THE IMPENDING DANGER OF CYBER CRIMES IN SME

By Shivani Mayaker &
Prachi Ajit Puro

Abstract

SME (Small and medium enterprises) contribute effectively to domestic production, earn significantly through exports and is one of the leading contributor to the GDP of their countries. The last decade has witnessed exponential growth of the information technology and this IT has enabled businesses, irrespective of their size and nature of growth to create specific niche for themselves in the market.

While internet has occupied a major part of our life, it has also brought in array of associated evils, innovative risks and threats namely, spam, bad- ware, viruses, phishing etc. which threaten the trust, confidence security in the internet.

The paper expounds on the different aspects of security, need and importance of security, the tools which are required for effective fight against cybercrimes.

Keywords

Security, Information, Secrecy, Encryption, Protect, Safe, SMEs, Success, Hacking, Challenge, DDos attacks, Innovation, Sabotage, Insider threats, Cryptography, Firewalls

Introduction

Since the very inception of internet, it experiencing a rapid growth stage. Organizations irrespective of their size, invested heavily with the intention of creating their very own presence in the global network. Such rapid growth observed in the internet, has impacted every aspect of a modern life – starting from the manner in which we communicate, conduct our businesses, achieve the goals etc. The last decade has witnessed exponential growth of the information technology and this IT has enabled businesses, irrespective of their size and nature of growth to create specific niche for themselves in the market. IT has triggered the establishment of a large number of small and medium enterprises in different nations of the globe.

However like everything this also has a flipside. While internet has occupied a major part of our life, it has also brought in array of associated evils, innovative risks and threats namely, spam, bad- ware, viruses, phishing etc. which threaten the trust, confidence security in the internet (Siponen & Oinas-Kukkonen, 2007). Hence, cybercrimes has made the presence of information security mandatory.

The facts

Take a look at of the most alarming facts when it comes to cyber security.

1. The most expensive computer virus of all time known as My Doom cost an estimated £31 billion in financial damages.
2. Around 600,000 Facebook accounts are compromised every single day!
3. 68% of funds that were lost in cyber-attacks were deemed unrecoverable.
4. It takes on average 170 days to detect a malicious or criminal cyber-attack.

Research Objectives

The research objectives of this research are as follows;

1. Conducting a thorough assessment of the awareness of the small and medium enterprises regarding the information security system and determining the different benefits of the SMEs in the process of implementation of such information security aspects in their businesses
2. Identification of the different barriers and the challenges which the small and medium enterprises experience during the process of implementation of such information security system in their businesses

Industry Overview

The small and the medium sized enterprises are an important constituent of the global economy. These enterprises are specifically characterized and due to these characteristics, their approach to security of information will be different from the ones developed for the larger organizations (Chang et al., 2012). The similar approaches would not be feasible. For such implementation, a number of specific challenges are in existence which should be critically removed. With an immense popularity of cyber technology and a growing adaption of such by the small and medium enterprises, ascertaining their information security becomes a crucial aspect of the industry for its growth and sustenance.

For example with the start of the planned economy and the different conducive policies adopted by the Indian Government, the nation saw a splurge of establishment of SMEs from 1951 to 1991 (Jahanshahi et al., 2011). These SMEs now contribute effectively to domestic production, earn significantly through exports, has operational flexibility, contributes towards defence production etc.

The scale and cost of a security breach to these businesses has nearly doubled since 2013, however, with the average cost for the worst incident reaching between £63,000 and £115,000 – a figure which doesn’t take into account the unquantifiable goodwill lost through reputational damage or business closure.

The bigger picture is more worrying. A recent report from McAfee and the Centre for Strategic and International Studies (CSIS) on the effects of cybercrime on the economy of technology and IP driven economies such as the UK, shows that it is particularly damaging to wealth and job creation. In the UK alone, the total cost of cybercrime to the economy was £6.8bn (0.47%) of GDP meanwhile, statistics from the US show that 60% of small companies are unable to sustain their business within six months of a cybercrime attack.

What is Security?

Security is a concept can be defined as the state of being free from different danger and depicts a specific protection against its relevant adversaries, elements which can instil harm intentionally or maybe otherwise. For an organization to operate successfully, it is critical that it achieves a multi layered security in its operations. Such security is in the form of physical security, which is protection of its assets and physical items; personnel security whereby employees and other individuals accessing the organization are protected; operations security which depicts the protection of the operation of organizational activities; security of the communications which is protection of the technology, media and tools of communication; network security and lastly information security (Herath & Herath, 2008). Information security is the concept by which the information assets of the organization are protected and its confidentiality, availability and integrity are thoroughly secured whether such information is stored, is in the process or is already past transmission. Information security thus mentioned is achieved by the application of training, awareness, policies, education and technology (Zafar, 2012).

Benefits of Information Security

The present global economy is characterized by ever changing and increasing risks of the enterprise, online trading, collaboration between organizations, etc, and in such a scenario it has become an imperative for companies to treat information security as an enabler of business (Khansa & Liginlal, 2009). With advancements in technology, and innovations undertaken in this field, it has become possible for the companies to now consist mechanisms by which the business transactions are secured by improving the information and infrastructure associated. However, in spite of such, companies are often found to be struggling to match the different regulatory requirements, conduct risk management etc. due to the insufficient understanding about the importance of information security in organizational settings. While some companies still view such information security as an expense element, it has been witnessed by organizations and scholars alike, that an effectively management system of information security helps companies in achieving its strategic business goals, and improves the efficiency of the business and helps in realizing a greater alignment of the business operations with that of the strategic business objectives (Cremonini & Nizovtsev, 2009).

Organizations of today, should critically understand the benefits associated with information security and the importance of such. Of the major benefits associated with an information security system is that, such a system helps in keeping the vital and prioritized information out of the wrong hands, where such information can be used against the information owner (Grossman, 2013). The information security system helps the companies in maintaining its top secret information regarding the market and its own strategic plans, and keeps such out of the competitors' access and thereby can operate in the market in an efficient fashion. The information security system helps in protecting the valuable information of the users both in the process and during the storage. Information security also enables the companies to acquire and protect valuable information regarding the market and the consumers and also promote the brand image of the company (Qing et al., 2011). This can be particularly true for financial institutions and financial companies, online retailers etc. Financial institutions namely, banks are concerned with top security information regarding the consumers and users. Consumers at all times prefer those financial institutions, which can provide them with complete data security and transaction security, so that their assets are kept safe from external intrusions. Similarly, for online retail companies, where consumers need to provide them with important top security banking detail to make payment, must install high information security systems, as such would ensure the users that their information would be protected from hackers and other external threats. Hence, companies having in place strong and well established information security systems help in generating preference amongst the perceptions of its consumers and thereby can also ensure a higher customer preference and improved profitability (Il-Horn et al., 2007).

Information security practices besides having immense importance in large organizations, have also found imminent usage and importance amongst the small and medium enterprises too (Spears & Barki, 2010). For the purpose of this dissertation, the importance of information security in SMEs has been highlighted in the later sections.

Challenges of Information Security

Acquiring information, disseminating it and utilizing it innovatively has established itself as the key success factor for leading organizations. Though this serves as the key objective of nearly every organization, conducting such in an effortless fashion requires the protection of such valuable knowledge and information from the host of inadvertent incidents, malicious intentions, hacking attacks, natural disasters etc. To protect the information from such requires a robust framework of information security.

In this section, the different challenges associated with the formation and maintenance of the information security is highlighted. As per the security professionals, the type of changes in the information security strategies of attack has undertaken drastic changes (Ahmed et al., 2012). The APTs or the advanced persistent attacks have been more mobile and common, with significant threats presented to the wireless securities. The vectors gained importance and their public visibility enhanced. The DDos attacks also were observed to gain more prevalence. In such a backdrop, as per these experts a number of the challenges pertaining to the industry can be highlighted.

At the wake of the present political situation globally, there is a need to protect the data from such politically generated threats or financially motivated ones. Hence this serves as a critical challenge to protect such important information in order to drive innovation and efficiently manage businesses. Along with this, as there has been an increased occurrence of the Ddos or the Distributed Denial of Service attacks, the professionals are of the opinion that in the future there would be the prevalence of this kind in a higher emergence (Coles-Kemp, 2009).

With the popularity and prevalence of ecommerce and online shopping, it is now required by the consumers to share their passwords and bank details online, which in the absence of an effective security system has the higher chance of getting copied and used elsewhere (Fabian & Gunther, 2009). It becomes a critical challenge for these companies to put in place stronger and difficult to break passwords in their systems which makes the hacking a difficult task. Along with such, sabotage of the computers and their network can serve as a critical challenge, and this has the characteristic of being perverse, as it effectively combines the software tools with that of the social engineering in order to create a very complex attack profile of the multi vector kind (Hui et al., 2012).

As per scholars of this field, an importance challenge of the organizations in achieving a strong information security system is the insider threat (Puhakainen & Siponen, 2010). Often attacks of the information system of an organization can originate from a dis-satisfied employee, who know the nuances of the information security system of the organization and can inadvertently inject malicious software through different openings of web interconnections or the removable media etc. Hence, such network security violation can also originate in an organization from the insiders.

Probably the biggest challenge which plagues the professionals of information security is the belief and assumption that the internet is a secured infrastructure of critical network. As the internet is formed from a set of diverse networks, the main challenge is in treating such networks as being critical to the organizational operations. One needs to establish policies and frameworks by which these network platforms are segregated as per their importance on the criticality of the business to manage risks in a more conscious and effective manner (Puhakainen & Siponen, 2010).

Reduction of Insider Fraud, Theft and Data Leakage

External attacks garner most of the headlines, but insider threats can be even more damaging – compromising invaluable intellectual property and even jeopardizing national security. We’re all familiar with WikiLeaks, but few organizations have come to grips with the true risk of insider threats. Would you know if an employee was sending key product plans to a competitor, anonymously publishing confidential information, or accessing financial information that could be used for insider trading? With Security Intelligence solutions, organizations can identify and mitigate those inside threats and many more, by detecting the following:

1. Unauthorized application access or usage
2. Data loss such as sensitive data being transmitted to unauthorized destinations

3. VoIP toll fraud
4. Application configuration issues such as privileged access exceptions
5. Application performance issues such as loss of service or over-usage

A multi-billion-dollar branded consumer products firm recently used its SI solution to detect an attempted data exfiltration by a trusted employee for financial gain. The company's executives suspected its intellectual property was being leaked but couldn't identify the source. When they applied flow-based network activity monitoring to the situation, they were able to quickly track down the data leakage and stop the employee. With application content capture (via Deep Packet Inspection or DPI), they could even drill down and view the specific emails sent by the employee through his personal email account to the third party. This prevented the problem from snowballing and potentially causing millions of dollars in damage to the firm.

Present tools of Information Security

Information security uses the tool of cryptography to run its basic applications. Cryptography is the process of translating the information in a specific format which makes it difficult and often unusable by others who are not the authorized users. The process is known as encryption, and the information thus encrypted can again be translated back to its original readable format by an authorized individual, by providing a specific key called cryptographic key, and such a process is known as the decryption. Cryptography is the main and basic application tool which is used in the process of information security and protects such information from the external and accidental threats from outside, especially during the process of information transit, both in the electrical and the physical formats (Chen et al., 2012). Cryptography is also utilized by organizations in attempting to protect the stored information. Cryptography helps information security by providing a set of such cryptography-based tools and applications. Such include, the message digests, the non-repudiation the encrypted communications of the network, the digital signatures, the host of authentication methods etc. Every communication mode, be in wireless or wired can be encrypted with the help of such tools which promotes and enhances the security aspect greatly.

However, when such a tool is not utilized effectively and efficiently can lead to creation of a number of such security problems. These cryptography based applications and solutions must be installed as per the industry accepted and prevalent norms and solutions, which have been subjected to an immense measure of the peer reviews by the experts of such information security (Gupta & Zhdanov, 2012). The structure and the length and the breadth of the key of encryption play as critical role in elevating the protection of such information security. A key which can be easily anticipated and can be copied cannot fully protect the information. The encryption and decryption keys must be protected thoroughly and treated as critically important information themselves. These keys must be hid and have very limited and restricted access through authorization. However, these keys must also be stored in a manner which can be accessed when the urgency arrives.

Apart from these tools as mentioned above, firewalls and intrusion detectors are very effective in protecting the information and at least making the personnel responsible for protecting such aware of the impending attacks. The present trends of the information protection and security give rise to challenges which can be countered by the security tools and minor adjustments of them (Bulgurcu et al., 2010). The firewalls which are built and installed with the intention of keeping out a type of messages are effective on most of the occasions. Intrusion detectors are specific tools which determine and identify activities which are not normal in the networking communication and undertake actions depending on the nature of the out of ordinary activities – namely, alert the administrators, reduce the privileges provided to the users. Though firewalls and such intrusion detectors are not completely full-proof to protect the data and confidential information, these are improving as we write on a regular basis against the host of threats (Guo et al., 2011).

Case Study A

Company A is a facilities management company belonging to the small and medium enterprise industry of India. The 110 employee company does not have in place any information security system, and as per the executives operating in this company, the actual need for such does not exist, as the company does not deal directly with online transactions, and consumer purchase. The company operates with corporate clients, and till a recent time managed every operational detail in paper. With computerization of the documents, the company has established in place basic software through which it conducts business. The management of the company after investing a considerable amount in computerizing its operations were not keen on spending more to establish a data protection system, and as per them, such system is more required for financial businesses, retailers who have online purchase options installed.

The company officials have received training to work under the new computerized system and though they have comprehensive idea about the importance of information security, they initially felt they did not have a need for such information security. But a simple incident has recently got them all thinking. The company had established an interactive official website, through which prospective clients can contact the management regarding orders. As the company is now intending to move into internationalization, and open up branches abroad, it had maintained its website on a regular basis. However, due to a recent hacking attack, the website's data were all hijacked, and the prospective customers could not access the website. Though the problem had been identified and solved by the website maintenance team, this incident had critically impacted the brand image of the company to the market and has led the management thinking regarding the impact and far reaching implications of the information security system.

Now the company intends to install a sense of basic security system in their organization, but due to resource shortage, and lack of proper vision, it is becoming a leading challenge to them.

Case Study B

Company B is a retail company having its origin as a small and medium enterprise. The company has in place dedicated team of professionals for its website maintenance, governance of the online transactions, and information security. As the company is armed with sales and distribution of products through the internet, and they gain direct access into the consumers' data, as a mode of ethical management and effective operations, the company has installed strong and functional modes of information security. As per the respondents hailing from this company, the organization's management understands the importance of knowledge and information and has hence, installed strong modes of protection system by which information thefts, cybercrimes, and forgeries can be stopped.

The respondents cited a small example as the benefits of having such an information security system. As the company has an online e-business arm, often customers purchase the products from the company's website. As the company sells ethnic traditional products, often these are in much demand amongst consumers from foreign countries. The strong word of mouth and referrals of this company, from its existing local customers through their social circles and social media, has helped the company draw attractive consumers from abroad. The strong information security system helps in generating trust and a loyalty aspect of the brand name, which has made the international customers also do business efficiently and without any apprehension.

As per the respondents of the company B, information security and the focus for protection of the in house and stakeholders' information has helped the company in establishing a strong and effective brand image in the consumers mind as well as the industry. It is now considered to be a benchmark, for companies operating in the similar field. Company B implements a host of cutting edge security tools to protect its cyber presence and information. These are both firewalls, both host based as well as network based, a number of scrubbing tools, TCP view as well as active ports, tools to detect of spyware and removal of such along with virus detection tools namely, antivirus with stinger utility services to identify and remove the viruses. As per the respondents of Company B, information security will gain even more importance in the future with the landslide entrance of corporate in the field of ecommerce.

Conclusion

Ensuring that the networks are protected from both external and internal attacks by installing high security firewalls. Anti-virus software that addresses the SME Company's specific needs should be implemented on all systems – off the shelf virus software will not meet many business' IT security requirements. Encrypt all the data, particularly if there is a high use of personal devices and homeworking within your business and protect with robust passwords. For precaution is always better than cure.

References

- Zafar, H., 2012. Human Resource Information Systems - Information Security Concerns for Organizations. Human Resource Management Review, 23(1), pp.105-13.
- Yildirim, Y., Gizem, A., Serpil, A. & Nuran, B., 2011. Factors Influencing Information Security Management in Small and Medium Sized Enterprises - A Case Study from Turkey. International Journal of Information Management, 31(4), pp.360-65.
- Vuorinen, J. & Tetri, P., 2012. The Order Machine - The Ontology of Information Security. Journal of the Association for Information Systems, 13(9), pp.p695-713.
- Ahmed, A., Hadgliss, J. & Ruighaver, B., 2012. Incident Response Teams - Challenges in Supporting the Organizational Security Function. In Computers & Security, 31(5), pp.643-52.
- Askari, F., 2012. IT Security as a Service for SMEs. Support Biz, 28 December.
- Bulgurcu, B., Cavusoglu, H. & Izak, B., 2010. Information Security Policy Compliance: An Empirical Study of Rationality Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), pp.523-57.
- Bin Muhaya, F., 2012. On the Development of Comprehensive Information Security Policies for Organizations. International Journal of Academic Research, 4(1), pp.16-22.
- Chang, S.-I., Yen, C., Ng, S.-P. & Chang, W.-T., 2012. An Analysis of IT/IS Outsourcing Provider Selection for Small and Medium Sized enterprises in Taiwan. Securing Electronic Business Processes, 49(5), pp.199-209.
- Chen, P.-Y., Kataria, G. & Krishnan, R., 2011. Correlated Failures, Diversification and Information Security Risk Management. MIS Quarterly, 35(2), pp.397-403.

- Chen, Y., Ramamurthy, K. & Wen, K.-W., 2012. Organizations' Information Security Policy Compliance; Stick or Carrot Approach? Journal of Management Information Systems, 29(3), pp.157-88.

- Chopra, A. & Saini, S., 2011. Top Security Threats for Indian SMEs. PC Quest, 1 August.

- Coles-Kemp, L., 2009. Information Security Management - An Entangled Research Challenge. Information Security Management - an Entangled Research Challenge, 14(4), pp.181-85.

- Cragg, P., Caldeira, M. & Ward, J., 2011. Organizational Information Systems Competences in Small and Medium Sized Enterprises. Information and Management, 48(8), pp.353-63.

- Cremonini, M. & Nizovtsev, D., 2009. Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers. Journal of Management Information Systems, 26(3), pp.241-74.

- ET Bureau, 2013. How Internet and IT empower Indian SMEs. Times of India, 13 Feburary.

- Daud, N., Mamud, I. & Aziz, S., 2011. Customer's Perception Towards Information Security in Internet Banking System in Malaysia. Journal of Applied Sciences Research, 7(9), pp.101-12.

- Dojkovski, S., Lichtenstein, S. & Warren, M., 2007. Fostering Information Security Culture in Small and Medium Size Enterprises - An interpretive Study in Australia. Proceedings of the 15th European Conference on Information Systems , pp.1560-71.

- Fabian, B. & Gunther, O., 2009. Security Challenges of the EPC Global Network. Communications of the ACM, 52(7), pp.121-25.

- Guo, H., Yuan, Y., Archer, P. & Cornelly, E., 2011. Understanding Non Malicious Security Violations in the Workplace - a Composite Behavior Model. Journal of Management Information Systems, 28(2), pp.203-36.

- Gupta, A. & Zhdanov, D., 2012. Growth and Sustainability of Managed Security Services Network: An Economic Perspective. MIS Quarterly, 36(4), pp.1-29.

- Gupta, A. & Hammond, R., 2005. Information Systems Security Issues and Decisions for Small Businesses. Information Management & Computer Security, 13(4), pp.297-310.

- Gerber, M. & von Solms, R., 2005. Management of Risk in the information age. Computers and Security, 24(1), pp.16-30.

- Grossman, J., 2013. The Web Wont Be Safe or Secure Until We Break It. Communications of the ACM, 56(1), pp.68-72.

- Il-Horn, H., Kai-Lung, H., Sang-Yong, L. & Png, L., 2007. Overcoming Online Information Privacy Concerns - An Information Processing Theory Approach. Journal of Management Information Systems, 24(2), pp.13-42.

- Hui, K.-L., Hui, W. & Yue, W., 2012. Information Security Outsourcing with System Interdependency and Mandatory Security Requirements. Journal of Management Information Systems, 29(3), pp.117-56.

- Herath, H. & Herath, T., 2008. Investments in Information Security - A Real Options Perspective with Bayesian Postaudit. Journal of Management Information Systems, 25(3), pp.337-75.

- Hongziang, X., Rondeau, P. & Mahenthiran, S., 2011. The Challenge of Implementing an ERP System in a Small and Medium Enterprise - a Teaching Case of ERP Project Management. Journal of Information Systems Education, 22(4), pp.291-96.

- Jayaram, M., 2013. Lack of Internet Infra Stymies Indian SMEs. The Hindu, 17 April.

- Jahanshahi, A. et al., 2011. The Relationship between Government Policy and the Growth of Entrepreneurship in the Micro, Small and Medium Enterprises in India. Journal of Technology Management & Innovation, 6(1), pp.66-76.

- Johnston, C. & Hale, R., 2009. Improved Security through Information Security Governance. Communications of the ACM, 52(1), pp.126-29.
- Kumar, L., Park, S. & Subramaniam, C., 2008. Understanding the Value of Countermeasure Portfolios in Information Systems Security. Journal of Management Information Systems, 25(2), pp.241-79.
- Khansa, L. & Liginlal, D., 2009. Quantifying the Benefits of Investing in Information Security. Communications of the ACM, 52(11), pp.113-17.
- Kohli, R., Devaraj, S. & Ow, T., 2012. Does Information Technology Investment Influence a Firm's Market Value? A Case of Non Publicly Traded Healthcare Firms. MIS Quarterly, 36(4), pp.1145-63.
- Labodi, C. & Michelberger, P., 2010. Necessity or Challenge - Information Security for Small and Medium Enterprises. Annals of the University of Petrosani Economics, 10(3), pp.207-16.
- Qing, H., Zhengchuan, X., Tamara, D. & Hong, L., 2011. Does Deterrance Work in Reducing Information Security Policy Abuse by Employees? Communications of the ACM, 54(6), pp.54-60.
- Puhakainen, P. & Siponen, M., 2010. Improving Employees Compliance Through Information Systems Security Training - an Action Research Study. MIS Quarterly, 34(3), pp.767-84.
- Siponen, T. & Oinas-Kukkonen, 2007. A Review of Information Security Issues and Respective Research Contributions. ACM Sigmis Database, 38(1), pp.60-80.
- Spears, L. & Barki, H., 2010. User Participation in Information Systems Security Risk Management. MIS Quarterly, 34(3), pp.502-55.
- https://securityintelligence.com/what-are-the-benefits-of-security-intelligence/
- https://superfast-it.com/need-cyber-security/
- http://www.growthbusiness.co.uk/the-importance-of-cyber-security-for-smes-2485736/

Bio

Shivani Mayekar, M.A Philosophy. She is a gold medalist in M.A. She has presented many research papers both at national and International level. Currently she is an Assistant Professor at D.G.Ruparel College in BMS department.

Prachi Puro, M.COM In Accountancy. She has completed her Masters in Accountancy. She is also having a Corporate experience with love and passion towards teaching.Currently she is an Assistant Professor at D.G.Ruparel College in BMS department.