D2.1 Advanced Cyber Security threats digest and analysis

WP2 - Conceptualization, Use Cases and System Architecture

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Copyright message

Document information

Grant Agreement Number	826183	Acronym	SPHINX	
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry			
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures			
Funding scheme	RIA - Research and Innovation action			
Start Date	1st January 2019	**Duration**	36 months	
Project URL	http://sphinx-project.eu/			
EU Project Officer	Reza RAZAVI (CNECT/H/03)			
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA			
Deliverable	D2.1. Advanced Cyber Security threats digest and analysis			
Work Package	WP2 – Conceptualization, Use Cases and System Architecture			
Date of Delivery	Contractual	M9	**Actual**	M9
Nature	R - Report	**Dissemination Level**	P - Public	
Lead Beneficiary	HMU			
Responsible Author	E. Markakis	**Email**	markakis@pasiphae.eu	
		Phone	+302810379258	
Reviewer(s):	ICOM, SIVECO			
Keywords	Threat Report, Market Analysis			

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	15/02/2019	ToC	ToC for approval by the Consortium	Evangelos Markakis (HMU)
0.20	28/02/2019	Draft	ToC Changes based on New template	Evangelos Markakis (HMU)
0.21	10/04/2019	Draft	Incorporated Contributions	Evangelos Markakis (HMU)
0.22	15/05/2019	Draft	Incorporated Contributions	Evangelos Markakis (HMU)
0.23	21/7/2019	Draft	Incorporated Contributions	Yannis Nikoloudakis (HMU)
0.24	22/7/2019	Draft	Incorporated Contributions	Yannis Nikoloudakis (HMU)
0.25	23/7/2019	Draft	Incorporated Contributions	Yannis Nikoloudakis (HMU)
0.26	8/8/2019	Draft	Incorporated Contributions	Yannis Nikoloudakis (HMU)
0.30	10/8/2019	Draft	Review 1	Ilia Pietri (ICOM)
0.31	10/8/2019	Draft	Review 2	Dana Oniga (SIVECO)
0.27	10/8/2019	Draft	Incorporated all review comments	Yannis Nikoloudakis(HMU)
0.28	22/8/2019	Pre-Final	Minor changes	YANNIS NIKOLOUDAKIS(HMU)
0.30	3/9/2019	Pre-Final	Validation of changes	Michael Kontoulis, Christos Ntanos (NTUA)
0.31	4/9/2019	Pre-Final	Quality Control	Christos Ntanos (NTUA)
1.00	4/9/2019	Final	Final Version	Christos Ntanos (NTUA)

Executive Summary

The purpose of this document is to research and elaborate upon the current existing and emerging standards on cybersecurity and the corresponding directives and regulations from the European Union. Additionally, the document provides a thorough and comprehensive taxonomy of cyber-threats and the existing research concerning cybersecurity in the Healthcare domain. The content of this document will be utilised as an input for tasks T2.4 and T2.5 for formulating or refining the project's use cases and application scenarios, thus providing sufficient information to extract the envisioned system's requirements.

Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table of Figures

Table of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

1.1 Purpose & Scope

This document serves as an initial input for the consequent tasks that will introduce and iteratively refine user stories, use cases and ultimately, system/user requirements. Within this document the current and emerging cybersecurity standards are presented and elaborated upon. A comprehensive taxonomy of the known cybersecurity threats is provided and an overview of existing research initiatives concerning cybersecurity on the Healthcare domain is presented. Finally, qualitative results from the questionnaires collected during the first project's workshop on cybersecurity awareness in the healthcare domain, are presented.

1.2 Structure of the deliverable

This document is structured as follows. Section 1 and its subsections, present the existing cyberthreat landscape and foreseen future steps, concerning the evolution of cybersecurity in ICT in general, and in the healthcare domain in particular. In Section 2 we present the existing and emerging cybersecurity standards, regulations and mandates derived from the European Union and other standardization entities. In Section 3 we present current research initiatives concerning data security in the healthcare domain. In Section 4, we present the qualitative and quantitative results from the questionnaires collected during the first project's workshop on Cyber situation awareness, that took place in Brussels in July, 2019. Finally, we conclude this document in Section 5 by presenting the outcomes of this research and future steps.

1.3 Relation to other WPs & Tasks

This document is tightly related to the tasks that partake in the production and iterative refinement of user stories, use-cases, and user/system requirements of the SPHINX project, namely tasks T2.4 and T2.5.

1.4 Cyber Security Landscape

Cybersecurity has never been a higher priority, with recent attacks such as the Facebook breach that saw 50 million user accounts compromised in September 2018, the WannaCry ransomware attack bringing down dozens of National Health Service Trusts in May 2017, the Yahoo breach that saw millions of accounts compromised in December 2016, and the Dyn attack, which saw IoT devices turned into a huge botnet that brought down several online services. Cyber-attacks are increasing in scale and severity, and organisations are starting to recognise that Cyber security is more than ever a hot topic in the agenda.

The reason is evident: the last years have seen a consistent, steady growth in cyber threats and breaches, with 2018 hitting a new record high: the 2018 Annual Data Breach Year-End Review by the Identity Theft Resource Centre revealed a 44.7% growth in the number of cyber incidents compared to 2016 [1]. In 2016, Kaspersky revealed that 758 million malicious attacks occurred, representing an attack launched every 40 seconds [2]. It seems that 2019 will again set a new record.

Over the past five years the number of ways hackers can get into an organisation has changed. There used to be a clear distinction between the inside and outside of an organisation and infrastructures had clearly defined boundaries. However, with the rise of mobile computing and cloud services, that endpoint has expanded and there is no clear, easily protected line that can keep data secured. Now that IoT has also been adopted and has entered the mainstream, the perimeter and number of vulnerabilities are set to expand yet again. Adversaries are constantly using more sophisticated methods to attack organisations digital surfaces, from mobile to IoT, and the cloud. Defenders should prepare to face self-propagating network-based threats that will be hiding in encrypted traffic. The use of encryption has grown as a way of protecting payloads, but it can also conceal bad traffic from security systems. A recent Cybersecurity report by Cisco found out that threat actors are also using popular cloud services for command and control, making malware very difficult to find with traditional security tools, because it looks like normal traffic. Malware are becoming self-propagating, and ransomware aren't only for obtaining ransom but also for the purpose of destroying systems and data. The recent Nyetya (NotPetya) threat posed as tax software that was actually something called "wiper malware" that killed multiple organisations' supply chain systems. Businesses of all sizes are deploying IoT devices at a furious rate, which is a critical component of digital transformation, but it also poses a number of new security problems, according to 2018 Cisco study [49], because of the following:

- 60% of IoT devices are deployed by operational technology not IT.
- Many IoT devices are unmonitored.
- IoT devices can potentially create "back doors" to other systems.
- Patching for IoT devices is often done poorly.
- IoT endpoints often have no inherent security capabilities.

Any of these points can be problematic but combined all together can become disastrous for many companies. Mirai[1] and Reaper[2] may have been the first couple of highly publicized IoT botnets, but they certainly won't be the last. With the estimation of connected IoT devices reaching some billions by 2020, the attack surface will expand exponentially. This expansion along with the fact that security is rarely built into the design of these devices and their software increases the risk of breaches.

Building upon the exploitation of system and network vulnerabilities, the types of cyberattacks are almost as numerous as the number of hackers. From individuals' personal information to confidential industrial product data, the field is vast, and the consequences can be multiple: impersonation, banking data fraudulent use, blackmail, ransom demand, power cuts, etc.

Developing at this pace, cybercrime threatens to become even more devastating for all types of businesses in years to follow. For public services and private companies across the globe, this strengthens the need to implement advanced data security strategies.

But, in order to do so efficiently, these organisations have to understand which the most significant cyber security threats are.

1.5 Threats Landscape

Cyber threats, big hacks and data leaks are nothing new, but during the last decade, there has been an increasing number of reported attacks and a specific surge in reported breaches, which has been viewed as a direct consequence of the EU Member States' adoption of the EU General Data Protection Regulation (GDPR) in May 2018 [3]. Indeed, the XXI century has seen the most spectacular cyberattacks, most of them were the biggest or most significant breaches of the century [4, 5]. See Annex II for details. In the following subsections, we firstly present a review on recent cybersecurity-related reports, to outline the current threat trends. Following, we present a generic categorisation of cybersecurity threats, and finally we present well-known cybersecurity issues concerning Healthcare Institutions.

1.5.1 Cybersecurity Trends

In January 2019 ENISA published the Threat Landscape Report 2018, presenting the top 15 cyber threats and trends [6]. Malware is the most frequently encountered cyber threat, involved in 30% of all data breach incidents reported. Compromised email (phishing, spam and spear-phishing) is the dominating attack vector for malware infections. In 2018, there was no global malware outbreak similar to WannaCry and NotPetya but

[1] https://en.wikipedia.org/wiki/Mirai_(malware), [date accessed: 12/8/19]

[2] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/reaper-botnet/, [date accessed: 12/8/19]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

the malware landscape evolved and malware authors are adjusting their tactics, techniques and procedures (TTPs) in order to maximise their profits and effectiveness rates. One of the noteworthy events of 2018 was the VPNFilter multi-stage malware campaign that targeted home and small office routers and Network Attached Storage (NAS) devices, compromising around 500.000 devices worldwide. Also, in 2018, an increase was observed in file-less attack detections, with 77% of the attacks successfully compromising organisations. File-less attack techniques will continue to be used by cybercriminals due to their effectiveness in evading detection by organisations' security controls.

The acceleration of data breaches targeting individual information, such as Equifax (the 198 million US voter registration breach), the IRS taxpayer information breach and the ongoing medical information breaches, denounce that the increasing sophisticated networks, the increasing advanced systems and the increasing amounts of data gathered by organisations remain highly prone to data security failures and exceedingly vulnerable to hacking.

In addition, the increased usage of laptops, smartphones and IoT devices all represent network endpoints that are increasingly difficult to secure, as most individuals are always connected via multiple devices. Indeed, the Internet of Things virtually makes every aspect of information governance more complex: there are more devices, more vulnerabilities, more information flowing. Symantec already found a 600% increase in overall IoT attacks in 2017, which means that cyber criminals could exploit the connected nature of these devices to mine "*en masse*". More importantly, Gartner estimates that 5.5 million new products connect daily and that, by 2020, the number of connected things is projected to jump to 20.8 billion [7].

Furthermore, digital transactions have grown exponentially, reaching 1.9 billion transactions in 2018. These transactions were hit by 30% more cyberattacks and registered 80 million fraud attempts, a 47% increase over the previous year, according to the cybercrime report for Europe by risk firm ThreatMetrix [8]. Across Europe, digital businesses have experienced an evolution from short and isolated attack peaks to more sustained, high-volume attacks during several days or weeks.

According to Fortinet, organisations experienced a staggering 82% increase in attacks [9]. There is an increased focus on innovation, with the number of malware families increasing by an alarming 25% in Q4 and unique malware variants growing at 19%. This combination of rapid development combined with the increased propagation of new variants is successfully catching organisations unprepared. Figure 1 and Figure 2 illustrate the daily attack volume for 2018 and exploit categorisation respectively.

Indeed, digital threats are evolving fast: ransomware attacks have increased by 300% since 2015 and the economic impact of cybercrime rose fivefold from 2013 to 2017 and could further rise by a factor of four by 2019 [10]. In terms of frequency, ransomware attacks led from the front with several malware families such as WannaCry, Upatre, Cerber, Emotet, Locky, Petya, Ramnit, Fareit, PolyRansom and Terdot/Zloader causing havoc on a global scale, followed by other tools such as crypto-miners, wallet-swiping trojans, and malicious code that exploited firmware and hardware vulnerabilities [11].

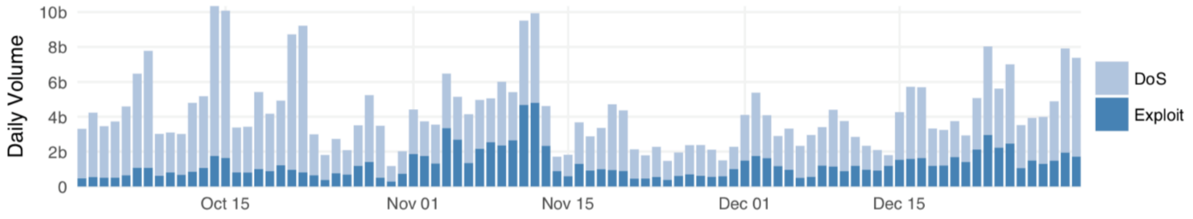


Figure 1 Daily attack volume for 2018

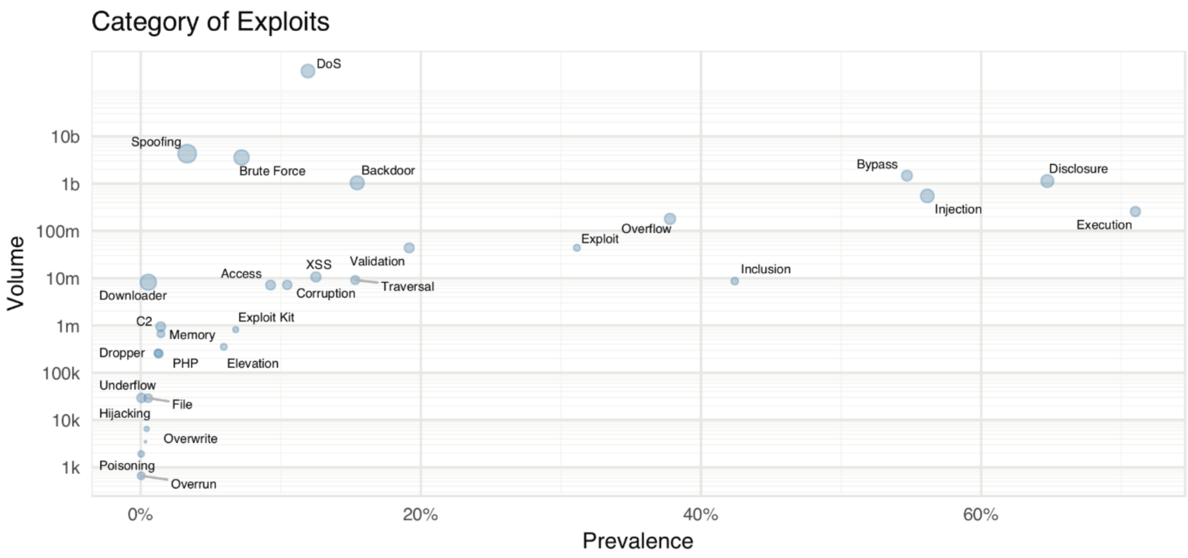
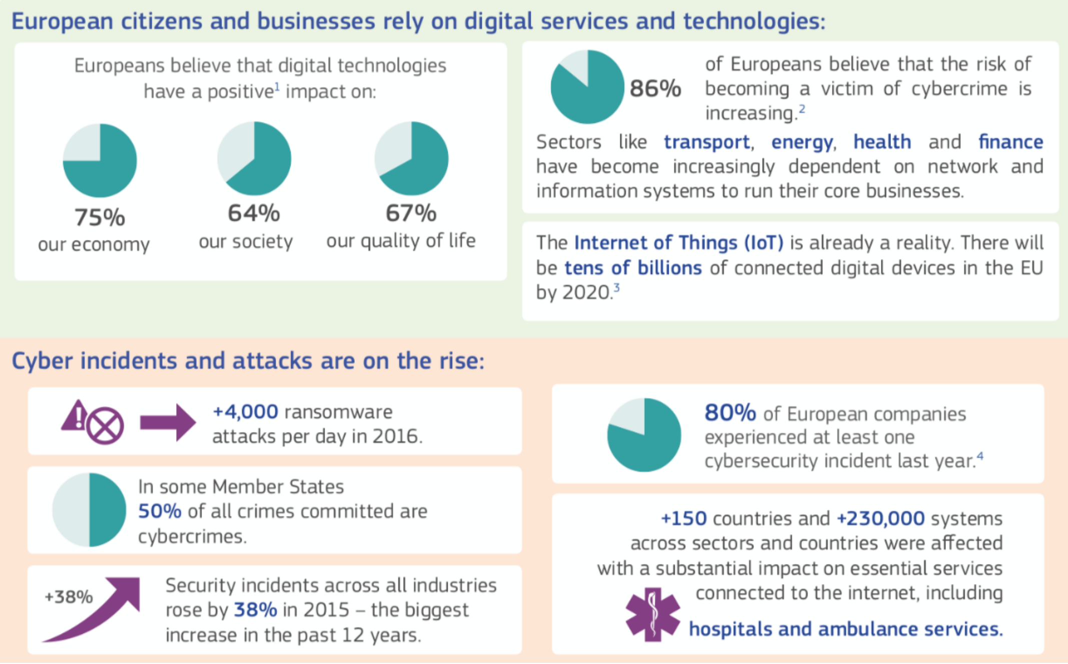


Figure 2 Exploit categorisation



European citizens and businesses rely on digital services and technologies:

Europeans believe that digital technologies have a positive[1] impact on:

75% our economy

64% our society

67% our quality of life

86% of Europeans believe that the risk of becoming a victim of cybercrime is increasing.[2]

Sectors like **transport**, **energy**, **health** and **finance** have become increasingly dependent on network and information systems to run their core businesses.

The **Internet of Things (IoT)** is already a reality. There will be **tens of billions** of connected digital devices in the EU by 2020.[3]

Cyber incidents and attacks are on the rise:

+4,000 ransomware attacks per day in 2016.

In some Member States **50%** of all crimes committed are cybercrimes.

+38% Security incidents across all industries rose by **38%** in 2015 – the biggest increase in the past 12 years.

80% of European companies experienced at least one cybersecurity incident last year.[4]

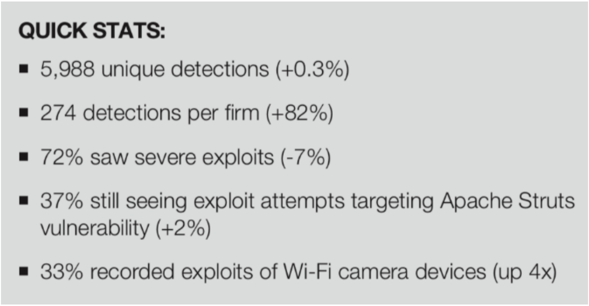
+150 countries and **+230,000** systems across sectors and countries were affected with a substantial impact on essential services connected to the internet, including **hospitals and ambulance services.**

Figure 3 Digital technologies adoption and cybersecurity overview

Personal identity, such as social security or credit card information, is extremely valuable. As long as there is a demand for this data, hackers will continue to attack large data repositories and networks, aiming to explore all possible vulnerabilities. The IBM Security and Ponemon's latest Cost of Data Breach Study established that, for the 477 companies taking part in the study, the average total cost of data breach rose from $3.62 to $3.86 million, an increase of 6.4% [15]. In this report, all companies experienced a data breach ranging from approximately 2,600 to slightly less than 100,000 compromised records, with an average cost per each lost record rising to $148, an increase of 4.8%. Data breaches of 1 million records yield an average total cost of $40 million, whereas a breach of 50 million records yields an average total cost of $350 million, with a $1.55 million net cost difference privileging the organisations that fully deploy security automation.

Overall, analysts predict that the cost of data breaches will reach $2.1 trillion globally by 2019 [16]. This is four times the estimated cost of data breaches in 2015. Although the majority of future breaches will come from existing IT and network infrastructures, smart devices will also account for a significant portion of the losses.

Europe faces increasing cybersecurity challenges that are constantly evolving and rapidly expanding. The UK is Europe's most breached country in cybersecurity terms, according to a new report by Thales: 37% of businesses in the UK reported cyberattacks in 2017, compared to 33% in Germany, 30% in Sweden and 27% in the Netherlands [12]. Europol estimates that cybercrime costs the EU €265 billion per year [13] and the global economy €400 billion [14].



QUICK STATS:

- 5,988 unique detections (+0.3%)
- 274 detections per firm (+82%)
- 72% saw severe exploits (-7%)
- 37% still seeing exploit attempts targeting Apache Struts vulnerability (+2%)
- 33% recorded exploits of Wi-Fi camera devices (up 4x)

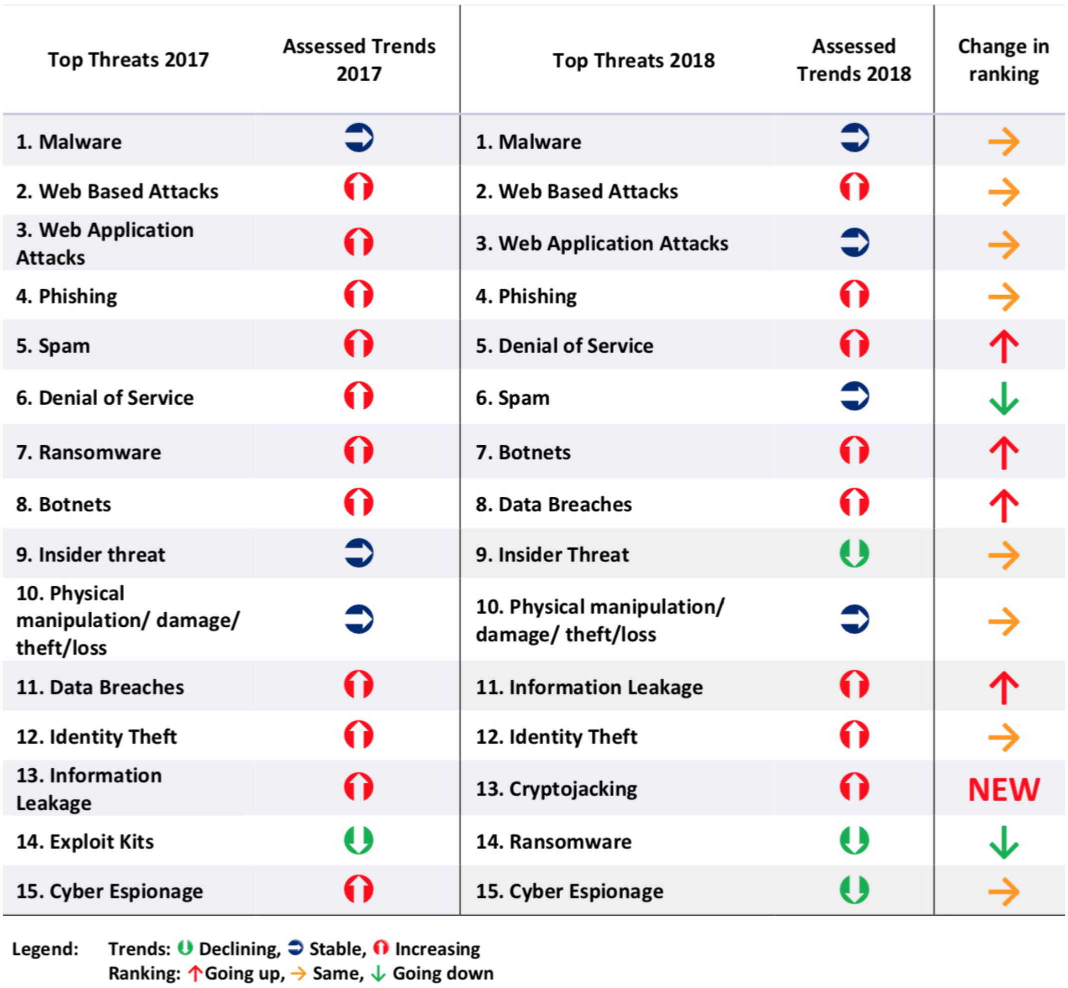
It is therefore evident that the ever-increasing cybercrime rate requires immediate action, at the European level. Evidence suggests that citizens across the world identify cyberattacks among the leading threats to national security. To answer to their concerns, the European Union aims to strengthen its cybersecurity rules in order to tackle the increasing cyber threat, as well as to take advantage of the opportunities of the new digital age. On October 18th, 2018, the European Council called for measures to build strong cybersecurity in the European Union. EU leaders referred to restrictive measures able to respond to and deter cyber-attacks. The basis for the renewed EU commitment is a European Commission's reform package on cybersecurity tabled in September 2017 that aims to build on the measures put in place by the cybersecurity strategy and its main pillar, the directive on security of network and information systems, the NIS directive. Other initiatives include to reinforce the EU cybersecurity agency and to introduce an EU-wide cybersecurity certification scheme. EU leaders regard cybersecurity reform as one of the main ongoing aspects on the road to completing the EU Digital Single Market.

1.5.2 What the Future Holds for Cyber Threats

Ransomware, mobile device exploits and cloud based-data breaches are amongst the major cyber threats for organisations in the years to follow [45]. The attack vectors used by cybercriminals are evolving: built up a repertoire of automation, increasingly using artificial intelligence and machine learning, in an attempt to rapidly attack their targets. Automation (*spray and pray attacks*) has taken various forms, from the weaponization of word documents to phishing emails. A big portion of created malware continue to be designed to run exclusively on Windows computers, but cybercriminals are abusing legitimate admin tools on the Windows operating systems, such as PowerShell, WMI and Windows Scripting Host, to evade detection and bring a new wave of attacks. Users of mobile devices are increasingly subject to malicious activity that is pushing malware apps to their phones, tablets and other devices running Android and iOS. The favoured tactic of cybercriminals is to sneak malicious apps past Google's Play Store and Apple's App Store. Another technique is to hijack IoT devices to use as nodes in massive botnets (e.g., Mirai malware and subsequent variants that caused massive large-scale attacks impairing several networks [46]). These botnets are then leveraged in DDoS attacks, as well as for crypto-mining and network infiltration activities. Attacks such as these are difficult to detect as it is rarely apparent that the device is affected.

It is critical to ensure that information communication technology (ICT) infrastructures are secure, a task that is exponentially more complicated due to the enlargement of the attack surface in all organisations, namely in the healthcare sector.

Ransomware is likely to be propagated through phishing scams, a user-based mechanism that tricks people into facilitating malicious network connections. The movement of large pools of confidential data to the cloud represents serious security and compliance risks for all types of organisations. And the need to ensure connectedness at all times, for all devices, remains a major challenge to cyber security, with data privacy at the top of the list. Still, above all, the human-in-the-loop is the weakest link: the absence of employee awareness and education presents itself as a grave cyber threat, compounding to the lack of preparedness and understanding of security policies aiming to prevent the improper exposure of sensitive data. **Error! Reference s ource not found.** illustrates a brief comparison of the current threat landscape, between 2017 and 2018, based on the ENISA report.



Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➡	1. Malware	➡	→
2. Web Based Attacks	⬆	2. Web Based Attacks	⬆	→
3. Web Application Attacks	⬆	3. Web Application Attacks	➡	→
4. Phishing	⬆	4. Phishing	⬆	→
5. Spam	⬆	5. Denial of Service	⬆	↑
6. Denial of Service	⬆	6. Spam	➡	↓
7. Ransomware	⬆	7. Botnets	⬆	↑
8. Botnets	⬆	8. Data Breaches	⬆	↑
9. Insider threat	➡	9. Insider Threat	⬇	→
10. Physical manipulation/ damage/ theft/loss	➡	10. Physical manipulation/ damage/ theft/loss	➡	→
11. Data Breaches	⬆	11. Information Leakage	⬆	↑
12. Identity Theft	⬆	12. Identity Theft	⬆	→
13. Information Leakage	⬆	13. Cryptojacking	⬆	NEW
14. Exploit Kits	⬇	14. Ransomware	⬇	↓
15. Cyber Espionage	⬆	15. Cyber Espionage	⬇	→

Legend: Trends: ⬇ Declining, ➡ Stable, ⬆ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Figure 4 Overview and comparison of the current threat landscape

Based on the experience from the last decade and the continuous evolution of cyber challenges, the biggest cyber threats for the upcoming years are:

1. Insider cyber security threats and inadequate security strategies

Historically, cyber security has placed emphasis on data, data processes, services, servers and networks. However, the user is the weakest link in the cyber security chain, with thousands of privileged account misuse episodes. Thus, it is of the outmost importance to enforce adequate security strategies and place an increased focus on user behaviour analytics over cyber assets, including identity and access management, encryption and the use of artificial intelligence (AI)-based analysis of behavioural biometric data.

2. Organised hacking efforts

It is widely acknowledged that one of the most significant cyber security threats are organised hacking efforts. More attacks from organised hackers will take place, including large-scale nation state social attacks trying to influence political or modern events, bolstered by the evolution of increasingly more advanced hacking

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

technologies. Nation state attacks have made many cybersecurity news over the past twelve months, raising interesting points around the role and the tasking of nation state hackers.

Spam[3], the abusive use of email and messaging technologies to flood users with unsolicited messages, is still one of the major attack vectors observed in 2018, primarily because of its low cost to send messages and of its time consuming and costly effect in terms of network bandwidth and storage. During 2018, botnets were highly active, serving different malicious activities, from Necurs[4] and Gamut[5] (almost 97% of spam-related attacks) to the variation of IoT-related botnets. IoT attacks diversify as attackers and seek new types of devices to add to botnets. Attacks are so frequent that botnet operators are fighting over the same pool of devices and have to configure their malware to identify and remove malware belonging to other botnets.

3. Ransomware and zero-day attacks

Ransomware and zero-day attacks are considered top-ranking cyber threats. Past attacks have proven that these threats work and are very profitable, therefore there is no reason why they should not increase. More importantly, the level of sophistication in ransomware and zero-day attacks is bound to make these attacks more difficult to detect. In response, cyber security should emphasise endpoint security (AI-based malware prevention should be the *de facto* standard on all endpoints) and also data protection.

4. New technologies create new loopholes

With the advent of the Internet of Things, the use of smart devices for malicious activities, such as DDoS, will become more commonplace. Similarly, the widespread use of cloud services continues to be threatening, as organisations forsake that the *attack surface* enlarges and continue to display blind trust on cloud companies' security and relax their cloud services' access controls and settings. Emphasis will also be placed on tracking and managing how users access data across each of their devices, using advanced search and analytic tools able to deliver actionable intelligence.

With the rise of Bitcoin, Ethereum, and other cryptocurrencies, many businesses started exploring blockchain technology, focused in building the right security infrastructure to protect themselves from hackers who are taking advantage of the vulnerability of the blockchain technology at this early stage. 2019 has been dubbed the year of Kubernetes and Containers in production, so it can be expected that attackers will be attentive to Docker and Kubernetes for post-exploitation. Also, attackers will likely continue to use the large number of mobile IoT devices to launch sustained DDoS attacks, namely against infrastructures such as GitHub and Dyn.

Distributed Denial of Services (DDoS) is one of the highly impactful threats in cyber landscape that has been targeting almost any business or organisation (16% increased activity). The rise in the number of connected services globally and their dependency on the Internet of Things (IoT) raises concerns over DDoS that may potentially cause nation-wide failures for businesses and critical systems – a clear example is the concept of connected hospitals and related services. DDoS attacks, in some cases, are used as a decoy. By keeping systems admins busy, DDoS hinder them from noticing that a targeted attack is underway.

5. Cyber skills gap

The absence of cyber security training for users in a way that intertwines with the organisational culture is a must for the next years. Social engineering has become the top-ranked attack vector, along with identity theft as one of the top cybercrimes. The information obtained from these breaches provide attackers with substantial insight into how to best compromise the assets of an organisation. Organisations should stay vigilant and invest

[3] https://en.wikipedia.org/wiki/Spam, [date accessed: 12/8/2019]

[4] https://en.wikipedia.org/wiki/Necurs_botnet, [date accessed: 19/8/2019]

[5] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/gamut-spambot-analysis/, [date accessed: 19/8/2019]

in employee education, training and awareness, as well as increase controls on identity, access and anomalous activity detection. Email phishing scams will remain the primary attack vector, as dubbed by Mailsploit, an exploit designed to spoof email senders' names to bypass Domain-based Message Authentication, Reporting and Conformance (DMARC). Again, employee education, training and awareness, from daily reminders to gamification, serve as a critical barrier against these attacks.

Phishing is the preferred way of compromising organisations, reported by 75% of EU Member States. 90% of malware infections and 72% of data breaches in organisations originate from phishing attacks. In 2017, spear-phishing emails were the most widely used infection vector, employed by 71% of those groups that staged cyber-attacks [48]. The number of targeted phishing attacks continue to grow, focusing on personal information or sensitive business data and clearly moving from consumers to businesses.

6. Lack of cyber security talent

Finally, it is also important to acknowledge the lack of skilled cyber security professionals, a situation that hampers the definition and implementation of strong cyber security strategies and defences in all organisations. Existing personnel lack the understanding of potential cyber threats and are usually unfamiliar with the state of the cyber threat and cybersecurity landscapes. The need to recruit and engage adequate cyber security talent is paramount for organisations to demonstrate active control over cyber hygiene (identify cyber assets, update software, patch software, run standard controls and educate the users) and thus efficiently remediate top cyber threats.

For the organisations that do not understand the threat landscape is evolving, problems will persist, and they will fall further behind attackers. Organisations need to act now to ensure their cybersecurity strategies, and those of the enterprises within their supply chain, are up-to-date and able to respond to new forms of attacks quickly. Only then will organisations be safer against the ever-evolving cyber threat landscape.

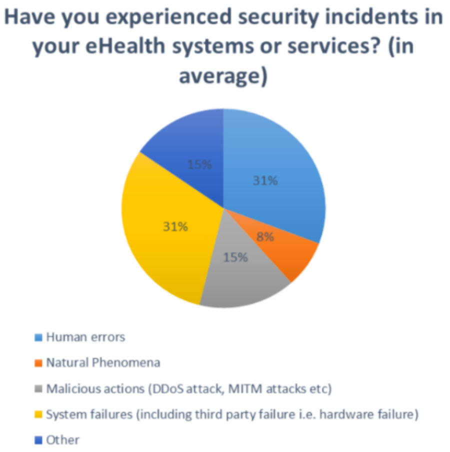
1.5.3 Threat Landscape for Hospitals

Healthcare technology is prevalent around the world and creates huge potential to improve clinical outcomes and transform care delivery, but there are also increasing concerns relating to the security of healthcare data and devices. With the healthcare sector's rapid adoption of digital systems and the spending in technology growing, so does the sector's cybersecurity attack surface. Today, healthcare networks not only include hospitals, clinics and doctor's offices, but also start to accommodate Internet-based medical consulting with remote healthcare providers or patients, multi-cloud Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) environments, and connected medical devices both inside hospitals and deployed at the patients' homes.

The range of systems that can be affected includes some of the most important devices used for diagnostics and patient care [17]. The FDA lists examples including "*systems that obtain, archive and communicate pictures on networks within health care facilities, such as computed tomography (CT), magnetic resonance (MR), ultrasound (US), nuclear medicine (NM) and endoscopy; systems that monitor patient activity, such as electrocardiographic (ECG) systems; and systems that communicate with clinical laboratory analysers, such as laboratory information systems*." [18]. That encompasses computers, routers and switches that connect operating rooms to databases.

Increasingly, healthcare organisations rely on information sharing across departments, users, borders, patients and carers demand instant access to medical information and scheduling, owning their commitment and engagement to their health and treatment plans. Medical professionals now store, manage and share far more medical images than ever before. Picture archiving and communication systems (PACS) and cloud-based vendor-neutral archives (VNAs) enable healthcare practices to provide their users with access to medical images anytime, anywhere [19]. Advancing the ability of medical devices to exchange and use information safely and effectively with other medical devices, as well as other technology, offers the potential to increase efficiency in patient care.

Merger and acquisition activity in the healthcare sector is also speeding up, with its associated IT integration challenges, including different medical technologies, combined with the need to share information between newly merged organisations creating new vulnerabilities. This tendency does not seem to be slowing down and these new vulnerabilities have not gone unnoticed by cybercriminals seeking to access and exploit the data being shared.



And, indeed, the healthcare sector experiences twice the number of cyberattacks as other industries [20]. A global study by NetDiligence of cyber insurance claims in 2017 found that healthcare accounted for 18% of breaches across all sectors and that 63% of healthcare breaches were caused by criminal or malicious activity [21].

In 2017, healthcare saw an average of almost 32,000 intrusion attacks per day on average per organisation as compared to over 14,300 attacks per organisation in other industries [20]. FortiGuard Labs also found that almost half of the top 10 threats in healthcare were triggered by botnets, some of which leveraged through compromised IoT medical devices [20]. In fact, 2017 was a particularly difficult year for the sector, which was hit with several high-profile ransomware and malware attacks that clearly demonstrated both the vulnerabilities of healthcare organisations and their exposure to complex cyber risks.

And cyber security incidents in the healthcare sector cause a severe societal impact. In a recent ENISA study [22], twelve out of eighteen EU Member States (MS) considered healthcare as a critical sector. Cyber security incidents affecting healthcare have as root causes, human errors, natural phenomena, malicious actions (DDoS and Man-in-the-Middle or MITM attacks) and system failures (including third party failure, i.e. hardware failure). System failures and human errors account equally for the majority of the incidents reported. Human error also includes incorrect security practices by personnel which may result in security negligence, oversight or incidents. Deliberate human intervention to disrupt the workflow (i.e. malicious actions) also accounts significantly for jeopardising security. The study therefore suggests the need to develop an eHealth specific incident reporting, classification and alerting mechanism at a pan-European level.

In the past five years, healthcare has been plagued by a myriad of cyber threats, with weaponised ransomware, misconfigured cloud storage buckets and phishing emails dominating [23]. Healthcare data breaches grew in both size and frequency, with the largest breaches impacting as many as 80 million individuals, exposing highly sensitive information, from personally identifiable information to health insurance information and patients' medical histories [24]. In 2018, these threats continued, and cybercriminals seem to display more creativity, as healthcare organisations develop better awareness of cyber threats and adequate security strategies. See details of the biggest data breaches in the healthcare sector in Annex III [25, 26, 27].

A study by Osterman Research for Malwarebytes found that the healthcare industry has been among the hardest hit by ransomware attacks [28]. Proofpoint goes further to announce that ransomware dwarfed *all other types of cyberattacks against healthcare companies combined* [29]. In May 2017, the WannaCry ransomware outbreak provided an early indicator. This attack affected 40 hospitals belonging to the National Health Service in the United Kingdom [30] and also hit medical devices using embedded versions of Windows XP [31]. Later in the year, SamSam exploited external-facing vulnerabilities or stolen credentials to penetrate targeted health organisations and used well-orchestrated execution to exert maximum pressure. The attack on the Rainbow Children's Clinic was a typical ransomware attack that took the traditional route of encrypting digital records and holding them hostage. However, a new wave of ransomware attacks is emerging, focusing on disrupting access to digital systems and then demanding ransom in exchange for releasing the services for their normal operation. This happened in the Hollywood Presbyterian Medical Centre attack, in which computers were offline for a week, and also in a German hospital, which lost its email services and hospital employees were forced to return to paper and fax machines. The effectiveness of holding hospital data or systems for ransom lies in the urgency to regain control. Hospitals face losing not just money, but critical resources for keeping patients alive.

Ransomware is one of the most dangerous threats to healthcare security because it can disable workstations, medical devices and critical record-keeping systems. These threats can pose life-or-death situations if they target hospital devices that can be disabled or altered, and security pumps. The MedJack malware can be injected into medical devices and then fans out across a network and the attackers usually target medical devices running outdated operating systems, such as Windows XP and Windows Server 2003 [32]. By attacking legacy technology, attackers can avoid detection more easily, since outdated operating systems may not flag the attack.

The increasing use of connected medical devices in home care and other medical services further complicates security. If compromised, these devices can potentially lead to widespread attacks and directly impact the individual's physical well-being. As the number of intelligent devices rises, the potential damage that could be caused will continue to increase. A survey by security company ZingBox, found that U.S. hospitals on average have between 10 and 15 connected devices per bed and that a large hospital can have more than 5,000 beds compounding to as many as 85,000 connected medical and IoT devices, putting massive strain on the healthcare network [33, 34]. The same survey revealed that over 90% of healthcare networks support IoT medical devices.

Every connected device, and the systems managing them, represent a potential target for cybercriminals and malware. Just to illustrate this cyber threat, it is important to recall that a Trend Micro survey, found that more than 36,000 medical devices can be scanned and found by a tool called Shodan and that a significant portion of exposed healthcare systems still use outdated operating systems, which can make them vulnerable [35]. A survey by researchers in Britain and Belgium uncovered security flaws in the communication protocols of the new generation of implantable cardiac defibrillators [36], and that in 2016, Johnson & Johnson warned patients using its insulin pumps that a hacker could exploit a security flaw in the device to overdose them with insulin [37]. Already in 2013, former Vice-President Dick Cheney had the wireless functions of his heart defibrillator disabled because he was warned it could be hacked in an assassination attempt [38].

Threat actors have also been known to inject fraudulent data or otherwise falsify patients' health records. They might modify a record to show that a patient has a serious condition from which he or she does not suffer, or that the patient requires medication that could be dangerous. This environment creates a virtually unlimited number of attack vectors for threat actors to exploit.

Breaches are widely observed in the healthcare sector and can be caused by many different types of incidents, including credential-stealing malware, an insider who either purposefully or accidentally discloses patient data, lost laptops or other devices. Distributed denial of service (DDoS) attacks are a popular tactic used by cybercriminals to overwhelm a network to the point of inoperability. This can pose serious problems for healthcare providers who need access to the network to provide proper patient care or need access to the Internet to send and receive emails, prescriptions, records and information.

Although these cyber threats urge healthcare organisations to defend the integrity of their systems and networks from external threats, it is also important to address the very real and dangerous risk that may lie within the organisation, the insider. The insider poses a threat because their legitimate access renders useless traditional cybersecurity defences, such as intrusion detection devices or physical security. The insider threat concept encompasses a variety of employees, from those unknowingly clicking on a malicious link that compromises the network or losing a work device containing sensitive data, to those maliciously giving away access codes or purposely selling personal health information for profit. According to Verizon [39], healthcare is the only industry in which internal actors represent the biggest risk to an organisation: 58% of all healthcare data breaches and security threats are caused by insiders, those who have authorised access to healthcare assets.

As hackers are aware that systems, networks and/or medical devices compromised in an infection process are often crucial to the healthcare organisations' mission, and the ransomware renders them inaccessible, the delay of patient care is a tremendous pressure to remediate the issue immediately. This pressure, combined with the fact that healthcare organisations generally have financial resources on hand, potentially increases the likelihood the attackers to be paid.

In this context, healthcare data tends to be richer in both volume and value than financial services or retail data. A report from the Healthcare Information and Management Systems Society, found that a stolen health record can be sold for $50, compared with $3 for a Social Security number and $1.50 for a credit card number [40]. Also, not only healthcare organisations are privileged targets for cyberattacks and data breaches – Thales Security stated that 77% of healthcare organisations have been breached, with some of the most valuable personal data about their patients and customers being exposed [41] –, but also they present the highest costs associated with data breaches, an average of $408 per lost or stolen record, which represents nearly three times higher than the cross-industry average, according to IBM Security [15].

In the future, with technologies becoming more sophisticated, cyberattacks have the potential to be correspondingly more advanced. A particular worrisome topic currently being discussed among experts in the field is *brainjacking* [42]. Advances in brain implant technology, such as deep brain stimulation, provide excellent tools for the treatment of a range of neurological and potentially mental health conditions, for example by inhibiting movement in Parkinson's patients. Such devices enable neurosurgeons to take precise control over the human brain through wireless stimulators. Unfortunately, this opens up the possibility for cybercriminals to hack into the system and alter stimulation settings. Other futuristic possibilities address the inducing of behavioural changes in patients [43]. While thankfully there has been no such cases to date of the above occurring, experts warn that this is a distinct future possibility.

The Harvard Business Review argues that most of these security challenges can be attributed to a lack of awareness on the part of the healthcare sector, which has been slow to adopt effective strategies to protect medical data stored on stolen or lost mobile devices [44]. However, healthcare organisations are increasingly looking to their health IT infrastructure as a foundation for value-based care initiatives. They are interested in reducing costs by consolidating IT infrastructure resources and using advanced technology to more accurately diagnose patients at the point of care. By introducing more connectivity, remote monitoring and information gathering, the Internet of Health Things (IoHT) can encourage better use of healthcare resources, more informed decisions, a reduction in inefficiencies or waste and the empowerment of health consumers. IoHT transforms raw data into simple, actionable information and can be leveraged to improve access to health, quality of care, consumer experience, and operational efficiency. Ultimately, cybersecurity is critical to patient safety.

To combat the existing and emerging healthcare security threats, a holistic approach to cyber security needs to be developed, enabling cybersecurity to become an integral part of patient safety. New legislation and regulations are in place to facilitate change, which applies to human behaviour, technology and processes. Understanding and adapting to threats as they evolve better allows an organisation to create a layered security framework that promotes technological innovation to better protect patient data, minimise threats to patient health and safety and also ensure the privacy and confidentiality of sensitive information shared through IoHT-enabled environments.

2 Cyber Security Standards

2.1 Cyber Security Standards

Standards that define procedures, techniques and measures are very important both for cyber and information security, especially when it comes to areas such as healthcare. There are critical infrastructures, that process data deserving special attention and must adhere to the Confidentiality, Integrity, Availability (CIA) principles[6] at all times and equipment based on different technologies, e.g. medical devices, servers where patient files are stored, IoT devices that provide services to patients. These can be connected to home or hospital networks and managed either locally or via remote connection.

It is considered critical for any Organisation to take into account the benefits that come with a cyber security standard, as well as the challenges that will emerge when it is adopted. They ensure that security products can be combined into systems that can detect threats and vulnerabilities and responding in real time, making them essential for health services. In particular, standard interfaces and protocols make systems' integration much simpler and allow products to interoperate in heterogeneous environments [50]. Standardization of testing methods also makes it possible to compare security products in a meaningful manner ('benchmarking') and provides a means for the end-user to assess new products or services. It must be made clear though, that there are no borders in the cyber world, nor is there a single legal system, and there is no common approach to the concepts of security and data protection. Nevertheless, in the virtual world, there is a relative homogeneity in the technologies being applied.

Standards such as ISO / IEC 27001: 2013, encourage organisations to implement and adopt a structure as clear and comprehensible, as it makes it easier for customers to understand how internal procedures work and reduces the cost of audits (when having an already established and maintained Information Security Management System, according to the appropriate specifications). This is mainly due to the fact that these standards provide, on the one hand, a layout for the implementation of a security management system, and on the other hand, a layout for which it will be used to inspect and control an organisation's compliance with information security practices.

All of the above-mentioned factors have a major influence on whether the systems, devices and applications of health and welfare systems are being prepared to address modern threats. Standardized technologies and approaches enhance the harmonious operation between the different devices and systems used by both healthcare professionals and the public benefitting daily.

2.1.1 ISO/IEC 27032

A Standard that can help with cyber security threats is ISO/IEC 27032:2012. As stated in ISO's official webpage, "ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- information security,
- network security,
- internet security, and
- critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

[6] https://resources.infosecinstitute.com/cia-triad/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- an overview of Cybersecurity,
- an explanation of the relationship between Cybersecurity and other types of security,
- a definition of stakeholders and a description of their roles in Cybersecurity,
- guidance for addressing common Cybersecurity issues, and
- a framework to enable stakeholders to collaborate on resolving Cybersecurity issues." [51]

First, it's crucial to give a proper definition of the term referred as "Cyberspace". The Cyberspace, is a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks.

"Cybersecurity" or "the Cyberspace security", is defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace". [52] While a variety of information risks are connected with 'the Cyberspace', many (such as network and system hacking, spyware and malware, cross-site scripting, SQL injection, social engineering, plus information security issues relating to "Web 2.0", cloud computing and virtualization technologies that typically underpin virtual online environments and applications) could be classified as normal or conventional systems, network and application security risks. In practice, the standard is largely concerned with information risks associated with the Internet, rather than 'the Cyberspace' per se. However, since these risks are already pretty well covered by other ISO or ISO/IEC information security standards, either published or under development, it is uncertain what information risks are truly unique to 'the Cyberspace'.

The first area of focus of this International Standard is to address Cyberspace security or Cybersecurity issues which concentrate on bridging the gaps between the different security domains in the Cyberspace [51]. In particular, this International Standard provides technical guidance for addressing common Cybersecurity risks, including:

- social engineering attacks;
- hacking;
- the proliferation of malicious software ("malware");
- spyware; and
- other potentially unwanted software.

The technical guidance provides controls for addressing these risks, including controls for:

- preparing for attacks by, for example, malware, individual miscreants, or criminal organisations on the Internet;
- detecting and monitoring attacks; and
- responding to attacks.

The second area of focus of this International Standard is collaboration, as there is a need for efficient and effective information sharing, coordination and incident handling amongst stakeholders in the Cyberspace. This collaboration must be in a secure and reliable manner that also protects the privacy of the individuals concerned. Many of these stakeholders can reside in different geographical locations and time zones and are likely to be governed by different regulatory requirements. Stakeholders include:

- consumers, which can be various types of organisations or individuals; and
- providers, which include service providers.

Thus, this International Standard also provides a framework for

- information sharing,
- coordination, and
- incident handling.

The framework includes

- key elements of considerations for establishing trust,
- necessary processes for collaboration and information exchange and sharing, as well as
- technical requirements for systems integration and interoperability between different stakeholders.

Given the scope of this International Standard, the controls provided are necessarily at a high level. Detailed technical specification standards and guidelines applicable to each area are referenced within this International Standard for further guidance.

2.1.2 ISO/IEC 27001

ISO/IEC 27001:2013 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information risks (called 'information security risks' in the standard) [54]. The ISMS is an overarching management framework through which the organisation identifies, analyses and addresses its information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts. Addressing any health care institution as an organisation, makes possible for the ISO/IEC 27001:2013 to integrate with already set procedures, goals, data and infrastructures, in order to enhance its security status and data protection principles.

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continuously improving an information security management system (ISMS), within the context of the organisation [55]. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature. It provides guidelines and requirements for the staff of an organisation to be aware of any new security threats, new privacy features and data protection techniques, through constant communication with the management and the IT support department. For this reason, frequently updated documentation must be always available to the employees.

The establishment and implementation of an organisation's information security management system is influenced by the organisation's needs and objectives, security requirements, the organisational processes used and the size and structure of the organisation. All of these influencing factors are expected to change over time, while new technologies, management needs and security incidents may occur.

As stated in the ISO/IEC 27001:2013 in Chapter 5 titled "Leadership", "top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities" [55]. The management of any health care institution, be it a hospital or just a physician's office, must define different roles, and for each one of them, different responsibilities should be given. In the end, a security policy must be authored which will include the rules needed for the ISMS to operate as planned and the penalties that should be given when actions are taken that do not follow the policy's principles. Also, a User Rights Agreement policy should be authored, in which the rules for the appropriate handling of equipment and behaviour within each of the organisation's different facilities are enacted. Additionally, this documented information must be communicated through the staff of the organisation and be maintained frequently from the people in charge.

The very essence of the ISO/IEC 27001:2013 lies in the 6th chapter, titled "Planning". This chapter outlines the process to identify, analyse, plan the treat information risks, and clarify the objectives of information security. The assets (i.e hardware, special equipment, facilities, software, data) must be specified and their importance

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

for the organisation must be evaluated. Then, any incident that will pose a threat to the assets defined, must be recognized and the risk of any of the threats damaging the assets should be estimated.

ISO/IEC 27001:2013 includes Annex I, which has the list of controls that can be used in order to counter these threats and give feedback for the procedures that must be launched in order for the system to recover.

In Chapters 9 and 10 of the ISO/IEC 27001:2013 the guidelines for the ISMS's internal auditing are placed. As stated in the documentation, "**9 Performance evaluation** - monitor, measure, analyse and evaluate/audit/review the information security controls, processes and management system, systematically improving things where necessary [55]. **10 Improvement** - address the findings of audits and reviews (e.g. nonconformities and corrective actions), make continual refinements to the ISMS."

ISO 27001:2013 Certification

ISO/IEC 27001 is a formalised specification for an ISMS with two distinct purposes [54]:

- It lays out the design for an ISMS, describing the important parts at a fairly high level;
- It can (optionally) be used as the basis for formal compliance assessment by accredited certification auditors in order to certify an organisation compliant.

Certified compliance with ISO/IEC 27001 by an accredited and respected certification body is entirely optional but is increasingly being demanded from suppliers and business partners by organisations that are concerned about the security of their information, and about information security throughout the supply chain or network. The certificate has marketing potential and demonstrates that the organisation takes information security management seriously. However, the assurance value of the certificate is highly dependent on the ISMS scope. It must be noticed that certified ISO/IEC 27001 compliance is a positive sign but not a cast-iron guarantee about an organisation's information security.

ISO 27032:2012 VS 27001:2013

ISO/IEC 27032:2012 is not a standard that an Organisation can certify; perhaps this is one of the most important differences with respect to ISO/IEC 27001:2013, which allows for the certification of an Information Security Management System (ISMS) [53]. ISO/IEC 27032:2012 mainly aims to provide a guide for cybersecurity through specific recommendations, while ISO/IEC 27001 sets requirements to establish an ISMS. So, the focus of ISO 27001 is each organisation and its ISMS, while ISO/IEC 27032:2012 focuses on cyberspace and is a framework for collaboration and addresses issues focused on different security domains in cyberspace. Therefore, both standards have different objectives, but they are closely related.

2.1.3 NIST Cybersecurity Framework (Best Practices)

The National Institute of Standards and Technology (NIST) is a non-regulatory agency, based in the United States that aims to promote innovation and competitiveness. Therefore, its aim is to produce standards, directives and frameworks concerning emerging ICT topics and issues. In its recent report "*Framework for Improving Critical Infrastructure Cybersecurity*", 2018, [68], researchers stated: "*The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: The Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities.*"

It proposes a voluntary guidance, based on existing standards, guidelines and practices, that an organisation can follow to manage adequately the cybersecurity risks and at the same time poses a sound ground for a clear understanding of all stakeholders of the cybersecurity and risks the business is coping with.

The framework as such provides the adequate tools that have to be customised for each sector or organisation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

It enables the organisation or sector to characterize properly the cybersecurity risk the organisation or sector is facing and was on this characterization the framework provides the adequate practices that should put in place to minimize those risks.

The framework focuses on the assurance of the critical operations and service delivery. This provides benefits beyond having a cybersecure business but clearly identifies where the investments of cybersecurity should be made.

"The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: The Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities. These components are explained below.

- *The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organisation from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organisation's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.*
- *Framework Implementation Tiers ("Tiers") provide context on how an organisation views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organisation's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organisation's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organisation should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organisational constraints.*
- *A Framework Profile ("Profile") represents the outcomes based on business needs that an organisation has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organisation can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organisation's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organisation or between organisations."*

The overall idea of the framework is focused in the five main actions that must be taken when dealing with cybersecurity risk management which are Identify, Protect, Detect, Respond and Recover. For each of these, the list of functions and category IDs used in the framework is provided. Below is an example extracted from the above-mentioned document [68]:

Table 1 Action categorisation

Function	*Category*	*Subcategory*	*Informative References*
PROTECT (PR)	***Identity Management, Authentication and Access Control (PR.AC):*** *Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.*	***PR.AC-1:*** *Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes*	***CIS CSC*** *1, 5, 15, 16* ***COBIT 5*** *DSS05.04, DSS06.03* ***ISA 62443-2-1:2009*** *4.3.3.5.1* ***ISA 62443-3-3:2013*** *SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9* ***ISO/IEC 27001:2013*** *A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3* ***NIST SP 800-53 Rev. 4*** *AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11*

As shown in the example the framework core provides a detailed list of the Informative References to the standards and documents that each category can be supported with:

- *Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx*
- *CIS Critical Security Controls for Effective Cyber Defence (CIS Controls): https://www.cisecurity.org*
- *American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731*
- *SI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785*
- *ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: https://www.iso.org/standard/54534.html*
- *NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organisations, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Informative References are only mapped to the control level, though any control enhancement might be found useful in achieving a subcategory outcome.*

Additional standards that the NIST considers when dealing with Identity and Access Management related with health are:

- *HL7-Healthcare Privacy and Security Classification System (HCS), Release 1, August 2014 (https://www.hl7.org/implement/standards/product_brief.cfm?product_id=345) – It enables interoperable exchange of security metadata to ensure that only authorized users access protected health information*
- *HL7-PASS; SLS Release 1 June 2014 - Privacy, Access and Security Services (PASS); Security Labelling Service (SLS) describes the conceptual-level viewpoints associated with the business requirements that relate to the content, structure, and functional behaviour of information important to the Access Control area of the Privacy, Access, and Security domains within the healthcare environment.*
- *ISO 13485:2016 Provides management requirements for medical devices and related services.*
- *ISO 27799:2016 covers information security management in health using ISO/IEC 27002.*
- *IEC 82304-1:2016 for the safety and security of health software products.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- *AUTO11-A2 October 31, 2014 - Provides a framework for communication of information technology security issues between the in vitro diagnostic system vendor and the health care organisation. (https://clsi.org/standards/products/automation-and-informatics/documents/auto11/).*

Another interesting document in the NIST is the NIST SP 800-53 Rev. 5 (DRAFT): Security and Privacy Controls for Information Systems and Organisations, https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf. It provides a catalogue of security and privacy controls for information systems and organisations to protect organisational operations and assets, individuals, other organisations from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks. The controls are flexible and can be customised and implemented as part of a process to manage risk within an organisation.

2.2 European Commission Directives and Regulations

2.2.1 Directive (EU) 2016/1148. NIS Directive

The Directive on the security of information systems and networks (NIS Directive) is the first cyber security directive introduced by the European Union (EU). It was adopted on 6 July 2016 and aims to achieve a common high standard of network and information security in all EU Member States. The Directive was enforced in August 2016, with the EU Member States having 21 months to incorporate its requirements into their national legislation and an additional 6 months to identify companies subject to NIS compliance.

NIS defines a set of network and information security requirements applicable to OESs and DSPs. The term "operators of essential services" that is referred in the legislation, includes businesses in the energy, transport, banking, health, drinking water supply and distribution sectors and the digital infrastructure sectors. The NIS Directive requires each EU Member State to draw up a list of organisations in the areas that are considered key service providers.

The number of requirements depend on the appropriate incident response and the implementation of technical security measures based on risk. The requirements are designed to improve cross-border cooperation in information and network security and foster a culture of risk management.

- **EU Security Network:** To improve cross-border cooperation, the Directive will create a network of Computer Security Incident Response Teams (CSIRTs) in each Member State. Member States are also required to designate National Competent Authorities (NCAs) and Single Points of Contact (SPoC) for cybersecurity monitoring, reporting, incident response, and other cross-border coordination. CSIRTs are also required to have access to “adequate resources and equipment” including a secure and resilient infrastructure. The CSIRTs from each Member State will have a range of tasks, including monitoring national security incidents, disseminating early warnings, alerts, and announcements about cybersecurity, providing dynamic risk analysis, and coordinating with CSIRTs from other Member States.

- **Member State Strategy:** EU Member States are required to implement a national cybersecurity strategy defining security goals as well as relevant policy and regulations needed to enforce the strategy. The Directive requires that any strategy should include things like governance frameworks, response and recovery measures, public and private sector security cooperation planning, security awareness education programs, risk assessment plans, and lists of people and organisations involved in the strategy. Member States are also required to designate a minimum of one NCA to monitor the impact and implementation of the NIS Directive at national level. Each Member State SPoC must communicate with other Member States SPoCs to enhance cooperation as well.

- **Cooperation Group:** In addition to the other bodies established by the NIS Directive, there is a further requirement to create a Cooperation Group whose purpose is to facilitate collaboration around cybersecurity between Member States. The Cooperation Group is made up of representatives from Member States and ENISA with a member of the European Commission acting as secretariat. The Cooperation Group is focused on planning, steering, and reposting on the implementation of the NIS Directive. The Group's chief responsibilities include offering guidance to the newly-established CSIRTs network, helping Member States pinpoint which services should be categorised as "operators of essential services," engaging with relevant bodies on security-related incidents and issues, sharing security best practices, and generally raising awareness on cybersecurity in the EU. The Group must also file a report every 18 months providing some detail on the level of cooperation taking place and the progress of NIS Directive implementation.

- **Incident Reporting:** Those organisations who qualify as Data Security and Protection (DSP) under the Directive's criteria must implement a range of risk management measures both technical and operational. DSP organisations must comply with the Directive's incident reporting protocol, which requires that organisations notify "without undue delay" CSIRTs and other relevant bodies about any significant security incidents encountered.

There are a number of steps every organisation should take to ensure they remain in compliance with the NIS Directive.

- **Contact NCAs:** Organisations within the scope of the Directive should contact their Member State's NCA to find out which authority to contact in the event of a security incident and also to figure out which body can sanction them in the event of non-compliance.
- **Liaise with CSIRTs:** Organisations should contact CSIRTs to obtain information about current security threats and get further clarity on cybersecurity issues.
- **Implement technical and organisational security measures:** The Directive requires organisations to implement a range of security measures in areas like system security, incident management, testing, and compliance with international standards. While the Directive is short on specifics, organisations should follow all industry cybersecurity best practices and look to meet other compliance regulations such as the GDPR, many of which have overlapping requirements. Organisations should also conduct risk assessments regularly and implement measures to mitigate identified risks.
- **Implement an effective security incident response process:** Incident reporting is a key part of the Directive. You should hone your own incident reporting process including things like number of users affected, duration of incident, geography, economic impact, and service disruption. Upon discovery of an incident, notification should be made to the NCA or CSIRT "without delay." [56]

ENISA's recommendations for the Healthcare sector are listed below [57]:

ENISA recommendations – for Hospitals

- Establish effective **enterprise governance** for cyber security
- Implement **state-of-the-art security measures**
- Provide specific IT security requirements for IoT components in the hospital
- **Invest** on NIS products over IoT components
- Establish an **information security sharing mechanism**
- Conduct **risk assessment and vulnerability assessment**
- Perform **pen testing and auditing**
- Support **multi-stakeholder communication platforms** (ISACs) and information sharing alternatives

ENISA recommendations – For IoT devices manufacturers

- Incorporate security into existing quality assurance systems

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- Involve third parties in testing activities
- Consider applying medical device regulation to critical infrastructure components
- Support the adaption of **information security standards** to healthcare

ENISA recommendations – For Policy makers

- Promote collaboration on cyber security across Europe
- Develop **awareness raising** on IoT threats and risks
- Establish a **governance model** for cyber security
- Integrate (trade-off risk/investment) **security in business processes**
- Define security requirements to ensure "security for safety"

2.2.2 Regulation (EU) 2016/679 GDPR

The General Data Protection Regulation (GDPR) is a legal framework setting the regulations on how to collect and process the personal information of EU citizens. GDPR sets the principles for information management and citizens' rights. These regulations also contain safeguards to ensure that healthcare data is safe for any cyberattacks, misuse, or embezzlement. Misuse of healthcare data by any citizen of the European Union or improper law enforcement can have particularly serious long-term consequences. Anyone in the EU who controls data and/or undertakes data processing, is bound by the GDPR. This includes the health care sector and also affects organisations located outside the EU. In addition, the GDPR has extensive responsibilities and obligations for data controllers and processors.

Auditors should determine or modify technical and organisational measures to ensure and demonstrate that the processing of personal data is fully compliant with GDPR requirements. The way in which data protection policies are implemented will be important here. Processors will be required to keep records of all their processing activities and to maintain readiness to disclose this information to demonstrate compliance. In addition, processing on behalf of a controller should be specified in a contract or other "legal act" in accordance with the criteria set out in the GDPR. The healthcare sector should therefore adopt a more holistic approach to data management. If done properly, the burden will be moderated by rewarding the knowledge of where the data is and where it is going, thus allowing good compliance practice and risk reduction.

Data concerning health has special mention under the GDPR. It defines "personal" data as "any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Further, the GDPR contains three additional important definitions that pertain to health data:

"Data concerning health" by the GDPR is defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

"Genetic data" is defined as "personal data relating to inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question".

"Biometric data" is "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

It is important to notice that "data concerning health," "genetic data" and "biometric data" will be subject to a higher standard of protection than personal data in general. The processing of these three forms of health data is prohibited, unless one of several conditions applies. These health-specific conditions are as follows:

The data subject must have given “explicit consent” to the processing.

“Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (GDPR article 9 section 2.h)[7]”.

“Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices (GDPR article 9 section 2.h).”

When processing health data, the healthcare sector will have to implement their data processing operations in accordance to these conditions (or one of the other conditions). Healthcare organisations will as a result have to be more careful with the data and more exact in knowing where it is being stored, how it is being processed and whether consent has been given.

Consent has been fine-tuned under the GDPR, and it is described as: “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.” An active process will have to be put in place, which “could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data.” It must also be demonstrated that consent has been provided. A clause of the GDPR permits consent to be valid where given prior to the full 25 May 2018 date of the application of the GDPR, if it is given in conformity with the GDPR. One of the GDPR’s health data conditions calls for “explicit consent,” but the general definition makes no reference to the word “explicit.” This has led to an on-going debate about whether there is a difference between “unambiguous” consent and “explicit” consent, and if so, what that difference might be. This issue could affect the practical implementation of consent in products, services, websites, etc. However, explicit consent for healthcare purposes is very likely to always require the strongest forms of agreement, such as an opt-in tick-box or a declaratory statement. The healthcare sector will also have to take a cutting-edge approach to obtaining consent. Consent will need to cover as many potential transfers of health data as possible, including international data transfers and cloud storage. Also, the consent must include the personal health data storage period and the rights regarding access, rectification, erasure, restriction of processing and withdraw.

Data Protection Impact Assessments (DPIAs) will be required when health data of the three kinds mentioned above is processed on a large scale. A DPIA is a type of risk assessment of the impact of the anticipated processing activities on personal data. A data protection regulator will also have to be consulted prior to personal data being processed when an assessment “indicates that the processing would result in a high risk in the absence of measures taken by a data controller to mitigate the risk.

One of the most important changes under the GDPR, is mandatory data breach reporting. Breaches must be reported to a data protection regulator within 72 hours, and those affected by the breach must also be informed. The healthcare sector will therefore have to put in place clear, practical and effective procedures that can be acted upon immediately—this should be at the top of its GDPR compliance checklist. It cannot be emphasised enough how important it will be to undertake training and fire drills [58].

2.2.3 Comparison between the GDPR and the NIS Directive

With these in mind, the European Directives of NIS and GDPR deal with different issues: GDPR focuses on the

[7] https://gdpr-info.eu/art-9-gdpr/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

protection of the personal data of any Organisation that holds European citizens' data, while NIS focuses on the security of the organisations' systems operating within the European Union.

NIS is about the security of the networks, the information systems and digital data in them. By using the term "digital data", it is understood that any physical data is not covered by NIS. By contrast, with GDPR, personal data can be, for example, a filing system etc. On the other hand, the NIS is wider than the GDPR because it covers "digital data", which not only includes personal data, but any data about an organisation's networks and information systems that ensure its functionality and continuity.

Another thing to be taken into account, is the fact that there is an overlap between the two regulations due to the security requirements of GDPR and those of NIS. For example, GDPR also includes the classical information security concept of the CIA Triplet (Confidentiality Integrity Availability). This means that there is much greater alignment between the requirements of the GDPR Directive and the NIS Directive. GDPR security provisions and the likelihood that most organisations are already covered by NIS, go to the effect that they will also control personal data or even process personal data.

Finally, GDPR is a law to be followed by all Member States. The law will not differ from one EU Member State to another. An excellent example is the size of the fines and penalties imposed on them. While the GDPR has set the number of fines imposed on law enforcement agencies, there is no such clarity in the case of NIS. It is the responsibility of the individual governments of the States to determine the fines. While the GDPR applies to all organisations dealing with the personal data of EU residents within the EU and abroad, NIS only deals with a specific set of agencies operating within the EU.

3 Research Initiatives

3.1 Ongoing EU Research in healthcare data security

Healthcare is an attractive and soft target for cybercrime due to two reasons:(1) it is a rich source of valuable data and (2) its defences are weak. Cybersecurity breaches include stealing health information and ransomware attacks on hospitals and could include attacks on implanted medical devices. As a consequence of such attacks primarily aiming to cripple health systems and threaten human life, a reduced patient trust is observed. Ultimately, cybersecurity is critical to patients' data safety. Changes are required in terms of enhancing the privacy of medical data to be stored as well as privacy mechanisms for accessing such data as part of a holistic solution.

Among the most sophisticated techniques, de-identification and anonymisation are devised for medical data protection in an EU funded project called BIGMEDILYTICS (www.bigmedilytics.eu). This project also uses the HTTPS protocol and single factor authentication to protect the medical data. In an EU project called SHIELD (www.project-shield.eu), risks in exchanging health data from insecure mobile devices were addressed. For better security, such data are reported to be encrypted using AES 256 in many EU projects, however this reduces the usability of the data. Although data privacy is partly addressed, medical systems suffer due to lack of privacy preserving access mechanisms. The searchable encryption technique (homomorphic encryption, Figure 5) that is developed by Tech-Inspire (TEC-I) allows one to search through a database of encrypted documents. This is based around partial homomorphic encryption hence it is computationally efficient and provides the maximum level of privacy by protecting against statistical and information leakage attacks.

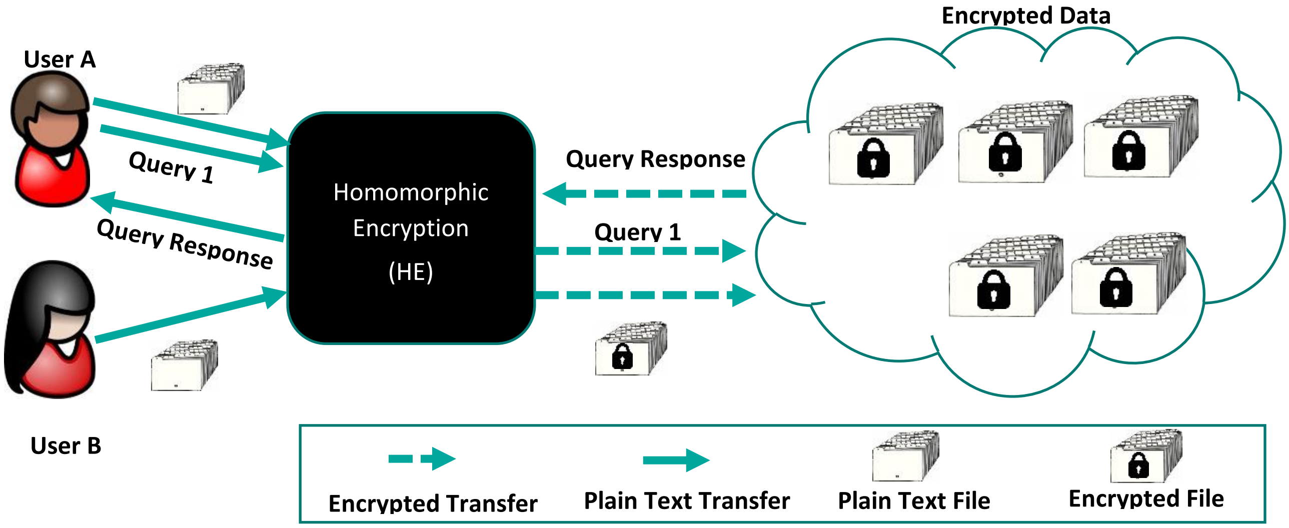


Figure 5 Homomorphic Encryption

Following is a comprehensive list of EU related projects that are in some way related to the cybersecurity landscape.

SHIELD - **European Security in Health Data Exchange** (H2020-DS-2015-1, 2017-2020, https://www.project-shield.eu): SHiELD aims to create an open and extendable security architecture supported by security mechanisms and privacy by design modelling and analysis tools to provide systematic protection for the storage and exchange of health data across European borders, subject to control by the data subjects, compatible with existing regulatory frameworks, ensuring the privacy, availability and correctness of the data while improving trust of patients in the security of their data and its use to address their needs.

ENACT Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems – H2020, 2018-

2020. The main technical goal of ENACT is to develop novel IoT platform enablers to: i) Enable DevOps in the realm of trustworthy smart IoT systems, and enrich it with novel concepts for end-to-end security and privacy, resilience and robustness strengthening trustworthiness, taking into account the challenges related to “collaborative” actuation and actuation conflicts; ii) Facilitate the smooth integration of these to leverage DevOps for existing and new IoT platforms and approaches (e.g., FIWARE, SOFIA, and TelluCloud).

This will be accomplished by evolving current DevOps methods and techniques to support the agile development and operation of smart IoT systems and provide a set of novel mechanisms to ensure quality assurance and trustworthiness, such as actuation conflict handling, continuous testing and delivery across IoT, edge and cloud spaces and end to end security and privacy management. Through this ENACT will provide a DevOps framework for smart IoT Systems. There is an eHEALTH use case in which privacy threats on IoT environments is address.

PoSeID-on - Protection and control of Secured Information by means of a privacy enhanced Dashboard (H2020 DS-08-2017, 2018-2020, https://www.poseidon-h2020.eu/): PoSeID-on is aimed at developing a novel Privacy Enhancing Dashboard for personal data protection supporting the pillars of the new EU’s GDPR with regards to digital security, that will be implemented within a single, integrated tool, adopting blockchain and smart contracts technology. The aim of PoSeID-on is empowering data subjects in having a concise, transparent, intelligible and ease access, as well as tracking, control and management of their personal data processed by public and private organisations, acting as data controllers and/or data providers, as well as supporting organisations in data management and processing while ensuring GDPR compliance.

SPARTA is a novel Cybersecurity Competence Network, supported by Europe’s H2020 program, with the objective to develop and implement top-tier research and innovation cooperative actions. Strongly guided by concrete challenges forming an ambitious Cybersecurity Research & Innovation Roadmap, SPARTA will setup unique collaboration means, leading the way in building transformative capabilities and forming a world-leading Joint Competence Centre Infrastructure. From basic human needs (health) to economic activities (energy, finance, and transport) to technologies (ICT and industry) to sovereignty (eGovernment, public administration), four research and innovation programs will push the boundaries to deliver advanced solutions to cover emerging challenges.

KONFIDO (https://konfido-project.eu/**)** will enable secure exchange, processing and storage of health related data, using privacy by design principles. The federation architecture will enable cross-border interoperation of eHealth services provided by individual countries while each participating entity (private and public actors, empowered citizens) will be able to implement specific policies for the protection and control of personal and health related data.

The potential threats of healthcare cybersecurity vulnerabilities on storage medical data and medical devices inspire the work of many researchers and business companies around the world (Table 2 Scientific papers published on cybersecurity field topic). The table presents scientific papers published in the healthcare cybersecurity field. All of the articles are in agreement in acknowledging the growing threat of cyber-attacks in healthcare and the systematic unpreparedness in dealing with cyber threats.

Table 2 Scientific papers published on cybersecurity field topic

Wu et al. [59]	Introduces the topic of new wireless applications of medical devices left vulnerable to cyber-attacks and how safety risk management in manufacturing is being redefined to address growing cybersecurity threats.
Blanke & McGrady [60]	Discusses the emerging threat of cyber-attacks. The article provides a useful checklist tool to assess and monitor common risks.
Koppel et al. [61]	Discusses cybersecurity issues and why some overly burdensome cybersecurity rules and regulations are prompting physicians to work around cyber safety measures to complete their work.
Page et al. [62]	Analyses cybersecurity within Telehealth technologies and how end-to-end encryption methods could make cloud storage and access of Protected Health Information.
Rios [63]	Discusses how medical devices in cybersecurity as medical devices become increasingly networked and wireless. There is the possibility of knowing the motivations for attacks and what attackers will be targeting.
Coronado et al. [64]	Explores the idea of cybersecurity of medical devices and how increased integration of medical devices into healthcare IT systems leaves new networked medical devices exposed to cyber threats in ways they have not been in the past. The author goes on to provide steps hospitals can take to prevent attacks.
Zubaydi et al. [65]	Presents the vulnerabilities of mobile devices in online medical appointments.
Fu & Blum [66]	Overview of the cybersecurity risks of medical device software.
Kruse et al [67]	Systematic review to identify cybersecurity trends, including ransomware, and identify possible solutions by querying academic literature.

4 Workshop on Cyber Situation Awareness (ALL)

Within the context of SPHINX project, a workshop on cyber situation awareness, was organised on July 2019 in Brussels, hosted by VUB. Various stakeholders participated, whose expertise gave rise to a variety of interesting discussions. Thanks to the content of the talks, and the diversity of the participants, the elicited results provide us with useful insight about the cybersecurity landscape. The following subsections present and elaborate on the produced outcomes.

4.1 Targeted Stakeholders

Several diverse stakeholders who work in the ICT domain, participated in the workshop. The workshop specifically targeted healthcare institutions' personnel (IT, administrative, etc.). Nevertheless, it attracted various other stakeholders from the wider area of ICT, such as IT-oriented SMEs, European Initiatives for cybersecurity (ENISA), and related EU-funded projects. The purpose of gathering such a diverse audience and participators, was to initiate a wide conversation concerning cybersecurity, elaborating on the current situation and existing solutions, exchange opinions about current issues and potential solutions, and finally gain an overview of the current standards, directives and mandates, imposed by the EU or other national or international bodies.

4.2 Questioner for Stakeholders, End-users and Experts

During the workshop, a structured/weighted questionnaire was circulated for the participating stakeholders, end-users and experts to fill in. The questionnaire posed questions concerning cybersecurity incidents in their organisations, the assets that were compromised and the actions that were taken to address/mitigate the impact of those attacks.

4.3 Initial Findings

The questionnaire itself, and the diversity of the participants, produced some very interesting qualitative and quantitative results. The participating stakeholders were mostly between 35-50 years old (61,5%) and 25-35 years old (30,8%).

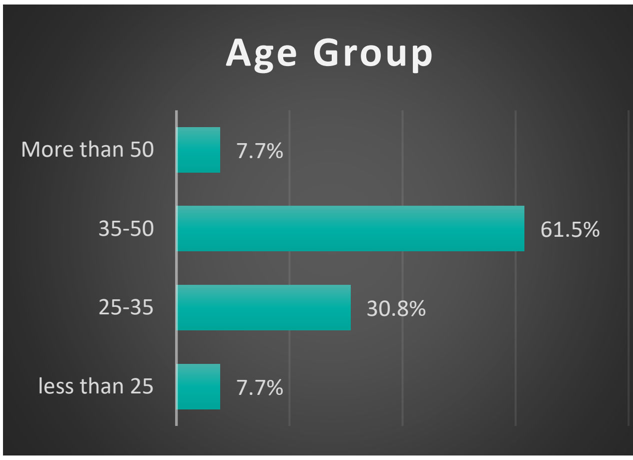


Figure 6 Age group

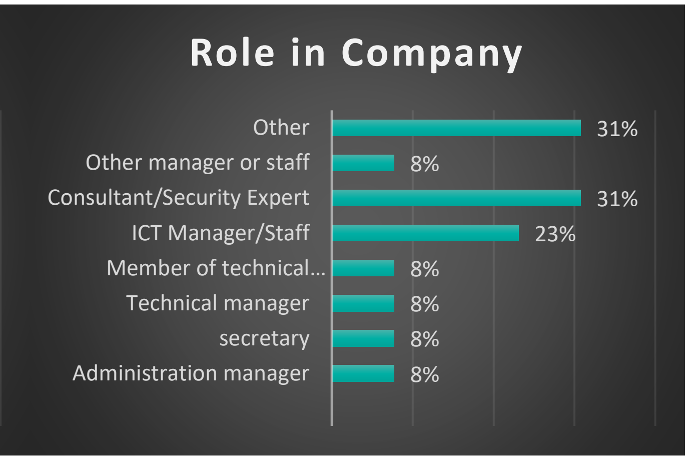


Figure 7 Role in the company

Their IT level was mostly level 5 (proficient computing, applications and programming) by 53,8%. Stakeholders with IT skills at level 4 and 3 were by 23,1%. 31% of the participants were Consultants or security experts. 23% were OCT managers or staff. Interestingly, 69,2% of the participants indicated that their organisations do not formally comply with any cybersecurity certification whatsoever. 23,1% said that they were certified under ISO/IEC27001:2013 certification.

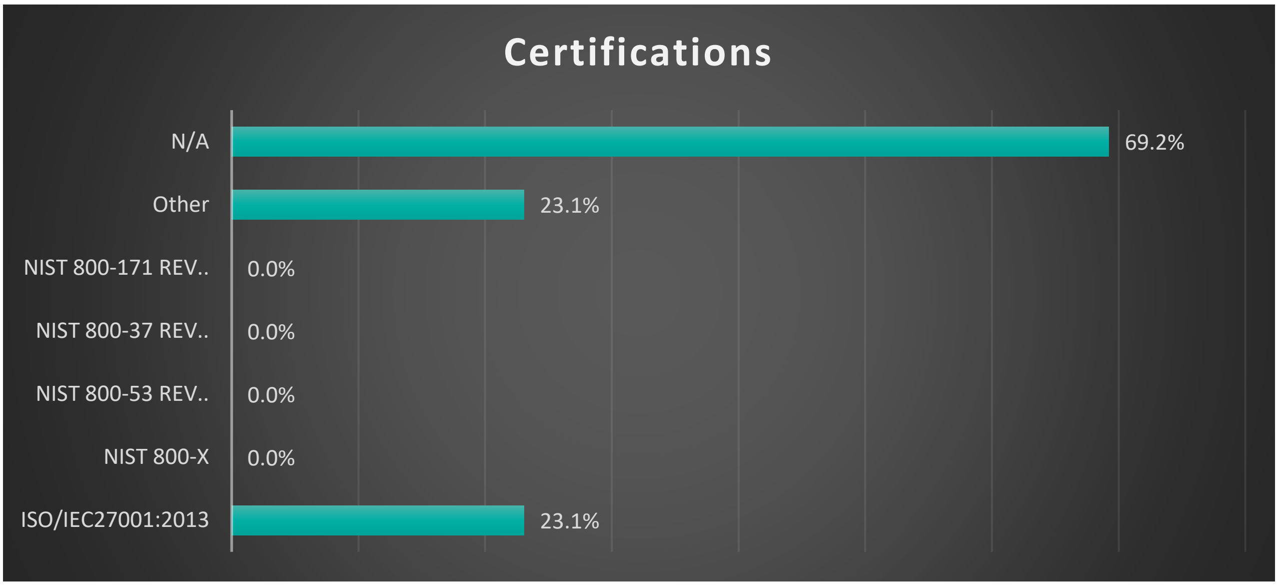


Figure 8 Organisations' certifications

The participants were asked to provide a prioritisation of cybersecurity risks, according to their corporate/personal point of view. 69,2% indicated that missing authorization for critical actions is the most critical cyber threat to their organisations. Moreover, 46,2% indicated that path traversal, cross-site scripting and download of malicious code, poses a severe threat no ICT infrastructures.

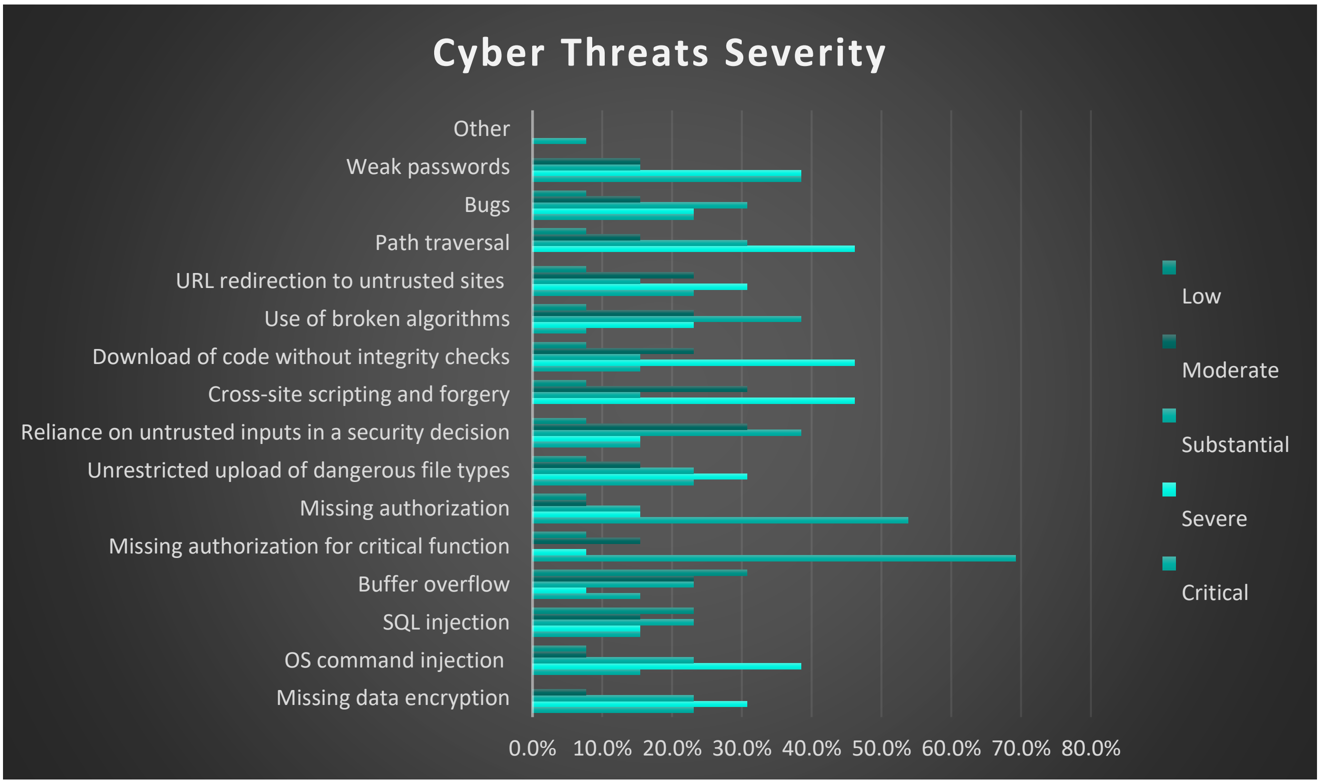


Figure 9 Cyber threats severity

Consequently, they were asked to provide information about specific incidents that took place within their organisations, what assets were compromised, and what measures were taken to address/mitigate them. 69,2% indicated that they were attacked by phishing methods, 53,8% replied that they suffered from ransomware and denial of service attacks. Moreover, 46,2% mentioned that malware programs were unwillingly installed on employees' terminals. 23% indicated that their organisations are attacked almost every

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

week

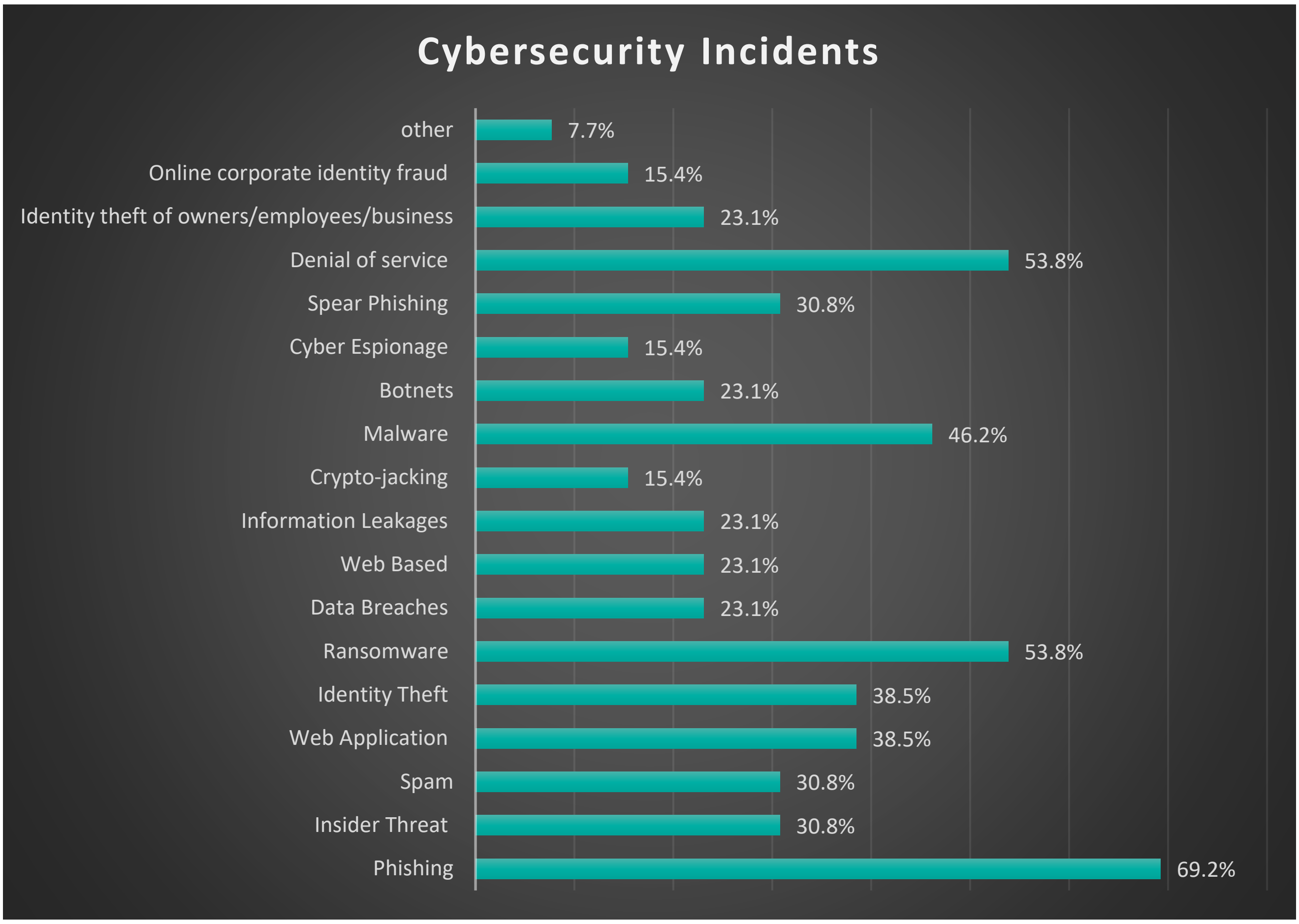


Figure 10 Cybersecurity incidents

The attacks were reported to be successful by 30,8% of the participants. By majority, the assets that were compromised were clinical or administrative data (46,2%) and specialised services or infrastructure were partially harmed (23,1%). Finally, 15,4% indicated that more novel firewalls were deployed, and user awareness internal campaigns were initiated to mitigate the problem.

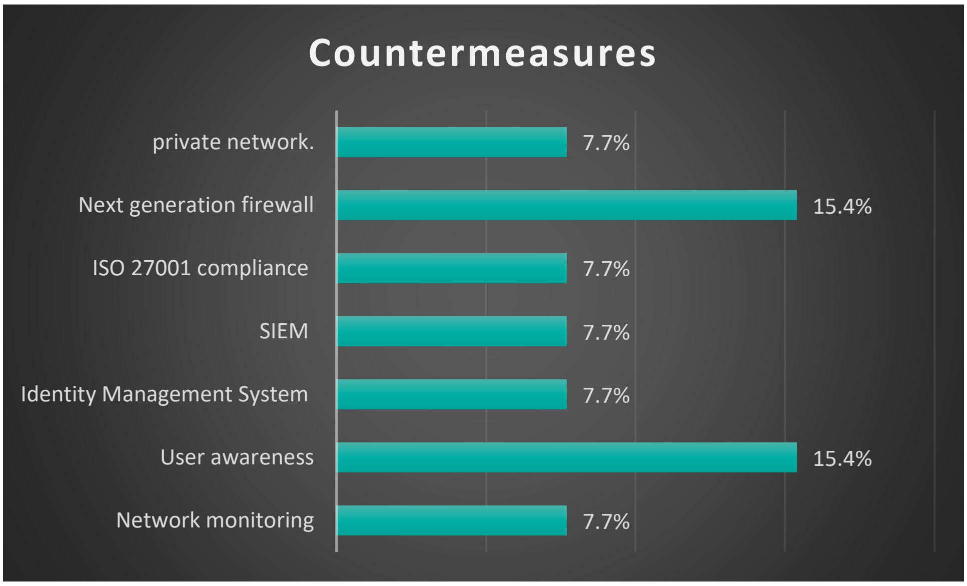


Figure 11 Countermeasures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

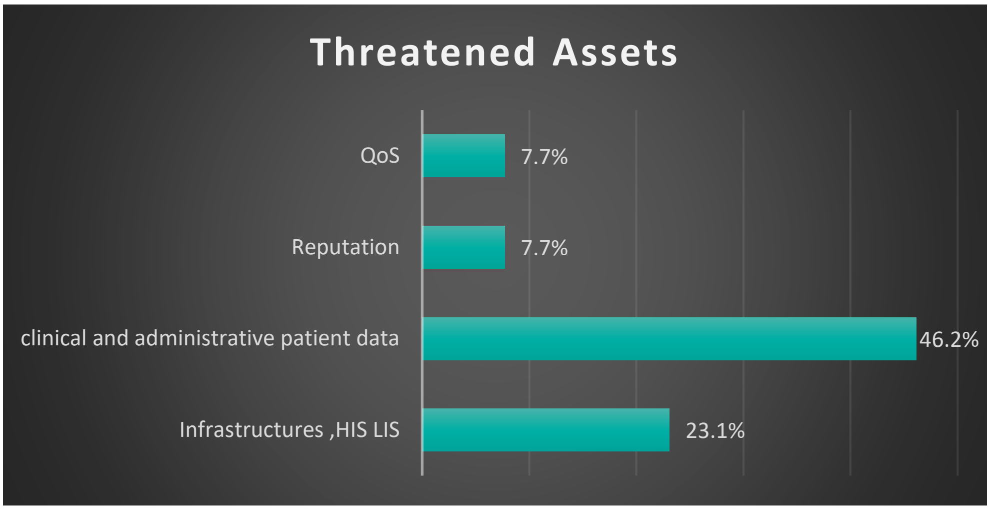


Figure 12 Threatened assets

4.4 Conclusions

The workshop was successfully concluded, and very useful outcomes were produced. The most prevalent insights that were gained, were that organisations, struggle with the certification (ISO27001, NIST 800-171, etc.) of their infrastructures and workflows, thus remaining exposed to well-known system vulnerabilities, and persist on employing bad tactics concerning routine procedures. Ransomware, denial of service and malware attacks more often manifest through phishing attacks, or network propagation. Almost 31% of the attacks are successful, and attackers keep attacking the same infrastructure almost every week by 23,1%. Finally, the main reasons for the successful manifestation of attacks is the lack of (cyber) security awareness from the side of the end user, and the poor configuration of systems, networks and authorisation frameworks.

The outcomes of the questionnaires will be rather useful for SPHINX, as certain results, such as the attack occurrence and the attack type probability will act as input for core cybersecurity components such as the risk assessment module. Additionally, developers will also take these outcomes under consideration to design and build more robust and secure APIs and applications.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5 Conclusions

This document provided a thorough overview of the current status of the cyberthreat landscape by providing a detailed taxonomy. Additionally, existing and emerging standards, policies and mandates deriving from the EU and other standardisation entities, were presented and detailed. Current research initiatives concerning cybersecurity and data security in the healthcare domain were presented. Finally, the aggregated quantitative and qualitative results, from a series of questionnaires gathered during the first workshop that was organised by the SPHINX consortium, in July 2019, were presented and elaborated upon. This document will act as a direct complementary input for the tasks related to the production and iterative refinement of user stories, use cases and finally user/system requirements of the SPHINX architecture (T2.4, T2.5).

Annex I: **References**

[1] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Centre, January 2019, https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/.

[2] David Emm, Roman Unucheck and Kirill Kruglov, *Kaspersky Security Bulletin 2016 – Review of the Year*, Kaspersky, December 14th 2016, https://www.kaspersky.com/about/press-releases/2016_kaspersky-labs-threat-review-for-2016.

[3] Kate O'Flaherty, *Breaking Down Five 2018 Breaches -- And What They Mean For Security In 2019*, Forbes, December 19th 2018, https://www.forbes.com/sites/kateoflahertyuk/2018/12/19/breaking-down-five-2018-breaches-and-what-they-mean-for-security-in-2019/#2cb1006741c4.

[4] Taylor Armerding, *The 18 biggest data breaches of the 21st century - Security practitioners weigh in on the 18 worst data breaches in recent memory*, CSO Online, December 20th 2018, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[5] *Significant Cyber Incidents*, Centre for Strategic and International Studies, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

[6] Andreas Sfakianakis, Christos Douligeris, Louis Marinos, Marco Lourenço and Omid Raghimi, *Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends*, Final Version 1.0, ETL 2018, ENISA, January 2019.

[7] John Lovelock, *The Internet of Things is Shifting Hackers' Targets*, Gertner, March 11th 2016, https://www.gartner.com/smarterwithgartner/the-internet-of-things-is-shifting-hackers-targets/.

[8] *ThreatMetrix European Cybercrime Report: Q1 2018,* ThreatMetrix, 2018, https://www.threatmetrix.com/info/2018-cybercrime-europe/.

[9] *Threat Landscape Report - Q4 2017*, Fortinet, February 2018, https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q4-2017.pdf.

[10] *State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks*, European Commission, Brussels, September 19th 2017, http://europa.eu/rapid/press-release_IP-17-3193_en.htm.

[11] Jay J., *Healthcare sector suffered more than half of all cyber-attacks in 2017*, 2018. https://www.scmagazineuk.com/healthcare-sector-suffered-half-cyber-attacks-2017/article/1472744.

[12] *2018 Thales Data Threat Report – Trends in Encryption and Data Security – European Edition*, Thales Security, https://www.thalesesecurity.co.uk/2018/euro-data-threat-report.

[13] Camino Mortera-Martinez, *Game Over? Europe's Cyber Problem*, Centre for European Reform, Open Society – European Policy Institute, July 2018, https://www.cer.eu/sites/default/files/cover_pbrief_game_over2_9.7.18.pdf.

[14] *Reform of cybersecurity in Europe*, European Council, https://www.consilium.europa.eu/en/policies/cyber-security/.

[15] *2018 Cost of a Data Breach Study: Global Overview*, IBM Security and Ponemon Institute, July 2018, https://www.ibm.com/downloads/cas/861MNWN2.

[16] *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation*, Juniper Research, May 2015, https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2trillion.

[17] Michael Ash, *The Looming Threat of Health Care IoT Devices*, Security Intelligence IBM, May 15th 2017, https://securityintelligence.com/the-looming-threat-of-health-care-iot-devices/.

[18] *Information for Healthcare Organisations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software"*, US Food and Drug Administration, https://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm.

[19] Salwa Rafee, *Data Activity Monitoring Gives Health Care Organisations X-Ray Vision Into Medical Imaging Security Risks*, Security Intelligence IBM, September 25th 2017, https://securityintelligence.com/data-activity-monitoring-gives-health-care-organisations-x-ray-vision-into-medical-imaging-security-risks/.

[20] Ladi Adefala, *Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries*, Fortinet, March 6th 2018, https://www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.

[21] *2018 Cyber Claims Study*, Net Diligence, Version 1.0, https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf.

[22] Dimitra Liveri, Anna Sarri and Christina Skouloudi, *Security and Resilience in eHealth – Security Challenges and Risks*, European Union Agency for Network and Information Security - ENISA, 2015, https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services.

[23] *Cyber Attacks: In the Healthcare Sector*, Center for Internet Security, 2019.

[24] Nate Lord, *Top 10 Biggest Healthcare Data Breaches of All Time*, Digital Guardian, June 25th 2018, https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time.

[25] *The biggest healthcare data breaches of 2018 (so far)*, Healthcare IT News, https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far.

[26] Alex Dobuzinskis and Jim Finkle, *California hospital makes rare admission of hack, ransom payment*, Reuters, February 19th 2016, https://www.reuters.com/article/us-california-hospital-cyberattack/california-hospital-makes-rare-admission-of-hack-ransom-payment-idUSKCN0VS05M.

[27] Sir Amyas Morse KCB, *Investigation: WannaCry cyber attack and the NHS*, National Audit Office, April 25th 2018, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[28] Understanding the Depth of the Global Ransomware Problem – An Osterman Research Survey Report, Malwarebytes, August 2016, https://www.malwarebytes.com/surveys/ransomware/?aliId=13242065.

[29] *An Ounce of Prevention – A 12 Month Analysis of Ransomware, Email Fraud and Other Healthcare Threats – And How You Can Stop Them*, Proofpoint, 2018, https://www.proofpoint.com/sites/default/files/pfpt-us-tr-2018-healthcare-threat-report-181005.pdf.

[30] Henry Bodkin, Barney Henderson, Laura Donnelly, Robert Mendick, Ben Farmer and Chris Graham, *Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms*, The Telegraph, May 13th 2017, https://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/.

[31] Thomas Brewster, *Medical Devices Hit By Ransomware For The First Time In US Hospitals*, Forbes, May 17th 2017, https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#360e4ae6425c.

[32] Linn Foster Freedman, *Medical Device Malware Medjack.3 Poses Threat to Hospitals*, March 9th 2017, Data Privacy+Security Insider, https://www.dataprivacyandsecurityinsider.com/2017/03/medical-device-malware-medjack-3-poses-threat-to-hospitals/.

[33] *Survey Reveals Healthcare IT Decision-Makers' Approach to IoT Security*, ZingBox, PRNewswire, July 19th 2017, https://www.prnewswire.com/news-releases/survey-reveals-healthcare-it-decision-makers-approach-to-iot-security-300490630.html.

[34] *Edge Computing in Healthcare*, HIMSS, January 29th 2019, https://www.himsslearn.org/executive-summary-2-edge-computing-strategic-considerations-and-benefits.

[35] Mayra Rosario Fuentes, *Cybercrime and Other Threats Faced by the Healthcare Industry*, TrendLabs Research Report, Forward-Looking Threat Research (FTR) Team, TrendMicro, 2017, https://www.trendmicro.com/content/dam/trendmicro/global/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf.

[36] Eduard Marin and et.al., *On the (in)security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them*, ACSAC 2016, December 05th-09th 2016, Los Angeles, United States, DOI: http://dx.doi.org/10.1145/2991079.2991094.

[37] *Johnson & Johnson Warns Patients of an Insulin Pump Cyber Bug*, Fortune, October 4th 2016, http://fortune.com/2016/10/04/johnson-johnson-insulin-pump-cyber-bug/.

[38] Lisa Vaas, *Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking*, naked Security SOPHOS, October 22nd 2013, https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/.

[39] *Protected Health Information Data Breach Report*, Verizon, 2018, https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pdf.

[40] Preston Gralla, *Medical IoT devices: the security nightmare that keeps CIOs up late at night*, Hewlett Packard Enterprise, September 25th 2017, https://www.hpe.com/us/en/insights/articles/medical-iot-devices-the-security-nightmare-that-keeps-cios-up-late-at-night-1709.html.

[41] *2018 Thales Data Threat Report Healthcare Edition*, Thales Security, https://dtr-healthcare.thalesesecurity.com.

[42] Laurie Pycroft, *Brainjacking – A new cyber-security threat*, The Conversation, August 23rd 2016, https://theconversation.com/brainjacking-a-new-cyber-security-threat-64315.

[43] James Coker, *Combatting The Threat Of Cyber Attacks In Healthcare*, European Medical Group, August 10th 2018, https://www.europeanmedical-group.com/omnipresent/combatting-the-threat-of-cyber-attacks-in-healthcare/.

[44] Rebecca Weintraub and Joram Borenstein, *11 Things the Health Care Sector Must Do to Improve Cybersecurity*, Harvard Business Review, June 1st 2017, https://hbr.org/2017/06/11-things-the-health-care-sector-must-do-to-improve-cybersecurity.

[45] Nathan Eddy, *5 cybersecurity threats healthcare faces in 2019 and beyond*, Healthcare IT News, February 8th 2019, https://www.healthcareitnews.com/news/5-cybersecurity-threats-healthcare-faces-2019-and-beyond.

[46] McAfee Labs Threats Report, April 2017. Available at: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2017.pdf

[47] Inside Mirai the infamous IoT Botnet: A Retrospective Analysis. December 2017. Available at: https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

[48] Internet Security Threat Report (Symantec) http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

[49] Cisco 2018 annual cybersecurity report https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2)

[50] Steve Purser, Best Practices in Computer Network Defense: Incident Detection and Response, European Union Network and Information Security Agency (ENISA), 2014 The authors and IOS Press

[51] ISO, ISO/IEC 27032:2012(en), https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

[52] ISO/IEC 27032:2012 — Information technology — Security techniques — Guidelines for cybersecurity, http://www.iso27001security.com/html/27032.html

[53] Antonio Jose Segovia, August 25, 2015, ISO 27001 vs. ISO 27032 cybersecurity standard, https://advisera.com/27001academy/blog/2015/08/25/iso-27001-vs-iso-27032-cybersecurity-standard/

[54] ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements (second edition), http://www.iso27001security.com/html/27001.html

[55] ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements, https://www.iso.org/standard/54534.html

[56] Nate Lord, Wednesday September 12, 2018, what is the NIS Directive? Definition, Requirements, Penalties, Best Practices for Compliance, and More, https://digitalguardian.com/blog/what-nis-directive-definition-requirements-penalties-best-practices-compliance-and-more

[57] ENISA, The NIS Directive and Cybersecurity in eHealth, https://www.enisa.europa.eu

[58] JONATHAN P. ARMSTRONG - ANDRÉ BYWATER, WHAT HEALTHCARE ORGANISATIONS SHOULD KNOW ABOUT THE GDPR, 2017, https://whitepapers.em360tech.com/wp-content/uploads/GDPR-Implications-of-the-GDPR-in-Healthcare-042717-d1.pdf

[59] F. Wu, S. Eagles, and S. Eagles, “Cybersecurity for Medical Device Manufacturers : Ensuring Safety and Functionality,” no. February, pp. 23–35, 2016.

[60] B. S. J. Blanke and E. Mcgrady, “When it comes to securing patient health information from breaches , your best medicine is a dose of prevention : A cybersecurity risk assessment checklist,” vol. 36, no. 1, 2016.

[61] R. Koppel, S. Smith, J. Blythe, and V. Kothari, “Workarounds to Computer Access in Healthcare Organisations : You Want My Password or a Dead Patient ?,” pp. 215–220, 2015.

[62] A. Page et al., “Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance,” pp. 1–10, 2014.

[63] V. From and T. H. E. Top, “Cybersecurity Expert : Medical Devices Have ‘ A Long Way to Go ,’” no. June, pp. 197–202, 2015.

[64] A. J. Coronado, T. L. Wong, and J. Anthony, “Healthcare Cybersecurity Risk Management: Keys to an Effective Plan,” pp. 26–31, 2014.

[65] F. Zubaydi, A. Saleh, F. Aloul, and A. Sagahyroon, “Security of Mobile Health (mHealth) Systems,” 2010.

[66] K. Fu and J. Blum, “Inside Risks Controlling for Cybersecurity Risks of Medical Device Software,” pp. 21–23, 2011.

[67] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, “Cybersecurity in healthcare: A systematic review of modern threats and trends,” vol. 25, pp. 1–10, 2017.

[68] N. Institute of Standards, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” 2014.

Annex II: Significant Cyber Attacks (2006-2019)

II.1 TJX Companies, Inc.

Date: December 2006

Impact: Data of 94 million credit cards exposed.

Details: The source of the attack is still unclear: either the hackers took advantage of a weak data encryption system and stole credit card data during a wireless transfer between two Marshall's stores in Miami, or the hackers broke into the TJX network through in-store kiosks that allowed people to apply for jobs electronically.

II.2 Heartland Payment Systems

Date: March 2008

Impact: Data of 134 million credit cards exposed; Heartland was deemed out of compliance with the Payment Card Industry Data Security Standard and was not allowed to process the payments of major credit card providers until May 2009; Heartland paid $145 million in compensation for fraudulent payments.

Details: Albert Gonzalez and two unnamed Russian accomplices used SQL injection to install spyware on Heartland's data systems, an attack that was only discovered in January 2009, when Visa and MasterCard notified Heartland of suspicious transactions from accounts it had processed.

II.3 Power Grids, Water Supplies and Public Transportation Systems

Date: January 2010

Impact: Destruction of 984 uranium enrichment centrifuges in fifteen Iranian nuclear facilities, representing a 30% decrease in enrichment efficiency.

Details: Attributed to a joint effort by the US and Israel, this cyberattack used the malicious Stuxnet malware to target the Siemens SCADA systems and Iran's nuclear power program. It is believed that this attack was initiated by a random worker's USB drive. It also served as an example for real-world intrusion and service disruption of power grids, water supplies or public transportation systems.

II.4 VeriSign

Date: 2010

Impact: Undisclosed information stolen.

Details: Hackers gained access to privileged systems and information in the company’s computers and servers.

II.5 EMC RSA Security

Date: March 2011

Impact: Personal data of 40 million employees was stolen; EMC spent more than £66 million on remediation costs.

Details: Two separate hacker groups worked in collaboration to launch a series of phishing attacks against the security giant’s employees, posing as individuals the employees trusted, to penetrate the company's network.

II.6 Sony’s PlayStation Network

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Date: April 2011

Impact: Personal data (names, passwords, e-mails, home addresses, purchase history, credit card numbers and PSN/Qriocity logins and passwords) of 77 million users was leaked; banking information of tens of thousands of players was compromised; Sony closed operations of the PlayStation Network, the Sony Online Entertainment and Qriocity for one month bearing losses estimated at $171 million; Sony paid $15 million in compensation to those whose bank accounts were illegally used.

Details: Hackers used a well-known network vulnerability to breach the Sony network and, as the players' data was unencrypted, it was easily hijacked through a very simple Structured Query Language (SQL) injection.

II.7 Yahoo!

Date: July 2012

Impact: Account data (username and passwords) of 400 million customers was compromised.

Details: The hacker Peace stole a cache of e-mail addresses and encrypted passwords of 400 million customers of Yahoo! and sold it online for $1900. The hacker said the attack was meant as a warning to Yahoo to handle the security holes in their web servers.

II.8 US Office of Personnel Management (OPM)

Date: November 2012

Impact: Personal information (security clearances and fingerprints) of 22 million current and former federal employees were stolen.

Details: Hackers from China, the X1 Group, entered the OPM system in 2012 and remained undetected until March 2014, with time to exfiltrate personal data – including in many cases detailed security clearance information and fingerprint data. OPM implemented the big bang, a system reset that would purge the attackers from the system, on May 27th, 2014, when the attackers began to load keyoggers onto database administrators' workstations. Unfortunately, on May 7th, 2014, an attacker group dubbed X2 used credentials stolen from KeyPoint to establish a foothold in the OPM network and install malware to create a backdoor. This breach was undetected, and the big bang did not remove X2's access or backdoor. X2 hackers used an Active Directory privilege escalation technique to obtain root access and install the Sakula malware and a variant of the PlugX malware, a remote access tool that allowed the attackers to navigate around OPM's systems and compress and exfiltrate data from several OPM servers, including the administrative server used to log into other servers, namely a Department of Interior server where personnel records were stored, exfiltrating another 4.2 million personnel records.

II.9 Yahoo!

Date: August 2013

Impact: Account data (username and passwords) of 3 billion customers was stolen.

Details: The users of the Yahoo! Mail reported that their accounts had been hacked. The accounts were targeted via phishing attacks, in which users were encouraged to click on links within e-mails and, once they clicked, their accounts were hijacked.

II.10 Adobe

Date: October 2013

Impact: Personal data of 150 million accounts (logins, passwords, names, credit card numbers and expiration dates) was stolen; theft of over 40Gb of source code, including the entire source code for the ColdFusion product and parts of the source codes for Acrobat Reader and Photoshop; Adobe paid $1.1 million in legal fees and another $1 million to users to settle claims.

Details: Hackers took advantage of a security breach at the publisher, specifically related to security practices on passwords (the stolen passwords had been encrypted instead of being chopped, as recommended).

II.11 Target Stores

Date: December 2013

Impact: Personal data of 110 million customers was hijacked (names, postal addresses, telephone numbers and email addresses of 70 million customers and banking data of 40 million customers); Target paid over $18 million as a settlement for state investigations into the attack; Target estimated the cost of the breach at $162 million.

Details: Hackers located in Eastern Europe attacked Target from November 27th, 2013 to December 15th 2013, by using the RAM scraping technique, that is, the installation of malware in cash registers to read information from the credit card terminals. The hackers gained access through a third-party HVAC vender to its point-of-sale payment card readers and collected 40 million credit and debit card numbers. The attack was detected by the American secret services that detected abnormal bank movements and warned the company. The hijacked data was resold in the black market.

II.12 Yahoo!

Date: January 2014

Impact: Account data (username, passwords, birthdates, telephone numbers) of 500 million customers was stolen; theft of Yahoo's proprietary code.

Details: Only in 2016 did Yahoo! acknowledged this cyber-attack. The hackers used forged cookies to access users' accounts without a password, misidentifying themselves as the owners of the accounts.

II.13 South Korea Banking System

Date: January 2014

Impact: Personal data of 3 million customers was stolen; 100 million credit cards were stolen; 20 million bank accounts were hacked.

Details: Over the course of several years, an employee of the Korea Credit Bureau (KCB), a solvency company, stole the personal information from customers of credit card companies when he worked as a consultant, by simply copying the data to an external hard drive. The thief resold the data to credit traders and telemarketing companies.

II.14 eBay

Date: May 2014

Impact: Personal data (names, addresses, dates of birth and encrypted passwords) of 145 million users compromised.

Details: The online auction giant reported hackers got into the company network using the credentials of three corporate employees and had complete inside access for 229 days, during which time they were able to make their way to the user database.

II.15 JP Morgan Chase

Date: July 2014

Impact: Personal (names, addresses, phone numbers, email addresses, dates of birth, social security numbers) and sensitive data (account numbers, passwords, user IDs, customer profiles, financial data) of 76 million households and 7 million small businesses was stolen; the compromised data was used in 2015 in pump-and-dump schemes to boost stock prices.

Details: The largest bank in the US was the victim of a hack during the summer of 2014 that gave three hackers, Gery Shalon, Joshua Samuel Aaron and Ziv Orenstein, root privileges to more than 90 of the bank's servers, allowing them to compromise the data of 76 million households and 7 million small businesses.

II.16 Hold Security

Date: August 2014

Impact: 1.2 billion logins and passwords of 420 thousand websites; illegal access to 500 million email accounts; large spam campaign on social networks.

Details: The Russian hacker group "CyberVor" stole 1.2 billion logins and passwords on 420,000 websites around the world and accessed 500 million email accounts using programmed botnets to visit sites and perform vulnerability tests in order to exploit SQL injection vulnerabilities and access databases.

II.17 Marriott International

Date: September 2014

Impact: Personal data (names, contact information, passport numbers, travel details and Starwood Preferred Guest numbers) of 500 million customers stolen; credit card numbers and expiration dates of more than 100 million customers were stolen.

Details: In September 2018, Marriott discovered that a Chinese hacking group remained in the organisation's system since 2014, following a breach on the reservation systems supporting the Starwood hotel brands. A security tool alerted Marriott official to the unauthorised attempt to access Starwood's guest reservation database, prompting the company to investigate and discover the attack.

Home Depot

Date: September 2014

Impact: Credit/debit card data of 56 million customers was stolen; Home Depot paid $19.5 million to compensate the custome

rs and the shoppers; Home Depot estimated $161 million of pre-tax expenses for the breach.

Details: The hardware and building supply retailer announced its POS system had been infected with a custom-built malware posing as anti-virus software. In September what had been suspected for some weeks – that beginning in April or May, its POS systems had been infected with malware. The company later said an investigation concluded that a "unique, custom-built" malware had been used, which posed as anti-virus software.

II.18 Sony Pictures Entertainment

Date: November 2014

Impact: Personal data (names, addresses, emails, social insurance numbers, and salaries) of 47 thousand

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

employees was stolen; 100 Tb of data (4 unreleased feature films, business plans and contracts) was stolen; Sony cancelled the broadcast of several movies; Sony paid $8 million dollars in compensation to its employees and former employees.

Details: The hacker group Guardians of Peace attacked Sony Pictures Entertainment taking advantage of a Zero-Day vulnerability, using a Server Message Block (SMB) Worm Tool to conduct the attacks. The SMB Worm Tool was equipped with five components, including a Listening Implant, a Lightweight Backdoor, a Proxy Tool, a Destructive Hard Drive Tool and a Destructive Target Cleaning Tool. It propagated throughout the network via brute-force authentication attacks and connected every hour to home, a command and control infrastructure with servers located in Thailand, Poland, Italy, Bolivia, Singapore and the United States.

II.19 Anthem

Date: February 2015

Impact: Personal information (names, addresses, Social Security numbers, dates of birth, and employment histories) of 78.8 million current and former customers was stolen; the total cost of the data breach exceeded $100 million.

Details: The second-largest health insurer in the U.S., formerly known as WellPoint, said a cyberattack to the organisation exposed the personal data of current and former customers. The attack reportedly began when a single user at an Anthem subsidiary clicked on a link in a phishing email.

II.20 Adult Friend Finder

Date: May 2015

Impact: Personal information (pseudonyms, dates of birth, postal codes, IP addresses and sexual preferences) of 4 million customers was leaked.

Details: A hacker nicknamed ROR[RG] attacked the dating site Adult Friend Finder and made public the information of 4 million accounts on a form only accessible on Tor. The hacker sold this information in the black market for 70 bitcoins (around $16,800/€15,300).

II.21 Adult Friend Finder

Date: October 2016

Impact: Personal information (pseudonyms, dates of birth, postal codes, IP addresses and sexual preferences) of 412 million customers was stolen.

Details: Hackers took advantage of a Local File Inclusion (LFI) vulnerability to steal more than 20 years of personal data retrieved by Adult Fried Finder Network from its 400 million customers. The technique used consisted of introducing a local or remote file into an online resource and preyed on poorly stored passwords, saved as plain text or encrypted using the insecure SHA-1 cipher.

II.22 Uber

Date: November 2016

Impact: Personal data (names, emails, phone numbers) of 57 million users and 600,000 drivers exposed; Uber paid $100,000 for the hackers to destroy the data.

Details: Uber learned that two hackers were able to steal the names, email addresses and mobile phone numbers of 57 users of the Uber app and the driver license numbers of 600,000 Uber drivers. The hackers accessed Uber's GitHub account, where they found username and password credentials to Uber's AWS account.

II.23 Yahoo!

Date: March 2017

Impact: Account data (username, passwords, birthdates, telephone numbers) of 32 million customers was stolen; Yahoo's selling price was adjusted from $4.8 to $4.5 million.

Details: Hackers used the code stolen in the 2014 Yahoo! attack to create malicious cookies and log in without passwords.

II.24 UK National Health Service (NHS)

Date: May 2017

Impact: 80 NHS hospitals and 603 primary care in England and Scotland and up to 70,000 devices, including computers, MRI scanners, blood-storage refrigerators and theatre equipment, were affected, cancelling thousands of appointments and operations; other affected health systems were the Indonesian Dharmais and Harapan Kita Hospitals, the Slovakian Fakulty Hospital, the Colombian Instituto Nacional de Salud and Lakeridge Health; breach of systems at Nissan, Renault, Dacia, Hitachi, Honda and Boeing; on telecommunications, the breach hit Spain's Telefónica, Germany's O2, Portugal Telecom, the Saudi Telecom Company, Telenor Hungary, the South Africa Telkom and the Brazilian Vivo; on services, the biggest attacks occurred in Fedex, the Deutsche Bahn and the Russian Railways, and also in Brazil's Petrobrás and Petro China; numerous public regional government networks were also affected in India, China, Brazil, Sweden, Russia and Romania; breach of systems in Universities such as Greece's Aristotle University of Thessaloniki, Canada's Cambrian College, the Dalian Maritime University, the Guilin University, the Hezhou University, the Shandong University , the Sun Yat-sen University, the Indonesian Universitas Jember, the University of Milano-Bicocca and the University of Montreal; more than 230,000 computers across 150 countries affected; Total damages ranging from hundreds of millions to billions of dollars.

Details: A May 2017 worldwide cyberattack carried out by the Lazarus Group and the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting digital files and data and demanding ransom payments of $300 in the Bitcoin cryptocurrency. It propagated through EternalBlue, an exploit developed by the US National Security Agency (NSA) for older Windows systems that was released by The Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organisations that had not applied these, or were using older Windows systems that were past their end-of-life. WannaCry also took advantage of installing backdoors onto infected systems. The attack was stopped within a few days due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. Meanwhile, hospitals were forced to cancel operations and resort to the use of pen and paper to record patient data. Hundreds of computer users reported being sent an email from someone (or multiple people), claiming to be the developers of WannaCry. The email threatened to destroy the victims' data unless they sent 0.1 BTC to the Bitcoin address of the hackers.

II.25 Businesses in Russia and Ukraine

Date: June 2017

Impact: Damages of more than $10 billion; Shutdown of the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant; breaches in the Ukrainian government, banks and metro systems and more than 80 companies, including the National Bank of Ukraine; breach in the British advertising company WPP and the consumer goods company Reckitt Benckiser; breach in the Danish Maersk Line, the world's largest container ship and supply vessel operator (estimated $300m in lost revenues); breach in the American pharmaceutical company Merck & Co., the food company Mondelez International, the Heritage Valley Health System operator, the Princeton Community Hospital and the multinational law firm DLA Piper; breach in the Russian oil company Rosneft, the aircraft manufacturer Antonov and two postal services; breach in the French construction company Saint-Gobain; breach in the Netherlands' TNT shipping company; breach in the German personal care company Beiersdorf, and the logistics company DHL; breach in the Australian company Cadbury's Chocolate Factory; breach in India's JNPT, the largest container port in the country.

Details: On June 27th, 2017, a major global cyberattack began (Ukrainian companies were among the first to state they were being attacked), using a variant of the Petya malware (NotPetya). 2,000 attacks were reported, most in the Ukraine, Russia and Poland, but also in France, Germany, Italy, the United Kingdom and the United States. The NotPetya's payload infects the computer's master boot record (MBR), overwrites the Windows bootloader, and triggers a restart. Upon startup, the payload encrypts the Master File Table of the NTFS file system, and then displays the ransom message demanding a payment made in Bitcoin. The radiation monitoring system at Chernobyl was taken offline, forcing scientists to monitor radiation manually.

II.26 Equifax

Date: July 2017

Impact: Personal data (names, addresses, birth dates, social insurance numbers, driver license numbers) of 143 million American, Canadian and British customers was stolen; 209 thousand credit card numbers were exposed.

Details: The American credit company Equifax suffered a cyberattack that, over the course of three months, stole the personal data of 143 million customers and 200 thousand credit card numbers. The hackers exploited a known vulnerability of the Apache Struts to conduct the attack. The patch solving the vulnerability was made available by Apache long before the attack, but Equifax did not update its systems.

II.27 Alteryx

Date: December 2017

Impact: Exposition of personal information (248 different data fields covering a wide variety of specific personal information including address, age, gender, ethnicity, contact information, education, occupation, marital status, as well as mortgage ownership, financial information, personal interests and the number of children and pets in the household) of 123 million US households.

Details: The marketing analytics company Alteryx left online an unsecured database (a publicly accessible misconfigured Amazon Web Services S3 cloud storage cache) that publicly exposed the data of 123 million households.

II.28 Coincheck

Date: January 2018

Impact: $533 million worth of the cryptocurrency of 260 thousand customers was stolen; Coincheck froze its trading services; Coincheck reimbursed the customers who lost the currency.

Details: The Japan-based cryptocurrency exchange revealed it lost $533 million worth of the cryptocurrency NEM in a hack, in what amounts to possibly the largest cryptocurrency heist of all time. The 500 million NEM tokens were taken from Coincheck's digital wallets and the company first restricted deposits, trading and withdrawal of XEM, the token running on the NEM blockchain and later announced the trading of all cryptocurrencies. The attack seems to have been facilitated by the company's negligent storage practices.

II.29 Under Armour (MyFitnessPal)

Date: February 2018

Impact: Personal information (usernames, email addresses and login information) of 150 million user accounts was stolen; 4% drop of shares' price in after-hours trading.

Details: In February 2018, the sports apparel brand Under Armour disclosed that a hacker gained access of user accounts of its food and nutrition website, MyFitnessPal. The stolen data was protected with SHA-1, a 160-bit hashing function that has had known flaws for a decade and was further discredited by 2017 research findings.

II.30 Baltimore's 911 Dispatch

Date: March 2018

Impact: 911 system rendered non-operational for 3 days; 911 system used manual operations to handle 911 calls.

Details: Baltimore's 911 dispatch system was taken down for 17 hours after a ransomware attack, forcing the city to revert to manual dispatching of emergency services. A limited breach affected Baltimore's computer-assisted dispatch system, which is used to support and direct 911 and other emergency calls. Details of incoming callers seeking emergency support were unable to be relayed to dispatchers electronically and instead had to be manually managed by call centre support staff. The hackers demanded more than $2,000 in bitcoin to turn it back on. Refusing payment, the call centre support staff tracked emergency calls with pencil and paper for three days, as the system was rebuilt.

II.31 City of Atlanta

Date: March 2018

Impact: Atlanta's online municipal services were disrupted; years of data (police and court system databases and WiFi network at the Atlanta International Airport) destroyed; the city of Atlanta spent $2.6 million to recover.

Details: Online municipal services for the city of Atlanta were disrupted after a ransomware attack struck the city's networks, demanding $55,000 worth of bitcoin in payment. The city spent $2.6 million recovering from the attack that used the SamSam malware. While the city was considering payment, the attackers (from Iran) took the payment portal offline and the city had to recover for itself. The city believes that full recovery requires a $9.5 million investment.

II.32 Panera Bread

Date: April 2018

Impact: Personal data (birthdays, names, emails, physical addresses, social account information, food preferences, dietary restrictions and the last four digits of credit card numbers) of 37 million customers was stolen.

Details: Information has been presented that the online bakery company was aware that the customer data leak was ongoing since September 2017. The identified security vulnerability in Panera Bread's network refers to an unauthenticated API endpoint that allows anyone to access the information about those who signed up for an account to order food from Panera Bread.

II.33 Ticketmaster

Date: June 2018

Impact: Personal data of 40 thousand customers was stolen.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Details: Organised by the credit-card skimming criminals Magecart, the attack involved a third-party supplier, Inbenta Technologies, which operates a chatbot on the Ticketmaster site. Without Inbenta's knowledge, Ticketmaster used the chatbot's Javascript code on its payment page, where it was discovered by hackers and modified to extract payment information. Ticketmaster's customers reported the theft of their money and others claimed that their credit card details were being sold in the dark web.

II.34 MyHeritage

Date: June 2018

Impact: Personal data (email addresses and encrypted passwords) of 92 million users was stolen.

Details: Hackers breached the servers of the DNA analysis company MyHeritage and stole the personal data of over 92 million sensitive records. Still, the affected website uses a hashing algorithm with a unique salt to protect users' passwords, making them more resilient to cracking. MyHeritage also reported that the breach did not compromise any of its other systems, namely the servers storing family trees and DNA data and that the company does not store credit card information.

II.35 TicketFly

Date: June 2018

Impact: Personal data (names, addresses, phone numbers and email addresses) of 27 million customers was stolen.

Details: The hacker group IShAkDz took responsibility for the cyberattack and demanded 1 Bitcoin ($7500) to divulge the TicketFly vulnerability. The ransom was not paid, and the hacker posted the user data online.

II.36 Exactis

Date: June 2018

Impact: Personal data (phone numbers, home and email addresses, interests, the number, age, and gender of their children, ethnicity, hobbies, smoking habits, religious and political preferences, browsing habits and purchase data) of 340 million records was stolen;

Details: The marketing firm reported that the personal and behavioural data pertaining to consumers and businesses had been stolen from the company's database, sitting on a publicly accessible server.

II.37 Macy's and Bloomingdale's

Date: July 2018

Impact: Undisclosed number of personal data (names, phone numbers, addresses, emails, birthdays and credit card information) records were breached.

Details: The data breach occurred between April 26th and June 12th 2018, enabling an unauthorised third-party to retrieve sensitive information from the company's servers. The hackers obtained valid usernames and passwords through websites not related to macys.com or bloomingdales.com and used those to gain access to customers' accounts, which were then blocked by the retailer company.

II.38 HBO

Date: July 2018

Impact: Theft of 1.5 Tb confidential data (TV show episodes, series scripts, emails and telephone numbers).

Details: A network of Iranian hackers breached the HBO network servers. The hackers demanded $6 million in Bitcoin from HBO executives in exchange for stopping the leaks. The hackers also claim they spend nearly $500,000 USD a year purchasing so called zero-day exploits that let them break into networks through holes not yet known to Microsoft and other software companies.

II.39 British Airways

Date: September 2018

Impact: Personal data (names, traveling plans, bank card numbers, expiry dates and cvv codes) on 380 thousand booking transactions were stolen; breach costs rising to $12 million; hit felt on IAG's shares in the market; IAG/BA faced a penalty from GDPR of £800 million (4% of its turnover).

Details: Organised by the hacker group Magecart, the attack occurred from August 21st to September 5th using a 22-line script (modification of JavaScript code) designed to steal financial information by 'skimming' the payment page before it was submitted, without disrupting the payment flow. The credit card details were sold in the dark web for $10 a card.

II.40 Facebook

Date: September 2018

Impact: Personal data (names, relationship status, religion, birthdate, employers, search activity, and check-in locations) of 50 billion users compromised.

Details: One of the most severe breaches affecting Facebook, this attack was perpetrated by hackers who exploited a weakness in Facebook's code to access the 'View As' privacy tool that allows users to see how their profile looks to other people.

II.41 Quora

Date: December 2018

Impact: Personal data (names, email addresses, encrypted passwords, IP addresses, user IDs, personalisation data, questions, answers, comments, posts and data imported from linked networks like Facebook and Twitter) of 100 million users was stolen.

Details: The popular question-and-answer website Quora announced that personal data of its users had been compromised by a malicious third party who gained unauthorised access to its systems.

II.42 German Public Figures

Date: January 2019

Impact: Personal data (names, contacts, private communications and financial data) of 882 German politicians, celebrities and public figures were publicly disclosed; Internal party documents were publicly disclosed.

Details: Hackers released online the personal data of German public figures, celebrities and politicians (from all political parties with the exception of the far-right party Alternative for Germany AfD) via a Twitter account, then shut-down. Preliminary analysis showed the data had been obtained through a wrongful use of login information for cloud services, email accounts or social networks. The motive for the leaks remains unclear.

II.43 Airbus

Date: February 2019

Impact: Undisclosed number of employee records (personal and IT identification) was stolen.

Details: The aerospace company Airbus revealed that Chinese hackers stole the personal data and IT credentials of specific European employees in the organisation. Airbus said it detected a cyber incident on its Commercial Aircraft business information systems, which resulted in unauthorised access to data. The purpose of the attack is thought to be the stealing of trade secrets.

Annex III: **Most Significant Cyber Attacks in Healthcare (2011-2019)**

III.1 TRICARE

Date: September 2011

Impact: Personal data (Social Security numbers, phone numbers, home addresses, and other personal data) of 4.9 million patients was stolen.

Details: Science Applications International Corporation (SAIC) announced a data breach that affected approximately 4.9 million military clinic and hospital patients who were enrolled in TRICARE, the federal government's military healthcare provider (SAIC oversaw TRICARE's data security). The data had been stolen from an SAIC employee's car, and the victims included active and retired military personnel as well as their families.

III.2 Advocate Health Care

Date: August 2013

Impact: Personal data (names, addresses, dates of birth, Social Security numbers and certain clinical information, such as diagnoses, medical records numbers, medical service codes and health insurance information) of 4.03 million patients was stolen; Advocate Health Care paid $5.55 million on penalty fines.

Details: Advocate Health Care divulged that several data breaches, including at least two involving the theft of 4 computers, had revealed personal information and unencrypted medical records of 4.03 million patients.

III.3 Boston Children's Hospital

Date: March 2014

Impact: The Hospital's system lost Internet connectivity; Medical personnel could not use online accounts; the Boston Children's Hospital paid $40 thousand on penalty fines; the Boston Children's Hospital spent more than $300,000 mitigating the damage from the attack.

Details: The hacktivist group Anonymous targeted the Boston's Children's Hospital with a DDoS attack after the hospital recommended one of their patients, a 14-year-old girl, be admitted as a ward of the state and that custody be withdrawn from her parents. The networks experienced outages for almost a week, and some medical patients and medical personnel could not use their online accounts to check appointments, test results, and other case information. The DDoS traffic in the Hospital's website and network hit 27 Gbps. The Hospital counterattacked by taking down all websites, shutting down email and directing the staff to communicate using a secure text messaging application developed by the Hospital.

III.4 Community Health Systems

Date: June 2014

Impact: Personal data (Social Security numbers, dates of birth, phone numbers, and physical addresses) of 4.5 million patients was stolen; Community Health Systems incurred in losses up to $150 million.

Details: Community Health Systems, which operates 206 hospitals throughout the U.S., announced a major healthcare breach that affected 4.5 million patients. The attackers (Chinese hacker group APT 18) exploited the software vulnerability OpenSSL, CVE-2014-0160, better known as Heartbleed, to access the patient data. It is believed that hackers were searching for intellectual property on medical devices and other equipment, but

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

instead stole data on patients.

III.5 Premera Blue Cross

Date: January 2015

Impact: Personal data (bank account numbers, Social Security numbers, dates of birth, and claims information) of 11 million customers was stolen; Premera Blue Cross offered two years of free credit monitoring and identity theft protection to affected customers.

Details: Hackers breached the health insurance company's systems and gained access to computers holding the personal and medical data of over 11 million Americans. The Office of Personnel Management (OPM) found numerous security flaws during a routine audit of Premera's systems, which it reported to Premera a few weeks before the breach. A month later, a Premera employee fell victim to a phishing email, which led to hackers planting malware on the organisation's network.

III.6 Anthem Blue Cross

Date: February 2015

Impact: Personal data (names, Social Security numbers, home and email addresses, dates of birth, insurance membership numbers, medical IDs, employment information, income data) of 78.8 million patients was stolen.

Details: The company noticed suspicious database queries being made and soon confirmed that unauthorised data queries were issued to the company's servers. This hacking attack resorted to phishing techniques, through which hackers were able to acquire network credentials of multiple individuals within the company who had high-level access to the IT system. Then, hackers managed to access the personal information of patients because the files were not encrypted.

III.7 Medical Informatics Engineering

Date: May 2015

Impact: Personal data (names, Social Security numbers, insurance policy information, phone numbers, mailing addresses, dates of birth, diagnoses, lab results, reports and medical conditions) of 3.9 million patients was stolen.

Details: Medical Informatics Engineering, a company that creates electronic medical records software, announced a data breach that affected at least 11 healthcare providers, 44 radiology centres and 3.9 million patients. The company discovered suspicious activity in one of its servers and was able to counter this unauthorised access almost a month later.

III.8 University of California Los Angeles Health System

Date: July 2015

Impact: Personal data (patient names, dates of birth, home addresses, Social Security numbers, Medicare numbers, health plan/health insurance identification numbers and health information) of 4.5 million patients was exposed; the hospital group offered one year of identity theft recovery services to affected patients and staff.

Details: Hackers accessed the University's databases and copied a database containing the Protected Health Information (PHI) of patients and hospital staff members. It is not clear how hackers gained access to the systems and managed to bypass its defences, but advanced methods of exfiltration were employed to avoid detection.

III.9 Excellus BlueCross BlueShield

Date: September 2015

Impact: Personal data (Social Security numbers and financial information) of 10 million customers was stolen; Excellus incurred in losses of $17 million as a result of the attack.

Details: Unknown hackers were able to rummage through the company's data banks for nearly 20 months before being detected. The company states the data was encrypted and therefore could not be used but subsequent litigation claims of the plaintiffs indicates that at least part of the stolen data was available in dark-web marketplaces.

III.10 Banner Health

Date: June 2016

Impact: Personal data (names, birthdates, addresses, physicians' names, dates of service, claim information, and some health insurance information and Social Security numbers) of 3.7 million patients was exposed; Personal data (names, addresses, birthdates and Social Security numbers) of physician and healthcare providers was exposed.

Details: Hackers accessed Banner's payment processing system at its food and beverage outlets, which they used as a gateway into the network and eventually into the servers containing patient data from 27 different locations.

III.11 NewKirk Products

Date: August 2016

Impact: Personal data (member's name, mailing address, type of plan, member and group ID number, names of dependents enrolled in the plan, primary care provider, date of birth, premium invoice information and Medicaid ID number) of 3.47 million patients was stolen.

Details: The healthcare ID card-issuer NewKirk Products announced a data breach that victimised 3.47 million patients, most of the insurer Blue Cross Blue Shield, which is one of the largest health insurance providers by enrolment in the United States. Unknown hackers acquired unauthorised access to a company's server and stole the information. This access the result of the exploitation of a weakness in the administrative portal of the 3rd party software on the single isolated server. After the attack, some members have reported being targeted by scam phone calls.

III.12 LifeBridge Health

Date: September 2016

Impact: Personal data (demographic information, dates of birth, medical history, clinical and treatment information, insurance data and Social Security numbers) of 500 thousand patients was exposed.

Details: LifeBridge Health was hit by a malware attack that potentially exposed the private information of its patients for more than a year. The breach discovered was a malware infection on the servers that hosted the EHR and the patient registration and billing systems. Several affected patients became victims of credit card fraud.

III.13 Mirai malware attack

Date: September 2016

Impact: At its peak, Mirai temporarily crippled several high-profile services such as OVH, Dyn, and Krebs on Security via massive distributed Denial of service attacks (DDoS). OVH reported that these attacks exceeded 1Tbps—at the time, the largest on public record [47].

Details: Mirai malware explores vulnerabilities present in networked devices (e.g., routers and IP cameras) to turn them into remotely controlled "bots" and thus build botnets capable to launch large-scale attacks. It is believed that Mirai enslaved over 600,000 vulnerable IoT devices [46].

III.14 Mirai variants

Date: October-November 2016

Impact: On October 31, 2016 and over the following months, Lonestar Cell, one of the largest Liberian telecom operators started to be targeted by a Mirai variant. Its author confessed during his trial that he was paid $USD 10k to takedown Lonestar by a competitor [47]. On November 26, 2016, one of the largest German Internet provider Deutsche Telekom suffered a massive outage after 900,000 of its routers were compromised by another Mirai variant [47].

Details: The Mirai botnet’s source code was released in October 2016, opening the opportunity for many cybercriminals to create Mirai variations and instances that can be sold or operated as a service on underground forums and black markets [46]

III.15 Florida Medicaid

Date: January 2018

Impact: Personal data (names, addresses, birth dates, Medicaid ID numbers, social insurance numbers, diagnoses and medical conditions) of 30 thousand patients was exposed.

Details: An employee of Florida’s healthcare agency fell victim of a phishing email, which allowed hackers to access Medicaid patient data. After the breach, the agency required employees to change login credentials to prevent further access and took steps to remediate the breach. Further, the agency implemented new security training. It's not clear who was responsible for the attack or what their motivations might be.

III.16 Coplin Health Systems

Date: January 2018

Impact: Personal data (patient names, Social Security numbers, financial information, addresses, dates of birth and medical data) of 43 thousand patients was exposed.

Details: A laptop of a Coplin Health Systems employee was stolen from a car and enabled the data breach of the patient information, since it was not encrypted on the hard drive. Coplin Health notes that the laptop had various security protections in place to ensure the privacy of patients in the event of the laptop being stolen. While the laptop could potentially be used to gain access to patient data, a password would have been required and it is not suspected that the thief had the sophisticated knowledge and resources necessary to bypass the laptop’s security mechanisms. No attempts have been made to access Coplin’s systems using the laptop since the device was stolen.

III.17 Oklahoma State University Centre for Health Sciences

Date: January 2018

Impact: Personal data (patient names, Medicaid numbers, provider names, dates of service and treatment information) of 280 thousand patients was exposed.

Details: A hacker gained access to the Oklahoma State Health Sciences network and accessed folders containing Medicaid billing data. The affected Medicaid folders were removed from the network and third-party access was terminated the next day.

III.18 University of Virginia Health System

Date: February 2018

Impact: Personal data (patient names, diagnoses, treatments, dates of birth and addresses) of 1,882 patients was exposed.

Details: A hacker named Phillip Durachinsky developed a computer malware known as Fruitfly, was able to download it on a physician's computer and used it to breach the network of the University of Virginia Health System. The Fruitfly malware infected physician devices that allowed the hacker to access medical records of 1,882 patients for 19 months. The malware also enabled the hacker to simultaneously view opened data on the computer at the same time as the physician. When the attacker was caught, the FBI learned that he did not have an interest in using or further disclosing any patient information.

III.19 St. Peter's Surgery and Endoscopy

Date: March 2018

Impact: Personal data (patient names, addresses, dates of birth, service dates, diagnoses, procedures and insurance information) of 135 thousand patients was exposed.

Details: A malware attack on St. Peter's Surgery and Endoscopy Centre in New York gave hackers access to 134,512 patient records, which makes it the second-largest breach this year. Quickly detecting the malware limited the time hackers had access to the server. Those patients with breached Medicare information have been offered one year of free credit monitoring. Officials did not explain how hackers were able to install malware onto the impacted server.

III.20 ATI Physical Therapy

Date: March 2018

Impact: Personal data (patient names, addresses, dates of birth, Social Security numbers, driver's license or state identification numbers, financial account numbers, Medicare or Medicaid identification numbers and medical records) of 35 thousand patients was exposed; ATI offered a year of free credit monitoring and a $1 million identity theft insurance policy to affected patients.

Details: Several employee emails were breached by a hacker, exposing a range of patient data. ATI discovered the direct deposit information of some employees was changed in its payroll system. The investigation revealed the email accounts of certain employees had been compromised and were accessed by unauthorized individuals between January 9 and January 12, 2018. An analysis of the emails in the accounts revealed they contained the protected health information of tens of thousands of patients. No evidence of misuse of information has been uncovered.

III.21 Associates in Psychiatry and Psychology

Date: March 2018

Impact: Personal data (demographic information, insurance claim processing data, medical details) of 500 thousand patients was exposed.

Details: Hackers breached APP's servers between the evening of March 30 and the morning of March 31. All

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

the data files on its main servers were locked down with a RSA2048 encryption protocol, and the hackers disabled the system's restore function on all impacted computers. The virus reformatted the network storage device where local backups were contained. Hackers left a ransom note and used "Triple-M" crypto-ransomware, with the sole objective of getting victims to pay a ransom.

III.22 Middletown Medical

Date: April 2018

Impact: Personal data (patient names, client identification numbers, birthdates, radiology services received by the patient and the date services were provided, radiology images and radiology reports) of 63.5 thousand patients was exposed.

Details: Middletown Medical left a misconfigured radiology interface open to the public, exposing patient data in the process. The following day the interface was secured to ensure unauthorized individuals were prevented from accessing patient information. It is unclear for how long patient data was accessible. No reports of misuse of PHI have been received.

III.23 Centres for Orthopaedic Specialists

Date: April 2018

Impact: Personal data (demographic data, medical records, insurance information and Social Security numbers) of 85 thousand patients was stolen; COS offered free identity protection services for two years along with protection from a $1 million insurance policy.

Details: Hackers hit the IT vendor of three Centres for Orthopaedic Specialists locations in February with a ransomware attack that locked down their systems and encrypted patient data for the purposes of extortion.

III.24 MedEvolve

Date: May 2018

Impact: Personal data (patient names, client identification numbers, birthdates, medical records and Social Security numbers) of 205 thousand patients was exposed; MedEvolve is offering affected patients 24 months of complimentary credit monitoring services, which includes up to $1,000,000 of identity theft insurance.

Details: MedEvolve, a practice management software vendor, left its FTP server open to the public without the need for a login and exposed the data of 205,000 patients from two separate healthcare providers. The FTP server was configured to allow anonymous login, did not require login credentials and failed to display a banner that would direct users to keep out of patient files. Upon discovery of the breach, the FTP server was secured to prevent any further unauthorised access. While MedEvolve is unaware if all the content left exposed has been viewed, it knows for certain the PII of 15 people was definitely compromised. This took place when a screenshot containing the data of these 15 individuals was posted online in a news article covering the breach. The information in the screenshot included first names, city, state and zip code, but not patients' last names or street addresses.

III.25 SingHealth

Date: July 2018

Impact: Personal data (demographic information, patient identification numbers and outpatient dispensed medication) of 1.5 million patients was exposed; SingHealth and IHiS were fined for $1 million for the data breach.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Details: Hackers breached the Singapore government's health database (SingHealth) with a deliberate, targeted and well-planned cyberattack, accessing the data of about 1.5 million patients, including Prime Minister Lee Hsien Loong, for almost a full week. The cybercriminals breached a front-end workstation to gain privileged account credentials to obtain privileged access into the database. Hackers targeted clinical visits between May 1, 2015, and July 4, 2018. The Personal Data Protection Commission (PDPC) presented a fine of $250,000 to SingHealth and a fine of $750,000 to Integrated Health Information Systems (IHiS), the technology vendor for Singapore's healthcare sector, for lapses in securing patient data.

III.26 UnityPoint Health

Date: July 2018

Impact: Personal data (names, addresses, medical data, treatment information, lab results, payment card and/or insurance information, including Social Security numbers) of 1.4 million patients was exposed.

Details: The health system's business email system was hit by a series of targeted phishing emails that looked like they were sent from an executive within UnityPoint. An employee fell victim to the emails, which gave hackers access to internal email accounts from March 14 until April 3. The hackers tried to use the email system to divert vendor or payroll payments (business email compromise) to accounts they controlled.

III.27 Augusta University Health

Date: August 2018

Impact: Personal data (demographic information, medical record numbers, medical data, treatment information, surgical details, diagnoses, medications, dates of services and/or insurance information) of 417 thousand patients, faculty and students was exposed.

Details: Targeted phishing attacks on August University Health may have breached the personal records of 417,000 patients after two cyberattacks. Hackers targeted the university health system with phishing emails, soliciting usernames and passwords that gave them access to twenty-four internal email accounts. Upon discovery of the attack, the email accounts were disabled to prevent data access and misuse of the accounts and they were monitored for any sign of suspicious activity. No reports were received by Augusta University Health to suggest that the patient data records had been misused.

III.28 Fetal Diagnostic Institute of the Pacific

Date: September 2018

Impact: Personal data (names, dates of birth, addresses, medical data and other types of information) of 41 thousand patients was exposed.

Details: The Fetal Diagnostic Institute of the Pacific was hit by a ransomware attack that potentially breached the data of 40,800 patients. File-encrypting software was installed on an FDIP server and encrypted a wide range of file types, including patient medical records. The company was able to successfully remove the virus, clean the system and confirm no malware remained. The investigation did not uncover any evidence to suggest that patients' protected health information was accessed, viewed, or stolen by the individuals behind the attack.

III.29 MedCall Advisors

Date: October 2018

Impact: Personal data (names, email and postal addresses, phone numbers, dates of birth, Social Security

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

numbers, patient evaluations and conversations with doctors, medications, allergies and other detailed personal health data) of 10 thousand patients was exposed.

Details: MedCall, a worker compensation and healthcare solutions vendor, left a storage bucket containing 10,000 files exposed to the internet, available for download or deletion or editing. MedCall's 7Gb database was listed on the searchable tool grayhatwarfare.com, which publicly lists current open Amazon Web Service S3 buckets.

III.30 Centres for Medicare and Medicaid Services

Date: October 2018

Impact: Personal data (names, dates of birth, addresses, portions of Social Security numbers, expected income, family relationships, health insurance status and credit card data) from 94 thousand users were stolen; business data of transportation businesses, local government entities, school districts, and individual locations of large franchise chains, like Piggly Wiggly, KFC, and Hampton Inn, was exposed; the companies provided credit protection to the affected users.

Details: Hackers gained access to HealthCare.gov, the government's Affordable Care Act enrolment portal and accessed the personal data of Medicare and Medicaid Centres' users. The agent and broker accounts that were associated with the anomalous activity were deactivated, and – out of an abundance of caution – the Direct Enrolment pathway for agents and brokers was disabled.

III.31 Cabrini Hospital

Date: February 2019

Impact: Medical data of 15 thousand patients was stolen.

Details: A cyber-crime syndicate has hacked and scrambled the medical files of patients from a specialist cardiology unit at Cabrini Hospital and demanded a ransom. The malware used to penetrate the unit's security network is believed to be from North Korea or Russia, while the origin of the criminals behind the attack has not been revealed. The online gang responsible for the data breach demanded a ransom be paid in cryptocurrency before a password would be provided to break the encryption. The hospital has been unable to access patient files for more than three weeks, after the malware attack crippled its server and corrupted data.

III.32 Medicall

Date: February 2019

Impact: Personal data (telephone numbers) of 57 thousand users was exposed; 2.7 million of medical calls were exposed.

Details: Calls recorded by a Swedish National Health Service hotline were stored on an unencrypted system that was publicly accessible to anyone with an internet connection. The phone calls (wav on MP3 files) were discovered to have been left open by an unprotected NAS (network attached storage) system and were accessible without a password or any authentication. 57,000 Swedish phone numbers appear in a database associated with the audio files.