The importance of integration of information security management systems (ISMS) to the organization's Enterprise Information Systems (EIS)

A. Luma*, B. Abazi*
* South Eastern European University / Faculty of Contemporary Sciences and Technologies, Tetovo, Macedonia
a.luma@seeu.edu.mk
* University for Business and Technology / Faculty of Information Systems, Prishtina, Kosovo
blerton.abazi@ubt-uni.net

***Abstract* - The interconnected information systems and networks drive the organizations into a critical situation that determines the need for explicit measures for information protection. The "culture of security" becomes a very important part of the business competition and security policy is a crucial component of business management. The organizations generate, use, store and transmit a huge amount of information which is vital to their functioning and prosperity. It is necessary the information be kept confidential when required, to be available when and where needed and protected from modification and loss of integrity. On this paper, I would like to explain the importance and the impact that information security management system may have on the general enterprise information system. This paper explains the processes that must be taken to integrate the ISMS to EIS, how this integration will help the organizations to protect their data and how this integration will affect on the growth of the business value and trust to the consumers.**

Keywords* - *information security, enterprise information system, integration, data protection, business value

I. INTRODUCTION

Almost all Business processes in organizations are transformed by information technologies. These include both the core processes, such as manufacturing, purchasing or distribution, as well as supporting processes, such as working time management or payroll. In addition to this, confidential information is available in almost every organization and information's, such as employee data or secret construction plans now are relying on the IT infrastructure, respectively on the data information protection services and which are managed by IT systems engineers. Ensuring safe and reliable IT operations are also governed by numerous regulations and laws [1]. Current threats, complex spy programs and data theft, such as Sony, Yahoo, Visa, Deutsche Telekom etc. demonstrated that IT risks have become a corporate risk. In order to prevent deliberate outflow of business-critical information, it is not only required concrete technical measures, but it is necessary to build a package of technical, organizational, physical, procedural and personnel measures and to consider them consistently and on holistically approach. [2] To address the many aspects of such holistic protection of business-relevant information and activities and to ensure the information security of an organization efficiently and effectively managed, the support of a software system for the management of Information Security Management is a need.

The diversity of opinions and factors influencing the process of IT adaption to information security needs is emphasized in many papers [3]. The literature has identified a number of factors affecting this process and most of them have listed factors such as senior management, government, IT consultants, organizational behavior, and so on [4]. Organizations are often affected by the models and standards that are implemented on information security within the same industry, but however not all the models and standards are implemented in the same way. For small organizations that operate with a small staff and which distribute information with key staff only, the implementation of information security does not seem to be a necessary option. However, companies where information is distributed to more people simultaneously, it is impossible to manage them without a proper system, thus, presenting the problem of data vulnerability. The third group of organizations is on where the main product is information [5].

Information Security Management System is defined by ISO 27001 as a set of policies and procedures for systematically managing an organization's sensitive data [6]. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

Organizations have different approaches when deciding to implement an information security system. Some organizations see information security systems as a competitive edge in the market that can provide them with greater credibility in their client relationship, as well as an increase of credibility in their organization and products. Another group of organizations implements information security systems only when they see that their competitors are operating in the same way. The

views create cultural diversity within organizations of the same industry and no doubt enables them to improve.

The objective of security policy is to protect the organization's sensitive and critical information in the best manner. In this way, the organization achieves at least two important results: reducing the risk and damage to its business interests and reputation due to harm to own sensitive information or partner's organization information and increasing the confidence in business partners an opportunity for outsourcing activities [7].

II. THE IMPORTANCE OF INFORMATION SECURITY

Information, support processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving the security of information is essential to maintain a competitive edge, cash flow, profitability, legal compliance and trade image.

Their organizations and systems and networks face security threats from a wide range of areas including computer fraud, espionage, sabotage, vandalism, fires or flooding. Causes of malware such as malicious code of programming, computer piracy and Denial of Service Attacks (DoS) have become more common, more ambitious and more sophisticated. Information security is important for both types of public and private sector organizations and it serves to protect critical infrastructures.

In both sectors, information security will function as an incentive, eg. to achieve e-governance or e-business and to avoid or reduce the risks involved. Liaison between public and private networks and the sharing of information sources increases the difficulty of achieving access control.

The tendency to use distributed IT systems has also weakened the effectiveness of centralized and specialized control Many information systems have not been designed to be safe. Security that can be achieved by technical means is limited and should be supported by appropriate management and procedures. Identifying which security control should be active requires careful planning and attention in every detail. Information security management requires participation by all employees in the organization. Participation of shareholders, suppliers, third parties, customers or other external parties may be required. Advice from specialists or organizations outside the main organization has often proved to be necessary.

The threat of external hackers and malicious attackers of information systems are still a major issue for information security and widely reported in the current events and highlighted in practicing managers' publications, for example. However, many researchers now believe the biggest threat to information security remains internal. This is outlined in several cases in which employees stole data while still working for their company, yet most employee security breaches occur accidentally or unintentionally.

Information security is important and decisive from the protection of organizational assets' view. Information is an asset and like any other asset of an organization it has its value. According to [5], [6] information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Information security is important and decisive from the protection of organizational assets' view. Information is an asset and like any other asset of an organization it has its value.

The existing and new businesses have to face with the fact that information security risks may have a negative impact on the process of business continuity, public image, the relationship between organizations, financial loss, affect relationships with clients, partners, and may create problems with legal authorities in case of discrepancies with the law. Information, support processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving the security of information is essential to maintain a competitive edge, cash flow, profitability, legal compliance, and trade image [10]. Organizations, systems, and networks face security threats from a wide range of areas including computer fraud, espionage, sabotage, vandalism, fires or flooding. Causes of malwares such as malicious code of programming, computer piracy and Denial of Service attacks (DoS) have become more common, more ambitious and more sophisticated. Information security is important for both types of public and private sector organizations, and it serves to protect critical infrastructures. In both sectors, information security will function as an incentive to avoid or reduce the risks involved. [11] The relation between public and private networks and the sharing of information sources increases the difficulty of achieving access control. The tendency to use distributed IT systems has also weakened the effectiveness of centralized and specialized control. Many information systems have not been designed to be safe. Security that can be achieved by technical means is limited and should be supported by appropriate management and procedures. Identifying which security control should be active requires careful planning and attention in every detail. Information security management requires participation by all employees in the organization.

III. THE IMPORTANCE OF ISMS INTEGRATION

Even though cyber-attacks are primarily reported as threatening IT systems, it should not be forgotten that the information must be protected regardless of the medium.

The organizational setup and embedding of an ISMS in the overall organization is a fundamental success factor for your ISMS project.

Our research found that there are three essential points that should be considered when setting up and integration the ISMS:

1. **Derivation from Business Strategy:** You increase the meaningfulness and appreciation of the ISMS when it is heavily wired to the

business strategy of your organization. A good understanding of business strategy will help you better understand what information assets are essential to your business. This can be incorporated into the design of the information security strategy. In addition, the demonstration of the business understanding helps you in the constant dialogue with organizational units, since you have a common basis for discussion.

2. **High management commitment:** The acquired understanding of the business strategy will pay off at the latest to increase the management commitment. Present the top management with the ISMS as a business case. Explain how the ISMS mitigates significant business risks, creates competitive advantages and nonetheless creates new value. [12] Ideally, the ISMS may even increase your organization's revenue and revenue (for example, if you are an IT service provider and your customers consider an effective ISMS as an added value. Details for the design of a business case for ISMS we have also put together for you. Even after setting up the ISMS, continuous dialogue with top management is important to ensure long-term survival. It is the responsibility of the management to make changes to the ISMS (eg. new or changed policies) [13]. Nevertheless, as an IS manager, you are responsible for providing essential information to management as needed. We recommend a combination of regular reporting (eg quarterly) and ad hoc reporting in case of significant changes or incidents.
3. **Dialogue with organizational units:** The interfaces of the ISMS with the specialist departments and asset (information value) owners first enable the ISMS to be filled with life. In most cases, the departments or their managers have the organizational responsibility for information assets and are therefore responsible for their protection. So you also know the meaning of the information values and are your contact for risk management. [14] If you have created an open dialogue with the organizational units, the continuous risk management will achieve much higher quality. The typical problem of "hushing up" risks can be addressed very well by you.

The success of your ISMS can be influenced very early by the correct touchdown. When setting up the ISMS, business-oriented integration into the organization is crucial.

IV. CONLUSION

With the aim of always being alert to Security, Fire and Automation issues, not only facing current threats but also monitoring technological developments, it is necessary to have Information Security Management System integrated into the organization structure, so that organization can read its existing security plans based on current requirements.

The right choice of ISMS and integrated management of an infrastructure of an organization can support decision-making, both at regular and daily level and in the strategic area at the administration level.

In combination with the possibility of an integrated management system, there is direct information about authorized maintenance personnel in case of any information security data breach [15].

Based on research, to accomplish the mission, the Integration of Systems should serve three (3) main areas:

- Consolidation of "dispersed" sources of an organization's security data in order to maximize the existing infrastructure, along with new investments in physical infrastructure.
- Provide the appropriate procedures that enable the transformation of the data collected into useful information at the lowest possible cost. To this end, Integration of Security Systems should be equipped with a high degree of automation and sufficient builder intelligence in order to efficiently manage a large number of buildings from a central office with resources of limited, assisted by some local guards. As an example, we mention the automated correlation of an alarm event from a recorded video.
- Supporting integrated management systems for the maximum extent possible actions by the structures and users of the facility. For example, through a unified platform, the right people with the right information will be informed via appropriate communication tools and in a timely manner, and then it is mandatory to support communication and cooperation between users, different operators and addressing each step alarm event management or access control, until final issues resolution and outcome evaluation.

In addition, with the common control platform and the gradual establishment of compatible systems, it generates enough infrastructure for common policies and security practices in all organizations, helping to implement future actions that are designed and certified by improved procedures.

Lastly, this is achieved through the homogeneity/interchangeability of the centralized management tool and architecture that supports backup centers at both local and regional level (backup/servers and redundant databases) and at the level of decentralized (disaster recovery sites).

With the evolution of technology and the gradual support of open communication protocols - the interaction of equipment from different manufacturers, the choice of a suitable integrated management program increases the desired efficiency, thereby improving investment reliability over time.

References

[1] C. Keller, “Implementation of information security policies in public organizations : success factor,” no. May, 2017.

[2] B. Abazi, “An approach to the impact of transformation from the traditional use of ICT to the Internet of Things: How smart solutions can transform SMEs,” *IFAC-PapersOnLine*, vol. 49, no. 29, 2016.

[3] J. Businge, A. Serebrenik, and M. van den Brand, “An Empirical Study of the Evolution of Eclipse Third-party Plug-ins,” in *Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE)*, 2010, pp. 63–72.

[4] A. Joshi, L. Bollen, H. Hassink, S. De Haes, and W. Van Grembergen, “Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role,” *Inf. Manag.*, no. January, pp. 0–1, 2017.

[5] D. T. Burgeois, *Information Systems for Business and Beyond*. 2014.

[6] ISO/IEC 27001:2013, “Information Technology — Security Techniques — Information Security Management Systems — Requirements,” *Int. Organ. Stand.*, 2013.

[7] G. Gluschke, *SECURITY POLICIES AND CRITICAL INFRASTRUCTURE PROTECTION*. .

[8] SANS, “Information Security Resources,” 2008. [Online]. Available: https://www.sans.org/information-security/.

[9] B. Maule-Ffinch, “Key trends in information security,” *Netw. Secur.*, vol. 2015, no. 11, pp. 18–20, 2015.

[10] B. Abazi, *The implications of Information security to the Internet of Things*. 2017, p. 4.

[11] M. Antonakakis *et al.*, “Understanding the Mirai Botnet,” *Proc. 26th USENIX Secur. Symp.*, pp. 1093–1110, 2017.

[12] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology,” *Nist Spec. Publ.*, vol. 800–30, p. 55, 2002.

[13] Z. Al-rashdi, M. Dick, and I. Storey, “Literature-based analysis of the influences of the new forces on ISMS : A conceptual framework,” pp. 116–124, 2017.

[14] A. Council, “Information Security Management,” no. April, pp. 1–25, 2011.

[15] M. Karyda and L. Mitrou, “DATA BREACH NOTIFICATION: ISSUES AND CHALLENGES FOR SECURITY MANAGEMENT,” 2016.