International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 5 (Sept - Oct, 2016), PP 114-117

Information Security of the Enterprise

Zahari Goranov Ph D
Institute of Metal Science, Equipment, and Technologies "Acad. A. Balevski" with Center for Hydro- and Aerodynamics at the Bulgarian Academy of Sciences – (IMSETHC-BAS)
zgoranov27@e-dnrs.org

***Abstract*: - The paper reviews the connection between the information security of the enterprise and its competitiveness. Increasing Information Security automatically increases the competitiveness of the entire enterprise.**

Keywords: **information security, information system, security, enterprise, competitiveness.**

I. INTRODUCTION

The problem with the protection of information security in the enterprise is now extremely topical. Information Security is protection of information and information systems from unauthorized access, use, disclosure, alteration, reading, recording and destruction. Information security is the protection of information, regardless of its form - electronic, printed or otherwise. Computer security focuses on the integrity of computer systems and networks and their processing of information. Information security management practices are the risks associated with the use, handling, storage and transmission of information and the systems and processes used for those purposes. Enterprises should increase the level of their information security, otherwise they are going to lose their competitiveness.

II. DEFINITIONS OF INFORMATION SECURITY AND COMPETITIVENESS

What does Information Security (IS) mean?

Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. This triad has evolved into what is commonly termed the Parkerian hexad, which includes confidentiality, possession (or control), integrity, authenticity, availability and utility.

Technopedia explains Information Security - information security handles risk management. Sensitive information must be kept - it cannot be changed, altered or transferred without permission. For example, a message could be modified during transmission by someone intercepting it before it reaches the intended recipient. Good cryptography tools can help mitigate this security threat. Digital signatures can improve information security by enhancing authenticity processes and prompting individuals to prove their identity before they can gain access to computer data. Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. This triad has evolved into what is commonly termed the Parkerian hexad, which includes confidentiality, possession (or control), integrity, authenticity, availability and utility. Information security handles risk management. Anything can act as a risk or a threat to the CIA triad or Parkerian hexad. Sensitive information must be kept - it cannot be changed, altered or transferred without permission. For example, a message could be modified during transmission by someone intercepting it before it reaches the intended recipient. Good cryptography tools can help mitigate this security threat.

A. Information Security Policy

Information security policy is a set of policies issued by an organization to ensure that all information technology users within the domain of the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority. The evolution of computer networks has made the sharing of information ever more prevalent. Information is now exchanged at the rate of trillions of bytes per millisecond, daily numbers that might extend beyond comprehension or available nomenclature. A proportion of that data is not intended for sharing beyond a limited group and much data is protected by law or intellectual property. An information security policy endeavors to enact those protections and limit the distribution of data not in the public domain to authorized recipients.

Every organization needs to protect its data and also control how it should be distributed both within and without the organizational boundaries. This may mean that information may have to be encrypted, authorized through a third party or institution and may have restrictions placed on its ditstribution with reference to a classification system laid out in the information security policy.

An example of the use of an information security policy might be in a data storage facility which stores database records on behalf of medical facilities. These records are sensitive and cannot be shared, under penalty of law, with any unauthorized recipient whether a real person or another device. An information security policy would be enabled within the software that the facility uses to manage the data they are responsible for. In addition, workers would generally be contractually bound to comply with such a policy and

would have to have sight of it prior to operating the data management software.

A business might employ an information security policy to protect its digital assets and intellectual rights in efforts to prevent theft of industrial secrets and information that could benefit competitors.

A typical security policy might be hierarchical and apply differently depending on whom they apply to. For example, the secretarial staff who type all the communications of an organization are usually bound never to share any information unlesss explicitly authorized, whereby a more senior manager may be deemed authoritative enough to decide what information produced by the secretaries can be shared, and to who, so they are not bound by the same information security policy terms. To cover the whole organization therefore, information security policies frequently contain different specifications depending upon the authoritative status of the persons they apply to. [1]

In science there is no definition of competitiveness. Each author takes competitiveness differently. Theory of competitiveness is of paramount importance for business development. It provides a system of knowledge about how we can achieve lasting success in the fight against competitors and - higher living standards of society. According to some authors more competitive now boils down to increasing the competitiveness of its products. They believe that if a product is in demand and purchased in the market, the entity that is offering them competitive. Information Security is an important part of the competitiveness of the enterprise (it is one of the most important factor for competitiveness). The term competitiveness is used in a bewildering variety of ways, both in the policy community and in academic research. Some equate competitiveness with the ability to achieve certain overall outcomes, such as a high standard of living and economic growth. Other definitions focus on the ability to achieve specific economic outcomes such as job creation, exports, or FDI(foreign direct investmants). Yet other definitions see competitiveness as defined by specific local conditions such as low wages, stable unit labor costs, a balanced budget, or a 'competitive' exchange rate to support a current account surplus. These different views of competitiveness have confused the public and scholarly dialogue.

The evolution of the competitiveness debate has oscillated around three ideas: market share, costs, and productivity. When the term competitiveness first gained prominence in the1980s, the public debate in the United States was dominated by fears about the seemingly [2]. Another view of competitiveness focuses on measures related to a location's costs. Work on cost competitiveness has various interpretations. Low labor costs (compensation per hour, per employee) are seen as a sign of competitiveness leading to lower unemployment, higher exports and higher FDI. Other studies examine the relationship between (labor) costs and output. Unit labor costs are often used to evaluate whether a country's balance of payments is likely to be sustainable (e.g., European Central Bank, 2008) [3].

There is another theory about competitive use of our resourses and labour. Competitiveness is defined by the productivity with which a nation utilizes its human, capital and natural resources. To understand competitiveness, the starting point must be a nation's underlying sources of prosperity. A country's standard of living is determined by the productivity of its economy, which is measured by the value of goods and services produced per unit of its resources. Productivity depends both on the value of a nation's products and services – measured by the prices they can command in open markets – and by the efficiency with which they can be produced. Productivity is also dependent on the ability of an economy to mobilize its available human resources. True competitiveness, then, is measured by productivity. Productivity allows a nation to support high wages, attractive returns to capital, a strongcurrency – and with them, a high standard of living [4].

There are also more than one definitions for computer and information security. Computer security is a branch of technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users [5].

Information Security - this term is more commonly found not only in specialized publications. Almost everyone has experienced one or another his appearance because the information has become almost the most important part of our daily lives. A valuable things must be kept.

In the business world, information security has its own specific and versatile manifestation. In today's dynamic world gets advantage this organization has accurate and timely information that can store, process and communicate reliably. Information management is critical for internal - business processes and competitiveness of each company - this applies both to the conditions of normal business activity and in the case of unforeseen crises. Therefore, information security is becoming a decisive factor for the existence of any organization, regardless of the subject of its activities. In fact, in some areas of the business that has long been a fact [6].

III. INFORMATION SECURITY AS A PART OF THE COMPETITIVENESS OF THE ENTERPRISE.

If we can not protect our information we will loose our business. Here some more definitions of information security:

- State of protection of the information environment.
- Concept of protection of programs and data from accidental or deliberate modification, destruction, disclosure and use without permission.
- Process of ensuring the protection of information technology, providing the work of information systems.
- Lack of unacceptable risk associated with leaks technical channels, unauthorized or unintended impacts on data or other resources of information system [7].

Security objectives:

- To secure the values of the system;

- To protect and ensure the accuracy and integrity of information;
- To minimize the damage resulting from the modification or destruction of information [8].

IV. HOW TO PROTECT OUR INFORMATION

To make sure that we provide high quality protection must meet the standard ISO 27001:2005. If we meet the requirements of the standard it means that much of the information is defended from our coqurents.

The ISO 27001 specifies the requirements for systems to manage information security and is applicable to all organizations, regardless of size, activities and processes. Implementation of ISO 27001 in the organization's strategic decision and aims to achieve a certain level of data protection, ensuring its confidentiality, integrity and availability. Level of protection of ISO 27001 does not cover only the risks associated with IT infrastructure and covers physical security, human resources, legal protection, compliance with legal and regulatory requirements. [9]

In the most enterprises are kept similar rules for IT security.

A. Split up the Users and Resources

For an information security system to work, it must know who is allowed to see and do particular things. Someone in accounting, for example, doesn't need to see all the names in a client database, but he might need to see the figures coming out of sales. This means that a system administrator needs to assign access by a person's job type, and may need to further refine those limits according to organizational separations. This will ensure that the chief financial officer will ideally be able to access more data and resources than a junior accountant. That said, rank doesn't mean full access. A company's CEO may need to see more data than other individuals, but he doesn't automatically need full access to the system. This brings us to the next point.

B. *Assign Minimum Privileges*

An individual should be assigned the minimum privileges needed to carry out his or her responsibilities. If a person's responsibilities change, so will the privileges. Assigning minimum privileges reduces the chances that Joe from design will walk out the door with all the marketing data.

C. *Use Independent Defenses*

This is a military principle as much as an IT security one. Using one really good defense, such as authentication protocols, is only good until someone breaches it. When several independent defenses are employed, an attacker must use several different strategies to get through them. Introducing this type of complexity doesn't provide 100 percent protection against attacks, but it does reduce the chances of a successful attack.

D. Plan for Failure

Planning for failure will help minimize its actual consequences should it occur. Having backup systems in place beforehand allows the IT department to constantly monitor security measures and react quickly to a breach. If the breach is not serious, the business or organization can keep operating on backup while the problem is addressed. IT security is as much about limiting the damage from breaches as it is about preventing them.

E. Record, Record, Record

Ideally, a security system will never be breached, but when a security breach does take place, the event should be recorded. In fact, IT staff often record as much as they can, even when a breach isn't happening. Sometimes the causes of breaches aren't apparent after the fact, so it's important to have data to track backwards. Data from breaches will eventually help to improve the system and prevent future attacks - even if it doesn't initially make sense.

F. Run Frequent Tests

Hackers are constantly improving their craft, which means information security must evolve to keep up. IT professionals run tests, conduct risk assessments, reread the disaster recovery plan, check the business continuity plan in case of attack, and then do it all over again. [10]

CONCLUSION

In conclusion we can say that information security is vital to the existence of enterprise. In modern and rapidly developing world, our company is obliged to respond to any challenge. In the modern world, technology is developing at a very great pace and we need to keep up with them. Today, effective management of any company, regardless of its size and scope of economic activity is impossible without providing opportunities for processing of all relevant information, and this in the short term for the design and management decisions. Everything is reasonably practicable only in terms of making full use of information systems. No less important for organizations to understand also that the introduction of an information system it is all over, and switching to a higher stage of organizational development and information. The introduction of any information system for management purposes is only one step in a continuous process of improving their general and in particular their information base. [11]

If our systems are working well, we can do our work better and faster. If we can protect our systems from competitors will be able to keep their information advantages. We shoul work every day to increase our IT securirty.

References

[1] Texhnopedia http://www.techopedia.com/definition/10282/information-security-is

[2] Mercedes Delgado THE DETERMINANTS OF NATIONAL COMPETITIVENESS Working Paper 18249 NATIONAL BUREAU OF ECONOMIC RESEARCH 1050 Massachusetts Avenue Cambridge, MA 02138 July 2012 http://www.nber.org/papers/w18249.pdf

[3] Op Cit http://www.nber.org/papers/w18249.pdf

[4] IESE http://www.iese.edu/en/ad/AnselmoRubiralta/Apuntes/Competitividad_en.html

[5] Wikipediahttp://en.wikipedia.org/w/index.php?title=Computer_security&&oldid=30994438

[6] CIO BGhttp://cio.bg/1923_informacionnata_sigurnost_v_promishleno_predpriyatie__luks_ili_neobhodimost

[7] Tuzarov S.Information Security http://tuj.asenevtsi.com/Sec2009/Sec02.htm

[8] Tuzarov S.Information Security http://tuj.asenevtsi.com/Sec2009/Sec02.htm

[9] Lirex IT Innovations http://www.lirex.bg/bg/Konsultantski-uslugi/Informatzionna-sigurnost/Penetration-Test

[10] Technopedia http://www.techopedia.com/2/27825/security/the-basic-principles-of-it-security

[11] http://znanieto.net/index.php?option=com_virtuemart&func=downloadRequestFree&page=shop.browse&product_id=6798.