INFORMATION SECURITY MANAGEMENT FOR SMALL AND MEDIUM SIZE ENTERPRISES

Jawad Abbas
Institute of Business and Management (IB&M), University of Engineering and Technology, Lahore, Pakistan
Correspondence: jawad.abbas@gmail.com
+92-321-4722314
Hassan Khawar Mahmood
Institute of Business & Finance, Ali Block Garden Town, Lahore, Pakistan
imskhawar@gmail.com
+92-300-9689743
Fawad Hussain
National University of Science & Technology (NUST), Islamabad, Pakistan
hussain.fawad@gmail.com
+92-321-9232923

ABSTRACT: *Information Security Management(ISM) is a crucial factor for all organizations under current scenario of business globalization. Companies are making efforts to make best use of technology including e-business. Organizations have made huge amount of information available on their database, but has made it vulnerable to all types of attacks by numerous hackers in the form of spams, malwares etc. Therefore, organizations have to keep their database protected with latest security measures to ensure privacy and confidentiality of data. Semi-structured interviews of 19 managers at various levels out of 48 requested SMEs' were done to probe into their views about confidentiality, integrity, availability and non-repudiations which are the major objectives of information security. It is found that industrialist generally believe in security of information and its importance to organization but mostly are only reactive in administrating information security. The result is that they react in unprepared manner which finally results in loss of business as well as reputation. The findings provide strong baseline for SME organizations to review their existing operating style and improve it by applying adequate security* measures.

Key Words: Information Security, SME, Technology, Performance, Confidentiality, Pakistan

1- INTRODUCTION

History stands witness to human endeavors which aimed at making this world a better place for living. Efforts have always been made to bring the world closer, and with the advent of internet technology this dream of mankind turned to reality. Since, its arrival internet has grown and is still growing substantially. It paved the way for businesses to look beyond their range and attract customers from all around the world. Considerable investments have been made by both large and small-to-medium sized enterprises (SME) to make the maximum use of the internet in reaching out and getting the attention of the global network. However, there exists no real utopia in this world; with the revolutionary effects of internet over business there came the risks and threats to information security.

As the businesses have opted to utilize the internet based platform in attempting to reach out to the world, huge amount of information is created (and in some cases converted) into digital format. This digital information travels across the globe through "plethora of interconnected networks" [1], which is prone to cyber-attacks such as phishing, spams, malware, viruses, trojans and other forms of cyber terrorism. In the present day economically competitive business scenario, information is a valuable asset, and businesses may suffer huge blows economically as well as to their repute if they fail to safeguard it. This con of internet, has not only resulted in loss of information, but has also shaken the trust and confidence of the internet user over technology.

Business needs keep on changing with the passage of time and so does the requirement of the information security measures. The security policies of the SMEs should be able to adapt to change and align it with the changing business objectives. In order to ensure that the business is driving forward with the correct security policies in place, security infrastructure transformation shall take place according to the enterprise's strategic business objectives.

Locked houses, safes in banks, security guards, and barb wired facilities etc. all aim at providing physical security to assets. Information security is analogous to all such security measures however it is responsible for providing data security in digital domain. There are four objectives of Information Security:

i. Confidentiality – Information shall be transferred to people on a need to know basis i.e. to keep the information from reaching to unauthorized people.

ii. Integrity – Information stored in the computers should be kept guarded from being corrupted or contaminated.

iii. Availability – Ensuring the availability of the data to the authorized people at right time. Both confidentiality and availability ensures data integrity.

iv. Non-repudiation – Ability to prove the authenticity and integrity of the data

In order to have a successful business an organization needs to assess and analyze their organizational information security requirement, make a clear strategy in dealing with the information security issues, link their business objectives with the evolving needs of information security and communicate the importance of information security and the implementation of the plan. SMEs with IT infrastructure aim at challenging the larger businesses owing to their flexibility, efficiency and customized solutions. The stakeholders of any business demand assurance towards information security as loss of it would cause a lot of damage. Having a well-defined

Information Security policies, plan and strategies would outshine an SME amongst its competitor and would become an obvious choice for the customers to approach. Therefore, information security will not only assist the SMEs in having a better and secure IT structure it will yield in customer satisfaction and a good reputation which in turn will attract more business.

Information security cannot be realized without embracing it in the day-to-day working scenario. The link between the enterprise's goals and information security is crucial and SMEs shall align its security policies with the evolving needs. Apparently tough decisions need to be made in terms of financial effects, but as mentioned earlier in this paper to have an edge against competitors addressing the evolving needs of information security and linking it with the business objectives would yield good reputation, contented customer and greater business opportunities.

Network security concerns faced by large enterprises or SMEs are of the same nature. Larger enterprises having greater budget in hand can opt out of numerous authentication products while SMEs with limited budget and personnel have to cope their way through simple Microsoft passwords or other such security protocols. Biometric security devices tend to provide access to the authorized user only through scanning their finger prints or eye-pupil. It eliminates the need of punching user passwords every time an authorized personnel needs to access the requisite information, providing user convenience and enhancing productivity.

2- Literature Review

The Information Technology (IT) infrastructure has brought great opportunities towards SMEs improving their productivity and enabling them to compete against their larger enterprise adversaries. However this bounty came with IT related risks and threats which if not addressed will cause serious blows towards the business and demands for "sophisticated management" [2].

SMEs generally invest fewer resources and possess less expertise in establishing and maintaining IT security policies and strategies. This deficiency of information security awareness and lack of proper information security policies by SMEs make them an easy target for the cyber-terrorists. Despite the challenges and threats faced by the SMEs, their employment and reliance on information technology is rapidly increasing, and the business goals are directly being associated with the utilization of information technology. Symantec Global SMB Survey of 2013 reports that owing to the weaker security measures of the small-to-medium sized businesses almost 31 percent (which is thrice the frequency from 2012) of targeted attacks are focused on them [2]. An information security breach survey undertaken in April 2012 by PricewaterhouseCoopers (PwC) LLP in United Kingdom revealed that 76 percent of small business faced security breaches which on average cost £ 15,000 - £ 30,000 in the worst of security breach [3].

According to [4], Information Security incorporates four levels within SMEs i.e. Organizational Level – It includes decision making processes, defining security strategies, and corporate security culture and risk management. Workflow Level is the integration of standardized security workflow methodologies and development of secure business processes. Information Level involves access and control to facilities and information storage sites / computers, data authorizations etc. The last but the least is Infrastructure Level which states that at this level business network is being protected through hardware and software protections like firewalls, anti-malware, anti-virus etc.

SMEs (or any organization for that matter) would suffer substantial damage towards their reputation as they fall prey to information security attack. Incident response management enables the SMEs to identify and discover if it is under attack, absence of such management would render the SMEs oblivious towards such an attack, not to mention the harm which it would cause. Subsequently, disaster recovery strategy would assist the SMEs to "contain the damage, eradicate the attacker's presence and recover in a secure fashion" [5]. Owing to the importance associated with Incident Response Management and Disaster Recovery for an organization, SANS Institute of Internet Security United States has placed it in their list of 20 Critical Security Controls. Furthermore, National Institute of Standards and Technology (NIST) United States have provided detailed guidelines for the planning and implementation of these plans in their NIST Special Publication 800-61.

A clear and effective incident response management and disaster recovery plan would comprise of six phases namely preparation, identification, containment, eradication, recovery and lessons learned [6]. SMEs should be prepared to handle threats to their business critical information via their IT structure by having the right people and tools placed in the enterprise. A prepared SME would be able to identify any breach in its information security and would first contain the damage being caused by the breach followed by its complete eradication. Subsequently, recovery process would be initiated which would close strengthen the weak links. Subsequently lessons learned from the breach would assist in fighting similar breaches in future.

Moreover, this Incident Response Management and Disaster Recovery plan shall also include careful planning to handle occurrences other than cyber intrusion like fire, storm, power surges etc. Survey results suggest that 55 percent of SMEs think that they would lose 40 percent of the information stored in their computer in case of calamity like fire [7]. Considering the fact that in the present day scenario all the data of an enterprise is mainly stored on computer drives, losing 40 percent of the data will be enough to put you out of business for a considerable time.

3- Methodology and Description of Concept

To work on current issue, detail interviews were conducted to know different issues associated with information security. Semi-structured interviews help to keep interviewee on relevant area and share his opinion more appropriately. Total 48 different SMEs' owners were contacted via letter and reminders out of which 19 people respond. However, none of them permitted to record the interview and allowed to make notes. Industrialists were requested to give their views on different aspects of information security. All the interviews were written and then coded into short words to make categories as identified by [8]. Most of SME outsource their

IT structure and contract with external IT service provider. Majority of professional believe that importance of systems is based on its impact on customer instead of organizations. Interviewees believe that organization's good will cannot be protected if customers see any problem & leakage of information.

SMEs has to be a pawn in the global technology and table revolution to keep abreast with the growing technology as it promises to yield your business more productivity and customer satisfaction. However, the swift employment of this technology by SMEs, have resulted in many SMEs who are unaware of the challenges that came as part and parcel with this technology. It is important for the SMEs to realize the management of mobile devices, services and mobile application security as a mandatory phase of adopting and adapting to new technology.

"Cyber forensics is the science of acquiring, retrieving, preserving and presenting data that has been processed electronically and stored on computer media." [9] Cyber forensic incident response shall assist the enterprise in determining how the breach occurred? What systems were compromised? What information might have lost its confidentiality? Which data would have lost its integrity? How to remediate the incident?

SMEs shall be equipped with required tools and techniques to identify, track and contain advanced adversaries and remediate incidents. Although, SMEs do not find much of cyber forensics employed in their enterprises however, they do possess incident response plan. Cyber forensics however is also essential to make sure that similar breach does not take place again and vulnerabilities are removed.

SMEs shall first determine their needs of the mobile devices before blindly following the revolutionized business world. Their employment of the mobile devices shall be justified with the enterprise needs. Just like any other inventory, mobile devices shall also be managed through Inventory Management System (IMS) to keep an eye on the expenses and assets. Clear and detailed policies shall be established concerning the usage of mobile devices to tackle enterprise needs, usage of personal mobile devices, apps that are allowed to be installed on the mobile devices and access of social media sites through mobile devices. Company data should have security protocols and only allow a limited number of approved mobile devices to have access to it through remote networks. Employees shall be well trained and educated regarding the policies and internal controls shall ensure effective implementation of these policies.

Biometric security devices ensure to meet all the four objectives of information security (confidentiality, integrity, availability and non-repudiation) provided its employment concept is well planned. An ill planned and mismanaged biometric security device would prove disadvantageous for the business.

3.1- Security Training and Education

The PwC's information security breach survey referred earlier in the document revealed that 75 percent of small business which the security policy was poorly understood had employee related information security breaches. It also revealed that 54 percent of the small businesses lacked employee education program pertaining to information security management. [3]

An SME with a refine and well-defined security policy which is not communicated and understood by the employees is prone to information security threats just as badly as an SME that is lacking such security policy. SMEs should not only formulate their Information Security policies and procedures but should also publicize them in their employees. Training programs to ensure understanding and compliance to these policies shall be conducted and employees should be made to sign a non-disclosure of information agreement and agreement of understanding and adherence to the enterprise security policy.

3.2- Defending Against Internet-based Attacks

Internet has made it possible for the SME to reach out to the entire world and has provided them a place to compete against the business giants on the same footings. However, the danger of internet based attacks is also same for both the enterprise structures. Defense against internet based attacks require proper education of employees against targeted attacks, SMEs are more prone to these attacks as cybercriminals are aware that SMEs possess lesser security technology as compared to large enterprises. Proper security technology like firewalls, anti-virus, anti-malware, phishing filters shall be installed by the SMEs to combat the internet based attacks.

A comprehensive security plan addressing all the possible vulnerabilities and internet based attack shall be drafted to address the internet based threats. This plan shall be modified and adapted to the changes in internet scenarios instead of modifying it on periodic basis.

3.3- Industrial Espionage and Business Intelligence Gathering

"Industrial espionage refers to covert methods and techniques employed to gather competitive information that is not publicly available. It aims at giving a competitive edge to its employer in terms of time saving, economic advantage, providing a lead in the market, anticipate the rivals business strategy, and forehand knowledge of the new products and emerging technologies by the rival business companies.

Business Intelligence refers to the techniques and processes employed for gathering, storing, and analyzing competitive information to enable enterprises to make better decisions for their business in order to improve upon its competitiveness. Keeping in view the Industrial Espionage definition provided in the preceding paragraph, it can be inferred that there is a very fine line demarcating the differences between the two information gathering activities. The main difference between the two data collection methods is that business intelligence is considered legal whereas industrial espionage is considered to violate law constitutes of illegitimate data collection practices.

Individuals and corporate firms both take actions to safeguard themselves against the industrial espionage. They undertake risk assessments and chalk out the policies governing the data handling and information security. Confidentiality agreements are prepared to bind the employees legally to refrain from sharing trade secrets or working on similar projects after changing their jobs. Copyrights and patents are

also made to safeguard the right to using a new technology." [10]

4- Issues in Information Security Management

Organizations must understand the score of information security. An appropriate and comprehensive information security management system and professionals plays vital role in organization's approach to supervising liability for privacy and security hazards. To lower the liability and risks from electronic and physical threats IS practitioners must understand the current legal environment thoroughly and stay updated and watch new and emerging issues. By educating the management and work force of an organization on their permissible and ethical responsibility and the appropriate use of information technology and information security, security experts can help organization to keep it focus on its primary objectives.

Numerous types of issues are faced in information security management e.g. ethical issues, legal issues, governance issues etc.

4.1 Ethical Issues in Information Security Management

Information Security Management works with a fine line between ethical and unethical behavior towards the access of information available to the Information Security Manager or IT Personnel. SMEs generally do not have a large team of IT personnel, it usually comprise of a single person who acts as the IT manager or a small team of two to three personnel. These IT professionals are trained and educated in information security and possess technical knowledge and skills to counter threats faced by a business. At the same time they also possess the ability to monitor the communication that is taking place in the organization as well as outside of the organization.

The ethical issues involving Information Security Management involves privacy of information to a great deal.

- Enterprises are responsible to safeguard the privacy of their clients, not only on ethical grounds but also because losing such information will cause bad reputation and may even bring the enterprise to courts.
- Information Security personnel has the access to the emails of their networks and they should demarcate the fine line needed to ensure the right and wrong in reading the employees' email. And whether or not the employees are aware of the fact that there correspondence can be monitored.
- Is it ethical to monitor the websites being visited by network users?
- Is it ethical to install key loggers and screen capture programs to monitor the employees. Are the employees informed of such monitoring?
- Is it ethical to browse through the files that are stored on employee's workstations without their consent?

4.2- Governance Issues in Information Security Management

Information Security Management can only be made effective and efficient if top-level management of SMEs implement the security policy in true letter and spirit and assists the IT personnel in enforcing the same over all the employees. If the top level management fails to follow the same and leave the implementation over the IT personnel then the enterprise will not take the Information Security seriously.

Good governance of Information Security Management requires security to be made an integral part of the enterprise culture. This governance of Information Security Management shall come from the top-down while being promoted by the IT personnel. An organizational culture embracing the Information Security policy from top to down is destined to have improved efficiencies.

4.3- Personnel Issues in Information Security

The present day economic scenario witness high degree of turnover in employment, which can expose the SMEs to damaging losses of information. These risks are great when it the employee turnover is taking place in the IT personnel or some other key position of the SME. Enterprises should take great care in hiring personnel; comprehensive interviews shall be conducted to analyze the candidate's integrity along with his / her professional abilities. An investigation with the previous employer and references would reflect upon the true character of the candidate.

The employees when hired shall be made to sign as obligatory practice a non-disclosure agreement to abide by the company's policy of protecting the trade secrets while on job and thereafter. At the same time when an employee decides to quit the job the same agreement shall be reviewed. Enterprises shall also have a defined document which shall comprehensively list down all the characteristics of the trade secrets which an employee is bound to keep secret from the adversaries, failure to which may result in legal actions. In addition, enterprises in attempt to reduce the personnel issues related with Information Security shall give better working environment to the employees so that they do not think about the turnover.

4.4- Physical Security Issues in Information Security

Physical security issues in information security refer to the physical lock and key of the storage devices. Moreover, the key place where all the confidential information is stored shall also be allowed to visit only by authorized personnel. Surveillance cameras, security guards, biometrics, RFID and likes shall be employed to ensure the physical security. A log book for the visitors shall also be maintained and they should not be allowed to enter the places where there is a risk of business information being leaked.

A closed check on the inventory shall also be kept by monitoring which devices are leaving the premises and which are coming in. All the systems shall be blocked from the usage of USBs and other such storage media devices so that the risk of information theft is minimized. Document shredders shall be employed to ensure that all the documents are being shredded and destroyed before being dumped, to ensure that business critical information cannot be inferred from these documents.

5- Recommendations for Improvement

Assessment of risk is an ongoing process and needs continuous improvement. SMEs' should continually review their operations and procedures to make sure they are able to safeguard their crucial information. In this regard, adequate security guidelines should be designed and followed by the institution to control the risks. Following are some of security

techniques which should be adopted according to level of organizations;

1) Access to critical information should only be given to authorized and concern person and restrict it from sharing with unauthorized persons i.e. dissemination of information strictly on "need to know basis"
2) Dual authorization system (all information endorsed by at least two people) should be implemented along with segregation of duties for access to critical information.
3) Adopt and implement a system which ensures that customer and organization's information system is consistent with information security program.
4) Important customer and organization information stored in networks and systems to which unauthorized or irrelevant individual has access should be encrypted.
5) Evaluating the adequacy of policies, procedures, information systems and other arrangements to control any potential risks.
6) Implementation of an appropriate system to detect actual and attempted attacks on information systems.
7) Quick response program which identifies actions to be taken on identification of suspicious access to information systems.
8) Maintaining backup to keep the duplicate record of information.

CONCLUSION

In current era, privacy and security has become one of the most important areas in the field of information technology. Organizations are spending millions of rupees to ensure the privacy of their data. "Prevention is better than cure", SMEs shall not wait till an Information Security breach has taken place. Information security breach in any organization can has devastating effects. The loss of product information or any knowledge pertaining to organization client, strategic business plans etc. can result on loss of existing customers as well as potential ones. It can even cause operational breakdown and affecting profitability.

It has been found that most of SMEs' are reactive in administrating information security despite knowing that security of information is crucial for smooth operations of their business. In the event of breach of information security, most of companies react in unprepared manner which result in loss of business as well as reputation.

Efforts shall be made by the SMEs to identify their business critical information, define policies in handling the data, incident response plans, disaster management plans, employing appropriate software and hardware to protect the data. With all the proper methods and techniques as discussed in this paper and others which are important and are not listed SME may surpass all the barriers and be more productive and attain better reputation and business.

REFERENCES

1. TAWILEH, A.; HILTON, J.; MCINTOSH, S. Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. **ISSE/SECURE 2007 Securing Electronic Business Processes**, p. 331-339, 2007.
2. SYMANTEC. **Global SMB IT Confidence Index**. California. 2013.
3. PWC. **Information Security Breaches Survey**. [S.l.]. 2012.
4. JI-YEU PARK, R. J. R. C.-H. H. S.-S. Y. T.-H. K. IT Security Strategies for SME's. **Iternational Journal of Software Engineering and Its Applications**, p. 91-98, 2008.
5. SANS. The Critical Security Control. **SANS Organization Web site**, 2009. Disponivel em: <http://www.sans.org/critical-security-controls/>. Acesso em: 17 October 2013.
6. POKLADNIK, M. **An Incident Handling Process for Small and Medium Business**. [S.l.]. 2007.
7. WHITEHOUSE, L. **Small Business Data Protection Basics: What Small Business Owners Need to Know to Ensure Business Continuity**. Massachusetts. 2009.
8. ABBAS, J. et al. Impact of Technology on Performance of Employees (A Case Study of Allied Bank). **World Applied Sciences Journal**, p. 271-276, 2014.
9. ZUCKER, S. **Cyber Forensics**. [S.l.]: [s.n.], 2010.
10. ALJERI, A. A. Workshop 8, Perth, 15 October 2013.