How Much ICT Security has Improved During the Last Decade

Mefat Shabani[1], Jozef Bushati[2], Virtyt Lesha[3], Imelda Zadeja[4]

[1] Faculty of Engineering Vidzeme University of Applied Sciences, Latvia
[2] Faculty of Education Sciences, University of Shkodra "Luigj Gurakuqi"
[3] University Metropolitan Tirana, Albania
[4] Canadian Institute of Technology, Albania

INTRODUCTION

Since 2000, information security has begun to develop at a significant pace. Many companies are adopting modern information and communication technologies, without fully considering the fact that it is necessary to manage new types of ICT threats, different from those of the past.

It is for these reasons that the security of access to ICT systems needs to be fundamentally rethought. Furthermore, modern IT environments are not ideal because they are constantly growing and evolving, becoming more and more complex. Their stepwise development also dictates at least the temporary coexistence of old and new technologies, thus leaving behind many cracks and gaps through which attackers can attack.

The purpose of this paper is to address this gap and outline how far we have come in terms of information security and protection, as well as the challenges faced by modern companies. It also investigates the other factors contributing to ICT security. This paper provides certain guidelines on where companies should begin, and which aspects of security are especially vulnerable nowadays. By studying the evolution of ICT security, the paper aims to determine the most effective way to protect information systems from modern threats.

MATERIALS AND METHODS

Scientific and professional literature in the field of computer and information technologies with special interest in the field of information security was used in the preparation of the final paper. In processing the topic, secondary data were used, from the official website where texts or papers related to the thematic area of this final paper were published. The paper uses methods of descriptive analysis (in analysing and describing the elements of the units that are discussed in this paper in order to determine the elements, content and components of the observed unit and the relationship as a whole) and synthesis (combining simple mental creations into more complex connecting elements, processes, phenomena and relations as a whole), inductive and deductive method (for the purpose of presenting general laws and reducing abstractions) and the method of compilation (when quoting and graphical representations taken from the used literature). Statistical data was also used, taken from official agencies, databases and research centres.

RESULTS

The security of information systems has always been important for an organisation to operate successfully. With the modernisation and informatisation of business, the risk of information systems security increases. It is the networking of computers and the dislocation of an organisation's business that leads to the need for greater protection of confidential information. When information is not properly protected, it is very likely that it can jeopardise an organisation's competitiveness and present the same organisation as a failure. Since security is not something that is the final product or condition, but a process, it is logical that the security of information systems is a constant action and the whole process of protection. It is not enough just to determine which information systems are suitable for business, it is necessary to constantly check the operation of the system in order to maintain an acceptable level of risk that threatens each information system and thus the business system as a whole. There are a number of parts of a system or organisation that need to be protected, and information security takes care of three basic aspects of maintaining confidentiality, integrity, and availability of information. Through these three aspects and their proper protection, it is possible to lead to the progress of an organisation's business.

These conclusions and the completed work proved the hypothesis that there are a large number of ways, methods and practices governing information security. However, businesses and individuals are still not sufficiently educated or concerned so they remain extremely vulnerable. This is why ICT security is still a problematic issue – and it looks like it will be even more in the future.

DISCUSSION

The reason for the complexity of information security protection is precisely due to the security of information systems being a very broad concept, and it is necessary to look at it as a whole, and not pay attention to certain parts only. When the information system is understood as one large entity branched into different areas, and when the laws, rules, procedures, and instructions in this area are respected, only then can it be said that an information system is secure. However, due to the ramifications and complexity of this topic, it is very difficult to fully monitor the security of information systems, because they are vulnerable in many ways, so it is necessary to continuously check and guard against threats that systems are becoming more open to.

CONCLUSIONS

Since information is the main resource of business and it is the core of everything that an organisation possesses, the correct application of protection methods increases the competitiveness and business success of a particular organisation. An important aspect of business is correctly deciding on the protection measures to be used, depending on the organisation and the activity with which a particular organisation is engaged; it is important to implement proper protection. The security of information systems doesn't only include the storage of confidential data in a special place; it is necessary to protect the facilities themselves, equipment and premises, all the way to programs and documents that contain information. This paper can be used as a starting point for choosing and deciding on protective measures, as well as an wake-up call for everyone to think more about ICT security. ICT gives numerous benefits – but they come at a cost – so, we need to stay alert to tech trends and constantly strive for better protection.

KEYWORDS: ICT security, Cybersecurity, ICT security evolution, Threat, Vulnerability