THE IMPORTANCE OF RISK MANAGEMENT IN INFORMATION SECURITY

EBRU YENIMAN YILDIRIM

Uludag University, Computer Technologies Department, Turkey
E-mail: yeniman@uludag.edu.tr

Abstract- Information is critically important at increasing risk of loss or compromise. The heart of an information risk management program is an ongoing process of risk assessment which involves an understanding of possible risk tolerance, knowledge of likely risks and threats, measured assessments of established controls, and executed plans to address identified vulnerabilities. Information Security Standarts must be implemented in all organizations for the risk management to be applied in all levels. If the risk management is practised well, Information Security will be more effective.

Keywords- Information Security, Risk Management, Information Security Standarts, Information Security Risks, ISO 27001

I. INTRODUCTION

In today's competitive business mediums, every kind of information is always under the threat of many sources. With the continous increase in the use of new technologies for storing, transmitting and accessing information, information becomes more vulnerable to an increasing number and type of threats. So, no matter which form it has or with which ways it is stored or shared, information always needs to be protected by suitable means.

The heart of an cyber risk management program is an ongoing process of risk assessment. This involves an understanding of risk tolerance, knowledge of likely risks and threats, measured assessments of established controls, and executed plans to address identified vulnerabilities. The strategy of information risk management is focused on the preservation of confidentiality, maintenance of data integrity and assurance of the availability of information for authorized users. An effective information risk management program can only be assured through the diligence of every individual who has access to confidential information. Along with personal integrity, diligence is the one critical asset that touches just about every trusted individual in the enterprise. The notion of individual accountability is the model to be followed if information is to be truly secured. The key to proactive protection is the recognition that threat is truly dynamic. It is constantly changing and adapting to our efforts to safeguard vital information assets [1].

II. INFORMATION SECURITY RISKS AND RISK MANAGEMENT

Any work on cyber risk in the organisation must begin with an understanding of the organisation's wider view of business risk, which must necessarily examine the impacts or consequences of unexpected events. These can result in any of the following:

- Financial loss, which can include loss of business or intellectual property.
- Legal and regulatory penalties, which can arise from either a breach of regulatory practice or failing to meet regulatory deadlines.
- Reputational damage, which generally begins with adverse reports in the media.
- Damage to the organisation's operations, which may result in subsequent reputational damage.
- Harm to the organisation's staff or the public-at-large, which again can result from damage to the organisation's operations and reputation.

Although many of these are not based on pure finance, the bottom line is that it is mostly about money, since many of the other types of impact will ultimately result in some form of financial loss, whether directly or indirectly [2].

Today, with the risks and threats having become more sophisticated, there are now two additional foundational tasks:

•Define the organization's ecosystem
•Introduce security awareness training for employee

A comprehensive assessment of the vulnerability to information compromise requires visibility into the root causes of information security risk. To that end, most texts on information security focus on technology when identifying issues requiring remediation. An exclusive focus on technology ignores organizational issues that drive information security risk but are manifest as technology problems. In fact, a virtual avalanche of information is generated by security technology controls. These controls can be effective in identifying tactical issues but the broader risk associated with security data so derived can be difficult to interpret pursuant to identifying systemic security problems. As mentioned previously, the principal sources of information security vulnerabilities in organizations are as follows:

• business practices
• a lack of security governance
• IT implementation
• the physical security of information assets
• user behavior

Business practices are inexorably linked to the organizational culture where the former is a by-product of the latter. In fact, it is not an exaggeration to say that the culture establishes the security posture in any organization, and reflects the outcome of the security–convenience dialectic that is being played out every day.

A lack of security governance is arguably driven by organizational culture as well. A lax approach to developing and enforcing information security policy follows from a culture of permissiveness or where creativity is encouraged on every level. In particular, a lack of well-designed security policies and standards correlates with a proliferation of information security vulnerabilities.

IT implementation is clearly a source of risk factors for information compromise. Poor implementation of technologies used to store, process, and/or transmit confidential information contributes to the overall risk profile of an organization, and must be addressed on both a tactical and a strategic level, but not to the exclusion of other sources of risk.

User behavior is deserving of scrutiny in identifying root causes of information security risk. User behavior in this context includes the history of websites visited, electronic access privileges (eg, Windows user, local administrator, domain administrator), physical access system privileges, history of internal resources accessed, and password complexity.

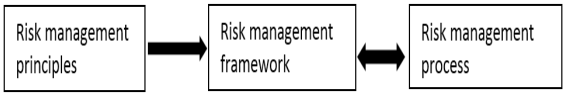


Fig.1. Risk Management Components

Risk management is key to the governance of the organisation and to the protection of its, information assets. If an organisation does not know the risks it faces, it will not be able to implement proper and effective protection. The risk process is as below:

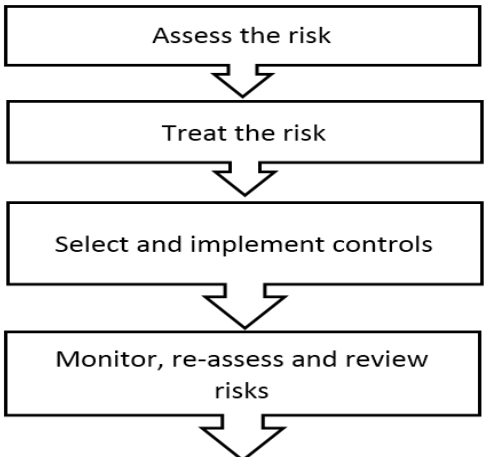


Fig.2. Risk Management Process [3]

In general, comprehensive assessments of information security risk are required to establish a thorough understanding of the risk factors affecting an organization. Furthermore, such assessments must be made with respect to risk-based policies and standards in the absence of useful statistics on incidents. Adopting a process to rigorously assess the risk associated with information security threats is essential to developing a coherent information security risk management strategy [4].

Table1: Risk Management Principles [5]

Key Risk Management Principles…	… Applied to Cyber Risk
1. **Focus on what matters most** Must align to your unique business and risk culture	**Know your critical information assets** Identify critical business assets most vulnerable to cyber attack
2. **Measure and report** Include qualitative statements and quantitative measures	**Make cyber risk more tangible** Clearly define cyber risk and underlying metrics
3. **Comprehensive in nature** Should cover all risk types, current and forward-looking	**Align with existing risk frameworks** Financial, operational, regulatory, customer, reputation, etc.
4. **Allocation of risk appetite** Allocation of appetite to business units and risk types	**Make cyber risk relevant to the business** Link organizational-level risks to individual business units and their information assets
5. **Integrate with business planning** Regulators are increasingly looking for evidence	**Embed risk appetite in investment decisions** Prioritize investment where critical, empower businesses to make informed local decisions

III. INFORMATION SECURITY STANDARTS (ISO 27001)

The ISO 27001 necessitates enterprises to prepare risk management and risk processing plans, duties and responsibilities, business continuity plans, management procedures of emergency state case and to hold the records of them. Enterprises must publish information security policies and make their personnel conscious about information security and threats. As an ongoing process, information security management covers selected control goals, and their assessment. Controls' suitability to their aim and their performance are continuously monitored and this can only be accomplished by the active support of the management and participation of personnel [6] [7].

Information Security Standarts must be implemented in all organizations for the risk management to be applied in all levels. If the risk management is practised well, İnformation security will be more effective. All levels to be managed in organizations are as below:

- At organizational level, it determines responsibilities and guarantees benefits of applying enterprise information security at every level.
- At legal level, it shows to other authorities that the enterprise has complied with all related rules and regulations and completes other standards and principles.
- At enterprise level, it directs the enterprise about information systems, their weaknesses and how they will be protected and therefore safer access is provided to the enterprise information systems.
- At commercial level, business partners, shareholders and customers have increased confidence in the enterprise; thanks to the importance the enterprise gave to information protection, leading to better places in market and increased competitiveness.

- At financial level, as a consequence of identifying security loop holes and taking some measures, costs will decrease.
- At employee level, it increases knowledge of the employee about security subjects and responsibility of himself within the organization and provides him to be made conscious individually.

DISCUSSION

All organizations are exposed to risk, and most organizations do some kind of risk management. However, if we aim to precisely understand the kinds and nature of the risks, and to manage them in a systematic and effective manner, we need a well-defined process for risk management. We moreover need to understand the underlying principles and framework for the risk management process [8].

Given that organizations cannot prevent all incidents, the traditional discipline of security, isolated from a more comprehensive risk-based approach, is not enough to protect against threats. Moreover, improving information risk management is not always about spending more money, and it is also not just about buying the latest risk management technologies and tools. To be effective, risk management programs require effective managerial cognition, judgment, and decision making, each of which are key drivers of successful risk management system dynamics. Systemic factors such as management's perceived risk, desired levels of risk management investment, risk detection capabilities, and trust of personnel dynamically interact and can create feedback loops that either reinforce risk mitigation capabilities, or produce and expose organizations to insider threat vulnerabilities. Reducing such vulnerabilities to the emergence of insider threats involves improving risk information acquisition, risk information management, and targeted training of personnel in judgment and decision making [9]. In general, comprehensive assessments of information security risk are required to establish a thorough understanding of the risk factors affecting an organization. Furthermore, such assessments must be made with respect to risk-based policies and standards in the absence of useful statistics on incidents. Adopting a process to rigorously assess the risk associated with information security threats is essential to developing a coherent information security risk management strategy [10]. An effective process advances an organization's ability to work with outside partners. Information security insurance carriers, for instance, have become increasingly rigorous and sophisticated with their requirements; to be insurable at a cost-effective rate (or at all), companies are being asked to provide detailed information about their cyber risk management programs. Insurers are also creating coverage exclusions for risky behaviors. In addition, working with third parties as a service provider, or even becoming party to a merger, acquisition, or joint venture becomes much easier with an effective cybersecurity process. Practically every good business transaction agreement today has substantial information security related representations and diligence requirements. This issue is often overlooked by companies until the deal gets tanked because one side realizes during its diligence that the other side is clueless about cybersecurity and exposes them to massive risk. This outcome is a real tragedy in an age when a majority of new startup companies' exit strategy hinges on being acquired by a larger entity[11]. The EY's Global İnformation security Survey 2015 [12], one of the most recognized annual surveys within the global information security arena, the responses of which were collected either with face-to-face interviews or the online questionnaire was conducted with 1,755 respondents from 67 countries with 25 industry sectors. EY's Global İnformation security Survey, the aim of which is to create trust in the digital world, investigates the most important cybersecurity issues facing businesses today. As a result, it helps customers to focus on risks which identify the strengths and weaknesses of their information security management systems and create an analysis regarding information security [13]. One question asked in the survey [12] to underline the effectiveness of information security, and risk are these: "Which of the following information security areas would you define as "high, medium or low priorities" for your organization over the coming 12 months? the result of which is that the Insider risks and threats is 49% as a medium priority. According to the 2014 Deloitte "information security survey" in Central Asia, it aims to better understand the current state of information security programmes and governance structures at organisations in the region. The survey focused on information security risks within approximately 100 companies through the online survey questionnaire. However, IT departments are aware of information security risks, business management and end-user awareness is considered to be insufficient. IT department awareness of information security risks is mainly through publicly available information and reports. IT departments appear to be informed about and aware of information security risks, end-user and (senior) management awareness is less apparent [14]. Many organizations still struggle to achieve a strategic view of information security. The human factor remains the weakest link in information security. Most organizations are unwilling to outsource key information security activities. Few companies hedge information security risks with insurance [15].

CONCLUSIONS

In this study, important aspects of providing risk management in information security are reviewed. The key point is that enterprises must be provided

with an effective risk management in İnformation security, they need to apply ISO 27001.

It is also necessary to adapt ISMS standards to enterprises, to explain them to all related parties, to employ security specialists in the body of enterprises, training users, technical personnel and managers, or to hire consultancy services. After ISMS applications are applied by enterprises successfully, it is important for enterprises to have an internationally valid certification for managing information security [13].

To provide high level information security in enterprises, understanding and applying information security standards as well as knowing current threats is important. It is shown that, to provide high level information security, an approach managed in the triangle of technology-human-education should be taken into account. It is necessary for enterprises to apply Risk Management in information security for the purpose of minimizing the risk level of security and providing business continuity [15].

As a result of, the purpose of this study is to accentuate the actual developments by emphasizing the significance of providing information security and risk management in enterprises which is a recent business model.

REFERENCES

[1]. J. F. Courtney, J.D. Haynes and B. D. Paradice, "Inquiring Organizations: Moving from Knowledge Management to Wisdom", England: Idea Group Inc (IGI), ISBN: 1-59140-309-X, pp.90-220, 2005.

[2]. D. Sutton, "Information Risk Management a Practitioner's Guide", Bcs the Chartered Institute for IT, ISBN 978-1-78017-265-1, pp.68-76, 2010.

[3]. Edward Humphreys, Information Security Technical Report, Elsevier, "Information Security Management Standards: Compliance, Governance and Risk Management", pp.247-255, 2008.

[4]. C. Young, "Metrics and Methods for Security Risk Management", Boston: yngress, pp.45–75, 2010.

[5]. Carol A. Siegel, Ty R. Sagalow, and Paul Serritella, Information Security Management Practices, Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security", pp.33-49, EBSCO, 2002.

[6]. Y. Vural, S. Sagıroglu, "A Review on Enterprise Information Security and Standarts", Vols. 23, pp.507-522. J. Fac. Eng. Arch., Gazi Univ., 2008.

[7]. R. Saint-Germain, "Information Security Management Best Practice Based on ISO/IEC 17799", The Information Management Journal, vol. 39, pp.61-62, 2005.

[8]. A. Refsdal, B. Solhaug, K. Stølen, "Cyber-Risk Management", SpringerBriefs in Computer Science, ISBN 978-3-319-23569-1, pp.9-47, 2015.

[9]. I.J. Martinez-Moyano et al., "Modeling the Emergence of Insider Threat Vulnerabilities", Proceedings of the 2006 Winter Simulation Conference. pp.42-51, 2006.

[10]. C. Young, The science and technology of counterterrorism; measuring physical and electronic security risk. Waltham, A: Butterworth-Heinemann, pp.73-89, 2014.

[11]. K. L. Miller , "About "Reasonable Cybersecurity": A Proactive and Adaptive Approach" The Florida Bar Journal/September/October, vol.90, pp.22, 2016.

[12]. Ernst & Young. EY's Global İnformation security Survey Report 2015: Creating trust in the digital world. (2016) http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

[13]. E. Yildirim, Advances in Human Factors in Cybersecurity, The Importance of Information Security Awareness for the Success of Business Enterprises, vol.501, pp.211-222, ISBN: 978-3-319-41931-2, Springer, USA, 2016.

[14]. Deloitte. Information Security Survey Report 2014. (2016)

[15]. http://www2.deloitte.com/kz/en/pages/risk/articles/risk-ca-security-survey-2014.html

[16]. E. Yeniman Yildirim, Akalp, G. Akalp, S. Aytac and, N. Bayram.:Factors Influencing Information Security Management in Small and Medium-sized Enterprises:A Case Study from Turkey. International Journal of Information Management, ISSN: 0268-4012, (31), pp.360-365. Elsevier, 2011.

★★★