Expert Perspectives on Information Security Awareness Programs in Medical Care Institutions in Germany

Jan Tolsdorf[1](✉) and Luigi Lo Iacono[2]

[1] The George Washington University, Washington D.C., USA
jan.tolsdorf@gwu.edu

[2] Bonn-Rhein-Sieg University of Applied Sciences, Sankt Augustin, Germany
luigi.lo_iacono@h-brs.de

Abstract. Human factors play a crucial role in the increasing number of information security incidents in the medical sector. European medical institutions, especially in Germany, have long neglected these factors, lacking legal obligations. Legislators recently responded with new regulations mandating medical facilities to implement information security awareness programs. To gain insights into how German medical institutions approach this challenge, we conducted an interview study with six information security experts from the medical sector. Using thematic analysis, we find that human factors are seen as both a risk and an opportunity for information security. We identified various target groups, goals, and obstacles for the implementation of information security awareness programs. Existing structures and regulations promote the risk of a checklist mentality, potentially resulting in ineffective measures being implemented. One great opportunity for effective information security awareness programs lies in the exchange with staff units on safety and hygiene, who have decades of experience with awareness programs in medical facilities. The study results serve for future research and tailored awareness programs in the medical sector.

Keywords: Information Security Awareness · Medical Care · Expert Interview Study

1 Introduction

Healthcare facilities are repeatedly affected by information security incidents and attacks from cyberspace [4,11,13,33], leading to medical data breaches and temporary interruptions and delays in patient care [37,43]. Indeed, in 2023, the healthcare sector was among the top three targeted sectors and leading in the number of incidents with data breaches [2]. Studies indicate that human factors play a decisive role here, showing that they make up for 52% [53] to 92% [18] of security incidents in hospitals in the United States (U.S.) and the European

A. Moallem (Ed.): HCII 2024, LNCS 14729, pp. 98–117, 2024.
https://doi.org/10.1007/978-3-031-61382-1_7

Union (EU) [2]. Clearly, the success or failure of maintaining a healthcare facility's information security depends largely on its staff's actions and ability to make safe decisions with respect to information security [7,27]. However, unlike in the U.S., there is no EU-wide explicit legislation for dealing with information security and data protection issues in the healthcare sector. This situation has made the medical sector lagging behind on these issues in the EU [12,35]. Germany is one of the member states that has addressed this shortcoming by introducing national regulations, including mandatory consideration of human factors by raising Information Security Awareness (ISA). This poses enormous challenges for many medical facilities, as many have to make up for their deficits from previous years. Given that the healthcare sector in Germany has little experience with human factors in information security and ISA, the question arises as to what challenges facilities face in implementing and rolling out ISA programs.

To gain initial insights, we conducted an interview study with six cybersecurity experts from five different medical institutions and service providers in Germany between May and June 2022. The experts acknowledged the importance of the human factor, but emphasized that the main problem lies in an insecure infrastructure and organizational culture that either overburdens medical staff or neglects the human factor altogether. Consequently, technical measures are prioritized to minimize reliance on the "human firewall." The experts emphasized the importance of creating a basic understanding of information security, promoting self-efficacy, offering practical solutions to enhance the learning experience, and not seeing ISA as an IT problem. However, significant challenges remain, including the lack of ISA materials specifically tailored to the medical sector and time and resource constraints for IT and medical staff. Hospitals seem hesitant to conduct evaluations of potential interventions due to concerns about objections from staff councils or the lack of usefulness of evaluation results, as they are also not required to provide evidence of effectiveness in audits. The study highlights the potential benefits of sharing knowledge with other safety and hygiene departments to improve the implementation of ISA in medical facilities and to benefit from the experience of others. Our findings contribute to a better understanding of the frameworks that need to be considered for implementing effective ISA programs in medical institutions.

2 Background

Below, we introduce the regulatory framework on information security in Germany, provide a working definition of ISA and review related work.

2.1 Information Security in Healthcare Facilities in Germany

Information security in healthcare facilities in Germany has historically been an area of limited attention and investment. In response to an increase of cyberattacks on hospitals and other critical infrastructure facilities, the German legislature responded by enacting the IT Security Act in 2015. This law mandates hospitals with an annual admission of 30,000 full stationary cases to implement a sector-specific information security standard. The standard is known as B3S [1] and was successfully accredited in 2019. In the wake of further changes by the legislature, all other hospitals and medical practices have also been required to implement information security measures since 2021. As a result, the issue of information security in the medical sector has gained in importance in Germany in recent years. Regarding the B3S, it essentially provides for the implementation of an Information Security Management System (ISMS) and introduces the two additional protection goals of patient safety and treatment effectiveness. Next to obligations on implementing well-defined structures and protection measures, the B3S specifically requires accounting for information security threats posed by social engineering, identity misuse like phishing, and human error in general. Hospitals belonging to the critical infrastructures are thus obliged to raise their employees' ISA by running trainings at least every two years. Proof of implementation is part of the mandatory audits. Failure to comply with the B3S may result in fines ranging from €100,000 to €20 million.

2.2 Information Security Awareness in the Medical Care Sector

It has been argued early on that an adequate ISA is a necessary prerequisite for the secure handling of information systems in organizations [48]. The literature has defined ISA [27] (1) as a state of security-related behavior, (2) as a cognitive state of mind in the form of general and specific knowledge and understanding of security problems and their (possible) consequences [3], and (3) as a continuous process to achieve this state of mind *"aimed at changing individuals' perceptions, values, attitudes, behaviors, norms, work habits, and organizational culture and structures toward secure information practices"* [51]. Since ISA has a positive impact on the information security of organizations, numerous approaches and methods have been developed to increase ISA. Today, guidance and best practices are available to organizations from government agencies (e.g., ENISA [16] and NIST [52]) and academia [3,21]. In the remainder of this section, we review related work on ISA in the medical care sector.

Quantifying Levels of ISA and Drivers of Behavior. A number of studies has aimed at quantifying the level of ISA among staff in healthcare facilities. Some work has developed analysis methods and new scales that are supposed to be particularly useful for surveying ISA in health care [10,29]. Few surveys provide snapshots of the extent of ISA in healthcare facilities. A Spanish study highlighted issues in medical staff's security practices, including weak passwords and unawareness of data protection procedures [20]. A Polish survey found a gap between theoretical knowledge and practical application of cybersecurity measures in healthcare [19]. Danish and Kuwaiti studies revealed positive correlations between ISA and overall system satisfaction among healthcare professionals [5,47]. Physicians in Kuwait, however, exhibited lower ISA, possibly due to high workloads hindering participation in security training. A survey in Greece, Portugal, and Romania exposed deficiencies in cybersecurity training for both IT-personnel and medical staff, with limited awareness of threats but positive attitudes towards security policies [24].

Beyond quantifying ISA, numerous studies have examined antecedents of secure behavior and compliance with healthcare information security policies using sound theoretical models. These studies have recently been summarized in a systematic literature survey, identifying a total of 31 individual factors and 26 organizational factors [46]. The results indicate that factors such as self-efficacy, perceived severity, attitudes, subjective norms, ISA, and organizational support are found to favor secure behaviors. ISA is special in that it has both positive effects on desirable behavior and negative effects on undesirable behavior like intentional misconduct, thus favoring secure behavior.

Education and Training. Studies in Canada and the EU revealed several challenges for executing training and education on information security in hospitals, including limited uninterrupted time by medical staff, outdated IT infrastructure and software, lack of IT standardization, lack of support, and difficulty accessing (e-)learning modules [9,19,26,41]. While shorter e-learning modules had a more positive impact on ISA compared to longer modules [9], the use of one-size-fits-all solutions proved to be insufficient, as the demographics of hospital staff are highly diverse and different staff may feel that the content is irrelevant or outdated to them [9,19,26,41]. In this regard, few studies have focused on designing and developing education and training material on information security for medical care facilities. Early approaches stayed purely on a theoretical basis [8,30]. In [22], a comprehensive framework for ISA programs in the health sector is presented, collaborating with a Malaysian university hospital. The framework guides healthcare institutions in determining content, selecting educational methods, developing material, and implementing and evaluating ISA programs. The authors extended the framework to include a serious game, demonstrating increased ISA levels and willingness to participate in training among clinic staff in a study, though long-term effects were not investigated [23].

Drivers of Misconduct and Security Incidents. A recent interview study with 50 IT-personnel and medical staff across Ireland, Italy and Greece identified seven common insecure behaviors and their underlying drivers [12,14]. Facilitators of insecure behavior were found to be lack of awareness and training, shadow working processes such as sharing passwords, prioritization of seeing patients and medical expenditure over cybersecurity, and environmental factors like high workload but poor IT infrastructure. Barriers to security included perceiving security as a hindrance to productivity and patient care, poor awareness of consequences, and a lack of policies and reinforcement. An interview study in the UK investigated how employees in a health board perceive and experience information governance policies [44]. The findings highlight issues such as feeling controlled, lack of support, and pressure to comply. The study recommends mediation strategies such as recognition and reward systems, incident response processes, improved communication, and a strong security culture. An interview study with 21 Saudi medical interns and 8 IT-personnel of a university hospital explored neutralization techniques used by medical staff to justify security policy violations [6]. It found that medical interns' security behavior is mainly influenced by their peers and superiors. Justifications for misconduct included prioritizing job completion over security, sharing accounts to assist colleagues with their work, attributing similar behavior to others, and denying any harm caused. An ethnographic study conducted in the emergency department on HIPPA compliance in the U.S. showed that staff often find alternative solutions or workarounds to address the challenge of balancing information availability (e.g., patient data) and privacy compliance [39]. The study concluded that accountability for privacy violations in collaborative environments is often unclear due to interactions among medical staff and varying privacy practices, leading to conflicts and ambiguity. The same authors interviewed 20 IT-personnel, finding that their understanding of unsafe workarounds used by medical staff is limited [15]. This hinders finding suitable solutions and implementing more effective strategies by IT. An interview study with nine privacy officers from U.S. hospitals indicated that organizational factors are the primary causes of human errors resulting in privacy breaches [36]. Active involvement of upper management in policy enforcement and workflow analysis is considered crucial for effective error management. Human factors ranked second in importance. Training programs and awareness initiatives were highlighted as effective measures to address human errors. An interview study with 19 Information Security Officers (ISO) in U.S. hospitals examined key challenges and defense strategies in relation to information security under HIPAA regulations [28]. The findings indicate that ISOs perceive the IT landscape and infrastructure in hospitals as highly complex, with numerous devices and systems to manage. The organizational structure of hospitals was also identified as complex, posing difficulties in achieving alignment across multiple clinics. Furthermore, inadequate financial and personnel resources emerged as significant challenges in the implementation of effective information security measures.

2.3 Contributions

Our literature review reveals that there is currently a dearth of insights from the field on how healthcare facilities actually approach the implementation of ISA programs. Our study aims to address this gap by providing valuable insights from Germany, where the medical sector is still quite inexperienced in implementing ISA programs. Unlike previous research, our study specifically examines the perspectives of information security experts, with a particular focus on human factors and ISA. Furthermore, our study identifies the top priorities identified by field experts in terms of program targets, target groups, and training methods for successful ISA program implementation. These findings contribute to the knowledge base in the field and offer implications for research and practitioners on how to support healthcare organizations aiming to enhance their ISA practices.

3 Methodology

To gain the necessary insights, we conducted six semi-structured interviews with experts on information security in medical institutions in Germany between May and June 2022. Below, we explain how we addressed ethical concerns, provide details on our study and participants, and discuss limitations of our study.

3.1 Ethical Concerns

To address ethical concerns, we adhered to the German Sociological Association's code of ethics and the standards of good scientific practice of the German Research Foundation. Our study design and data management plan were approved by our institution's data protection officer, complying with national and European data protection regulations. Personal data collection was performed on our institution's servers. Participants were informed and gave consent before interviews. After separating audio and video tracks and removing identifiers, we used a German transcription service, ensuring adherence to privacy guidelines. Raw data were deleted post-transcription. Contact information was stored separately on encrypted drives, and data processing occurred on secure computer and network drives. Raw data access is limited to a selected group of researchers.

3.2 Study Procedure and Analysis

In the interviews, we welcomed our participants, provided information about the study, and obtained informed consent for audio and video recordings. The interview began with introductions, followed by questions about the unique aspects of information security in medical facilities, types of attacks faced, and the impact on patients. We then asked about our participants' experiences with the human factor in information security and explored their experiences with ISA programs, including implementation status, goals, and target groups addressed. We also discussed the creating of ISA materials, and preferred delivery methods. We specifically asked for activities on evaluating the effectiveness of ISA measures, measuring success, and the utilization of resulting information. Additionally, we touched upon the expected efficiency and costs associated with implementing ISA programs. Participants were asked to summarize the main problems and potential improvements of ISA programs. At the end of the interview, participants had the opportunity to add any additional points to the discussion. We then concluded the recording and addressed any follow-up questions participants had about the project or other topics. The interviews lasted between 34 and 56 min. All interviews were conducted online and audio recorded. The transcripts were analyzed using Thematic Analysis in the MAXQDA software.

3.3 Participants

We recruited participants using expert sampling with elements of random sampling [17]. In total, six participants were recruited from five different facilities and service providers. Our participants break down into four males and two females. Three individuals were aged 35 to 44, two individuals were aged 45 to 54, and one individual was aged 55 to 64. Furthermore, four individuals worked directly at medical care facilities, whereas two individuals worked in external consulting, auditing, or training. The four individuals with direct employment had worked for the respective facility for between zero and four years. In contrast, the participants with external consulting roles had been in their current positions for over 10 to over 20 years. An overview of the demographics of our participants is presented in Table 1.

Table 1. Overview participants

ID	Job title/job description	Job experience
P1	Information Security Officer	0–4 years
P2	Information Security Manager	0–4 years
P3	Consultant IT, information security, data protection	≥20 years
P4	Auditor, trainer, consultant for quality management, patient safety, information security	10–19 years
P5	ISMS Project Leader & Manager	0–4 years
P6	IT Manager, Project Manager	0–4 years

Detailed demographic backgrounds are omitted to protect the individuals and their organizations from being identified.

3.4 Limitations

The results of our study are certainly not representative of all medical facilities in Germany. Nevertheless, our respondents cover a broad spectrum from hospitals with 1k to 10k employees, to medium-sized medical practices. Recruitment and self-disclosure biases are likely, as not all organizations responded to our invitation and our respondents disclosed only the information they wished to disclose. Our results also do not form a complete or saturated picture. By capturing expert perspectives on ISA in the medical field, our study helps fill research gaps and provide a baseline for desperately needed future research.

4 Findings

Below, we present the findings of our interview study, grouped according to the hierarchy of our coding procedure.

4.1 The Human Factor and the “Human Firewall”

A fundamental assumption underlying the (mandatory) implementation of ISA programs in medical facilities is acknowledging the crucial role of the human factor. With this in mind, we first asked our participants to explain the role they attribute to the human factor in information security in medical institutions. In this regard, our participants engaged in a discussion on the human factor, recognizing its dual nature as both a risk and an opportunity for information security. While the human factor was acknowledged as central to information security, it was emphasized that it should not be seen in isolation, but rather as a link in the chain or a “measure” itself. Our participants reported that successful attacks are frequently the result of a series of organizational and technical circumstances, spanning across various departments and responsibilities, rather than the fault of an individual. This concatenation of events and failures within the overall construct of the organization contributed to the actual damage incurred. Still, the human factor was seen as the decisive factor that triggers a security incident:

> *“So the human factor is the final, decisive factor. And the human factor is the one, in my experience, that currently [...] ensures that malware is triggered just in case.”* (P3)

Moreover, negligence and unintentional misconduct were identified as key factors associated with the human factor as a risk. Participants highlighted instances such as leaving workstations unlocked, failing to secure access cabinets, or leaving patient files unattended. In addition, the prevalence of phishing emails was a notable concern, with five participants associating the human factor with this issue. Emails were identified as gateways for attacks, often designed to entice employees, including those in management positions, with professionally crafted content and attachments. Despite efforts to raise awareness and educate employees about risks, our participants acknowledged that risky behavior persists, with employees still falling victim to phishing attacks. To reduce the impact of human error, three participants discussed the importance of creating contact channels for employees to report back in case of an incident. Our participants explained that direct (feedback) reports are incredibly helpful for them to initiate countermeasures. In this context, the problem was raised that on weekends often only the first level support could be reached, but they do not have an information security background. Therefore, it is absolutely necessary to provide comprehensible procedural instructions and to establish reporting chains.

As opposed to seeing the human factor as a risk only, our participants continued to discuss the human factor from the perspective of viewing it as an opportunity for information security. In this context, three participants referred to the “human firewall” that must be trained and makes up a *“a central component in addition to all the technical security measures.”* (P1) Generally speaking, however, our participants agreed that the “human firewall” should be the last resort. As such, three participants expressed high confidence in technical solutions and security concepts to either reduce risks by avoiding the human factor or mitigate the consequences. Specific technical solutions included separating networks, performing vulnerability scans, patch management, email filtering, anomaly detection, log analysis, implementing a roles and rights concept, and taking client or end-point security measures such as installing virus scanners. For long-term management of information security issues, one participant emphasized the need for better overall approaches to replace inherently insecure IT systems and practices with inherently secure solutions to reduce the burden on the "human firewall." At last, participants highlighted the IT personnel's responsibility to make a significant contribution to information security, as *"IT is of central importance and is also very, very central in many places and can also prevent a lot."* (P1)

4.2 Goals, Target Groups, and Implementation of ISA

Interviews revealed that the medical facilities overseen by our experts generally lack experience with ISA programs. Subsequently, we outline our participants' strategies for bridging this gap, specifying key objectives for ISA, identifying target staff groups, and assessing challenges associated with ISA implementation.

Expected Goals of ISA. Our participants emphasized the importance of fostering a fundamental understanding of information security as a key objective of ISA measures. Continuous sensitization was highlighted as crucial in this regard, for example, by continually reinforcing the significance of handling sensitive data responsibly and the potential consequences of lapses in security:

> *"But [awareness] doesn't come from one seminar, of course. It is a process of development. And that is also the great challenge with this topic. I know this from other topics. It's the same with quality management, it's the same with error management. It's the same with awareness management. So this has to be integrated into everyday life on a regular, regular basis. And that will be the big challenge"* (P4)

Furthermore, participants emphasized the need to expand the perspective on information security beyond being solely an "IT problem." It was noted that seemingly unrelated issues, such as open access doors or momentarily unattended offices, can have security implications and should be recognized as such. However, they noted that these are generally not currently associated by employees with information security issues. Moreover, our participants emphasized they want to provide helpful and specific content, such as password guidelines and instructions, with practical significance. Practical problems and their corresponding solutions can be highlighted to create "Aha!" moments and empower staff with a sense of self-efficacy:

> *"[T]here is always a certain amount of fear [...], because they [...] think that the topic might be too complicated to really understand. [But] everywhere we go now, there is a great 'Aha!-experience'. [...] And this 'Aha!-experience' must be maintained. And not to become anxious now [...]. And*

> *this 'Aha!-experience' is simply there, because they now know, hey, there are these dangers, but I have now been equipped with a toolbox to be able to decide [...] what could be dangerous for me or not."* (P3)

Target Groups. In total, we identified seven target groups for which our participants assumed that ISA measures would be useful: (1) physicians, (2) nursing staff, (3) IT staff, (4) administrative staff, (5) management staff, (6) patients, and (7) visitors. However, participants who were already planning or implementing ISA programs generally prioritized only one to three target groups at a time. When implementing measures, our participants stated that in practice, no distinction was usually made between different target groups, i.e., the same content was taught to all target groups. In response to our explicit questions in the interviews, they also stated that they currently had no concrete plans as to how and whether they wanted to address different target groups with different content.

Key Issues and Challenges in ISA Implementation. Our participants highlighted several key issues and challenges in the implementation of ISA measures. One prominent concern was the lack of motivation, understanding, and overestimation of employees' own capabilities. It was noted that many employees viewed ISA training as a mandatory task and simply went through the motions without fully grasping the importance of information security. This lack of engagement was observed across all levels of the organization, including senior-level staff who exhibited overconfidence in their knowledge and abilities. One participant acknowledged that this mindset could lead to security breaches.

Time constraints emerged as a significant challenge, particularly for medical personnel responsible for critical patient care. Limited time and competing priorities hindered their engagement with ISA initiatives. One participant explained that ISA measures must certainly not impede patient care, yet they recognized that shortage of time dedicated to these topics would eventually also pose a risk to patient care. As our participants underscored the need for effective strategies to integrate ISA measures into the daily routines of healthcare professionals to foster long-term behavioral changes, they pointed to the possibility of pursuing participatory models in the future:

> *"I think we really have to ask the hospital staff and sit down with the nursing director to see how we can eliminate certain conditions that we would find during an inspection without hindering them in their work."* (P5)

Furthermore, participants identified the inadequacy of existing ISA materials, particularly in the context of the medical field. Generic content and irrelevant examples, such as phishing simulations with emails unrelated to healthcare, failed to resonate with medical staff. Overall, participants agreed that there was a clear need for tailored and specific awareness campaigns that address the unique challenges faced by healthcare professionals. Recommendations and guidance should be actionable and relevant to the healthcare environment to maximize their impact. In light of these challenges, participants emphasized the importance of delivering focused and meaningful awareness programs while avoiding excessive warnings that could desensitize employees:

> *"And often what I experience is that many generic recommendations for action are always channeled watering can-like to everyone. Although very few people can do anything with these recommendations and the perfect example is always this statement with 'please pay attention to the trustworthiness of this email' and the like, without even laying out what I understand by this [...]"* (P2)

4.3 Development and Evaluation of ISA Materials

Lastly, our interviews delved into how participants and their organizations approach the development and provision of ISA material, including their strategies for maintaining and ensuring its quality.

Teaching Methods and Topics. The delivery methods for ISA discussed by our participants encompassed a range of approaches, including face-to-face training, online training, flyers, brochures, screensavers, and physical items like cell phone display cleaning cloths and writing pads. While some participants had experience with these methods, others expressed intentions to incorporate them in the future. Additionally, plans to introduce e-learning platforms, icons, posters, quizzes, short lectures, and intranet articles were mentioned. The topics covered thus far focused primarily on data protection, user guidelines, and email, with future plans to expand into non-IT areas such as paper file processing and access controls. When evaluating the effectiveness of different delivery methods, our participants generally had positive views regarding computer-assisted and instructor-led methods, particularly in online formats. Instructor-led methods were valued for facilitating discussions and providing direct feedback to the trainer. Computer-based methods, especially online ones, were praised for their increased awareness frequency and flexibility, since *"employees can deal with it more frequently than these events, which are only held once a year."* (P6) In contrast, offline computer-aided methods were seen as having limited applications, while conventional methods like handouts and posters were criticized for relying too heavily on employee initiative and potentially failing to achieve their intended impact:

> *"Handouts are of course very nice, posters, stickers, newsletters. The problem is, do you produce it for the garbage can? Is it really received? You don't know."* (P5)

One of our participants referred to similar problems with hand hygiene in medical care facilities:

> *"[T]he conventional methods that you have also listed here, all okay. But you won't reach anyone with them, because no one has time to read anything anymore. [...] So, we have always tried to make sure that people who work in these [(healthcare)] facilities disinfect their hands according to a very specific procedure. [...] This is somewhat similar to what we are planning now [with information security]. [...] So how do you get that to the people? There are an infinite number of posters, but they don't work at all."* (P4)

Preparation and Quality Assurance. Our participants reported that efforts are made to ensure the quality of ISA materials either by contracting external service providers with appropriate expertise in the respective field. Or by relying on journals and sources of authority to create the content themselves. In the latter case, for example, information was taken from the Federal Office for Information Security (BSI) or the state data protection supervisory authorities. However, personal experience also went into the creation of the materials. As a result, the materials must be updated regularly for quality assurance purposes.

In the future, our participants explained, they would like to rely more on collaborative methods. In particular, information security departments that are relatively young would like to enter into a more intensive exchange with other departments which have longer experience with the topic of sensitization and awareness. Specifically, the departments of corporate communications and patient safety were mentioned. But also the exchange with external specialist companies was mentioned as a possibility.

Evaluation and Measurability. The evaluation and measurability of ISA measures seemed partly interesting and partly uninteresting to our participants. Those seeing added value were interested in incorporating the evolution results into future awareness-raising activities. However, none of our participants reported any systematic evaluation already taking place. Instead, they relied on unsystematic qualitative feedback, if any, because they worried about conflicts with the staff council:

> *"We can't really ask like that, [(because we work in)] public service. We have a very strong staff council, which goes to the barricades at the mere smell that there might be a performance role for people or employees. Therefore, it is quite difficult."* (P5)

4.4 Structural Problems of Information Security in Medical Care

Our participants delved into additional challenges related to information security in medical care that go beyond human factors and ISA alone. While not the primary focus of our study, we find it crucial to acknowledge and report on these challenges to provide a comprehensive understanding of the issues hindering information security in medical care, as perceived by our participants.

Impediments. Our participants expressed awareness that information security measures potentially impede healthcare, slowing down healthcare treatment and innovation. Despite concerns that constant technological progress and increasing connectivity are raising the threat level, they nevertheless agreed that risk avoidance is neither a feasible nor a satisfactory solution. This is especially the case for university hospitals. However, we find that flawless integration of information security into workflows is also often impeded by insecure designed infrastructure, procedures, and medical devices. Participants highlighted the widespread use of email, despite it being unencrypted and vulnerable to identity fraud and human error. One participant compared the situation with a flawed postal system, explaining that *"there's something wrong with the postal system, if I go to the mailbox and have to worry every time if there's a bomb in there."* (P3) However, the demand from patients or use cases has led to the acceptance and tolerance of such insecure communication channels. Additionally, participants noted that medical device providers prioritize the benefits of their products for patient care without adequately considering the associated information security risks, particularly in relation to human error, such as failing to lock computers.

Missing and Inconsistent Processes and Structures. The heterogeneous environment of university hospitals, akin to a corporate structure with multiple clinics operating under the hospital's name, adds to the complexity of information security. This setup allows certain freedoms for the clinics, which may not always adhere to centralized services or specifications. However, this setting favors lack of early communication and feedback on planned information security measures. One participant stressed the importance of getting early feedback, explaining that often *"we have really great ideas at our desk, spread them around and then somehow get grumbling after three weeks 'we can't work properly anymore'."* (P5) Next to inconsistencies within the organization, participants also criticized the lack of networks or organizations specifically dedicated to information security in the healthcare sector:

> *"For example, there is the Patient Safety Action Alliance, where there are always working groups. Whether it's medical devices, whether it's hygiene, whether it's patient safety. [...] But there is no such thing for information security."* (P4)

Resource Shortage. Resource shortage presents a significant challenge, according to our participants, impacting various aspects of implementation and enforcement of information security. Staff shortages among medical personnel and IT staff hinder the ability to effectively respond to risks and act preventively. Especially, the scarcity of resources and personnel within the IT department was seen as a challenge in rolling out ISMS to the entire clinic. Additionally, medical, therapeutic, and nursing staff were thought to feel overwhelmed already by the additional requirements they had to fulfill due to staff shortages. In this regard, sensitizing management to information security issues and securing the necessary resources becomes crucial for addressing these common problems, to allocate the required funds:

> *"I think the biggest problem is that management needs to have a greater understanding that data protection and information security are becoming more and more important. [...] And I believe that as long as this understanding is not there, and no funds are made available for this purpose—because it cannot be achieved through manpower alone—nothing will change in a big way."* (P6)

5 Discussion

Below, we summarize our main findings and discuss implications of the results.

5.1 Summary

Our interview study with six information security experts in the healthcare sector, including professionals from hospitals and consulting, provides insights into various aspects of information security and especially ISA programs in medical facilities. Our study confirms challenges related to organizational structures, legal requirements, and limited resources for implementing and expanding ISMS in medical care institutions. The experts also highlighted the ongoing presence of security vulnerabilities and the challenges posed by increasing computerization and networking. These findings highlight that the medical sector cannot overlook technological advancements, especially given the proliferation of heterogeneous devices that increase vulnerability. Manufacturers' focus on individual device components, rather than the overall information security concept, exacerbates this vulnerability. In this context, the surveyed experts recognized the relevance of the human factor for information security. However, they pointed out several unresolved issues in the medical field that currently take precedence over the human factor. They emphasized the need to prioritize prevention and defense measures, such as network and endpoint security, and highlighted the urgency of addressing these pervasive threats, especially given the medical sector's efforts to catch up in this area [13].

Nevertheless, our results confirm the common view in ISA research that the human factor poses a risk and an opportunity for information security [12,13]. In particular, phishing attacks were presented as an acute problem, which coincides with recent research [40]. For countervailing the risks posed by the human factor, our interviewees explained the importance of technical measures to minimize the attack surface. Meanwhile, they emphasized the importance of the "human firewall" in case of everything else failing. In terms of support through ISA programs, we identified specific objectives. The main goal is creating a basic understanding of information security throughout medical facilities and to instill a sense of self-efficacy rather than fear in employees, which has known favorable effects on secure behavior [46]. ISA is seen as a process that allows for continuous sensitization with the aim to broaden each individual's view to understand information security as more than just an IT problem. Contextually, ISA materials must be able to be integrated into the stressful workday without taking up too many additional resources. With regard to target groups for ISA programs, our results complement the usual stakeholders such as physicians, nursing staff and administration in particular by focusing on IT, patients but also visitors.

Looking at ISA materials discussed by our experts, we found that in addition to specific content, such as password policies or user guidelines, practical problems in particular, but also practical solutions, should be highlighted to achieve an "Aha!" experience. Face-to-face methods are considered effective, but are costly due to the large number of employees involved. Online-methods are considered effective, especially because of the time flexibility and high frequency of training. However, in our interview, there was little reported experience with such offerings. Criticism was voiced that methods and content are not tailored to the medical field, so that they simply cannot be understood by the target group of medical professionals. For preparation, hospitals in particular would like to rely on the use of experts or evaluated designs in the preparation of materials. In this context, our participants identified opportunities to profit from the exchange with other departments in order to better implement ISA in medical facilities with their decades of expertise in designing and communicating awareness programs. Key challenges include the regular and low-threshold integration of ISA measures into the daily work routine, and creating sufficient time and flexibility for employees to participate.

5.2 Implications

Our findings add to the state of research on ISA in medical care by suggesting new directions for future approaches.

ISA for Expanded and Specific Audiences. Our interviews suggest that ISA programs need to cover more audiences and provide content for specific audiences. Regarding the former, our participants pointed out that patients and visitors also need to be targeted through ISA campaigns. In addition, our respondents made clear that ISA is essential among IT staff to protect information security in hospitals. Equally important is raising awareness among management, in order to obtain resources and create role models for staff, for example. The results of previous studies in other contexts support this view [50]. Nevertheless, with few exceptions [38], current research does not appear to address ISA among either IT staff or managers in medical care, and neglects patients and visitors completely. Since IT has limited understanding of medical staff's workarounds, too [15], future research may target ISA programs incorporating these aspects.

Furthermore, we note that the experts interviewed do not anticipate a separation in content of information security training between, e.g., physicians, nurses, and administration on a day-to-day basis. This contradicts research finding that not making a distinction lowers employees' satisfaction [9]. Our finding may be explained by the fact that experts are unaware of these issues, or that they give low priority to content separation due to scarce resources.

Overcoming the "Checklist Mentality". Our interviewees made it explicit that management must take an active role in ISA. ISA must be more than a box to check on an executive's governance compliance checklist and budget provision. Although our participants partially value feedback on ISA methods and materials, ISA programs are not currently evaluated in medical settings. Nor are there specific plans to implement evaluations. As a result, those in charge lack evidence on staff acceptance, effectiveness, and persistence of the ISA interventions. From the interviews, we see that the experts' uncertainty on this topic also leads to certain delivery methods being assessed as unusable from the outset (e.g., posters), but other formats are maintained for compliance reasons (e.g., e-learning). This is partly due to a lack of methods and tools for needs-based and systematic evaluation, but perhaps also due to a checklist mentality that does not provide for reflection on the effectiveness of the ISA measures used. Here we also see the risk of focusing on standalone solutions, whereas research on ISA generally shows that it is always necessary to use a mix of methods in order to be effective [3,21].

In addition, the combination of external pressure to act, but at the same time being exposed to the danger that the staff council could prevent evaluations, could lead to ineffective solutions being introduced or accepted. Indeed, German data protection and labor laws place high demands on an evaluation to prevent inadmissible performance monitoring. In line with recent findings from a phishing study in Italy [45], establishing effective ISA programs in medical care in Europe depends on the harmonization of numerous stakeholders' interests. To our knowledge, this aspect is currently missing from research on ISA in medical settings. To prevent the implementation of arbitrary and potentially ineffective ISA measures due to these issues, it may be useful to provide all stakeholders with customized information tailored to their needs. This would relieve information security officers in their communication efforts.

Inspiration from Non-security Fields. To reach the various user groups in medical institutions with ISA materials they can understand, our findings highlight the merit of drawing on already established knowledge of procedures, measures, and materials from other areas of medical care that have been dealing with awareness issues for much longer. One promising approach mentioned in the interviews is to learn from safety officers and the major hand hygiene awareness campaigns. Indeed, there are notable parallels with information security, as evidenced by studies on ISA in healthcare [6,12,14,25,31,47]. For example, leading personnel, such as physicians, have been found to neglect sanitation and overestimate their own practices compared to nurses, while sanitation is also often abandoned due to time constraints or inconvenience [34,42]. As a result, large-scale awareness campaigns have emerged in the medical field. By linking information security to known concepts and thought models that medical staff are already familiar with, it might be possible to break down barriers, promote understanding, and improve risk perception. Given the success of similar techniques applied on ISA in nonmedical sectors by drawing up on literature on safety risk communication [32, 49], we consider this an actionable solution worthy of investigation.

6 Conclusions

In this paper, we presented an expert interview study with six experts from medical care on information security, focusing on the human factor in information security and ISA topics. Our goal was to gain insight into the specifics that need to be considered when designing and implementing ISA programs in healthcare facilities. Our findings confirmed the fundamental challenges and cybersecurity risks faced by medical facilities, aligning with previous work [11,13,33,40]. We identified goals, target audiences, content, delivery methods, and ideas for collaboration to enhance information security awareness in medical facilities, complementing existing research. One area that requires attention is the design of ISA delivery methods and materials that are tailored to the specific needs of the target group. Additionally, previously underrepresented target groups such as management, patients, and visitors should be included in ISA programs. Drawing on established knowledge and practices from other healthcare areas, which have been addressing awareness issues for a longer time, can be beneficial. For instance, aligning information security concepts with familiar healthcare procedures and terminology, such as "cyber hygiene," can help bridge the understanding gap. Furthermore, the lack of evaluation of ISA programs in medical settings raises uncertainty about their long-term impact. Future research should focus on assessing the effectiveness of ISA measures in practice and academia. One significant challenge is the scarcity of resources, particularly time, in healthcare settings. Designing materials that require less time but are still effective seems crucial. Likewise, the aim should be to strengthen the "human firewall" as a last line of defense when technical measures fail. Management has a significant role to play in fostering a culture of information security that goes beyond a mere "checklist mentality." Overall, our findings provide valuable insights and directions for future research in the field of information security awareness in medical care institutions.

Acknowledgment. We thank our participants for participating in our study and the anonymous reviewers for their valuable feedback on our research. This research was funded by the German Federal Ministry of Health (grant number ZMI1-2521FSB801).

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (2019)
2. ENISA Threat Landscape 2023. Technical report (2023). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
3. Abawajy, J.: User preference of cyber security awareness delivery methods. Behav. Inf. Technol. **33**(3), 237–248 (2014)
4. Abu Ali, K., Alyounis, S.: CyberSecurity in healthcare industry. In: Proceedings of the International Conference on Information Technology (ICIT), pp. 695–701 (2021)
5. Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., AlDuaij, S.: Information security awareness and behaviors of health care professionals at public health care facilities. Appl. Clin. Inform. **12**(04), 924–932 (2021)
6. Altamimi, S., Renaud, K., Storer, T.: I do it because they do it?: social-neutralisation in information security practices of Saudi medical interns. In: Kallel, S., Cuppens, F., Cuppens-Boulahia, N., Hadj Kacem, A. (eds.) CRiSIS 2019. LNCS, vol. 12026, pp. 227–243. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-41568-6_15
7. Amankwa, E., Loock, M., Kritzinger, E.: A conceptual analysis of information security education, information security training and information security awareness definitions. In: Proceedings of the 9th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 248–252 (2014)
8. Amro, B.M., Al-Jabari, M.O., Jabareen, H.M., Khader, Y.S., Taweel, A.: Design and development of case studies in security and privacy for health informatics education. In: Proceedings of the 15th IEEE International Conference on Computer Systems and Applications (AICCSA), pp. 1–6 (2018)
9. Arain, M.A., Tarraf, R., Ahmad, A.: Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. J. Multidiscip. Healthc. **12**, 73–81 (2019)
10. Aydın, Ö.M., Chouseinoglou, O.: Fuzzy assessment of health information system users' security awareness. J. Med. Syst. **37**(6), 9984 (2013)
11. Bhuyan, S.S., et al.: Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. J. Med. Syst. **44**(5), 98 (2020)
12. Branley-Bell, D., Coventry, L., Sillence, E.: Promoting cybersecurity culture change in healthcare. In: Proceedings of the 14th ACM Pervasive Technologies Related to Assistive Environments Conference (PETRA), pp. 544–549 (2021)
13. Coventry, L., Branley, D.: Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas **113**, 48–52 (2018)
14. Coventry, L., et al.: Cyber-risk in healthcare: exploring facilitators and barriers to secure behaviour. In: Proceedings of the 2nd International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT), pp. 105–122 (2020)
15. Eikey, E.V., Murphy, A.R., Reddy, M.C., Xu, H.: Designing for privacy management in hospitals: understanding the gap between user activities and IT staff's understandings. Int. J. Med. Inform. **84**(12), 1065–1075 (2015)
16. ENISA: The new users' guide: how to raise information security awareness (EN). Report/Study TP-30-10-582-EN-C. ENISA (2010)
17. Etikan, I.: Comparison of convenience sampling and purposive sampling. Am. J. Theor. Appl. Stat. **5**(1), 1–4 (2016)

18. Evans, M., He, Y., Maglaras, L., Yevseyeva, I., Janicke, H.: Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. Int. J. Med. Inform. **127**, 109–119 (2019)
19. Fabisiak, L., Hyla, T.: Measuring cyber security awareness within groups of medical professionals in Poland. In: Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS), pp. 3871–3880 (2020)
20. Fernández-Alemán, J.L., Sánchez-Henarejos, A., Toval, A., Sánchez-García, A.B., Hernández-Hernández, I., Fernandez-Luque, L.: Analysis of health professional security behaviors in a real clinical setting: an empirical study. Int. J. Med. Inform. **84**(6), 454–467 (2015)
21. Gardner, B., Thomas, V.: Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats, 1st edn. (2014)
22. Ghazvini, A., Shukur, Z.: A framework for an effective information security awareness program in healthcare. Int. J. Adv. Comput. Sci. Appl. **8**(2), 193–205 (2017)
23. Ghazvini, A., Shukur, Z.: A serious game for healthcare industry: information security awareness training program for hospital universiti Kebangsaan Malaysia. Int. J. Adv. Comput. Sci. Appl. **9**(9), 236–245 (2018)
24. Gioulekas, F., et al.: A cybersecurity culture survey targeting healthcare critical infrastructures. Healthcare **10**(2), 327 (2022)
25. Hedström, K., Karlsson, F., Kolkowska, E.: Social action theory for understanding information security non-compliance in hospitals: the importance of user rationale. Inf. Manag. Comput. Secur. **21**(4), 266–287 (2013)
26. Hepp, S.L., Tarraf, R.C., Birney, A., Arain, M.A.: Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. Health Inf. Manag. J. **47**(3), 116–124 (2018)
27. Jaeger, L.: Information security awareness: literature review and integrative framework. In: Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS), pp. 4703–4712 (2018)
28. Jalali, M.S., Kaiser, J.P.: Cybersecurity in hospitals: a systematic, organizational perspective. J. Med. Internet Res. **20**(5), e10059 (2018)
29. Kang, J., Seomun, G.: Development and validation of the information security attitude questionnaire (ISA-Q) for nurses. Nurs. Open **10**(2), 850–860 (2023)
30. Katsikas, S.K.: Health care management and information systems security: awareness, training or education? Int. J. Med. Inform. **60**(2), 129–135 (2000)
31. Kessler, S.R., Pindek, S., Kleinman, G., Andel, S.A., Spector, P.E.: Information security climate and the assessment of information security risk among healthcare employees. Health Inf. J. **26**(1), 461–473 (2020)
32. Khan, B., Alghathbar, K.S., Khan, M.K.: Information security awareness campaign: an alternate approach. In: Kim, T., Adeli, H., Robles, R.J., Balitanas, M. (eds.) ISA 2011. CCIS, vol. 200, pp. 1–10. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23141-4_1
33. Kruse, C.S., Frederick, B., Jacobson, T., Monticone, D.K.: Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol. Healthc. **25**(1), 1–10 (2017)
34. Lambe, K., et al.: Understanding hand hygiene behaviour in the intensive care unit to inform interventions: an interview study. BMC Health Serv. Res. **20**(1), 1–9 (2020)
35. Landolt, S., Hirschel, J., Schlienger, T., Businger, W., Zbinden, A.M.: Assessing and comparing information security in Swiss hospitals. Int. J. Med. Res. **1**(2), e11 (2012)

36. Liginlal, D., Sim, I., Khansa, L., Fearn, P.: Human error and privacy breaches in healthcare organizations: causes and management strategies. In: Proceedings of the Fifteenth Americas Conference on Information System (AMCIS) (2009)
37. Lyngaas, S.: Brooklyn hospital network reverts to paper charts for weeks after cyberattack. CNN (2022). https://edition.cnn.com/2022/12/20/tech/hospital-ransomware/index.html
38. Maggio, L.A., Dameff, C., Kanter, S.L., Woods, B., Tully, J.: Cybersecurity challenges and the academic health center: an interactive tabletop simulation for executives. Acad. Med. J. Assoc. Am. Med. Coll. **96**(6), 850–853 (2021)
39. Murphy, A.R., Reddy, M.C., Xu, H.: Privacy practices in collaborative environments: a study of emergency department staff. In: Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work and Social Computing, CSCW 2014, pp. 269–282. Association for Computing Machinery, New York (2014)
40. Nifakos, S., et al.: Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors **21**(15), 5119 (2021)
41. Özaslan, G., et al.: Evaluation of the effects of information security training on employees: a study from a private hospital. Int. J. Health Manag. Tour. **5**(3), 336–347 (2020)
42. Pittet, D.: Improving compliance with hand hygiene in hospitals. Infect. Control Hosp. Epidemiol. **21**(6), 381–386 (2000)
43. Ralston, W.: The untold story of a cyberattack, a hospital and a dying woman. WIRED (2020). https://www.wired.co.uk/article/ransomware-hospital-death-germany
44. Renaud, K., Goucher, W.: Health service employees and information security policies: an uneasy partnership? Inf. Manag. Comput. Secur. **20**(4), 296–311 (2012)
45. Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., Coventry, L.: Phishing simulation exercise in a large hospital: a case study. Digital Health **8**, 20552076221081716 (2022)
46. Sari, P.K., Handayani, P.W., Hidayanto, A.N., Yazid, S., Aji, R.F.: Information security behavior in health information systems: a review of research trends and antecedent factors. Healthcare **10**(12), 2531 (2022)
47. Schmidt, T., Nøhr, C., Koppel, R.: A simple assessment of information security awareness in hospital staff across five Danish regions. Stud. Health Technol. Inf. **281**, 635–639 (2021)
48. Siponen, M.T.: Five dimensions of information security awareness. ACM SIGCAS Comput. Soc. **31**(2), 24–29 (2001)
49. Stewart, G., Lacey, D.: Death by a thousand facts: criticising the technocratic approach to information security awareness. Inf. Manag. Comput. Secur. **20**(1), 29–38 (2012)
50. Taylor, R.: Management perception of unintentional information security risks. In: Proceedings of the 27th International Conference on Information Systems (ICIS) (2006)
51. Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E.: Managing the introduction of information security awareness programmes in organisations. Eur. J. Inf. Syst. **24**(1), 38–58 (2015)
52. Wilson, M., Hash, J.: Building an Information Technology Security Awareness and Training Program. Technical report NIST SP 800-50. National Institute of Standards and Technology (2003)
53. Yeo, L.H., Banfield, J.: Human factors in electronic health records cybersecurity breach: an exploratory analysis. Perspect. Health Inf. Manag. **19**, 1i (2022)