

![Figure 1. Fraud statistics on UK distributed cards 2004-2011](Financial Fraud Action UK, 2012)

The statistics demonstrate that security regarding using EMV cards when used in person has shown effective results to a certain degree when it comes to having your card lost or stolen, with losses declining to £50 million by the year 2011 compared to its introduction phase in which was £114 million, this has demonstrated a 56% reduction in losses. However certain banks are loyal to the concept that EMV on cards are infallible (Clark and Clarke, 2006) and the reason behind those losses after being lost or stolen was because of negligence, or not protecting their PIN appropriately. This will be discussed in detail on Section III.
Unfortunately this does not speak volumes when your customers are not present when the fraudulent behavior takes place. As current EMV systems do very little to protect the consumers and the merchant. Between the years 2004 to 2008 Financial Fraud Action UK (2012) reported an average of £291 million of losses in that period. This demonstrates that the concept of e-commerce was disregarded and overlooked when its importance should have emulated with other fraudulent methods, thankfully action was taken when the rise in losses could not be ignored any longer. From the year 2008 banks worldwide started to authenticate online card purchase with an additional layer of security, using a protocol called ‘3D Secure’ or other names such as ‘Verified by Visa’ or ‘MasterCard SecureCode’ according to Murdoch and Anderson (2010) The losses dropped significantly, but it still remains high, compared to other transaction methods.

Fortunately, something else followed from the year 2008. Counterfeit fraud fell by 79% by 2012. There are many reasons for this substantial drop including:

- More countries around the world have introduced Chip and Pin technology, which makes it significantly difficult to use counterfeit UK cards abroad.
- More banking companies use sophisticated fraud prevention software
- Banking industries working closely with the business community, to raise awareness of ways to protect their terminals from criminal attack.
- The rollout of credit/debit cards with enhanced security features including Card Verification Value, a three digit code on the back of your card (Visa, 2010), No technology can obtain this physical imprint, especially for counterfeiting, thus providing an extra layer of verification, that can validate the real card is used in “card not present” situations.

(Financial Fraud UK, 2012)

To summarise this section you need to consider the fact that although improvements have been made and demonstrated effectiveness, this technology is hardly infallible and it would be an insult to business owners around the world if they were instilled with confidence with this system.

III. THE REPORTED PROBLEMS WITH EMV (CHIP AND PIN)

It is unrealistic to assume that we should anticipate a flawless system, where electronic fraud is a thing of the past, but what we should aim for a satisfactory information system that can be of assurance and confidence with present day technology.

However according to White (2012) who investigated a sophisticated type of fraud that can affect one of your payments terminals, where a fraudster attempts to make a payment using a malicious card, that can inject a Trojan into your system, when it gets declined, he/she simply makes an alternative payment, the merchant will have no idea the device has been hijacked, and the consumers will be simply too oblivious to notice that their details are being extracted when making a payment. The fraudster then simply returns to the premises, attempts to make another payment, and finds the opportunity to retrieve all the details stored on the terminal. Although this flaw has been acknowledged, VeriFone who are the makers for many of the terminals, agreed to have them reprogrammed (Farivar, 2012). It is still something to be concerned of since this was reported last year. Keep in mind an associate of the fraud community may very well be a member of your staff.

Professor Ross Anderson of the University Of Cambridge argues that Chip and Pin and its EMV protocol is flawed and broken, and criminals can use genuine cards to make transactions using sophisticated technology, by tricking the machines in believing the correct pin was entered. This is carried out using a man in the middle approach (MITM). The following figure will illustrate his point of view.

![Figure 2. The man in the middle traps the PIN verification command between the card and the terminal, and tells the terminal the pin has been verified correctly. (Murdoch et al., 2010)](Financial Fraud UK, 2012)

Keep note that the Cards Association disputes this controversial claim, as it is too complicated to pose a real threat to your customers (The UK Cards Association, 2010). Even if figures show low levels of fraud, a security flaw, is something that will challenge the public in trusting these devices.

Could this be the reason why some individuals become a victim of card fraud, even though they are adamant to not divulging it? Or accused of using their card fraudulently to make financial gain? According to a documentary by the BBC (2008) the customers are held responsible for negligence, and seldom given a refund for the money lost, although evidence by the banks to prove it was “their” fault is hardly brought forward (Lythe, 2012). This does somewhat differ to what is explained in the voluntary Banking Code (2005) which makes very little mention in whom will assume responsibility.

IV. STAFF TRAINING

Streamline (2011) who have a reputation of making payment terminals for merchants in the United Kingdom, believe that
adequate staff training can significantly reduce fraud in your business! They even make a statement that if theft occurs due to carelessness, they may stop trading with you. However what was discussed previously, that carelessness pretty much exists in the very technology that we are supposed to use vigilantly. But training your staff is valid, and makes a difference, in most cases anyway.

Having a small or medium enterprise still requires some sort of compliance to ensure your staff are well trained and are setting standards to prevent financial implications if you or your associates become a victim of sophisticated fraud.

A Standard that requires all businesses to be compliant with is the Payment Card Industry Data Security Standard (PCIDSS), (Pci Security Standard, 2013).

This was set up by the PCI Security Standards Council, that states all businesses who store customer data, must be compliant, if they don’t and there a loss of data or a breach, then you could be imposed with heavy fines and could end up with legal complications. This is a global organisation so it essential for everyone who handles payment card data to be compliant (The UK Cards Association, 2012). Legal advice should be sought if you are uncertain this applies to your geographical location.

The council states that you are responsible for handling your customer’s personal details, even if it is handled by a member of your staff. Taking legal action against people who are not compliant is usually by the banks themselves and has nothing to do with the council. So how you are penalised varies, and leniency may not be the desired outcome.

Security of information is paramount to ensure business continuity, to minimise risk, and maximise investments and for future opportunities (BSI, 2005). Having an extra layer of assurance may well be worth the investment.

To summarise, the training of your staff, and being PCIDSS compliant will protect you and prevent complications in the long run. Although EMV technology may have its flaws, this can be compensated by setting standards, legal compliance and being cautious in handling everyday transactions and confidential data.

V. FINGER VEIN BIOMETRICS

Although in its early stage, Hitachi have developed a biometric payment system that uses your fingertips vein pattern to authenticate payments, unlike fingerprints or retinas, it is much more difficult to counterfeit (Enterenetworks, 2013).

This technology is already operating in cash machines in Japan and Poland (Kleinman, 2013), and there is a possibility that in could be rolled out to other parts of the world in the future.

However Chip and Pin has not had its day, because biometrics will not be fully implemented anytime soon, this is because Chip and Pin has only been around for 8 to 10 years and it would be a costly investment for the banks to introduce newer solutions so suddenly (Ryland, 2013).

Keep in mind the latest smartphones are increasingly rolling out Near Field Communications systems or contactless payment phones (Carter, 2013), whether it should be assumed as a safer payment option is indeed a different matter, but it is a reason to space out any proposed solutions in the future, including biometrics.

What may sound appealing and promising may not be convincing to some, as Professor Ross Anderson, who has spent many years investigating bank fraud, is sceptical for the need to change, he believes it is not ethical to change an entire system because a new one comes along (Kleinman, 2013).

This raises an important question; is it possible to improve on existing technologies to accomplish a satisfactory security infrastructure? The statistics shown in Section II proves it is happening already.

To summarise, Chip and Pin has firmly integrated itself in society, and it doesn’t indicate signs of its presence being obsolete anytime soon, Section II discusses how it is rolling out to more countries than ever before. Biometrics like all security systems will not be perfect, but may one day prove to be a better solution over the humble Chip and Pin. Only time will tell.

VI. CONCLUSION

This paper has shown that EMV cards and its associated payments systems, is not infallible, but at the same has shown tremendous improvements over the last decade. Unfortunately card not present situations have shown that more needs to be done to tackle this kind of fraud even though action has been taken.

Despite all the controversial claims that current technologies may be worse off than what was present in the past, statistics illustrated in this paper cannot deny that there has been a change in figures in the past few years, and losses are indeed being reduced as time goes by. One cannot predict the future in whether emerging technologies should be brought in as a matter of urgency, but it should be a welcoming addition to the SME world ever wanted it.

Whether you have a business with an employee count of 50 or 250, being compliant with a standard that is set out by the payment card industry, or whatever may be relevant in your country set out by your banks, is a major step in tackling electronic fraud. With that in mind, alongside having a vigilant and well trained staff, you will find that Chip and Pin is not out there to get you, but the fraudsters will feel you are out there to get them. This is an encouraging thought indeed.
REFERENCES


Social Networking

Employers are Watching!

Gerald Vaughan
University of Derby
Derby, UK
100128025@unimail.derby.ac.uk

Abstract - This paper explores the use of social networking within organisations and how this affects employees and employers out lining the positives and negatives on how this can affect our day-to-day lives.

Keywords - Social, Network, Site, Facebook, Friend, Boss.

I. INTRODUCTION – SOCIAL NETWORKING DEFINED

Since their introduction, social networking sites (SNSs) such as Facebook, Twitter and LinkedIn have attracted millions of users, many of which have SNSs engraved in their every day lives. There are many SNSs, with multiple technological environments, which support a wide range of interest. Among all SNSs that are around today their features are fairly consistent with regards to their overall aspect, but at the same time can obtain various cultures. With the discussion of cultures in a social networking instance it can be a variant from strangers connecting based on shared interest, political view, activities or work place. Some SNSs can cater to diverse audiences such as music whilst other SNSs can attract users on a common language, sexual or religious aspects. With the ever-increasing technology that is among us most SNSs vary with regards to how they incorporate new information and adapt communication tools, such as mobile connectivity, tablets, blogging and photo/video sharing.

Due to SNSs being relatively new there is no common international regulatory body; it is difficult to find an official or universally agreed definition. Boyd and Ellison’s overview of the field in the Journal of Computer-Mediated Communication (2007) comments on the particular communication opportunities provided by social network sites (SNSs):

“We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) Articulate a list of other users with whom they share a connection, and (3) View and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site... What makes social network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks... While SNSs have implemented a wide variety of technical features, their backbone consists of visible profiles that display an articulated list of Friends who are also users of the system... The public display of connections is a crucial component of SNSs. Beyond profiles, friends... SNSs vary greatly in their features and user base... Some have photo sharing or video-sharing capabilities; others have built-in blogging and instant messaging technology." (Boyd & Ellison, 2007, p.1).

Sites vary in security when it comes to what users are able to visibly see and access on another users profile. Fortunately most allow to some degree user control of what people are able to see such as personal details of another user. Most social networking sites incorporate a range of communication tools such as mobile connectivity, blogs, and photo/video sharing.

There are also communication tools in place, which allows the user to be able to perform cross posting between the SNSs that they are affiliated to. This allows the user if they desire to post a comment on Facebook and it will appear on your Twitter.

When a user joins a social networking site, they are able to start building their social network by linking with others – commonly termed “followers”, “contacts”, “friends” or something similar. As an increased security feature most SNSs require confirmation by both users for the friendship link to be made. Connections are generally made public which is an important component as it allows users to generate more friends on their personal social network by linking to friends of friends. It is encouraged on most SNSs to search the ‘friends’ links of ones connections in order to find new connections for the searching user to increase their own private network.

Once users connect with each other they can freely exchange messages and view each other’s profiles, however many of these exchanges are public unless you send a private message. Users often write with the public audience in mind – described by (Boyd & Ellison, 2007, p.3) as “offering users an imagined audience to guide behavioural norms”.

II. HISTORY OF ONLINE SOCIAL NETWORKING

The idea of connecting people by using networked computers in order to boost their knowledge and their ability to learn, dates as far back as the 1960s and the thoughts of JCR Licklider (Walldrop, 2002).

Tim Berners-Lee, the inventor of the World Wide Web, foresaw the development of an active suite of tools that would allow users to create rather than just passively browse (Dertouzos et al., 1999).

During the 1990’s the first protocol of “social” users on the World Wide Web evolved when Eric Thomas invented ‘Listserv’ in 1986. Listserv was a type of discussion software,
which allowed users to link to each other around the world that may have common interests to communicate with each other (L-Soft, 2010).

The first social networking site, SixDegrees.com, appeared in 1997. SixDegrees.com was the first platform that had the all in one-combined features that other SNSs had not yet achieved, for they could only offer a few features as their development had not yet reached the potential which SixDegrees.com had achieved.

Social networking was slow in development at first until 2003 where a boom of new social technology formed. Below is a diagram, which documents the timeline of social networks from when they were first launched.

![Timeline of major social networking sites](image)

Figure 1: Timeline of major social networking sites (Boyd & Ellison, 2007)

### III. THE ADVANTAGES OF SOCIAL NETWORKING IN A WORKPLACE

When used diligently, social networking sites used in a work place can be useful when expanding in market reach, widening the business’s circle of contacts, creating a communication platform with clients allows them to contact the organisation direct which at times can be seen as a disadvantage for others will be able to see what the client writes but at the same time this allows the organisation to broadcast advertisements for free for all clients to see (GFI, 2011).

When using social networking sites, businesses are able to reach new markets but at the same time remain with existing customers and use the ‘snowball’ effect to market its services or products (GFI, 2011).

By using social networks organisations can create a positive presence online, which in turn can boost an organisations reputation and establish their name in new areas before taking the ‘physical’ plunge (GFI, 2011).

Communication whether it’s internal or external is the key to great business success. Once of the fastest forms of communication that allows you to talk publically or privately in a quiet environment is social networking. Apart from the use of email communication social networking is one of the best immediate forms of communication you can find. Employees may be communicating with the outside world, but many of those people could be consumers or even possible clients (Wallen, 2012).

As social networking is a free source of marketing and advertising organisations will not have to invest large quantities of money. However the only cost an organisation would have to invest in would be time and effort which would be required to maintain their social network and if it exists their official website (GFI, 2011).

### IV. THE DISADVANTAGES OF SOCIAL NETWORKING IN THE WORKPLACE

It can be seen that if you do not take prompt action to “lock down” your social networking profiles, potential new employers or your current boss have the ability to simply search for your name that you would supply on your CV and check out what you as a person perceive to be like in the “real world”. This can be seen as a grey area in the legal aspects of today for a potential employers looking on social networking sites at their future candidates can be seen as employment discrimination (Klein et al., 2010).

According to a study undertaken by Nucleus Research, companies that allow their employees to use the social networking site Facebook during a normal working day lose 1.5 percent of productivity due to Facebook’s wealth of applications, status update and games. For this reason employees could find themselves compulsively checking their Facebook through the working day instead of performing work related tasks (Zeiger, 2013).

By allowing employees to access social networking sites to perform business related tasks may have some benefits when communicating to clients promptly but, as there are distractions available on social networking websites this often outweigh and benefits (Yamanouchi, 2012).

Not everything can be prevented outside a work place where by for example if employees started to add one another via their desired social networking sites this could lead to the potential where employee relations can have an effect during the work place. The reason for this can fundamentally come down to how employees treat one another. Employees could send negative messages or harass one another via social networking sites hindering their ability to work together. Following on from this potential risk, an employee could harmlessly relay a bad day via their desired social networking site and another employee could display this to their
supervisor, which could lead to tension during a normal work day and resentment among employees (Yamanouchi, 2012).

As social networking is a communication tool this could lead to employees communicating to one another via a private chat throughout a working day which would increase in off-tasking (Zeiger, 2013).

V. CASE STUDY

A recent news article (Gladwell, 2013) on the BBC website explores a real life issue where an employee called into work stating that she was ill and did not come into work for two days. After these days had passed the employee named Kelly Doherty explained how her boss gave her a call to ask her if she had been having a nice time over the past few days. It then occurred to Kelly that her work colleagues had grassed her up telling their boss what she had been up to for Kelly had posted what she had been doing with posts and photos via the popular social networking site called Facebook. Instead of detailing why she should not have committed the lie to her boss Kelly stated: “I should have set my privacy settings.” Along side this story there is also a section that details how a person named ‘Dan’ for he wished to not be identified recently hit an issue where he lost out to a job with a popular café chain for he was joking about the chain over twitter. Dan explained how he thinks the decision should have been made on his skills but it can be argued that if he was joking about the company before he joined… what would his attitude be at work? (Gladwell, 2013).

The recruitment society has noticed that there is an increase of inappropriate photos and comments, which are public on sites such as Facebook and Twitter if the user has not set up privacy restrictions. Both are working it is legal for employers to search social media sites as long as they do not discriminate (Gladwell, 2013).

VI. SHOULD YOU ADD YOUR BOSS?

As discussed in order to make a link between two people, they must first both accept to be friends. What happens if one day you look at your friend invite box and you see your boss? If by ignoring the request sent what could this imply? It could appear that you have something to hide or the worry that a friend may write something embarrassing to you on your person “wall”. There could even be the potential where you may not get better acquainted with you like you do with the rest of your friends. Kiisel (2012) states that you need to set an inner filter for yourself, which is:

“Will this update embarrass my employer or my Mum? If I feel good about it after that, I post – If not, I don’t”.

A recent survey conducted by a survey site named ‘SodaHead’ and a feedback site ‘YouTell’ asked 722 anonymous people whether you should add your boss at work? 81 percent of people said that you should not add your boss with the age range of 25 – 34 year olds (Kleinman, 2013).

Other reasons why you should not add your boss can effect how you use social networking for there are little steps that can get you in trouble if you are not careful. For example if you create a status whilst at work, your boss will be able to see this and if noticed that this was done during work time and not during a break then he would know that you have been slacking off. You will no longer be able to vent out about a bad day you had at work (Schawbel, 2012).

VII. CONCLUSION

In this report is has been discussed whether it is a good idea to add your boss at work. There have been advantages discussed such as how using social networking from a business point of view can benefit the company keeping up with technology trends. But on the flip side there are many distractions which employees can still access. From the research gained on whether you should fundamentally add your boss concludes that you should not if you need to alter the way you act on social networking site for not all users display their daily lives via social networking sites. There are benefits that can be gained by adding your boss for you are then able to gain an insight to their outside lives and learn what their interests are to help form a bond ship which in conclusion could help with the progression of your career.
REFERENCES


Abstract - Cloud computing provides a new environment which small to medium sized enterprises (SME’s) can utilise to lower overheads and expand exponentially (when compared to conventional hosting). A number of important points need to be considered however, before an SME ventures into the cloud. Failure to do so could result in catastrophic damage to an SME’s reputation and/or customer base. This article outlines these key issues, providing solutions and best practices which should be adhered to, in order for SME’s to avoid the issues and therefore use cloud services with confidence.

Keywords - Cloud, SME, pitfall, legislation, solution.

I. INTRODUCTION

Research undertaken by Haroon (2013) suggests that the implementation of a cloud platform can save an SME around 45% of its operating expenses. With such a large potential cost saving, it comes as no surprise that Gartner (2010) estimated that cloud computing vendor revenues are set to increase from a reported $81.3bn in 2010 to $148.8bn in 2014. With such a large increase in cloud computing, SMEs will be considering their approach to IT and discussing whether now is the time to join other SMEs who are venturing into cloud computing.

To best address SME queries about cloud computing, this paper highlights the key concerns for SMEs considering cloud infrastructure for their business rather than traditional IT outsourcing products. The paper then offers assurances that provided issues with the cloud are adequately assessed, there is no reason why they cannot be overcome.

II. CLOUD COMPUTING VS TRADITIONAL HOSTING

Cloud Computing is defined as the delivery of services (offered remotely) via a network such as the internet (NIST, 2011). Cloud computing is a relatively new product which originally emerged in 2006. Since then it has undergone many radical changes and currently comprises of 3 service models (Cheng & Lai, 2012); Infrastructure as a service (IaaS), Platform as a service (PaaS) & Software as a service (SaaS). Although each of these cloud services are defined as cloud computing solutions, they perform very different functions and all benefit SME’s in different ways. Ultimately though, cloud solutions aim to provide an increase in resilience and performance (Figure 1) whilst providing a reduction in costs compared to traditional hosting solutions (Esayas, 2012).

III. TYPES OF CLOUD SOLUTIONS AND BRIEF OVERVIEW

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Public Cloud</th>
<th>Conventional Data Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appearance of infinite computing resources on demand</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Elimination of an up-front commitment by Cloud users</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Ability to pay for use of computing resources on a short-term basis as needed</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Economies of scale due to very large data centers</td>
<td>Yes</td>
<td>Usually not</td>
</tr>
<tr>
<td>Higher utilization by multiplexing of workloads from different organizations</td>
<td>Yes</td>
<td>Depends on company size</td>
</tr>
<tr>
<td>Simplify operation and increase utilization via resource virtualization</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Figure 1. Advantages of Public Cloud Systems over Conventional Data Centres (Armbrust et al, 2010).

Each type of cloud solution; IaaS, Paas and SaaS provide distinct products for customers. IaaS is the most simplistic and widely used of the cloud computing genre. It refers to the rental of physical or virtual machines, storage solutions and other hardware to a customer in order to host or run any software the customer requires. It is best suited to an organisation that requires raw computing power for a limited period of time as the support for any software will still lie with the end user (i.e. an SME).

The key benefit of IaaS is that if the requirements of the SME rapidly change, so too can the number and/or specification of the IaaS services. In effect – you are only billed for what you have used, saving an SME money on (what is often) a monthly basis. This type of arrangement with a cloud provider also delivers further financial benefits; the only cost incurred is a rental charge, thus removing the often high initial financial commitment required to purchase the hardware outright when hosting services in-house. The downside with such an arrangement is that an SME will still be required to maintain the hosted servers; this includes the patching of security vulnerabilities and installation/support of applications and operating systems, if an SME does not have the expertise to perform these tasks, then IaaS will not be the best option.

The second type of cloud computing is PaaS. This is where a cloud provider provides the same foundations as those in IaaS solutions, but includes built-in functionality to improve and simplify the development and deployment of applications across a customer network. Software provided
with PaaS solutions typically includes: operating systems, programming environments and web servers. This means that an SME can completely outsource their IT requirements, as the vendor will support the key pieces of software and therefore remove a key section of in-house support requirements. However, by handing over responsibility of key software to the vendor, an SME is likely to see a proportional increase in rental cost, as well as being presented with a number of ethical and legal considerations, which will be discussed later in this paper. This type of solution would best benefit an SME looking to centralise their IT systems, with the inclusion of a hierarchical organisational rollout i.e. introducing Microsoft Active Directory. As with IaaS, the implementation of PaaS will still require key skilled individuals from the SME in order to administrate the network effectively.

The third type of cloud computing is SaaS. This is the most comprehensive of all cloud solutions and describes the rental of a completely managed and supported service from a cloud computing vendor. Although SaaS solutions do offer cost savings in terms of licensing fees for software, often benefitting from hefty wholesaler discounts, it does warrant a much larger rental cost than other models. However, the cost is often offset by the peace of mind provided by complete management/support solutions afforded by the vendor. Although very little work is required by an SME with a SaaS solution, it is important to remember that this level of outsourcing does not reduce the importance of key ethical and legal documentation that should be created and maintained by the SME. As a result, SaaS is typically utilised only by large organisations that fully understand both their exact IT requirements as well as key legislation and have the capital and knowledge to completely outsource their IT needs.

IV. WHY IS THE ISSUE RELEVANT TO SME’S

Research provided by the Office for National Statistics (ONS) has shown that 99.9% of enterprises in the UK are SME’s and these businesses provide almost 60% of all jobs in the UK private sector (Mills, 2011). As a key driving force in the UK economy, it is therefore imperative that SME’s succeed and flourish to aid economic recovery and ensure future prosperity.

In order to succeed, SME’s need to evaluate their IT requirements and examine whether their capital is being used both appropriately and wisely. Ayers (2012) explains that evolving business requirements are resulting in the need for SMEs to consider moving their data and backups to cloud solutions. Synchronously, research conducted on behalf of PricewaterhouseCoopers (PwC) (2012) suggests that a quarter of small businesses utilise cloud solutions and that a third of all SME’s in France now use cloud computing solutions or are expecting to by 2014. Similar research (Sumastre, 2013) also confirms the increase in cloud computing usage among SME’s, suggesting that cloud computing use by SME’s worldwide is set to double by 2015. This large uptake of cloud services by SME’s is fuelled by a number of key benefits. The most obvious of which is cost. The solutions offered by many cloud computing vendors simply offer better value for money than in-house alternatives. Secondly, the reliability and security of systems are much higher than those managed in-house, in addition there are also significant benefits in; scalability, maintenance, centralisation, reduction of carbon footprint and access to data. Ayers (2012) however, highlights that it is important to remember that outsourcing all IT systems to cloud companies does not remove the need for the development and maintenance of what he describes as ‘standard’ IT policies including; compliance, auditing and reporting.

Another key factor was identified by Svantesson (2012), who notes that unlike conventional hosting methods, the power balance held by a cloud computing vendor is much greater than traditional hosting companies, meaning that they have much more control over an SME than they are probably used to. This means that it is sometimes difficult to ensure that work and compliance is undertaken using the same advertised and compliant methods as the SME.

ENISA (2012) explain that most SME’s are wary about contractual clauses and in particular contract lock-ins. Marston et al (2011) note that a carefully examined contract and/or pre-contractual negotiations should negate these concerns and Hon et al (2012) suggest that if a contract is not completely appropriate for an SME then they should not feel bullied into signing.

Cloud computing contracts do however provide clauses that benefit the customer. Cloud vendors frequently outline service level agreements (SLA’s) where a cloud vendor provides statistics demonstrating service uptime guarantees. Good cloud vendors also allow for the inclusion of service credits into contractual agreements. This is where the cloud company agrees to waive all or part of a customers’ fee, should the customer suffer service outages which bring their SLA’s below those specified in the contract (Martson et al, 2011). Most importantly, this type of agreement surrenders power back to the customer often providing a more balanced agreement than other contracts.

V. KEY ISSUES OF CLOUD SOLUTIONS

Fontana (2013) on behalf of The Cloud Security Alliance (CSA) identified the 3 main concerns with cloud services in 2013 to be: data breaches, data loss and account hijacking. These findings coincide with other research performed by The Identity Theft Resource Centre (2013) which identified approximately 146 data breaches in the first 3 months of 2013, these incidents amount to the loss of nearly 900,000 personal records – a deeply worrying statistic. Another key issue with cloud environments is ‘nuisance neighbours’, Ayers (2012) suggests that shared infrastructure can result in performance issues and even the compromise of data by malicious or ignorant tenants. It is made clear by Fontana (2013) that a poorly designed multitenant cloud platform could mean that a breach of security on another customers’ account is possible - meaning that all customers who share resources with them are vulnerable.
Many SME’s may feel that in light of potential financial savings, a data risk is an acceptable one, however both Oosterhof (2012) and Ayers (2012) note that both the UK Information Commissioner’s Office (ICO) and the Financial Services Authority (FSA) have been applying large fines to companies that have breached data privacy policies and the organisations remain vigilant for future offenders.

Despite these risks, most industry analysts (Gartner, 2010; Ayers, 2012; Sumastre, 2013) predict large rises in cloud computing use among SME’s, it is therefore important to emphasise the key legislation that could affect an SME when migrating to a cloud based environment. Failure to comply with this legislation would expose an SME to legal action, a loss of brand confidence and large fines.

VI. KEY LEGISLATION

One key piece of legislation is the Data Protection Act (DPA) (1998). As the name suggests, this legislation governs the protection of customer data for which an SME acts as custodian. Under this legislation, customer data must not be transferred outside of the European Economic Area (EEA) unless that country can provide guarantees of adequate protection. As cloud companies store data in datacentres around the globe, the migration onto cloud computing environments is potentially a DPA (1998) breach waiting to happen. To avoid this, the cloud vendor should be contacted and asked to provide adequate assurances in line with the DPA (1998) that customer data will not be stored outside of the EEA in any country that cannot offer adequate assurances.

The DPA (1998) also requires customer consent to store any of their information in the cloud. If an SME is just considering the move from in-house technology to the cloud, it is unlikely that initial customer contracts/agreements included the necessary consent for cloud migration. In this instance it is imperative that an SME ensures that customers are made aware before such a move is considered. Unless customers are secure or governmental in nature, it is improbable that they will oppose such a move, provided that both the SME and cloud vendor can provide a level of assurance.

Joint, Baker & Eccles (2009) warn that in reality, customer consent is almost impossible to actually achieve as cloud vendors are under no obligation to digress where sensitive information is stored within their network. However in practice, so long as assurances have been provided by a cloud vendor and there are reasonable plans in place, there should not be an issue with achieving customer consent.

Another key factor to remember is that Joint, Baker & Eccles (2009) note that the majority of cloud vendors use 3rd party organisations as part of their network, which may be managed in other countries. It is important therefore for the SME to understand how the cloud vendor organises its network, what access to customer data these 3rd party organisations will have and what assurances there are with regard to data control. Principally, the assurances should be at least the same level as those championed by the SME, any less could lead to a loss of customer confidence should things go wrong.

The International Organisation for Standardisation (ISO) provides guidelines (ISO 27001 & ISO 27002) for businesses with regard to information assurance. This work builds upon the British Standard 7799 (2005) and provides a set of standards that an organisation of any size should adhere to in order to become fully compliant. Compliance to the ISO27001 (2005) and ISO27002 (2005) standards provide a global recognition of confidence, credibility, trust and satisfaction to customers and also to organisations that wish to perform business with an SME. Full compliance with these standards is anticipated to protect an SME from most of the major causes of data breaches in the cloud environment, and also to limit the damage should a breach occur. The easiest method for ensuring this compliance is demonstrated by the FSA (2011). The FSA provide a ‘1 minute guide’ aimed directly at SME’s to allow businesses to ensure they are fully compliant with regards to data security.

VII. THREAT OF MALICIOUS INSIDERS

Both Waqar et al (2013) and Sood (2012) note that the threat of a ‘malicious insider’ is one of the most serious risks for an SME utilising cloud infrastructures. This is because an insider generally has full and often unrestricted access to all sensitive data once it is in the cloud and this could result in information being used for untoward purposes (such as marketing), modified or even corrupted/deleted.

VIII. CONCLUSION

The best way for an SME to avoid the issues mentioned in this paper is to thoroughly research cloud providers and solutions before entering into an agreement. ENISA (2012) explain that the main concern of SME’s using the cloud is actually confidentiality, in effect – can a chosen cloud vendor maintain the level of confidentiality that the SME provides for its customers. If the result is unclear then a cloud computing approach is probably no better for the SME than traditional hosting products.

On balance Ayers (2012) notes that most data protection issues in cloud environments can actually be overcome simply by using a layered approach to security. This is often through the utilisation of an industry standard encryption technique. That way, even if cloud systems are breached, company and customer data will remain private and malicious individuals will not be able to view and therefore manipulate any sensitive data.

As a result, provided that the issues highlighted in this paper are addressed appropriately, SMEs should not be deterred from venturing into cloud based environments. Provided the risks have been adequately assessed and the SME is compliant to industry standards highlighted in this paper, the potential benefits of cloud computing to SMEs on a scalability and financial basis, should outweigh the potential risks in most situations.
Storage Backup

Why is this Important for Small and Medium Enterprises?

Scott Whittaker
University of Derby
Derbyshire, UK
S.whittaker1@unimail.derby.ac.uk

Abstract - every computer is at risk of failure or being part of a disaster, which goes hand in hand with data loss. This is why it is important for companies (small and medium enterprises in particular) to have a backup plan, where any fragile data can be recovered if lost. There are a number of devices and services that can be used in order to make sure the enterprise has a contingency plan.

Keywords - SME, Data Loss, Storage Backup, Backup Devices, Downtime, NAS.

I. INTRODUCTION

This article will look into what storage backup is, why it is important to small and medium enterprises (SMEs) and how the tools and services can be implemented and the effect that will have on an SME. It will also look into the advantages and disadvantages of each of the backup storage devices, to give an insight into which one would be the most appropriate for a company. It will also look at some interesting, and scary, figures about data loss and the effects that can have on a company.

II. WHAT IS STORAGE BACKUP?

Storage backup in computing is a useful tool which could potentially save a small/medium enterprise from collapse due to loss of important data. Storage backup is storage that is a direct copy of data that is already in use. If the hard drive that holds the current data becomes corrupt then the backup data can be used to recover the loss of data in a short amount of time, because loss of data could be catastrophic to a small enterprise (Rouse, 2005).

Loss of data can occur through several means, whether they are due to human error or not. The following statistics show us about the leading causes of data loss (see figure 1): 44% of data loss is due to hardware or system malfunctions, 32% is due to human error, 14% is due to software corruption, 7% is due to computer viruses and 3% is due to natural disasters such as flooding. These statistics show us several different ways data can be lost, most of which is out of human control. Therefore backup is essential (Protect Data, 2004).

Fig. 1. Statistics about leading causes of data loss. (Protect Data, 2004)

There are several ways to backup, and an SME should use more than one to make sure the data is even safer from disaster. These are some of the devices and services are available for data backup; Hard drives, USB Drives, Network Attached Storage and ‘The Cloud’ (Tanner, 2011).

III. WHY IS IT IMPORTANT TO BACK UP DATA?

It is highly important for an SME to back up data because loss of important data can lead to a large loss of money and time, which ultimately could be the demise of an SME.

A survey by The Diffusion Group in 2001 showed very interested statistics that displayed the impact of loss of data to more than 1,000 small business organizations; the most shocking of which is that 40% of SMEs do not back up their data at all. This means that if some sort of disaster were to happen to these SMEs, then it is more than likely that they will not be able to continue their practice. It is important to note the age of this survey, and how that means that is likely that the amount of money in the next statistics are likely to have increased as the rise of dependence on technology and data has risen within SMEs and businesses in general. This study shows that it takes 19 days and costs around $17,000 to retype 20 megabytes of data, if the data is not backed up within storage which shows the severity of not backing up data. Of the companies participating in the survey, 46% of them said that each hour of downtime would cost their company up to $50K. 28% said each hour would cost between $51K and $250K. 18% said each hour would cost between $251K and $1 million. 8% said it would cost their companies more than a million per hour (NetworkSystems.com, 2008).
Money lost due to data loss and downtime (per hour)

<table>
<thead>
<tr>
<th>Percentage of companies</th>
<th>Money lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>46%</td>
<td>Up to $50K</td>
</tr>
<tr>
<td>28%</td>
<td>Between $51K and $250K</td>
</tr>
<tr>
<td>18%</td>
<td>Between $251K and $1 million</td>
</tr>
<tr>
<td>8%</td>
<td>$1 million +</td>
</tr>
</tbody>
</table>

These statistics show us the severity of the situation and how important it is to backup the data. Remember that this is after only an hour of downtime! It is possible to see why an issue like this could cause an SME’s profit and loss numbers to be unsustainable and can cause up to 70% of businesses to fail within the next five years after the data loss incident (Boston Computing Network, 2013).

Quite often, data loss can cause more trouble than loss of time and money. For example, loss of integrity and trust can happen if the loss of data is sensitive to several people. In November 2007, HM Revenue and Customs (HMRC) lost computer discs containing the entire child benefit records, with personal details of over 25 million people. Included in these records were the names, addresses, date of birth and bank account details of every person. This goes to show how severe data loss can be, and the loss of trust in the HMRC. This can be applied to any SME, where customers/users could lose their trust in them which in turn leads to a loss of money etc. (BBC News, 2009).

IV. HOW TO BACKUP DATA AND THE ADVANTAGES/DISADVANTAGES FOR SME’S

There are many ways that an SME could back up their data, all of which have advantages and disadvantages that should be taken into consideration when deciding which route to take with regards to storage back up. Some are cost effective, whilst others are more safe or larger.

One of the most common backup devices, especially for an SME is a NAS or network attached storage. A NAS is a server which specialises in saving data, and once configured it can be displayed as a separate drive on a computer so that you can wirelessly back up data to it. Whilst it is a pricey option, it has several advantages. It can be attached to several computers at once, so at an SME, everyone working with a computer can back up their data to the same drive which in turn allows everyone to share the data. It can also be set up to do automatic backups so that the user does not have to constantly manually save their data. However, as this would be an onsite device, it is subject to the same disasters that a computer is. For example, if a fire were to wipe out an entire office then the backup would most probably be destroyed too. However, it still acts as a backup and as the statistics show more disasters occur due to hardware and software malfunction than natural disasters, so it is likely that the data would be safe (Levine, 1998).

Another way to backup data is to save the data to an external or portable hard drive. This differs from the NAS devices as they only connect to a single computer at a time. The size of these devices can range from small to large, so there is no end of storage possible with them. As they are portable, it is possible to backup the data and remove the hard drive from the premises which will avoid the risk of a natural disaster ruining it with the original data. Of course this can lead to human error, if the hard drive is misplaced or lost then the backup data is gone. This has risks to confidentiality, where sensitive data is lost. This is why the majority of organisations will ban the use of external hard drives for the saving sensitive data, unless sufficient encryption on the device is in place. The encryption on the devices is very important because it is expensive to recover from identity theft, and it will also lose the SME integrity with customers. Portable hard drives are easy to use, as they appear as an extra drive on the computer when attached that the user would simply save data to, manually or automatically with the correct software. Like a computer, the software and hardware on them can also fail, so using one almost acts as an extra layer of safety rather than 100% certified backup (School of Medicine University of Miami, 2008).

The next option is a valid one, but relies on the use of the format in the future. This format is CD, DVD or Blu-ray discs. It is possible to burn data to them and then access that data from a computer with the appropriate drive. Like portable hard drives, CDs, DVDs and Blu-ray discs can also be prone to human error, where they can easily be misplaced or broken. However, unlike a portable hard drive, drive failure is not an issue. It is also easily to safely secure a CD outside of the SME’s premises, such as in a safe or lock box. As the format slowly dies out, this may not be a great investment for the future. It is also time consuming to burn data to a disc, as several gigabytes can take up to hours to convert onto a disc. Furthermore, it can be expensive to buy discs with a sufficient and large enough amount of data that would be useful to an SME. (School of Medicine University of Miami, 2008)

Using USB Flash Drives are a smaller yet cost effective way of backing up data that can easily be kept safe in your pocket. Conversely they could also be lost easily in your pocket. As technology advances, the amount of data that can be held on a small drive like these increases, and the price is steadily dropping. A SME could buy several USB Flash Drives for the same price of say a NAS server, so this aspect is very good. However, because they are so small physically they can easily be misplaced and should not be used for long-term storage (they are better for moving data from one computer to another). Last year, the Greater Manchester Police lost a USB stick that contained sensitive data about an investigation, and they ended up being fined £150,000 which goes to show that USB flash drives may not be the safest option if even arguably the most responsible of people can loss them (Kobie, 2012). Also they can easily be destroyed due to their size. SMEs should only considering using USB Flash Drives as short term back up at the most (Johnston, 2013).

![Fig. 2. Statistics on money lost due to data loss. (NetworkSystems.com, 2008)](image-url)
The next option (and possibly the most interesting option) that an SME could use as storage backup is ‘The Cloud’ or Cloud Computing. This means backing up data through the internet to a remote location, otherwise known as the cloud. The data is secured safely in a bank of servers which are run and maintained by a company that specialise in the field (Griffith, 2013). The advantage of cloud computing as a backup service is that it is offsite which means that it is not prone to a disaster at the SME (even though the server bank in whatever location it is at is obviously vulnerable to the same disasters). Furthermore, this is currently the most cost effective way of backing up data because it eliminates the need to pay for software, hardware and wages for maintaining the data. This will severely lower the company’s IT expenses, as cloud computing services are available at pay-as-you-go and monthly rates as well as one-time payments. Cloud computing almost has unlimited storage too, so an SME with a constant stream of data will always be able to back it up, as long as the service provider allows it (which most do). Cloud computing services allow all the data to be accessed from any computer too, as long the security details are correct. This is key when considering the number of disasters that occur and the number of laptops that are lost (around 800,000 laptops are lost in airports alone a year according to a study by the Ponemon Institute for computer manufacturer Dell Inc.); a user would be able to access the data from home and then would be able to use the same data when at work without having to move a device between the locations, which solves the problem of human error and losing devices (Smith, 2008).

However, cloud computing is prone to technical issues which can affect the businesses on each end of the service. The SME needs to have a constant internet connection in order to be connected to ‘the cloud’, so if that connection is lost for whatever reason then the data cannot be accessed. Although, as technology progresses this is not always the biggest issue. Even though most cloud computing providers have the highest level of maintenance, they are still prone to outages and other issues so that should always be taken into consideration. Two years ago, Amazon’s cloud computing servers failed which in turn saw many websites that use their service be taken down which shows the risk involved when companies rely on cloud computing (Miller, 2011). Additionally, when an SME uses cloud computing they are more or less surrendering their security plans to a third party company. This of course could put the company at risk so you need to make sure the service you use is completely reliable and that you have contingency plans and legal plans in place just in case the trust you have with the third party company is broken. Just like any computer in the world, the servers provided by the cloud computing service are prone to attack from hackers and viruses and would possibly be targeted due to the fact that it is known the servers will have such a high level of data, so of course this should be taken into consideration by an SME (Kumar, 2012).

V. RECOMMENDATIONS

It is easy to see how severe data loss can be to an SME, with some shocking statistics to support this. Therefore it is possible to recommend that any SME that handles any kind of data via a computer should have a contingency plan with regards to data loss. The majority of causes of data loss are out of the hands of any employee so it is important to have something in place to save the data. This is of course storage backup devices. Whilst it is advisable to backup data with any means necessary, the most popular and most advised option is currently cloud computing as the benefits of not having to maintain your own servers and having data saved offsite solves many of the problems that the other devices have. It is advisable that an SME also uses another backup storage device such as a NAS because the benefits of on-site shared backup storage are also important. If you don’t have data backed up and a disaster occurs within your SME, you can expect to struggle and close in the coming years.
REFERENCES


Abstract - Cloud computing offers a range of benefits to SME’s that can be appealing, however there are also a number of significant risks which need to be considered. The various risks and benefits are discussed with an aim of providing information to SME’s that will help them to decide whether cloud computing is right for them. Methods for helping SME’s analyse the cloud environment are also discussed, concluding with recommendations on a suitable approach.

Keywords - Cloud Computing, SMEs, Benefits, Concerns, Threats, Risk Assessments.

I. INTRODUCTION

This paper looks at the issues of security in cloud computing, from the perspective of small to medium enterprises (SME’s). Aiming to analyse and present the risks and the benefits, to help enable SME’s to understand the various considerations, when they are deciding whether to invest in a cloud-computing model for their organisation.

II. CLOUD COMPUTING BACKGROUND

Cloud computing makes computing, technology, services and applications available as a self service utility. Services and application are run over a network that uses virtualised resources, which can be accessed using normal network standards and Internet protocols. The physical systems running the services are not visible to the users, as they are presented with resources that seem virtual and limitless (Sosink, 2011).

There are a variety of different platforms of cloud computing, the main recognised areas are; Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) (Sosinky, 2011). SaaS offers a user the ability to access and run software over the internet often through their web browser, supplied and hosted by a cloud based organisation (NIST, 2011). PaaS allows the user to deploy their own software on the cloud providers’ hardware, this can be software they have acquired or designed themselves (NIST, 2011). IaaS provides the user with computing resources for processing, storage and networking, it also allows the user to customise the operating system (NIST, 2011).

III. ATTRACTION AND UPTAKE

The cloud-computing model offers a lot of benefits to SME’s, these benefits include increased computer power with the ability to lease additional processing power as and when it is required. SMEs are able to add additional computing resources without the risk that it may no longer be needed in a few months (Marston et al, 2011). By utilising the cloud there is the potential to save money as SME’s can mange their computing resources on a flexible model, making changes whenever they need to, meaning that in theory they will only need to pay for the actual resources they need, when they need them (Marston et al, 2011).

Sultan (2011) states that studies show SME’s are keen to adopt cloud computing, as 47% report planning to utilise cloud services within the next 5 years (Stening, 2009). The survey of SME’s conducted by ENISA (2009a) cited the main reasons for SME’s utilising the cloud as flexibility and scalability (64%) and reducing the expenditure on; hardware, software and information security (68%).

IV. CONCERNS

The potential benefits can make cloud computing a very attractive proposition to SME’s, however so far there has been a lack of uptake on a large scale (Nair et al, 2010). There are a variety of concerns that hold back SME uptake in the use of cloud computing. Organisations are concerned about the loss of the physical control over their data if they choose to store it in a cloud-based environment, they have to put their trust in the cloud provider. A further concern for SME’s is the fact that cloud providers are not able to guarantee the physical location of their data. SME’s will also have to put a lot of trust in the infrastructure of their chosen cloud provider if they are going to run mission-critical applications via their services (Marston et al, 2011).

Studies carried out by ENISA (2009a) have highlighted that 86% of SME’s are concerned about their confidentiality when using the cloud. The study also showed that 87% are concerned about the integrity of their data and the services on offer. In addition there are also concerns about cost, with 74% concerned about the uncontrollable variable cost, as well as 67% being concerned with the clarity of pay per use schemes. Figure 1 shows the results of the survey question on SME’s concerns from ENISA (2009a).
V. THREATS AND FAILURES

There have been previous failures that have resulted in the loss of data and problems for users of cloud computing infrastructures, which will cause significant concern for SME’s. For example when charges were brought against Megaupload, the data of 50 million users was seized and could potentially be erased, even though these users were not implicated in the charges (Duranti & Rogers, 2012). Gartner research has shown that over the last 10 years there have been 48 cases of cloud service outages with an average down time of 17 hours (ENISA, 2012).

ENISA (2012) conducted a further study, looking at the potential threats that cloud computing poses, as part of this study they identified a variety of different threats. The threats include; Cyber attacks, Systems failure and legal disputes, another paper written by ENISA (2009b) also highlighted the risk of lock in.

Cyber attacks are a significant threat as cloud providers have often been targeted, as shown by recent cases such as that of Epsilon. The company was recently hacked, resulting in the loss of data from at least 50 companies (ENISA, 2012). This included customer data from high profile clients such as Barclays Bank, JP Morgan Chase and the Marriott (Bhadauria et al, 2011). Global payments, a company that processes credit card details was the victim of a cyber attack, exposing details of 1.5 million customers. This particular security breach is estimated to have cost Global payments around $84.4 million dollars (ENISA, 2012).

Systems failures can also cause outages, in 2011 an error on an internal server at Amazon spread through the system and caused a multi-hour outage in its s3 storage service (Pfeffer & Pfeffer, 2007). In February 2012 the Microsoft Azure service went offline in multiple regions due to a leap year problem. Most customers had their service restored within 9 hours, however it took 24 hours for a full restoration of services (ENISA, 2012).

Legal or administrative disputes should also be considered as a major concern, as previously mentioned the Megaupload case caused data to be lost affecting many users, in total 180,000,000 users were registered storing 25000 terabytes of data. In 2008 the Linkup service lost access to its customer’s data and as a result shut down its service, it had over 20,000 customers that used the service to store data (ENISA, 2012).

SME’s may also become locked in to their cloud service provider, as there is not currently any easy way of transferring from one provider to another. There is a lack of; data standards, procedures and tools to transfer services to another provider, which could result in an SME becoming dependent on one cloud service provider (ENISA, 2009b).

VI. SOLUTIONS AND ADVANTAGES

Cloud computing does offer a variety of advantages that should also be considered and there are some solutions that can help to mitigate some of the previous risks and threats mentioned.

Kandukuri et al (2009) discuss how service level agreements (SLA’s) can be used to reach a suitable agreement between, the SME and the cloud service provider to govern a variety of issues. This includes agreeing certain security standards that should be adhered to during the term of the contract.

The physical location of the data stored with the cloud provider is a concern, as depending on where it is stored different laws and legislation will apply to the data (Schwerha, 2010). An SLA could be used to form an agreement between the two parties as to where any data would be physically stored (Kandukuri et al 2009).

In contrast to the security threats as highlighted by ENISA (2009b) there are also some security benefits. Because cloud providers are implementing security features on a large scale this will make them cheaper, as a result the same level of investment can offer SME’s better protection. Cloud service providers will also be conscious of their reputation. When investing in their security, they will likely want to ensure they offer high levels of security as a selling point to consumers. The ability of cloud providers to dynamically reallocate their vast resources can be used as a defensive measure. Which will make them more resilient to Denial of service attacks, for example when attackers flood a server with connection requests, filling its connection queue and causing it to time out, thereby preventing it from accepting other genuine requests (Pfeffer & Pfeffer, 2007).

The elasticity of cloud computing can be a benefit, in 2012 a Dutch website giving emergency advice was overloaded, when a local radio station directed people there for information. The large computing resources available in a cloud-computing model could have prevented this (ENISA, 2012).
Cloud computing is more resilient to power cuts and natural disasters. Data centres have backup generators for such situations however their fuel supplies will only last for a limited time. Cloud computing models have a vast amount of resources and make use of multiple data centres, an outage at one data centre will therefore only have a limited impact (ENISA, 2012).

Case studies such as the study by Khajeh-Hosseini et al (2010) have shown that migrating services to the cloud can be considerably cheaper as well as potentially eliminating support related problems. They do however highlight that there are significant risks that need to be considered.

In contrast to the failures in cloud computing there have also been some success stories. After the earthquake in Japan the resilience of cloud computing meant that organisations were able to take advantage of their infrastructure to get their services up and running as well as providing support for the emergency services (ENISA, 2012).

VII. DISCUSSION

The previous sections have highlighted a wide range of risks and threats as well as benefits and solutions to some of the problems. For example the work completed by ENISA (2009b) has shown that cloud providers are in a good position to be able to offer higher levels of security on a more cost effective basis than an SME would normally be able to provide. In contrast to this, the examples mentioned earlier and high profile cases in the media. Have shown that cloud service providers are a more likely target for cyber attacks.

The decision whether to invest in cloud computing for SMEs is a complex one, they need to analyse how the risks and advantages will affect them. Kourik (2011) suggests that one way to do this would be to use risk assessments. Government and industry groups have produced various guidelines and frameworks that can be used by SME’s to examine the cloud-computing environment enabling them to make an informed decision.

New services such as Cloud Compare (2013) launched in February 2013 and currently only available in Ireland offers to help SME’s assess whether cloud computing is suitable for them, as well helping them through the whole process.

Kourik (2011) has identified seven different models that can be used together to form a detailed study that an SME can conduct, in order for them gain a good level of understanding and thoroughly examine the impact on their organisation (table 1). The first four models consist of the open-group taxonomy which will make a good starting point as it defines a lot of the key concepts. The CSA-Top threatens to cloud computing then discusses some significant threats. The NIST-Guidelines on Security and privacy in public cloud computing give broad guidelines on a variety of areas, as well discussing significant barriers. Finally the ENISA – Information Assurance Framework provides a concise guide to evaluate the different cloud service providers.

<table>
<thead>
<tr>
<th>Order</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open-group taxonomy</td>
</tr>
<tr>
<td>2</td>
<td>CSA-Top threats to cloud computing</td>
</tr>
<tr>
<td>3</td>
<td>NIST-Guidelines on Security and privacy in public cloud computing</td>
</tr>
<tr>
<td>4</td>
<td>ENISA – Information Assurance Framework</td>
</tr>
<tr>
<td>5</td>
<td>CSA - Security Guidance for Critical Areas of Focus in Cloud Computing V2.1</td>
</tr>
<tr>
<td>6</td>
<td>ENISA-Cloud Computing: Benefits, Risks, and Recommendations for Information Security</td>
</tr>
<tr>
<td>7</td>
<td>CSA-Domain 12 Guidance for Identity and Access Management (IAM) V2.1</td>
</tr>
</tbody>
</table>

Table 1. Assessments for SME’s to complete

After studying the first four models, an SME should have a good idea whether cloud computing will be of benefit to them, if they are still interested at this point then it would be wise to look at the final three models suggested by Kourik (2011). The first of these CSA - Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 which can be used to assess whether or not the SME is ready to start using specific areas of cloud computing. The ENISA-Cloud Computing: Benefits, Risks, and Recommendations for Information Security study can be used to further analyse the different risks and uses a chart to measure the impact. Finally the CSA-Domain 12 Guidance for Identity and Access Management (IAM) V2.1 model can be used to focus on specific areas and identify key points that an SME will need to discuss with cloud service providers.

Completing this process should give SME’s a clear understanding of the different concepts of cloud computing, as well as how the varying risk and potential advantages are likely to impact on their organisation. It will also help enable them to test their readiness and prepare them for negotiations with a cloud service provider. However it is also important to note that the cloud environment is constantly changing, developing and new studies are being carried out. SME’s should also take this into account and look for additional resources and information that can help them to make the right decision. As discussed by Sultan (2011) it is a decision based on trade off, the risk of occasionally losing service, against the potential benefits such as cost savings. Assessing the impact the potential risk could have on an SME’s customers.

VIII. CONCLUSION

Cloud computing is a complex area and from the perspective of an SME there are a variety of concerns that need to be considered and analysed. For them to be able to make an informed decision, on whether or not cloud computing is the right choice for their organisation and whether they should put their trust in a cloud service provider. Cloud computing can offer many advantages and benefits that will make it seem very appealing, these advantages need to be weighed against the different risks and threats that cloud computing poses. By taking all of this into account and conducting their own research, an SME will be able to decide on the best route for their organisation. The method suggested by Kourik (2011) represents a good way of achieving this. However the main point is that it is vital that SME’s conduct thorough research and analyse the impact cloud computing will have on their organisation before deciding to invest in cloud computing.
REFERENCES


<table>
<thead>
<tr>
<th>Author Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ademujimi, Adedeji</td>
<td>7</td>
</tr>
<tr>
<td>Anderson, Jermaine</td>
<td>11</td>
</tr>
<tr>
<td>Arthur, Joe</td>
<td>15</td>
</tr>
<tr>
<td>Bell, Michael</td>
<td>19</td>
</tr>
<tr>
<td>Benson, Andrew P</td>
<td>23</td>
</tr>
<tr>
<td>Brevett, Adrian</td>
<td>27</td>
</tr>
<tr>
<td>Gladyn, Cal</td>
<td>31</td>
</tr>
<tr>
<td>Hall, David</td>
<td>35</td>
</tr>
<tr>
<td>Hanify, James</td>
<td>39</td>
</tr>
<tr>
<td>Harrison, Jack</td>
<td>43</td>
</tr>
<tr>
<td>Howden, Chris</td>
<td>47</td>
</tr>
<tr>
<td>Ikott, Mfon-obong Edwin</td>
<td>51</td>
</tr>
<tr>
<td>Jones, Daniel</td>
<td>55</td>
</tr>
<tr>
<td>Kestle, Rebecca</td>
<td>59</td>
</tr>
<tr>
<td>Maclean, Robert N L</td>
<td>63</td>
</tr>
<tr>
<td>Maisey, Jon</td>
<td>67</td>
</tr>
<tr>
<td>Mander, Liam</td>
<td>71</td>
</tr>
<tr>
<td>Mlotshwa, Natsavi</td>
<td>75</td>
</tr>
<tr>
<td>Moore, Robert</td>
<td>79</td>
</tr>
<tr>
<td>Mott, Greg</td>
<td>83</td>
</tr>
<tr>
<td>Orzeszek, Max</td>
<td>87</td>
</tr>
<tr>
<td>Page, Luka</td>
<td>91</td>
</tr>
<tr>
<td>Pell, Luke C</td>
<td>95</td>
</tr>
<tr>
<td>Presland, Luke</td>
<td>99</td>
</tr>
<tr>
<td>Reid, Iayesha</td>
<td>103</td>
</tr>
</tbody>
</table>