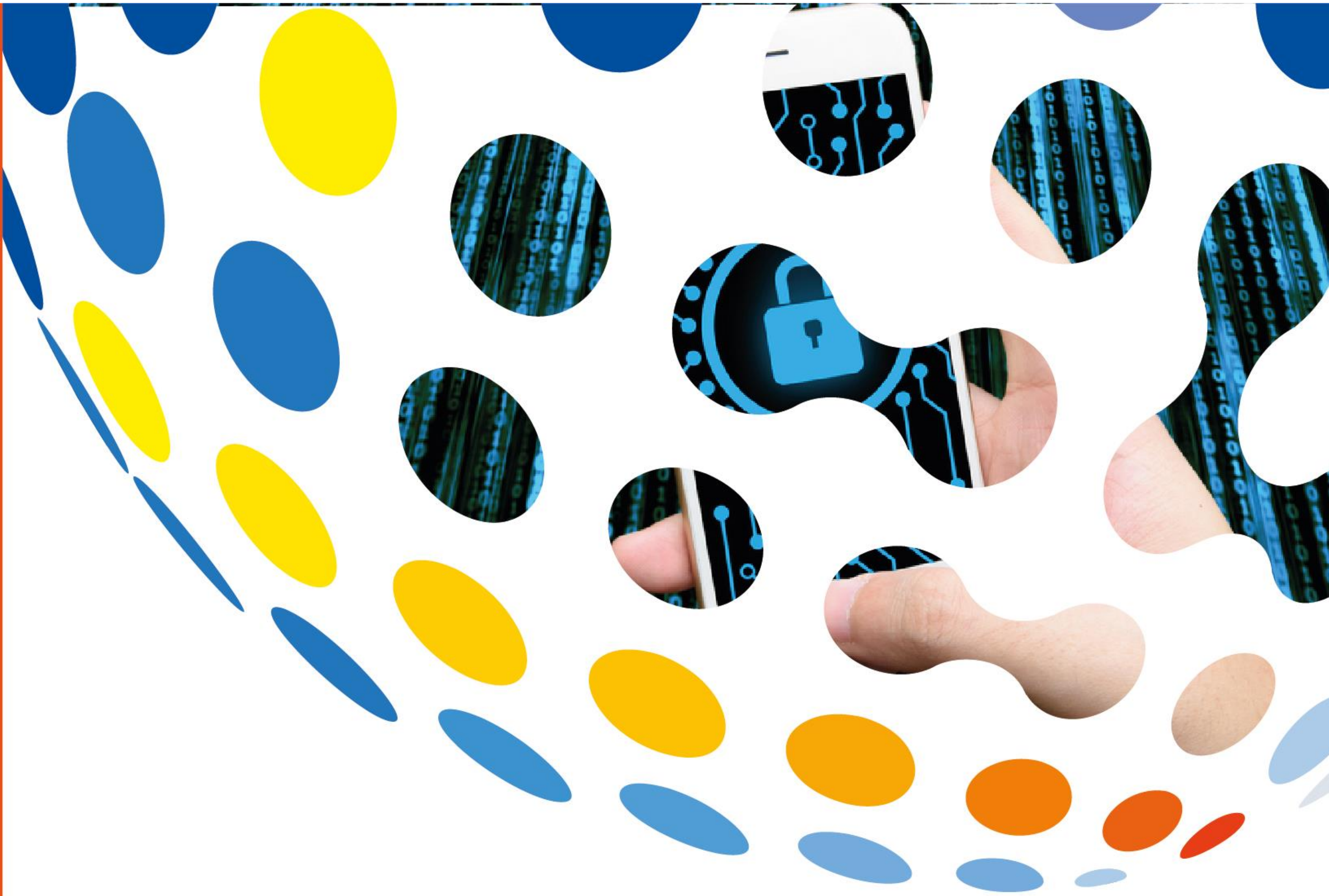


NIS Cooperation Group publication

Threats and risk management in the health sector

Under the NIS Directive

June 2023

NIS COOPERATION GROUP

Contents

1. Executive Summary

The “Threats and risk management in the health sector – Under the NIS Directive” shines a light on the different cybersecurity threats targeting the health sector of the European Union in times of ever-growing interconnections between traditional health care services and internet-connected networks and information systems.

Starting with the analysis of the cyber threat landscape and the most relevant threat taxonomies and cyber incident data, this report highlights the main current and emerging cyber threats which the European heath sector is likely to be confronted with. In this sense, the report also presents a set of business continuity and mitigation recommendations to limit the likelihood and impacts of a cyber related incident.

Finally, the present document provides an analysis of the results of a questionnaire that was disseminated by Member States to Operators of Essential Services and that focused *inter alia* on the cybersecurity and risk management culture, cybersecurity awareness, cybersecurity measures currently in place and the cyber threat perceptions of institutions of the European healthcare sector.

In conclusion, this “Threats and risk management in the health sector – Under the NIS Directive” aims to enhance the awareness of the European health sector with regards to the cyber threats it faces and to enhance the general cybersecurity posture of institutions being part of the European health sector.

2. Context

The **most valuable asset** to any healthcare organisation is the **patient**, who expects from healthcare organisations and professionals help to get better, saving or sustaining his life. But health organisations are also comprised of digital and technological systems and tools that enable them to increase patients' safety and care. Thus, **electronic health data** is also the **lifeblood of a healthcare organisation**, and this data must be kept confidential, it's integrity must be preserved, and it must be made available on demand wherever and whenever it is needed.

Healthcare is increasingly the target of malicious cyberattacks, which result not only in data breaches but also increased healthcare delivery costs, and they can ultimately affect provision of care. Health information systems, networks and medical devices are particularly targeted and vulnerable because they host and process information such as patients' protected health information, personal identifiable information, and intellectual property related to medical research and innovation which represents high monetary and intelligence value to cyber thieves and nation-state actors. On the other hand, more and more cybersecurity incidents arise because of the lack of maintenance and technological updates of these systems, even if there is no targeted attack. Often, healthcare providers rely on legacy systems, outdated computer systems that are still in use and provide less protection and increased susceptibility for an attack.

Cybersecurity incidents on electronic health records and other health information systems stand out when we talk about health cyberattacks and incidents, but the **attack surface of a hospital is much broader**, considering the supply chain, cloud-based infrastructures, the building automation systems (HVACs, for example), the internet of medical things, etc. It is crucial that the health ecosystem actors (people, manufacturers and facilities) work together to manage the risks and to protect patient safety.

The connection between cybersecurity and patient safety may be naively seen as somewhat abstract as the impacts of cyber-attacks do not seem to immediately present harm or mortality to patients, however there are plenty of examples that disprove this[1]. Losing access to medical records and lifesaving medical devices, such as a ransomware attack holding them hostage, disrupts the ability to effectively care for the patients. Hackers' access to private patient data not only opens the door for them to steal the information, but also to either intentionally or unintentionally alter the data, which could lead to serious effects on patient health and outcomes.

It is crucial that healthcare organisations understand that **cybersecurity is directly related to patient safety** and know how to keep health data ecosystems secure. Aligning these two domains and initiatives not only will help health organisations to protect patient safety and privacy but will also ensure the continuity of effective high-quality delivery of care by mitigating disruptions that can have a negative impact on clinical outcomes and business continuity.

Another important consideration is that **cyber risks need to be incorporated into the overall enterprise risk management governance** and receive the attention and support of executive leadership, including the C-suite and Board. The Board of health organizations must lead and support all the necessary efforts to ensure the existence of resilient and secure services with the IT department performing an important role since, as

[1] Please see some examples on the Chapter 4.3

we have seen, a cybersecurity incident can have a direct impact on the provision of healthcare or the organisation's business.

Hospital leaders generally do recognize the importance of safety culture; thus, one needs to extend this awareness to cybersecurity.

2.1. Scope, target audience and objectives of the document

The “Threats and risk management in the health sector – Under the NIS Directive” is a deliverable from the Work Stream (WS) on Health constituted under the NIS Cooperation Group, with the primary objective to facilitate the implementation of the NIS Directive in the health sector and to provide support to Member States, NIS authorities, healthcare providers identified as Operators of Essential Services (OES) and other relevant healthcare institutions on addressing the particularities of the sector when tackling cybersecurity issues.

A task group made up of the Luxembourg Regulatory Institute (ILR), the Portuguese National Cybersecurity Centre, the Danish Health Data Authority and the European Cybersecurity Agency (ENISA) was formed under the WS on Health to take stock of threats targeting the healthcare sector in order to assist Member States in their efforts to identify, mitigate, and manage cyber risks in the health sector.

This document intends to summarize some of the most prevalent threats in the health sector, presenting mitigation and business continuity measures helping hospitals and healthcare organisation leads’ facing the challenges of managing cybersecurity in their own organisations. It also includes information on cybersecurity taxonomies as the classification used to structure the threat ecosystem.

Finally, the document contains an overview of the cybersecurity measures related to risk management that are currently in place within the healthcare sector, as well as information about incidents and threats as the result of a questionnaire that was disseminated to the Member States.

The **target audience** of the deliverable are health OES, institutions that carry out their activities in the health sector, National Health Sector Authorities and Health NIS Authorities.

2.2. Methodology

The information presented in this report is based on public information about health cybersecurity incidents and threats, national work and knowledge from the authors, and also from the results of an online survey completed by 81 operators providing services in 19 Member States of the European Union.

3. Cybersecurity Threats

Threat, Vulnerability and **Risk** are terms frequently used together which represent components of cybersecurity.

For the threat to translate into risk, there must be a ***vulnerability*** to the ***threat***, which represents a weakness, flaw or some other shortcoming in a system (infrastructure, database or software), for example, the way that something has been implemented or deployed, such as an unpatched software vulnerability (a vulnerability exposes the organisation to threats); but it can also exist in a process or in a set of controls.

A threat is a malicious or negative event that takes advantage of a vulnerability which could affect the confidentiality, integrity or availability of systems, data and/or people.

The organisations need to assess the ***impact*** to the organisation, data and patient safety in the event that a cyber threat exploits a vulnerability.

Next, the organisation must determine the ***probability*** of the attack and the ***velocity*** of the threat exposure. Is the malware that is exploiting the vulnerability currently in use and frequently targeting victims (as the Ryuk malware does), or is the threat distant, but certain, such as the set time leading up to the expiration of support for Windows 7? The Windows 7 expiration has increased risk of medical devices being exploited; therefore, it is necessary to update this software or create new layers of protection in order to mitigate related vulnerabilities.

(Threat + Vulnerability + Impact) x (Probability + Velocity) = Risk

Finally, the ***risk*** is the potential for loss and damage when the threat does occur, represented by the probability of a negative (harmful) event occurring as well as the potential of scale of that harm.

3.1. ENISA Threat Landscape

The **ENISA Threat Landscape (ETL)** report is the annual report of the European Union Agency for Cybersecurity, on the state of the cybersecurity threat landscape. The report identifies threats, major trends observed with respect to these threats, threat actors and attack techniques, impact and motivation analysis, as well as relevant mitigation measures.

Over the years, the ETL has been used as a key instrument in understanding the current status of cybersecurity across the EU and to provide insight in terms of trends and patterns, leading to relevant decisions to protect services, prioritisation of actions and recommendations.

The ENISA Threat Landscape 2022[2], published in October 2022, identifies and focuses on eight prime threat groups based on the analysis of a series of cyber threats that emerged and materialised in 2021 and 2022. What is outlined in this chapter summarizes the threat information but does not dispense from reading the original document.

[2] ENISA Threat Landscape, November 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

The eight identified threat groups are as follows:

- **Ransomware:**

Ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability. Generally, there are four high-level actions (lock, encrypt, delete and steal) used by ransomware to impact the assets' availability, confidentiality, and integrity.

  - Ransomware as a service (RaaS) is increasingly common and consists of a subscription-based model that enables affiliates to use already-developed ransomware tools to execute ransomware attacks.
  - Phishing is the most used attack vector to gain an initial foothold in an organisation. The second most important initial attack vector for ransomware attacks is the compromise through RDP (Remote Desktop Protocol), especially when multifactor authentication (MFA) is not enabled.
  - Classic ransomware operations would collect information before engaging in additional actions such as extortion with or without encrypting the files. If the company refuses to pay, the leak is made public and/or the data is made public on so-called leak sites.
  - The average time to exploit is within eight days of a vendor's publication of the vulnerability. This trend highlights the importance of proper patch management and a threat-informed approach to the risk management of vulnerabilities.

- **Malware:**

Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system. Examples of malicious code types include viruses, worms, trojan horses or other code-based institutions that infect a host.

  - The rise in malware is attributed mainly to crypto-jacking and IoT malware.
  - Malware distribution is also achieved by so-called supply chain attacks. Open-source frameworks are either cloned with infected malware, with the goal of infecting anyone who implements these as tools or packages within their projects.
  - Malware distribution campaigns shifted away from macros because office applications block macros from the internet.
  - Targeted mobile malware is an important threat throughout 2021 and 2022.

- **Social engineering:**

Social engineering encompasses a broad range of activities that attempt to exploit a human error or human behaviour with the objective of gaining access to information or services. In cybersecurity, social engineering lures users into opening documents, files or e-mails, visiting websites or granting unauthorised persons access to systems or services. And although these tricks can abuse technology, they always rely on a human element to be successful.

  - Phishing remains a popular technique, but new forms of phishing are arising such as spear-phishing, whaling, smishing and vishing.

- In general, the objective of social engineering (and consequentially the impact for victims) is gaining access to information or services or obtaining knowledge about a specific subject but it is also used for financial profit.
- Criminals turn more and more to ready-made material offered by phishing kits or they make use of a service model through 'Phishing-as-a-Service'.
- The use of multi-factor authentication (MFA) has reduced the opportunities for attackers to use compromised accounts as a pivot point for starting social engineering campaigns. So instead of targeting individual mailboxes, we have witnessed attackers shifting to abuse legitimate infrastructure to execute their operations. One example includes compromising a Microsoft Exchange server via ProxyShell or ProxyLogin and then distributing phishing e-mails to internal and external user accounts.
- Business E-mail Compromise (BEC) is one of the most financially impactful types of cybercrime. One of the reasons for the 'popularity' of BECs is that instead of having to go through all the trouble of multi-stage attacks and finding their way in an unknown environment, attackers can just 'ask' to execute a financial transaction (or a variant depending on their objectives).
- Criminals are using QR codes to redirect victims to malicious sites that steal login and financial information.

- **Threats against data:**

Threats against data form a collection of threats that target sources of data with the aim of gaining unauthorised access and disclosure, as well as manipulating data to interfere with the behaviour of systems. Technically speaking, threats against data can be mainly classified as data breach and data leak.

These threats are also at the basis of many of the existing threats such as ransomware and DDoS (Distributed Denial of Service) which aim to deny access to data and possibly collect a payment to restore this access, and disinformation and misinformation build on data manipulation.

- Machine Learning (ML) and Artificial Intelligence (AI) are increasingly being adopted and are boosting the migration from traditional software systems based on deterministic algorithms to systems where ML or AI models bring a new wave of risks.
- The central role assumed by data as the enabler of a data-driven economy makes data a major target for cybercriminals.
- Web applications, e-mails, and carelessness (e.g., errors and misconfigurations) are among the main data breach vectors, coupled with the use of stolen credentials, ransomware and phishing as the types of action forming the basis of breaches.
- 82% of data breaches involve a human element.
- Servers were the most important assets targeted by an attack (almost 90%), followed by persons (less than 30%) and user devices (less than 20%).
- Financial gain is the most common motivation for these attacks.
- The motivation of cybercriminals has shifted and instead of targeting consumers in order to steal large amounts of personal information, they focus on specific data types.
- One of the major threats in the data domain is the data poisoning and manipulation. Data integrity is not the only property to protect and guarantee, but also data provenance, non-repudiation, and accountability should be supported.

- **Threats against availability - Denial of Service (DDoS) and Internet Threats:**

Availability is the target of a plethora of threats and attacks, among which DDoS stands out. Attacks occur when users of a system or service are not able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or overloading the component of the network infrastructure.

  - DDoS recently moved to mobile and sensor-based scenarios, where the availability of devices and sensors is decreased by speeding up battery consumption and because their limited resources that often results in poor security protection.
  - Ransom Denial of Service (RDoS) is the new frontier of denial of service attacks. RDoS aims to identify vulnerable systems that become the target of the attack and put in place different activities that result in a final request to pay a ransom.
  - Shift from UDP-based to TCP-based attacks.
  - Cybercriminals are targeting cloud services and take advantage of deficiencies in cloud assets and configuration management.
  - Public APIs can be used as attack vectors to gain access to individual endpoint devices.
  - Resource Public Key Infrastructure (RPKI) is a way to sign certificates that will attest to holding the IP address space and AS number.

- **Disinformation – misinformation:**

Disinformation and misinformation campaigns represented by wrong or purposely falsified information are still on the rise, spurred by the increased use of social media platforms and online media, sometimes without it being validated.

  - The role of AI-enabled disinformation is increasingly becoming central in the creation and spreading of disinformation, and it can make the future supply of disinformation infinite.

- **Supply chain targeting:**

A supply chain attack targets the relationship between organisations and their suppliers. For an attack to be classified as a supply chain attack, both the supplier and the customer have to be targets. More specifically, a first attack on a supplier that is then used to attack a target to gain access to its assets. This target can be the final customer or another supplier.

  - While the complexity of the supply chain and dependencies on third parties will only increase, organisations will be required to gain more control and visibility into the web of their supplier relationships and dependencies, possibly by consolidating the number of partners they rely on.
  - Threat groups have an increased interest and exhibit an increasing capability in supply chain attacks and attacks against Managed Services Providers (MSPs).

3.2. Cyber Threat Taxonomies

An important element of the methodology for delivering a cybersecurity threat landscape is the definition of taxonomies as the classification used to structure the threat ecosystem. The taxonomies therefore dictate the structure of the data collected and produce a reliable and consistent output.

This section provides a mapping of the types of threats, threat actors, their motives, and the impact identified during the reporting periods for the ETL 2021[3] and 2022[2] together with ISO 27005:2022.

ISO 27005:2022 'Information security, cybersecurity and privacy protection - Guidance on managing information security risks' is a standard applicable to all organisations regardless of type, size or sector which provides guidance to perform information security risk management activities, specifically information security risk assessment and treatment and to fulfil the requirements of ISO/IEC 27001 regarding information security risks' management. It is noted that the ETL 2022 report was developed using the established ENISA Cybersecurity Threat Landscape Methodology[4]. ISO 27005:2022 was selected in line with the survey results presented in Chapter 7, i.e., as per the majority of the survey respondents, when an international framework is used for risk assessments, this is a standard of the ISO 2700x family.

3.2.1. ISO 27005:2022 cyber threat taxonomy

When taking into account the value and dependencies of the assets to the organisation, risks can be assessed through the evaluation of assets and the respective threats and vulnerabilities (asset-based approach). A threat exploits a vulnerability of an asset to compromise the confidentiality, integrity and/or availability of the related information.

Information on threats could be obtained from incident reporting, asset users and owners, as well as external sources. ISO 27005:2022 provides examples of typical threats which can be deliberate, accidental or environmental (natural) and could result in damage or loss of essential services. The said **examples of threats** are grouped into **7 categories**:

- *Physical threats* – fire, water, pollution/harmful radiation, major accident, explosion, dust/corrosion/freezing
- *Natural threats* – climatic, seismic, volcanic, meteorological phenomenon, flood, pandemic/epidemic
- *Infrastructure failures* – failure of a supply chain, failure of cooling/ventilation system, loss of power supply, failure in telecommunications network or equipment, electromagnetic or thermal radiation, electromagnetic pulses
- *Technical failures* – failure of device/system, saturation of the information system, violation of information system maintainability
- *Human actions* – terror/attack/sabotage, social engineering, interception of radiation of a device, remote spying, eavesdropping, theft of media, equipment or documents, theft of digital identity or credentials, retrieval of recycled or discarded media, disclosure of information, untrustworthy data input, tampering with software or hardware, drive by exploits using web-based communication, replay attack, man-in-the-middle attack, unauthorised processing of personal data, unauthorised entry to facilities, incorrect use of devices, damaging devices/media, fraudulent copy of software, use of counterfeit/copied software, corruption of data, illegal data processing, sending/distributing malware, position detection
- *Compromise of functions or services* – error in use, abuse or forging of rights/permissions, denial of actions
- *Organisational threats* – lack of resources, failure of service providers, violation of laws and regulations

[3] ENISA Threat Landscape, October 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[4] ENISA Threat Landscape Methodology, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

The standard also defines an approach to classify risk sources by providing examples and usual methods of attack. The said examples of usual **attacker profiles – risk sources** are:

- *State-related* – states, intelligence agencies
- *Organised crime* – cybercriminal organisations (mafia, gangs, criminal outfits)
- *Terrorism* – cyber-terrorism, cyber-militias
- *Ideological activism* – hacktivists, interest groups, sects
- *Specialised outfits* – cyber-mercenaries
- *Amateur* – motivated by the quest/fun/challenge
- *Avenger* – motivated by vengeance or injustice
- *Pathological attacker* – opportunistic

The main criteria for classification are the risk source's motivation and ability to act. Motivation could be defined as a risk source's intention to reach an overall situation. While there is a wide range of **motivations**, the standard provides the below examples to express the "**desired end state**":

- *Conquer* – long-term capture of resources or economic markets, gaining political power or imposing values
- *Acquire* – predatory approach, resolutely offensive, driven by capturing resources or benefits
- *Prevent* – offensive approach to limit the actions of a third party
- *Maintain* – efforts to maintain an ideological, political, economic or social situation
- *Defend* – adopting a strictly defensive fallback stance, or an explicitly threatening attitude (e.g., intimidation) in order to prevent the aggressive behaviour of a clearly designated opponent or prevent their action by slowing them down, etc.
- *Survive* – protecting an institution at all costs, which can lead to extremely aggressive actions

Another criterion for classification is the **consequence**, which is defined in the standard as the "outcome of an event" affecting the objectives. It could be direct or indirect, certain or uncertain, qualitative or quantitative, and the impact on the objectives could be either positive or negative.

A qualitative approach to classify **consequences** is defined as follows:

- *Catastrophic* – sector or regulatory consequences beyond the organisation
- *Critical* – disastrous consequences of the organisation
- *Serious* – substantial consequences for the organisation
- *Significant* – significant but limited consequences for the organisation
- *Minor* – negligible consequences for the organisation

Finally, when defining consequence criteria, ISO 27005:2022 takes into consideration the below:

- loss of life or harm to individuals or groups;
- loss of freedom, dignity or right to privacy;
- loss of staff and intellectual capital (skills and expertise);
- impaired internal or third-party operations (e.g., damage to a business function or process);
- effects to plans and deadlines;
- loss of business and financial value;

- loss of business advantage or market share;
- damage to public trust or reputation;
- breaches of legal, regulatory or statutory requirements;
- breaches of contracts or service levels;
- adverse impact on interested parties;
- negative impact on the environment, pollution.

3.2.2. ENISA cyber threat taxonomy

As explained in chapter 3.1, the analysis in **ETL 2022** highlighted the below eight prime - consolidated - **threat groups**, due to their prominence during the reporting period, their popularity and the impact when materialised:

- *Ransomware* - phishing, social engineering, brute-force RDP credentials are some attack vectors used to deliver ransomware
- *Malware*
- *Social Engineering threats* - phishing, spear-phishing, whaling, smishing
- *Threats against data* - data breaches, data leaks
- *Threats against availability: Denial of Service* (DDoS)
- *Threats against availability: Internet threats* - physical take-over and destruction of infrastructure, active censoring, state-owned certificate authorities, BGP hijacking/withdraw
- *Disinformation / misinformation* - RU-UA war, AI enabled, Disinformation-as-a-Service, Covid-19
- *Supply-chain attacks* - increased system complexity and lack of visibility, vulnerabilities commonly present in used business technologies, targeting cybersecurity researchers for access to their findings, threat actors linked to Russia and North Korea

Similarly, the prime **threat groups** identified during the reporting period for **ETL 2021** were:

- Ransomware
- Malware
- Crypto jacking
- E-mail related threats
- Threats against data
- Threats against availability and integrity
- Disinformation - misinformation
- Non-malicious threats
- Supply chain attacks

Also, both ETL 2021 and 2022 considered the below four categories of cybersecurity **threat actors** - due to their prominence during the reporting periods:

- State-sponsored
- Cybercrime
- Hacker-for-hire
- Hacktivists

This list is not exhaustive and could be extended to include more actors, such as insider actors.

Additionally, in the context of ETL 2022, the below **types of impact** were defined:

- *Reputational* - potential for negative publicity or an adverse public perception of the institution
- *Digital* - damaged or unavailable systems, corrupted data files or exfiltration of data
- *Economic* - direct financial loss, damage to national security
- *Physical* - injury or harm to employees, customers or patients
- *Social* - effect on general public or a widespread disruption that could have an impact on society

Knowing the motivation behind a cybersecurity incident or targeted attack provides insights on the adversaries' objectives and can help organisations determine and prioritise their mitigation actions. For this purpose, ETL 2022 has also identified the below **motives linked to threat actors**:

- Monetisation
- Geopolitics/Espionage
- Geopolitics/Disruption
- Ideological (e.g., hacktivism)

3.2.3. Key takeaways

The tables below summarise the cyber threat taxonomy (i.e., threat groups, threat actors, impact and motivation) defined and utilised for ETL, in comparison with the relevant taxonomy in ISO 27005:2022. It is noted that the standard provides guidance on organisational information security risk management activities while the scope of ETL is to provide the status of the cybersecurity threat landscape, i.e., identify intentional cyberattacks – there is no available data on physical and accidental incidents.

Using a taxonomy provides a structured and consistent approach to understanding, managing and responding to cyber threats. By leveraging such taxonomies, organisations could benefit from improved threat awareness and enhanced overall risk management practices. Such practices help to ensure that all types of threats have been considered, while facilitating classification and categorisation. In turn, awareness enables risk mitigation strategies and incident response planning.

Table 1 – Threat Groups: ETL threat groups Vs ISO 27005 typical threats

ETL THREAT GROUPS	ISO 27005 TYPICAL THREATS
Ransomware	Human actions
Malware	Human actions
Social Engineering threats	Human actions
Threats against data	Human actions
Threats against availability: Denial of Service	Human actions
Threats against availability: Internet threats	Human actions
Disinformation – misinformation	Human actions
Supply-chain attacks	Technical failures Infrastructure failures Organisational threats
N/A*	Compromise of functions or services
N/A*	Physical threats
N/A*	Natural threats

*The ETL threat groups relate mainly to human actions and therefore the mapping with the ISO 27005 typical threats is not 1 :1

Table 2 – Threat Groups: ETL threat groups Vs ISO 27005 risk source

ETL THREAT ACTOR	ISO 27005 RISK SOURCE
State-sponsored	State-related
Cybercrime	Organised crime
Hacker-for-hire	Specialised outfits
Hacktivists	Ideological activism
N/A*	Avenger
N/A*	Terrorism
N/A*	Amateur
N/A*	Pathological attacker

*The mapping of ETL threat actors with ISO 27005 risk sources is not 1 :1

Table 3 – Impact

ETL IMPACT	ISO 27005 CONSEQUENCE
Reputational	damage to public trust or reputation breaches of legal, regulatory or statutory requirements adverse impact on interested parties
Digital	N/A*
Economic	loss of staff and intellectual capital (skills and expertise) loss of business and financial value loss of business advantage or market share breaches of legal, regulatory or statutory requirements impaired internal or third-party operations (e.g., damage to a business function or process) effects to plans and deadlines breaches of contracts or service levels negative impact on the environment, pollution
Physical	loss of life or harm to individuals or groups
Social	loss of freedom, dignity or right to privacy negative impact on the environment, pollution

*The mapping of the ETL impact with the ISO 27005 consequence is not 1 :1

Table 4 – Motivation

ETL MOTIVATION	DESIRED END STATE
Monetisation	Conquer Acquire Survive
Geopolitics/Espionage	Conquer Acquire Defend Survive
Geopolitics/Disruption	Prevent Maintain Defend Survive
Ideological (e.g., hacktivism)	Prevent Maintain Defend

4. Cybersecurity incidents

4.1. Cybersecurity incidents with a significant impact reported

In the EU, critical service providers have to notify incidents with a significant impact to the national authorities in their country in order to comply with legislation such as:

- DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018, establishing the European Electronic Communications Code (EECC) in Article 40;
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (EIDAS) in Articles 10 and 19;
- DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) in Article 23.

The incident notification to the national authorities is an important step during an incident response process since the information can be used by the competent authorities to determine new security policies, risk management strategies or other compliance standards to improve the resilience of essential services through the EU. In situations that the national authority is also the national CSIRT team, the report of the incident can also trigger support activities for the organization related to incident handling. Additionally, the report of the incident can be used to proactively prevent similar incidents in other organizations.

Annual summary reports about these incidents are collected, aggregated and analysed by ENISA on the Cybersecurity Incident Reporting and Analysis System (CIRAS[5]). This chapter aims to **summarize** the data from the **annual summary reports submitted in 2020, 2021 and 2022 for the health sector**.

In 2020, 495 incidents were reported under all these legislations, of which 88 occurred in the health sector **(17%)**.

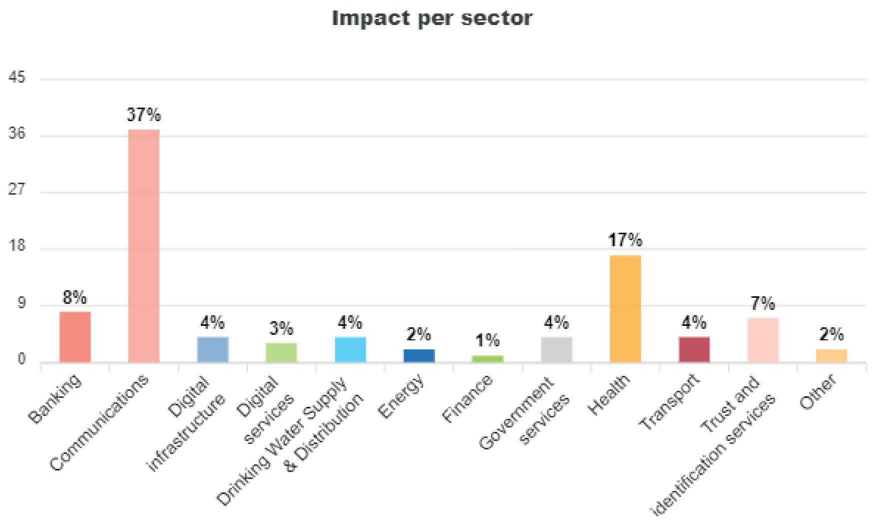


Figure 1 - Impact by sector 2020

[5] https://ciras.enisa.europa.eu/

One important consideration is that, in 2020, considering only the reports of incidents under the NIS Directive (NISD), **the most impacted sector was the health sector**, with 31% of the incidents with significant impact reported under article 14 and 16 of NISD.

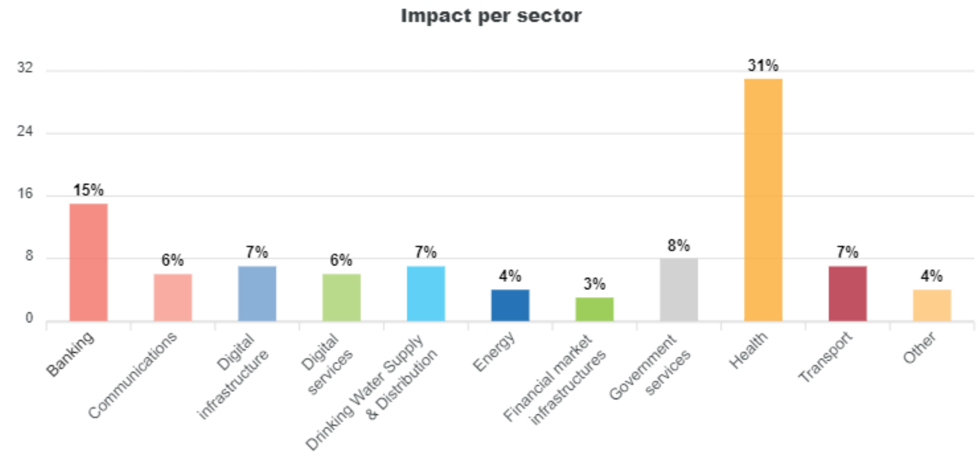


Figure 2 - NISD reported incidents by sector 2020

As shown in the following images and graphs, the nature of the incidents in more than 50% of the cases related to system failures (59%). Human errors and malicious actors are the nature of the remaining incidents (at 19% each) and 2% was caused by nature phenomena.

As technical causes, software bugs (22%), faulty software changes and updates (17%), and hardware failure (15%) were reported. On the other hand, phishing and malware & viruses only represent 6% of the technical causes of the reported incidents with significant impact.

The technical assets most affected were workstations (in 64% of the cases).

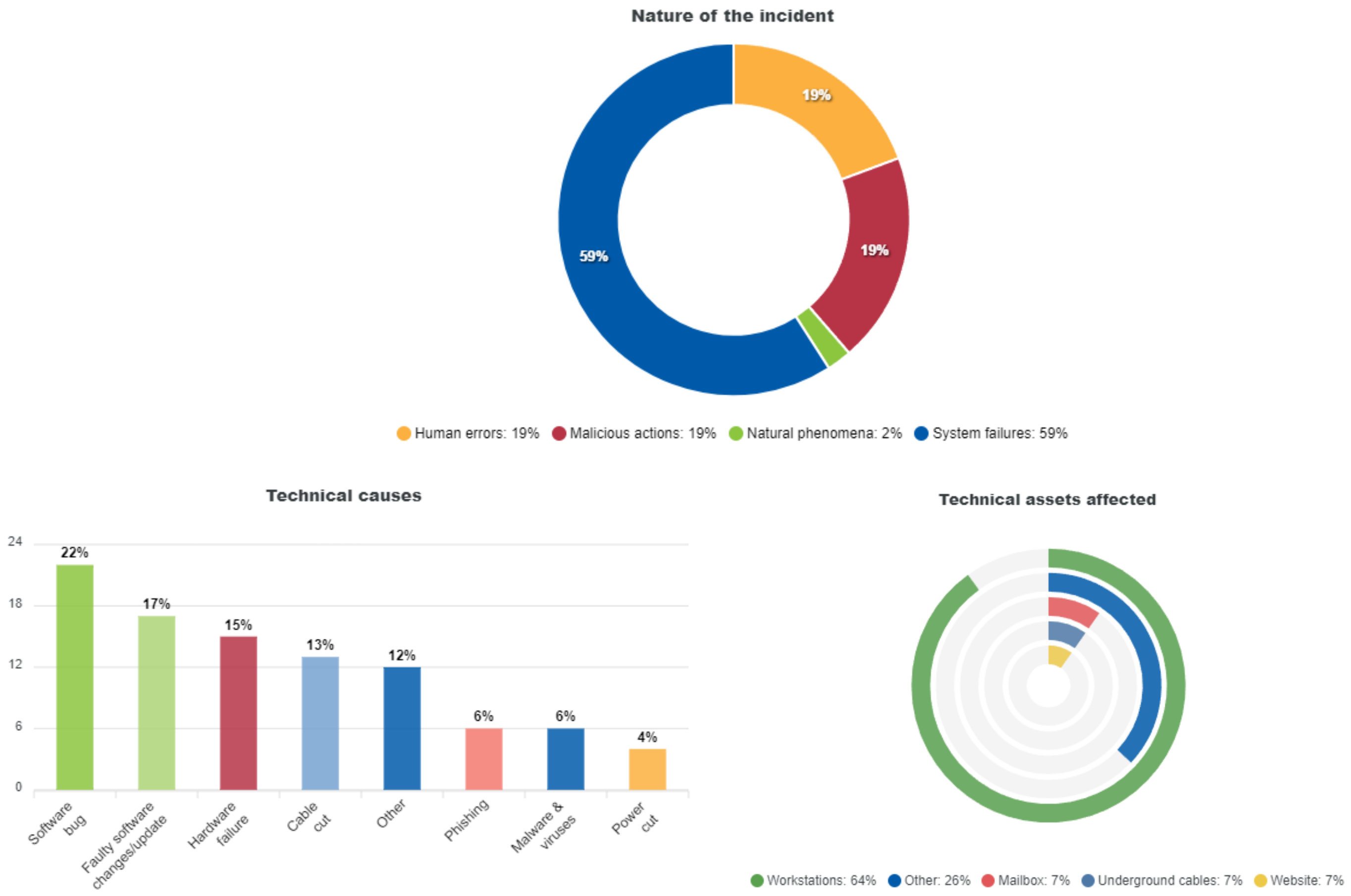


Figure 3 – NISD incidents information from 2020

In 2021, 559 incidents were reported under all the legislations referred, of which 98 occurred in the health sector **(17%)**.

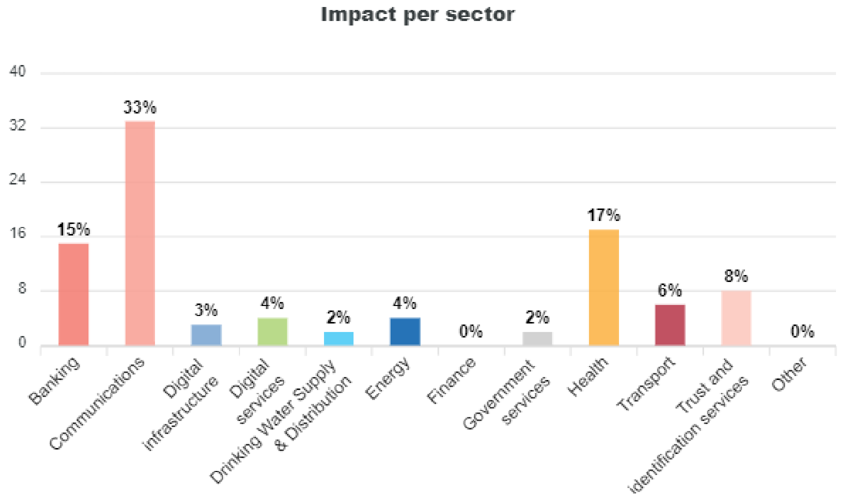


Figure 4 - Impact by sector 2021

With a situation similar to 2020, **in 2021 the health sector continues to have a prominent role in the reports of incidents under the NIS Directive (NISD)**, representing 28% of the total of incidents reported.

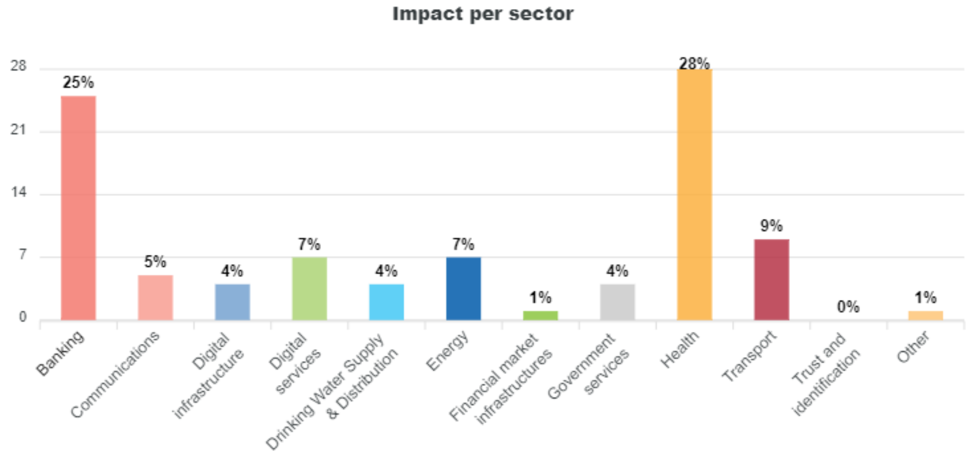


Figure 5 - NISD reported incidents by sector 2021

The following images and graphs show that the more predominant nature of the incidents continues to be system failures, with an incidence of 54%. Incidents caused by malicious actors increased 7% since 2020, representing 26%. Human errors continue to represent a significant cause of incident in the health sector with a percentage of 18% (1% less than in 2020).

The technical causes for the incidents in 2021 were slightly different than those from 2020, where software bug cause decreased 13% (in 2021 representing 9%), ransomware appears as a new relevant cause with 14% and phishing causes have no relevant expression in the reported incidents. Cases related with faulty software changes and updates represented 21% (4% more than in 2020) of the reported incidents, hardware failures 18% (3 % more than in 2020) and, other causes 15% (3% more than in 2020).

Workstations continue to be the most affected technical asset, with a percentage of 56% and servers/domain controllers increased its predominance with 28%.

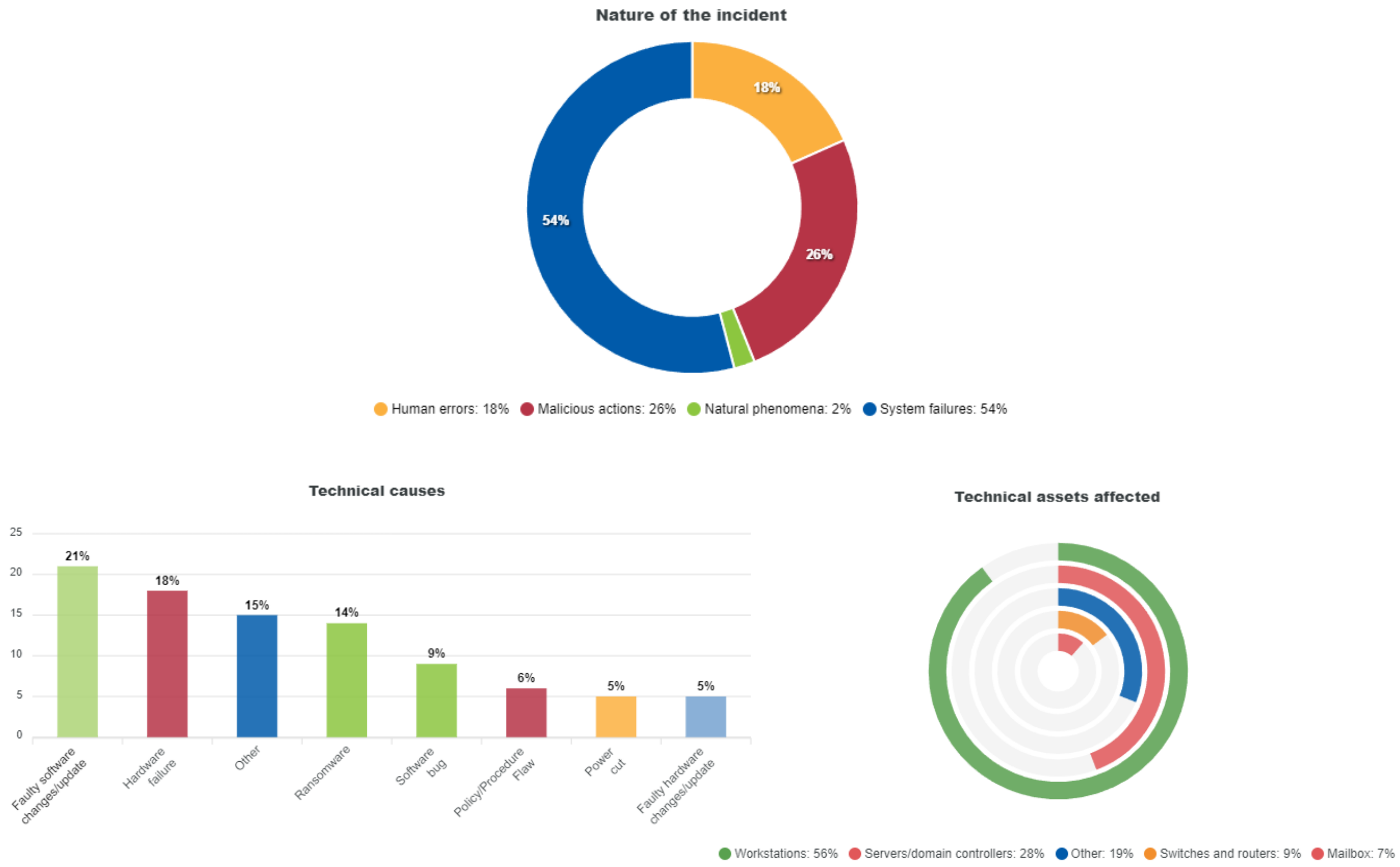


Figure 6 - NISD incidents information from 2021

In 2022, 1083 incidents were reported, of which 284 occurred in the health sector **(26%)**.

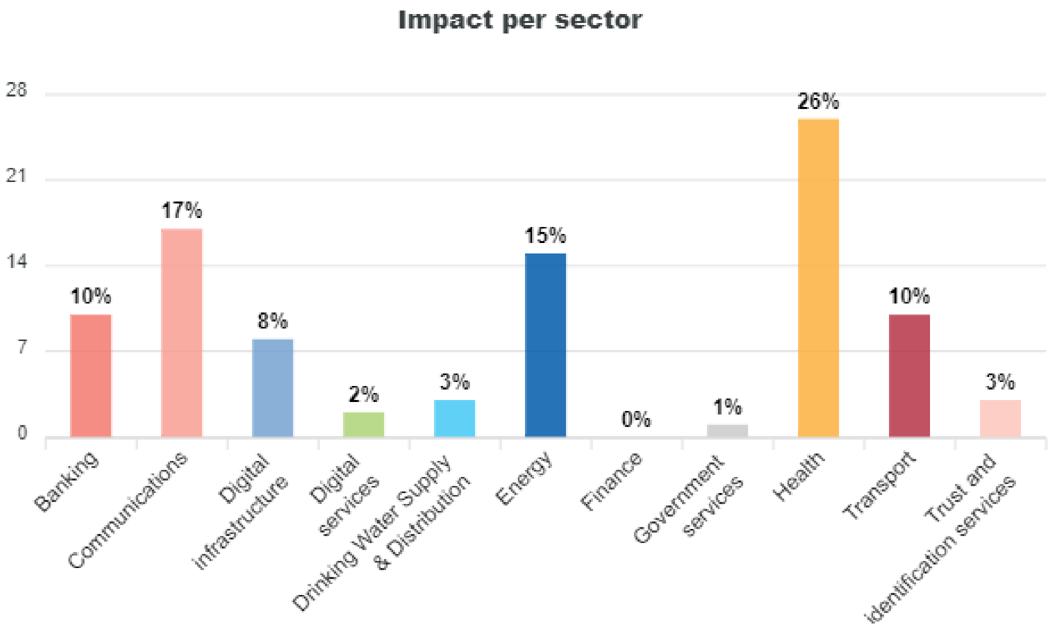


Figure 7 - Impact by sector 2022

In 2022 the health sector, as in 2020 and 2021, **was the most impacted sector as per the NIS Directive annual summary reporting**, representing 32% of the total of incidents reported (284 incidents in total).

All the detailed information presented can be consulted in **Figure 8** and **Figure 9.**

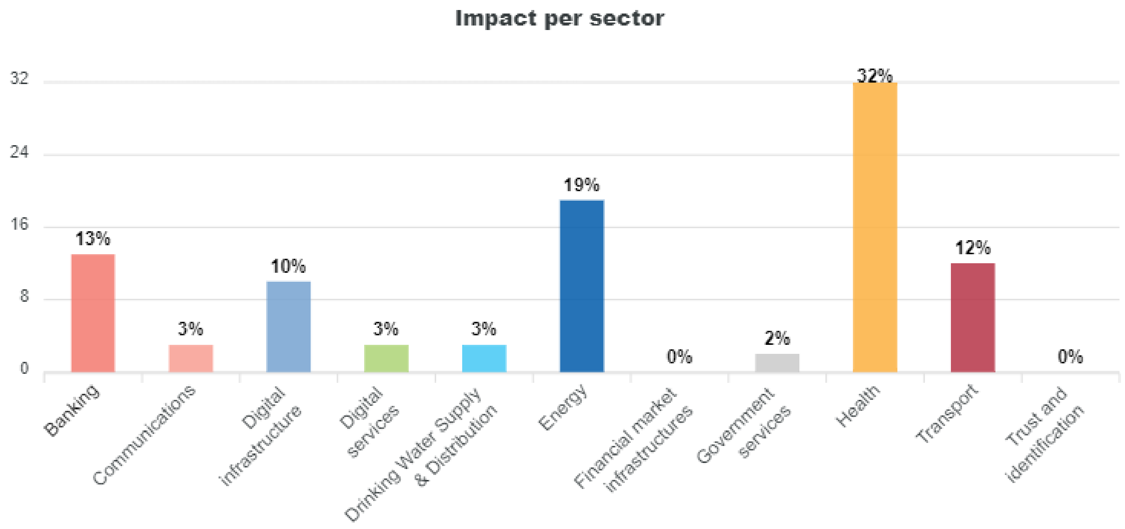


Figure 8 - NISD reported incidents by sector 2022

Maintaining the trend observed in the last 2 years, most incidents were originated from system failures (account for 68% of all occurrences) and malicious actors were responsible for 16% of accounted incidents. Also similar to 2021, human errors accounted for 16% of the reported incidents in 2022.

The main technical causes, besides the 63% of "other”, were the software changes and updates which represented 10% (same than 2021), the hardware failures (7%) and software bugs (5%). Ransomware decreased from 14% (2021 data) to 2% of the technical causes of the reported incidents with significant impact. Contrary to what happened in 2021 (no phishing incidents), but closer to what happened in 2020 (6% in 2020), phishing was the technical cause in 4% of the incidents.

Regarding the technical assets affected, in 2022 the results were different from 2020 and 2021. In addition to the 65% identified as “other”, apps and servers/domain controllers were the most impacted with 17% and 12%, respectively. The incidents reported show that workstations were affected in 7% of occurrences and that mailbox incidents now account for 5% of the occurrences.

In the future, for a more precise analysis, it would be important to understand what "other" represents, since it has been taking a predominant technical cause of incidents over the years: 12% in 2020, 15% in 2021, 63% in 2022. Also in the technical assets, the option “other” is considered with relevance: 20% in 2020, 19% in 2021 and 65% in 2022.

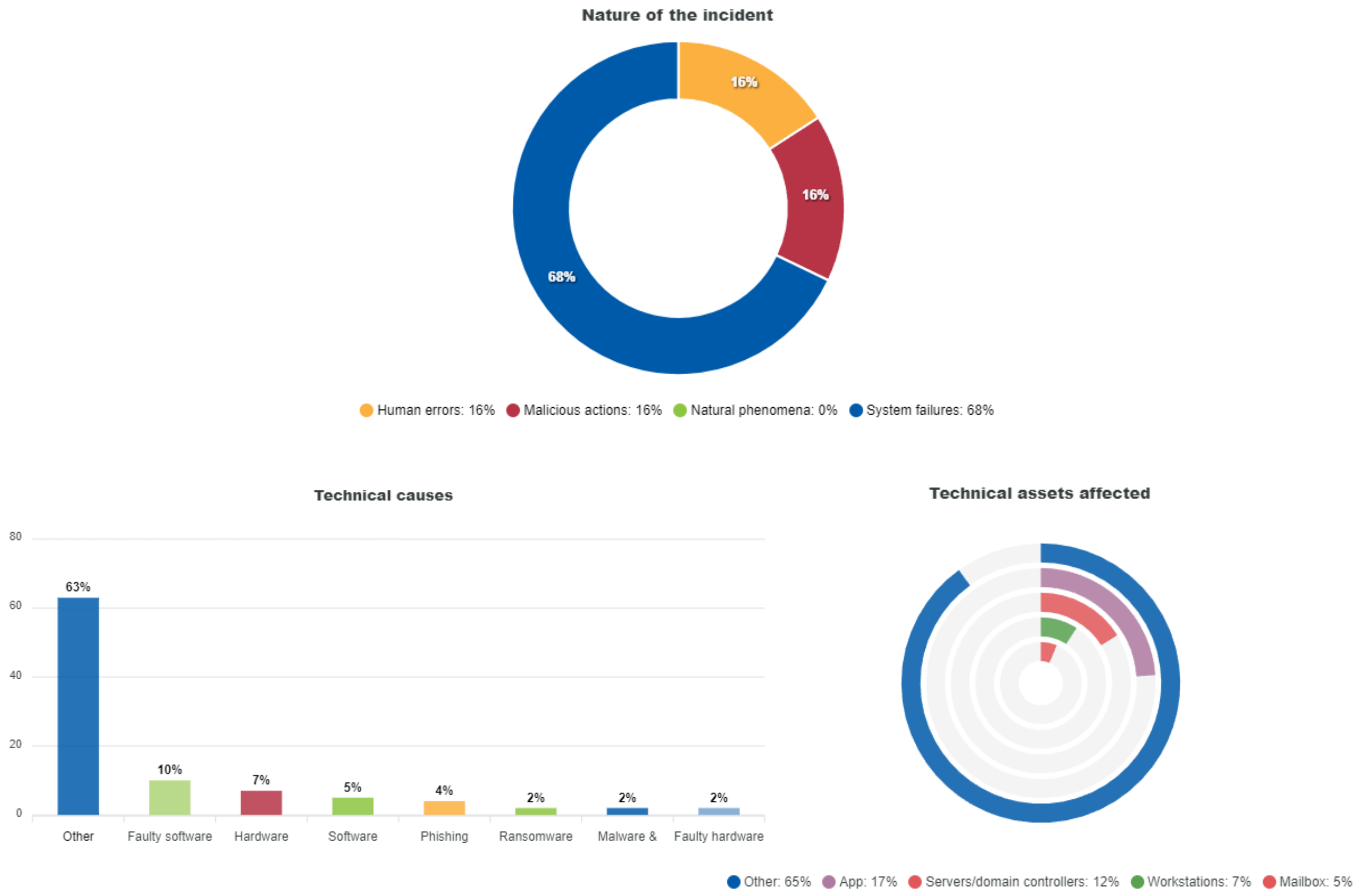


Figure 9 - NISD incidents information from 2022

4.2. Health cybersecurity incidents in 2021, 2022 and early 2023

This section focuses on open-source data and other sources of Cyber Threat Intelligence (CTI) including data from ENISA CTI partners related to incidents in the EU Member States involving any institutions that can fall under the health sector scope and from 2021 to early 2023.

As per the information collected for the **ENISA Threat Landscape for the health sector**[6], 215 incidents occurred in the EU: 91 incidents in 2021, 81 in 2022 and 40 during the first quarter of 2023. It is noted that what is outlined in this chapter does not dispense from reading the original document.

Out of these 215 incidents, 63 had an impact on medical records/patient personal data and 59 incidents impacted non-medical IT systems and networks that are not essential for patient care, such as administrative systems. Also, it was identified that EU healthcare providers and hospitals were affected the most.

[6] ENISA Threat Landscape: Health Sector, June 2023. https://www.enisa.europa.eu/publications/health-threat-landscape

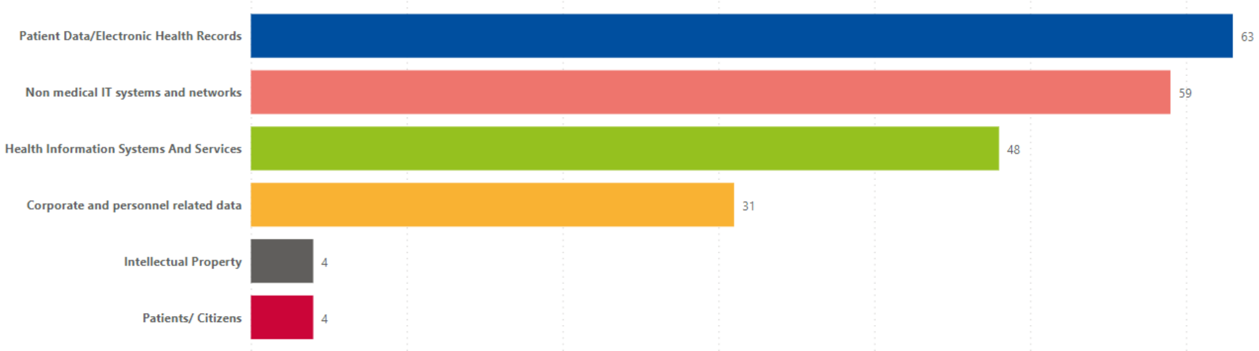


Figure 10 - Assets affected

In is worth noting that in this data set, a high number of ransomware incidents was observed, with **more than half being incidents confirmed to be ransomware related** (54%) and being the majority of the attacks motivated by financial gain.

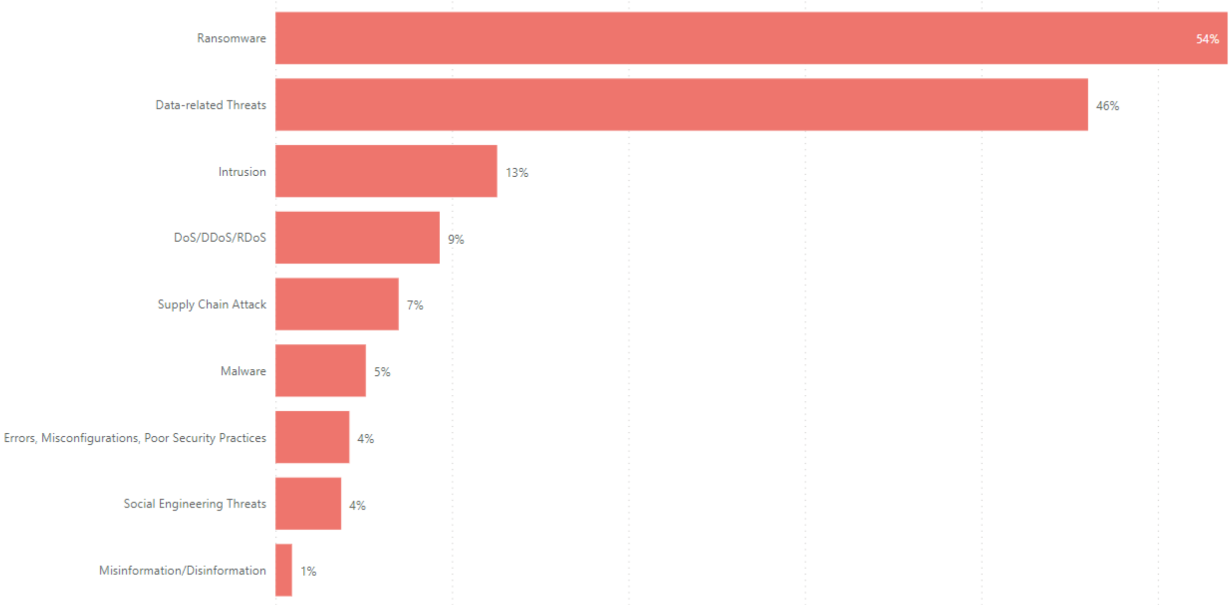


Figure 11 - Attack category

4.2.1. Main Threat Actors

The majority of cyber incidents affecting the European healthcare sector remain unattributed and likely some of them can be State sponsored APTs (Advanced and Persistent Threats) targeting of this sector due to espionage purposes.

The actors assessed to be most active in the EU health sector during the period are cybercriminal ransomware groups such as Lockbit 3.0 (20 incidents), Vice Society (9 incidents), and BlackCat/ALPHV (5 incidents).

- **Lockbit** is the group responsible for developing LockBit ransomware, which is available under a malware-as-service model, operating since 2019. They have been targeting health institutions and demanding ransomware in exchange for decryption. The LockBit group operates on a double extortion model whereby failure to pay the ransom results in stolen data being publicly posted to the group's dark web leak site.

- **Vice Society** is a ransomware group thought to have been operating since at least June 2021. They have been observed primarily targeting health and education sectors. They make considerable efforts to detect security solutions, cover their tracks, and delete backups, making it more likely that a ransom is paid.
- **BlackCat/ALPHV** is a ransomware gang presumed to originate from Russia with records since November 2021. They use triple-extortion tactics whereby affiliates supplement their initial ransom with an additional threat of performing a Distributed Denial of Service (DDoS) attack against the victim's network after stealing, encrypting, and selling their data. This method of extortion puts further pressure on the victim to pay the ransom.

4.3. Other relevant health cybersecurity incidents

The following incidents are real-life incidents that occurred in the health sector in several countries and should stand as a warning to remind the importance of having adequate technical and organisational measures to reduce the risk of cyberattacks.

- **UK's National Health Service attack**

On May 12th 2017, the UK's National Health Service was attacked by criminals using the WannaCry ransomware. These ransomware attacks exploited a vulnerability in computers running an old version of Windows without a security update to prevent a remote takeover. The attack disrupted health services in hospitals across Britain. The NHS cancelled approximately 19,000 appointments, radiology sessions, outpatient appointments, and elective admissions. Emergency ambulances were forced to be diverted to unaffected medical facilities. The NHS lost about £20M due to cancelled appointments and spent around £72M on technology to recover data and improve the security of the existing infrastructure.

- **Singapore's SingHealth data breach**

In 2018, Singapore's SingHealth suffered a data breach incident where the health information of 1.5 million patients was seized. Names, National Registration Identity Card (NRIC) numbers, addresses, dates of birth, race, and gender of patients who visited specialist outpatient clinics and polyclinics between 1 May 2015 and 4 July 2018 were maliciously accessed and copied.

- **Düsseldorf University Hospital cyberattack**

In September 2020 a patient death directly attributable to a cyber-attack was reported. While a patient was scheduled to undergo critical treatment at Düsseldorf University Hospital in Germany, a ransomware attack disabled the systems that supported their medical devices. Due to the attack and the limited capabilities to provide adequate care, the hospital was forced to transfer their patient to another hospital that was 19 miles (30 kilometres) away. The patient died during the transfer.

In a later stage, German prosecutors railed back on their accusations and stated that no sufficient legal causation could be established between the cyberattack and the death of the patient, as her health conditions were already too bad to survive and even an operation in Düsseldorf would probably not have saved her.

- **Trinity Health ransomware attack**

Trinity Health experienced the largest impact among healthcare providers due to the 2020 ransomware attack on Blackbaud, a vendor of cloud-based customer relationship management software. The attack on one of Blackbaud's self-hosted cloud servers affected hundreds of customer organisations around the world, including more than two dozen healthcare organisations, and led to the compromise of more than 10 million records. Blackbaud stopped the cybercriminals before they fully encrypted files in the hacked databases, but not before they exfiltrated sensitive data.

- **Health Service Executive of Ireland cyberattack**

On 14 May 2021, the Health Service Executive of Ireland suffered a major ransomware attack which caused its IT systems nationwide to be shut down. The initial vector of attack was a malicious Microsoft excel file that was downloaded and allowed the attackers to access HSE systems. More than 80% of IT infrastructure was affected, with the loss of key patient information and diagnostics, resulting in severe impact on the health service and the provision of care. The attack occurred during the COVID-19 pandemic. Ireland's COVID-19 vaccination programme was not affected, but the attack caused a significant disruption with routine appointments being cancelled, including maternity check-ups and scans. Several hospitals described situations where they could not access electronic systems and records and had to rely on paper records.

- **Shields Health Care Group attack**

In May of 2022, Shields Health Care Group, a medical imaging service provider reported that a cybercriminal had gained unauthorized access to some of its IT systems back in March. All told, over 2 million patients had their personal health information stolen, including names, addresses, social security numbers, insurance information, and medical history information. Because Shields Health Care Group is a third-party vendor that provides MRI, PET/CT, and outpatient surgical services for the sector which supplies management and imaging services for approximately 50 healthcare providers, the scope of the attack was massive.

- **French Hospital targeted by hackers**

A hospital in Versailles was hit in December 2022 by a cyber-attack and had to shut down telephone and computer systems due to a ransomware attack. The Hospital has been forced to cancel several operations, some patients had been transferred and has called in extra staff to the intensive care unit because while the machines there were still functioning, additional staff were needed to monitor the screens as they were no longer connected to the hospital's network. The cyberattack had led to a total reorganisation of the hospital.

4.4. Key takeaways

The number of cybersecurity incidents with significant impact in the health sector have been growing in the recent years. Since 2020, the health sector has been the most impacted sector under the NIS Directive with an average of 29% of the total incidents reported. The vast majority of reported incidents originated from system failures, however, incidents involving malicious actors have been increasing over the years. In the health sector, human error is also an important incident cause to take into consideration.

One of the important assets to consider and protect are the workstations since these directly relate to medical diagnosis equipment, whose data supports other hospital information systems such as electronic health record systems, radiology information systems, etc. Several of the reported incidents with significant impact had the workstations as the asset affected.

Looking at the health sector in a more transversal way and not just necessarily at operators of essential services who have the obligation to report incidents of relevant impact under the NIS directive, healthcare has also been affected by different ransomware attacks for financial gains. These incidents are damaging to day-to-day operations by blocking access to files and systems essential to patients and healthcare provision. They impact the integrity and availability of data and, sometimes, also confidentiality.

There are examples of known and impactful cybersecurity incidents which resulted in disruptions and constrains on the provision of the health services and that indirectly impacted the patients' life.

The health sector needs to better evaluate the connection between patient safety and cybersecurity. The number of serious adverse events or patient deaths are largely unknown, as mechanisms generally do not exist to examine such problems within the context of cybersecurity concerns because hospitals are dealing with patient safety issues only when adverse events happen from a traditional people and process perspective.

5. Current and Emerging Healthcare Cyber Threats and Vulnerabilities

Based on a trend analysis of tactics, techniques, and procedures (TTPs) used by cyber criminals, we found **six significant cyber threats** the health sector faces retroactively for 2020, 2021 and 2022 and looking ahead towards 2023: **ransomware**, **threats against data**, **DDoS attacks**, **supply chain attacks, malware and social engineering threats (phishing).**

Other important cyber threats affecting the health sector are intrusion, errors/misconfigurations and misinformation/disinformation. Additional and detailed threat analysis can be also consulted in the ENISA Threat Landscape: Health Sector[6].

I. Ransomware

In 2022, an increasing trend in double extortion was once again observed, where after extraditing a key for decryption, cybercriminals subsequently threatened both companies and citizens with leaking information that was stolen in connection with the ransomware attack.

There is a tendency to carry out several further extortions in a continued ransomware attack, also referred to as 'quadruple extortions', where cyber criminals further exploit the leakage e.g., threats that carry out DOS-attacks as well as contacting third-party suppliers, partners, clients, employees, media etc., which will then further impact the targeted organisation.

The healthcare sector is particularly vulnerable to ransomware, and these attacks can disrupt critical operations, prevent healthcare professionals' access to patient data and health records, and thus disrupt patient care and the general healthcare services used on a daily basis.

An attack can also result in the loss and/or theft of sensitive patient information, which can be used for identity theft or other malicious purposes, such as data leaks.

There have been major attacks against the health sector, which have had particular financial consequences, but also consequences for the individual citizen.

II. Threats against data

Threats against data, typically known as data breaches and data leaks result in unauthorised data access, manipulation and disclosure and are interconnected with other threats, such as ransomware, malware or DDoS.

Breached data can in turn be used for identity theft, financial fraud or other malicious activity and could cause financial loss, reputational damage and legal implications.

The exploitation of vulnerabilities, misconfigurations and poor security practices and human error are some common examples of ways for cybercriminals to gain access to the organization's assets (including data).

Patient data was leaked on multiple occasions during the Covid-19 pandemic.

III. Distributed Denial of Service (DDoS) attacks

DDoS attacks can present a challenge for the healthcare sector, as they can disrupt the functioning of systems and services by overwhelming a network with traffic and exhaust its resources. It is difficult to disrupt the healthcare sector's critical services to a serious degree with DDoS attacks, since the services that are critical in relation to patient treatment are initially kept on the internal networks of the treatment facilities. However, it is possible that DDoS attacks will have moderate consequences for the citizen by, for example, making a website for a medical practice and hospital inaccessible.

While DDoS attacks can cause inconvenience and temporary disruption, it's important to note that they don't necessarily result in permanent data loss or harm to patients. However, it's also crucial to be aware that DDoS attacks can be used as a smokescreen for other cyberattacks, such as accessing sensitive data or planting malware.

To minimize the impact of DDoS attacks and to protect against other potential threats, healthcare organisations can implement various security measures, such as firewalls, intrusion detection systems, and incident response plans. By taking a proactive and comprehensive approach to cybersecurity, healthcare organisations can help ensure that their systems remain available and secure for their patients and staff.

Even though DDoS attacks do not seem to have significant impact and cause limited downtime, they are on the rise due to the hacktivist groups targeting the sector with the goal of fear, confusion and publicity in the media.

IV. Supply Chain Attacks

A trend has emerged over the past few years, where hackers target Managed Service Providers (MSP) in order to compromise a vendor that may have access to a large customer base. The attacks against an MSP are often carried out by Advanced and Persistent Threat actors, who spend time undertaking reconnaissance, evading detection, escalating privileges, moving across environments, collecting data, gaining control, leaking data and encrypting data.

Cybercriminals are more likely to focus on supply chains as a viable attack vector, especially given the successful breaches of SolarWinds, Kaseya and the exploitation of Apache's Log4j. Cybercriminals know that a supply chain breach will provide them with access to a larger attack surface than by targeting them individually.

Supply chain attacks are considered to pose a very high threat to the healthcare sector. It's worth noting that 90% of the top 10 worldwide health data breaches reported during 2022 were caused by third-party vendors, just like in 2021. These incidents should serve as a warning to revisit third-party vendor relationships, ensure the institution is at least annually performing a review of vendors relationships and dependencies, and consider consolidating vendors where possible.

It has been assessed that there is a high frequency of supply chain attacks, and it is anticipated that cybercriminals will try to exploit the sector's vendors in future attacks against the healthcare sector.

The healthcare sector relies on many different vendors that supply both IT systems and infrastructure to all those within the healthcare sector. The continued operations of networks and information systems are heavily reliant on these vendors. Therefore, an attack against the supply chain is believed to have serious consequences should the IT support to these healthcare services ever be compromised.

V. Malware

Malware, also called malicious code or malicious logic, is often used in incidents that have major consequences for the organization that is affected and the citizens whose information is processed. In particular, malware is distributed in phishing campaigns, to which the healthcare sector is also vulnerable.

The malware components used in an attack depend on the threat actor's goals. It can be anything from gaining control over systems and networks (initial access brokers, botnets) or over data (ransomware threat actors, information theft) to making them completely inaccessible.

An attack against the healthcare sector involving the use of malware would have consequences for access to patient data and patient records, thus disrupting patient treatment and the general healthcare services that are used on a daily basis. Furthermore, an attack can result in the loss and/or theft of sensitive patient information that can be used for identity theft or other malicious purposes, such as data.

VI. Social engineering threats (phishing)

Many of the hacking or malware attacks targeting the healthcare sector use social engineering threats as phishing that attempt to exploit a human error or human behaviour to initially gain access to the sector’s network and information systems, which is why the potential consequences have been assessed to be severe.

Phishing is also closely associated with ransomware since most of the impactful attacks in the healthcare sector were ransomware attacks that had phishing to reconnaissance, weaponize and deliver the attack.

The healthcare sector in particular is a target for cybercriminals using phishing attacks, particularly because healthcare data is at a premium and can provide large financial gains for the attacker. It can be easy to carry out a phishing attack, and it only takes one click to install malicious files or scripts.

5.1. Related vulnerabilities

As the risk surface and the threat landscape is expanding, this gives rise to numerous cybersecurity vulnerabilities. By understanding these vulnerabilities, entities can implement measures to secure their systems, networks and information from potential threats. The most common vulnerabilities faced by the health sector are outlined in this section.

I. Insiders

There is a very high frequency of breaches related to insider threats. This is primarily due to the number of accidental incidents, where an employee accesses or shares data due to negligence, error or misuse in the work process. In cases where technical personnel act in negligence or make errors, serious operational consequences could occur.

Although less frequently than insider errors, it is also important to consider the insider actors who act in bad faith because they are unhappy with the organisation and see an opportunity to take financial advantage with malicious action.

Insiders are also subject to social engineering and phishing techniques, which exploit trusted humans within an organisation and manipulate them into revealing sensitive information or performing unauthorised actions.

II. Legacy Systems

It is often expensive for vendors to certify specialized IT systems in markings such as CE and GXP, which is why they are keen to maximize the lifespan of these certifications. Unfortunately, this means that the cybersecurity standards of specialized IT systems become outdated over time. The healthcare sector works to secure legacy systems on a daily basis by using WAF (Web Application Firewall) solutions or segmentation.

There will always be questions surrounding how accurate critical health systems need to be in order to save lives, or whether they need to adhere to best-practice patching standards for the system to be secure.

In order to achieve the desired outcome with these systems, which are otherwise deemed safe and accurate for use in the healthcare sector and to comply with cyber security standards, much higher requirements should be placed on the vendors providing the solutions, to ensure that they comply with common patch management standards.

It is assessed that legacy systems are very frequently in place, and it is anticipated that cybercriminals will try to exploit the sector's vulnerability in future attacks against the sector.

5.2. Key takeaways

For a risk management procedure and subsequent implementation of technical and organizational measures, it is recommended that health organizations take into account at least ransomware, threats against data, DDoS attacks, supply chain attacks, malware and social engineering threats (phishing) and vulnerabilities such as insiders and legacy systems. During the last years the combination of these threats and vulnerabilities as well as their impact and probabilities have resulted in a very high risk to health organizations.

6. Business Continuity & Mitigation recommendations

To ensure the smooth running of the organisation, it is recommended to implement the following best practices to prevent incidents and minimize risks.

I. Incident Response

- Develop a comprehensive incident response plan to ensure a swift and effective response to security incidents.
- Regularly test and refine the incident response plan to ensure its effectiveness.
- Train employees on incident response procedures.
- Build a team of specialists with skill and knowledge to prevent and response to incidents.
- Ensure that the infrastructure of your organisation collects relevant logs and with sufficient details to support incident response investigations.

II. Access Control

- Implement access control procedures to ensure that only authorized individuals have access to information.
- Regularly review and update access control policies and permissions.
- Monitor and audit user access to sensitive information.

III. Backup and Restore

- Regularly back up critical systems and data.
- Use a backup system that allows multiple versions to be saved.
- Test backups regularly to ensure data integrity and restoration capability.
- Consider the need for offline backups.

IV. IT preparedness

- Regularly review and update emergency plans and related documents to ensure their effectiveness.
- Make sure all relevant parties have access to emergency plans, even in the event of IT system failure.
- Test secondary means of communication.

V. Physical Security

- Implement physical security measures to prevent unauthorized access to the organisation's facilities, equipment, and sensitive information.
- Conduct regular security assessments to identify potential physical security weaknesses.
- Train employees on physical security measures and procedures.

VI. Patch Management and Anti-malware Protection

- Regularly update all hardware, software, applications, and cloud solutions.
- Use a central patch management system and whitelist approved applications.
- Ensure all endpoints have updated anti-malware software.

VII. Awareness Training

- Provide employees with training on social engineering and phishing.
- Consider adding warning banners to all emails from external sources, reminding users of the dangers of clicking links and opening attachments.

VIII. Supplier Management

- Set high security standards for suppliers.
- Regularly audit supplier security, if necessary, through security statements.
- Ensure security requirements are met throughout the entire supply chain, including sub-contractors.

IX. Compliance

- Ensure that the organisation's security practices and policies are following relevant regulations and industry standards.
- Regularly review and assess the organisation's compliance with relevant regulations and industry standards.
- Develop a plan to address any compliance gaps.

X. Knowledge Sharing

- Participate in networks where information on incidents, Indicators of Compromise, alerts, etc. can be shared.

6.1. Key takeaways

Appropriate measures need to be implemented in order to mitigate risks and therefore ensure an organisation’s resilience to cybersecurity incidents. Such measures could relate to incident response plans, procedures for access control, backup, IT security, patch management and third-party management, anti-malware protection, physical security of the facilities and infrastructure, awareness raising to internal and external parties, compliance to legal, regulatory and contractual requirements, and information / knowledge sharing.

The list of measures provided in this chapter is not exhaustive but merely a guidance towards sound business continuity.

7. Cybersecurity context by health organisations

In order to get an overview of the cybersecurity measures currently in place within the healthcare sector, a survey was performed with several stakeholders. The main target audience of the survey were institutions from Member States that carry out their activity in the health sector, regardless of whether they are considered operators of essential services in the context of the NIS Directive.

The survey was published on the EU survey website and was sent out to points of contact in the workstream on Health under the NIS Cooperation Group to the ENISA eHealth Security Experts Group and to the EU Health ISAC mailing list. The runtime was from end of July 2022 until beginning of October 2022.

The questions focused on the different approaches in relation to risk assessments, and on associated difficulties and barriers, as well as on the context of the cybersecurity in the health sector, i.e., what are the most important assets, the major threats and the most impacting incidents.

To get a holistic overview of the security postures of the different entities, the survey was divided in 4 main parts:

1. Identification - Information on the institution, size, and main activity field
2. Risk Management
3. Threats and Types of incidents
4. Certification and Guidance

The survey was completed by 81 operators providing services in 19 Member States of the European Union.

7.1. Identification

The majority of participants that took the survey were from hospitals (of the 81 participating operators 52 are hospitals), the head count is mostly over 250 employees. The remaining participants (29 institutions) are organisations that belong to national eHealth services, medical analysis and clinical biology laboratories, paramedical offices, establishments of assistance and care, while two participants chose "other".

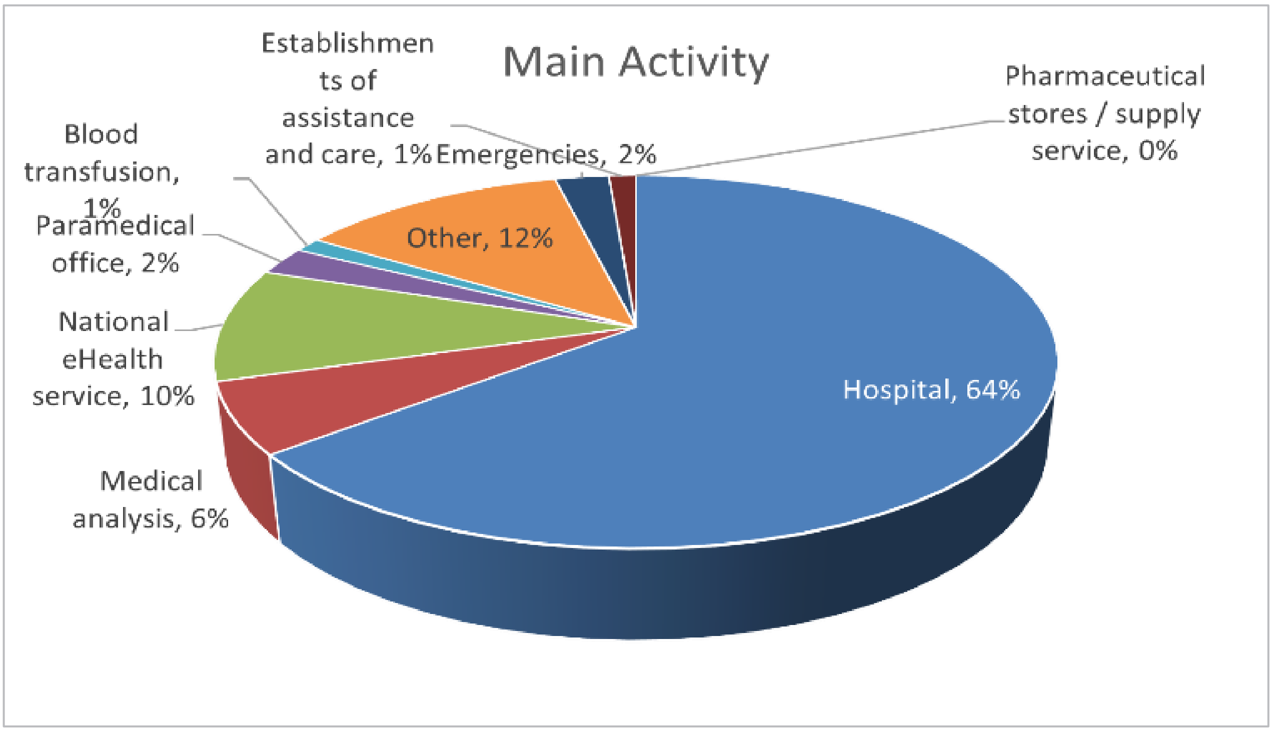


Figure 12 - Activities overview

Figure 13 shows the size of the participating institutions in the survey. It shows that the majority of institutions are to be considered as large institutions as they indicate having 250 employees or more. Out of the 52 participating hospitals, all of them except one selected a head count over 250 employees. The smallest head counts belong to the national eHealth service institutions.

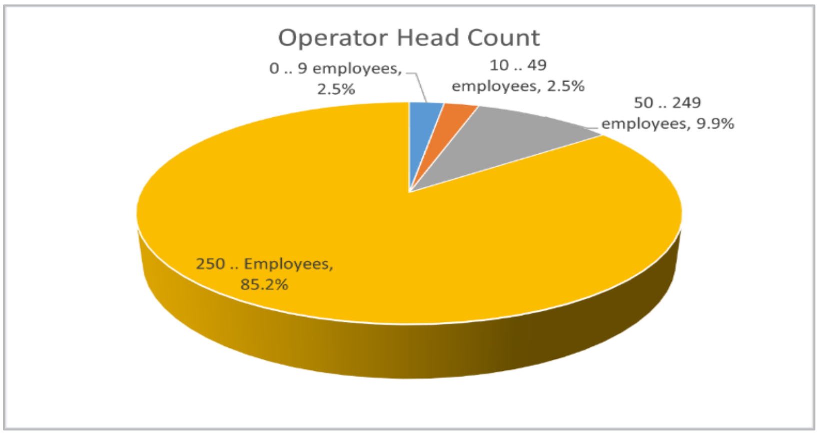


Figure 13 - Operator head count

Almost 93% of the operators are active in only one EU member state.

Geographic area of activity	Number of operators	Operators in %
Only in one EU member state	75	92,6%
Only in EU, in more than one EU member state	2	2,5%
In and outside EU	4	4,9%

Table 5 - Geographic area of activity

7.2. Risk Management

In this chapter, an attempt was made to understand the culture and practices about the information security risk management within the institutions.

7.2.1. Cybersecurity and Risk Management Culture

In **Figure 14** one can see that 63% of the institutions have defined risk management governance responsibilities, and more than half of the participating entities have procedures in place for incident response (54%) and have indicated that they perform a risk analysis (54%).

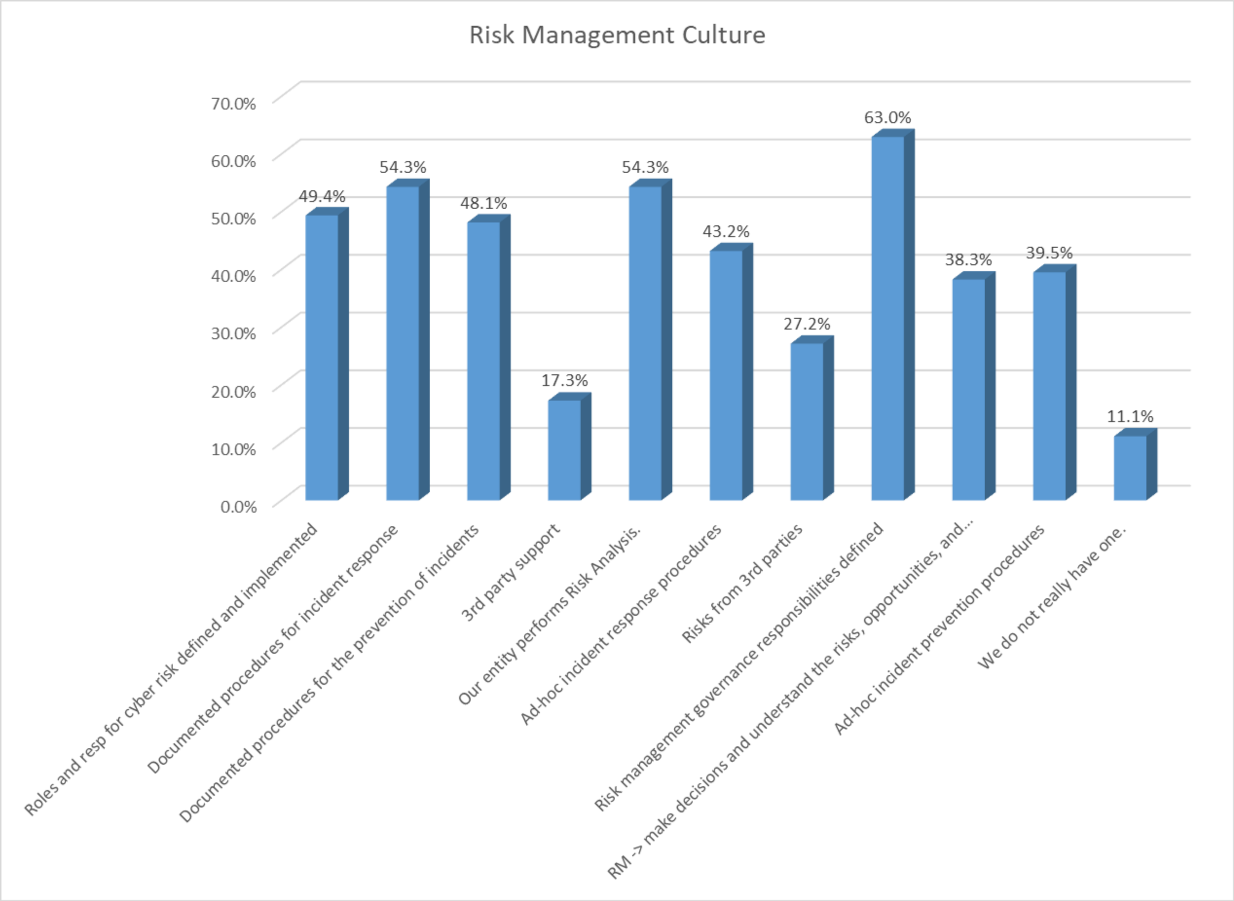


Figure 14 - Risk management culture

Even if both percentages are identical, it does not mean that the entities doing risk assessments also have incident response procedures in place. In total, only one third (33%) of the participants have both incident response procedures and risk assessment in place, whereas both of them are required to minimize both the risk of cyber-attack and its negative impact. **Table 6** shows that 21 % of participants have only incident response mechanisms in place and 21% of participants conduct only risk analysis.

Incident Response & Risk Analysis	Only Incident Response	Only Risk Analysis
33,3%	21,0%	21,0%

Table 6 - Security risk management culture

Considering again the data in the **Figure 14**, although the majority of the participants have risk management procedures in place, only 27,2% take the risks coming from 3rd party supply into account and 11,1% of the operators mention not really having a risk management culture.

In the survey, participants had to identify the different activities that are performed in their institution, in order to understand what parts of a risk assessment are considered and what kind of security measures are in place or ongoing. 79% of the institutions perform an inventory of the assets, 68% of the institutions have implemented business continuity plans or are otherwise implementing them.

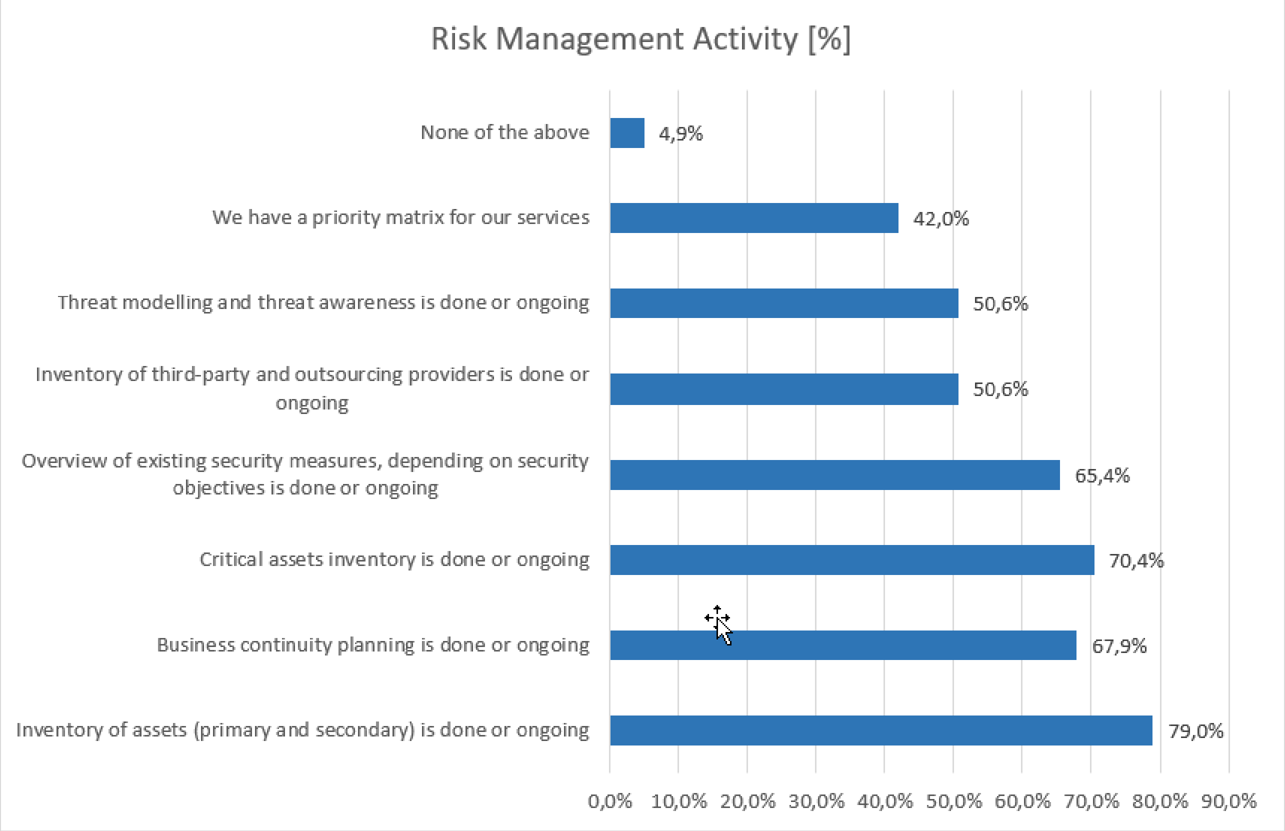


Figure 15 - Type of risk management activities

Besides knowing what activities are performed at the institution, the participants also had to identify the relevance of each task. The average outcome shows that overall, every task should be considered as important, but the most relevant task is considered to be the critical assets inventory (**Figure 16**)

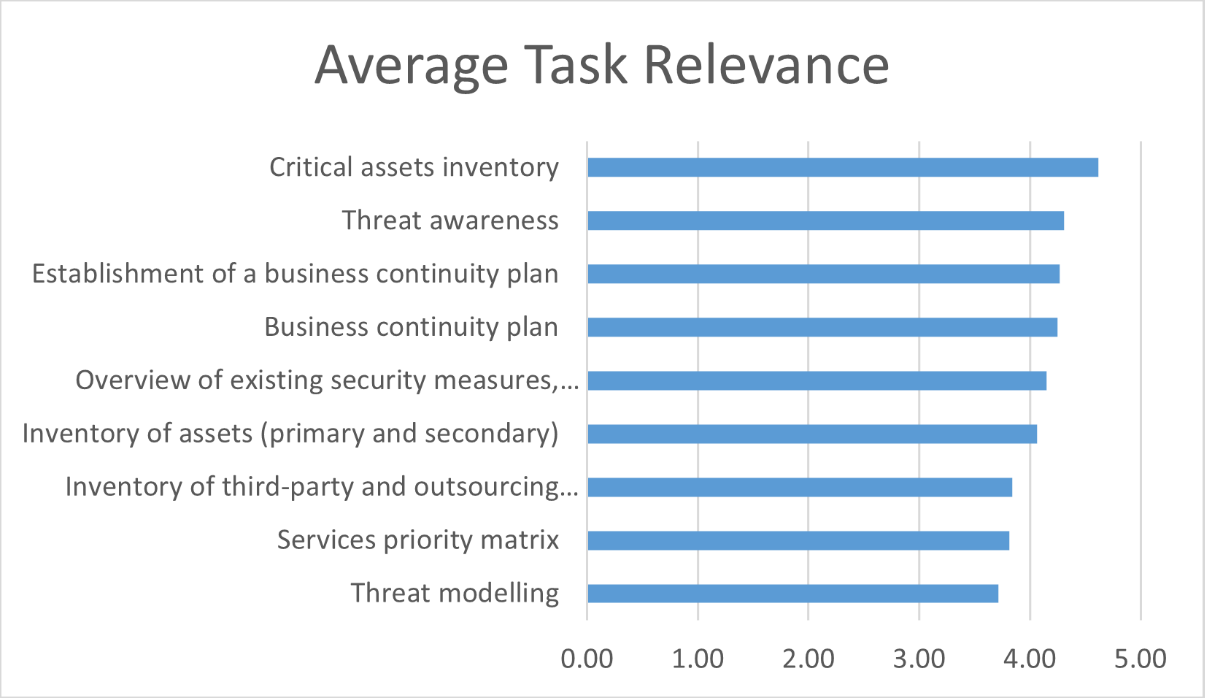


Figure 16 - Average Task Relevance (1 - irrelevant; 5 - most relevant)

7.2.2. Risk Assessment and Analysis

The participants were asked in the survey to identify the difficulties for carrying out a risk assessment (**Figure 17**). One can see that only 5% of the operators indicate not facing any difficulties with the risk assessment. This means that 95% of the operators face some difficulties with the risk assessment, namely in:

1. Identifying a methodology to be adopted;
2. Determining the scope of the analysis, i.e., which are the scenarios to be included (56% of the operators face difficulties determining the scope);
3. Evaluating the risks (44% of the operators indicate that they have difficulties in this evaluation);
4. Lack of information (44% of the operators) or the lack of knowledge in where to find the information;
5. Lack of practice of conducting a risk assessment.

Moreover, out of the 5% not facing any difficulties with the risk assessment, 75% indicate not performing a risk analysis.

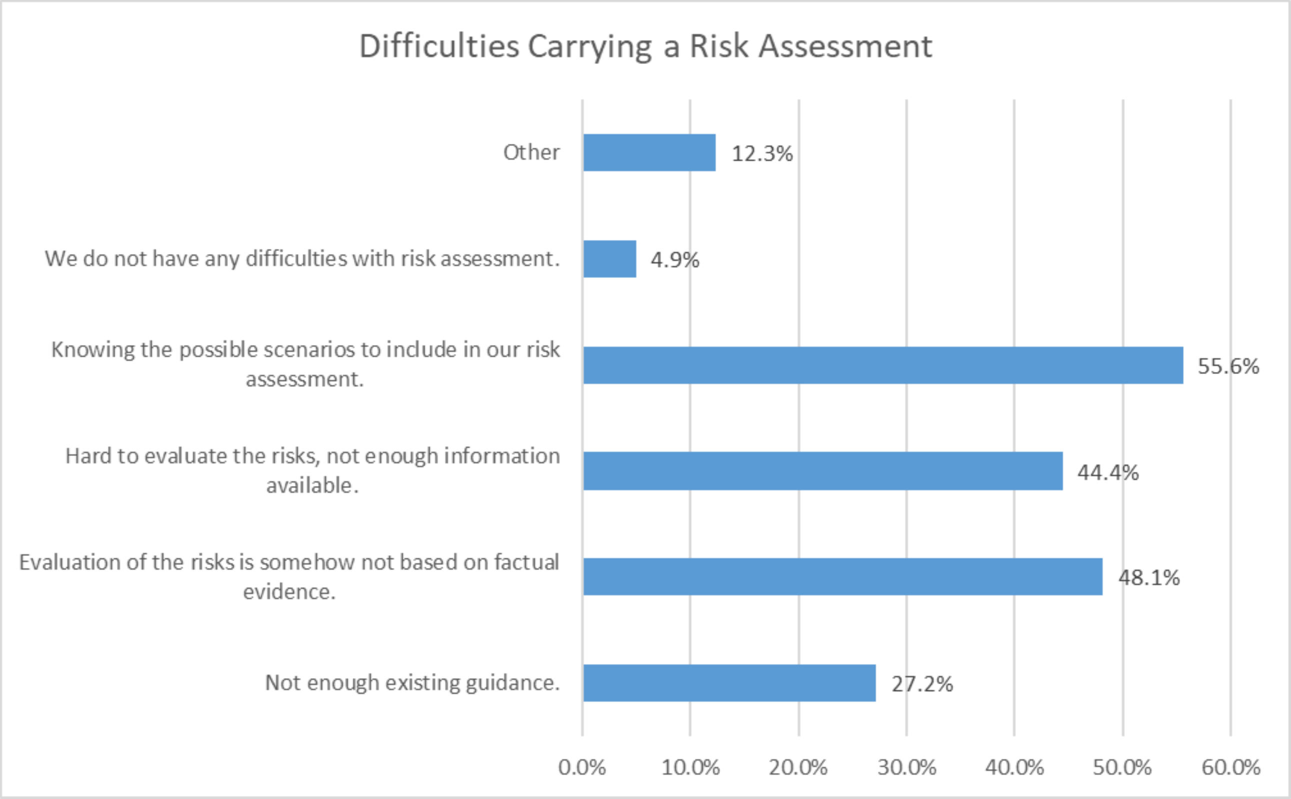


Figure 17 - Difficulties faced in view of performing a risk assessment

People having entered "other" in Figure 17, have listed the following difficulties (**Table 7**).

Our organization must do some preliminary work to inventory the information systems and classify them in terms of criticality. At the same time, it is necessary to inventory the assets that support the information systems and to correlate the assets with the information systems so that they can inherit the criticality classification, as well as to define the respective responsible persons. When this work is concluded we will be able to assess risks more assertively and effectively.
Access to system owners etc.
Lack of resources having the necessary skills to perform the specified functions (people & budget)
Getting the right people involved and understand the impact of certain risks. Risk ownership is difficult.
limited resources available for the evaluation
Outdated Infrastructure and systems. Currently in the process of implementing a new Integrated Health Information System.
Finance

Table 7 - Other difficulties faced during risk assessment

The best practice in terms of risk analysis frequency is to perform it regularly (at least yearly) and to update it after incidents or substantial structural or operational changes. This is the case for 22% of the operators (see **Figure 18**). Nevertheless almost 40% of the operators that perform a risk analysis, do it at least once a year. On the other side 46% of the operators have never performed a risk analysis.

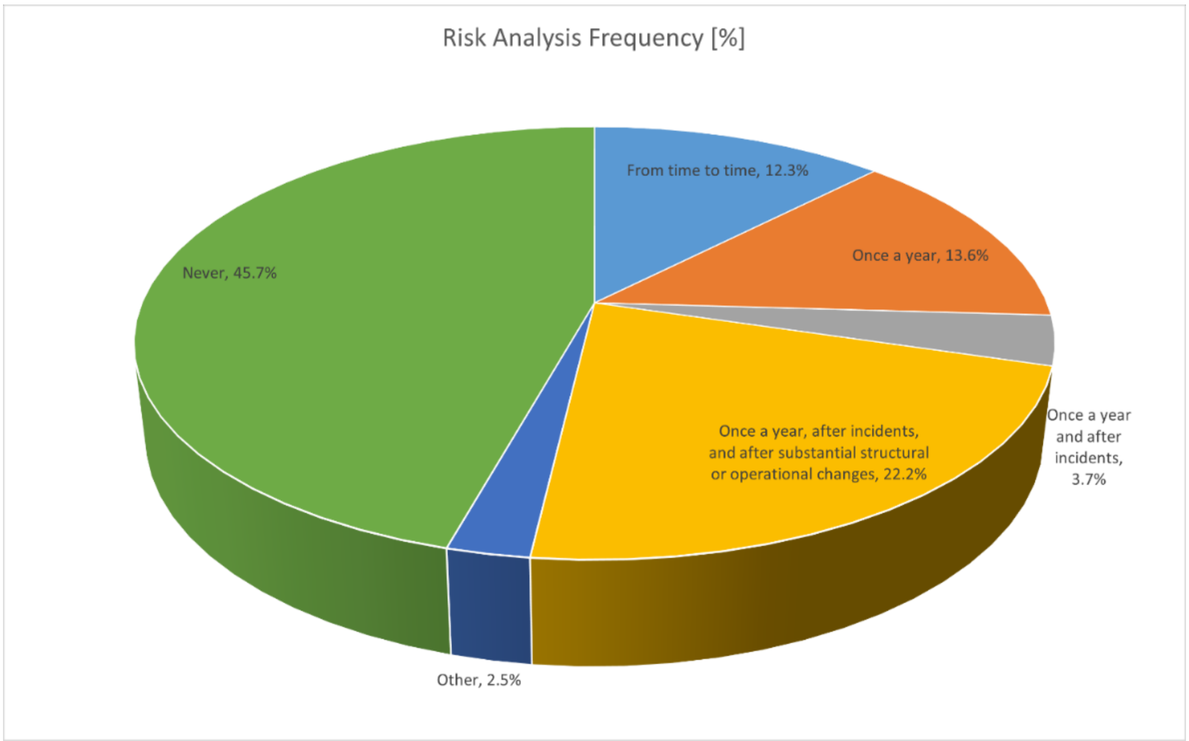


Figure 18 - Risk analysis frequency

In order to have a better understanding of the risk assessment process in the health sector, the participants were invited to identify the process, teams/people involved, tools and responsibilities. **Figure 19**shows that 45,7% of the institutions have internal processes defined and implemented, while 44,4% have roles and responsibilities for risk management defined. 32,1% make use of an international framework for conducting risk assessments and 27,2% are using a specific process other than an international framework.

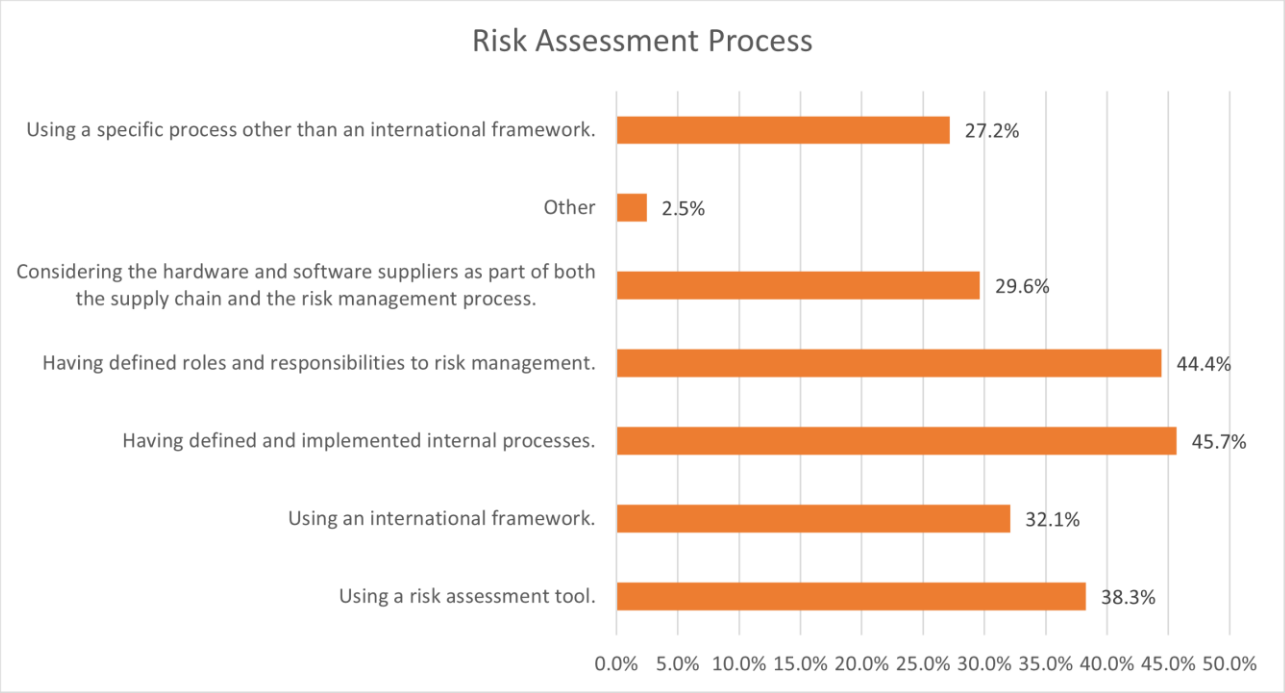


Figure 19 - Risk assessment process

With regard to the use of international frameworks (used by 32,1% of the respondents as Figure 19 shows) in relation to their risk assessment, the large majority of those operators applying an international framework make use of the ISO 2700X framework, followed by the ISO 31000 ERM Framework and the NIST ERM Framework (**Figure 2**0).

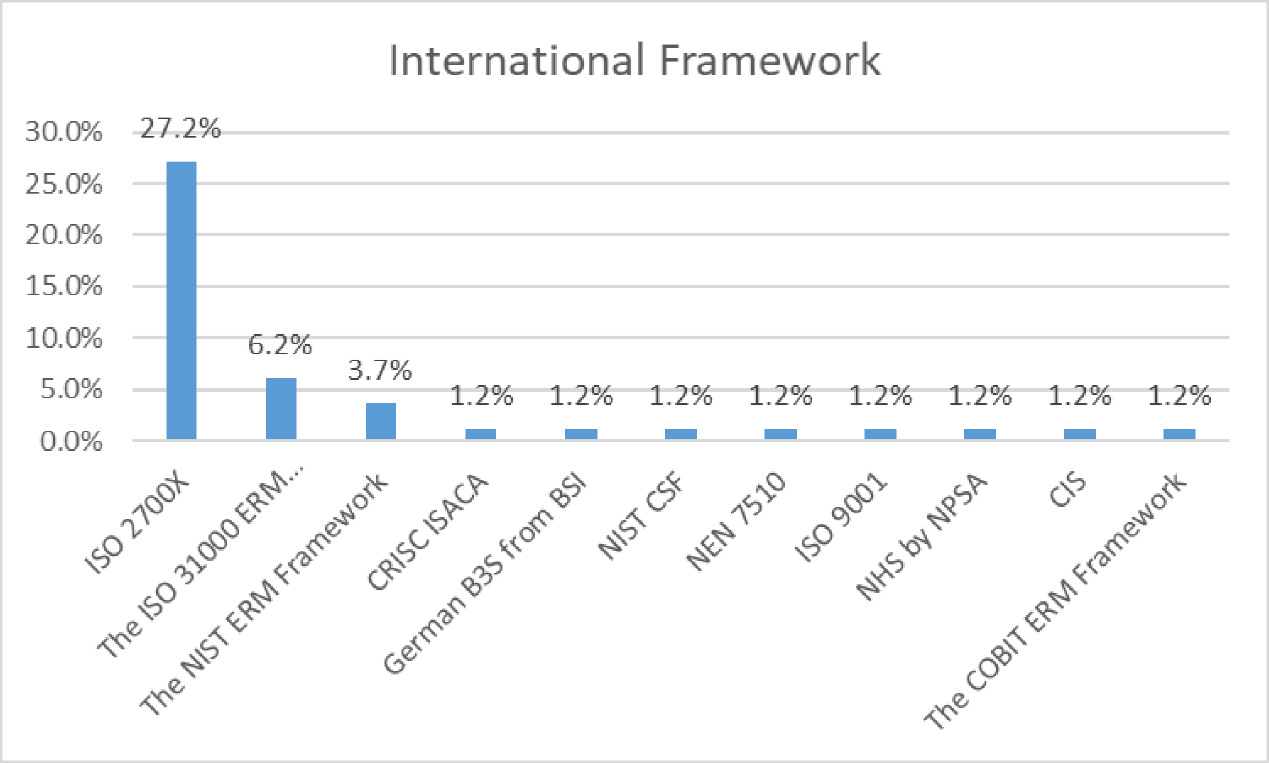


Figure 20 - International frameworks used during risk assessment process

7.2.3. Quality Control and Internal Audits

The health sector is one of the most controlled sectors, as the different kinds of examinations and practices need to be done following specific rules. These rules are mainly controlled via different types of quality controls (e.g., ISO 9001), which are out of scope of this document. However, the participants were asked whether their quality controls included information security or cybersecurity controls, with 45,7 % of participants (37 operators) indicating that this is the case.

Not only quality controls but also audits are quite common in health institutions. Therefore, participants were asked whether cyber risks are part of the audit assessment and reporting towards the board of the institution, which is the case for 56,8% of the participants (46 operators).

7.2.4. Health assets

Figure 21shows that 88% of the operators' state that data (e.g., patient data, financial and organisational data) is the most important health-specific asset. 70 % consider interconnected clinical information systems and 52% networking equipment (e.g., transmission media and network interfaces) as the most important assets. Only 4% of the participating operators consider identification systems (e.g., tags, bracelets, labels, smart badges, biometric scanners, RFID systems) as the most important health-specific asset.

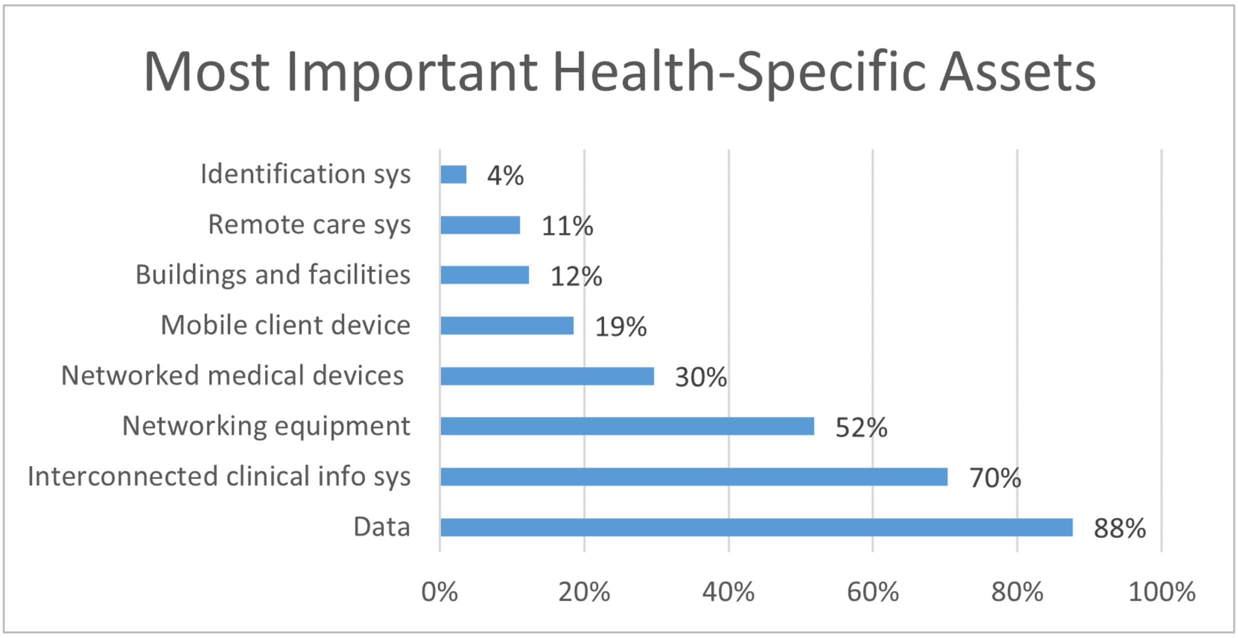


Figure 21 - Most important health specific assets

7.3. Threats and Types of incidents

In order to get an overview on the different kind of threats most common in the health sector, this section focuses on the threats and their importance level as well as the different types of incidents with relevant impact.

Table 8 shows the top 8 threats as perceived by the operators. The list of these threats was based on ETL 2021 (as ETL 2022 was not yet available at time of the survey preparation) and was answered by the participating institutions by rearranging the threats according to the relevant to their own organisation. As expected, ransomware is at the first position, because there were numerous ransomware attacks against hospitals in the last years, as referred in the previous chapters. The second position is occupied by e-mail related threats like for example phishing e-mails, which can be for instance used as a starting point for a ransomware attack.

Table 8 - Top 8 threats

Top 8	Threats
1	Ransomware
2	E-mail related threats
3	Malware
4	Threats against data
5	Threats against availability and integrity
6	Cryptojacking
7	Disinformation – misinformation
8	Non-malicious threats

Participants were also asked in the survey, to rank the type of threats towards cybersecurity that are most significant and relevant for their sector and organisation based on the ISO27005:2018

It is noted that at the time of completing the survey ISO 27005:20022 was not available. There are significant changes in how the standard's annex is presented in the new version. The new version provides specific guidance on techniques in support of the risk assessment process, via examples and the annex. Specifically for the threat examples, both the categories and the descriptions of threats have been significantly changed in the 2022 version. Some categories of threats have been merged while some new categories have been introduced (e.g., human actions, organisational threats) and several new threats have also been introduced (e.g., pandemic/epidemic, failure of supply chain).

Figure 22shows the outcome of the ranking, the type of threats that is ranked most of the time as number 1 (36 % of the operators) is compromise of information.

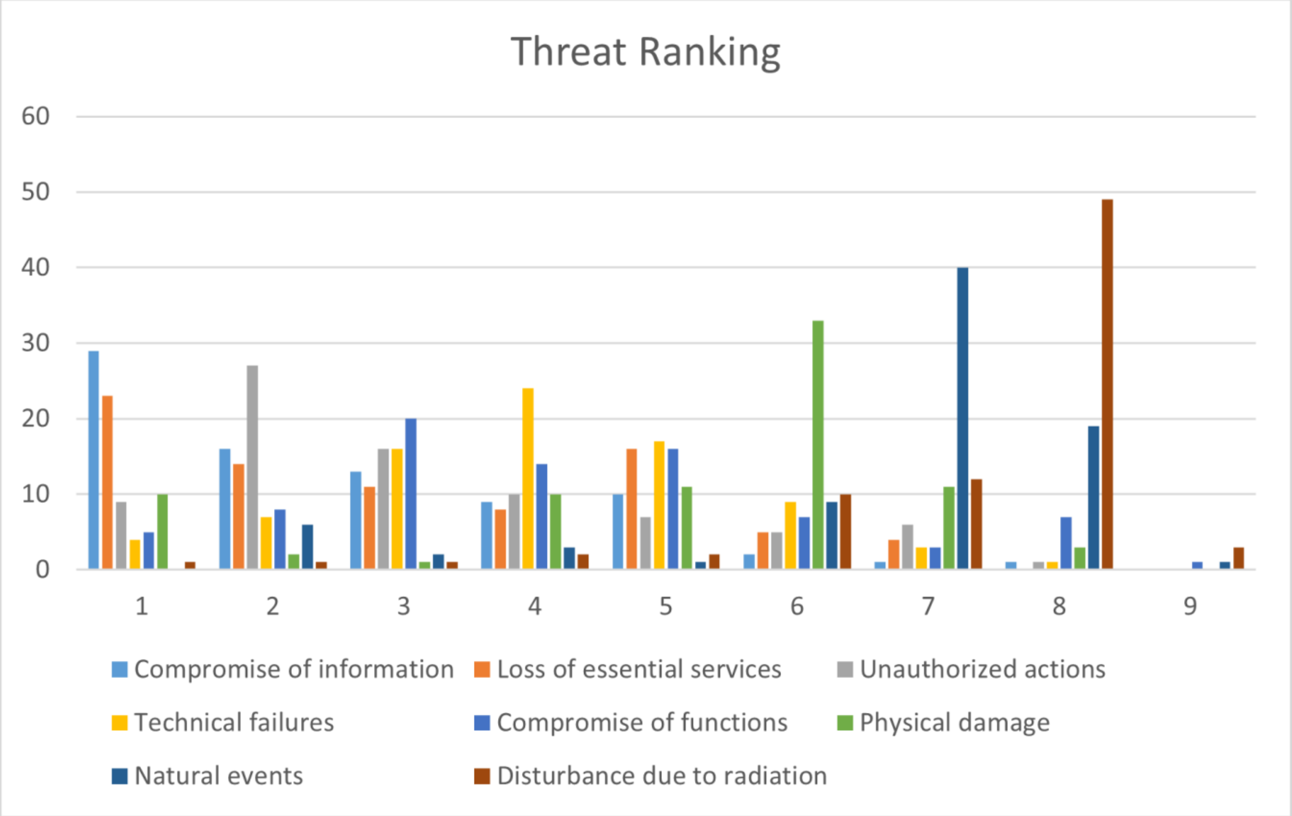


Figure 22 - significant and relevant type of threats ranking

This is in line with external threats (namely hacker/cracker) being the highest rated risk type as perceived by the participants (**Figure 23**). Nevertheless, not only external threats are considered to be of high risk, but also insider threats (due to poorly trained employees) have been ranked in the top tier by the participants of the survey.

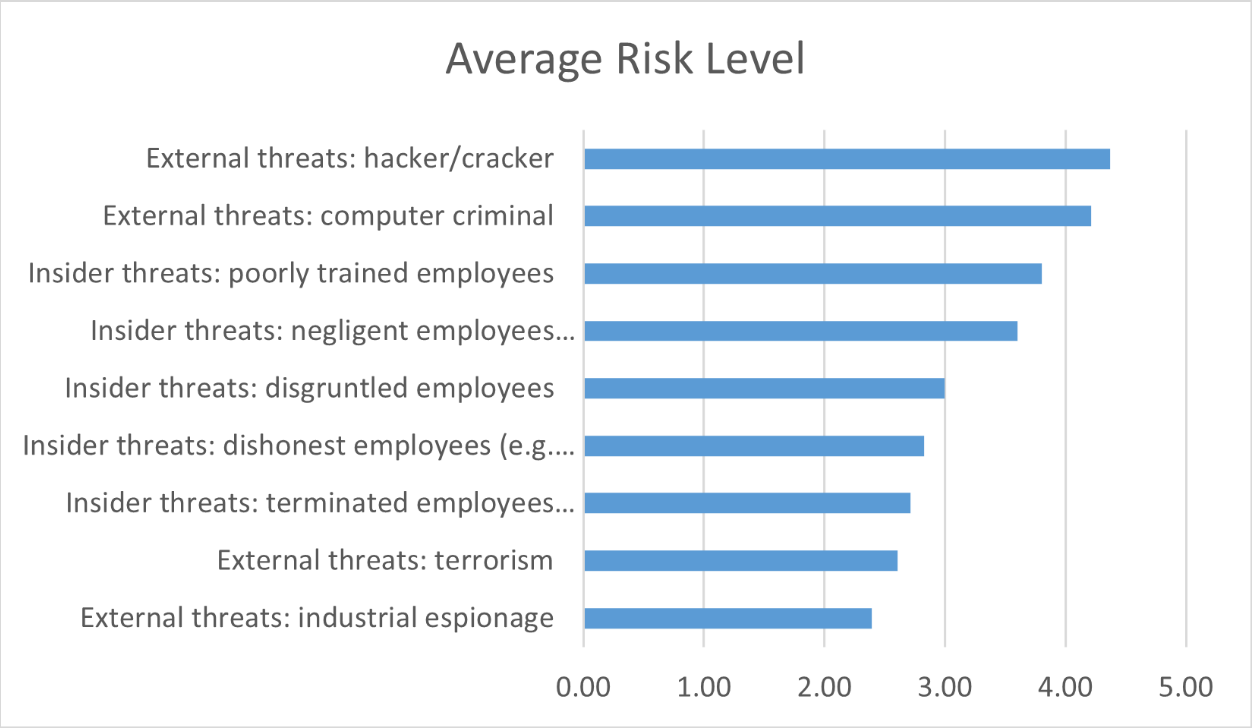


Figure 23 - Average rated risk level of threats (1 – not relevant; 5 – major threat)

The outcome of the most relevant type of threat being compromise of information and the highest ranked relevant cyber-attack being ransomware in the previous figures, is in line with the outcome of the question related to the most important health-specific asset, as described in Section 7.2.

This also explains why incidents targeting the availability of the operators' systems and consequently the availability of their data are the most reported incidents and those with the highest impact during the last 2 years (**Figure 24**).

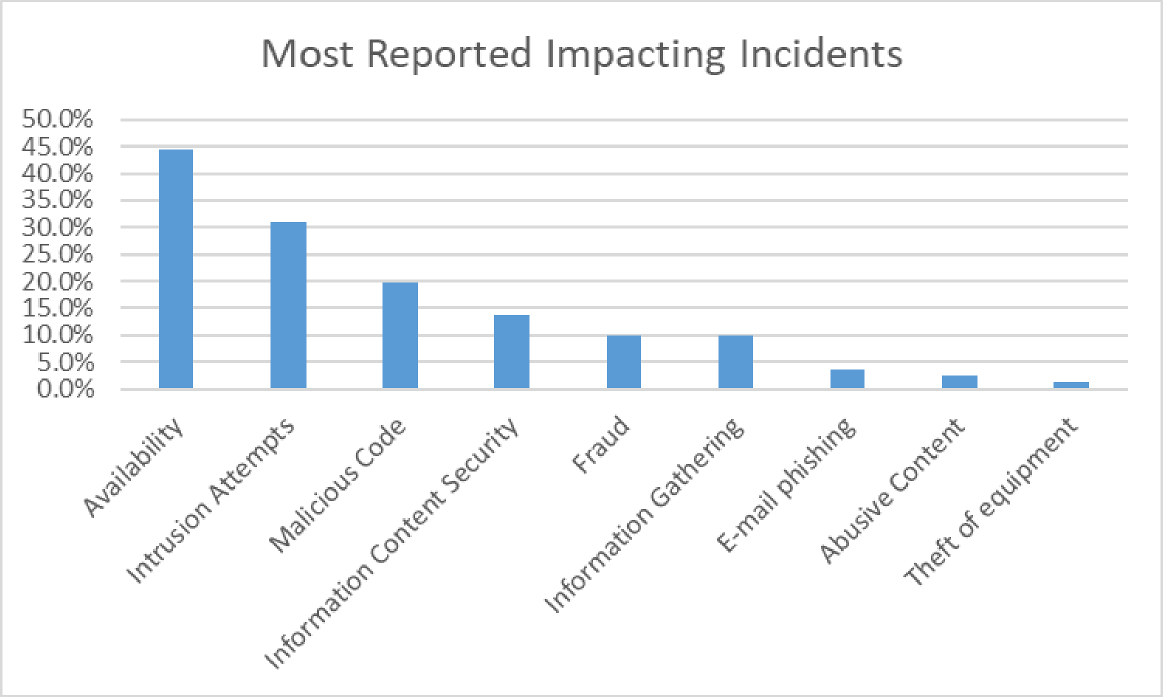


Figure 24 - Most reported impacting incidents

7.4. Certification, Barriers and Guidance

Some final questions were related to the usage of certification for information security / cybersecurity. Among the 81 participants, 18 have certification in place. Of these 18, 14 participants have the ISO/IEC 27001 certification in place (**Figure 25**).

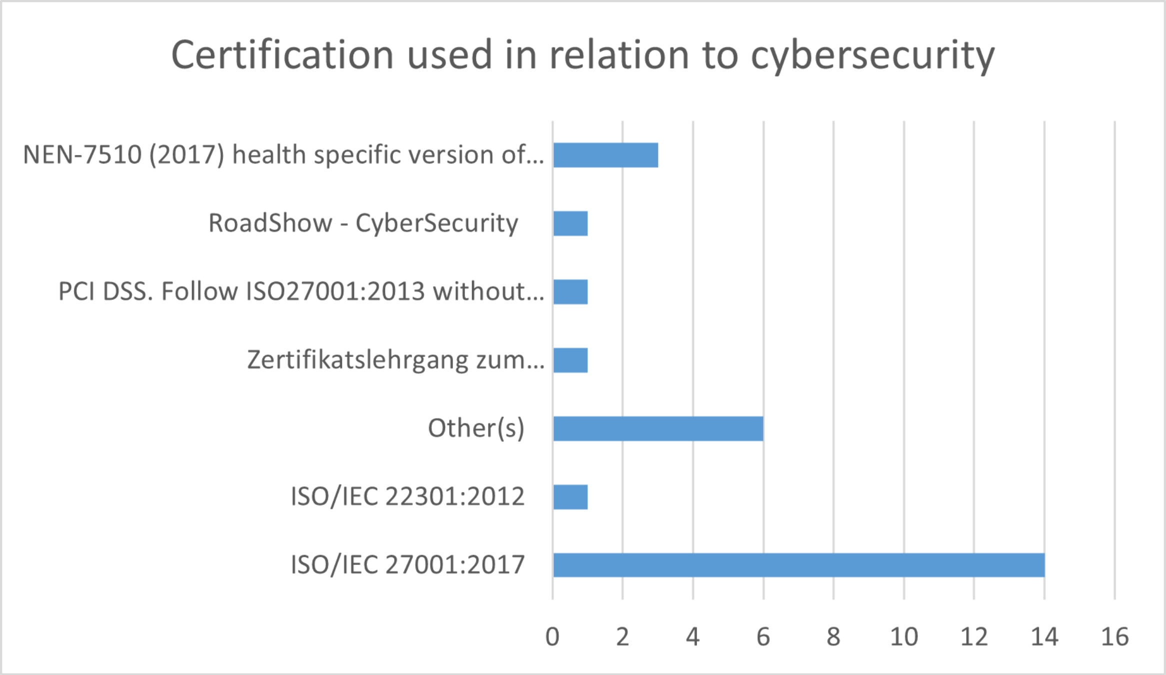


Figure 25 - Certification used in relation with cybersecurity

The participants had the possibility to indicate which barriers they encounter while improving the entity's cybersecurity posture.

The classification of the barriers against cybersecurity (**Figure 26**) was consistent between the operators. For most of them budget, time and skills appear to be missing.

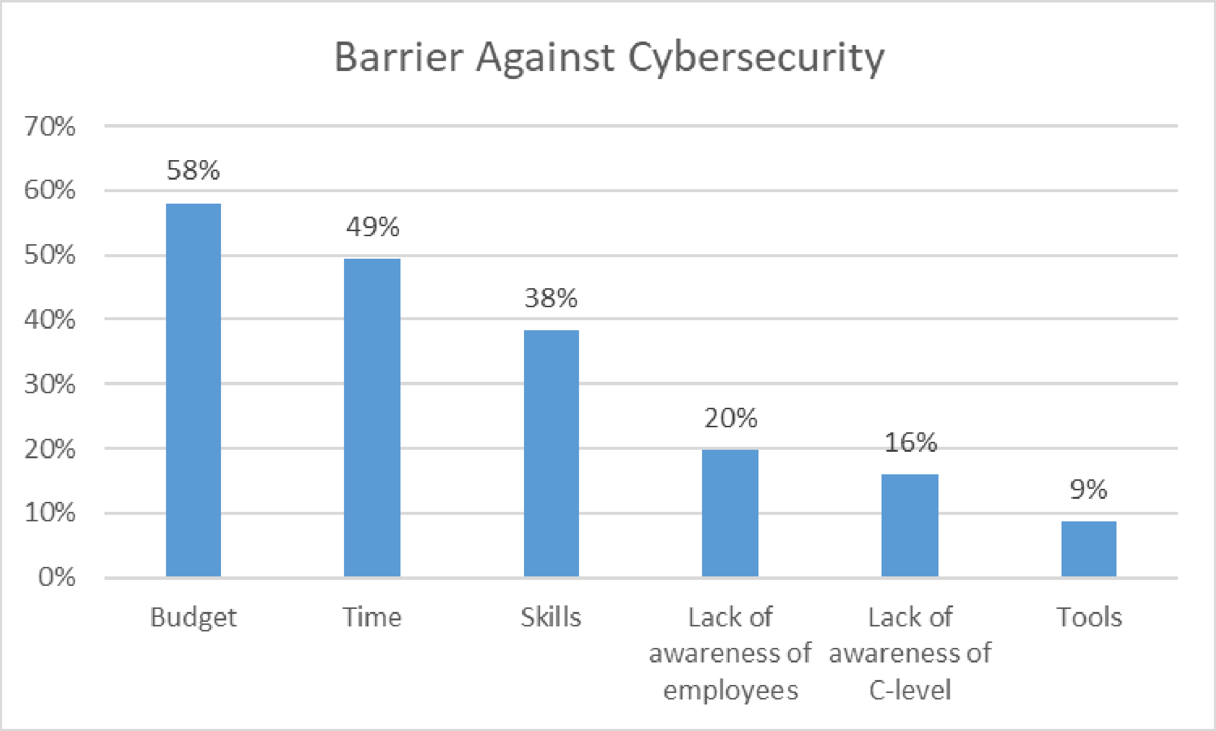


Figure 26 - Barriers against cybersecurity

Apart from the barriers, the participants were also asked to identify whether they receive guidance concerning technical or organisational measures on cybersecurity. A large number of institutions indicate to receive guidance: from national authorities (59%), from CSIRT (49%) and from ENISA (47%) (**Figure 27**). However, 5% indicate not receiving any guidance.

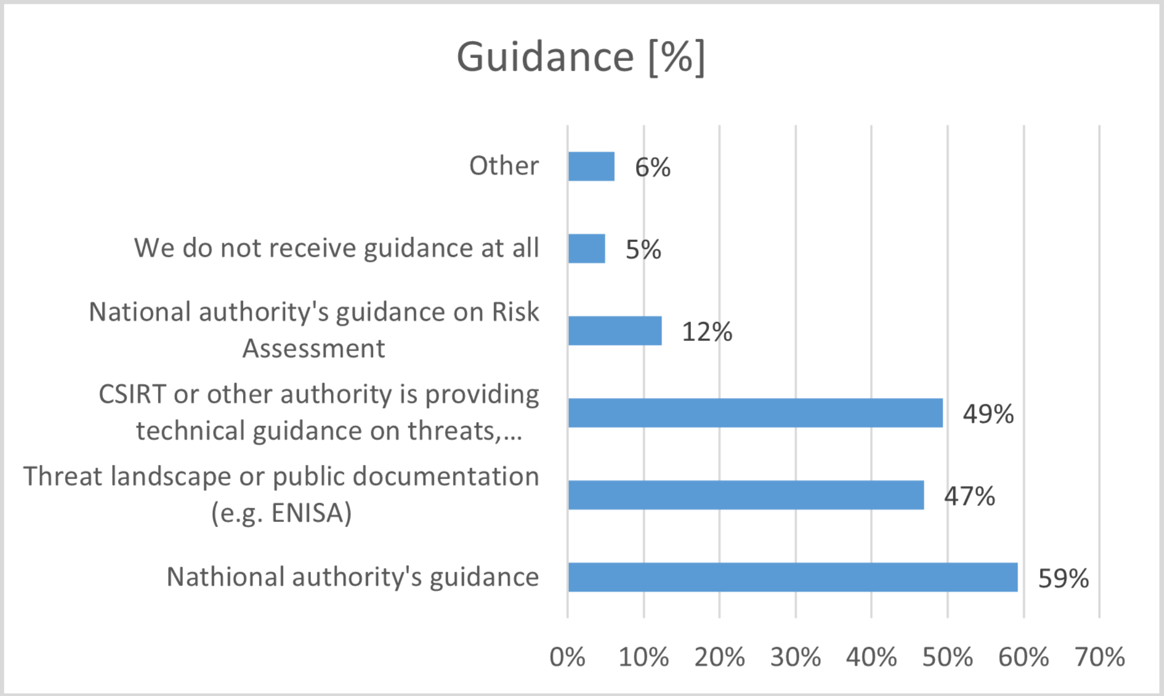


Figure 27 - Receiving guidance

The outcome of the survey shows that there is room for improvement when it comes to having specific cybersecurity measures in place, especially on the preventive side, namely risk assessments. Combining this information with knowing that not every institution already received guidance, also puts the national authorities in responsibility to help their organisations for creating a mature cyber posture.

7.5. Key takeaways

Risk management responsibilities and incident response procedures seem to be defined for the majority of the organisations, but only 33% of them have both in place. Some of the measures that are implemented by the majority of respondents in an effort to manage risks, relate to asset inventory and business continuity plans.

Data was identified as the most important health-specific asset by the majority of the respondents (88%). Additionally, the majority of respondents (27%) utilise ISO2700x family of standards to carry out their risk assessments. Risk assessment and analysis comes with challenges though; this was confirmed by 95% of the respondents. Knowing the scenarios to include in the risk analysis was the top challenge identified by the organisations.

Furthermore, 46% of the organisations indicated that they have never performed a risk analysis, while 56% of them indicated that cyber risks are in the scope of their audits which are reported to the board.

The cybersecurity threats identified by ENISA Threat Landscape 2021 were ranked in priority by the survey respondents: first was ransomware, followed by email related threats and malware. A similar ranking based on ISO 27005:2018, indicated that the most relevant threat is compromise of information and the top risk is for external threats (hacker/cracker). This information is in line with data being identified as the most important health-specific asset and availability being reported as the highest impact of incidents during the past 2 years.

Finally, it seems that budget, time and skills are the most important shortcomings when it comes to cybersecurity. Overall, the results indicate that there is room for improvement for cybersecurity maturity in the surveyed organisations.

8. General Conclusions

- Throughout the different chapters, some key takeaways were introduced by way of conclusion on the topics covered. Using a cyber threat taxonomy (e.g., threat groups, actors, impact, motivation) provides a structured and consistent approach to understanding, managing and responding to cyber threats. It also serves as input to the information security risk management activities and incident response planning.

- There's a rising trend of cybersecurity incidents with significant impact over the past few years. The health sector seems to be the most impacted NIS sector since 2020, with the majority of incidents involving system failures. Also, the correlation of cybersecurity and patient safety does not seem to be adequately evaluated in healthcare organisations.

- At the time this document was drafted, the prominent threats were ransomware, threats against data, DDoS attacks, threats posed by third parties, malware and social engineering as phishing. The most commonly identified vulnerabilities were insiders and the use of legacy systems. Ransomware and DDoS attacks increasingly target healthcare organisations, disrupting daily operations, healthcare provision and in turn impacting patient safety.

- Risks arising from such threats could be mitigated by the implementation of appropriate measures. E.g., incident response plans, backup procedures, third-party risk management, awareness raising, etc. This would help to ensure an organisation's resilience to cybersecurity incidents and business continuity.

- Currently, risk management responsibilities and incident response procedures seem to be defined by the majority of the organisations in the EU - while not both are in place most of the times. Some of the implemented risk mitigation measures related to asset inventory and business continuity plans. Also, many organisations have never performed a cyber risk analysis.

- Data was identified as the most important health-specific asset and the impact on availability was reported as the highest for incidents during the past 2 years.

- Budget, time and skills are the most important shortcomings when it comes to cybersecurity in healthcare.

9. Additional ENISA Relevant Materials

ENISA Threat Landscape for Supply Chain Attacks, July 2021
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ENISA Threat Landscape 2021, October 2021
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA, Risk Management Standards, March 2022
https://www.enisa.europa.eu/publications/risk-management-standards

ENISA Threat Landscape Methodology, July 2022
https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

ENISA Threat Landscape for Ransomware Attacks, July 2022
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

ENISA Threat Landscape 2021, November 2022
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

ENISA, NIS Investments 2022, November 2022
https://www.enisa.europa.eu/publications/nis-investments-2022

ENISA, Cyber Europe 2022: After action report, December 2022
https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report

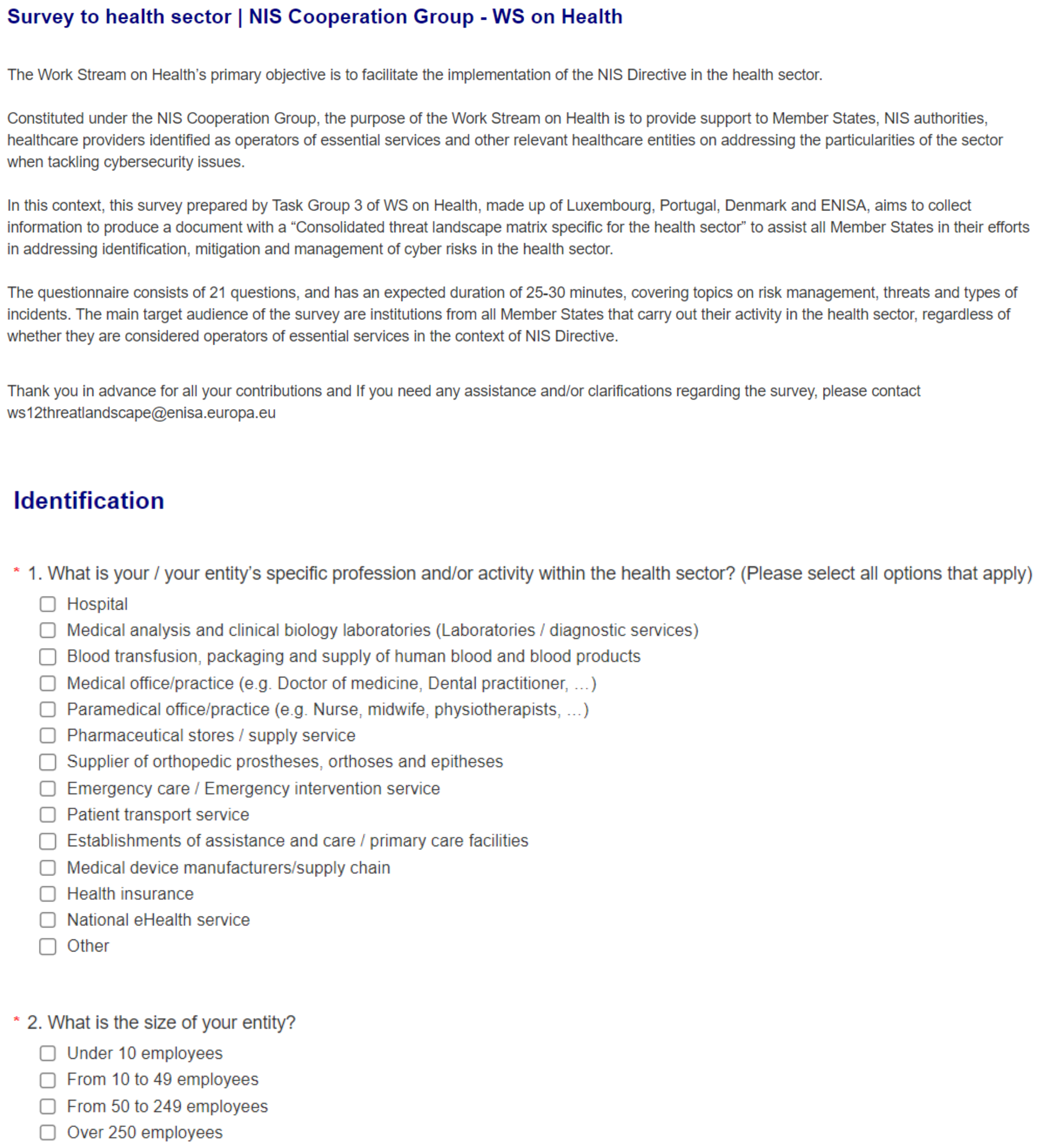
ENISA, Interoperable EU Risk Management Framework, January 2023
https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

ENISA, Compendium of Risk Management Frameworks with Potential Interoperability, January 2023
https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks

ENISA Threat Landscape for the Health sector, July 2023

https://www.enisa.europa.eu/publications/health-threat-landscape

10. Annex



Survey to health sector | NIS Cooperation Group - WS on Health

The Work Stream on Health's primary objective is to facilitate the implementation of the NIS Directive in the health sector.

Constituted under the NIS Cooperation Group, the purpose of the Work Stream on Health is to provide support to Member States, NIS authorities, healthcare providers identified as operators of essential services and other relevant healthcare entities on addressing the particularities of the sector when tackling cybersecurity issues.

In this context, this survey prepared by Task Group 3 of WS on Health, made up of Luxembourg, Portugal, Denmark and ENISA, aims to collect information to produce a document with a "Consolidated threat landscape matrix specific for the health sector" to assist all Member States in their efforts in addressing identification, mitigation and management of cyber risks in the health sector.

The questionnaire consists of 21 questions, and has an expected duration of 25-30 minutes, covering topics on risk management, threats and types of incidents. The main target audience of the survey are institutions from all Member States that carry out their activity in the health sector, regardless of whether they are considered operators of essential services in the context of NIS Directive.

Thank you in advance for all your contributions and If you need any assistance and/or clarifications regarding the survey, please contact ws12threatlandscape@enisa.europa.eu

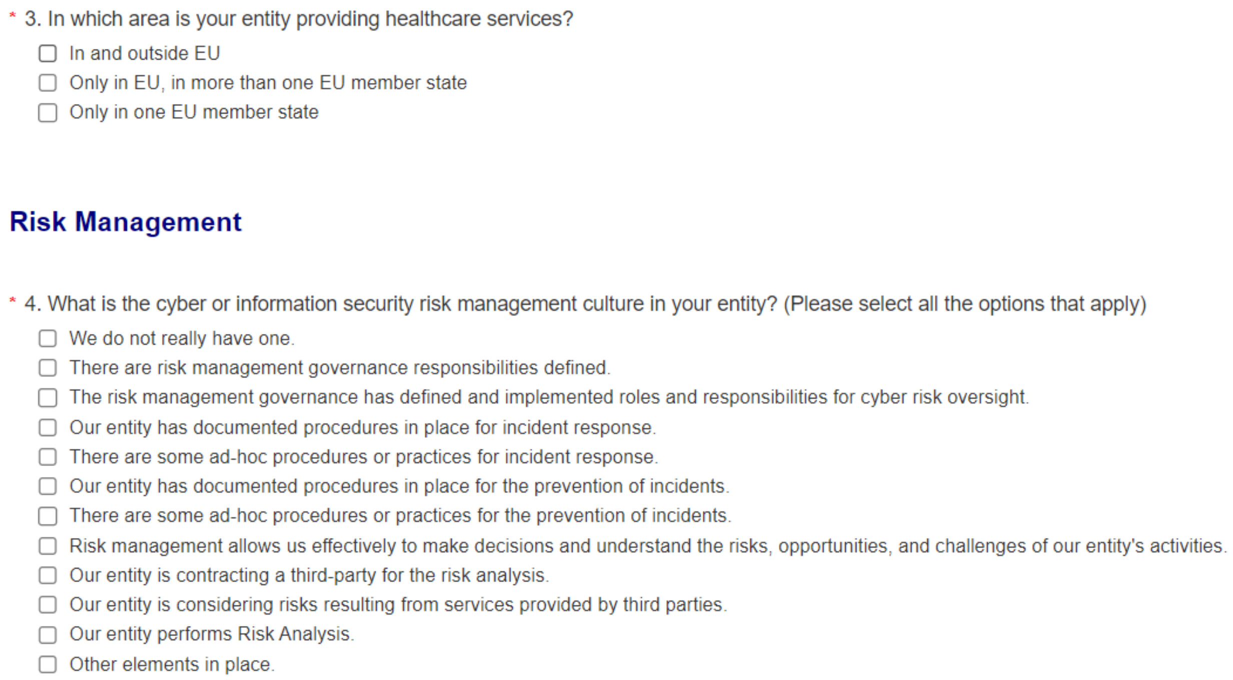
Identification

* 1. What is your / your entity's specific profession and/or activity within the health sector? (Please select all options that apply)

□ Hospital
□ Medical analysis and clinical biology laboratories (Laboratories / diagnostic services)
□ Blood transfusion, packaging and supply of human blood and blood products
□ Medical office/practice (e.g. Doctor of medicine, Dental practitioner, …)
□ Paramedical office/practice (e.g. Nurse, midwife, physiotherapists, …)
□ Pharmaceutical stores / supply service
□ Supplier of orthopedic prostheses, orthoses and epitheses
□ Emergency care / Emergency intervention service
□ Patient transport service
□ Establishments of assistance and care / primary care facilities
□ Medical device manufacturers/supply chain
□ Health insurance
□ National eHealth service
□ Other

* 2. What is the size of your entity?

□ Under 10 employees
□ From 10 to 49 employees
□ From 50 to 249 employees
□ Over 250 employees



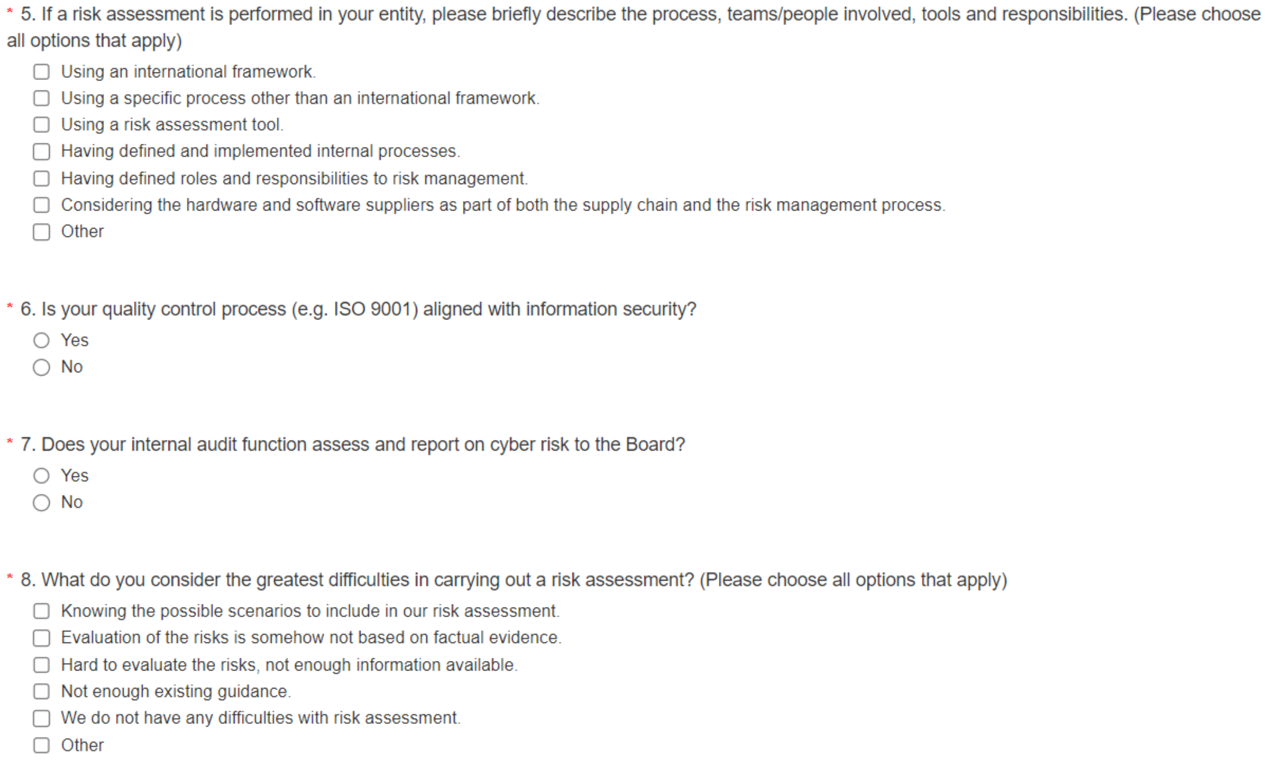
* 3. In which area is your entity providing healthcare services?

□ In and outside EU
□ Only in EU, in more than one EU member state
□ Only in one EU member state

Risk Management

* 4. What is the cyber or information security risk management culture in your entity? (Please select all the options that apply)

□ We do not really have one.
□ There are risk management governance responsibilities defined.
□ The risk management governance has defined and implemented roles and responsibilities for cyber risk oversight.
□ Our entity has documented procedures in place for incident response.
□ There are some ad-hoc procedures or practices for incident response.
□ Our entity has documented procedures in place for the prevention of incidents.
□ There are some ad-hoc procedures or practices for the prevention of incidents.
□ Risk management allows us effectively to make decisions and understand the risks, opportunities, and challenges of our entity's activities.
□ Our entity is contracting a third-party for the risk analysis.
□ Our entity is considering risks resulting from services provided by third parties.
□ Our entity performs Risk Analysis.
□ Other elements in place.



* 5. If a risk assessment is performed in your entity, please briefly describe the process, teams/people involved, tools and responsibilities. (Please choose all options that apply)

□ Using an international framework.
□ Using a specific process other than an international framework.
□ Using a risk assessment tool.
□ Having defined and implemented internal processes.
□ Having defined roles and responsibilities to risk management.
□ Considering the hardware and software suppliers as part of both the supply chain and the risk management process.
□ Other

* 6. Is your quality control process (e.g. ISO 9001) aligned with information security?

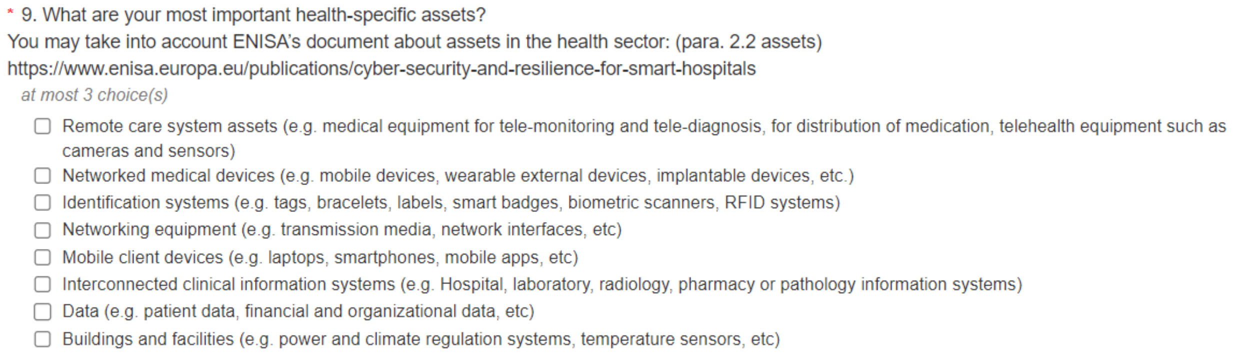
○ Yes
○ No

* 7. Does your internal audit function assess and report on cyber risk to the Board?

○ Yes
○ No

* 8. What do you consider the greatest difficulties in carrying out a risk assessment? (Please choose all options that apply)

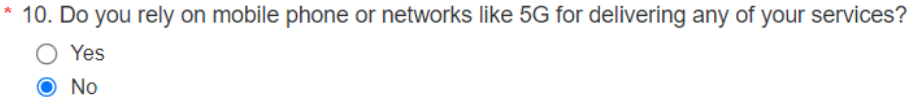
□ Knowing the possible scenarios to include in our risk assessment.
□ Evaluation of the risks is somehow not based on factual evidence.
□ Hard to evaluate the risks, not enough information available.
□ Not enough existing guidance.
□ We do not have any difficulties with risk assessment.
□ Other



* 9. What are your most important health-specific assets?
You may take into account ENISA's document about assets in the health sector: (para. 2.2 assets)
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

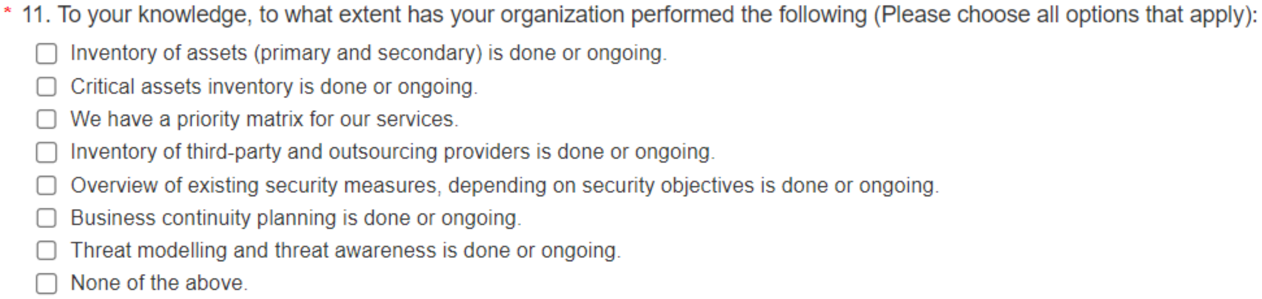
at most 3 choice(s)

□ Remote care system assets (e.g. medical equipment for tele-monitoring and tele-diagnosis, for distribution of medication, telehealth equipment such as cameras and sensors)
□ Networked medical devices (e.g. mobile devices, wearable external devices, implantable devices, etc.)
□ Identification systems (e.g. tags, bracelets, labels, smart badges, biometric scanners, RFID systems)
□ Networking equipment (e.g. transmission media, network interfaces, etc)
□ Mobile client devices (e.g. laptops, smartphones, mobile apps, etc)
□ Interconnected clinical information systems (e.g. Hospital, laboratory, radiology, pharmacy or pathology information systems)
□ Data (e.g. patient data, financial and organizational data, etc)
□ Buildings and facilities (e.g. power and climate regulation systems, temperature sensors, etc)



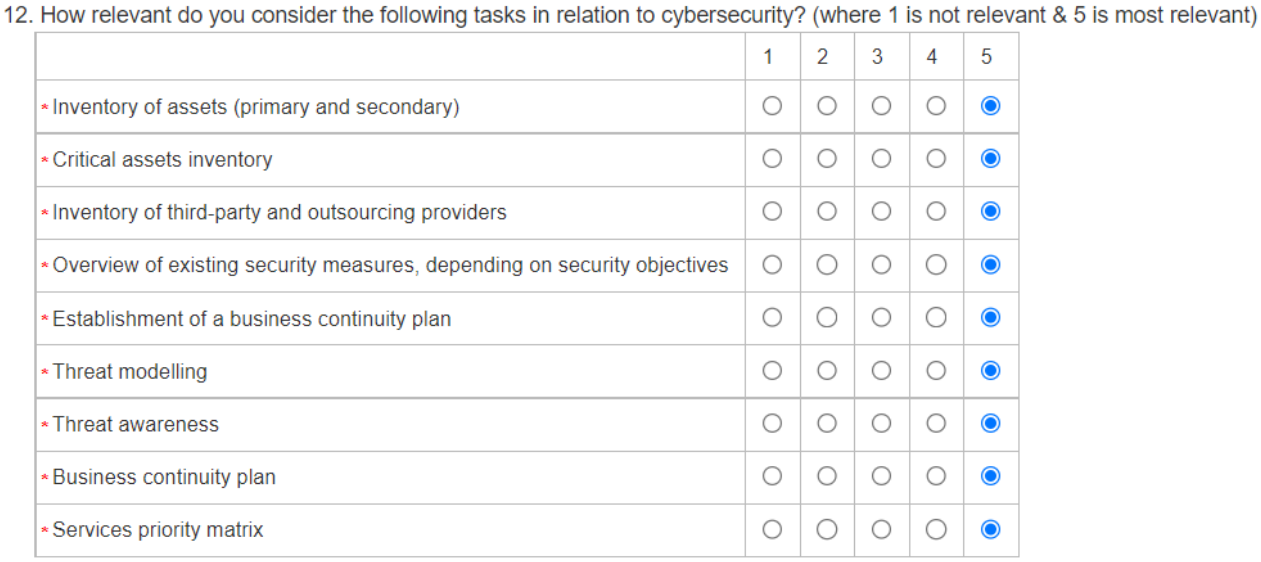
* 10. Do you rely on mobile phone or networks like 5G for delivering any of your services?

○ Yes
● No



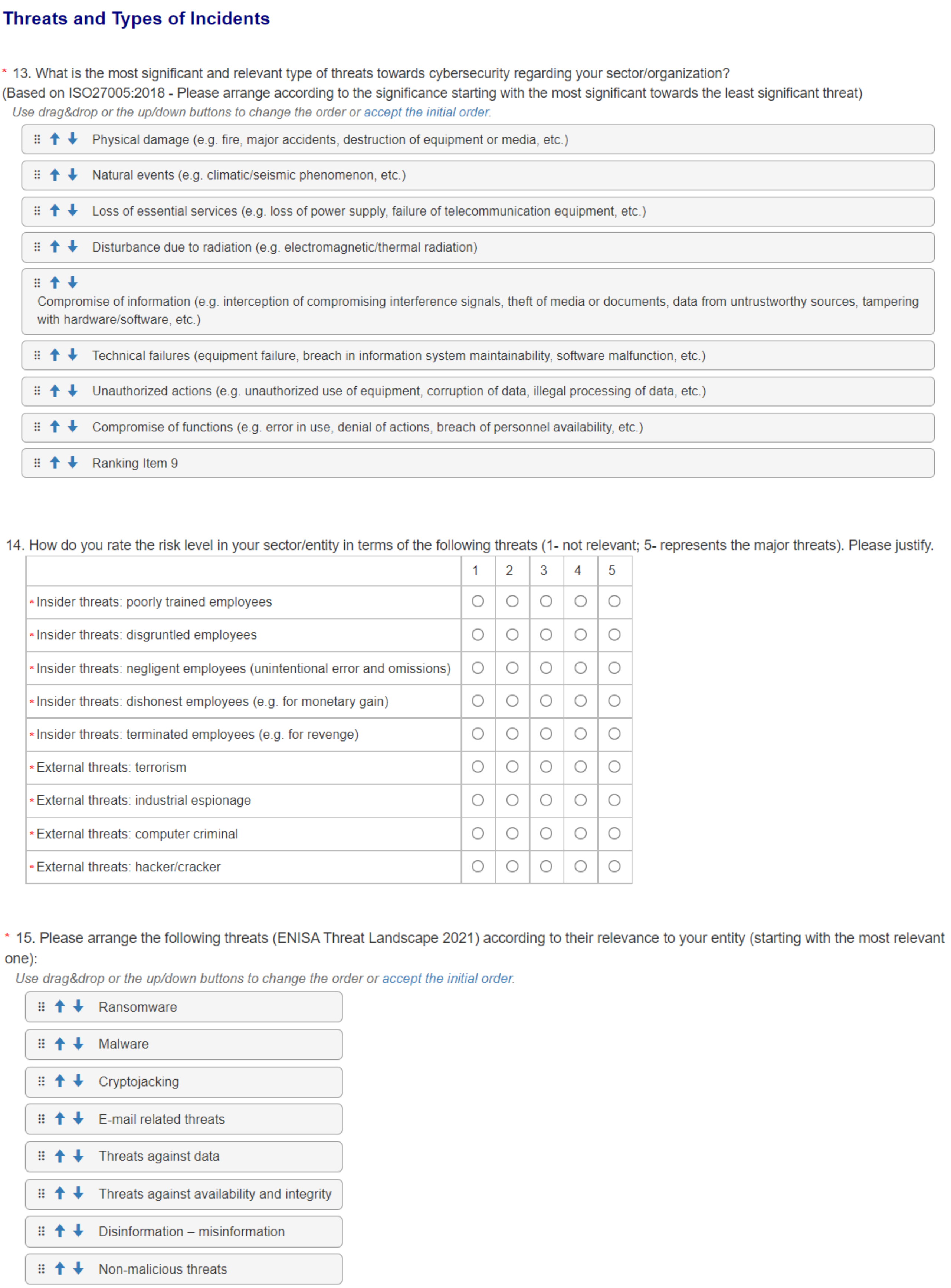
* 11. To your knowledge, to what extent has your organization performed the following (Please choose all options that apply):

□ Inventory of assets (primary and secondary) is done or ongoing.
□ Critical assets inventory is done or ongoing.
□ We have a priority matrix for our services.
□ Inventory of third-party and outsourcing providers is done or ongoing.
□ Overview of existing security measures, depending on security objectives is done or ongoing.
□ Business continuity planning is done or ongoing.
□ Threat modelling and threat awareness is done or ongoing.
□ None of the above.



12. How relevant do you consider the following tasks in relation to cybersecurity? (where 1 is not relevant & 5 is most relevant)

	1	2	3	4	5
* Inventory of assets (primary and secondary)	○	○	○	○	●
* Critical assets inventory	○	○	○	○	●
* Inventory of third-party and outsourcing providers	○	○	○	○	●
* Overview of existing security measures, depending on security objectives	○	○	○	○	●
* Establishment of a business continuity plan	○	○	○	○	●
* Threat modelling	○	○	○	○	●
* Threat awareness	○	○	○	○	●
* Business continuity plan	○	○	○	○	●
* Services priority matrix	○	○	○	○	●



Threats and Types of Incidents

* 13. What is the most significant and relevant type of threats towards cybersecurity regarding your sector/organization?
(Based on ISO27005:2018 - Please arrange according to the significance starting with the most significant towards the least significant threat)

Use drag&drop or the up/down buttons to change the order or accept the initial order.

- Physical damage (e.g. fire, major accidents, destruction of equipment or media, etc.)
- Natural events (e.g. climatic/seismic phenomenon, etc.)
- Loss of essential services (e.g. loss of power supply, failure of telecommunication equipment, etc.)
- Disturbance due to radiation (e.g. electromagnetic/thermal radiation)
- Compromise of information (e.g. interception of compromising interference signals, theft of media or documents, data from untrustworthy sources, tampering with hardware/software, etc.)
- Technical failures (equipment failure, breach in information system maintainability, software malfunction, etc.)
- Unauthorized actions (e.g. unauthorized use of equipment, corruption of data, illegal processing of data, etc.)
- Compromise of functions (e.g. error in use, denial of actions, breach of personnel availability, etc.)
- Ranking Item 9

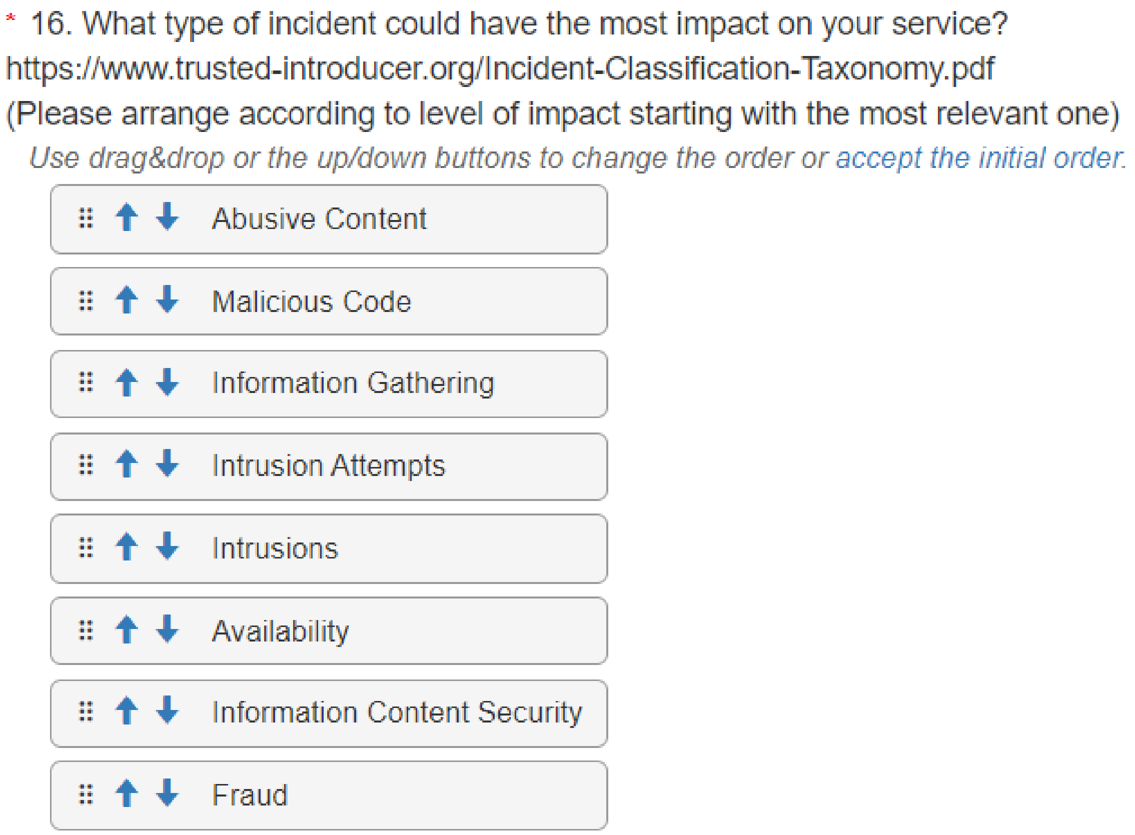
14. How do you rate the risk level in your sector/entity in terms of the following threats (1- not relevant; 5- represents the major threats). Please justify.

	1	2	3	4	5
* Insider threats: poorly trained employees	○	○	○	○	○
* Insider threats: disgruntled employees	○	○	○	○	○
* Insider threats: negligent employees (unintentional error and omissions)	○	○	○	○	○
* Insider threats: dishonest employees (e.g. for monetary gain)	○	○	○	○	○
* Insider threats: terminated employees (e.g. for revenge)	○	○	○	○	○
* External threats: terrorism	○	○	○	○	○
* External threats: industrial espionage	○	○	○	○	○
* External threats: computer criminal	○	○	○	○	○
* External threats: hacker/cracker	○	○	○	○	○

* 15. Please arrange the following threats (ENISA Threat Landscape 2021) according to their relevance to your entity (starting with the most relevant one):

Use drag&drop or the up/down buttons to change the order or accept the initial order.

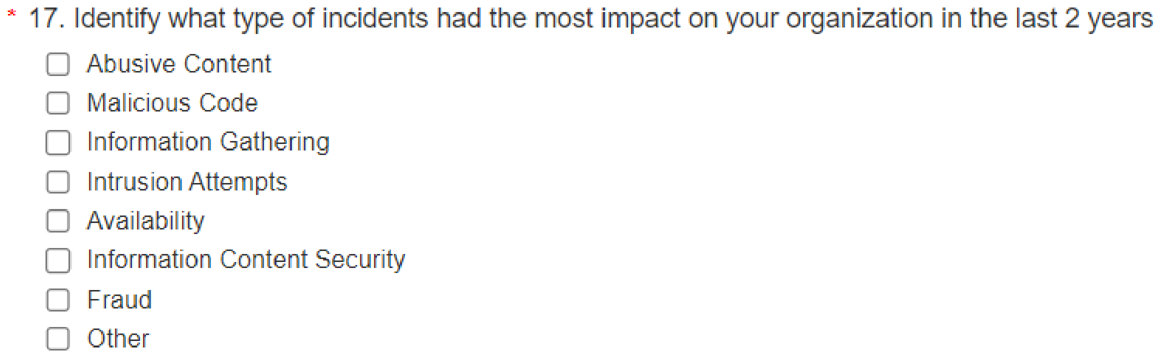
- Ransomware
- Malware
- Cryptojacking
- E-mail related threats
- Threats against data
- Threats against availability and integrity
- Disinformation – misinformation
- Non-malicious threats



* 16. What type of incident could have the most impact on your service? https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (Please arrange according to level of impact starting with the most relevant one)

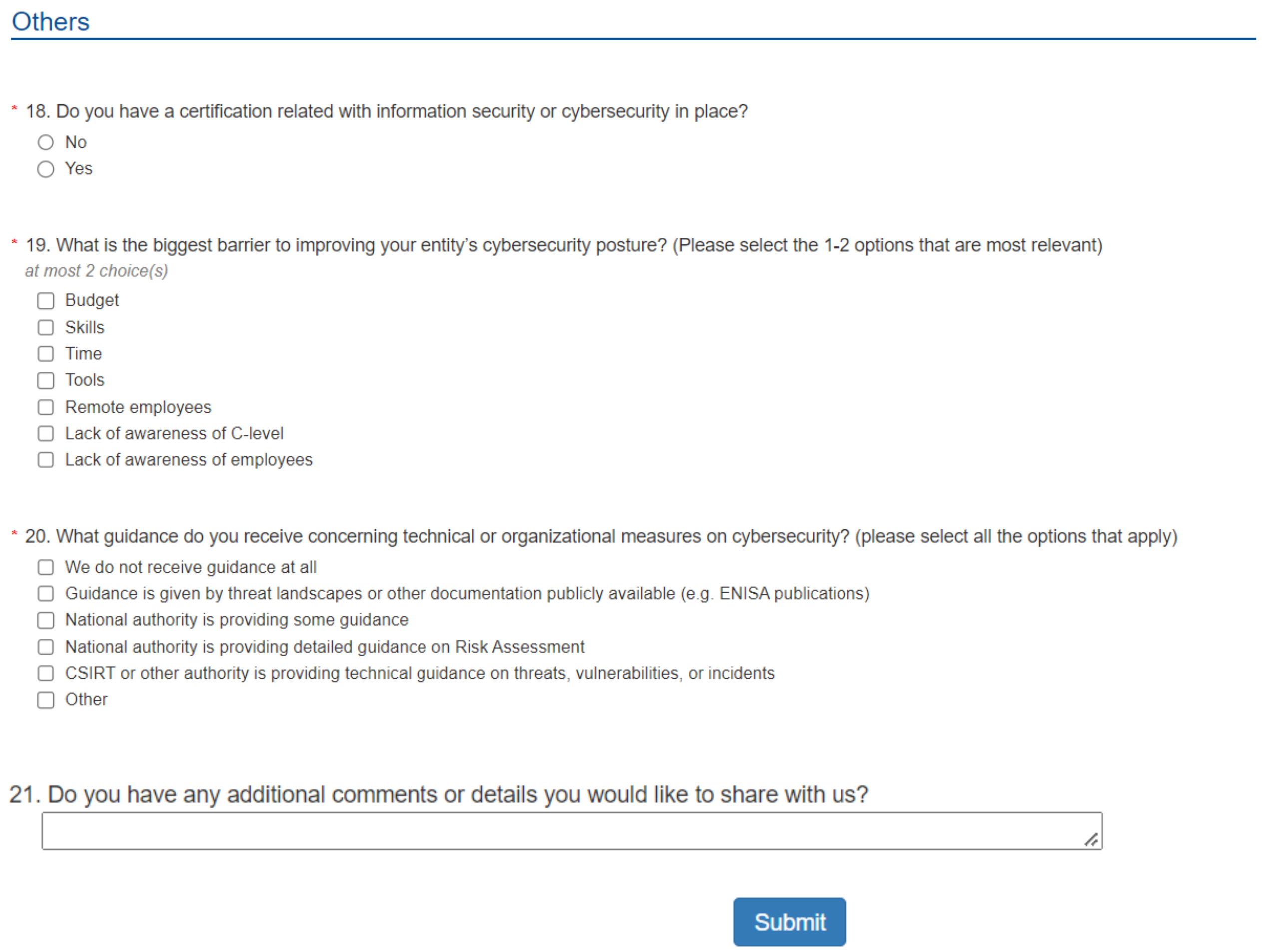
Use drag&drop or the up/down buttons to change the order or accept the initial order.

- ⠿ ↑ ↓ Abusive Content
- ⠿ ↑ ↓ Malicious Code
- ⠿ ↑ ↓ Information Gathering
- ⠿ ↑ ↓ Intrusion Attempts
- ⠿ ↑ ↓ Intrusions
- ⠿ ↑ ↓ Availability
- ⠿ ↑ ↓ Information Content Security
- ⠿ ↑ ↓ Fraud



* 17. Identify what type of incidents had the most impact on your organization in the last 2 years

□ Abusive Content
□ Malicious Code
□ Information Gathering
□ Intrusion Attempts
□ Availability
□ Information Content Security
□ Fraud
□ Other



Others

* 18. Do you have a certification related with information security or cybersecurity in place?

○ No
○ Yes

* 19. What is the biggest barrier to improving your entity's cybersecurity posture? (Please select the 1-2 options that are most relevant)

at most 2 choice(s)

□ Budget
□ Skills
□ Time
□ Tools
□ Remote employees
□ Lack of awareness of C-level
□ Lack of awareness of employees

* 20. What guidance do you receive concerning technical or organizational measures on cybersecurity? (please select all the options that apply)

□ We do not receive guidance at all
□ Guidance is given by threat landscapes or other documentation publicly available (e.g. ENISA publications)
□ National authority is providing some guidance
□ National authority is providing detailed guidance on Risk Assessment
□ CSIRT or other authority is providing technical guidance on threats, vulnerabilities, or incidents
□ Other

21. Do you have any additional comments or details you would like to share with us?