# Security Aspects of Healthcare Organization from the Perspective of Digitization of Facility Management

LUKÁŠ PAVLÍK
Department of Computer Science and Applied Informatics
Moravian Business College Olomouc
tř. Kosmonautů 1288/1, 779 00
Olomouc
CZECH REPUBLIC
lukas.pavlik@mvso.cz

EKATERINA CHYTILOVÁ
Department of Management and Marketing
Moravian Business College Olomouc
tř. Kosmonautů 1288/1, 779 00
Olomouc
CZECH REPUBLIC
ekaterina.chytilova@mvso.cz

JARMILA ZIMMERMANNOVÁ
Department of Economics
Moravian Business College Olomouc
tř. Kosmonautů 1288/1, 779 00
Olomouc
CZECH REPUBLIC
jarmila.zimmermannova@mvso.cz

*Abstract:* - Many healthcare organizations are exposed to various cyber threats. The increase in the frequency of these cyber threats can also be observed during the Covid-19 pandemic. The security of information systems in hospitals and their management is also not part of the management of facilities in these organizations. The paper presents the possibilities of securing facility management processes in healthcare organizations from a security point of view. There is an analysis of security aspects of a particular medical facility and its information system with emphasis on the application of regular facility management. Analysis and evaluation of tools for ensuring the security of the hospital information network is also applied. The contribution of the paper is the identification and expression of the correlation between cyber threats and the following modules of the information system in the medical facility. Another part of the proven research compares safety mechanisms and their possible failure in a selected hospital. The main research results, which are based on the evaluation of safety aspects in these organizations, can be further used as a platform for the effectiveness of processes in healthcare and thus increase synergies between safety levels and ensure facility management processes.

*Key-Words:* - facility management, security, information system, analysis, module, healthcare, tool

## 1 Introduction

Nowadays we have seen a rapid increase in cyber attacks in healthcare organizations. In the health sector, more technical equipment, software and applications are being used to improve the quality of healthcare. While this aspect moves the capabilities of current medical organizations more forward, it brings new risks and vulnerabilities that potential attackers can take. In many healthcare organizations, safety is only one of the other parts of management that needs to be ensured. For this reason, in most organizations, cyber threats and their prevention are not adequately addressed. This

creates more vulnerabilities in the information environment of hospitals, which are potential attackers for breaches of information system security. Most healthcare facilities are directed to digitizing their processes and procedures. The facility management also began to respond to this fact, where research had to focus on the development of new applications and software tools. Security management is also part of facility management, whose procedures should also be digitized and integrated into the organization's management [1,5].

Many healthcare organizations are targeted by attackers mainly because of disruption of their activities and information system. For this purpose, various types of cryptoviruses are used, which primarily have the task of encrypting data that can be decrypted (but not necessarily) upon payment of the ransom. The second motivating factor that can lead to targeted attacks on hospitals and their information environment is the acquisition of sensitive personal data. Healthcare organizations collect large amounts of personal data relating primarily to patients, employees, etc. Obtaining such sensitive data can be particularly beneficial to attackers in trading this data and selling it to other subjects [2,12].

The area of facility management is also related to the issue of ensuring cyber security. Given the ever-increasing digitization in healthcare, it is also necessary to adapt to developments in facility management from the perspective of ensuring facility management processes. This brings new challenges in this area that should respond to current trends. It is primarily the interconnection of different approaches and processes that take place in healthcare organizations into a user application, the use of which enables selected employees to better coordinate and manage important areas in the organization, including security. The aim of the research is to identify and evaluate key areas of the selected health information system, which are designed to ensure the protection of significant tangible and intangible assets. These assets are necessary protection against the effects of cyber threats that can be targeted at the information system of the medical facility [2,3,16].

# 2 Problem Formulation

To analyze and evaluate the digitization of facility management in the healthcare sector, the EFAS information system was used as a model example. This information system and its modules were solved within a professional project, in which all authors of this paper were involved.

The task of this project was primarily an economic evaluation of the usability and efficiency of the proposed modules of the information system with regard to ensuring activities and processes from the perspective of facility management. The EFAS information system consists of the following modules:

- registration module,
- agenda module,
- common basis functionalities [4].

## 2.1 Registration module

The registration module enables to record the physical form of premises, buildings, floors, roofs, rooms, outdoor surfaces, utilities and similar types of elements. These elements can be considered as location. As a locations are then, in the context of EFAS control, they are required and offered [4].

It is also possible to record technological equipment - typically TEB and similar technologies. Basis evidence is a technology tree, lists and technology cards. The registration module also displays an integrated list of instrumentation containing information on the registration the status of the instrument, the status of legal inspections or the existence of mandatory documents in the annexes [4].

## 2.2 Agenda modules

Agendas are specially programmed function circuits that can be applied to EFAS data. Typical agendas at EFAS are recurring activities and repairs, requisitions, orders, liquidation of invoices and CAD visualization. Agents are typically applied to particular atoms or at least in conjunction with specific atoms.

Agendas are presented in EFAS:

- custom panels in menu,
- lists on the tabs of the main window under, the selected atoms,
- context buttons [4].

## 2.3 Common basis functionalities

The third module of the EFAS information system contains a comprehensive user rights system. Users log in to the application, the user has a link to list of employees (can be a specific employee of the organization) and the user has been assigned a specific one role in the system. When logging in to

EFAS, the user selects the role under which he or she wants to work in EFAS [4].

After logging on to the user and role, the rules and competency scheme apply. The user is shown a menu with items to which they have permission and he only sees (changes) inserts into log windows and agendas. The competency scheme also contains competency settings for series of orders, requisitions, invoices, individual repetitive activities and repairs [4].

Based on the analysis of the modules in the EFAS information system, an assessment of these modules in terms of possible security threats will be performed in the second part of the research. To determine the impact of cyber threats on the organization's information system and its modules, selected risk analysis methods were used. A scale of 1 to 5 was used to determine the significance of modules that are considered here. The value 1 represents the least meaningful modules and 5 the most important modules.

For the purpose of modeling the impact of selected cyber threats on information system modules, ten possible types of threats were identified. These cyber threats could have very serious impacts for the information system of a medical facilities.

A risk matrix has been developed from the available data to illustrate the degree of cyber risk of the modules. The final step was to create the risk analysis table which illustrates the probability of a cyber threat to the module and the impact of that threat on the module. These results were obtained on the basis of the following mathematical calculation.

$$R = PI \times T \times H \quad (1)$$

R……risk
PI……probability
T……value module
H……module vulnerability

## 3 Problem Solution

The aim of this analysis is to determine the vulnerability of modules in the EFAS system to selected cyber threats. For this purpose, ten most common cyber threats with which organizations are threatened were selected.

Table 1. Identify organization parameters and determine their significance

| Module | Module value |
|---|---|
| Accounting modules | 4 |
| Agenda modules | 3 |
| Common basis functionalities | 3 |

As part of this research, an evaluation of selected cyber threats that may have significant impacts on health information system modules was also performed. The cyber threats and their severity are shown in the following table.

Table 2. Identification of cyber threats and their values

| Cyber threat | Probability of the threat |
|---|---|
| Ransomware | 5 |
| Hacking | 5 |
| Unauthorized access | 4 |
| Malware | 3 |
| Data leak due to employee negligence | 4 |
| DDoS attack | 3 |
| Lightning strike | 1 |
| System failure | 1 |

The next step is to create a table showing the impact of cyber threats defined by the modules of the EFAS information system.

Table 3. Modules matrix, threats and impact

| Vulnerability matrix | Module | Accounting modules | Agenda modules | Common basis functionalities |
|---|---|---|---|---|
| | Module value | 4 | 3 | 3 |
| Cyber threat | Probability of the | | | |

| | threat | | | |
|---|---|---|---|---|
| Ransom ware | 5 | **3** | **5** | **5** |
| Hacking | 5 | **3** | **3** | **4** |
| Malware | 3 | **2** | **2** | **3** |
| Data leak due to empl. neg. | 4 | **1** | **4** | **5** |
| DDoS attack | 3 | **2** | **4** | **4** |
| Lightning strike | 1 | **2** | **2** | **2** |
| System failure | 1 | **3** | **3** | **3** |
| Unautho - rized access | 4 | **2** | **4** | **4** |

The last part of the assessment of the impacts of cyber threats on the identified modules is the compilation of a risk matrix.

Table 4. Vulnerability matrix

| Vulnera bility matrix | Module | Accounting modules | Agen da modu les | Common basis functiona lities |
|---|---|---|---|---|
| | Module value | 4 | 3 | 3 |
| Cyber threat | Probabili ty of the threat | | | |
| Ransom ware | 5 | **60** | **75** | **75** |
| Hacking | 5 | **60** | **45** | **60** |
| Malware | 3 | **24** | **18** | **27** |
| Data leak due to empl. neg. | 4 | **16** | **48** | **60** |
| DDoS attack | 3 | **24** | **36** | **36** |
| Lightnin g strike | 1 | **8** | **6** | **6** |
| System failure | 1 | **12** | **9** | **9** |
| Unautho - rized access | 4 | **32** | **48** | **48** |

Table 5. Risk rating scales

| **Risk** | **Value range** | **Colour** |
|---|---|---|
| Low risk | 1 to 30 | |
| Moderate risk | 31 to 65 | |
| High risk | 66 or more | |

Table 5 shows the level of vulnerability of particular organizational modules and individual cyber threats. As can be seen, ransomware and hacking are the threats to which the organizational modules are the most vulnerable. It should be noted that these two threats are among the most common problems in organizations that are associated with data leakage or disruption. On the contrary, the registration module is the least vulnerable to the organization's cyber threats.

From the point of view of facility management, it is necessary to implement security in the agenda module and common basic functionalities. The agenda module is focused primarily on logistics operations, such as orders, creation of invoices, etc. In case of limitation of the functionality of this module, the continuity of these operations and activities is also disrupted. This fact then affects the operation of the entire organization. If the creation of orders, issuance of invoices or control of repairs is not ensured, the organization may become insolvent towards its business partners.

In the case of the common basis functionalities module, the impacts caused by any of the selected cyber threats can be even more severe. This module contains broader coverage of areas such as user rights, workflow or employees. In the case of the implementation of some of the cyber threats, individual rights to the information system may be violated in the area of users. This can contribute to the misuse of access to the EFAS information

system, which can be a relatively serious problem in the case of hacking. Acquiring users rights regarding their access to the information system already allows a potential attacker to obtain sensitive data, such as personal information about employees, the organization's know-how, etc.

### 3.1 Elements of protection for the EFAS information system

Based on the performed analysis it is possible to propose security protection that should increase the resilience of individual modules of the information system. From the technical point of view, the functionality of some selected hardware and software elements is necessary for the agenda module. As you can see, these elements are as follows:

Table 6. Elements of protection

| **Elements of protection** | **Present** | **Absent** |
|---|---|---|
| Antivirus | ✓ | |
| Firewall | ✓ | |
| Antispam | | ✓ |
| Antispyware | | ✓ |
| Regular external data backup | ✓ | |
| Strongly secured passwords | ✓ | |
| Electronic signature | ✓ | |

For each listed protection element, it is indicated whether it is present in the information system or not. These elements were selected on the basis of statistics from the Czech Statistical Office. The assessments of the presence or absence of individual elements were applied to the EFAS information system, which is implemented in an unnamed medical facility in the Czech Republic. The elements that are present in this medical facility provide a certain degree of security to a given information system. A risk analysis has also been performed on these elements, which shows various ways of failure or attack of these elements. You can see these failures in the following table.

Table 7. Identified risks or failures and their rating

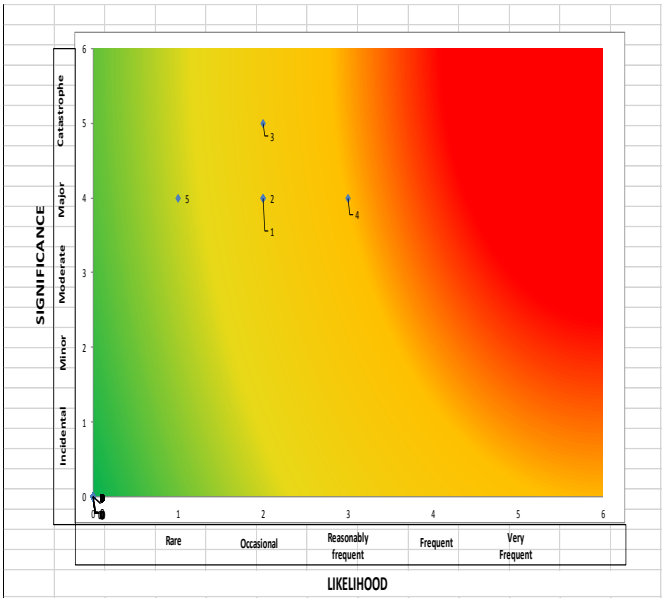
| ID number | Identified risks or failures | Likelihood [1-5] | Significance [1-5] | Fraud risk rating |
|---|---|---|---|---|
| 1 | Inactivity of antivirus system (outdated virus database etc.) | 2 | 4 | 8 |
| 2 | Firewall out of order | 2 | 4 | 8 |
| 3 | Irregular data backup | 2 | 5 | 10 |
| 4 | Weak passwords in the information system | 3 | 4 | 12 |
| 5 | Insufficient security of electronic signature (incorrect encryption, etc.) | 1 | 4 | 4 |

Each of these possible security failures and risks is assessed for probability and significance (or impact). The probability was determined on the basis of a rating scale between 1 and 5, where the number one means the lowest probability and the number 5 the highest probability of realization. Significance (or impact) was also rated on a scale of 1 to 5, where number one means the least significance (almost no harm occurs) and number 5 means the highest significance (major financial damage, long - term damage to reputation, etc.).

In the next step, you can see the heat map of risks, on which you can identify the distribution of individual risks depending on their severity. As you can see, the identified risks or failures number one, two and three are located in the middle level of the heat map of risks. Risk number five is at the lowest level of risk Therefore, these failures do not pose a

serious risk to the EFAS information system. Risk number four is on the borderline between medium and high levels of danger. The implementation of this danger can pose a relatively serious threat to the security of the information system. The effects of this risk can significantly disrupt the basic functions of this system and thus disrupt the functioning of the organization.

Fig. 1 Heat map of risk




## 4 Conclusion

The purpose of this paper was to analyze and evaluate the implementation of information systems in medical facilities from a security perspective. The results obtained on the basis of the application of risk assessment methods show that this is a relatively complex issue, which requires primarily a systemic approach. The EFAS information system, which was the subject of a vulnerability assessment for selected cyber threats, is one of many systems used in healthcare facilities. Based on the risk analysis, which was performed in the research part of our paper, it is possible to state that other influences that are not included here also enter into this process [6].

The result of this process is a representation of the impact of selected cyber threats on the defined modules of the EFAS information system. Based on this analysis, possible security features to prevent these cyber threats and their impacts should be identified. These safety elements were identified and evaluated in the previous step of the analysis, which was focused on the occurrence of these elements in a particular medical facility [7,8].

The biggest benefit of the performed analysis of the EFAS information system is the identification of the impacts of selected cyber threats on the defined modules of the information system. These impacts were determined on the basis of analysis and assessment of information system modules and their interaction with selected cyber threats. The results of this process were further used to identify and evaluate security mechanisms. Based on the expression of the probability and significance of the breach of selected security mechanisms, a temperature map of risks was displayed, which can be used for further steps in ensuring the security of the EFAS information system. Based on the obtained results, it is possible to determine another procedure for assessing the negative impacts of cyber threats on the information environment of the organization, which should include not only technical but also non-technical factors. Obviously, the EFAS information system also consists of intangible parts, which should be included in the risk assessment and determination of the possible impacts of selected cyber threats. These intangible assets include, for example, sensitive organizational data, know-how or personal data about employees. These intangible assets also occur in the individual modules of the EFAS information system and it is therefore necessary to include these assets in the assessment of the security level of the entire information system, which is not usually part of the assessment and evaluation of possible cyber threats and their impacts [9].

Determining the potential impact of cyber threats on this type of assets is very difficult. The biggest problem in this process is the price of these assets. However, a number of factors are involved in the process of determining the price of assets, which at present cannot be precisely expressed financially. This is, for example, the determination of the significance of a given intangible asset with regard to the costs that were necessary for its creation. Possible approaches to this problem can be found in the available literature, and based on the analysis, it can be stated that there are not enough published approaches published, the application of which would bring satisfactory results. Some of these methods or approaches cannot be applied to all types of tangible and intangible assets. In the case of an organization's good reputation, the financial expression of potential damage caused by cyber threats is very difficult. [9,10].

In conclusion, it can be said that the issue of cyber security in health care facilities is gaining more and more importance. The large number of attacks faced by medical facilities in recent times show us that this is a societal problem, the intensity of which will continue to increase in the future. Current developments surrounding Covid-19 can also make a significant contribution to the vulnerability of healthcare facilities and their information systems. This fact is already manifesting itself all over the world. Medical facilities are overloaded due to higher patient intake, which potential attackers can use to carry out a cyber attack. A number of major institutions around the world warn of the increased likelihood of cyber attacks. One such organization is, for example, ENISA (European Union Agency for Cybersecurity) [12,14].

The current methods, which were used to evaluate the impacts of selected cyber threats on the defined modules, represent one of the possible combinations that can be applied to this issue. From the point of view of possible future development of this area, it would be appropriate to create a tool for risk analysis, by means of which it would be possible to determine the impacts on individual technical and non-technical elements of the information environment. These elements can be part of the organization's information system (hardware, software) or are part of the organization's information environment (reputation, etc.) [11,13,15].

*References:*

[1] COVENTRY, Lynne and Dawn BRANLEY. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, Vol. 113, 2018, 48 – 52.

[2] LUCAS, Jason, Tanyel BULBUL and Walid THABET. An object-oriented model to support healthcare facility information management. *Automation in construction*, Vol. 31, 281 – 291.

[3] OLUVERO, Elena et al. E-tools for hospital management: An overview of smartphone applications for health professionals. *International Journal of Medical Informatics*, Vol. 124, 2019, 58 – 67.

[4] BRANDYS, Roman, *EFAS user documentation*, EFA Services Ltd., 2019.

[5] CIARAPICA, Emanuele Filippo, PACIAROTTI Claudia and GIACHETTA G. Facility management in the healthcare sector: Analysis of the Italian situation. *Production Planning and Control*, Vol. 19, 2008, 327 – 341.

[6] AUSTIN, J. Jodie, TARIQ, Amina and SMITH R. Ian, The impact of closed-loop electronic medication management on time to first dose: a comparative study between paper and digital hospital environments, *International Journal of Pharmacy Practice*, Vol. 26, 2018, 258 – 265.

[7] BLYTHE, Robin et al. The impact of closed-loop electronic medication management on time to first dose: a comparative study between paper and digital hospital environments, *BMJ Open*, Vol. 9, 2019, 351 – 358.

[8] CUCCINIELLO, Maria, LAPSLEY, Irvine and NASI, Greta. Managing health care in the digital world: A comparative analysis, *Health Services Management Research*, Vol. 29, 2016, 132 – 142.

[9] SHOHET, Igal, LAVY, Sarel. Facility maintenance and management: a health care case study, *International Journal of Strategic Property Management*, Vol. 21, 2017, 170 – 182.

[10] CHOI, Jong Soo, RHEE, Poong-Lyul, LEE, Woo Baik. Cost-Benefit Analysis of Electronic Medical Record System at a Tertiary Care Hospital, *Healthcare Informatics Research*, Vol. 19, 2013, 205 – 214.

[11] DOWIE, Jack et. al. Towards generic online multicriteria decision support in patient-centred health care, *Health expectations: an international journal of public participation in health care and health policy*, Vol. 18, 2013, 689 – 702.

[12] ALHARAM, K Aysha, ELMEDANY, Wael. The Effects of Cyber-Security on Healthcare Industry, *The 9th IEEE-GCC conference& Exhibition*, 2017, 554 – 560.

[13] BURNS, AJ, JOHNSON, M. Eric and HONEYMAN, Peter, A brief chronology of medical device security, *Communications of the ACM*, Vol. 59, 2016, 66-72.

[14] ZHANG, Meng, RAGHUNATHAN, Anand and JHA, N. K. Towards trustworthy medical devices and body area networks, *Proceedings of the 50th Annual Design Automation Conference*, 2013, 1 – 6.

[15] ILAHI, Latifa, GHANNOUCHI, Sonia Ayachi and MARTINHO, Ricardo. Healthcare Information Systems Promotion: From an Improved Management of Telemedicine Processes to Home Healthcare Processes, *International Conference TEEM 2014*, 2014, 333 – 338.

[16] SHARBAF, Mehrdad, Reengineering Cyber Security Process: A New Perspective on Cyber Security Quality Management, *2019 IEEE Intl. Conf. on Dependable, Autonomic and Secure Computing*, Vol. 1, 2019, 332 – 337.