Global Scientific JOURNALS
GSJ: Volume 10, Issue 7, July 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

INFORMATION SECURITY RISK ASSOCIATED WITH SMALL AND MEDIUM SIZE ENTERPRISES

Tani Schmidt Paul Ngo

MSc. Information Systems and Networking
Head of IT for Azire Cooperative Credit Union Limited (AZICCUL)
IT Consultant in Information Management Systems
Email: tanischmidt@yahoo.com Tel: +237673651790

Abstract

In today's rapid changing technological evolution, small and medium-sized enterprises (SMEs) are exposed to serious information security risks as they depend more and more on technology to run their businesses. This is because SMEs have not considered information security risk as an essential factor before diving into the use of technology. SMEs can be exposed to three categories of information security risk, which include risk associated with human errors, malicious intent to cause harm and risk associated with technology and natural disasters. Apart from this, SMEs are also facing some information security challenges. This study seeks to provide some recommendations to SMEs and to the government on how SMEs can operate securely despite the information security risks and challenges they face.

Keywords: Information Security, SMEs

I. GENERAL OVERVIEW OF SMES AND INFORMATION SECURITY

With the rapid evolution of technology in the world, many small and medium-sized enterprises are grapping the opportunities offered by technology to increase their market shares as they provide flexible services to their customers in response to their changing needs. (Aksoy, 2017) (Povolná, 2019) However, the majority of SMEs haven't taken appropriate measures to ensure their reliance on technology doesn't make them vulnerable to technology-related attacks that can lead to the destruction of their business with one of such measures been information security. (Wilson, 2018). Information security does not only involve securing information from unauthorized access. It is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information. This information can be in either a hard copy or a soft copy. (Sajikumar, 2020)

Information here includes anything from viewing basic login details of a social media profile, data on mobile phones, to complex issues like unauthorized access to company data, theft of company data, and disruption of company services for malicious reasons. (Prescott, 2016). Information security is not something that started today, it is written that during the First World War, Multi-tier Classification Systems were developed for the keeping of mind sensitivity of information and at the beginning of the Second World War, the formal alignment of the classification system was created. (Loveridge, 2016) According to **ISO/IEC 27001:2013**, information security is built on the following three core fundamental principles, also commonly known as C.I.A. – Confidentiality, Integrity, and Availability.

i. **Information Confidentiality:** It is the non-disclosure of information to unauthorized users, entities, and processes. Information is said to be compromised or non-confidential if any unauthorized access has access to this information.

ii. **Information Integrity:** means maintaining accuracy. This means insuring that data cannot be edited in an unauthorized way.

iii. **Information Availability**: means information must be available when needed. For example, if one needs to access information about a particular system at a given time, both the information system and the needed information need to be available for that process. One of the most popular attacks that can hamper the availability of information is the denial of service attack.

Apart from the core principle that governs information security cited above, the following are some additional concepts that need to be taken into consideration to make this concept complete.

iv. **Non repudiation**: It is the principle of authentication information between the sender and the receiver such that the sender of information is provided with proof that information arrives at the right receiver the same way it was sent. While the receiver is also provided with proof of the sender's identity, so neither can later deny having processed the information.

v. **Authenticity**: It is a principle that verifies that users are who they say they are and that each input arriving at destination is from a trusted source. This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission.

vi. **Accountability:** It **is** the act of ensuring that the actions of an entity should be traced uniquely to that entity.

Information security is frequently thought as something for larger enterprises, but recent studies show that there is a growing concern about information security in SMEs. (Bada, 2019) Information security has been a concern for large enterprises for years in that all the security models and guidelines laid down by international organizations for standardization, like ISO/IEC27001: 2015 have been focused more on large companies, which in most cases are difficult to apply to SMEs due to the size and capital of SMEs. (Merroun, 2022) Although different countries and governments have written regulations in place for the implementation of information security in companies, the majority of SMEs still neglect the risk to information security by putting forth the argument that their business is too small to allocate a budget for information security management, forgetting that they constitute part of the present day global financial activity. (Kwateng, 2022)

II. SOME FUNDAMENTAL CHALLENGES OF INFORMATION SECURITY IN SMES.

i. **The Challenges of Technology**: SMEs want to explore the advantages offered by the evolution of technology to expand their business as they increase their market share. However, they lack the capital to invest in these technologies, such as buying licensed software, up-to-date licensed equipment, and a budget to hire qualified personnel to manage these technologies. SMEs generally use unlicensed software that is generally exposed to computer viruses and cyber-attacks. (Baruah, 2018)

ii. **Absence of an Information Security Management Framework:** While SMEs lack access to adequate technologies, these technology challenges limits the preliminary efforts of SMEs to manage information security risks.

iii. **Non-Implementation of the ISO 27001:2015 standard:** It is often difficult for SMEs to comprehensively implement the prescriptive requirements of ISO/IEC 27001:2015. This is frequently due to SMEs' inability to create a framework for implementing necessary guidelines such as risk management policies and procedures. This is also due to the fact that the ISO/IEC 27001:2015 requirements were designed for large companies and not SMEs. (Ahler, 2021)

iv. **Untrained resources and non-maintenance of software tools**: The majority of SMEs lack the financial means to train and equip their critical manpower with the required technologies to fight threats to information security. This is normally supposed to be a continuing process as new threats are discovered every day.

III. THE MOST COMMON IT THREAT TO SMEs

The adoption of the digital age by SMEs comes with an information security risk associated with it, to which SMEs need to pay great attention as they contribute more and more to the economy of the nation. The most common risks associated with SMEs are grouped into three main categories as follows.

i. **Risk associated with human errors**: Everyone can make errors, no matter how well trained and motivated they are. However, in the workplace, the consequences of such human failure can be severe. Human error accounts for 52% of the root causes of information loss, according to a report by (Maurer, 2015) In a study conducted in January 2015 concerning 700 business executives and technology professionals at U.S. companies, on the effects of human error in information security, 42% of the respondents cited "end user failure to follow policies and procedures," another 42% cited "general carelessness," 31% named "failure to get up to speed on new threats," 29 percent named "lack of expertise with websites/applications," and 26 percent cited "IT staff failure to follow policies and procedures." The above statistics thus show that information security training programs need to be incorporated into the companies' budgets. (Maurer, 2015)

ii. **Risk associated with malicious intend to cause harm:** Malicious threats are threats resulting from a deliberate attempt to do harm to a system. This can either be from an internal persona or an external person in a company. Malware can be in the form of a computer virus, a worm, a Trojan horse, or spyware. (Jumaeva, 2021) These malicious programs aim to steal, encrypt, and delete sensitive data; alter or hijack core computing functions; and monitor end users' computer activities. According to a report conducted on the rate of malware infection in a company in the year 2020, 61% of organizations experienced malware activity that spread from one employee to another (Mahboubi, 2020).

iii. **Risk associated with technology failure and natural disasters:** Natural disasters such as fire, cyclones, and floods also present risks to IT systems and data infrastructure. Damage to buildings and computer hardware can result in the loss or corruption of customer records and transactions. Such a disaster can cause SMEs to completely go on operational, leading to an abrupt termination of the contracts of their employees, thereby increasing the rate of unemployment. (Cvetković, 2017) As businesses rely more and more on technology to operate, a failure in technology can have a detrimental impact on the ability of the business to function as the downtime of the business increases, causing customers to cause long waiting periods. SMEs in which technology plays a crucial role in their operations need to understand the reasons behind technology failures and take appropriate measures to mitigate this. (Yi, 2016) Uncovering the general causes of technology failure can go a long way toward ensuring the systems remain stable and provide the performance they need. The following are five main reasons why technology fails

- **Poor Implementation:** A poorly implemented technical solution has the potential to cause complex repercussions affecting an organization's IT infrastructure.

- **Poor Maintenance:** A lack of regular IT maintenance on applications and services that run the business could not only lead to poor system performance but could ultimately result in the entire infrastructure failing.

- **Overutilization of IT resources:** Over utilization of the IT team and IT equipment more than their functioning capacity can cause machines to break down and staff to break out, thus slowing down productivity.

- **Complexity:** With the fast growing evolution of technology, businesses need to allocate a budget for continuing education to ensure the technology they use is not obsolete and that they have an IT staff that understands the management of these technologies.

- **Misalignment:** Misalignment generally occurs when the implemented technology is not aligned with the solution to a specific business requirement. When this occurs, the IT system will fail to deliver.

IV. IT SECURITY RECOMMENDATIONS TO BE ADOPTED

a. Recommendations for SMEs

i. Evaluate the company's IT situation objectively and regularly

It is important to constantly do a review of the general status of the IT systems and data security on a regular basis so as to have a complete knowledge of the IT infrastructure. It will also help to have a good knowledge of the security strengths and weaknesses, which will help the IT department to focus more on those areas. If the business does not have the manpower or the skills required, they should try to seek external review assistance that has the required skills.

ii. Continued education of staff

It is very important for businesses to set aside a budget for staff training. Staffs need to be aware of the recent threats that affect other businesses and ways in which to mitigate these challenges. As previously mentioned above, continued training of staff will help mitigate risk due to human errors, which is the cause of more than 60% of all IT security breaches.

iii. Provision of a personnel task manual:

Since the majority of SMEs often have a single staff tasked with handling multiple rules and duties, a personnel manual written by a professional should be enforced; this is a manual that takes into consideration all the IT security risks, outlines simple and clear operational procedures on how a staff member should operate. This will be a great way to mitigate any IT security risk as the staff will be charged with following the procedures outlined in this manual to carry out their job.

iv. Work together to create a risk aware culture

It is critical to educate and involve staff on key aspects of IT security on a regular basis, with a focus on data security beginning with how data is collected, processed, and transmitted. It is also important for SMEs to have laid down rules on how their essential operational assets can be disposed of, such as company computer hard disks, RAMs, backup systems and even office documents for disposal. This is because some of these may contain some sensitive data that may help any potential attacker to have clear knowledge of the operations taking place in the company.

v. Use of a proven recipe for success

Learning and applying best information security practices that have been discovered and developed over time is a tried and tested recipe for success in this field. ISO/IEC 27001:2015 is the best world standard recipe for IT security. It specifies the requirements and best practices for information security management controls for SMEs.

b. Recommendation to the Governments

i. The role of the government

Since SMEs are becoming more and more important contributors to the economy of the country, the government needs to put in place regulations and control measures to ensure that SMEs don’t fall victim to potential IT security risks. This can be done by providing them with financial incentives, free training, sensitization policies, procedures for operations, and so on. The government should also have an effective IT regulatory body that can go around different SMEs in the country to see that the security policies and procedures put in place are being followed by the different organs involved.

REFERENCES

Ahler, E. (2021). The ISO/IEC 27001 standard provides a systematic approach to information security. *Ekaterina Ahler*, 37.

Ahler, E. (2021). The ISO/IEC 27001 standard provides a systematic approach to information security management. *Upravlenie kachestvom (Quality management)*, 36-38.

Ahler, E. (2021). The ISO/IEC 27001 standard provides a systematic approach to information security management. *Upravlenie kachestvom (Quality management)*, 36-38.

Aksoy, H. (2017). How do innovation culture, marketing innovation and product innovation affect the market performance of small and medium-sized enterprises (SMEs). *Technology in Society*, 133-141.

Bada, M. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information &amp; Computer Security*, 393-410.

Baruah, N. (2018). Software Project Management and SMEs of India. *International Journal of Advanced Research in Computer Science and Software Engineering*, 11.

Cvetković, V. (2017). Perception of risks from natural disasters caused by floods. *Vojno delo*, 160-175.

Jumaeva, H. M. (2021). The system of protection of students from internal threats. *current research journaL of pedagogics*, 122-126.

Kwateng, K. O. (2022). Enterprise risk management and information technology security in the financial sector. *Information &amp; Computer Security*, 422-451.

Loveridge, S. (2016). Another Great War?: New Zealand interpretations of the First World War towards and into the Second World War. *First World War Studies*, 303-325.

Mahboubi, A. (2020). Stochastic Modeling of IoT Botnet Spread: A Short Survey on Mobile Malware Spread Modeling. *IEEE Access*, 228818-228830.

Maurer, B. R. (2015, April 13). *Human Error Cited as Top Cause of Data Breaches*. Retrieved July 24, 2022, from shrm.org: https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/human-error-top-cause-data-breaches.aspx

Merroun, M. E. (2022). Industry 4.0 as an Opportunity to Achieve Environmental Sustainability: The Difference between SMES and Large Companies. *International Journal of Information Technology Convergence and Services*, 1-13.

Milis, K. (2008). Critical analysis of policy measures for the advancement of the level of computerization of SMEs. *Information Technology for Development*, 253-258.

Povolná, L. (2019). Innovation Strategy in Small and Medium Sized Enterprises (SMEs) in the Context of Growth and Recession Indicators. *Journal of Open Innovation: Technology, Market, and Complexity*, 32.

Prescott, M. E. (2016). Big Data: Innovation and Competitive Advantage in an Information Media Analytics Company. *Journal of Innovation Management*, 92-113.

Sajikumar, H. (2020). Security Risk Assessment System for Detection and Prevention Of Unauthorized Access. *International Journal of Multidisciplinary in Cryptology and Information Security*, 11-15.

Wilson, A. (2018). Better Safety Performance Measures Can Lead to Change by Improving Conversations. *Journal of Petroleum Technology*, 76-78.

Yi, Y. (2016). The role of other customers during self-service technology failure. *Service Business*, 695-715.