Strategic Dimensions of Information Security Risk Management

Ayush Gupta

Faculty of Science and Engineering, University of Turku, Finland
Email Id: aygupt@utu.fi

Abstract. Information security is thus a big threat to the survival of enterprises. In all context and forms, it is an imperative to provide adequate safeguards and measures to management the risk arising from flow of information and data. The business models of organizations are highly dependent on flow of information during the business processes. The management of information security has several perspectives. In this paper, the legal, quality and human resource perspectives have been discussed. The Information Security Risk Management Model must balance these perspectives to optimize for best value derived out of it.

Keywords: Information Security, ISRM, Business Model, Data Breach, Cyber Security

_____

I. Introduction

Internet has created a revolution in the business and social structures in in various spheres of life. The data flowing through this medium has disrupted our working and thinking styles and in context of corporations, the business models. The speed of flow of data has broken all barriers with dynamic flows and real time dissemination observed in various environments. However, this has raised issues of data protection from piracy and leakages in various forms, thus requiring a continuous monitoring. In all context and forms, it is an imperative to provide adequate safeguards and measures to management the risk arising from flow of information and data. The information security risks have increased tremendously because of the dependence on information technology. These risks include financial and business risk, model risk, horizon risk and the subject matter of interest in the paper – the information security risk. Information assets are most critical and most vulnerable in any enterprises.

Information Security is described as "the processes and methodologies which are outlined and carried through to protect either by print, electronic or whatever variety of confidential, private

and sensitive information from unauthorized access, use, disruption, destruction or alteration" (SANS, 2019).

Cybersecurity and information security are used interchangeably, but the cyber security is primarily concerned with protection of information held electronically. Thus, information security is a wider concept. In ISO 27000, information security is defined as: "The preservation of confidentiality, integrity, and availability of information" which inherently includes cyber security. Information security risk management defined by Rapid7(2018) "is the process of managing risks associated with the use of information technology. It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets. The end goal of this process is to treat risks in accordance with an organization's overall risk tolerance."

Implementation of Information Security Risk Management (ISRM) requires a "multi-phased approach to achieve its objectives. Since, various stakeholders are involved in the process, the roles and responsibilities of each stakeholders needs to be clearly defined for its success. The stakeholders or owners of ISRM owners are (a) process owners – which are involved directly in implementation and assist the ERM process, and (b) risk owners – includes people involved in risk management for the organization – ERM staff. We find various designation of people associated with ISRM implementation like Chief Information Officer, Enterprise Architect, Chief Acquisition Officer etc.

Knowledge Security Management is a new concept linked to ISRM because of the complexity of business processes. In management of information security, knowledge security is absolutely essential. The knowledge security threats identified by He (2013) include data privacy issues, failure of systems, and malware. The problems to ISRM are poor governance, cloud data leakage, and various inefficiencies (Braun and Essen, 2012).

The cost of information security is huge. The risk in public or government departments are more than any other sector e.g. increase in incidents of breach at Federal Trade Commission (FTC) in 1997 according to Marsh and Marsh (2014). According to Accenture (2019), the amount stolen from data beaches were 27.4 Million USD in 2018 and average cost of cybercrime was $13.0 Million. Table 1 shows the biggest data hacks of 2019.

Table 1 – Biggest Data Hacks of 2019

Name of Enterprise	Business	Number of records hacked
Zynga	Mobile game producer	218 million
Dubsmash	Video messaging app	161.5 million
Capital One	Credit Cards	100 million
Houzz	Home design website	48.9 million
Quest Diagnostics	Lab-testing company	11.9 million

Source: *https://www.cnbc.com/2019/12/17/the-5-biggest-data-hacks-of-2019.html*

Information security breaches, particularly the cybercrimes, about 93% come from three industries that are retail, government and technology and a significant portion is from small industries (Milkovich, 2019). Information security is thus a big threat to the survival of enterprises.

Information security is widely criticized for being interruptive, hindering the business processes, consuming large energy and adds complexity to systems. Information security in organizations being highly complex issue having varied social and technology dimensions (Crossler e*t al.*, 2013) requires considerations from various perspectives and associated dimensions. In the following sections, the legal, quality and HR dimensions of Information Security Risk Management are discussed.

II. Legal Dimensions

Information security from a legal perspective is described in the form of the objectives of law. These objectives either prevent the harm e.g. "protect systems and information against unauthorized access, use, disclosure or transfer, modification or alteration, processing, and accidental loss or destruction" (Smedinghoff,2019) or seek to maintain some ethical or operational standards (like *confidentiality, integrity, and availability* of information) of information security aspects.

Legal definition of information security is direct and indirect in different countries. According to Smedinghoff (2019), the US federal law has defined the term information security as – "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide — (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving

authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information."

Information Technology Act, 2000 of India has defined the terms information and cyber security as follows -

"information‖ includes [data, message, text,] images, sound, voice, codes, computer programmes, software and data bases or micro film or computer-generated micro fiche;"

"cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction".

A thorough understanding of the legal responses to information security threats is absolutely essential to analyze its application of the obligation of enterprise. In addition to a specific law, it is the general duty of every person or enterprises to ensure the information security. Summarization of the various approaches to information security in various legislations globally yields that main objectives of information security are to ensure the confidentially of information, ensure only authorized access to information, authenticity of the information in various contexts and integrity of information assets and infrastructure. Understanding corporate obligations to address data security begins with a high-level understanding of the legal response to security threats.

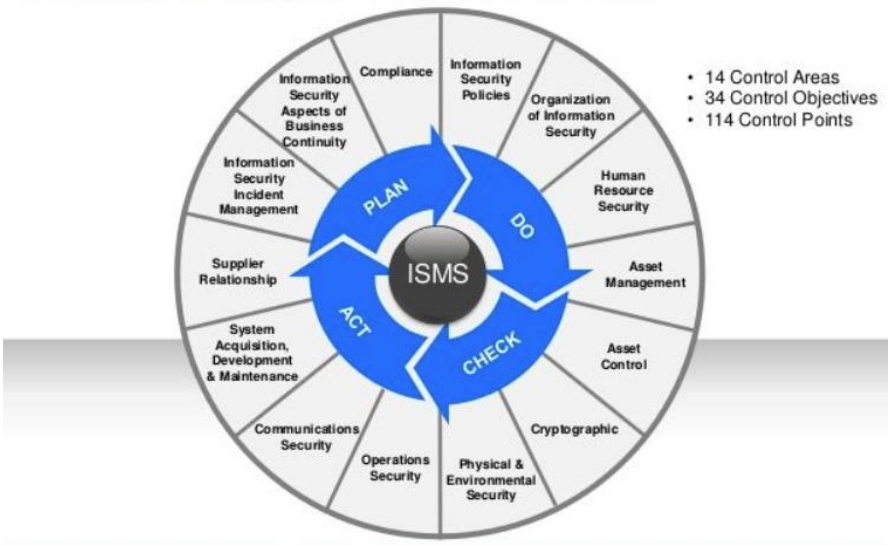
III. Quality Dimensions

Protection of data is required at all levels and for everyone. The task of protection of data is complicated because of perceptual differences in thinking and operations. Moreover, the protection comes at a cost and also the adaptability of technology. All these considerations have accentuated the need for developing a quality standard of information security that can be applied on global basis.

The recent known standard that deals with Information Security Management Systems is ISO 27001:2018. The standard endeavors to protect the Information assets. The need for protection of Information assets include loss reduction, ensuring efficiency of operations in particular and protection of the business model in general. This standard has become a norm in the business arena on a global basis. In addition, we find National Institute of Standards and Technology (NIST) framework for identification and management of information security risks.

Quality assurance approach to Information Security Risk Management is process-based (Figure 1). It determines the style of implementation the process and control areas. In context of ISRM, the quality dimension focuses on the evolution of the best practices for information and data security. The survival of enterprise business model is essential from quality perspective of ISRM. Irrespective of size and nature of enterprises, the ISO 27001 is applicable to all operations given its generic nature.

Figure 1 - ISO 27000 Global Standard on ISRM



Source: https://my-cybersecurity.blog/2018/06/04/risk-management-and-iso-27001-guidance/

The key compliances in quality standards include defining the nature and scope of ISRM, its processes and operational structure. The quality is ensured through concurrent audits.

The mandatory requirements under the standard are based along the principle of "trusted access." The major security hazard that needs to addressed in priority by every organization is the "Encrypted and unmanaged privileged access" is a security risk that no system should face.

Adoption of ISO 27001 is non-mandatory similar to other standards, however, if the standard or similar type norm is not accepted, the conduct and efficiency of business operations are seriously affected. In various studies, it has been established that for specific industrial sectors the standards need to customized. The text of implementation given by Vanderburg (2019) is as follows-

- *"Risk assessment* – a quantitative or qualitative approach to determining the risks to organizational assets. The degree of risk is based on the impact to the asset and the likelihood of occurrence.
- *Security policy* – formal statements defining the organization's security expectations.
- *Asset management* – inventory and classification of information assets.
- *Human resources security* – security aspects for employees joining, moving within or for those leaving an organization.
- *Physical and environmental security* – physical/tangible systems used to protect systems and data such as alarm systems, guards, office layout, locked doors, keypads, cameras, etc.
- *Communications and operations management* – management of technical security controls in systems and networks.
- *Access control* – restriction of access rights to networks, systems, applications, functions and data; maintaining the confidentiality of access credentials and the integrity of access control systems.
- *Information systems acquisition, development and maintenance* – building security into applications when they are designed or purchased.
- *Information security incident management* – planning and responding appropriately to information security breaches.
- *Business continuity management* – protecting, maintaining and recovering business-critical processes and systems when they become unavailable."

Failure Mode Effect and Analysis (FMEA) has been introduced in the US military in 1940s for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service (ASQ, 2018). Being a step-by-step approach to conduct process analysis, it is an effective approach to aid the ISRM process.

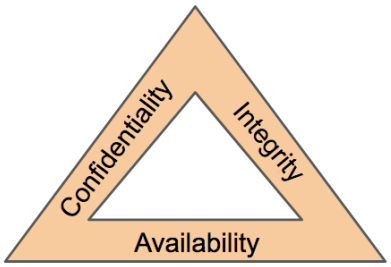
As a matter of further development in the area of ISRM, Pecb (2018) quotes – "ISO/IEC 27005 provides guidelines for the establishment of a systematic approach to Information Security risk management which is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system. This international standard supports ISO/IEC 27001 concepts and is designed to assist an efficient implementation of information security based on a risk management approach."

Quality dimensions of ISRM are often linked to the Quality Management Systems (QMS) in enterprises. The contractual obligations and protection from legal consequences are part of information security. The contracts prima facie does not offer protection, but create implication for controls and measures for concerned parties. QMS arrangements may be part of the covenants of an agreement e.g. a customer requiring confidentiality of his private data. This in turn create implications for information security specialists.

IV. Human Dimensions

The Human Resource dimension to ISRM can be viewed from the perspective of CIA triad (Figure 2) which means Confidentiality-Integrity-Availability of information. Heymsfeld (2018) quotes the CIA triad as "Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need."

Figure 2 - CIA Triad



Source : https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/

In every endeavor to protect the information assets in the, the human element plays a crucial role. McLaughlin *et al.* (2015) has shown that societal moral and ethical responsibilities are crucial concerns for enterprises apart from the visible costs and penalties and brand reputation risk in any information security breach. We observe various failure of ISRM due to poor governance and power conflicts. Poor incentivisation for ISRM significantly affects its success. The motivation, training, communication are buzz words.

The rreinforcement sstrategies for ISRM can be (a) positive – dynamic monitoring, training, linked reward-incentive system or (b) negative – legal consequences, penalties etc. The implementation of ISRM requires interaction, active involvement and dynamic communication to all stakeholders. High-Reliability Organizations introduced by Weick *et al.* (1999) pursue a

state of mindfulness which can ensure integrity and conscience leading to effective ISRM. In many breaches it is seen that financial gains are at the center of the motives for breach, thus human analysis of the involved staff is absolutely essential. In any ISRM implementation, if human assets are an important part of the process, the value conflict must be carefully addressed to achieve perfect goal alignment given the complexity of security environment.

Social engineering serves as a method of identification of information security breaches carried out with or without malicious intention whereby the breaches or crimes occur through a variety of social methods. It is a puzzling area of concerns since new methods and forms of breaches are evolving whose financial and non-financial implications are difficult to evaluate.

V. Conclusion

Information security is a critical concern for enterprises in current times. The business models of organizations are highly dependent on flow of information during the business processes. The costs of *information security breaches* are huge and are potential survival threats. The management of information security has several perspectives. In this paper, the legal, quality and human resource perspectives have been described. The legal recognition to the issue of information security is mow comprehensive in most of the countries of the world, though the terms information security and cyber security have been used interchangeably. Quality standards have developed over time with ISO 27000 series being the widely accepted norm. The ISO standard for ISRM has to be seen in conjunction with ISO 31000:2018 that deals with the principles and operational procedure of how the enterprise manage its risks. Human aspects of ISRM revolve around goal alignment, value conflict minimization and training, motivation and incentivisation for ISRM. The Information Security Risk Management Model must balance these aspects to optimize for best value derived out of it.

References

Accenture (2019), THE COST OF CYBERCRIME available at https://www.accenture.com /_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

ASQ (2018). Failure Mode and Effects Analysis (FMEA). Retrieved from https://asq.org/quality-resources/fmea

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future Directions for Behavioral Information Security Research, Computers & Security, 32, 90-101.

He W.(2013), "A survey of security risks of mobile social media through blog mining and an extensive literature search," *Information Management & Computer Security*, vol. 21, no. 5, 2013, pp. 381–400.

Heymsfeld, R. (2018, August 04). Confidentiality, Integrity and Availability - The CIA Triad. Retrieved from https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/

Marsh Koyame, Rita & Marsh, John. (2014). Data Breaches and Identity Theft: Costs and Responses, IOSR Journal of Economics and Finance (IOSR-JEF). 5. 36-45. 10.6084/m9.figshare.1284635.

McLaughlin, M., Hansen, S., Cram, W. et al. Snowfall and a stolen laptop. *J Info Technol Teach Cases* 5, 102–112 (2015) doi:10.1057/jittc.2015.12

Pecb, P. (2018). ISO/IEC 27005 Information Security Risk Management Trainings. Retrieved 13th March 2019 from https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27005.

R. Braun and W. Esswein(2012), "Corporate Risks in Social Networks–Towards a Risk Management Framework," in Proceedings of the Eighteenth Americas Conference on Information Systems, Seattle, 2012.

Rapid7 (2018). Information Security Risk Management (ISRI). Retrieved from https://www.rapid7.com/fundamentals/information-security-risk-management/

SANS(2019), Information Security Resources. Retrieved from https://www.sans.org/information-security/.../disruption.

Smedinghoff, T. (2019). Information Security Law: The Emerging Standard for Corporate Compliance. Retrieved July 17, 2020, from https://learning.oreilly.com/library/view/information-security-law/9781905356669/ch01.html

Vanderburg, E. (2019, January 16). ISO 27000 Compliance - Overview, History, Benefits, and Certification. Retrieved from https://www.tcdi.com/iso-27000-certification-history-overview/

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. In R. I. Sutton & B. M. Staw (Eds.), *Research in organizational behavior, Vol. 21* (p. 81–123). Elsevier Science/JAI Press.