

Article

Cybersecurity Challenges in Hospitals: International Incident Reports Analysis and Expert Validation

Grigori Rogge *  and Sabine Bohnet-Joschko 

Chair of Management and Innovation in Health Care, Faculty of Management, Economics and Society,
Witten/Herdecke University, 58448 Witten, Germany; sabine.bohnet-joschko@uni-wh.de

* Correspondence: grigori.rogge@uni-wh.de

Abstract

The healthcare sector is undergoing a digital transformation that improves the quality of care, increases efficiency, and enhances connectivity. With digitalization comes an increase in cyber threats. Hospitals are among the primary targets of cybercriminals. Adequate protective measures require knowledge and analysis of frequently occurring incidents. This study aimed to identify types of cyber risks and to evaluate factors influencing incident occurrence using a mixed-methods approach. Data on cyber incidents and data breaches from 2021 to 2024 were consolidated from five publicly accessible international datasets into a single unified dataset with 3459 entries and analyzed with a focus on hospital incidents. Results showed that hacking, especially involving ransomware, poses a key security risk in hospitals. The results were then discussed in four focus groups with 14 IT experts from hospitals. They highlighted threats and potential conflicts arising from the integration of new technologies, including the escalation of external risks as hacking activities become more organized and professionalized. The need for openly accessible and understandable data on hospital cyber risks, as well as for collaborative exchange among institutions, was emphasized. The study identifies gaps in current knowledge regarding the integration of technology into hospital networks, suggesting directions for future research.

Keywords: cybersecurity; hospital; healthcare; risk; database; dataset; ransomware; phishing; social engineering; DoS

1. Introduction

Over recent years, the healthcare industry has experienced a growing trend of digitalization that constantly increases the amount of processed patient data and improves patient care [1]. At the same time, it is leading to a growing number of endpoint devices connected to healthcare IT systems, including smartphones, computers, and medical devices [2,3]. This trend increases both the reliance on technology and the attack surface for cyberattacks [4,5]. Prior work indicates that the healthcare sector is less prepared for cyber threats than other sectors [6]. Legacy systems that do not receive regular updates from manufacturers and encounter compatibility issues with new security solutions introduce vulnerabilities [7,8]. Additionally, the fast-paced integration of new technologies can create a gap between technology adoption and the implementation of appropriate security protocols [9,10]. Hospitals, in particular, operate in a complex multi-stakeholder environment in which cybersecurity decisions must balance the needs of medical and administrative staff, patients, and visitors, as well as regulatory requirements. These often competing priorities, alongside the focus on patient care, complicate the implementation of standard



Academic Editor: Jiang Bian

Received: 17 December 2025

Revised: 27 March 2026

Accepted: 30 March 2026

Published: 2 April 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

security practices [11]. Further, patient data is constantly exchanged between healthcare institutions, thereby increasing security risks [12]. Patient data holds high value for cybercriminals, as it can be used for insurance fraud, identity theft, or medical condition-related extortion [13,14].

Consequently, healthcare institutions, including hospitals, have become primary targets for cybercriminals. Between January 2021 and March 2023, 53% of cyberattacks in Europe were directed at healthcare providers. Hospitals were the most frequently attacked facilities, accounting for 42% of those attacks [15]. In comparison to other sectors, cyberattacks in healthcare not only have financial and reputational consequences but also pose a risk to patient safety [16].

Humans are frequently considered a major risk factor for cyber incidents [17]. Employees in the healthcare sector face significant challenges through the constant adoption of new technologies and high workloads [18,19]. Criminals often exploit human behavior through social engineering. Phishing is described as the primary concern in this field [20–22]. Cybersecurity extends beyond technical solutions and fundamentally depends on the people within an organization who interact with and shape the use of technology [23,24].

This is reflected in the HOT-fit model, a theoretical construct positing that a balance among human, organizational, and technological elements is necessary for the successful implementation of technology. An organization is viewed as a socio-technical system, and the fit of these three dimensions is essential for success [25,26]. This model has previously been applied in cybersecurity research [27–30].

Factors in the human dimension include personal characteristics such as skills, position, and tasks. Organizational factors encompass both internal and external characteristics. Examples of internal characteristics include organization size, structure, and processes, while external characteristics include regulations and industry-specific conditions. Technological factors consist of technological characteristics and the requirements arising from users or organizational procedures. These characteristics are divided into system quality, which includes aspects such as security, accessibility, usability, and reliability, information quality, which refers to the information output and its usability for users, and service quality, which concerns the reliability, flexibility, and physical tangibility of the technology [25,26,31].

To gather further insight into cyber incidents, previous studies have analyzed related datasets. Many of those studies analyzed datasets that describe the technical signatures of cyber-attacks and are mainly used for training machine learning algorithms and intrusion detection systems [32,33].

A particular concern in the context of cyber incidents is healthcare data breaches [34].

Different studies used the Breach Portal of the US Department of Health and Human Services (HHS) as a data source. Accordingly, there is a strong US focus in prior studies [35,36].

There have been previous studies that aimed to expand information on cyber incidents by combining multiple databases into a single large dataset rather than relying on a single database. Abbiati et al. (2020) established a unified category system and applied it to three cybersecurity datasets using data between 2005 and 2018; however, they did not focus specifically on healthcare organizations [37]. Thomas et al. (2025) combined datasets on cyber incidents in the transportation sector, using an LLM-based approach to extract relevant incidents from four databases between 2018 and 2022 and categorizing them by transportation mode [38].

Previous studies described a general underreporting of cyber incidents [34,39]. Additionally, incident descriptions have been highlighted as generic or difficult to interpret [40]. As a result, detailed information on individual incidents, including causes and subsequent measures, remains limited [41,42].

Given the continuously evolving risk landscape [43,44] and the fact that available data on cyber incidents is often US-focused and rather generic, this study aims to provide a comprehensive overview of current cybersecurity risks for healthcare institutions, particularly hospitals, drawing on multiple international data sources and expert insights. Hereby, we aimed to identify influencing factors within the dimensions of the HOT-fit model. Additionally, we investigated whether and how expert opinions contextualize the risk situation based on public data and how they differ from it. This work seeks to support risk management, the development of cybersecurity strategies, the design of training programs, and further research.

2. Materials and Methods

2.1. Synthesis of Cybersecurity Datasets

To obtain a comprehensive overview of the frequency and nature of real-world cyber incidents, we combined five datasets into a single unified dataset. For dataset selection, data export had to be available and contain information on cybersecurity incidents in the healthcare industry. Additionally, it had to be documented how the data was collected and categorized. Datasets had to be available in English.

Selected datasets included:

- Breach Portal of the Department of Health and Human Services (HHS);
- The Incident Hub by TI Safe (TIS);
- Database by European Repository of Cyber Incidents (EuRepoC);
- Cyber Events Database University of Maryland (CED);
- Privacy Rights Clearinghouse (PRC).

For our analysis, we included incident data from 2021 to 2024 for incidents in healthcare institutions and businesses associated with healthcare. Data were first exported in January 2025. Due to a relatively low number of incidents in 2024, data for this year were again exported in autumn 2025.

To combine the datasets, similarly to Abbiati et al. (2020), we established a category system that could be mapped to the individual datasets [37].

As the HHS database is one of the most comprehensive datasets on data breaches and cyber incidents [45], we used its categories as the main categories for our unified dataset (Appendix A.1, Table A1).

To further detail the types of cyber incidents resulting from hacking, we established subcategories for the main category “Hacking/IT Incident” (Appendix A.1, Table A2) based on attack vectors commonly identified in the literature. For the remaining main categories, we established a different set of subcategories, inductively developed by analyzing our dataset in the context of the HOT-fit model (Appendix A.1, Table A3).

The established columns of the unified dataset are pictured in Table 1.

Table 1. Columns of the unified dataset.

No.	Year	Incident Date	Location (country)	Entity name	Incident Description	Main category	Subcategory	Source URL	Originated Dataset
-----	------	---------------	--------------------	-------------	----------------------	---------------	-------------	------------	--------------------

The process of mapping the individual datasets to our category system is described in Appendix A.2, Figure A1.

Following these steps, initially 6709 entries were included (2912 HHS, 2254 PRC, 1286 CED, 211 EuRepoC, and 46 TIS) in the unified dataset [46–50].

After consolidating all incidents into a single Excel file, we manually removed duplicates based on entity names, incident dates, and incident descriptions. When we identified

a duplicate, we kept the entries with more information. If the removed entry included additional information, we added it to the entry retained in the dataset.

Furthermore, we excluded entries lacking an incident description, incidents involving companies or institutions incorrectly classified as healthcare entities, and incidents at veterinary health institutions.

Given our primary focus on analyzing cyber risks in hospitals, we decided to develop a second dataset focused on hospitals and healthcare organizations that offer inpatient care. To establish this dataset, we first filtered the entity names and incident descriptions of the unified dataset for keywords such as “Medical Center” or “Hospital,” and evaluated whether the incident occurred in a facility with inpatient care. Afterward, we excluded entities with names containing keywords such as “Insurance” or “Trust”. We then filtered for “Clinic”, “Memorial”, and “University” and checked the respective websites to see whether the facilities provided inpatient care. Finally, we descriptively analyzed the datasets.

2.2. Expert Focus Groups

After descriptively analyzing our datasets and comparing the results with prior literature, we conducted focus group discussions to validate and further detail our analysis.

Focus group discussions offer the unique opportunity to exchange expert opinions on a defined matter, supporting understanding of the complex interactions that lead to cybersecurity incidents [51]. The focus group discussions were conducted as semi-structured guide-based interviews (see questionnaire in Appendix A.3, Table A4) [52].

For the focus groups, we recruited German hospital IT leaders and information security officers (ISO). There were no restrictions regarding hospital size and location within Germany. Before each discussion, participants were provided with study information and gave informed consent to participate. Table 2 provides further insight into the composition of our study panel.

Table 2. Characteristics of study participants and their hospitals.

Number of Participants	14
Role of Participants	
IT Leader	7
Information Security Officer	7
Hospital Characteristics	
Small (less than 400 beds)	4
Medium (between 400 and 799 beds)	3
Large (800 or more beds)	7

One researcher moderated each focus group. The discussions lasted around 90 min. Similar to Burke et al. (2024), we chose to conduct the focus groups in a small group size, as healthcare cybersecurity is a sensitive topic and a smaller group size may lead to participants being more open about their personal insights [51]. The focus groups were conducted in German, captured via Zoom, and later transcribed with the software aTrain (version 1.4.1) [53]. They were analyzed by performing a thematic analysis according to the methodology of Braun & Clarke [54]. To structure our inductive codes, we used the HOT-fit model. For the analysis, we used MAXQDA 24.

3. Results

3.1. General Characteristics of the Datasets

The merging process of our datasets is shown in Figure 1. After removing duplicates, we had 3459 entries remaining in the unified dataset and 609 (17.6%) in the hospital dataset.

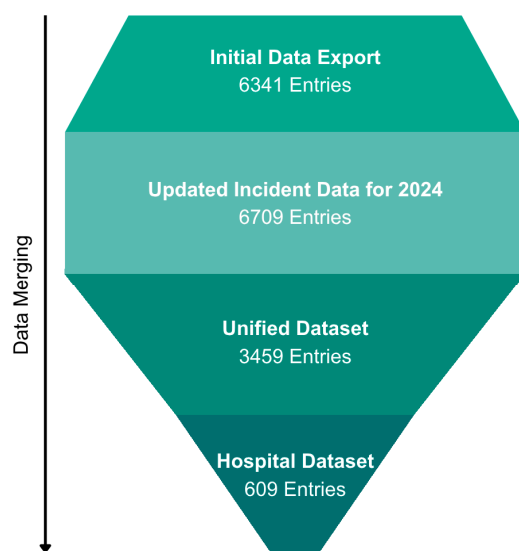


Figure 1. Merging process of datasets.

The distributions of entries in the unified dataset and the hospital dataset, based on the source datasets, are shown in Table 3. The HHS database, with 1762 incidents, is by far the most represented in our unified dataset, making up about 50% of all entries. The TI Safe Incident Hub has the fewest incidents in the unified dataset, with only 31 incidents.

Table 3. Datasets included in the unified and hospital dataset.

Originated Dataset	Entries in the Unified Dataset	Entries in the Hospital Dataset
PRC	762 (22%)	82 (13.5%)
HHS	1762 (50.9%)	268 (44%)
Cyber Events Database	722 (20.9%)	170 (27.9%)
EuRepoC	182 (5.3%)	77 (12.6%)
TI Safe Incident Hub	31 (0.9%)	12 (2%)

In the hospital dataset, 44% of entries are from the HHS database. Here, the Incident Hub is also the least represented dataset, with only 12 entries.

The unified dataset contains incidents from 54 countries. Most incidents occurred in the United States of America (3169), followed by France (32), Canada (27), and Italy (24).

In the unified dataset, most incidents were recorded in 2023 (979). The lowest number of incidents was recorded in 2022 (751). In 2021, 909 incidents were recorded, and in 2024, 820. Recorded incidents in 2024 sharply decreased after March, from the highest number in the first quarter (281) to the lowest in the second (190) and fourth quarter (178), compared to other years. May 2023 had the highest number of incidents recorded in a single month (115). In general, incidents were evenly distributed across the different months within a year.

As in the unified dataset, 2023 (171) was also the year with the highest number of incidents in the hospital dataset. 2022 (125) had the lowest. Whereas in the unified dataset, there was a significant gap of 89 incidents between 2021 and 2024, in the hospital dataset, 2021 (157) and 2024 (156) had nearly the same number of recorded incidents. March

2024 was the month with the highest number of incidents in the hospital dataset. Here, 41 incidents were recorded, representing a 64% increase compared to September 2023, the month with the second-highest number of incidents (25).

The detailed numbers for the unified dataset and the hospital dataset are shown in Appendix B, Tables A5–A9.

3.1.1. Analysis of the Categories of the Unified Dataset

Looking at the distribution of main categories, on average between 2021 and 2024, most incidents (83.7%) were attributed to the “Hacking/IT Incident” category. “Unauthorized Access/Disclosure” (13.1%) also contributed to a significant number of incidents (Figure 2).

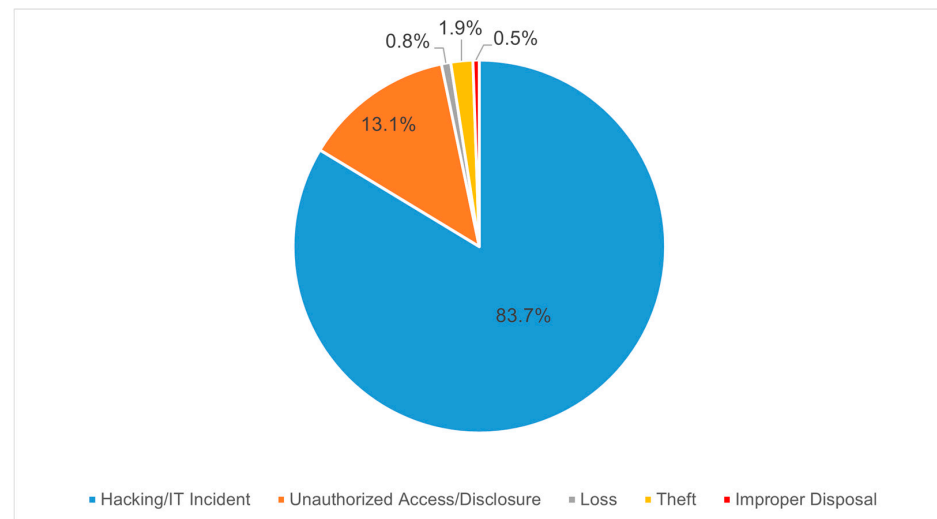


Figure 2. Average distribution of main categories in the unified dataset.

Looking at the subcategories, the highest proportion of incidents (37.8%) was categorized as “Hacking/Malware” (Figure 3). Here, we could not determine the attack vector of a hacking incident based on the available data. “Ransomware” accounted for 30.8% of incidents according to the subcategory. “Social Engineering, Phishing” accounted for 14.1%. To picture how incidents were categorized, we included an extract of our unified dataset in Appendix B, Table A10.

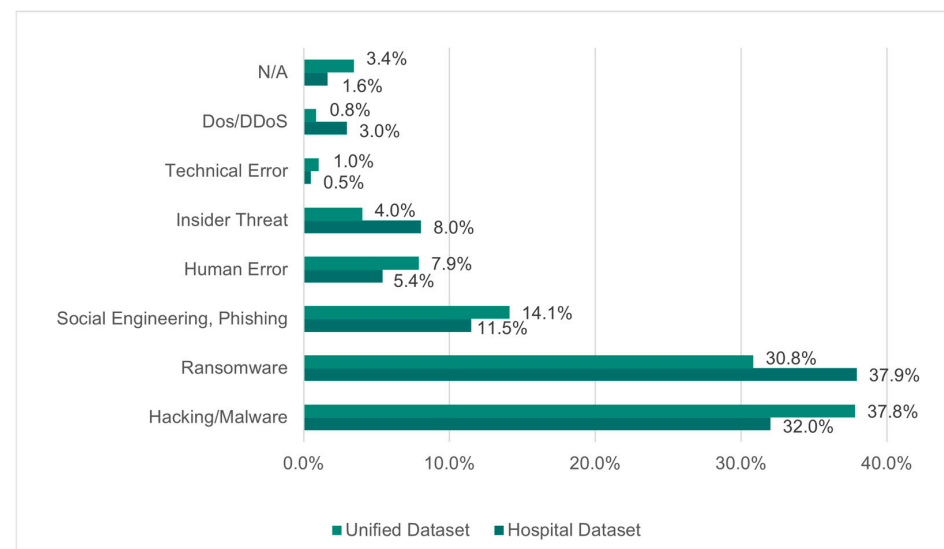


Figure 3. Comparison of the average distribution of subcategories between the unified dataset and the hospital dataset.

3.1.2. Analysis of the Categories of the Hospital Dataset

The distribution of main categories within the hospital dataset is comparable to the unified dataset, with 84.6% of incidents categorized as “Hacking/IT Incident” and 13.1% categorized as “Unauthorized Access/Disclosure”.

However, the average distribution of the subcategories differs (Figure 3).

Ransomware incidents are proportionally 7.1% higher in the hospital dataset. 8.0% of incidents in the hospital dataset were categorized as “Insider Threat”, double the amount of the unified dataset (4.0%)

26.0% of incidents in the unified dataset and 24.9% in the hospital dataset were directly related to the human factor, categorized as “Social Engineering, Phishing”, “Insider Threat”, or “Human Error”.

3.2. Focus Groups

Our focus groups revealed a diverse threat landscape in hospitals. Apart from growing risks and limited resources, positive developments were also reported. We categorized our identified themes into sub-themes and underlying topics within the dimensions of the HOT-fit model (Table 4). Each dimension is presented in more detail below, with explanations of the mapped sub-themes and selected quotations to demonstrate our findings.

Table 4. Influencing factors on cybersecurity derived from the focus groups.

Themes and Sub-Themes	Underlying Topics
Technological Factors on Hospital IT Security Risks	
Evolving Forms of Hacking	• Use of AI in Hacking
Balancing Usability and Security	• Technology Must Adapt to Users’ Everyday Lives
Technical Weaknesses Lead to Cyber Incidents	• Security Measures are Developed Reactively • Old User Accounts • Application Control • Lack of Multifactor Authentication • VPN Access
Integrating New Devices or Software Increases Security Risks	• Insufficient Security Architecture in Third-Party Software or Devices • Connected Medical Devices are of Exceptionally High Risk • Third-Party Manufacturers with Access Rights Increase Attack Surface
Technical Measures for Increasing Security	• Integration of SIEM Systems • Decrease in Phishing Risk Due to Technical Security Measures • Network Segmentation • Providing Secure Devices
Organizational Factors on Hospital IT Security Risks	
Lack of Sufficient Data for Risk Management and Organizational Learning	• Unwillingness to Share Data on Weaknesses and Incidents • Use of Informal Sources for Incident Data • Incomplete and Undetailed Data • High Variation in Maturity of Learning Process
Security Challenges in Supplier Management	• Complicated Access to Cyber Insurance • Expansion of Security Processes to Supply Chains • Conflicting Interests in the Integration of New Technologies

Table 4. Cont.

Themes and Sub-Themes	Underlying Topics
Lack of Expertise and Capacity	• Lack of Sufficient Physical Protective Measures • Turning a Blind Eye to Risks due to Overload • Outsourcing of Security Processes
Institutionalization of Hacking	• Destabilizing Critical Infrastructure • Hospitals Previously Avoided as Targets • Easier Access to Ransomware and Other Malicious Software
Organizational Measures for increasing Security	• Defined Responsibilities in Cybersecurity • Training of Employees • Information Security Management System (ISMS) • Specialized Security Teams • Positive Culture and Identification with the Organization
Human Factors on Hospital IT Security Risks	
Rise in Risk Awareness	• Phishing has Become Less Critical • User Awareness has Risen • Significantly Higher Risk Awareness after an Incident
Personal Security Habits Carry Over into Work	• Use of Personal Electronic Devices • Openly Sharing Data • Intentional Misconduct
Main Target of Cybercriminals	• Work Environment Leads to Incidents • The Human Factor is the Primary Contributor to Actual Incidents • Cybercriminals Deliberately Exploit the Human Factor
Employee Heterogeneity	• Difference in Competence and Openness Regarding Cybersecurity • Respectful and Targeted Communication

3.2.1. Technological Factors on Hospital IT Security Risks

The experts discussed various technological factors influencing cyber risks, with particular emphasis on the impact of AI. They noted that AI may accelerate the exploitation of system vulnerabilities and enable more sophisticated phishing attacks, for example, by generating convincing email texts. Concerns were also raised about partially autonomous AI tools with access to patient data that could be manipulated. In contrast, other experts argued that AI does not fundamentally change attack types but may increase attack frequency by streamlining criminal activities. At the same time, AI was seen as a means to strengthen cybersecurity through improved penetration testing and AI-based intrusion detection systems. The ambivalent thoughts regarding AI are reflected in the quote from Expert A.

“Yes, this is a new threat and a new weapon of defense. So, the means change, but the threat itself does not change.”

(Expert A, IT Leader)

The experts largely agreed that AI applications related to hacking are still in their early stages and that it is difficult to anticipate future development.

They indicated that cyber incidents often result from the exploitation of technical weaknesses. Examples include old user accounts with weak passwords and insufficient multifactor authentication.

The continuous integration of new devices into hospital networks was identified as an increasing risk factor. It was criticized that device and software suppliers request extensive access rights, such as manufacturer VPN access for maintenance.

In addition, participants noted that medical devices, in particular, lack a comprehensive IT security architecture, making them attractive targets for cybercriminals. For instance, publicly known vulnerabilities are not regularly updated because of regulatory constraints. In this context, they discussed whether suppliers should be held liable when a device's inadequate security architecture caused a successful cyberattack (Expert B).

"If manufacturers were held liable for every cybersecurity incident they caused [...], including financial liability, many problems would solve themselves, because they would simply put more quality into their products."

(Expert B, ISO)

Another identified risk factor was that adequate security measures are often implemented only retrospectively.

Positive technological developments were also discussed, including protective measures against phishing emails, such as advanced firewalls and app blockers.

With the increased use of SIEM systems (Security Information and Event Management), transparency into cyber threats has improved, enabling security measures to be taken accordingly. If a device acts suspiciously, it can be separated from other parts of the network through network segmentation, limiting the spread of malicious software.

In addition, many hospitals have created secure workplaces with limited internet access that can be separated from the rest of the network in the event of an incident. Most organizations restrict the use of private devices and provide internal alternatives. The experts agreed that technology must be integrated into users' workflows to be accepted. Expert C emphasized that it is essential to understand how users operate with technology in the organizational context.

"Give users things that just work [...], things you don't have to explain much, where you can simply say: here you go, this is your tool for the job. [...] Connecting the technical interaction with the organizational side and with the human side, bringing this triangle into balance is the real art, I think."

(Expert C, ISO)

3.2.2. Organizational Factors on Hospital IT Security Risks

Several participants emphasized that the data available for risk management is insufficient, especially in Europe. Many hospitals obtain incident information from public media or newsletters issued by private companies. However, in these data, information on the causes of incidents and the security measures taken afterward is minimal. Affected hospitals are often not permitted to share more detailed information due to reputational risks.

Expert D described using international sources because of better data availability.

"In some cases, detailed reports from the US BSI [cybersecurity agency] become available only two or three days after an incident, which I continue to find impressive. We mainly use these reports to examine whether our own systems might have been vulnerable in a similar way. Alarming, it must be said that in many cases we indeed would have been. In those instances, we were simply fortunate."

(Expert D, ISO)

The experts also noted that they have established informal networks for exchanging guidance and information on security incidents. In almost all focus groups, a desire for

increased networking among professionals and the formation of joint security working groups was expressed.

Among the participants, there was substantial variation in the extent to which information on external incidents was used to support internal learning processes. The learning process following an internal security event was described as highly structured in most hospitals.

The participants' experience confirmed our preliminary research finding that there were fewer cyberattacks in 2022.

However, they noted that, based on their experience, hacking accounted for a smaller proportion of actual incidents. Regarding DoS/DDoS attacks, they mentioned that the low frequency observed in our dataset may result from the limited impact on hospital procedures when the website was inaccessible for a few hours or days.

Participants highlighted risks related to IT suppliers and described the need to extend their security procedures. Expert E pictured technology integration as a process with conflicting interests that need to be balanced.

"Supplier and supply-chain attacks, that's a major issue. That's why we have a relatively strict supplier evaluation process and follow up on what suppliers are doing. But at the end of the day, it becomes disconnected when procurement or the project team says, 'We're buying this now.' Or when we get free devices from some manufacturers, and then the thing is sitting there, and of course the user says, 'Well, we have it now, so it has to work.' And then information security is in a bad position to say, 'We can't allow that.' The device is already there, possibly already being used, and then you somehow have to figure out how to work things out."

(Expert E, ISO)

Furthermore, based on the current risk situation, the experts reported that obtaining cyber insurance has become increasingly complex. Insurance companies impose stringent cybersecurity requirements, and insurance fees have risen substantially. In the context of financial and workforce-related pressure, this is a significant challenge for hospitals. High software licensing fees and the need to outsource security procedures, such as monitoring SIEM systems, further exacerbate this issue, especially for smaller hospitals.

They also acknowledged that identified security issues are often not addressed immediately due to conflicting interests with other departments or a lack of resources.

Participants stated that hospital management in the past has been willing to invest more in IT security. However, the available resources are still considered insufficient.

Hospitals face the dilemma of operating as open environments, with staff, patients, and visitors continuously entering and leaving, while simultaneously having to enforce physical security procedures. Participants perceived a high risk of criminals freely entering hospital premises and gaining physical access to IT systems.

The interviewees observed the institutionalization of the hacking scene. Previously, cybercriminals often avoided hospitals as targets for ethical reasons, but stronger financial motives have changed this. The experts argued that access to malicious software has been dramatically simplified, for example, through darknet marketplaces. Criminals without IT knowledge can now launch attacks against hospitals. Expert F emphasizes ransomware as a business model for hackers, which has increased the frequency of ransomware attacks.

"Ransomware is, of course, a very good business model. I mean, they're all just business people. [...] The days when someone had to sit down and find a security vulnerability are long gone. Now, you just have to say, 'I have a few customers, I need a few tools for that,' similar to what we do in IT, where I purchase a service."

(Expert F, IT Leader)

However, the experts explained that distinguishing between ransomware and social engineering attacks is difficult, since social engineering often serves as the initial attack vector for ransomware.

Apart from monetary motives, cybercriminals, including state-sponsored actors, increasingly target hospitals to destabilize critical infrastructure amid rising global tensions. In particular, participants from larger hospitals reported preparing for scenarios involving targeted state-sponsored attacks. Expert G observed an increase in scans for potential vulnerabilities by actors using foreign IP addresses since the beginning of the large-scale conflict in Ukraine.

“Attempts are made to find vulnerabilities via the human factor, but also via technical scans, vulnerability scans, and port scans with a wide variety of countries of origin, at least in terms of IP address assignment. Of course, since the Ukraine crisis began two years ago, we have noticed that the number of attacks or attempted attacks has increased.”

(Expert G, ISO)

It became evident that clearly defined IT security responsibilities are essential. Participants from institutions with dedicated information security officers demonstrated a stronger understanding of risk exposure and regulatory requirements, and larger hospital groups were reported to establish central security expert teams to lead incident response. Recurring and targeted training was identified as a key organizational measure for increasing awareness and security. Participants highlighted various best-practice examples for successful training, including targeted awareness campaigns, recurring simulations of phishing emails, and life-hacking sessions that demonstrate to hospital employees what hackers are capable of.

3.2.3. Human Factors on Hospital IT Security Risks

In line with the training concepts, awareness was the key human factors topic. An increase in risk awareness among hospital employees has been observed. The interviewees explained this assessment by a rise in the number of phishing emails reported by their colleagues and a decrease in the sharing of personal account login credentials. They also noted that in recent years, the willingness to learn about security topics and to accept security measures has risen. Especially after a security incident, there is a sharp increase in cybersecurity awareness and acceptance. However, these decline quickly once hospitals return to their routine procedures.

Experts emphasized that personal IT security habits carry over into the workplace. This has both positive and negative implications. On the one hand, employees approach the IT department to learn how to better secure their personal devices (Expert H).

“I think there is a different way of thinking than 10 or 15 years ago. [...] Lots of people come here with their private issues and ask, ‘How can I improve in this area, or can I still set up two-factor authentication, or whatever.’—I think awareness has changed in this regard.”

(Expert H, IT Leader)

On the other hand, participants reported that, in their daily work, they encounter more data protection issues caused by employees than by cyberattacks that compromise patient data. Employees who freely share personal data on social media in their private lives tend to do the same with patient data in the work context, for example, via personal electronic devices or AI applications. Consequently, personal habits should also be addressed in security training, as Expert D stated.

“In general, during our awareness trainings, we always aim to engage employees on a personal level as well, because we know how closely the private and professional spheres

are intertwined. Therefore, it is important to us that employees also have a secure IT environment at home."

(Expert D, ISO)

Further examples of human-related risk factors included cases of intentional misconduct, such as curiosity about the consequences of clicking a phishing link, data breaches resulting from taking information out of the hospital, or bypassing security measures to streamline workflows. Interviewees described that some employees perceive IT security as solely the responsibility of the IT department and regard security risks as too distant to change their behavior, which often leads to conflicts with IT.

Employee heterogeneity must be considered in this context. It was reported that employees from different employee groups behave differently. For example, physicians are more willing to take IT risks than nurses. Also, digital competencies vary considerably and are becoming increasingly important across employee groups.

This has a substantial impact on the structure of training and on communication within hospitals. It was repeatedly emphasized that accepting security measures and minimizing potential conflicts require respectful communication at eye level. According to Expert I, the reasons for security procedures that may result in additional work must be explained transparently.

"I think you have to try very hard to generate understanding first, so that people know why certain restrictions are in place. 'Why do we have to change our password after x days', or 'why don't we have to change it', depending on the guidelines that are in place."

(Expert I, IT Leader)

Finally, experts noted that despite a positive trend, cybercriminals still primarily exploit humans and that the human factor remains the most common cause of cyber incidents.

4. Discussion

In this work, we aimed to create a holistic overview of hospital cyber risks by developing a unified and a hospital dataset that expands upon prior research. This was done by incorporating multiple international data sources and by establishing a categorization system that provides greater detail on incident types. We used the HOT-fit model as a structural framework to better understand the interactions within hospitals that contribute to cyber risks.

Even though we incorporated incident data from various sources, our datasets retained a strong US focus. Additionally, many incident descriptions remained brief and generic, although we consolidated duplicate entries. Thus, assigning incidents to the dimensions of the HOT-fit model based solely on the available incident descriptions proved challenging and required a degree of interpretation. Cyber incidents are often the result of multiple interacting factors [55].

In line with that, it was often difficult to determine which specific devices, systems, or vulnerabilities were exploited in the reported cyber incidents. For example, although medical devices were identified as high-risk components in our focus groups, incidents explicitly associated with such devices are only minimally represented in our datasets.

This highlights a broader limitation in the granularity of publicly available data and is consistent with insights from focus group participants, who noted that detailed information on cyber incidents, particularly in Europe, is rarely accessible to the public. Instead, participants primarily relied on private data sources or personal networks to gather more detailed information. This underscores the need to contextualize the data of our datasets, which was done through focus group discussions.

Arguably, contextualizing predominantly US-focused data through the lens of German expert assessments may result in a degree of misalignment, as the US healthcare landscape differs from Germany's in several respects, including the regulatory environment, IT spending, and the level of digital maturity [56,57]. However, in recent years, measures have been taken to accelerate the digitalization of the German healthcare system and hospitals' IT infrastructure [58]. Additionally, in a prior analysis based on the Global Cybersecurity Index and the Global Health Security Index of 190 countries, Germany and the USA were clustered together in one of three clusters with various other European nations [59]. Further, studies suggest that hospitals globally face similar risks regarding cyberattacks, such as ransomware and phishing [60]. Expert D also highlighted that several vulnerabilities reported by the American Cybersecurity and Infrastructure Security Agency (CISA) also affected their hospital, underscoring the relevance of the German assessments in a broader international context. Still, the focus group results reflect the perspectives of a limited number of experts.

Reviewing the numbers in our datasets, we observed that in the unified dataset, 17.6% of incidents were attributed to hospitals. This is significantly lower than the average number in Europe (42%) [15]. This discrepancy may be explained by differences in incident reporting across global regions. In the EU, smaller healthcare organizations were only required to report cyber incidents after October 2024, following the transposition of the NIS2 Directive into national law [61,62]. Like previous studies [63,64], a substantial portion of our data comes from the HHS database, which also includes smaller healthcare organizations that experienced data breaches [65]. This affects the proportion of hospitals included in our dataset.

The incident numbers for 2024 were relatively low at the time of the first data export (January 2025). In autumn 2025, incidents for 2024 nearly doubled, indicating a significant time gap between incident occurrence and recording in the datasets. 2022 had the fewest incidents. Interestingly, this was supported by the focus group participants' experiences.

The hospital dataset shows a spike in incidents in March 2024. This is largely due to a ransomware attack at rehabilitation and long-term acute care hospital operator Ernest Health, which filed separate breach reports for its subsidiaries in different US states [66].

Regarding the incident types observed in the unified dataset, 83.7% of incidents were categorized under the main category "Hacking/IT Incident". This is a higher number than in previous work, which also indicated a rising risk of hacking in recent years [67].

The unified dataset draws on multiple databases with different incident inclusion criteria, potentially introducing noise into the analysis.

While datasets such as the EuRepoC exclusively include cyber incidents, the HHS database also includes data breaches resulting from lost paper records, stolen devices, or misdirected emails. Still, 1349 of 1762 HHS incidents in the unified dataset were categorized as "Hacking/IT Incident", showcasing the predominance of hacking incidents [47,50]. An explanation for the growing relevance of hacking in public incident datasets is that incidents resulting from hacking often lead to a higher number of breached patient records [68], increasing the likelihood of incident reporting and media attention.

These factors may have contributed to a class imbalance in our datasets, potentially influencing the overall risk assessments and experts in the focus groups. Notably, participants indicated that the number of hacking incidents in the datasets was perceived as relatively high.

Although "Hacking/IT Incident" was by far the most frequent main category, DoS or DDoS-related events accounted for less than 1% of the incidents documented in our unified dataset. This is likely because the primary aim of such attacks is not data exfiltration [69]. During the focus groups, it was noted that temporary inaccessibility of a hospital website

for several hours or even days may be less critical than in other sectors, leading to fewer incidents being reported. Recent studies nevertheless show that DoS or DDoS attacks also pose a risk to connected endpoint devices [70]. Combined with the experts' assessments that state-sponsored cybercriminals are increasingly seeking to destabilize critical infrastructure, the proportion of DoS/DDoS attacks could rise in the future.

The most significant threat identified in our datasets was ransomware, particularly in hospitals, where 37.9% of incidents involved it. For instance, ransomware attacks receive considerable media attention and are therefore more likely to be captured in the datasets we used [71].

Hospitals face a strategic dilemma when confronted with ransomware. If they decide to pay a ransom, they risk becoming targets of additional attacks. At the same time, ransomware can severely disrupt procedures and patient care [72]. This aligns with the institutionalization of ransomware attacks and the changing motivations of cybercriminals observed by the focus group participants.

49% of IT leaders in a 2025 survey reported paying a ransom when they fell victim to an attack. Among the reasons for successful ransomware attacks were a shortage of cybersecurity specialists capable of monitoring health IT systems during an attack and phishing [73].

This aligns with the experts in the focus groups, who said they needed to outsource IT security tasks, such as monitoring their SIEM systems, due to limited capacity and expertise. Additionally, they found that distinguishing ransomware from social engineering is challenging, as it is often delivered via phishing and therefore involves the human factor.

In both our unified dataset and the hospital dataset, approximately 25% of incidents were attributed to the human factor. Prior literature identified it as a leading risk factor for cyber incidents [74]. This was supported by the experts in the focus groups who identified the human factor as the main cause of successful cyberattacks.

For instance, the share of incidents related to the human factor could be higher due to the challenges in distinguishing between phishing and ransomware. Further, 37.8% of incidents in the unified dataset and 32.0% of incidents in the hospital dataset were categorized as the subcategory "Hacking/Malware", potentially influencing the distribution of subcategories, including "Ransomware" and "Social Engineering, Phishing," within the "Hacking/IT Incident" main category.

Even though experts saw a high risk in human-factor-related cyberattacks, they saw a general positive trend regarding phishing, characterized by higher awareness and improved technological security measures.

In this context, experts, similar to prior research, emphasized the importance of training [75,76]. However, they pointed out that comprehensive training concepts need to account for employees' private environments to be successful. They justified this by arguing that private security behaviors carry over into the professional context. This aspect, combined with employee heterogeneity, should be considered in the development of future training programs.

Furthermore, the focus groups identified the use of AI in hacking as an emerging threat that warrants further investigation. The experts argued that, at present, assessing the risk posed by AI in hacking remains challenging due to its potential positive and negative implications. Additionally, opinions among the experts were divided on whether AI will primarily exacerbate existing threats or create new ones.

Experts in the focus groups considered establishing practical security concepts for the physical protection of IT assets as another factor to investigate further. They highlighted issues in this process due to the open hospital environment.

In line with the HOT-fit model, participants emphasized that technologies and security processes must align with user requirements and the work environment. The management of third-party suppliers and the integration of new technologies were highly relevant in this context. Participants described conflicting interests, technological dependence, and increased vulnerability to cyberattacks that exploit external partners' access rights as risk factors to consider. Finding the right balance when integrating new technologies, potentially using the HOT-fit model, could therefore be a theme for future research.

Finally, greater availability of publicly accessible data, especially in Europe, beyond condensed reports and research initiatives such as EuRepoC would support risk management in hospitals and enable further research.

5. Conclusions

Cybersecurity is a pressing topic for healthcare institutions, including hospitals. By creating a single large, unified dataset with 3459 entries and implementing a unified category system with defined subcategories, we added an additional layer of detail that has rarely been provided in prior work. The conduct of focus groups helped us bridge knowledge gaps arising from generic incident descriptions and enabled a more nuanced understanding of hospital-specific IT risks. On the one hand, we identified positive trends such as rising awareness and more comprehensive security measures, including the integration of SIEM systems and network segmentation. On the other hand, emerging threats were observed, including the carryover of private security habits into the professional context, the growing institutionalization of cyber criminals, and the use of AI in hacking. In addition, the complex challenges associated with supplier management and technology integration represent promising areas for future research.

Author Contributions: Conceptualization, G.R. and S.B.-J.; methodology, G.R. and S.B.-J.; data collection, curation and analysis, G.R.; writing—original draft preparation, G.R.; writing—review and editing, S.B.-J.; visualization, G.R. and S.B.-J.; supervision, S.B.-J.; funding acquisition, S.B.-J. All authors have read and agreed to the published version of the manuscript.

Funding: This study was conducted as part of the ATLAS project 'Innovation and Digital Transformation in Healthcare,' funded by the State of North Rhine-Westphalia, Germany (grant number: ITG-1-1).

Institutional Review Board Statement: Ethical review and approval were waived for this study as we did not conduct human research, interventional and noninterventional clinical studies, nor clinical trials. We did not collect healthcare data and did not use (residual) human material for scientific purposes. Our study was based on publicly available data and expert assessments. Prior to their participation, experts were provided with comprehensive study information, information on the processing of their data in accordance with the EU General Data Protection Regulation, and were informed that their participation in the study was voluntary. Expert information included in the study was completely anonymized.

Informed Consent Statement: All experts participating in the focus groups provided their written informed consent and participated voluntarily.

Data Availability Statement: The data presented in this study are available on request from the corresponding author due to the privacy of our focus group participants.

Acknowledgments: During the preparation of this manuscript, the authors used DeepL, Grammarly (version 1.2.245.1868), and ChatGPT (model GPT-5) for the purpose of language editing, given that the authors are non-native English speakers. Transcripts of the focus groups were created with aTrain (version 1.4.1). The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
CED	Cyber Events Database University of Maryland
CISA	Cybersecurity and Infrastructure Security Agency
DDoS	Distributed Denial of Service
DoS	Denial of Service
EMR	Electronic Medical Records
EuRepoC	European Repository of Cyber Incidents
HHS	Health and Human Services
ISO	Information Security Officer
IT	Information Technology
MDPI	Multidisciplinary Digital Publishing Institute
PHI	Protected Health Information
PRC	Privacy Rights Clearinghouse
SIEM	Security Information and Event Management

Appendix A

Appendix A.1. Dataset Categories

Table A1. Main categories for the unified dataset based on the HHS database.

Main Category Name	Main Category Description
Hacking/IT Incident	Hacking/IT Incident applies, if systems were impermissibly accessed through technical intrusions (including by malware or directed hacking) including systems, servers, desktops, laptops, mobile devices and medical devices.
Loss	Loss applies if equipment (servers, desktops, laptops, back-up tapes, thumb-drives, mobile devices, copiers, or other hardware) or if paper records were lost. For example, if a workforce member left a laptop or paper records in a public place.
Theft	Theft applies if equipment housing electronic protected health information (servers, desktops, laptops, back-up tapes, thumb-drives, mobile devices, copiers, or other hardware) or if Paper records with patient data were stolen. If electronic protected health information was stolen as a result of a technical intrusion, Hacking/IT Incident is selected.
Improper Disposal	Improper Disposal applies if the electronic media (servers, desktops, laptops, back-up tapes, thumb drives, mobile devices, copiers, or other hardware) was not appropriately cleared, purged, or destroyed, or if Paper records were not appropriately shredded or otherwise destroyed prior to disposal.
Unauthorized Access/Disclosure	Unauthorized Access/Disclosure applies if no other category fits. For example, when patient data was breached due to misdirected mailing or other communication.

Table A2. Established subcategories for the main category “Hacking/IT Incident”.

Subcategory Name	Mapping Guideline
DoS/DDoS	Reviewed database either has a category which is called DoS/DDoS, or DoS/DDoS is mentioned in the incident description, or it is mentioned that systems were not accessible due to overwhelming traffic.
Ransomware	Reviewed database either has a category which is called ransomware, ransomware is mentioned in the incident description, or encryption of systems is mentioned.

Table A2. Cont.

Subcategory Name	Mapping Guideline
Social Engineering, Phishing	The reviewed database either has a category with the name phishing or social engineering, or these types of incidents are described in the incident description.
Hacking/Malware	A cyberattack is mentioned but it is not stated how it was conducted.

Table A3. Established subcategories for the remaining main categories.

Subcategory Name	Mapping Guideline
Human Error	An unintentional act by an employee. For example, unintentionally sending an email with patient data to the wrong recipient.
Insider Threat	An intentional act by an employee. For example, downloading patient data from the network and then selling it to a third party, purposefully accessing files without permission, or uploading files to the internet.
Technical Error	Technical errors leading to unintended exposure, access, or transmission of information. This includes misconfigurations and system malfunctions.
N/A	No digital intrusion by a third party, no technical errors, and no unintentional/intentional acts by employees could be identified with the provided data.

Appendix A.2. Editing of Source Datasets

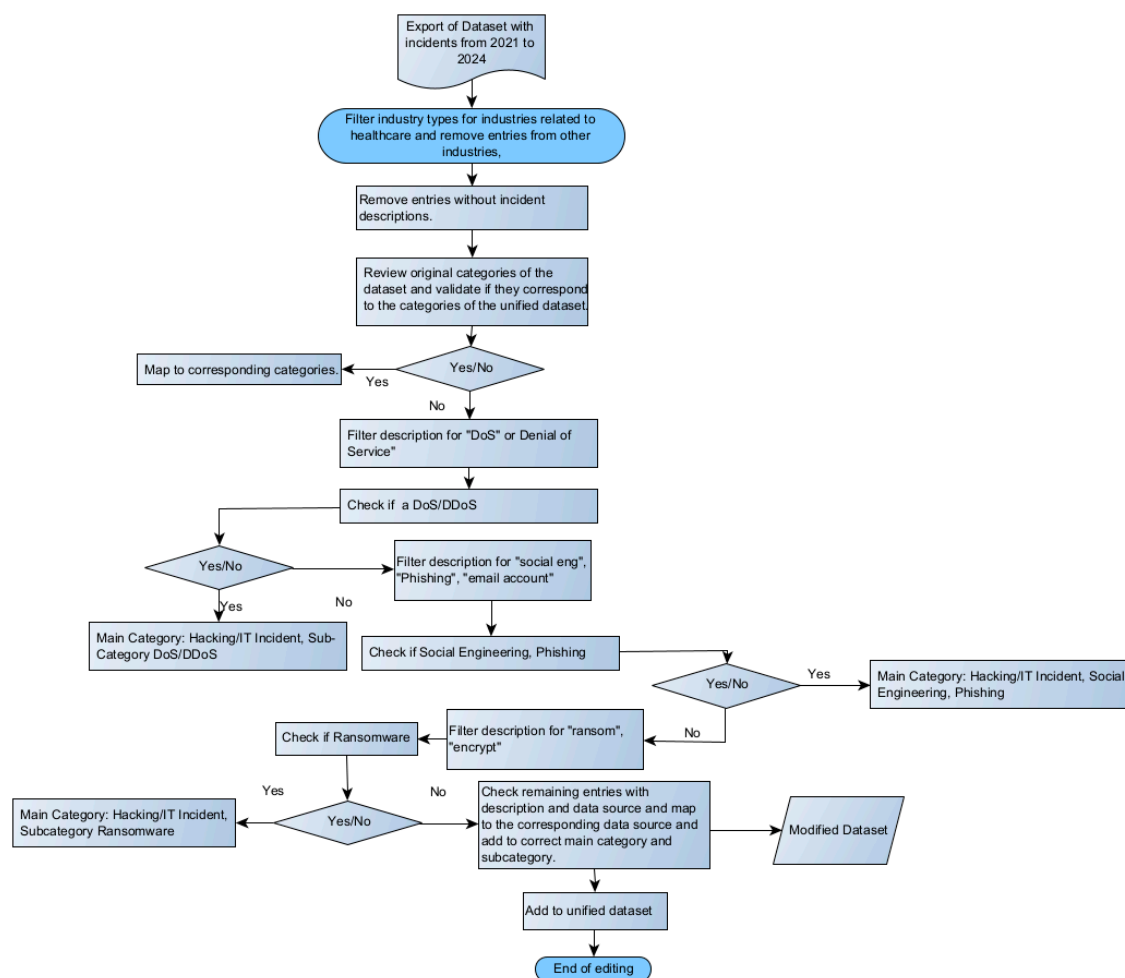


Figure A1. Schematic flowchart of the editing of the included datasets.

Appendix A.3. Semi-Structured Questionnaire

Table A4. Semi-structured guideline for focus groups on cybersecurity in hospitals.

Guiding Questions	Additional Questions
1. Opening Round	- Please briefly introduce yourself: Who are you, where do you work, and which typical cybersecurity challenge are you currently dealing with the most?
2. Which cyber risks are you particularly aware of at the moment?	- Are there any recent developments or incidents in the industry that you are following closely? - What threats do you perceive for your organization? - In which areas are you currently taking action to improve the protection of your organization?
3. How has the risk situation for your hospital changed when you look back over the past five years?	- Which new threats have emerged? - Where do you see positive developments or improvements? - What role has the Hospital Future Act (KHZG) played in the overall risk situation?
4. Presentation of preliminary study results	- Ransomware attacks in hospitals are a major problem. - Outdated medical technology is a potential entry point. - Repeated data breaches occur due to human error or intentional action.
5. What surprises you about the results, and how do you interpret them?	- Which aspects do you think are missing when we talk about cyber risks in hospitals? - Are there any points that are inaccurately represented? - Which external information or data sources play a role for you when assessing your own risk situation?
6. What role does the human factor play for you in cyber incidents in the hospital?	- What do you see as the biggest human-related risks? - Are there differences between administrative and medical staff in how they handle security? - Where do you experience conflicts between cybersecurity requirements and the demands of patient care? - What are the reasons why security requirements are sometimes not followed in everyday practice? - Where do you focus your awareness measures and training efforts?
7. How do you learn from cyber incidents?	- How do you ensure that the same mistake does not occur again? - Do you also use public data on incidents from other hospitals? - What obstacles exist when it comes to sharing experiences between departments or with other hospitals? - What is the typical process for reporting and documenting incidents?
8. Closing Round	- Which point was, in your view, not covered sufficiently today? - Which topic do you think we should pursue further?

Appendix B

Table A5. Distribution of incidents by month.

Month	Unified Dataset				Hospital Dataset			
	2021	2022	2023	2024	2021	2022	2023	2024
Jan	65	65	76	83	9	13	18	12
Feb	81	51	66	102	24	11	13	17
Mar	92	56	97	96	12	7	20	41
Apr	96	66	68	66	10	9	5	11
May	84	85	115	68	22	12	16	12
Jun	79	85	85	56	12	12	10	7
Jul	73	68	51	65	17	10	10	16
Aug	63	54	79	53	8	11	9	4
Sep	61	29	93	53	8	3	25	11
Oct	68	76	81	63	9	18	11	7
Nov	74	56	85	59	13	8	22	7
Dec	73	60	83	56	13	11	12	11
Total	909	751	979	820	157	125	171	156

Table A6. Incidents contained in the unified dataset according to their main categories.

Main Category	2021	2022	2023	2024	Total
Hacking/IT Incident	739 (81.3%)	631 (84%)	837 (85.5%)	687 (83.8%)	2894 (83.7%)
Unauthorized Access/Disclosure	126 (13.9%)	95 (12.6%)	121 (12.4%)	110 (13.4%)	452 (13.1%)
Loss	12 (1.3%)	6 (0.8%)	4 (0.4%)	6 (0.7%)	28 (0.8%)
Theft	26 (2.9%)	15 (2%)	12 (1.2%)	13 (1.6%)	66 (1.9%)
Improper Disposal	6 (0.7%)	4 (0.5%)	5 (0.5%)	4 (0.5%)	19 (0.5%)
Total	909 (26.3%)	751 (21.7%)	979 (28.3%)	820 (23.7%)	3459 (100%)

Table A7. Incidents contained in the unified dataset according to their subcategories.

Subcategory	2021	2022	2023	2024	Total
Hacking/Malware	265 (29.2%)	254 (33.8%)	450 (46%)	339 (41.3%)	1308 (37.8%)
Ransomware	305 (33.6%)	237 (31.6%)	295 (30.1%)	230 (28%)	1067 (30.8%)
Social Engineering, Phishing	167 (18.4%)	130 (17.3%)	80 (8.2%)	111 (13.5%)	488 (14.1%)
Human Error	80 (8.8%)	58 (7.7%)	80 (8.2%)	55 (6.7%)	273 (7.9%)
Insider Threat	48 (5.3%)	36 (4.8%)	28 (2.9%)	27 (3.3%)	139 (4%)
Technical Error	8 (0.9%)	7 (0.9%)	14 (1.4%)	7 (0.9%)	36 (1%)
Dos/DDoS	2 (0.2%)	10 (1.3%)	12 (1.2%)	5 (0.6%)	29 (0.8%)
N/A	34 (3.7%)	19 (2.5%)	20 (2%)	46 (5.6%)	119 (3.4%)
Total	909 (26.3%)	751 (21.71%)	979 (28.3%)	820 (23.7%)	3459 (100%)

Table A8. Incidents contained in the hospital dataset according to their main categories.

Main Category	2021	2022	2023	2024	Total
Hacking/IT Incident	124 (79%)	102 (81.6%)	151 (88.3%)	138 (88.5%)	515 (84.6%)
Unauthorized Access/Disclosure	31 (19.7%)	16 (12.8%)	19 (11.1%)	14 (9%)	80 (13.1%)
Loss	1 (0.6%)	3 (2.4%)	1 (0.6%)	1 (0.6%)	6 (1%)
Theft	1 (0.6%)	2 (1.6%)	0 (0%)	2 (1.3%)	5 (0.8%)
Improper Disposal	0 (0%)	2 (1.6%)	0 (0%)	1 (0.6%)	3 (0.5%)
Total	157 (25.8%)	125 (20.5%)	171 (28.1%)	156 (25.6%)	609 (100%)

Table A9. Incidents contained in the hospital dataset according to their subcategories.

Subcategory	2021	2022	2023	2024	Total
Hacking/Malware	45 (28.7%)	40 (32%)	71 (41.5%)	39 (25%)	195 (32%)
Ransomware	54 (34.4%)	37 (29.6%)	65 (38%)	75 (48.1%)	231 (37.9%)
Social Engineering, Phishing	24 (15.3%)	19 (15.2%)	7 (4.1%)	20 (12.8%)	70 (11.5%)
Human Error	12 (7.6%)	8 (6.4%)	10 (5.8%)	3 (1.9%)	33 (5.4%)
Insider Threat	19 (12.1%)	11 (8.8%)	8 (4.7%)	11 (7.1%)	49 (8%)
Technical Error	0 (0%)	1 (0.8%)	2 (1.2%)	0 (0%)	3 (0.5%)
Dos/DDoS	1 (0.6%)	6 (4.8%)	8 (4.7%)	3 (1.9%)	18 (3%)
N/A	2 (1.3%)	3 (2.4%)	0 (0%)	5 (3.2%)	10 (1.6%)
Total	157 (25.8%)	125 (20.5%)	171 (28.1%)	156 (25.6%)	609 (100%)

Table A10. Extract of incidents contained in the unified dataset.

No.	Year	Incident Date	Location (Country)	Entity Name	Incident Description	Main-Category	Sub-Category	Source URL	Originated Dataset
72	2021	3 February 2021	Belgium	Sacred Heart Hospital	The Sacred Heart Hospital in Mol is hit by a cyberattack.	Hacking/IT Incident	Hacking/Malware	https://www.databreaches.net/__trashed-12/ (accessed on 15 May 2025)	Cyber Events Data Base
94	2021	15 February 2021	United States of America	Capital Medical Center	Capital Medical Center is hit with an Avaddon ransomware attack.	Hacking/IT Incident	Ransomware	https://www.databreaches.net/cancer-patients-in-the-state-of-washington-had-their-sensitive-records-hacked-and-dumped-have-they-been-notified/ (accessed on 14 May 2025)	Cyber Events Data Base
1470	2022	5 October 2022	United States of America	Miller Miller Gerber LLP	The Montana Department of Justice reported a data breach involving Miller Miller Gerber LLP on 31 January 2023. The breach occurred on 5 October 2022, affecting 1 individual. The specific types of information compromised are unknown, and further details about the method of breach are not provided. The breach is classified as INSD (Insider Threat) based on the explicit description in the notification letter from University Hospital, as reported by the Montana Department of Justice. The letter states that a now-former employee with authorized access exceeded the authorized use of that access by providing patient information to unauthorized individuals. This clearly indicates deliberate misuse of access by an insider, satisfying the criteria for the INSD classification.	Unauthorized Access/Disclosure	Insider Threat	https://dojmt.gov/office-of-consumer-protection/reported-data-breaches/ (accessed on 11 June 2025)	PRC
1482	2022	14 October 2022	United States of America	Advocate Aurora Health	The covered entity (CE), Advocate Aurora Health, reported that web tracking technology transferred the protected health information (PHI) of 3,000,000 individuals to unauthorized recipients. OCR has consolidated this breach report into an existing compliance review of the CE.	Unauthorized Access/Disclosure	Technical Error	Not provided	HHS

Table A10. Cont.

No.	Year	Incident Date	Location (Country)	Entity Name	Incident Description	Main-Category	Sub-Category	Source URL	Originated Dataset
1720	2023	28 January 2023	Netherlands	University Medical Center of Groningen (UMCG)	The pro-Russian hacktivist group Killnet is suspected to be responsible for disrupting the information page of the University Medical Center of Groningen (UMCG) in the Netherlands, with DDoS attacks during 28–30 January 2023 according to Z-Cert, an expertise center for cybersecurity in healthcare. In addition, the websites of other European hospitals were also affected by DDoS attacks.	Hacking/IT Incident	DoS/DDoS	https://blog.cloudflare.com/uptick-in-healthcare-organizations-experiencing-targeted-ddos-attacks/ (accessed on 6 March 2025)	Eurepoc
2709	2024	8 February 2024	France	Viamedis and Almerys	Service providers Viamedis and Almerys have suffered phishing attacks that compromised user data. Bank, medical, and contact details were not exposed. However, information such as marital status, date of birth, and Social Security number was compromised.	Hacking/IT Incident	Social Engineering, Phishing	https://www.euronews.com/next/2024/02/08/data-of-33-million-people-in-france-stolen-in-its-largest-ever-cyberattack-this-is-what-we (accessed on 21 February 2025)	TI Safe Incident Hub
3034	2024	24 October 2024	United States of America	Stanislaus County Behavioral Health and Recovery Services	The covered entity (CE), Stanislaus County Behavioral Health and Recovery Services, reported that it mailed letters containing the protected health information (PHI) of 767 individuals to the wrong recipients. The PHI involved included names, addresses, and treatment information. The CE notified HHS, affected individuals, and the media. In its mitigation efforts, the CE implemented additional administrative and technical safeguards to better protect its PHI.	Unauthorized Access/Disclosure	Human Error	Not provided	HHS
3241	2024	29 March 2024	United States of America	Olive View-UCLA Medical Center	The covered entity (CE), County of Los Angeles Department of Health Services—Olive View—Medical Center, reported that paper documents containing the protected health information (PHI) of 3716 individuals were stolen during a burglary. The PHI involved included names, addresses, and financial and health insurance information. The CE notified HHS, the affected individuals, the media, and provided substitute notice. In response to the breach, the CE provided complimentary credit monitoring services and implemented additional administrative, technical, and security safeguards.	Theft	N/A	Not provided	HHS

References

1. Yeung, A.W.K.; Torkamani, A.; Butte, A.J.; Glicksberg, B.S.; Schuller, B.; Rodriguez, B.; Ting, D.S.W.; Bates, D.; Schaden, E.; Peng, H.; et al. The promise of digital healthcare technologies. *Front. Public Health* **2023**, *11*, 1196596. [\[CrossRef\]](#)
2. Giansanti, D.; Monoscalco, L. The cyber-risk in cardiology: Towards an investigation on the self-perception among the cardiologists. *Mhealth* **2021**, *7*, 28. [\[CrossRef\]](#)
3. Singh, J. Challenges with Medical Devices Connected to Hospital Network. *Int. J. Res. Appl. Sci. Eng. Technol.* **2024**, *12*, 735–749. [\[CrossRef\]](#)
4. Luna, R.; Rhine, E.; Myhra, M.; Sullivan, R.; Kruse, C.S. Cyber threats to health information systems: A systematic review. *Technol. Health Care* **2016**, *24*, 1–9. [\[CrossRef\]](#)
5. Tin, D.; Hata, R.; Granholm, F.; Ciottone, R.G.; Staynings, R.; Ciottone, G.R. Cyberthreats: A primer for healthcare professionals. *Am. J. Emerg. Med.* **2023**, *68*, 179–185. [\[CrossRef\]](#)
6. Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol. Health Care* **2017**, *25*, 1–10. [\[CrossRef\]](#) [\[PubMed\]](#)
7. Odedina, E.A. The impact of cyberattacks on patient safety and healthcare infrastructure: A risk management perspective. *Int. J. Eng. Technol. Res. Manag.* **2021**, *5*, 385–398.
8. Aldosari, B. Cybersecurity in Healthcare: New Threat to Patient Safety. *Cureus* **2025**, *17*, e83614. [\[CrossRef\]](#)
9. Wasserman, L.; Wasserman, Y. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Front. Digit. Health* **2022**, *4*, 862221. [\[CrossRef\]](#) [\[PubMed\]](#)
10. Ewoh, P.; Vartiainen, T. Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *J. Med. Internet Res.* **2024**, *26*, e46904. [\[CrossRef\]](#)
11. Jalali, M.S.; Kaiser, J.P. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *J. Med. Internet Res.* **2018**, *20*, e10059. [\[CrossRef\]](#)
12. Choi, S.J.; Chen, M.; Tan, X. Assessing the impact of health information exchange on hospital data breach risk. *Int. J. Med. Inform.* **2023**, *177*, 105149. [\[CrossRef\]](#)
13. Pilares, I.C.A.; Azam, S.; Akbulut, S.; Jonkman, M.; Shanmugam, B. Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS. *Sensors* **2022**, *22*, 4032. [\[CrossRef\]](#)
14. George, A.S.; Baskar, T.; Srikanth, P.B. Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partn. Univers. Int. Innov. J.* **2024**, *2*, 51–75.
15. Theocharidou, M.; Lella, I. Enisa Threat Landscape: Health Sector: (January 2021 to March 2023). Available online: <https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf> (accessed on 13 November 2025).
16. van Boven, L.S.; Kusters, R.W.J.; Tin, D.; van Osch, F.H.M.; de Cauwer, H.; Ketelings, L.; Rao, M.; Dameff, C.; Barten, D.G. Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals. *Ann. Emerg. Med.* **2024**, *83*, 46–56. [\[CrossRef\]](#)
17. Basil, N.N.; Ambe, S.; Ekhatior, C.; Fonkem, E. Health Records Database and Inherent Security Concerns: A Review of the Literature. *Cureus* **2022**, *14*, e30168. [\[CrossRef\]](#) [\[PubMed\]](#)
18. Dolezel, D.; Beauvais, B.; Stigler Granados, P.; Fulton, L.; Kruse, C.S. Effects of Internal and External Factors on Hospital Data Breaches: Quantitative Study. *J. Med. Internet Res.* **2023**, *25*, e51471. [\[CrossRef\]](#) [\[PubMed\]](#)
19. Hines, E.; Trivedi, S.; Hoang-Tran, C.; Mocharnuk, J.; Pfaff, M.J. Perspectives on Cybersecurity and Plastic Surgery: A Survey of Plastic Surgeons and Scoping Review of the Literature. *Aesthet. Surg. J.* **2023**, *43*, 1376–1383. [\[CrossRef\]](#) [\[PubMed\]](#)
20. Cartwright, A.J. The elephant in the room: Cybersecurity in healthcare. *J. Clin. Monit. Comput.* **2023**, *37*, 1123–1132. [\[CrossRef\]](#)
21. Suleski, T.; Ahmed, M. A Data Taxonomy for Adaptive Multifactor Authentication in the Internet of Health Care Things. *J. Med. Internet Res.* **2023**, *25*, e44114. [\[CrossRef\]](#)
22. Harvanek, M.; Bolcek, J.; Kufa, J.; Polak, L.; Simka, M.; Marsalek, R. Survey on 5G Physical Layer Security Threats and Countermeasures. *Sensors* **2024**, *24*, 5523. [\[CrossRef\]](#)
23. Cains, M.G.; Flora, L.; Taber, D.; King, Z.; Henshel, D.S. Defining Cyber Security and Cyber Security Risk with-in a Multidisciplinary Context using Expert Elicitation. *Risk Anal.* **2022**, *42*, 1643–1669. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Morgan, P.L.; Asquith, P.M.; Bishop, L.M.; Raywood-Burke, G.; Wedgbury, A.; Jones, K. A New Hope: Human-Centric Cybersecurity Research Embedded Within Organizations. In *HCI for Cybersecurity, Privacy and Trust*; Moallem, A., Ed.; Springer International Publishing: Cham, Switzerland, 2020; pp. 206–216, ISBN 978-3-030-50308-6.
25. Xu, J.; Lu, W. Developing a human-organization-technology fit model for information technology adoption in organizations. *Technol. Soc.* **2022**, *70*, 102010. [\[CrossRef\]](#)
26. Yusof, M.M.; Kuljis, J.; Papazafeiropoulou, A.; Stergioulas, L.K. An evaluation framework for Health Information Systems: Human, organization and technology-fit factors (HOT-fit). *Int. J. Med. Inform.* **2008**, *77*, 386–398. [\[CrossRef\]](#)

27. Kosasi, S.; Vedyanto, V.; Ayu Eka Yuliani, I.D. Appropriate Sets of Criteria for Innovation Adoption of IS Security in Organizations. In *Proceedings of the 2018 5th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Malang, Indonesia, 16–18 October 2018*; IEEE: New York, NY, USA, 2018; pp. 608–613, ISBN 978-1-5386-8402-3.
28. Amyra, N.; Mohd, S.M. Adoption of Digital Forensic Practice: A Framework Development for Malaysian Organizations. *J. Electr. Syst.* **2024**, *20*, 5764–5773.
29. Kumar, S.; Biswas, B.; Bhatia, M.S.; Dora, M. Antecedents for enhanced level of cyber-security in organisations. *J. Enterp. Inf. Manag.* **2021**, *34*, 1597–1629. [[CrossRef](#)]
30. Alhammad, A.; Yusof, M.M.; Jambari, D.I. Evaluating applied security controls for safeguarding medical device-integrated electronic medical records. *J. Eval. Clin. Pract.* **2025**, *31*, e14140. [[CrossRef](#)] [[PubMed](#)]
31. Dwivedi, Y.K.; Wade, M.R.; Schneberger, S.L. *Information Systems Theory*; Springer: New York, NY, USA, 2012; ISBN 978-1-4419-9706-7.
32. Sahu, A.; Mao, Z.; Wlazlo, P.; Huang, H.; Davis, K.; Goulart, A.; Zonouz, S. Multi-Source Multi-Domain Data Fusion for Cyberattack Detection in Power Systems. *IEEE Access* **2021**, *9*, 119118–119138. [[CrossRef](#)]
33. Alsolami, T.; Alsharif, B.; Ilyas, M. Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things. *Sensors* **2024**, *24*, 5937. [[CrossRef](#)]
34. Dolezel, D.; McLeod, A. Cyber-Analytics: Identifying Discriminants of Data Breaches. *Perspect. Health Inf. Manag.* **2019**, *16*, 1a.
35. Ignatovski, M. For-profit versus non-profit cybersecurity posture: Breach types and locations in healthcare organisations. *Health Inf. Manag.* **2024**, *53*, 198–205. [[CrossRef](#)]
36. Yaraghi, N.; Gopal, R.D. The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights from an Empirical Study. *Milbank Q.* **2018**, *96*, 144–166. [[CrossRef](#)]
37. Abbiati, G.; Ranise, S.; Schizzerotto, A.; Siena, A. Merging Datasets of CyberSecurity Incidents for Fun and Insight. *Front. Big Data* **2020**, *3*, 521132. [[CrossRef](#)]
38. Thomas, O.; Munir, M.B.; Tine, J.-M.; Rahman, M.; Cai, Y.; Akbar, K.A.; Uddin, M.N.; Khan, L.; Hockstad, T.; Chowdhury, M. Transportation Cyber Incident Awareness through Generative AI-Based Incident Analysis and Retrieval-Augmented Question-Answering Systems. *arXiv* **2025**, arXiv:2508.02523.
39. Simon, M.; Looten, V. Description of Data Breaches Notifications in France and Lessons Learned for the Healthcare Stakeholders. *Stud. Health Technol. Inform.* **2020**, *275*, 192–196. [[PubMed](#)]
40. Ronquillo, J.G.; Erik Winterholler, J.; Cwikla, K.; Szymanski, R.; Levy, C. Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information. *JAMIA Open* **2018**, *1*, 15–19. [[CrossRef](#)] [[PubMed](#)]
41. Zängerle, D.; Schiereck, D. Modelling and predicting enterprise-level cyber risks in the context of sparse data availability. *Geneva Pap. Risk Insur. Issues Pract.* **2023**, *48*, 434–462. [[CrossRef](#)]
42. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur. Issues Pract.* **2022**, *47*, 698–736. [[CrossRef](#)]
43. Portalatin, M.; Keskin, O.; Malneedi, S.; Raza, O.; Tatar, U. Data Analytics for Cyber Risk Analysis Utilizing Cyber Incident Datasets. In *Proceedings of the 2021 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 29–30 April 2021*; IEEE: New York, NY, USA, 2021; pp. 1–6, ISBN 978-1-6654-1250-6.
44. Waedlich, R.; Baumann, T. Digitalisierung und innovatives Cyber- und IT-Risikomanagement. In *Handbuch Klinisches Risikomanagement*; Euteneier, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2024; pp. 631–652, ISBN 978-3-662-67564-9.
45. U.S. Department of Health and Human Services Office for Civil Rights. Breach Notification. Available online: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html> (accessed on 16 May 2025).
46. Center for International Security Studies at Maryland. Cyber Events Database. Available online: <https://cissm.umd.edu/research-impact/publications/cyber-events-database-home> (accessed on 27 November 2025).
47. European Repository of Cyber Incidents. EuRepoC Database. Available online: <https://eurepoc.eu/database/> (accessed on 27 November 2025).
48. Privacy Rights Clearinghouse. Data Breach Chronology. Available online: <https://cdn.shopify.com/s/files/1/0571/5489/5955/files/README.pdf?v=1739201304> (accessed on 27 November 2025).
49. TI Safe. Incident Hub. Available online: <https://hub.tisafe.com/> (accessed on 27 November 2025).
50. U.S. Department of Health and Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Available online: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed on 14 October 2025).
51. Burke, W.; Stranieri, A.; Oseni, T.; Gondal, I. The need for cybersecurity self-evaluation in healthcare. *BMC Med. Inform. Decis. Mak.* **2024**, *24*, 133. [[CrossRef](#)]
52. Kallio, H.; Pietilä, A.-M.; Johnson, M.; Kangasniemi, M. Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *J. Adv. Nurs.* **2016**, *72*, 2954–2965. [[CrossRef](#)]
53. Haberl, A.; Fleiß, J.; Kowald, D.; Thalmann, S. Take the aTrain. Introducing an interface for the Accessible Transcription of Interviews. *J. Behav. Exp. Financ.* **2024**, *41*, 100891. [[CrossRef](#)]

54. Braun, V.; Clarke, V. Using thematic analysis in psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [CrossRef]
55. Quader, F.; Janeja, V.P. Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies. *J. Cybersecur. Priv.* **2021**, *1*, 638–659. [CrossRef]
56. Klauber, J.; Geraedts, M.; Friedrich, J.; Wasem, J. (Eds.) *Krankenhaus-Report 2019*; Springer: Berlin/Heidelberg, Germany, 2019; ISBN 978-3-662-58224-4.
57. Ridic, G.; Gleason, S.; Ridic, O. Comparisons of health care systems in the United States, Germany and Canada. *Mater. Sociomed.* **2012**, *24*, 112–120. [CrossRef]
58. Goldschmidt, A.J.W.; Marquardt, K.; Groneberg, D.; von Eiff, W. Aufbruch oder verspielte Zukunft der Krankenhausbigitalisierung in Deutschland. *Zbl Arbeitsmed* **2023**, *73*, 170–181. [CrossRef]
59. Dobrovolska, O.; Ortmanns, W.; Dotsenko, T.; Lustenko, V.; Savchenko, D. Health Security and Cybersecurity: Analysis of Interdependencies. *Health Econ. Manag. Rev.* **2024**, *5*, 84–103. [CrossRef]
60. Qureshi, R.; Koo, I. A Comprehensive Survey of Cybersecurity Threats and Data Privacy Issues in Healthcare Systems. *Appl. Sci.* **2026**, *16*, 1511. [CrossRef]
61. Busetti, S.; Scanni, F.M. Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Gov. Inf. Q.* **2025**, *42*, 102000. [CrossRef]
62. 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, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148: NIS 2 Directive. 2022. Available online: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> (accessed on 14 December 2025).
63. Gabriel, M.H.; Noblin, A.; Rutherford, A.; Walden, A.; Cortelyou-Ward, K. Data breach locations, types, and associated characteristics among US hospitals. *Am. J. Manag. Care* **2018**, *24*, 78–84.
64. Liu, V.; Musen, M.A.; Chou, T. Data breaches of protected health information in the United States. *JAMA* **2015**, *313*, 1471–1473. [CrossRef]
65. U.S. Department of Health and Human Services. Covered Entities and Business Associates. Available online: <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html> (accessed on 4 December 2025).
66. Alder, S. Healthcare Data Breach Statistics. Available online: <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (accessed on 17 January 2025).
67. Munoz-Cornejo, G.; Sakowski, J.; Lee, J.; Parks, A. Analyzing the urban–rural divide: The role of location, time, and breach characteristics in U.S. hospital security incidents, 2012–2021. *Discov. Health Syst.* **2024**, *3*, 38. [CrossRef]
68. Choi, S.J.; Johnson, M.E.; Lehmann, C.U. Data breach remediation efforts and their implications for hospital quality. *Health Serv. Res.* **2019**, *54*, 971–980. [CrossRef]
69. Salim, M.M.; Rathore, S.; Park, J.H. Distributed denial of service attacks and its defenses in IoT: A survey. *J. Supercomput.* **2020**, *76*, 5320–5363. [CrossRef]
70. Madanian, S.; Chinbat, T.; Subasinghage, M.; Airehrour, D.; Hassandoust, F.; Yongchareon, S. Health IoT Threats: Survey of Risks and Vulnerabilities. *Future Internet* **2024**, *16*, 389. [CrossRef]
71. Boutemour, J.; Lella, I.; Bakatsus, I.; Chatzichristos, G.; Foley, K.; Leskinen, J.; Otcenasek, J.; Ziolk, D. Enisa Threat Landscape. 2025. Available online: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf (accessed on 13 November 2025).
72. Munoz Cornejo, G.; Lee, J.; Russell, B.A. A thematic analysis of ransomware incidents among United States hospitals, 2016–2022. *Health Technol.* **2024**, *14*, 1059–1070. [CrossRef]
73. Adam, S. The State of Ransomware 2025: Findings from an Independent Survey of 3400 IT and Cybersecurity Leaders Across 17 Countries Whose Organizations Were Hit by Ransomware in the Last Year. Available online: <https://news.sophos.com/en-us/2025/06/24/the-state-of-ransomware-2025/> (accessed on 24 July 2025).
74. Tikanmäki, I.; Ruoslahti, H. Human Factors Make or Break Cybersecurity! *Inf. Secur. Int. J.* **2024**, *55*, 245–259. [CrossRef]
75. Giansanti, D.; Gulino, R.A. The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives. *Healthcare* **2021**, *9*, 1653. [CrossRef] [PubMed]
76. Waddell, M. Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. *Healthc. Manag. Forum* **2024**, *37*, 13–16. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.