Cyber Threats to Healthcare Technology Services: a Case Study

Eduardo Neves[1]

[1] Lusofona University of Porto, Portugal
eduardoneves_12@hotmail.com

Abstract. Health is a vital industry in our society, and as we speak, we are evolving too, to another level, because we feel this need to simplify things, and that's where technology plays the major role in order to simplify and help us.
Since, as is normal in many organizations, hospitals started using electronic-based-systems so they can have easy access to so much information at the same time, things that were impossible to do in the previous time. However, there's no such thing as perfection and so aren't we. Nowadays, the healthcare industry is one of the prime targets for cybercrime, cause just like every industry in this "recent world" is surrounded by vital and confidential data. Hospitals, for instance, have a lot of important information about their patients, like sensitive, personal information or even financial. Therefore, it is mandatory to invest in new technologies, tools or even ways to prevent and control the risks of cyber attacks, for example, and protect this vulnerable industry.
The purpose of this article is to identify cyber security "trends", methods, results, consequences and measures that must be taken to face this problem.
The document also includes a study carried out with the support of information collected in a survey carried out with several health professionals in Portugal from various health institutions.

Keywords: Cybersecurity, Health, Threats, Attacks, Integrity, Confidentiality, Vulnerabilities, Cybercrimes.

1 Introduction

In recent years, as digital technologies feed into the backbone of the world economy, it is a critical resource, underpinning the complex systems that keep economies running, such as finance, healthcare, energy and transportation. Many of today's business models are based on the constant availability of the Internet and functioning information systems [1].

Technology is being used in our day-to-day lives, both in our work and in our relationship with people, it allows us to create greater possibilities of interactions between several people, which also, consequently, increases the associated dangers, because not all interactions with third parties are known interactions. On the internet, it is easy for malicious people to impersonate other people to gather information for malicious

purposes, often without the knowledge of the people who provide the information in an innocent way because they do not know they are being victims of cyber assistance [2].

To steal data from a hospital, hackers use, for example, Social Engineering. For this to happen they send an email containing links or attachments to employees and when an employee clicks on the attachment or link it will immediately infect the user's computer and start to spread throughout the health care system and thus obtain a fair amount of data from both patients and hospital staff [3].

A cybersecurity attack can result in a variety of threats, from simple identity theft to extortion attempts and loss of personal data. There are several organizations that must be protected in order for our society to function normally, such as hospitals and financial services companies, because they contain a large amount of valuable information, such as personal data, addresses, telephone numbers, contacts, etc [4].

As for the evolution of cybercrimes in the health sector, we can see that there was an increase compared to the year 2019, as that year the health sector was in the tenth place of the most attacked sectors of the year, with only 3% of the methods, but in 2020 it went from tenth place to seventh place with 6.6% of all attacks. The most used attack against the healthcare industry in the year 2020 was ransomware, accounting for 28% of attacks. A ransomware attack can be particularly devastating, as we can see in September 2020 in a German hospital, where the attack forced an ambulance to take a patient to another hospital 20 kilometers away, after this trip the patient died. German authorities determined that the attack did not play a decisive role in the death, but nevertheless, prompted that the patient could not receive the help he needed [5].

The purpose of this document is to raise awareness of the current status of technological health services, the vulnerabilities and risks of cybersecurity in health, and also to analyze the data from the case study. The purpose of the case study is to understand whether healthcare professionals act to prevent attacks and also to understand what they know about cybersecurity. Therefore, a survey was carried out and answered by several health professionals from different institutions.

2 Cyber Security in Healthcare

Cybersecurity is not just about the software, but also about who uses the network, as many people think that cybersecurity is just about protecting the email, the operating system and the network. It is a fact that this represents a slice of cyber security, but the largest share are the system's users who play an important role in ensuring that organizations, in this case hospitals, are protected, for which it is necessary to provide prior training in the best practices that can help minimize the risk of a cyber-attack happening [6].

Cyber security in healthcare must be more efficient than in other areas due to the type of data circulating in the healthcare sector, because it can put a patient's data at risk and subsequently have consequences for the same. For example, when a credit card is stolen from us, the bank cancels the card and issues a new one and consequently refunds the customer. But in case the PHI (any identifying information linked to any kind of clinical data - for example a diagnosis) of a patient is stolen, the patient cannot

change the data that was there, for example the date of birth, his blood type generally cannot alter your genetic and health information, and this information is very valuable for a variety of crimes. Health information is considerably more valuable on the dark web where it sells for 10 to 20 times more than, say, your credit card number [7,8].

There are several factors that shape cyber health risks:

- A rapid introduction of digital systems by the healthcare industry.
- The emergence of health data as a high value to cybercriminals as it contains a lot of sensitive patient data and confidential data.
- The evolution of health associations as targets for hacktivists and nation-states.
- And the difficult implementation and maintenance of security controls derived from the technical and organizational aspects of the industry [9].

3 Risks and vulnerabilities of cybersecurity in the healthcare

A security vulnerability is a weakness that allows an attacker to compromise the confidentiality, availability, or integrity of a computer system. A weakness can be the result of design choice, poor management, implementation failures or even human error, which can compromise the security of the entire system and in addition, affecting the software can also affect the hardware [10].

3.1 Threats, Health Attacks and Consequences

Threats and vulnerabilities go hand by hand, but they are not interchangeable. Threats are internal or external activities or events with the potential to attack the quality, efficiency and profitability of an organization. For example, hurricanes are one at the external threats that can cause serious damages like power outages. A threat can also be an employee who decides to steal data or harm your practice [11].

Health attacks pass for cyberattacks. Cyberattacks can occur in many different ways hoverer the main attacks are always intended to harm control systems or valuate datas.

One is used to block or manipulate a physical structure, the other one is more diverted to steel fragile datas. You have to garantie that the confidential information's you consequently have may not "fall" on the wrong hands. They can norm others or systems for their own benefit [23].

As the healthcare industry becomes more dependent on technology, on a daily basis, its cybersecurity challenges are increasing. To help protect organizations, you need to understand these challenges. The following are the main cybersecurity challenges that healthcare organizations need to be aware of:

- Malware and ransomware attack
- Phishing attack
- Date breaches
- Insider threats

- Distributed denial-of-service (DDoS) attacks
- Cloud threats [12]

Threat: Malware and ransomware attack

Ransomware is a type of malicious software (malware) used without the knowledge of the owner or the common user. It is used to infect, block, and encrypt the victim's data, denying him access to that same data. In order for the victim's data to be rescued it is usually necessary to pay a ransom for the software to be removed, then it is up to the attacker to remove it or not [13].

This threat usually comes into contact with the user, through advertisements for websites that contain malware or through phishing campaigns. It works as follows, upon delivery, the ransomware identifies the data that is to be encrypted through a list of embedded file extensions and encrypts that data. After encryption, the ransomware leaves a notification for the user to pay the aforementioned ransom [14].

Threat: Phishing attack

Phishing is a method of using a fake email to try to collect private information, distribute malware or even commit fraud. It is usually carried out with the intention of committing identity theft, gaining access to the victim's credit cards and bank accounts or, in healthcare, having access to all patient data. Attackers use various tactics to trick the email recipient into believing that the email they received is genuine [15]. Phishing typically requires the recipient of the email to take an action, which relies on social engineering techniques, therefore impersonating trusted sites such as financial institutions, administrators, or healthcare personnel [16].

Threat: Data breaches

The healthcare industry experiences more data breaches than any other industry. Health has been impacted by an average of 2.8 million breaches per month, the need for proper device management and monitoring, as well as the protection of confidential information.

The problem is, although the requirements enforced by HIPAA (Health Insurance Portability and Accountability Act) law are in place, most organizations do not have the resources to stay informed about the security measures that must be up to date. This offers a great opportunity for cybercriminals to easily gain access to patient information [12].

Threat: Insider threats

An internal threat is one of the greatest threats to the health care environment. For example, we may have an attacker who could hide inside the healthcare organization to gain access to devices on physical media or even infect them through wifi, bluetooth or other tools. Internal attacks can leak confidential information from both patients and employees and can even paralyze the entire network [17].

These types of attacks can be caused by current or former employees, executives, administrators, in short, everyone working in the organization. A theft of credentials can be considered an internal threat because external attackers use these credentials to gain access to confidential and valuable data [12].

Threat: Distributed denial-of-service (DDoS) attacks

A DoS attack is parallel to a DDoS attack but takes very different forms. DoS requests exist in one of two broad ranges: Denial of Service (DoS) and Distributed Denial of Service (DDoS). Offers are offered by a single attacker with the aim of making an application, service, or machine inaccessible. DDoS attacks are an attempt to flood an organization's network with Internet traffic to the point where it cannot operate or function normally [18].

DDoS attacks use multiple devices to launch DoS attacks in one or multiple directions. A DDoS attack is made up of four elements:

- The real attacker.
- The compromised handlers or hosts, which manage to control multiple agents.
- Zombie hosts, responsible for producing the distribution of packages to the final recipient.
- Lastly, a victim or host [19].

Threat: Cloud threats

Cloud security is a big challenge and slows down the spread of cloud to cloud. In a CSA report related to cloud security, experts identified critical ratings such as data breaches and loss or unsafe APIs [20].

Healthcare associations are switching to cloud data storage solutions due to their data recovery simplicity, but unfortunately not all solutions are HIPAA compliant [12].

3.2 Prevention of Threats and Attacks

At this point, there are some measures and recommendations for improving cyber security in the health area. To improve cybersecurity in the vast healthcare IoT ecosystem, the following measures need to be taken:

- Cybersecurity training and awareness programs

- Ensure secure settings
- Remote administration of servers, work, and network devices, etc. on secure channels
- Computer technology standardization
- The cost-benefit sharing. It is important to understand the commitment between cyber security measures and their effect on services.

There are also recommendations that should be taken into account:

- Implement state-of-the-art security measures
- Conduct tests and audits regularly
- Risk assessment and vulnerability assessment
- Establish an information security sharing mechanism
- Maintain a firewall configuration, which firewall must be placed on each external network interface
- Promptly revoke access to users who should no longer have access
- Protect encryption keys from misuse or disclosure [21] [22].

4 Case Study

To carry out the case study, a survey was carried out, aimed at health professionals with and without computer park management responsibilities, in order to collect data relating to the evolution of technologies with the evolution of care for the common user and to verify whether the health professionals in Portugal are aware of cybercrime and cybersecurity.

This survey was carried out with 151 health professionals from various health organizations in Portugal and from various positions at the professional level.

The first piece of information obtained from the respective survey was whether people have any knowledge of cybersecurity, where the graph below was obtained.

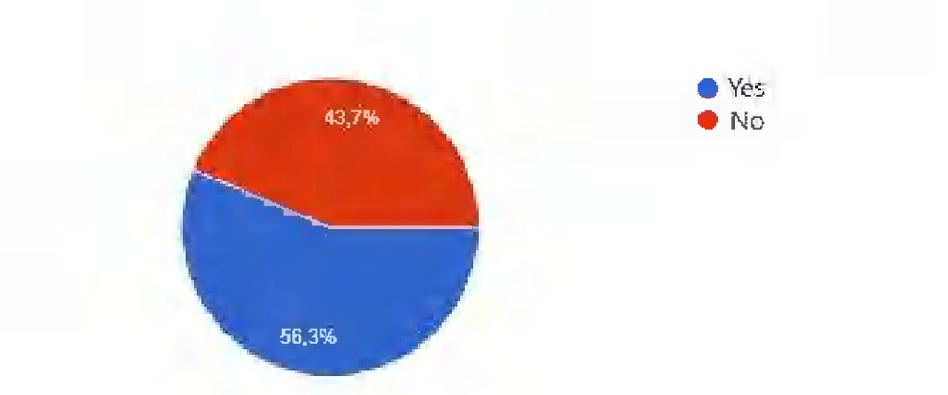

Fig. 1. Results obtained in the question: Do you have any knowledge about cybersecurity?

Observing the pie chart above, we can see that 56.3% (85) health professionals have some knowledge of cybersecurity or think they have some knowledge because many people say they have knowledge of cybersecurity when, in reality, they do not have it, and we also verify that the remaining 43.7% (66) confess that they are not sensitized to cyber security (figure 1).

With the information above only, we cannot conclude that our healthcare professionals are cybersafe, so we carried out more questions to verify their knowledge and actions in cybersecurity.

The first rule that a majority of people know is that we must have a strong password that is difficult guess, so to check if healthcare professionals were following it, a question was asked where we got the following data.

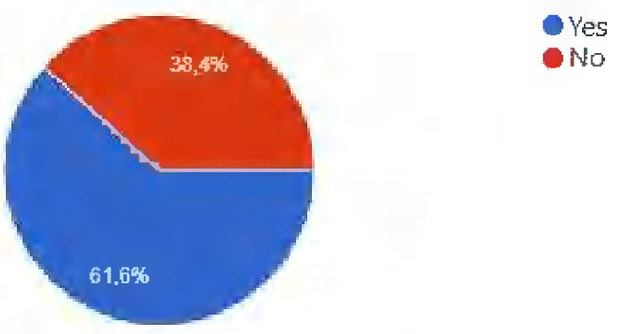

Fig. 2. Results obtained in the question: Do your passwords contain at least 9 characters and do they contain special characters (~ ! @ # $ % ^ &)?

Observing this chart, we can see that 61.6% (93) health professionals have a password with at least 9 characters and special characters, that is, here we can see that even some people who do not have cybersecurity knowledge use a secure or minimally secure password (figure 2).

But it's no use having a secure password if we use the same password for different services because even if the password is secure, it runs the risk of being discovered.

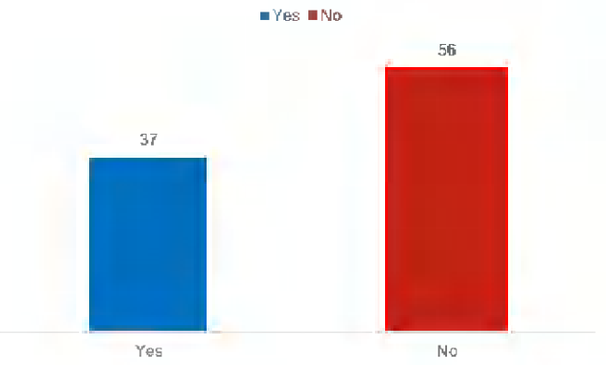

Fig. 3. This graph indicates the number of health professionals who have a secure password, but use it for the different services they use

As mentioned above, even with a secure password, we run the risk that it will be discovered. In this chart we have the number of health professionals who, despite having a secure password, use this password for the different services they use, which seriously increases the risk of data loss (figure 3).

For data to be lost, there must be an attack and two of the most frequent attacks on anyone's devices, not only in terms of health, are ransomware and phishing. To better understand if these healthcare professionals know what phishing or ransomware is, there are two questions in the survey that will give us that answer.

Fig. 4. This chart indicates healthcare providers' responses to the question: What do you understand by the term Phishing?

With the help of the graph, we can see that 56.3% (85) of health professionals correctly answered what phishing is when they say that it is the practice of sending

fraudulent emails that seem to come from a reliable source, but we still have a large number of people who simply do not know what phishing is, bearing in mind that this is one of the most well-known terms in society (figure 4).

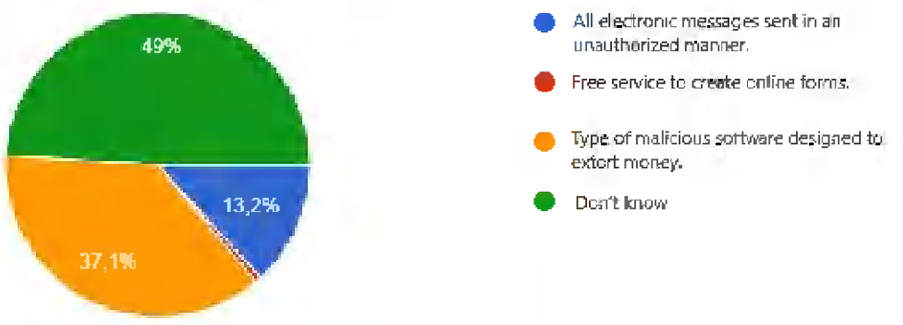

Fig. 5. This chart indicates healthcare professionals' responses to the question: What do you understand by the term Ransomware?

Ransomware is a term that is not as well known by society but it is one of the main threats to the healthcare sector as seen above, therefore it should be necessary that all healthcare professionals be alerted to this threat, but as we can see in the chart above only 37.1% (56) health professionals know what ransomware is, which highlights the fact that the vast majority do not know what ransomware is (figure 5).

A ransomware or phishing attack can attack the healthcare sector through healthcare professionals, so even in the survey there are 3 fundamental questions for us to verify that healthcare professionals act in a way to be safe personally, and for their organization.

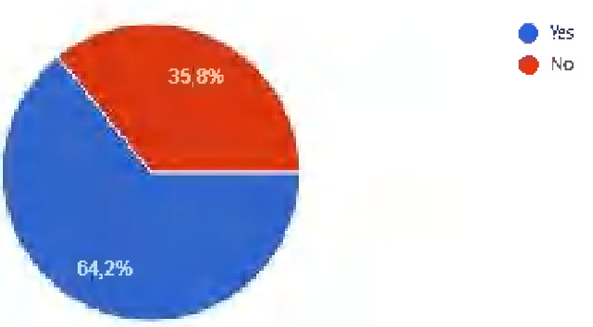

Fig. 6. This chart indicates the responses of healthcare professionals to the question: Do you access wireless networks in public spaces?

The first question concerns whether healthcare professionals access wireless networks in public spaces with their devices (figure 6). Based on the graph, 64.2% (97) of health professionals perform this bad practice that makes them susceptible to external attacks.

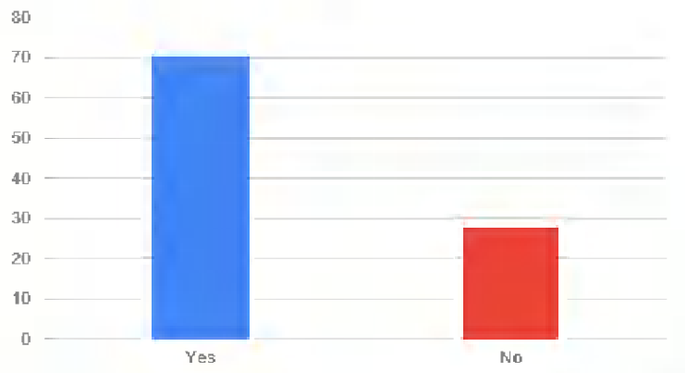

Fig. 7. This graph is the result of the answers of health professionals who answered yes to the previous question and the answer to the question: Do you access the wireless network in the workplace through your personal equipment? (ex: Mobile phone, laptop)

The second question concerns whether healthcare professionals access the wireless network of the organization where they work through their personal equipment. In figure 6 we can see that 97 professionals answered yes and 70 of these health professionals answered that they access the wireless network of their work organization with their personal equipment (figure 7). If these 70 had already performed a bad practice when accessing public wireless networks, they further aggravated the situation because their personal equipment could contain a virus that could pass to the network and contaminate the network and thus the organization is all contaminated.

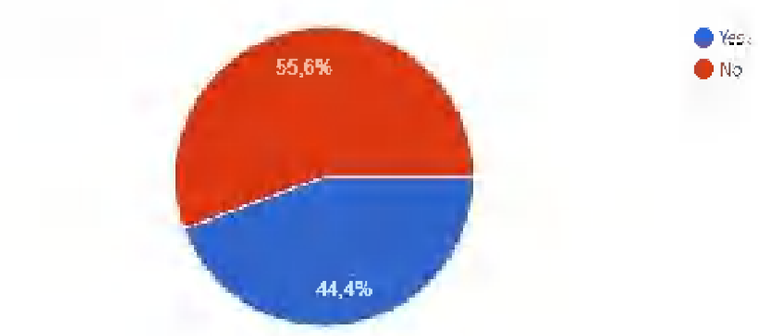

Fig.8. This chart indicates the responses of healthcare professionals to the question: Do you access your personal accounts on computers at the institution where you work? (ex: social media, email, etc.)

The third question concerns whether healthcare professionals access their personal accounts on the computers of the organization where they work. Based on the data acquired, we can verify that 44.4% (67) of participants pose a major threat to their work organization's network because they can mistakenly open an email that appears to be trustworthy and is actually a phishing email (figure 8). That's when the ransomware takes the opportunity to be masked in the links or files that the email contains. After this happens, we have a ransomware attack across the organization's network.

5 Conclusion

The healthcare industry is a sector that contains a large amount of sensitive data and continues to be very vulnerable.
Completing the case study, we can verify from the data collected from the survey that health professionals in our country are not properly informed about cybersecurity and cybercrime. To solve this problem, lectures to raise awareness of cybercrime / cyber security could be a step forward and policies created in their work organizations so that windows of opportunity are not created for an attack. While we can expect an increase in the number and types of threats throughout the years, we also have access to security measures that can reduce our exposure to being compromised.

References

1. "EU cybersecurity initiatives", https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf pp.1 (2017)
2. Cavalcanti, C., "Cyberdefense: Challenges and comparative legislation between Brazil and Portugal", (2017).
3. Shweta Vivekananda Kondewar, "Cyber Security in Healthcare", pp.146 (2021)
4. "What Is Cybersecurity?", https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works
5. IBM."X-Force Threat Intelligence Index ", pp.43 (2021)
6. Maria Christina,"What is Cyber Security", pp.1(2020)
7. Salem T. Argaw , Juan R. Troncoso-Pastoriza , Darren Lacey , Marie-Valentine Florin , Franck Calcavecchia , Denise Anderson , Wayne Burleson, Jan-Michael Vogel , Chana O'Leary , Bruce Eshaya-Chauvin and Antoine Flahault,"Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks", pp.2(2020)
8. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. "Cyber threats to health information systems", (2016)
9. Symantec, "Cyber Security and Healthcare: An Evolving Understanding of Risk", pp.2 (2017)
10. "Vulnerabilities and Exploits", https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits
11. U.S. Department of Health and Human Services, "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients", pp.5(2018)
12. "The Top 6 Cybersecurity Challenges in the Healthcare Industry", https://securityscorecard.com/blog/top-cybersecurity-challenges-in-healthcare-industry

13. David P. Paul III, Nikki Spence, Niharika Bhardwa, Alberto Coustasse Dr.PH, MD, MBA, MPH,"Healthcare Facilities: Another Target for Ransomware Attacks", (2018)
14. Dr. James Angle, Michael Roza, Vince Campitelli, Alex Kaluza, AnnMarie Ulskey "Ransomware in the Healthcare cloud", (2021)
15. Scott Rose, J. Stephen Nightingale, Simson Garfinkel, Ramaswamy Chandramouli,"Trustworthy Email", (2019)
16. Ward Priestman, Tony Anstis, Isabel G Sebire, Shankar Sridharan, Neil J Sebire "Phishing in healthcare organisations: threats, mitigation and approaches ", (2019)
17. Meng, Weizhi, Li, Wenjuan, Wang, Yu, Au, Man Ho "Detecting insider attacks in medical cyber–physical networks based on behavioral profiling" (2020)
18. Bhawna Tripathi, Dr. Devesh Katiyar, Gaurav Goel," A Study of DDoS (Distributed-denial-of- service) Attacks and Its Preventions", (2020)
19. Akhil K.M, Rahul C.T, Athira V.B, "Distributed Denial of Service (DDoS)Attacks and Defence Mechanism", (2021)
20. Jitendra Singh, "Cyber-Attacks in Cloud Computing: A Case Study", (2014)
21. Enisa, "Smart Hospitals", (2016)
22. Mohammed M. Alani, "Securing the Cloud: Threats, Attacks and Mitigation Techniques", (2014)
23. Filipa Capelão, Hugo Barbosa "Cybersecurity in Healthcare: Risk Analysis in Health Institution in Portugal"