Good research paper about cyber security

Business, Company

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Information System Security

Information System Security

Introduction

The information of an organization is protected using a security programme of an information system. The main purpose of an information system security is protection of company information through minimization of the risks of losing integrity, confidentiality, and accessibility of the company information to levels that are acceptable (Ginovsky, 2014). There are two major elements involve in an information security structure that is good and acceptable; analysis of risk and management of risks. In the phase of analyzing risks, the information system security protocol involves taking of an inventory of all information systems of a firm. For every system, the value it holds to the firm is determined and the level to which the firm is exposed to any kind of risk resulting from the system is determined. On the other hand, management of risks incorporates selection of the controls as well as

the security methods that minimize the firm's exposure to risks at a level that is acceptable (Spears &Barki2010). For efficient and effective results, a good information system security should involve reflective common sense and efficient systems. The management of risks must be carried out within a structure of security that is computerized to information system security protocols, have administrative personnel and carry out physical measures of security. Management of risks is therefore an issue to be handled by senior management in a firm. The firm has to establish a balance between the information values to the firm. On the other hand, the cost of administrative, personnel and technological safety measures have to be established too. The safety measures implemented in a firm must be less costly than the potential damages that may be caused through the risks of losing integrity, confidentiality, and accessibility of the company information (Spears &Barki2010). Due to the potential risks that information of a company pose to the welfare of the firm, this paper will carry a research on cyber attacks on the financial services and banks industry.

The internet has changed how the world thinks and operates. Its growth and expansion as well as the continued use in everyday life have presented the biggest technological and social changes in the 20th and the 21st centuries (Spears &Barki2010). It bears a lot of advantages to the world in the manner by which it drives expansion and growth of economies, reduces the many barriers to trade and commerce, and enables individuals from all over the globe to co-operate and communicate in a society-like social setting (Computer Weekly, 2011). The internet has also helped in voicing concerns from those that are unheard and hold governments and authorities to

account. For the developing nations, the internet has a huge responsibility in ensuring and supporting developments that are sustainable (Cyber-security, 2013). Nevertheless, the increased reliance on cyberspace has brought about new risks. These potential new risks involve the systems of information and major company and personal data that the world so much depends on. Damage or compromise of these information and data could be catastrophic. Even as costs of technology fall, this only means that accessibility to the internet will only become cheaper and affordable to all. Even as the internet brings more opportunities to the world, the threats presented are huge and imminent. The current trends in open markets and societies have made the world more vulnerable (Computer Weekly, 2011). Cyber security is threatened by individuals who have an aim of damaging and compromising critical systems and data (Cyber-security, 2013). This is especially so where the financial service markets are involved (Computer Weekly, 2011).

Cyber Attacks

Cyber attacks on institutions that offer financial services have over the last few years become more frequent, extensively spread and more sophisticated as days go by. Even though major financial services carry out extensive campaigns denying the attacks, this topic has continued to create more headlines everyday (McFarlin, 2011). The most affected financial service rendering institutions include regional and community banks, money transmitters, 3rd party providers of financial services like payment processors and credit cards as well as credit unions. The number of attempts that have been put in trying to get into these systems is unbelievably high.

This increased breadth and the frequency of the cyber attacks may be connected to several factors. Seeking intelligence and intellectual properties is the main reason why unfriendly nations breach a company's system. The cyber hackers have a purpose to make statements of a political nature by disrupting systems (McFarlin, 2011). However, cyber gangs, organized groups of criminals, and other identifiable groups of criminals carry out the disruption of systems for monetary benefits. These include stealing of funds through taking over financial accounts, ATM heists and other sophisticated mechanisms that all aim at breaching a system of information. The barriers of entry to the field of cyber crime have dropped due to the decrease in the cost of highly developed technology. This phenomenon has made it simpler and less costly for a criminal of any kind to find out new methods of perpetrating cyber attacks and fraud. Further, an expanding black market for the fraudulent data only serves to offer incentive to the cyber criminals to carry on with their illicit trade.

Cyber Space

A cyberspace is a domain of interaction that consists of digital systems and networks that are used to modify, communicate and store information. An example of a cyber space is the internet; however there are other systems of information that supports businesses, services and the infrastructure. The supply of water and electricity as well as connectivity to the financial services is already underpinned to the digital systems and networks (Ginovsky, 2014). All over the world, the digital systems and networks have replaced the tedious queues in banks and other financial offering physical institutions. In the present, people conduct all manners of payments through

the internet. Online banking is the new trend as people pay for goods and make purchases online. The option presents a chance to save money and time. Additionally, the option of conducting business online has been safe until the recent cyber attacks. Hackers have perfected the art of breaching into financial statements, interjecting purchases and stealing identities of innocent people in a bid to have monetary gains. Seeing why the growth and expansion of cyberspace has been dramatic is easy. The internet has transformed businesses, making it more effective and efficient to run or do business with someone online. The internet continues to open up markets. This in turn allows commerce to occur at reduced costs and enables people to carry out businesses as on the move. Cyber space has continued to promote new thinking, models of businesses that are innovative and fresh sources of expansion, development and growth. Through online conduct of businesses, it is now easier to provide cheaper, better and convenient services to a client.

Conclusion

As seen above, the internet has changed how the world thinks and operates. Its growth and expansion as well as the continued use in everyday life have presented the biggest technological and social changes in the 20th and the 21st centuries (Spears &Barki2010). It bears a lot of advantages to the world in the manner by which it drives expansion and growth of economies, reduces the many barriers to trade and commerce, and enables individuals from all over the globe to co-operate and communicate in a society-like social setting. However, this growth has also brought about threats to the information security systems of businesses and firms. The information of an

organization is protected using a security programme of an information system. Any firm must safeguard its data from potential criminals and threats of its well-being. The main purpose of an information system security is protection of company information through minimization of the risks of losing integrity, confidentiality, and accessibility of the company information to levels that are acceptable. As online banking and conduct of business over the internet expands steadily daily, almost every financial institution is now offering services of banking online to the large base of retail customers (Ginovsky, 2014). Cyber criminals are also expanding in the safe way. Every day, there are new reports of frauds that involve the internet and especially where financial institutions are concerned. In order to stop these trends, the information system securities of every company must be improved through the coordination of the risk assessment phase and the risk management phase. This will ensure that the company covers all possible loopholes in a certain aspect to prevent loss of data and crucial information.

References

Cybersecurity - An IT Issue or Compliance Issue?. (2013). Information Management Journal,
47(6), 19.

Financial sector completes cyber attack simulation exercise. (2011). Computer Weekly, 3.

Available at http://web. b. ebscohost. com/ehost/pdfviewer/pdfviewer? sid= 22eebc6d-fdda-42d7-874d-d5d89397dd45%40sessionmgr198&vid= 2&hid= 112

Ginovsky, J. (2014). UNDER ATTACK. ABA Banking Journal, 106(4), 30-45.

McFarlin, M. (2011). Cyber-attacks draw scrutiny. Futures: News, Analysis & Strategies For

Futures, Options & Derivatives Traders, 40(3), 10.

Spears, J. L., &Barki, H. (2010). USER PARTICIPATION IN INFORMATION SYSTEMS

SECURITY RISK MANAGEMENT. MIS Quarterly, 34(3), 503-A5.