*Achievements, Milestones and Challenges in Biomedical and Health Informatics*
*J. Mantas et al. (Eds.)*

*doi:10.3233/SHTI220951*

# Cybersecurity Challenges in Healthcare

Ramo SENDELJ[a,1] and Ivana OGNJANOVIC[a]
[a] *University of Donja Gorica, Oktoih 1, 81000 Podgorica, Montenegro*

**Abstract.** Cyber security attacks evidence has shown that many sectors and industries are still at an insufficient level of readiness to counter these threats, including healthcare organizations and the entire healthcare industry. The COVID-19 pandemic has additionally launched the issue of cyber protection of healthcare systems and connected medical and other devices as well as modern IT components, which are often the entry point for attackers against healthcare organizations. With the aim of a systematic approach to cyber security in healthcare organizations, this article comprehensively presents cyber risks and possible consequences of attacks in the context of healthcare organization services, as well as identifies the five most important cyber security challenges and provides recommendations for establishing protection mechanisms in line with best practices.

**Keywords.** Cyber security, cyber-attack, cyber risk management, cyber challenges, health organization

## 1. Introduction

Digital technologies have transformed the healthcare industry, and through the development of modern information systems and the integration of smart devices, it has facilitated communication with patients as well as patient access to treatments. Some of the components of modern information systems that had a significant impact on increasing the quality and availability of health services are: (i) electronic health records (EHR) that replaced paper records and increased the efficiency of health services; (ii) telecommunication networks and services to support communication and cooperation between patients and health workers; (iii) mHealth, telehealth and telemedicine have improved the process of patient management as well as improving the quality of services. However, the application of modern technologies in healthcare has supported the collection of patient data with simultaneous contribution to an increase in the quality of services. On the other side, all actions that include activities over personal data represent a potential vulnerability of the system that can arise either from software vulnerabilities, human error, or security flaws [1].

The Covid-19 pandemic has contributed to the rapid development and general use of digital services in healthcare [1], general remote functioning of the societies, and thus users' efforts on integration of various online components mainly with a deficiency or a low level of cyber protection [4]. Consequently, the growth and diversity of cyber security threats have been followed with significantly increased level of vulnerabilities and cyber risks for health organizations.

[1] Corresponding Author: Prof.dr Ramo Sendelj, University of Donja Gorica, Oktoih 1, 81000 Podgorica, Montenegro; E-mail: ramo.sendelj@gmail.com.

Violations of sensitive health data can occur because of both internal and external threats, and the most common among them are hacker attacks, unauthorized access and disclosure of data, theft, and loss of data, etc. The trend shows a rapid increase in the frequency of attacks, which have increased by 162% in the last three years, which represents over 700 attacks and illegal disclosure of health data in 2021 [2]. When talking about the consequences of such attacks, cyber security violations might have immediate consequences that arise as a direct response to the attack, as well as long-term consequences and intangible costs for the entire business that spread over a longer period of several years.

Cyber security is an obligation and imperative for all actors in the health care, including health service providers, insurance institutions, pharmaceuticals, and biotechnology institutions, as well as companies for medical devices and the production of software and other hardware components [3]. In this context, the basic tasks of cyber protection of health organizations can be defined as: (i) ensuring the availability of health services, (ii) ensuring the proper operation of medical systems and devices, (iii) preserving the confidentiality and integrity of data on patients and services, as well as (iv) ensuring timely response and prevention from external and internal cyber-attacks [4].

## 2. Current statistics and trends

The current cyber-attacks diversity, their scope and impact on healthcare organizations can be described with statistical indicators over cyber incidents that have occurred in the US healthcare system.

Data collected from the period 2016-2022 [2][6], shows that almost 30% of all major cyber incidents aimed on data abuse were targeting healthcare organizations, which undoubtedly lead to the conclusion that healthcare institutions are a very desirable target for cyber-attacks.

Even though healthcare institutions have invested over $65 billion in cyber protection [7], they still face a high volume of cyber-attacks. The number of cyber-attacks is continually increasing and since only those cyber incidents that affect at least 500 people are reported, it can be concluded that the number of cyber-attacks is significantly higher than reported. Table 1 shows the annual numbers of Data Breach Events and Data Records Breached for the period 2016-2022 [2] [6] [7].

**Table 1.** Healthcare Data Records Breached and Healthcare Data Breaches 2016–2022 [2] [6] [7]

| Year | No. of Data Breach Event | No, of Data Breached Records |
|---|---|---|
| **2016** | 115 | 13.429.721 |
| **2017** | 148 | 3.513.380 |
| **2018** | 164 | 9.992.440 |
| **2019** | 312 | 38.429.532 |
| **2020** | 416 | 26.424.309 |
| **2021** | 521 | 43.096.956 |
| **6 months of 2022** | 347 | 20.214.270 |

Cyber-attacks differ in their scope, techniques used by attackers and location of breached data. By extracting the cyber-attacks with the highest number of data records breaches, it can be concluded that 2% of cyber-attacks (10 of 521) in 2021 caused almost 44% (18,993,908 of the 43,096,956) of data records breach. Therefore, even large health organizations as carriers of critical IT infrastructure are the primary target of cyber-attackers, they have a great success in countering the attacks. However, the consequences

of inadequate cyber protection of larger health institutions might have a huge impact on the health system functionality collapse.

Sensitive patient data is usually key resource targeted by cyber attackers, and they are very often stored in different locations in the file system, databases distributed through the computer network, while being copied in certain reports, tables and other files that are attached to emails and other communication messages.

Table 2 shows the number of cyber-attacks related to different locations of compromised patient health data. It is evident that the highest percentage of Breached Data occurred on Network Servers (66.79%) and Email service (27.06%), while a smaller number of cyber-attacks were aimed at Electronic Medical Record and Endpoint devices. A similar trend continued in 2022 [2] [6] [7].

**Table 2.** The Top Healthcare Data Breaches of 2021 by Location of Breached Data [2] [6] [7]

| Location of Breached Data | Network Server | Email | Electronic Medical Record | PC/Laptop | Other |
|---|---|---|---|---|---|
| **2021** | 348 | 141 | 12 | 13 | 7 |
| **6 months of 2022** | 185 | 90 | 37 | 16 | 15 |

Table 3 shows that the largest number of cyber-attacks were caused by "Hacking/IT incident" and "Unauthorized Access/Disclosure", compared to those caused by loss, theft, and improper disposal. The similar trend is relevant for 6 months of 2022 [2] [6] [7].

**Table 3.** The Top Healthcare Data Breaches of 2021 by Location of Breached Data [2] [6] [7]

| Causes of Cyber Attack | Hacking/IT incident | Unauthorized Access/Disclosure | Loss | Theft | Improper disposal |
|---|---|---|---|---|---|
| **2021** | 340 | 142 | 10 | 24 | 5 |
| **6 months of 2022** | 277 | 52 | 4 | 11 | 3 |

## 3. Why healthcare organizations are the biggest target for cybersecurity attacks

The exposure to potential cyber-attacks can be explained by identification of key actors with different motivations for carrying out cyber-attacks, and further understanding of the key malicious drivers for the execution of the attacks. The main motives for carrying out a cyber-attack on the healthcare system/organization are [7]:

- *Wide range of attacks* - due to the connection of medical information systems with medical devices (Internet of Medical Things, IoMT) and other hardware and software components that may have a weak level of cyber protection, as well as connection with external components that have access to sensitive patient data (e.g., telemedicine, mHealth components, etc.), with significantly expanded mass use due to the recent COVID-19 pandemic.
- *High value of personal health data on the black market*- due to the wealth of information about patients stored in patient health records, there are potentially diversified ways for data abuse such as identity theft, illegal actions with insurance companies, etc.
- *High willingness of victims (especially healthcare institutions) to pay large amounts to attackers* in order to release inaccessible data about patients and ensure the smooth functioning of the health services. The unavailability of certain services and/or inaccurate patient data can result in fatal outcomes, so

some of the privacy regulations (e.g., HIPAA[2]) foresee large fines for institutions that violate "privacy, security, breach notification and electronic health transactions" or do not cooperate with the GDPR. Therefore, actors in the healthcare system are obliged to take appropriate measures to prevent leakage of patient data and/or permanent disabling of services.

The reasons why healthcare organizations are targeted by cyber attackers could be found in proper understanding of their specificities and resource characteristics, which can lead to the identification of key system vulnerabilities. The following key reasons can be considered [8]:

1. *High value of sensitive patient data* - patient data has an extremely high value on the black market, making the entire healthcare industry as a high-demanding target for attackers.
2. *Vulnerability of medical devices to cyber-attacks*- Medical devices have a specific medical purpose (e.g., heart monitoring, insulin pumps, x-ray imaging, etc.) and are not primarily designed to meet cyber security requirements. In addition, even medical devices do not contain patient information, attackers can use them as an entry point to the system (on the server) and further malicious use (which does not have to be based only on data theft, but the attacker can in the worst case take control of medical devices and endanger the lives of patients).
3. *Necessity of remote access to confidential data* - medical staff, due to the necessity of teamwork, often have the need for remote access to the patient data and the use of personal devices (smartphones, etc.). This is the reason why only highly secured systems can identify and block access to compromised devices, fully supported by highly trained personnel related to cyber prevention mechanisms, which is often not the case in healthcare.
4. *Unwillingness of staff members to accept modern technologies* – medical staff in health organizations is usually occupied with very specific interventions and other tasks related to health care provision, thus being in lack of time for continuous training in the field of IT. This is the reason why even some more modern IT solutions in everyday business (e.g., Office 365) cannot be used in healthcare institutions, even though being characterised with a significantly higher degree of built-in cyber protection compared to all other solutions. The only way for establishing proper protection mechanisms is to align security measures with existing software which usage is highly experienced by staff members.
5. *Inadequate level of cyber security knowledge by staff members* - medical staff are not educated to recognize potential attacks through the computer network and they are not skilled in how to apply best practices for proper use of IT services. Nevertheless, medical personnel cannot be expected to use cyber security tools, and the only action which can contribute to cyber security of the health organization is in setting up highly secured computer network that is used in an easy and simple way.
6. *Connection of many devices and hardware components to the health organization network* - modern healthcare organizations have a need to connect

[2] The Health Insurance Portability and Accountability Act of 1996 is a United States Act of Congress enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996

many medical devices that collect and/or transmit a large amount of confidential patient data, as well as providing external data access to their staff. External access is often made through personal devices, which further undermines the cyber security of the system as a whole.

7. *Health information sharing as a permanent task* – the emergency medical services have clear requirement of making patient data immediately available and assessable by any device and from any distance location. This means that any security procedures and checks must not cause any waste of time and waiting procedures that could have fatal implications for the patient.
8. *Smaller budgets for security mechanisms in smaller organizations* - large organizations usually have enough resources to provide effective cyber solutions from the market, but they are enriched with a huge amount of patient data and thus being a much bigger target for attackers. On the other hand, smaller organizations are a potential target for attacks due to use of digital technologies, but usually they do not have enough budgets to invest in cyber security.
9. *Outdated technologies from the aspect of unsatisfied modern security standards* – the need for making money savings in operations, health organizations often decide to stop ordering modern updates for implemented technologies. This means that even though the technologies were up to date at the time of ordering, the vendor may cancel services due to untimely upgrades. On the other hand, upgrades are the only way manufacturers improve their products. Also, creating additional layers of security at the network level can be helpful in blocking further access if an attacker gets into a compromised device, thereby denying access to patient data. It is the responsibility of the healthcare organization to protect its computer network.

## 4. The managing cybersecurity in healthcare organization

Cyber security information management includes three basic levels at the level of healthcare organizations that have a clear role in the implementation of cyber security and risk management, as presented in Figure 1 [9].

*Executive level* – responsible for providing information on available resources, as well as performing a periodical assessment of the tolerance level in accordance with cyber risks and defined priorities of cyber protection.

*Level of business processes* - a cyber risk management process is created in accordance with business processes and information received from the executive level, which is further forwarded to the level for implementation and operations. The basic result of this level is the Framework Profile, which is later supplemented with information from the implementation process.

*Level for implementation/operations* - oversees implementation of specific protection mechanisms based on the created Framework Profile, as well as generation of impact assessment results that are forwarded to higher levels. Also, implementation progress and observed changes in vulnerabilities and business risks are entered into Framework Profiles.

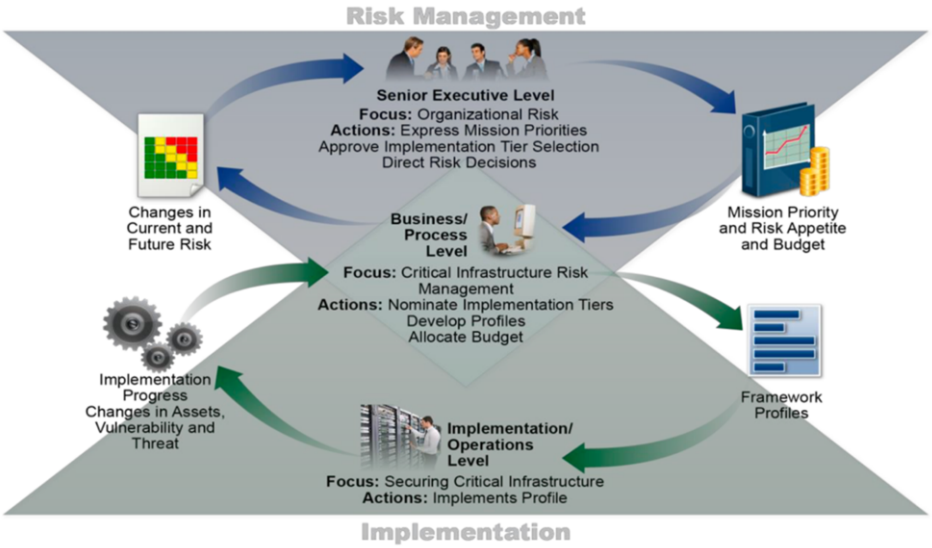


**Figure 1.** Information and Decision Flows within an Organization [9].

## 5. The five most important cybersecurity challenges for healthcare organization

For the adequate implementation of cyber security at the organizational level, it is not enough only to establish a department in charge of cyber security and provision of resources. The imperatives include close cross-sector cooperation in the cyber security industry and a proactive approach in terms of creating responses to increasingly sophisticated cyber-attacks, with rapidly growing varieties and improving approaches. Nevertheless, cyber-attacks on healthcare organizations can be categorized into five categories, which differ in terms of exploited system vulnerabilities, potential consequences of attacks, and protection mechanisms [10]. Recommendations are defined for each of the attack categories, in line with the recommendations in the HICP based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework[3]—the gold standard of cost-effective cybersecurity best practices.

### *5.1. The email phishing attack*

Email phishing is a common type of attack that is distributed in the form of an email with sending address that appears legitimate and known (usually a letter or two difference compared to the correct one) with a mandatory attachment in the form of a file or active link. After accessing an attached file or link, an automatic download of malicious software is made that further downloads files from the computer or a redirection is made to a website that may ask for sensitive information or proactively infect the computer [10].

*Realistic scenario*. Phishing e-mail can be sent to all employees who are in charge of patient billing in the form of a message by the IT department. The message can contain

[3] The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce.

a simple message about the necessity of changing the password for the payment system. If an employee from the billing department enters password data to access the billing system, an attacker will be able to damage the entire system and misuse financial data, as well as patient data [11].

*Impact*. Phishing attacks can serve as a way for attackers to obtain sensitive patient data (e.g., name, date of birth, insurance number, etc.) which can then be misused in terms of impersonation, selling on the black market, and harming healthcare institutions in the system. For example. one reported phishing attack from 2019 showed that by downloading credentials from healthcare workers (who were caught by phishing email), data for over 100,000 patients was downloaded [11].

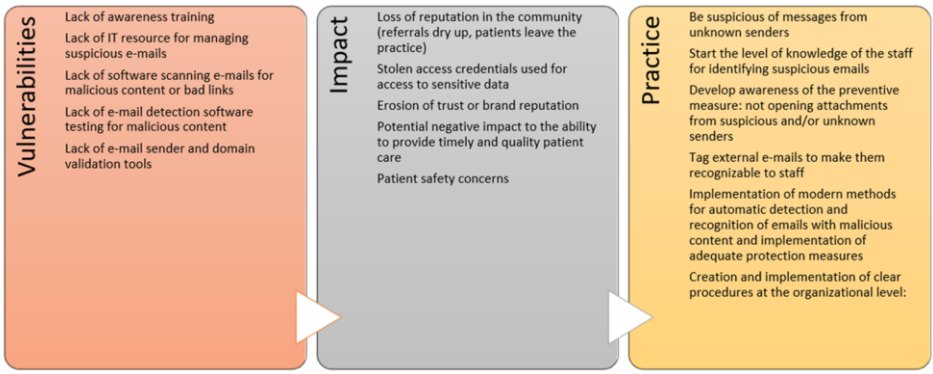


**Figure 2.** Suggested Practices to Combat E-mail Phishing Attacks **[11].**

### *5.2. The ransomware attack*

Ransomware is a type of malicious software (malware) that involves encrypting data and blocking access to the device and/or all its systems, unless the "key" for decryption, known only to attackers, is possessed [12]. This is a method that attackers use to extort certain amounts of money from victims through various types of blackmail. Blackmail usually refers to the public endangerment of the victim's reputation, the complete destruction of information and the deletion of backup copies, and usually the complete inability to recover parts of the system and stored data [10].

*Real Scenario*. When trying to access patient data through the system, a family practice doctor in a small town noticed a complete inability to access the data, as well as other components of the system: scheduled examinations, billing data and other records. In the message, the attackers demanded an amount of 10,000.00e for the “key” needed for access, with no guarantee that it would be delivered. Furthermore, the attackers would not continue to ask for additional money after the first payment is made [11].

*Impact*. These attacks usually have serious monetary losses (especially for small healthcare organizations) because the loss of data causes damage that organizations cannot easily recover from. It is important to point out that although organizations agree to make payments to attackers, this is not a guarantee that the data will be returned. These types of attacks are becoming more and more sophisticated, and the attackers significantly increase the requested amounts mainly because of the value of health data and the imperative to protect the interests of patients [11].

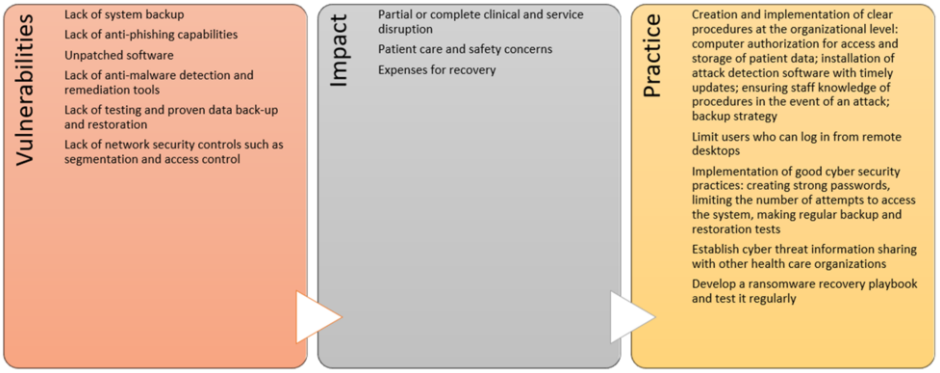


**Figure 3.** Suggested Practices to Combat Ransomware Attacks **[11].**

### *5.3. The lost and theft of equipment or data*

Losing and stealing portable devices (e.g., laptop, tablet, smartwatch, etc.) are integral parts of everyday life that result in the hackers getting into their possession. Thus, device owners do not only have this loss, but hackers, if they manage to access the devices, can further use them to lock up systems and cause large-scale damage both for this individual (device owner) and for organizations and systems [10].

*Real Scenario*. The family practice doctor stopped in the cafeteria to order a coffee and during the break he checked the results of the patient radiology reports which did not arrive during the morning shift. A public Wi-Fi network is available in the cafeteria, through which the doctor used a Virtual Private Network (VPN) to review radiology reports. The Doctor got up to collect the coffee, but upon returning to the table he noticed that his laptop had been stolen [11].

*Impact*. The loss of sensitive patient data can lead to a large-scale loss that directly tarnishes the reputation of the organization and the doctor, and can lead to the identity theft of all patients (e.g., in 2019, 572 security incidents were reported and a total of 41.1 million patient records were stolen) [11].

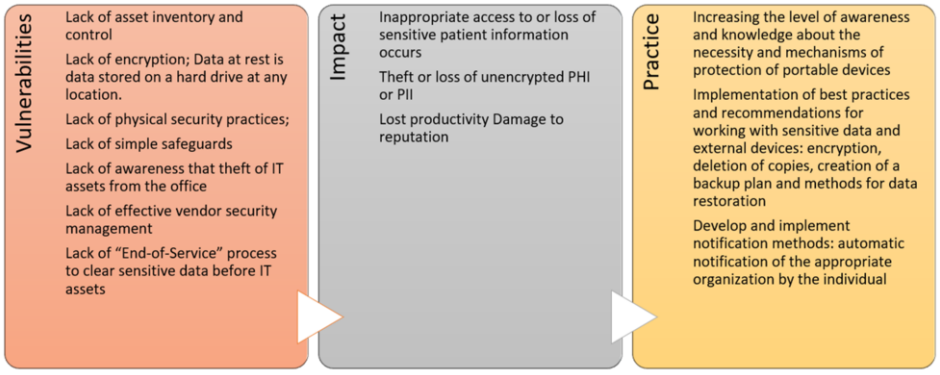


**Figure 4.** Suggested Practices to Combat Lost and Theft Equipment or Data **[11].**

### 5.4. The insider, accidental or intentional data loss

Insider threats exist in every organization where employees, associates and users have access to the IT system and/or its parts. Depending on the intent and awareness of the actor during the activity that causes the cyber-attack, malicious and accidental attacks are distinguished. Accidental attacks occur because of unintentional information sharing, procedural errors, or negligence. On the other hand, malicious insider attacks are the result of malicious intentions by an employee, associate, or user with the aim of personal gain or harm to the organization and/or other individuals/organizations [10].

*Real Scenario*. An employee with access rights to patient records makes random copies of patient data from the system. After enough copies, the employee tries to gain financial benefit by selling the data through the dark web [11].

*Impact*. Whether accidental or malicious, insider attacks can have serious consequences for patients, healthcare services and organizations. Also, this type of attack can be realized in a short period of time and immediately show consequences, while it can continue continuously for a long-time interval [11].

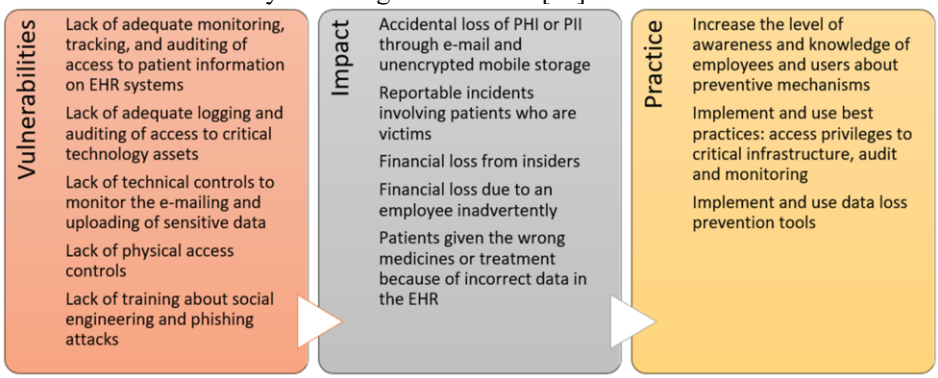


**Figure 5.** Suggested Practices to Combat Insider, Accidental or Intentional Data Loss [11].

### 5.5. The attack on connected medical devices that may affect patient safety

The Food and Drug Administration (FDA) defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them; intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease." If they are compromised, these devices can be used as an entry point into the computer network of a healthcare organization, which can further lead to misuse of data, malicious change of actions and results on the devices, which can even have fatal consequences for the patient [10].

*Real Scenario*. The attacker first carried out a phishing attack and entered the healthcare provider's system. In the system, a file with heart monitoring data was accessed, the control was taken over them (i.e., corrections over data are made) and incorrect heart data are displayed for all patients in the Intensive Care Unit (ICU), which potentially endangers the lives of most patients [11].

*Impact*. Medical devices are often of vital importance for patients, and the disruption of their operation can have direct consequences in the form of health impairment or even

fatal consequences. Furthermore, this significantly undermines the health organization's reputation [11].

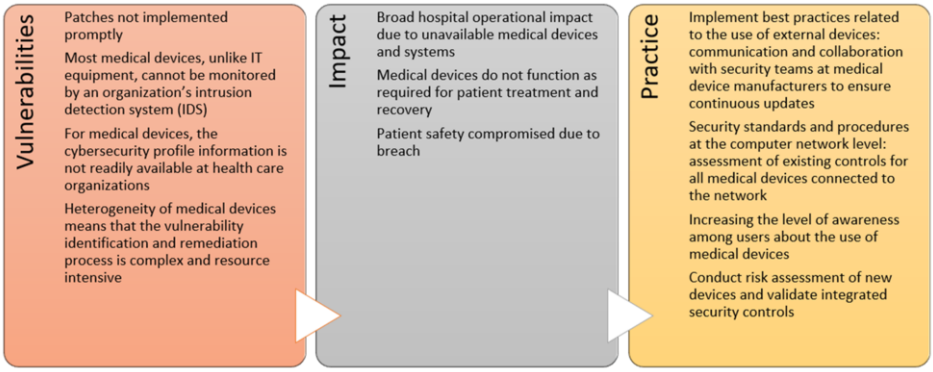


**Figure 6.** Suggested Practices to Combat Medical Devices that May Affect Patient Safety [11]

## 6. The best technical practice to mitigate cybersecurity threats in healthcare organizations

The presented practices for combating various types of cyber-attacks include the entire range of mechanisms, from the level of policies and procedures defined at the level of the organization, over the development of good cyber hygiene and ensuring an adequate reaction of the personnel of the health organization, to the implementation of technical practices and recommended protection mechanisms. It is important to emphasize that the implementation of technical practices alone is not enough, but continuous evaluation and assessment of risks in accordance with technical practices is crucial for the prompt improvements of an organization's cyber security posture.

Comprehensive instructions for the implementation of technical practices are provided in the HICP publication[4], which categorizes health organizations by size (small, medium, large), also corresponding to the level of critical functions for the health system performed by these organizations. Furthermore, depending on the size of the organization, it is possible to typically define subsystems that are interconnected to ensure the functioning of the system as a whole, as well as the amount of sensitive data that is stored [11].

Technical practices are defined comprehensibly for technically educated personnel in healthcare organizations and include the ten most effective groups of practices (defined in accordance with the CSA 405(d) Task Group): E-mail protection systems; Endpoint protection systems; Access management; Data protection and loss prevention; Asset management; Network management; Vulnerability management; incident response; Medical device security; Cybersecurity policies; which are further divided into corresponding Sub-Practices (a total of 88 sub-practices depending on the size of the organization and the application of the evaluation methodology) [11].

Figure 7 shows an example of the practices and sub-practices for medium healthcare organization, with further implementation recommendations available in the HICP publication [11].

[4] Health Industry Cybersecurity Practices: Managing Threats and Protecting Patient

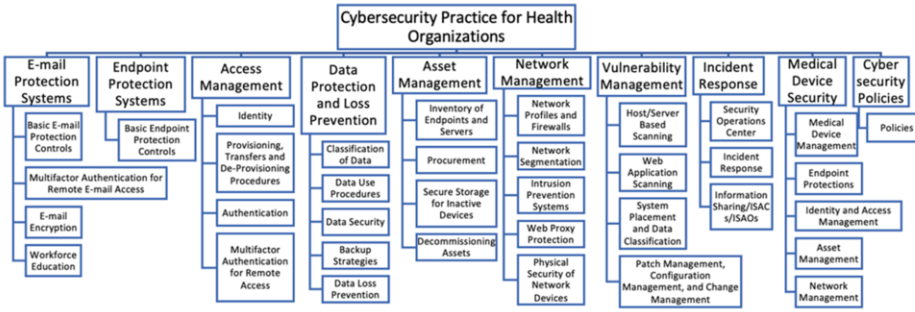


**Figure 7.** Cybersecurity Practices and Sub-Practices for Medium-Sized Organizations **[11].**

## Conclusions

Cyber security threats are an integral part of everyday life and cannot be ignored even when it comes to healthcare organizations. Furthermore, healthcare organizations are a very popular target due to the wide range and potential value that attackers can achieve, from potential popularity and public visibility to financial gain. The size of the healthcare organization is not a key criterion, but any information system that is used in medical practice and performs activities over patient health records, integrates medical devices and other subsystems is the potential target of cyber-attackers. Data shows that cyber-attackers are very successful even with the most robust systems [12].

Cyber-attacks are rapidly improving and becoming more sophisticated day by day, and health institutions have the important task of putting as a priority of making investments in cyber protection, which undoubtedly contributes to the protection of their patients, in addition to their permanent role in the field of health provision. Available information about recorded cyber-attacks on healthcare organizations should serve as a basis for summarizing key lessons in the development of cyber security settings in healthcare organizations [10]. The key categories that are important and in which it is necessary to invest and build the capacities of the health organization are defined as [10]:

1. *Making employees ready to face a cyber-attack*: Employee Awareness and Cyber Hygiene
2. *Making the organization ready to face a cyber-attack*: Policies and Procedures
3. *Understanding Vulnerabilities*: Risk Assessments, Continuous Monitoring
4. *Having* a *Response Strategy*: Training/ Preparedness, Communication/ Information Sharing
5. *Hardening Cyber Infrastructures*: Access Controls, Redundancy, Patching, Encryption

Additionally, best practices that represent promising approaches to combating cyberattacks include the following [11]:

- *Understanding the health organization's assets and assessing the consequences of a cyber-attack*. Cyber protection measures must be developed based on the principle of "when" an attack occurs, not "if". This implies that all resources and assets are categorized according to the principle of critical infrastructure and that the consequences for the entire system are determined in the case of disabling the work of a specific component and loss/destruction/change of data.

Based on the above assessment, backup copies of the data are created, and the system back-up strategy is developed.

- *Expert assessment of the cyber-security risks and continuous monitoring*. The basic elements of cyber protection must be implemented at the level of the health organization's computer network (e.g., marking external e-mails, firewalls), with continuous training of employees (e.g., training on "phishing attacks"). Additionally, highly qualified technical teams should carefully and comprehensively look at system vulnerabilities and make a risk assessment. If the healthcare organization does not have adequate staff, it is often possible to use support services free of charge through regional/federal cyber security agencies, but this task should not be left unfulfilled. Regular vulnerability testing of the system is necessary with additional assurance that the management of health organization understands the risks and subsequent consequences, as well as the processes that must be undertaken to raise the higher level of cyber security prevention and protection.
- *Continuous strengthening of knowledge and skills of employees*. The organization of training, which will include theoretical knowledge, practical scenarios and exercises for prevention, recognition of cyber-attacks and reporting of incidents, are necessary for all personnel in the healthcare organization. It is important that trainings are continuously organized and that employees acquire the necessary skills in case of a cyber incident or a potentially consequential disaster for the health organization (e.g., a cyber incident in the middle of a public health emergency/patient surge).
- *Creating and establishing downtime procedures and required resources*. The cyber-attacks can lead to a longer stoppage in the functioning of the healthcare organization, so it is necessary to clearly define all the procedures that employees should follow and in order to ensure the fastest reaction of the organization to the resulting interruption. This includes the creation of adequate supplies necessary for work, as well as additional training of key personnel who will oversee managing the process and leading other personnel.
- *Creating key copies outside the computer network, including staff and patient schedules, key contact information and relationships with suppliers and other collaborators*. Coordination, communication and information exchange with partners, stakeholders, regional and federal institutions is crucial in the fight against cybercrime.
- *Understanding the vulnerabilities that exist in devices, technologies, tools, software and third-party technology deployed throughout the facility/enterprise*. Any device or component that connects to the system can be used as a potential entry point into the healthcare organization's system. Therefore, it is necessary to ensure that suppliers of external devices and system components have developed cyber security standards and are integrated with the devices/components they supply. Additionally, modern protocols for authentication and privilege verification are necessary to ensure continuous control of remote access and usage of personal portable devices (smartphones, tablets, laptops, etc.).
- *Establishing and continuously improving the "cyber security culture" within the healthcare organizatio*n. The established protocols and standards must be adequately implemented by all employees in the healthcare organization.

Therefore, it is necessary to continuously check the implementation of cyber hygiene practices while simulating the real circumstances of cyber threats and cyber-attacks.

- *Establishing protocols and procedures for communication and information exchange with patients and staff members*. In case of identification of cyber-attempts or realization of cyber-attacks, it is necessary to send adequate information to patients and employees in an exactly appropriate manner. The key focus when selecting the information to be submitted should be on protecting the brand and mitigating further risks while considering the recommendations of law enforcement authorities.

## References

[1] He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. Journal of medical Internet research. 2021 Apr 20;23(4):e21747.
[2] HIMSS. HIMSS Healthcare Cybersecurity Survey for 2021. Healthcare Information and Management Systems Society, 2022.
[3] Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. Journal of medical Internet research. 2018 May 28;20(5):e10059.
[4] Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors. 2021 Jul 28;21(15):5119.
[5] Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S. Health care and cybersecurity: bibliometric analysis of the literature. Journal of medical Internet research. 2019 Feb 15;21(2):e12644.
[6] HIPPA. Healthcare Data Breach Report June 2022. HIPPA Journal, 2022.
[7] Protect Harbour. Healthcare Data Breach Trend Report 2021. Protect Harbour, 2022.
[8] Symantec. Cyber Security and Healthcare: An Envolving Understanding of Risk. Symantec, 2018.
[9] NIST. Framework for Improving Critical Infrastructure Cybersecurity. National Institut of Standard and Technology, 2018.
[10] Department of Health. Health Industry Cybersecurity Practices: Managing Threats and Protection Patients. Department of Health & Human Service, USA, 2021.
[11] Department of Health. Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations. Department of Health & Human Service, USA, 2021.
[12] American Hospital Association. Ransomware Attack Victims Speak Out: Best Practices & Lessons Learned from Ransomware Attack. American Hospital Association, 2022.