Gradus Vol 8, No 3 (2021) 172-178
ISSN 2064-8014

# DOMINO EFFECT AND OTHER MODELS IN THE IT PROCESS

*Krisztina Győrffyné Holló [1*], Adam Karisztl [2]*

[1] University of Pannonia, Veszprém, Hungary
[2] Magna Exteriors Ltd., Banbury, United Kingdom (Magna International Inc., Canada)

https://doi.org/10.47833/2021.3.CSC.005

***Keywords:***
IT Risk identification
Analysis
Methods
Risk treatment
personal data breaches

***Article history:***
Received 10 August 2021
Revised 13 October 2021
Accepted 25 October 2021

***Abstract***

*Based on the information security principles, it is essential to manage the risk of the information systems that collect, store and manage personal data. It can be existed many models and methods for risk identification, analyzing and evaluation, which ensues from each other and often evolving together with information technology. The present research aims to answer whether accident and risk management methods are suitable for identifying, analyzing, and mitigating information security risks.*

## 1 Introduction

Risk management is a proactive method to reduce security risks and improve security performance. Effectively implemented risk management is documented, process-based, and facilitates safe operation. Most industries support the process and application of IT risk management because reducing the IT risks, such as decreasing the number of the safety gap, IT system fails and human error indirectly way improve productivity and profit. The purpose of IT risk management is to minimize residual risk. The relevant aspects of IT Risk Management: Assessment, such as Identification, Analysis, Evaluation and Treatment, furthermore Control, or Communicate, Deliberate, and Documentation. This study presents the relevant risk management methods and models and the practical significance which highlight the potential vulnerabilities, threats, and the necessary security gap treatment of a company.

## 2 The relevant Risk Management models

The risk management process runs until the minimum level of IT risk is reached. It is not the purpose of IT risk management to identify all circumstances and influencing factors but to strive to detect the most potential threats or sources of danger. In IT risk management must take into consideration the input processes, which are affecting the organization, the resources that the system uses to perform the processes and operations, the environmental impacts and relationships, which impacts from outside the system and all of which determine

- the potential threats of organization and potential emergency level,
- occurrence probability of adverse effects,
- level of IT interruptions (abnormal system downtime, service outages),
- recovery cost,
- effectiveness of IT audit.

The type of required action can be a preventive, detective and corrective. The choice of the measuring types depends on the incident, and the applicable general principles and methods should be considered. The extent of cyber-attack can be different. The damage can be industrial or economic, or personal data breaches as well. There are several ways to investigate the causes of an incident, its process and possible outcome. Because the most incidents are complex, several

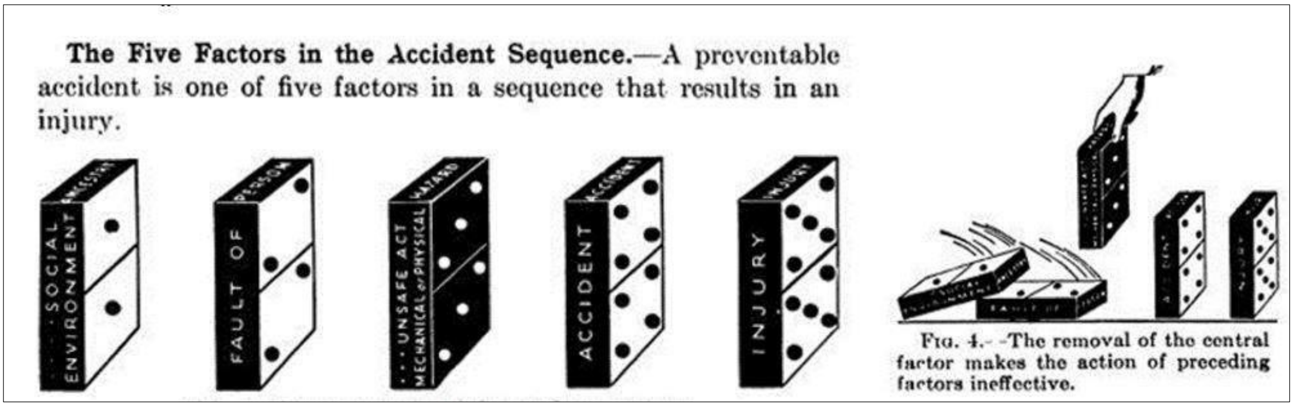
[*] Author. : gyorffy.kriszta@gmail.com

methods are needed to analyze them. During each analysis, it must consider the used tools and methods. The introduction of a new model does not mean that the old ones are obsolete, but rather only an improved version of them is more suitable for the task. Used principles and methods complement each other.

Each IT risk management is unique, includes a unique inventory, potential vulnerabilities and threats, incidents and actions. The listed methods help us to determine the IT risk as exact as possible.

In IT Risk Assessment the following models and methods needs to be considered:

- Security models that set up some hypotheses, which are included the security features (industrial, IT and national security) and assumptions that can contribute to increasing system security.
- Accident models are a set of accident hypotheses that record the principles and the occurrence methods, such as the Seveso directive. One of the foundations of accident models is the simple, random, sequential model, the domino model of H. W. Heinrich, of which are essential factors that the accident derives from a series of mechanical events that occur in a specific order and an accident can be prevented by removing one of the determinants of the domino series.



**The Five Factors in the Accident Sequence.**—A preventable accident is one of five factors in a sequence that results in an injury.

FIG. 4.- -The removal of the central factor makes the action of preceding factors ineffective.

*Figure 1. H. W. Heinrich, Accident sequence, 1941*[1]

The domino effect principles can be applied well in IT risk management because we can choose the potential weak point and the vulnerability. Improving vulnerabilities reduces the number of incidents that exploit vulnerabilities. During the cyber-attack, the hackers do not find a gap just a closed-door at a corrected place. The advantage of the model is simple and easy to see, understand and allow the identification of the relevant causal factors that contribute to the occurrence of the accident or incident. The domino principle combines with user behavior-based security applications, provides an opportunity to detect the weakest links, possible human errors, faulty human performance.

Based on the domino principle, the following risk, accident factors can be identified, which we can use in IT risk management:

- cause factor (provenance) and social environment (human factor: negligence, stubbornness, greed; undesirable or other disturbing factors),
- personal faults (causing danger due to any human property or behavior, such as violent temper, inconsiderateness or ignorance of safe practice),
- unsafe act, mechanical or physical hazard,
- accident,
- injury.

H. W. Heinrich's other accident model is the "safety pyramid" or "accident triangle", whose theory can be further thought, it can be diagnosed, that reducing the incidence of minor events decreases the likelihood of major accidents.

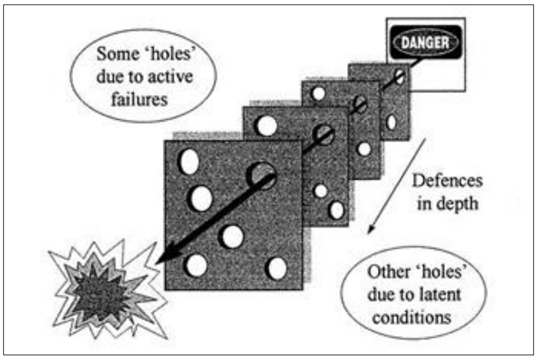

Some 'holes' due to active failures
DANGER
Defences in depth
Other 'holes' due to latent conditions

*Figure 2. Swiss cheese model*[2]

The potential model, according to the Swiss cheese model of James Reason if we assume that the incident is caused by a combination of active faults (faulty safety behavior) and latent environmental factors, and the accident can be prevented by strengthening the limits.

The essence of the method (Figure 2) is that an incident can only occur, if the unwanted attack attempt gets through each "cheese" layer, so all defense systems. Many industries or institutions use this model, such as in transportation (airlines) or healthcare. The defending possibilities are "cheese slices" with holes of different sizes and locations. If possible, "cheese slices" with holes of the same size and location should not follow each other. If this happens, the given layer of defense will not achieve the required effect, and the attack will pass through it. It is necessary to minimize the weak points and vulnerabilities.

As Low As Reasonably Practicable (ALARP) is a risk management framework for principles of the definition of risk reduction. The ALARP framework is used for several decision-making mechanisms or safety systems in the European Union. The criteria are the following:

- Unacceptable range: it is independent of the different activities. (Figure 3)

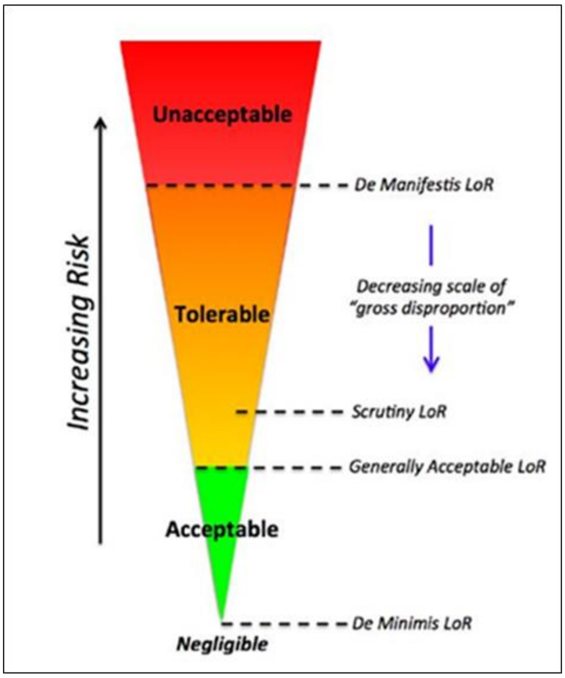


*Figure 3. ALARP principles*[3

- Acceptable ALARP range: the risk is acceptable, but there are some consequences. The proposed risk management should be implemented if the loss is not disproportionately greater than the benefit of implementation. The level of risk should be reduced as much as possible and taking into account to the level of its cost.
- Generally acceptable range: in this case, do not need more risk mitigation method.

## 3 The IT Risk Management in the practice

Our study aims to present the application of information security risk methods. In the risk management, we can use the domino effect, the Swiss cheese model, and the ALARP methods, as well. In the present investigation, the data of risk analysis has been originated in a Hungarian enterprise. In the research, the small-sized company gave the average value of economic, IT and service or product production data that can easier compare to other information security data statistics. Of course, a similar information security study was conducted in large enterprise environments as well as other businesses. In general, IT risk management, which is performed in a large enterprise environment contains confidential business data, so we cannot even refer to it in this publication as a comparison. We can only present our anonymous results. A secondary aspect of our research is to demonstrate that risk management results can show similar statistical results in a large and micro-enterprise environment, in a global and local study.

Before identifying the risks, the inventory of the entire asset, as influencing factors had to be analyzed. The investigated company has many sources of assets, which can be:

- IT system data:
  - servers (5-10), which can be WEB, proxy, file storage, application, database, mail, virtual or physical system,
  - personal computer (10-50), laptop (10-20),
  - routers, switches, racks, cables and other IT devices,
- business documentation in electronic and paper form,
- personal data,
- human resource (10-50),
- physical environment (such as office and server room),
- economic, trade and production data,
- religious and cultural data,
- geological data.

We applied more information security and risk analysis methods (based on ITIL, ISO 31000, ISO 27001, COBIT) in our investigation, whose processes we summarized in the following. Twice a year, we had to

- identify an inventory of hardware and software devices or human error, high-risk areas and potential threats, and necessary activities and training,
- analyze the risk management methods, IT action plan, practices and performances,
- create and apply a safety process for each risk factor, stating the values and practices for each processing,
- use observation techniques to measure safe human behavior and operation or business continuity.
- analyze the results of observation and delivery of feedback, which came from an investigation of IT system and user behavior, user feedback and management control.

Employees were informed of the outcome of action rules weekly and monthly feedback by management. Lists of employee suggestions and actions taken were also posted.

### 3.1 Using the Domino effect and the Swiss cheese model in the IT risk treatment

In our project, the Domino principles can be used as well. With the methods the assets, the causes factors and human factors, as unsafe act, mechanical or physical hazard can be identified. In this case can be analyzed the investigated IT assets, their vulnerability and threats, the effect of the potential incident. If we can estimate the potential incident, its effect and the likelihood of events occurring, we can remove the critical factors.[4] [5] [6] Removal of the critical factor makes the harmful action proceeding factors ineffective. In the risk analysis, it is necessary the number of assets, relevant vulnerability and threats. It has to measure our company resources and devices, such as the number and status of IT devices, data, documents, human resources, potential threats and safety gaps. (Figure 4). We investigated 120 assets which had 550 possible vulnerabilities and threats. Fewer of these, only 110 relevant vulnerabilities and threats were examined.

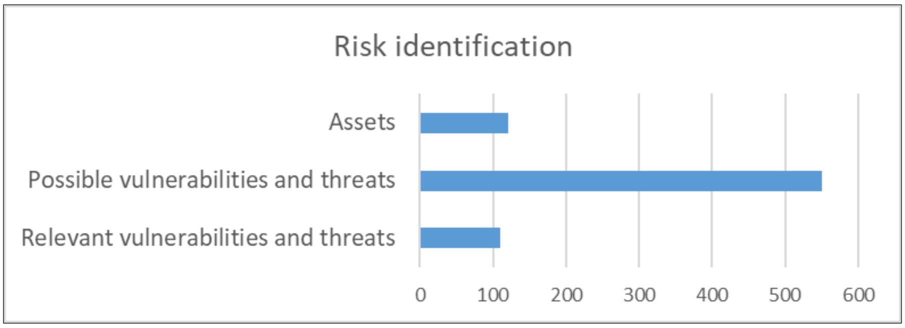


*Figure 4. Risk identification: number of assets, treats and vulnerability (based on own survey, 2020.)*

In examining threats, the threat orientation must be considered, because it may sometimes differ from the subject of damage. Based on the reach, the primary target of the threats is personal data (Human, 79%). The rate of personal data breaches (Social engineering, 59%) shows that its area needs to be better managed. The planned or actual target of the threat can be distinct. Some of the hardware threats effects may be personal data loss. (Figure 5) In this study, the secondary impact factor, such as economic harm or stealing of illegal profit has not been investigated.

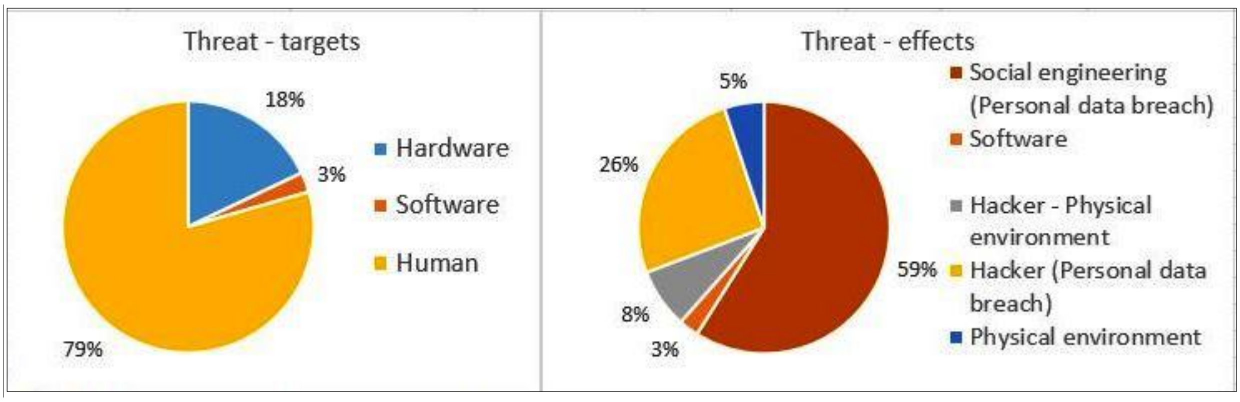


*Figure 5. Threat analysis: a set of the targets and the potential effects (based on own survey, 2020.)*

A Canadian survey (2017) shows that the number of manipulations of personal data (55%) and identity theft is the highest (Figure 6). Both the Canadian survey and our statistics show that personal data is the biggest risk factor, so it is also a top priority among information protection commands.

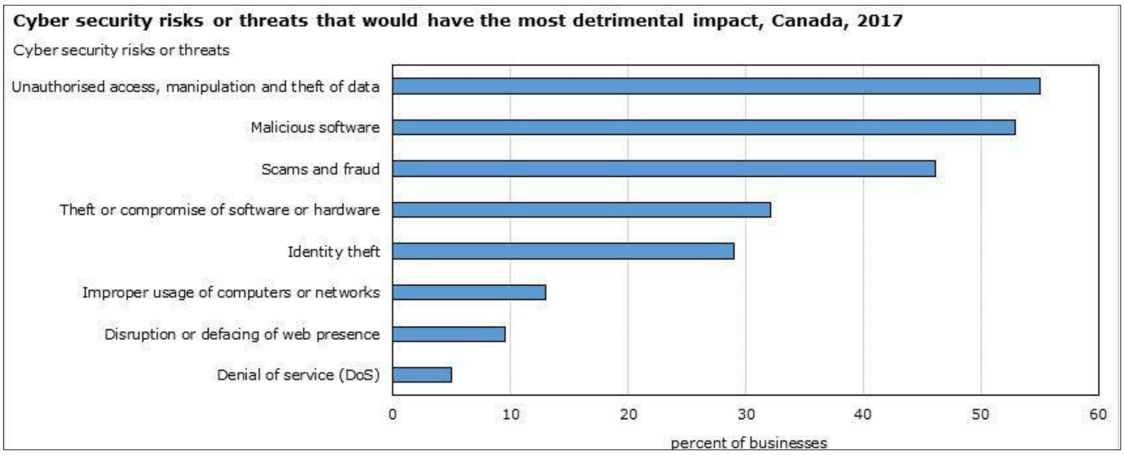


Figure 6. Canadian survey of Cyber security risks or threats [7]

Using the Swiss cheese model, the relevant vulnerability and impact can be selected and analyzed easier, and the weak point can be detected and removed more effectively. The potential weak point can be human error, fault code in the software or material defect of cable as well. With the implementation of the action plan, which includes the system audit, training of employees, and corrections of physical and software faults, the safety gap can be close on the „cheese" layer. The following figure shows that human factors have taken place in the focus of risk treatment. (Figure 7)

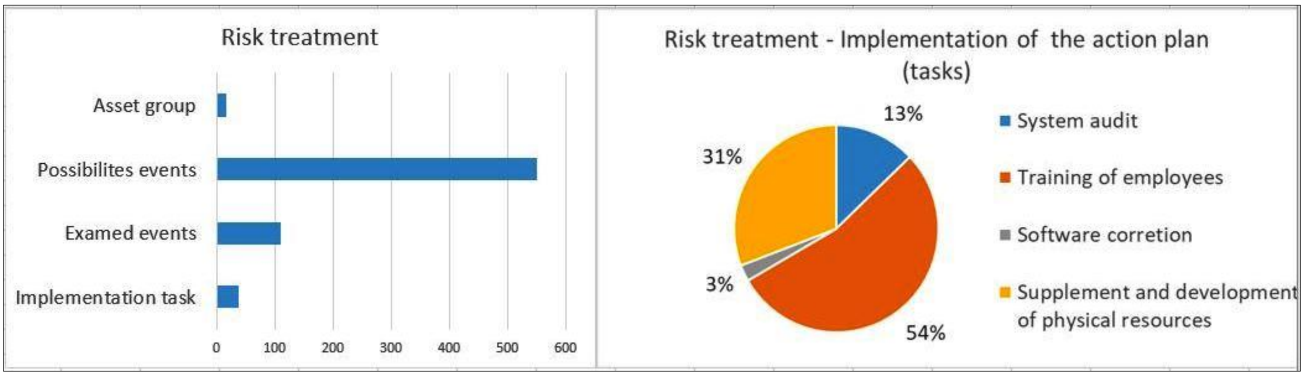


*Figure 7. Risk treatment: detecting the relevant events (number of investigated assets group, evens and tasks) and type of action plan tasks (based on own survey, 2020.)*

In the action plan, we highlighted the processes and conditions that need to be corrected. During the risk management, we removed or strengthened vulnerabilities that have weakened the security of the information system, such as old and faulty applications, more access controls: checking password strength, connecting own IT devices to the internal network. We had to strengthen the security zone (tightening the server room access rules), hard the security backup and data storing rules, apply software development version control (3%) and data access control and raise IT and GDPR awareness with employee training (54%). The purpose of this publication is not to detail the action plan. Implementation of the risk treatment tasks contributes to reducing faults factors, which can make ineffective the harmful action.[8]

### 3.2 Risk acceptable

In the IT risk process, the „Acceptable" of risk value is essential and its diagnosis it has to need more data. In this case, the tests and analysis originated from period 2016 and 2020, and we compared them with several information security statistics from around the world. The ALARP method has been used in the acceptance of the IT risk. Over the „De Manifest LoR" value of IT risks have to be treated. Based on the decision of the lead auditor, some of the relevant incident factor have to be treated, whose values of risk fall between the „De Manifest LoR" and „Generally Acceptable LoR" but they had „Tolerable" value. The risks, which had a value of „Tolerable" 10 or between 6 and 9, were presented separately. The lead auditor and management are also responsible for accepting value at risk and residual risk (20 of the 39 implementation tasks had a residual risk of between 10% and 19%). (Figure 8)

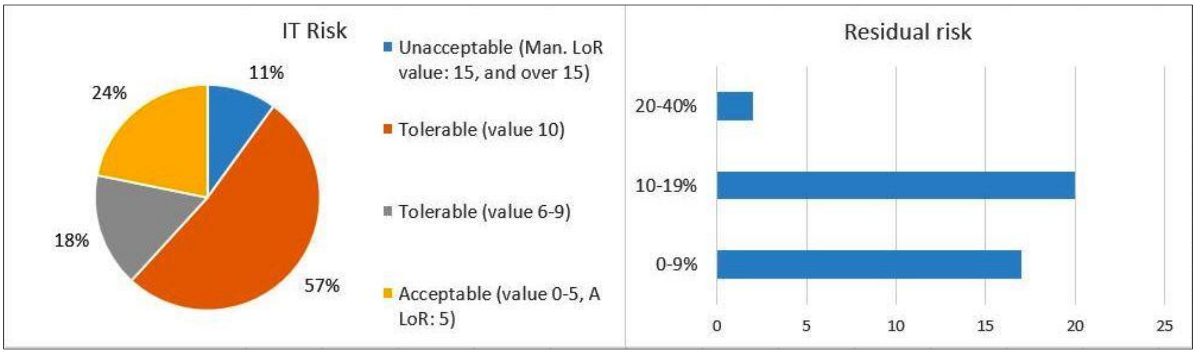


*Figure 8. IT Risk treatment and residual risk (based on own survey, 2020.)*

The result of the study is unequivocal. The information security risks could reduce by applying the information security risk methods, the incident simulation, action plan implementation, and tasks and security awareness instruction. [9, 10] With this method, we could decrease some risks, such as social engineering 20 per cent between 2016 and 2020.

## 4 Conclusions

The choice of the appropriate but specific method is always system-dependent or industry-dependent, because other methods are used by aviation safety, health or public administration. Our research has highlighted the methods, which can be used in many areas based on their principles, thus making their application more popular. The principles and methods that best serve the purpose of their application promote effective information security risk management, save costs for the organization because they also reduce the likelihood of incidents occurring and indirectly increase the level of security of the information system.

The results of the risk management research have highlighted that the presented methods and models are not only well-known, but they are well applicable to the analysis and management of information security risks. However, it has to be emphasized, that in the research of IT risk management selected events are significant in the aspect of the company's business continuity. In general, based on the business aspects, the relevant and treating events are selected, which can be subjective as well.

In our research, we published that the Domino effect, the Swiss cheese model, and the ALARP principles can be applied to the risk management of information systems. With mentioned methods, we applied more solutions, such as we closed the harmful, IT processes and developed the user safety awareness with advanced studies, which significantly reduce the IT risk.

## References

[1] H.W. Heinrich, Industrial Accident Prevention, A Scientific Approach, Second edition, McGraw-Hill Book Company, New York and London, 1941.

[2] J. Reason, Managing the Risk of Organizational Accident, Routledge, 1997.

[3] Reece A. Clothier, Brendan P. Williams, Neale L. Fulton, XunGuo Lin, ALARP and the Risk Management of Civil Unmanned Aircraft Systems, 2013.

[4] Hadarics K, Leitold F, Improving distributed vulnerability assessment model of cybersecurity, Central and Eastern European e|Dem and e|Gov Days 2018 : Conference proceedings, Wien, Ausztria : Facultas Verlags- und Buchhandels AG, (2018) pp. 385-394. , 10 p., 2018, DOI: 10.24989/ocg.v331.32, https://doi.org/10.24989/ocg.v331.32

[5] A. Arrott, A. Lakhotia, F. Leitold, C. LeDoux, Cluster analysis for deobfuscation of malware variants during ransomware attacks, 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 11-12 June 2018, Glasgow, UK, DOI: 10.1109/CyberSA.2018.8551432, https://doi.org/10.1109/CyberSA.2018.8551432

[6] F. Leitold, K. Hadarics, E. Oroszi, K. Győrffy, Measuring the information security risk in an infrastructure, In: Fernando, C Colon Osorio (szerk.) MALWARE 2015 10th International Conference on Malicious and Unwanted Software, Piscataway (NJ), Amerikai Egyesült Államok : IEEE (2015) pp. 93-100. , 8 p., DOI: 10.1109%2FMALWARE.2015.7413689, https://doi.ieeecomputersociety.org/10.1109/MALWARE.2015.7413689

[7] Cyber security and cybercrime challenges of Canadian businesses, 2017, https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.htm, download: 30 October 2020.

[8] K. Győrffy, F. Leitold, A. Arrott, Individual awareness of cyber-security vulnerability - Citizen and public servant, In: Hansen, Hendrik; Müller-Török, Robert; András, Nemeslaki; Pichler, Johannes; Prosser, Alexander; Scola, Dona (szerk.) Central and Eastern European eIDem and eIGov Days 2017 : Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?, Wien, Ausztria : Austrian Computer Society (2017) 597 p. pp. 411-421. , 11 p., DOI: 10.24989/ocg.v325.34, https://doi.org/10.24989/ocg.v325.34

[9] H. K. Győrffyné, Információbiztonság, avagy incidens kontra biztonságtudatos viselkedés, INFOKOMMUNIKÁCIÓ ÉS JOG XVIII., 76., pp. 17-23. , 7 p. (2021), https://infojog.hu/portfolio-item/76-szam-2021-augusztus/

[10] H. K. Győrffyné, The Human Factors of the IT Risk Management, DUNAKAVICS 9 : 7 pp. 47-61. , 15 p. (2021), http://dunakavics.uniduna.hu/Online_20217.pdf#page=47