INFORMATION PROTECTION AND SECURITY IN MODERN ORGANIZATIONS

Florin Dimitrescu, Valahia University, Romania

ABSTRACT

Information technology has now reached the opportunity to provide organizations with unparalleled capabilities in the field of data management, which can be used to gain competitive advantage. Information protection and security cannot be ignored by managers because they play a critical role, and a change in any of these components often leads to significant changes over the others. The purpose of this paper is to perform analyzes and develop considerations on information protection and security in modern organizations.

JEL: L86, M15

KEYWORDS: information protection, security policies, risk security.

INTRODUCTION

The environment in which modern organizations perform is based to a very large extent on information and implicitly on elements of its processing technology (Dhillon, G. & Backhouse, 2001). Due to the benefits that information technology brings, we are witnessing a deeper and deeper integration of these elements in the other components of an organization, which makes these elements directly influence the development of organizational processes, but especially their efficiency.

In the most general sense, the security of computer systems ensures the protection of information stored in these systems, prevents loss, accidental or intentional modification and unauthorized reading, ie what is expected of them, even if users do not do what they should do (Von Solms, 2006; Whitmore, 2001). However, the protection of moving data refers to the implementation of a set of measures to ensure their security during the transfer. Communication lines are an essential element as they are used for the delivery / access of services, and ensuring the security of the data within them is a critical element for the security of the whole system.

The state of cyber security can be achieved by applying proactive and reactive security measures that include security policies, standards and models, by managing risk and by implementing solutions for the protection of networks and information systems.

SECURING INFORMATION SYSTEMS IN MODERN ORGANIZATIONS

Protection and security mechanisms are implemented in the operating system to implement various security policies (Hershey & Silo, 2012). A security policy defines a set of requirements

that must be met by a computer system. Instead, the security mechanisms have the role of authenticating the subjects and authorizing their access to different objects.

In addition, the security policy must specify how the protection state can be implemented (Perkel, 2010). This is done by defining a set of rules that represent the policy of changing the state of protection. The implementation of the idealized model implies the departure from certain hypotheses, so that the system can be built effectively and at a reasonable cost. The key components of the implementation are: subject authentication modules, resource monitor and protection status representation. The last two components are new elements in the implementation of protection systems.

Therefore, a system security policy specifies how resources should be shared between members of the organization and with external users of the organization (Von Solms, 2005). The mechanism consists of specific tools and steps provided by the system to implement the policy. Establishing a precise policy is difficult since it requires a precise set of requirements to be specified in completing an unambiguous package of laws to control user activity.

Another extremely used information protection technique is cryptography, and with the development of the use of the Internet, its importance has increased (Coles-Kemp, 2009). As long as the information is not in the processing phase, or is in the file system and is transmitted over a network from one computer to another, then, for protection, it is encrypted. Because files are stored on devices shared by n users, a user's file may be read, executed, and modified by other users, despite the fact that the file owner wants the information in that file to be personal.

On the other hand, encryption has gained rapid and important development in modern computing systems. In computer networks and computer systems, it is very difficult to create a mechanism where the information is inaccessible to the unauthorized. The information is encrypted in a form in which its informational content is unintelligible without a decryption phase. The key point of encryption is to be able to perform efficient encryption so that, theoretically, the information cannot be decrypted by unauthorized users.

There are extremely many encryption algorithms, some of which are extremely simple and it is possible to define its own encryption mechanism by each user. An encryption function can be a simple mathematical function that satisfies some requirements. The most important of these requirements is that the function is bijective in order to give us the possibility to reverse the process and recover the original information that was the basis of the encryption process. Of course, advanced methods are far from available to every user and are patented by powerful companies working in this field.

CONCLUSIONS

Information systems can become powerful tools to make organizations more competitive and efficient. Information technology can be used to redesign and reshape organizations, to transform their structure, reporting and control mechanisms, current work practices, document flow, products and services provided.

To ensure the security of information systems, it is not enough to accumulate tools; we must have a real security policy. In most cases, the implementation of data security policies within organizations imposes limitations that have a negative impact on processes and limit their effectiveness.

REFERENCES

Coles-Kemp, L. (2009) "Information Security Management: an entangled research challenge", Information Security Technical Report, 14(4), 181-185.

Dhillon, G. & Backhouse, J. (2001) "Current directions in IS security research: towards socio-organizational perspectives", Information Systems Journal, 11(2), 127-153.

Hershey, P. & Silo, C. (2012) "Procedure for detection of and response to distributed denial of service cyber attacks on complex enterprise systems", In Proceedings of 6th Annual International Systems Conference, Vancouver, 19–22 March 2012.

Perkel, J. (2010) "Cybersecurity: how safe are your data?", Nature, 464, 1260-1261.

Von Solms, B. (2005) "Information Security Governance – compliance management vs operational management", Computers & Security, 24(6), 443-447.

Von Solms, B. (2006) "Information Security: The Fourth Wave", Computers & Security, 25(3), 165-168.

Whitmore, J.J. (2001) "A method for designing secure solutions", IBM Systems Journal, 40(3),747–768.