Reduction of Ict Security Risks Using Level Based Approach

Ivo Džakula[1], Branko Latinović[2]

[1]PhD Student at University „APEIRON", Banja Luka, BiH, dzakula.ivo@gmail.com

[2]Professor at University „APEIRON", Banja Luka, BiH, branko.b.latinovic@apeiron-edu.eu

Case Study

DOI: **10.7251/JIT1902099DZ** UDC: **006.3:[004.738.5:316.774**

Abstract: Security controls are certainly one of the most preferred ways of controlling the environment in which our system is "alive". But although they are heavily represented and used in practice, security controls tend to become the same and not change after they are introduced. To try to make the most of the opportunities that this approach provides, this paper will explain the importance of implementing ICT security controls and propose a new approach by adding emergency ICT control. This approach gives us the ability to integrate the entire organization into the development of control by providing a better, more accurate and faster basis for managing the security risks of ICT technology.

Keywords: ICT – Information and communications technology, Risk, Security controls.

Introduction

Business processes in the modern age depend largely on the degree of development of computer systems. The integration of sophisticated software solutions, the transfer of business data through computer networks and the creation of a cyber environment have proven to be very useful in the business world. But if we look at the other side, it is sure that the risk of data alienation is getting bigger and bigger. Cybercrime is a problem of a modern age that is causing headaches to companies around the world.

Like all other branches of business, an accelerated process of computerization through business processes did not pass by ICT. ICT resource management and in time reaction are key to the success and preservation of the process.

However, in order for the reaction to be timely, it is necessary to take steps that not only give promises but also results.

Risk Assessment and Systems

Risk is a product of a probability of an event and an impact on the event. With regard to the security risk of information systems, we can conclude that this risk definition is difficult to apply directly because of the intentional impact on the event and the unpredictability of threats, and is often approximate to the relative risk of comparing the likelihood of a security attack successfully executed against an asset on another asset. It follows that security risk is a combination of threats, possible system vulnerabilities to the threat, and consequences after a successful attack. Thus, the threat is generally accepted as part of the assessment associated with determining further probabilities.

Information Attack Method

The method of information attack is a method that is deliberately directed, causing a damaging impact on the confidentiality, integrity and/or availability of information assets. Security data deals

with the protection of its confidentiality, integrity, and availability. Informational Attack Method treats the following elements:

- Confidentiality is important for information that is sensitive to reputation, competitive advantage, or security. Theft or copying may compromise the confidentiality of the data.
- Data integrity refers to their accuracy. Information is useful if one can believe it is true. Without this element, the value of information is drastically reduced.
- The availability of information is taken care of by delivering the data to the correct destination in a timely manner. If information reaches your destination late, it will be considered that it was not available when needed.
- Authentication means that the information is true and original (the information is neither fabrication nor copy) - it should be borne in mind that falsification can also be done without the principle of breach of confidentiality (counterfeit uses own account), possession of information (some data is taken out of control) or integrity (information is a product of criminogenic activity). Hence, information assets are subject to threats of confidentiality, integrity, availability, and authenticity. The exact nature or causes of this threat will depend on a particular property issue.

Methods of an attack on information assets can be done physically (by stealing or property damage), by cyber-attacks, or by using electromagnetic spectrum interference suppression devices. For example, a physical attack method claims a copy of the information may be stolen or copied without permission and may potentially affect their confidentiality.

Similar information jeopardizes integrity, an attack of dissatisfied or forcible employees, deliberately or virtually exchanged through a computer virus.

ISO 27005 Information security risk management provides specific guidance on the risk management of information protection within the organization.

To begin with, it is most important to determine critical points that are potentially at risk of attack. It is also important to emphasize that poor asset management, using obsolete software and hardware, lack of device compatibility, lack of alternative solutions, and lack of adequate human factors are a very important component in risk assessment.

The classic threat model is a very good communication tool. The threat to the organization or system is visible when it is displayed in a clear, easy to understand, and graphical representation. The multifaceted, hierarchical development of the Model of threats allows those with no technical or non-security expertise to immediately assess where threats come from and identify which assets are attacked, and experts and operators point to the need for adequate security control. The graphic nature of the model facilitates its understanding and increases its communication advantages. Furthermore, this model offers common definitions and language for security threats, influences and controls to enable communication. The threat model allows you to identify property threats that could cause a major impact on process activities. It, therefore, enables the risk assessment organization to focus and resources on the asset that requires further testing.

Obviously, some security threats can and do a prolonged or delayed impact, and would be useful if this could be proven. The performance display procedure over a given period of time should be incorporated into the risk assessment methodology itself. This gives you additional benefit not only that you are able to communicate about the influence of time aspect, but also encourages contemplation of countermeasures that are time-constrained.

Means of Threats / Sources of Threats

Traditional sources of threats

Traditional threats in the narrow sense include espionage, sabotage, terrorism and subversion, and the definitions that can be found below briefly describe each of these threats:

- Espionage - Espionage is an act in which certain foreign accesses or takes information secretly or illegally through foreign forces, and for further goals has a subversive political goal.
- Sabotage - Sabotage is an unauthorized act where a certain party intentionally causes consequences that would slow down or stop

processes in the injured party in order to assist certain hostile groups or to further pursue the political goal.
- Terrorism - Terrorism is an act by which a certain party through the use of violence or intimidation for the outcome has a political goal.
- Subversion - activities that endanger the security or well-being of the State and are intended to undermine or abolish political ideology by industrial, political or violent means.

Non-traditional sources of threats

The number of non-traditional threats is on the rise and there are the following examples:
- Crime - Theft is a worrying rise especially for ICT and facilities with large budgets that are at risk of fraud of dissatisfied workers or criminal groups. Criminal activity may range from physical theft of equipment, computers, computer parts, back-up materials, etc. This activity also includes blackmail, illegal access, or corruption of IT data for fraud or crime purposes.
- Protesting Groups - Protest groups are conducting demonstrations, due to various causes, against a wide spectrum of facilities whether they are state or airport facilities and systems. They are mostly peaceful and democratic protests, but extreme elements can involve the pursuit of attacks against individuals or property and can pose a threat and be as significant as part of terrorism.
- Research journalists - Research journalists can try to get information on certain works, critical information, program data, and even the structure of the whole system for better research. Such a type of non-traditional threat can lead to disturbances in daily operations, such as airport operations, and can seriously affect the company's reputation.
- Industrial espionage - Industrial espionage is a type of unlawful act which through the appropriation of information secretly or illegally works to help the competition.

ICT security controls

In order to adapt to the Security System, security controls should be grouped into six levels as shown in Figure 1 – ICT security control levels. The key difference is at the risk level of a particular ICT system depending on each organization. The level of risk varies depending on the criticality of the service provided by these vulnerabilities of the ICT system and the nature of threats depending on the systems.

ICT security control can be organized at levels depending on the assessment of ICT system vulnerability. The lowest level of risk will require the lowest level of basic control; the highest level of risk will require the highest level of basic control.

International practice is the establishment of six levels of control: Level 1 to Level 6 are cumulative and meet the basic requirements of ICT control for organization. The degree of control depends on the complexity of the ICT system or the level of assessment of the vulnerability of ICT assets. For example, Level 1 is the lowest level of security and is appropriate for organizations with a limited and isolated ICT system. Level 6 is the highest level, requiring the implementation of all control requirements (from Level 1 to Level 6). The key difference is at the risk level of a particular ICT system. The level of risk varies depending on the criticality of the service provided by the organization, the vulnerability of the ICT system and the nature of threats.

It is necessary to create categories - tables for certain organizational functions and in detail to clarify each level. Since this kind of organization can not be categorized as a classical one, it is necessary for each and every individual before setting up control to determine critical assets depending on the organization's business processes. This means that the ICT assets that are not critical to the operation will fall into lower risk, while critical assets will be included in the highest level of risk and therefore control. Within each table, levels of control in the rising order from levels 1 to level 6 are described. Levels are cumulative, which means that a higher level of control contains all that is listed below.

Control levels are designed so that the organization is balanced Certainty will have similar levels of control in each of the organizational functions. The organization may request the revision of ICT security, assessing the level of control for each of the above-mentioned categories. This assessment may point to areas where controls are inconsistent at their levels.

Level	Information	Scope	Critical system isolation	Threats
1	Manage sensitive information	Critical	Isolated	Common threats (eg hacker attacks or potential criminals)
2	Manage sensitive information	All	Highly-connected IT system	Common threats (eg hacker attacks or potential criminals)
3	For sensitive information	Adds a medium level of control to the security system	Exposure to a larger area of threat is little compared to the overall ICT system within the organization	More modern and better equipped potential attackers (eg those dealing with serious and organized crime - cybercrime, including terrorist organizations)
4	For sensitive information	Medium level control for the entire organization	Highly Integrated Information System	More modern and better equipped potential attackers (eg those dealing with serious and organized crime - cybercrime, including terrorist organizations)
5	Information is of great value to the organization and potential attackers	High level of control is characteristic of risks and assets	Relatively isolated	The most powerful potential attackers. These types of attacks are in most cases associated with hostile governments (eg government-sponsored terrorism, industrial espionage or some highly capable offenders engaged by a criminal organization)
6	Information is of great value to the organization and potential attackers	High level of control for the entire organization	The distribution of assets can not be sufficiently isolated	The most powerful potential attackers. These types of attacks are in most cases associated with hostile governments (eg government-sponsored terrorism, industrial espionage or some highly capable offenders engaged by a criminal organization)

Figure 1. *ICT security control levels*

It is important to know that multiple business-critical networks and multiple non-critical networks can emerge at the organization level. This type of organization poses many different security requirements to us and it is very difficult to put everything in the same bin. Namely, it is a miracle to find yourself in a situation where all levels and all controls are applicable to all networks of the organization. To properly address this issue and set up valid security controls, you must do the following:

- Categorizing the importance of networks and network infrastructure
- Categorizing the importance of data
- Determining the points of contact between critical and non-business networks

For each of the above requirements, it is necessary to develop security controls that will be adequate for each individual network category. Particular attention should be paid to cases where these two types of differently categorized networks meet. In these cases, priority is given to controls over critical networks. Network staff categorized as critical to the network will always have "superiority" over staff working on a network of lesser importance to the organization. This is not to say that one network or staff is more dominant than another, but that in the event of a network crash, being categorized as critical would have a greater impact on the profitability and reputation of the organization.

In order to meet the requirements of international regulations, local Laws and provisions of international standards, which are increasingly implemented by organizations, it is necessary to develop a set of controls that will meet all of these requirements, and in addition, meet the needs of the organization and ensure confidentiality, integrity, and availability of data. All of these regulations, as well as international standards, give us requirements that must be met as well as guidelines for satisfying them. Although compliance with the provisions is considered to be a harmonized security system, in many cases there is a lack of security controls, which is visible only after conducting an audit, control or penetration test. In order for an organization to ensure that controls are fully aligned with operational requirements, it is necessary to enter into every message of the organization and examine the weakest links. From the human resources, the IT sector of the security staff, and even to the administrative staff itself, there is a certain degree of responsibility for conducting security controls.

The fact is that risk assessments cannot be accurate unless there is accurate input from all stakeholders, both inside and outside the organization. Given the importance of risk assessment, it is crucial to ensure accurate and timely information. If

there is no quality input or it is learned during the risk assessment that a particular part of the organization has failed or is unable to provide accurate information, then that same part of the process can be viewed as a risk.

Proposal for emergency security controls

It would be a good idea, when establishing security controls, to establish a mechanism for adopting emergency security controls that would serve as a coercive mechanism as well as a mechanism to protect certain organizational processes. In cases where certain organizational units are unable to carry out activities and thus place themselves in a situation of becoming a security vulnerability, this approach could provide additional security measures for a predetermined period of time. This type of control could be considered as the highest level and would only relate to processes that have proven to be vulnerable when assessing risk. Adopting emergency security controls would allow for faster response and would target a smaller target since they can only be adapted to one process as opposed to the previous approach in which controls are divided organizationally or by categorization of networks and processes.

We can also look at emergency security controls as a complement to process or system-dependent security controls. They could also be set up as a set of predefined controls that are only valid under certain conditions or within a specified period of time. Although all this can be achieved by establishing a well-known control system, by making precise provisions for each individual system or process, they would make such a large set of controls that, in the case of generalization, would be violated with itself. Therefore, we suggest that in addition to the already known system of security controls, it should be supplemented with controls depending on the process and the system and with a defined time period or activity that activates them.

Application of emergency security controls

We can see the application of this approach to security management during emergencies. In the event of an emergency, controls in the already prepared set should come into effect and not used until then. For example, let us say that at level 6, human resources control does not, in normal situations, contain specifically defined provisions on the prohibition of access to facilities with critical ICT systems. Should an emergency response event occur, an emergency plan should be in place. An Emergency Plan is a plan of measures that an organization must take to respond, reduce the consequences, or prevent hacker attacks. This applies exclusively to the operational part and covers strictly prescribed activities that must be fully complied with. But what about policies and security controls? They remain unchanged in this situation. Emergency controls should focus on access policies, ensure smooth operation, but at the same time tighten employee access.

During the period of validity of emergency security controls, they should be revised and their applicability checked in real-time. This approach would require a team of internal auditors to conduct an internal audit on the applicability of emergency provisions at predetermined periods of time. The same could be done through checklists.

System Control via Check Lists

Checklists are a tool to quickly and easily determine whether work processes are in accordance with the requirements. By using this tool, the examiner can prove in a very short time whether the processes are running smoothly. Controlling the network's operating system through a checklist requires constant updating and alignment of checklist issues with security requirements. For example, in the case of a high-level security checklist, the checklist should be filled in as short a time interval as possible and the width of the questions should be as narrow as possible. This means that any question that is put in the checklist must be directly question-free.

Good control and information gathering through checklists:

- The speed of collecting more information
- Possibility to set the pitch
- Possibility of changing issues with each internal control
- Broad-spectrum of interviewees (from technical to other staff)
- The ability to use data from checklists as a

data source to modify or supplement security controls

Poor control and information gathering via checklists:

- The accuracy of the information obtained
- Professional qualifications of respondents to answer questions of expert nature
- The accuracy of the data from the checklists as a data source for the risk assessment methodology
- Disclosure of matter by the examiner (resulting in a bad question, which leaves the possibility for the wrong answer of the interviewee)

From the above, we can see that the checklists can be used to check in a very short time interval the possibility of implementing the set of ICT security controls. Based on the checklist, it is possible to conclude that further adaptation of a certain level of security controls to the system is required.

Information systems audit

Audit of information systems represents the process of checking the success of information systems in accordance with business requirements, ie the process of analysis and verification of their accuracy, efficiency, efficiency, and reliability. It is a collection of complex management, auditing, and technology activities that examine (check) the effects, but also the risks of using information systems and ultimately evaluate their impact on business.

This is a complex process of collecting and evaluating evidence that can be used to assess the success of a business information system, whether to determine whether a business information system is in the function of asset retention, whether data integrity is maintained, whether it is effective to achieve business goals and use are the resources of the system in an effective way.

An information system audit is a systematic process for assessing whether IT complies with business operations to what extent it effectively and effectively supports the business objectives and the practice (maturity) of management and control of information systems at various hierarchical levels.

The audit information system is systematically and thoroughly inspecting controls across all parts of the information system, and the basic task is to evaluate its current state (maturity, performance level), detect risk areas, assess the level of risk, and give recommendations to management to improve its management practices.

Combining all the steps from above and making them meet the requirements of a specific organization, we will make sure that our controls are put in such a manner that will be effective and in time. The only thing left to do is making sure that our personnel is appropriate for tasks they are assigned for.

Conclusion

Given that the use of security controls is governed by regulations and international standards, practice shows that the benefits they provide are very rarely fully utilized. The globalization of IT systems and the pursuit of business activities in the virtual world increases the risk of information alienation or attack on systems. The use of security controls covers almost the entire organization and increases confidence in the system. However, as with other branches of the economy, the development of an IT system requires the development of a security system, and therefore a further modification of security controls that must at all times justify its reason for being.

Introducing emergency security controls can contribute to improving the security system and improving management's handling of the security system, which gives us an increased dose of confidence in an age when nobody is safe online.

Bibliography

[1] EUROCONTROL Manual for National Security Oversight 03 October 2013
[2] Frameworks for audit of an information system practice Dalibor Drljača Branko Latinović JITA 6(2016) 2:78-85
[3] Industry Consultation Body - Industry Developments in Cybersecurity October 2016
[4] The Complete Guide to Cybersecurity Risks and Controls: Anne Kohnke, Dan Shoemaker, Ken E 978-1-4987-4057-9

Submitted: October 20, 2019
Accepted: December 4, 2019

About the authors

Ivo Džakula was born on March 4th, 1989 in Čapljina, Bosnia and Herzegovina. A joint master's degree program at the Faculty of Information Technologies of Pan-European University "Apeiron" in Banja Luka in 2014. He is currently a doctoral student. Adress: Čeljevo BB, Čapljina 88300, BiH
Phone: +387 (0) 63739688, dzakula.ivo@gmail.com

Branko Latinović was born on April 28, 1956 in Prijedor, Bosnia and Herzegovina. He graduated from the Faculty of Economics in Banja Luka in 1980. At the same faculty he enrolls a master's degree that ends in 1994, and in 1997 successfully defended his doctoral dissertation. She works as a dean of the Dean of the Faculty of Information Technologies of Pan-European University "Apeiron" in Banja Luka.

For citation

Džakula I., Latinović B., Reduction of Ict Security Risks Using Level Based Approach, *JITA – Journal of Information Technology and Applications Banja Luka*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 2:99-105, (UDC: 006.3:[004.738.5:316.774), (DOI: 10.7251/JIT1902099DZ), Volume 9, Number 2, Banja Luka, december 2019 (49-128), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004