Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Healthcare Organisations

Elina Argyridou, Sokratis Nifakos, Christos Laoudias, Sakshyam Panta, Emmanouil Panaousis, Krishna Chandramouli, Diana Navarro-Llobet, Juan Mora Zamorano, Panagiotis Papachristou, Stefano Bonacina

Submitted to: Journal of Medical Internet Research
on: July 21, 2022

Table of Contents

Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Healthcare Organisations

Elina Argyridou[1*] PhD; Sokratis Nifakos[2*] BSc, MSc; Christos Laoudias[1*] PhD; Sakshyam Panta[3]; Emmanouil Panaousis[3] PhD; Krishna Chandramouli[2] PhD; Diana Navarro-Llobet[4]; Juan Mora Zamorano[5]; Panagiotis Papachristou[2] PhD; Stefano Bonacina[2] PhD

[1]KIOS Research and Innovation Center of Excellence, University of Cyprus Nicosia CY
[2]Karolinska Institutet Stockholm SE
[3]University of Greenwich, London GB
[4]Department of Research and Innovation, Fundacio Privada Hospital Asil de Granollers Barcelona ES
[5]Instituto de Invest, Sanitaria Puerta de Hierro, Servicio Madrileno de Salud , Majadahonda Madrid ES
[*]these authors contributed equally

Corresponding Author:
Sokratis Nifakos BSc, MSc
Karolinska Institutet
Tomtebodavägen 18a
Stockholm
SE

Abstract

Background: Cyber threats are increasing across all business sectors and the cost of cybersecurity and data privacy incidents is rising globally, especially in the healthcare domain. In response to the emerging threats, healthcare organisations are enhancing the technical measures with the use of antivirus, firewalls, and firmware/software patches to protect and preserve the business continuity of patient services. Despite such efforts the threat of cybersecurity is ever increasing, and such measures have not been sufficient to counter cyber-attacks as the role of personnel in the chain of cyber defence is often neglected. In practice, healthcare organisations are requested to apply general cybersecurity and data privacy guidelines that focus on the human factor. However, there is limited literature on the methodologies and procedures which can assist healthcare organisations to successfully map to specific controls (interventions), including awareness activities and training programs, with a measurable impact on personnel. To this end, tools, and structured methodologies for assisting the higher management to select the minimum number of required controls that will be most effective on the healthcare workforce are highly desirable, yet not available at the moment.

Objective: This paper introduces a Cyber Hygiene (CH) methodology that is developed based on a unique survey-based risk assessment tool for raising cybersecurity and data privacy awareness of different employee groups in healthcare organisations. The proposed CH methodology considers the human factor in the chain of cyber defence by focusing on the gaps and needs of individual employee groups. The main objective of the methodology is to identify the most effective strategy for managing cybersecurity and data privacy risks and recommend targeted human-centric controls (e.g., awareness activities, training programs, rewards, etc.) that are tailored to the organisation-specific needs (e.g., culture, personnel background, employee role and responsibilities, etc.) to implement the strategy. The recommended controls, which are selected from a larger set of candidate controls, ensure that cybersecurity and data privacy awareness will be improved, while keeping the cost low because only a smaller subset of controls is applied.

Methods: The development of the CH methodology relied on the collection of survey responses to extract knowledge and assess the needs and gaps of 4 different employee groups, i.e., i) Administrative; ii) Medical/Clinical; iii) IT/Technical; and iv) Executive/Security, across 3 European healthcare organisations. The online survey including 28 questions was released to evaluate the situation for all 4 employee groups at each organisation with respect to 7 types of cybersecurity and data privacy risks (i.e., risk categories). In total, 356 responses were collected and analysed, and we attained detailed results in terms of the risk levels per organisation, employee group, risk category, and selected topics of interest associated with specific survey questions. For anonymization purposes, the organisations are randomised and thereafter referred to as HO1, HO2, and HO3. Indicative high-level findings include: i) Administrative and Medical/Clinical employees at HO3 have fewer high risks compared to HO1 and HO2. This implies that these employee groups at HO3 seem to better understand the general concepts of cyber

hygiene and ii) Administrative and Medical/Clinical employees at HO1 and HO2 have medium-high risk evaluation in most risk categories. Thus, they are encouraged to adopt the controls recommended by our CH methodology to manage these risks and improve the situation with respect to the personnel's cybersecurity and data privacy perception and behaviour.

Results: The information gathered from the questionnaires have been processed and analysed resulting in the application of a risk assessment procedure to evaluate and quantify various cybersecurity and data privacy risks. These risks have been discretized into a range of 1 to 5 with 1 representing lowest form of risk and 5 representing highest form of risk from the employees' perspective. Thus, we identify the most effective strategy (ranging from 'acceptance' to 'mitigation') to manage each risk. Each risk category has been mapped to a set of human-centric, rather than IT-based, controls and implementation levels (e.g., quarterly training with beginners' level material) based on the corresponding risk management strategy. These are categorised as Training, Awareness, Motivation, and Rewarding controls. Our mapping empowers the recommendation of the optimal subset of human-centric controls to implement the identified strategy for managing each risk.

Conclusions: In this paper we present a structured methodology for improving the cyber hygiene perception and behaviour of personnel in the healthcare sector. The applicability and added value of the proposed CH methodology is demonstrated using real-life survey data collected at 3 European healthcare organisations. Our findings suggest that there are considerable differences with respect to human-oriented cybersecurity and data privacy risks across different organisations and diverse employee groups within the same organisation. By applying the CH methodology, we provide the risk strategies together with the list of recommended human-centric controls for managing a wide range of cybersecurity and data privacy risks related to healthcare employees.

(JMIR Preprints 21/07/2022:41294)
DOI: https://doi.org/10.2196/preprints.41294

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**
Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.
No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**
Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v
Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Healthcare Organisations

Abstract

Background: Cyber threats are increasing across all business sectors and the cost of cybersecurity and data privacy incidents is rising globally with healthcare being a prominent domain. In response to the ever-increasing threats, healthcare organisations are enhancing the technical measures with the use of cybersecurity controls (e.g., firewalls, secure configuration, patch management) that not only address the essential requirements for certification (e.g., ISO 27001, HCISPP) but also implement advanced solutions (e.g., incident management, supply chain security) for further protection. Ultimately, the goal of these controls is to protect and preserve the business continuity of patient services. Despite the need for technical controls, humans are evidently the weakest link in the cybersecurity posture of a healthcare organisation. This, in combination with the view that cybersecurity is as good as its weakest link, suggests that addressing human aspects of cybersecurity is a key step towards managing cyber-physical risks. In practice, healthcare organisations are requested to apply general cybersecurity and data privacy guidelines that focus on the human factor. However, there is limited literature on the methodologies and procedures which can assist healthcare organisations to successfully map these guidelines to specific controls (interventions), including awareness activities and training programs, with a measurable impact on personnel. To this end, tools and structured methodologies for assisting the higher management to select the minimum number of required controls that will be most effective on the healthcare workforce are highly desirable, but yet not available to healthcare personnel.

Objective: This paper introduces an exploratory Cyber Hygiene (CH) methodology that employs a unique survey-based risk assessment approach for raising cybersecurity and data privacy awareness of different employee groups in healthcare organisations. The proposed CH methodology considers the human aspects in the chain of cyber defence by focusing on the gaps and needs of individual employee groups. The main objective of the methodology is to identify the most effective strategy for managing cybersecurity and data privacy risks and recommend targeted human-centric controls (e.g., awareness activities, training programs, rewards, etc.) that are tailored to the organisation-specific needs (e.g., culture, personnel background, employee role and responsibilities, etc.) to implement the strategy. The recommended controls, which are selected from a larger set of candidate controls, ensure that cybersecurity and data privacy awareness are improved, while keeping the cost low due to the recommendation of the most effective combination of controls, which are, in most times, a subset of all the controls.

Methods: The development of the CH methodology relied on two key methods namely a cross-sectional exploratory survey study followed by a proposed risk-based approach survey analysis approach. First, the survey facilitated the collection of responses to extract knowledge and assess the needs and gaps of 4 different employee groups, i.e., i) Administrative; ii) Medical/Clinical; iii) IT/Technical; and iv) Executive/Security, across 3 European healthcare organisations (hospitals and research institutes). The online survey including 28 questions was released to describe the situation for all 4 employee groups at each organisation with respect to 7 types of cybersecurity and data privacy risks (i.e., risk categories). Each risk category is represented by an exclusive subset of questions. Next, we transcribed the responses to the proposed risk-based analysis approach to obtain insights about the risk levels per organisation, employee group, and risk category. In particular, 5 strategies were defined for managing the risks, while risks were discretized into a range of 1 to 5 with 1 representing lowest form of risk and 5 representing the highest, both from the employees' perspective. We defined the procedures for quantifying the risk by means of the risk marking computed from the survey responses. This quantification of risk based on information gathered form survey responses enabled us to identify the most effective strategy ranging from Mitigation, Reduction, Monitoring, Checking, and Acceptance.

Results: As a first result, a list of human-centric controls and implementation levels (e.g., quarterly

personnel training with beginners' level material) was created including a variety of controls categorised as Training, Awareness, Motivation, and Rewarding controls. These controls were associated with risk categories and were mapped to risk strategies for managing the risks related to all employee groups. Our mapping empowers the computation and subsequently recommendation of subsets of human-centric controls to implement the identified strategy for managing the overall risk of the healthcare organisation. An indicative example demonstrates the application of the exploratory CH methodology in a simple scenario. Finally, by applying the CH methodology in the healthcare sector we obtained results (i.e., risk markings, identified strategies to manage the risks, and recommended controls) for each of the 3 healthcare organisations, each employee group, as well as each risk category. For anonymization purposes, the organisations were assigned a random name identifier (HO1, HO2, and HO3). Indicative high-level findings include: i) Administrative and Medical/Clinical employees at HO3 have fewer high risks compared to HO1 and HO2. This implies that these employee groups at HO3 seem to better understand the general concepts of cyber hygiene and ii) Administrative and Medical/Clinical employees at HO1 and HO2 have medium-high risk evaluation in most risk categories. Thus, they are encouraged to adopt the controls recommended by our CH methodology to manage these risks and improve the situation with respect to the personnel's cybersecurity and data privacy perception and behaviour.

Conclusions: In this paper we present an exploratory methodology for improving the CH perception and behaviour of personnel in the healthcare sector. The applicability and added value of the proposed CH methodology is demonstrated using real-life survey data collected from 3 European healthcare organisations. Our findings suggest that the adoption of a risk-based approach to quantify the risk associated with various human-related cybersecurity and data privacy threats facilitates the effective management of individual cybersecurity risks across different organisations and diverse employee groups within the same organisation, i.e., different organisations and/or employee groups face different risks. By applying the CH methodology, we provide the risk strategies together with the list of recommended human-centric controls for managing a wide range of cybersecurity and data privacy risks related to healthcare employees.

Keywords: Cyber Hygiene, Cybersecurity, Awareness, Training, Healthcare, Risk Management

Introduction

According to the technical series published by World Health Organisation (WHO) on Primary Health Care [1], Information and Communication Technologies are nowadays very common with the introduction of smart phones, tablets and laptop computers. On one hand such technologies have resulted in a positive impact on patient care with the increasing growth of Electronic Health Records (EHR). However, such medical databases, which often include personal information and financial data among others, have resulted in becoming a target for cyber-attacks.

The origins of cybercrime can be traced to the late 1970s as the computer Information Technology (IT) industry took shape. What began as spam eventually transitioned into computer viruses and malware (e.g., Wannacry). Inevitably, the rise of cybersecurity incidents is a growing threat to the healthcare industry, in general, and to hospitals in particular [2]. While the impact of cybersecurity is not unique to the healthcare industry, the lack of concerted efforts in protecting the healthcare's stakeholder data has lagged in comparison to other industries [3]. With the fast digitisation of patient health records, the impact of data breaches on hospitals causes major economic and intangible damage. To counteract the impact of cyber-attacks, organisations have adopted governance strategies to promote best practices for securing the electronic infrastructure of hospitals and other clinical environments [2], [4].

Existing cybersecurity practices in healthcare organisations are insufficient [3]–[5] and have affected the integrity of medical data and the confidentiality of patients. Even with increasing instances and case-studies of cyber-attacks within healthcare organisations, many institutions still remain ignorant towards cybersecurity and rely on legacy systems such as Windows XP and Windows NT 3.1. Despite the warning from relevant vendors such as Microsoft who have stated that security updates and support has been withdrawn for such systems presenting a security risk. One of the main reasons for healthcare organisations becoming an attractive target for cybersecurity attacks is the large volume of personal data being handled, which present an economic value in the black market [6]. The weaker security posture in healthcare organisations is mainly due to the lack of cybersecurity budget, which results in minimal access to technology and expertise. Steve Morgan observes that healthcare industry will respond by spending $125 billion cumulatively from 2020 to 2025 to beef up its cyber defences [7]. Such an investment in cyber defence is necessitated by the increasing number of attacks that has increased five-fold after the COVID-19 pandemic [8]. Such incidents have been recently witnessed within the Health Service Executive (HSE) of Ireland [9]. A similar case has been reported in August 2021, where a ransomware attack was launched against the COVID-19 vaccination booking system in the Regione Lazio, Italy [10].

Traditionally, healthcare organisations have not considered an investment in cybersecurity as necessary, as the focus has predominantly been on providing patient care and people believed that there would be no motivation to attack these organisations. However, recent findings have illustrated that healthcare data is considerably more valuable than any other data. On the other hand, the increasing use of Internet of Things (IoT) technologies in healthcare have increased the attack surface beyond information security to physical safety. Following the increasing familiarity and convenience of using single digital devices for both personal and professional activities, Wani et al. notes that major challenges to healthcare IT infrastructure stems from the use of devices with insufficient security controls by hospital staff, lack of control or visibility for the management to maintain security requirements [11]. Additional factors such as lack of awareness among hospital staff and the lack of direction or guidance for secure use of Bring Your Own Device/Phone (BYOD/ BYOP), poor user experience, compliance on legal requirements for accessing secure healthcare IT systems, shortage of cybersecurity skills, and loss of devices are also cited as a cause for security threats. Despite advances in the field of IT systems to enhance the overall security of healthcare organisations, critical challenges remain due to the lack of emphasis on human factors in cybersecurity.

As a significant proportion of cyber-attacks are directed towards the users through deceptive means

such as spam emails and application masquerading, the users play a critical role in cybersecurity alongside technical controls. This is particularly the case in healthcare as deceiving a nurse, doctor, healthcare IT professional or administrator can impact the privacy and physical safety of patients. For example, Saxon et al. have demonstrated that implantable medical devices (e.g., pacemakers and cardioverter-defibrillator) are susceptible to adversarial interference (remotely) violating not only the integrity and confidentiality of patients' data and medical telemetry, but could also compromise patients' physical safety [12].

In a recently published systematic survey by Nifakos et al., the authors conclude that there is a fundamental paradigm shift from targeting IT infrastructure as a vulnerability of a healthcare organisation to focus on the human vulnerability who rely on the existing IT infrastructure [13]. One of the key observations from the authors relates to the crossover of personal information between social media usage by healthcare professions, which has proved to be a successful source of information for launching targeted phishing attacks. Jalali et al. conducted a research on the facts affecting employee decision-making that enables them to click on phishing links [14]. The study focussed on the clicking behaviour which was analysed using the Theory of Planned Behaviour (TPB). The authors conclude that there is a strong correlation between employee workload and the behaviour of non-compliance while responding to phishing attacks. As a result of the survey [13], the authors have proposed to implement training modules to promote the use of privacy setting options provided by the social media platforms. The authors additionally acknowledge that there needs to be a targeted organisational programme to undertake cyber risk and privacy impact assessment leading to the identification of potential healthcare infrastructure vulnerabilities. Such a programme should place a high degree of emphasis to consider a human-centric approach. Additionally, the authors also acknowledge the fact that despite several organisations and researchers have identified the need for delivering cybersecurity training to healthcare professionals, there is little consensus on the curriculum and systematic methodology for evaluating the impact of cyber hygiene. The review presents in detail several case-studies which are often experienced by the healthcare professionals, including front line medical staff, nurses, management teams and hospital administrators to name a few.

In the past, studies on security training in healthcare have investigated offering education to healthcare professionals aimed at gaining awareness on digital applications and platforms for raising knowledge on healthcare data privacy and security risks [15]. The authors have further highlighted the factors to consider while designing training and awareness programmes for healthcare personnel. The effect to which security training and awareness programmes work for different users has been studied from multiple angles. Heartfield et al. have shown that against deception-based attacks, such as semantic social engineering, self-study and work-based training are considerably more effective than formal education in cybersecurity [16]. While [17] has indicated that training materials from security experts, third-party organisations and peers can also positively influence cybersecurity practices.

Among the several barriers and reluctance in adopting several recommendations which have been summarised in the literature identified within the healthcare sector [13], the critical lack of funding dedicated to secure the IT infrastructure of healthcare organisations has been cited as a critical limitation. In contrast to the other digital industrial sectors, such as finance, banking, media and others, the main driver of revenue is successful delivery of healthcare services. Additionally, as all healthcare services are delivered to the patients by humans, the financial structure of healthcare organisations aims to prioritise expenses to retain human capital. This phenomenon is reflected in the lack of ‘Chief Information Security Officer’ serving as an official member of several healthcare boards.

Despite economic challenges often encountered by healthcare organisations, there is recently increasing evidence of investment, decided by hospitals' management to strengthen IT infrastructure [4]. While some of these endeavours might be voluntary, the data governance policies enacted by

national authorities have also acted as a catalyst to the increasing cybersecurity budgets. However, the successful adoption of digital transformation strategies within the healthcare industry relies on the successful acceptance among healthcare professionals towards addressing risks posed by cyber threats. Thus, it is important to deliver ***awareness*** and ***training*** programs for healthcare professionals. The role of human behaviour in coping with cyber-attacks and strengthening cyber defences is grouped into the theme of “human factor” in cybersecurity.

In general, healthcare organisations strive to apply cybersecurity and data privacy guidelines that focus on the human factor. This is because general guidelines are typically hard to map to specific controls (e.g., awareness activities and training programs) with a proven positive effect on the personnel, while avoid overspending by implementing unnecessary or less relevant controls. Currently, there is a lack of tools and methodologies for assisting the higher management to select the necessary controls that will have the greatest impact on the healthcare personnel. This is the key challenge that the proposed CH methodology addresses.

The exploratory CH methodology is outlined in Figure 1 and comprises five steps.

1. Knowledge extraction through a survey questionnaire: This step involves extracting knowledge and assessing the needs and gaps of different employee groups at healthcare organisations through a set of questions in a survey questionnaire.
2. Response processing and analysis: At this step, the responses collected from the participants are processed and analysed to evaluate the cybersecurity and data privacy risks and quantify them through their risk marking.
3. Risk strategy identification: At this step, the most effective strategy to manage each risk is identified.
4. Recommendation of controls: At this step, the human-centric controls that are mapped in advance with a specific strategy are recommended to implement the identified strategy.
5. Application of the controls to the personnel: At this final step, the management team can apply the controls to the workforce to improve the level of cybersecurity and data privacy awareness.

The empty arrow that closes the loop from step 5 to step 1 indicates that running the survey again after some time, to confirm that the situation in terms of cybersecurity and data privacy awareness has improved after the application of the recommended controls, is left as future work.

Figure 1 **- Outline of the exploratory Cyber Hygiene methodology based on survey data and risk assessment.**

Methods

Study design

A cross-sectional exploratory survey study together with a proposed risk-based survey analysis approach were designed and deployed in order to describe Cyber Hygiene awareness within three healthcare organisations participating in the CUREX project.

Survey construction

The survey was designed to capture different aspects of employee awareness in cybersecurity, data privacy/data protection, employee training and use of connected devices. The procedure to construct the survey is illustrated in the diagram in Figure 2. First, the working group for the CUREX project together with representatives from all three healthcare organisations formed a consensus group that performed an initial review of existing literature and resources on Cyber Hygiene including relevant documents by healthcare agencies such as the U.S. Department of Health and Human Services (HHS) that highlight the top threats in this sector [18], reports and recommendations by international cybersecurity organisations and centres such as the European Network and Information Security Agency (ENISA) [19],[20][21],[22] the European Cyber Security Organisation (ECSO) [23], and the Center for Internet Security (CIS) [24], as well as previous surveys on this topic [25, 26]. The consensus group consisted of sixteen members with a differential background ranging from IT and cybersecurity expertise, technical and medical academia, to healthcare professionals. Next, the consensus group identified the main employee groups in healthcare organisations, i.e., Administrative, Medical/Clinical, IT/Technical, and Executive/Security personnel; see the study population part below for details. The intuition is that employee groups are not equally vulnerable to cybersecurity threats because they have varying awareness level in cybersecurity and data privacy and undertake daily tasks that do not expose them to the same risks. Next, after consulting the representatives from the three healthcare organisations, various risks were recognised (e.g., employees not being aware of cyber threats in the healthcare sector, not considering cybersecurity during daily work, not knowing about internal security procedures, etc.) followed by clustering in representative risk categories; see the risk categories and descriptions in Error: Reference source not found. Then, an initial list of questions was prepared and associated with each risk category aiming to quantify the relevant risk according to the responses. The questions were reviewed and refined in multiple iterations. The process was repeated when new risks were recognised, leading to new risk categories and/or adaptation of previously defined categories followed by the addition of other questions. Finally, after several review rounds the consensus group concluded on a final survey with a total of 28 questions; see the list of questions in the Appendix. The survey questions were prepared in English, later translated to the native languages of the healthcare organisations in the CUREX project, and administered in all three languages.

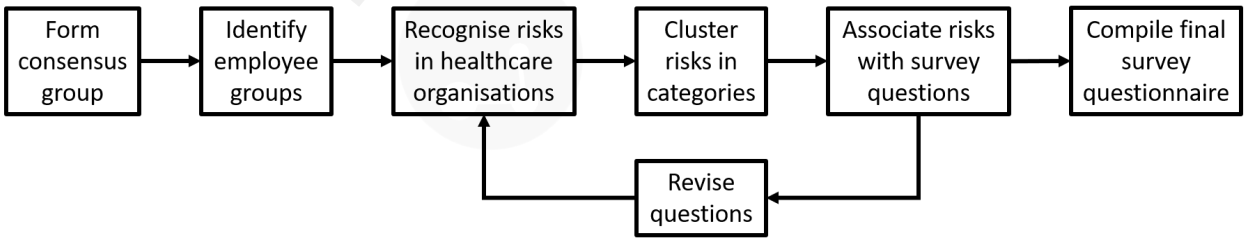

Figure 2 Diagram of the procedure to construct the survey.

Mapping the Cyber Hygiene landscape by reviewing existing literature and studying the available resources was fundamental for compiling the final survey questionnaire. For instance, driven by the list of top threats in healthcare, specific questions were included to reveal how familiar are the employees working in this sector with these threats, if they are aware of relevant incidents, both inside and outside their organisation, whether they are able to recognise such incidents at the early stages, and how confident they feel to handle them. In addition, given the nature of these top threats

it was decided to define the risk categories and the associated survey questions in a way that there is a clear distinction between the cybersecurity and the data privacy risks.
Finally, the recommendations by cybersecurity agencies and organisations are reflected in several risk categories and associated survey questions. These recommendations include, for instance, i) raising cybersecurity awareness, ii) secure medical and portable devices including Bring-Your-Own-Device (BYOD) and Bring-Your-Own-App (BYOA) schemes, iii) secure physical access and health information, and iv) educating users against social engineering attacks (e.g., phishing emails).

Study population
In each healthcare organisation we identified four main employee groups, which were all eligible for the survey study:

- Administrative (e.g., administration manager, secretary, reception, call centre, human resources, etc.)
- Medical/Clinical (e.g., department/unit manager, doctor, nurse, etc.)
- IT/Technical (e.g., IT manager, IT staff, software developer, etc.)
- Executive/Security (e.g., Director, Sub Director, Hospital Manager, Chief Information Security Officer (CISO), Chief Security Officer (CSO), Data Protection Officer (DPO), etc.)

The first two groups, i.e., the Administrative and the Medical/Clinical groups, typically had more employees compared to the IT/Technical and Executive/Security groups.
The participation of users in the study was carried out through a systematic recruitment process, which was launched using either proprietary (such as internal e-Learning tools or through email campaign) or open online survey tools (e.g., EU Survey tool). Additional channels of recruitment included participation through emails and use of existing eLearning platforms, which were often used by hospital doctors about medical learning and other events. The user recruitment process was carried out between mid-June 2020 and lasted until end of September 2020. All participants had access to the survey preamble with information about the purpose of the survey. All participants provided their digital consent before proceeding with the survey questions. Duplicate entries were avoided by preventing users with the same IP address access to the survey twice.
The confidence interval based on the survey responses with respect to the population size was determined by $P < 0.05$ (95% confidence level). For the calculation, the online confidence interval calculator was used [27]Error: Reference source not found. More specifically, the following formula is used:

$$Confidence\ Interval = \pm\sqrt{\frac{z^2 * p * (1-p)}{ss}}, ss = \frac{s}{1 + \frac{s-1}{pop}}$$

where z is the value of the confidence level (e.g., 1.96 for 95% confidence level), p is the percentage of picking a choice expressed as decimal (e.g., 0.5), s is the sample size (i.e., number of responses), and pop is the population size.

Risk Categories
The survey questions were grouped in seven risk categories based on their topic and structure, as shown in Error: Reference source not found, which facilitated risk analysis and profiling of each employee group. The first column provides the name of the risk category, the second column lists the number of the associated survey questions, while the third column describes the risks of the corresponding category.

Table 1: Risk categories for all employee groups

Risk Category	Survey Questions	Risk description

Cyber Hygiene	2, 3, 4	Not aware of what Cyber Hygiene is
Cybersecurity Awareness	8, 11, 13	Not aware of cybersecurity threats in healthcare and related incidents
Data Privacy/Protection Awareness	5, 6, 8, 12, 14	Not aware of what General Data Protection Regulation (GDPR) is, data privacy/protection threats in healthcare and related incidents
Cybersecurity Training	9, 15, 17, 20	Not attending existing training, not considering cybersecurity during daily work, not knowing about internal procedures for cybersecurity threats, limited knowledge about cybersecurity (self-assessed)
Data Privacy/Protection Training	7, 10, 16, 18, 19, 21	Not attending existing training, not considering data privacy during daily work, not knowing about internal procedures for data privacy threats and who is responsible for data protection, managing personal data frequently, limited knowledge about data privacy (self-assessed)
Communication Channels	22, 23, 24	Limited number of communication channels that are available in the organisation or preferred by employees, and limited communication with IT personnel
Secure connection and use of devices	25, 26, 27, 28	Not aware of or not following policies, guidelines, or best practices about remote connection, using public access networks, using personal devices (BYOD), and using personal USB sticks

Survey questions

Among the 28 survey questions, each question could be a single-answer or a multiple-answer question. Additionally, survey questions had one of the following Likert scale type questions to describe the extent of the respondent's awareness, agreement, frequency in use (adoption of cyber hygiene practices), knowledge, and satisfaction.

- YES/NO/ I don't know (awareness)
- 1 = I strongly disagree | 5 = I strongly agree (agreement)
- 1 = Never | 5 = In every daily activity (frequency in use)
- 1 = I have no knowledge | 5 = I am an expert (knowledge)
- 1 = Very disappointing | 5 = Very Satisfying (satisfaction)

Among the different types of questions outlined above, the scale of 1 represents the lowest value while 5 represents the highest value of the impact, that correspond to each question. Based on these marks we described the awareness and understanding of cyber hygiene for each respondent, but also of each employee group in total. Each of the employee group members were asked to go through identified statements to determine their awareness and relevance in terms of the survey purpose on a scale of 1 to 5, where 1 means no awareness or relevance, while 5 means high awareness or relevance. Based on the responses collected from the participants, we described the extent of awareness and relevance for each employee group and suggest an appropriate strategy and associated controls for raising cybersecurity and data privacy awareness.

Risk-based survey analysis approach

In the following, we describe a proposed risk-based approach for the analysis of the survey responses. The aim is to design effective processes to increase awareness and training on cyber hygiene. These processes include *identification*, *analysis*, *monitor*, *evaluation*, and *treatment* of various risks that each healthcare organisation may have. By applying these risk processes, we

describe the risks by using a risk matrix with a scoring system (1-5). Then, we proceed with evaluating the risks, which point to specific risk strategies for managing the associated risks towards raising cybersecurity and privacy awareness of different employee groups. Risk strategies are mapped to a recommended subset of controls to manage the risks of each employee group.

Risk strategies

The *impact-probability risk matrix* is shown in Table 2. This matrix has two dimensions, namely the *risk probability*, which shows the likelihood of a risk to happen, and the *risk impact*, which shows the importance and severity of the risk.

Table 2**: Impact-Probability risk matrix**

Risk Probability		**Risk Impact**				
		Negligible	**Minor**	**Moderate**	**Significant**	**Severe**
		1	**2**	**3**	**4**	**5**
Very Likely	**5**	Low Med	Medium	Med Hi	High	High
Likely	**4**	Low	Low Med	Medium	Med Hi	High
Possible	**3**	Low	Low Med	Low Med	Medium	Med Hi
Unlikely	**2**	Low	Low	Low Med	Low Med	Medium
Very Unlikely	**1**	Low	Low	Low	Low	Low Med

By multiplying the risk probability with the risk impact, we get the risk evaluation marking that shows whether the risk is low, medium, or high.

The *risk evaluation matrix*, which points to specific risk strategies based on the risk evaluation marking, is shown in Table 3. Each risk strategy corresponds to specific controls for *mitigating*, *reducing*, *monitoring*, *checking*, and *accepting* risks. For instance, when the risk is higher, then the trainings should be more often (e.g., weekly) starting from basic information (e.g., beginners' level material). In a similar fashion, when the risk is lower, then the trainings could be less often (e.g., monthly, or quarterly) including more details (e.g., advanced level material). Finally, if the risk is very low, then it is acceptable, and the employees are acknowledged and rewarded for following good cyber hygiene practices.

Table 3**: Risk evaluation matrix**

Risk Marking	**Risk Evaluation**	**Risk Strategy**	**High-Level Action Plan**
[20 - 25]	High	Mitigation	**Mitigate** the risk: Improve Skills / Raise Awareness / **Monthly or Weekly** actions for **Beginners** level
[15 - 19]	Medium-High	Reduction	**Reduce** the risk: Improve Skills / Raise Awareness / **Quarterly or Monthly** actions for **Intermediate** level
[10 - 14]	Medium	Monitoring	**Monitor** the risk: Increase Awareness / **Semi-Annually or Quarterly** actions for **Intermediate or Advanced** level

[5 - 9]	Low-Medium	Checking	**Check** the risk: Retain Awareness / **Annually** or **Semi-Annually** interventions for **Advanced** level
[1 - 4]	Low	Acceptance	**Accept** the risk: Acknowledgment / Rewards

Risk Procedures

To use the risk evaluation matrix (Table 3), below we define the *risk impact* and the *risk probability*. In Table 4 the risk impact is defined with a scoring system from 1 to 5 based on the structure of the survey questions. The lowest risk impact has the lowest mark (1), while the highest impact has the highest mark (5). Medium marks (2-4) indicate medium risk impacts.

Table 4: Risk impact definition for different types of survey questions

Risk Impact		**Frequency**	**Agreement**	**Knowledge**	**YES/NO/ I don't know**	**Multiple Answers**
1	Low	Daily	Strongly agree	In-depth	YES	All selected
2	Low-Medium	Weekly	Agree	Very well		Many selections
3	Medium	Monthly	Can't say	Well	I don't know	Enough selections
4	Medium-High	Rarely	Disagree	Heard of it		Few selections
5	High	Never	Strongly disagree	Never heard	NO	One or nothing

In Table 5, the risk probability is defined based on the total amount of the responses. When the total number of responses is high, then the likelihood of the risk to happen is higher, while when the total number of responses is small then the likelihood is low.

Table 5: Risk probability definition

Risk Probability		**Responses in total (Re)**	e.g., Re = 100
1	Very Unlikely	[0 - Re* (1/5))	[0-20)
2	Unlikely	[Re* (1/5) - Re*(2/5))	[20-40)
3	Possible	[Re*(2/5) - Re* (3/5))	[40-60)
4	Likely	[Re* (3/5) - Re*(4/5))	[60-80)
5	Very Likely	[Re*(4/5) - Re]	[80-100]

In order to calculate the *risk marking*, we apply the following formula:

$$Risk\ Marking = \sum_{i=1}^{n} risk\ impact(i) * risk\ probability(i) * RF$$

where,

i=1,… ,n is the number of responses and RF is the Risk Factor.

For the RF, the following formula is applied:

$$Risk\ Factor = \frac{5}{NoQ * NoR}$$

where

NoQ is the total number of questions of each risk category, NoR is the total number of responses of each employee group for each organisation. The number 5 is chosen as the maximum mark of the scoring system, so that we can reach the highest level of possible risk.

An example risk marking calculation as part of the risk-based approach is provided in the Results section.

Discussion

Rationale of human-centric controls

To implement the high-level action plans for the risk strategies shown in Table 3, we need relevant human-centric controls, i.e., measures and interventions[1], to be associated with each risk strategy. As most resources recognise training and awareness campaigns as a key prerequisite in increasing awareness and achieving a common understanding of cyber threats and security risks at all hierarchical levels, the proposed list includes targeted *Training* and *Awareness* controls. As the use of rewards has been reported in the literature to be beneficial for encouraging and motivating employees to adopt desirable behaviours [32], [33], our list includes also *Motivation* and *Reward* controls.

In particular, a subset of the proposed controls are inspired by the sub-controls presented in the CIS report "CIS Control 17: Implement a Security Awareness and Training Program v7.1" [28]. These controls are properly adapted to the objectives of Cyber Hygiene within the EU-funded H2020 project CUREX [29], e.g., there are separate controls for cybersecurity and data privacy. Notably, the CIS Controls report v8 released in May 2021 includes the control "Conduct Role-Specific Security Awareness and Skills Training", which is captured by our approach through the consideration of different employee groups. Some Motivation controls are adopted to incorporate the notion of nudges that are proposed in the Secure Behaviour Nudging Tool [30] developed in the context of the H2020 PANACEA project [31]. In general, nudges are behavioural interventions that usually take place timely, i.e., during the daily work, rather than "out-of-context" training in the classroom. Finally, additional controls are introduced by the CUREX research team and are inspired by guidelines and good practices applied across various domains. These include Awareness controls (e.g., inclusion of cybersecurity and data privacy in the agenda of each meeting that takes place in the healthcare organisation) and Reward controls that are intended mainly to acknowledge employees that behave responsibly and celebrate desirable practices within the organisation on various occasions.

Selecting controls for each risk strategy

The main idea for selecting controls that are relevant to each risk strategy (Table 3) is the following. As a risk is increasing and the risk strategy changes from "Acceptance" to "Checking" to "Monitoring" to "Reduction" and finally to "Mitigation", then the applied controls should move from "Rewarding" to "Motivation" to "Awareness" and finally to "Training" controls to address and properly manage the risk. The intuition is that, for example, the "Motivation" controls assume some level of awareness to be effective; thus, these controls cannot help in the case of "Reduction" or "Mitigation" risk strategies, where lack of awareness and/or knowledge is observed. Moreover, the "Training" controls are expected to have a larger impact in managing the risk when they are combined or applied after "Awareness" controls. In addition, moving from "Monitoring" to "Reduction" and finally to "Mitigation", implies that the frequency of the "Awareness" and "Training" controls should be increased, so that the employees are more frequently exposed to the awareness messages and training material. In contrast, the content level of awareness and training should be decreased, e.g., beginners level content is more appropriate in the "Mitigation" risk strategy, while advanced level content better fits the "Monitoring" risk strategy because the employees have a baseline awareness and/or knowledge of the corresponding risk.

Results

Candidate human-centric controls

For this study we came up with a list of 19 candidate controls C1–C19, which are listed in Error: Reference source not found, followed by the association of controls with each risk category, as

[1] The single term "controls" will be used hereunder to include measures, controls, and interventions.

shown in Error: Reference source not found.
The candidate controls in Error: Reference source not found are categorised as follows:

- Training controls: C1, C2, C6, C7, C8, C9, C10, C11
- Awareness controls: C3, C4, C5, C12, C13
- Motivation controls: C14, C15, C17
- Rewarding controls: C16, C18, C19

Table 6**: Candidate human-centric controls**

No	Control Title	Control Description	Related Resource
C1	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviours employees are not adhering to, using this information to build a baseline education roadmap.	CIS Sub-control 17.1
C2	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact employees' security behaviour.	CIS Sub-control 17.2
C3	Implement a Cybersecurity Awareness Program	Create a cybersecurity awareness program for employees to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organisation.	CIS Sub-control 17.3
C4	Implement a Data Privacy Awareness Program	Create a data privacy awareness program for employees to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organisation.	CIS Sub-control 17.3
C5	Update Awareness Content Frequently	Ensure that the organisation's security awareness program is updated frequently to address new technologies, threats, standards, and business requirements.	CIS Sub-control 17.4
C6	Train Workforce on Secure Authentication	Train employees on the importance of enabling and utilising secure authentication.	CIS Sub-control 17.5
C7	Train Workforce on Identifying Social Engineering Attacks	Train employees on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.	CIS Sub-control 17.6
C8	Conduct Mock Social Engineering Exercises	Conduct mock social engineering attacks (phishing, phone scams, and impersonation calls) to assess the readiness and response level of the employees	CIS Sub-control 17.6
C9	Train Workforce on Sensitive Data Handling	Train employees on how to identify and properly store, transfer, archive, and destroy sensitive information.	CIS Sub-control 17.7
C10	Train Workforce on Causes of Unintentional Data Exposure	Train employees to be aware of causes for unintentional data exposures, such as losing their mobile devices or a USB stick with sensitive data, emailing the wrong person, etc.	CIS Sub-control 17.8
C11	Train Workforce Members on Identifying and	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	CIS Sub-control 17.9

	Reporting Incidents		
C12	Include Cybersecurity in the meetings' agenda	Set Cybersecurity as a standing agenda item at meetings.	CUREX project
C13	Include Data Privacy in the meetings' agenda	Set Data Privacy as a standing agenda item at meetings.	CUREX project
C14	Introduce nudges to motivate cybersecurity behaviours	Introduce nudges as behavioural interventions to motivate and encourage employees to adopt desirable cybersecurity behaviours that they are already aware of.	PANACEA project
C15	Introduce nudges to motivate data privacy behaviours	Introduce nudges as behavioural interventions to motivate and encourage employees to adopt desirable data privacy behaviours that they are already aware of.	PANACEA project
C16	Acknowledge employees that behave in a cybersecurity and data privacy responsible way	Acknowledge employees that demonstrate cybersecurity and data privacy behaviours (e.g., report to the IT scam emails, suspicious incidents, etc.) and reward them (e.g., introduce awards like 'Cybersecurity Employee of the Year').	CUREX project
C17	Introduce a cybersecurity and data privacy champion role	Nominate an employee within each department/team in the organisation who, given some specific skills and knowledge, will be responsible to promote cybersecurity and data privacy best practices in daily work.	CUREX project
C18	Celebrate Cybersecurity awareness on specific occasions	Introduce a specific day/week/month during the year for celebrating cybersecurity, e.g., the National Cyber Security Awareness Month (NCSAM) observed in the USA and the European Cybersecurity Month (ECSM), both celebrated during October.	CUREX project
C19	Celebrate Data Privacy/Protection awareness on specific occasions	Introduce a specific day/week/month during the year for celebrating data privacy and protection, e.g., the Data Privacy Day in the USA and the European Data Protection Day both observed every January 28th.	CUREX project

Obviously, not all controls are appropriate for all risk categories shown in Error: Reference source not found for all employee groups. Note, however, that a specific control may be relevant to multiple risk categories. To this end, each risk category has a list of associated controls and either all or a subset of the associated controls can be applied as part of the identified risk strategy, as shown in Table 7.

Table 7: Recommended controls for the risk categories of all employee groups

Risk Category (All employee groups)	Recommended controls
Cyber Hygiene	C3, C4, C5, C12, C13, C16, C17, C18, C19
Cybersecurity Awareness	C3, C5, C11, C12, C16, C17, C18
Data Privacy/Protection Awareness	C4, C5, C11, C13, C16, C17, C19
Cybersecurity Training	C1, C2, C7, C8, C11, C12, C14, C16, C17, C18

Data Privacy/Protection Training	C1, C2, C9, C10, C11, C13, C15, C16, C17, C19
Communication Channels	C3, C4, C5, C14, C15, C17
Secure connection and use of devices	C3, C4, C5, C6, C9, C10, C14, C15, C16, C17, C18, C19

Moreover, different *implementation levels* can be considered for an individual control. For instance, a control that is related to training (e.g., C2 and C6) or a control that implements an awareness program and updates its content (e.g., C3, C4, and C5) may have varying *implementation levels*, e.g., *frequency* (i.e., weekly, monthly, quarterly, semi-annually, or annually), *content level* (i.e., beginners, intermediate, or advanced level), and *target audience* (i.e., Administrative, Medical/Clinical, IT/Technical, Executive/Security personnel). These implementation levels can be properly selected for the identified risk strategy depending on the employee group.

Mapping of controls to risk strategies

An indicative mapping of candidate controls (Table 6) with respect to risk strategies (Table 3) and risk categories (Table 1) is illustrated in Table 8.

For instance, for the “Cyber Hygiene” risk category, as we move from the “Acceptance” risk strategy to the “Mitigation” risk strategy more aggressive and effective controls are recommended to be applied for addressing the increasing risk. In this case, the controls C3 and C4, which are related to the implementation of a cybersecurity and a data privacy awareness program respectively, can be implemented monthly or weekly (i.e., frequency level) for beginners (i.e., content level) in the “Mitigation” risk strategy because the personnel is totally unfamiliar with Cyber Hygiene; while in the “Reduction” risk strategy the awareness programs can be implemented quarterly or monthly with intermediate level content, as the employee group has some basic knowledge of what Cyber Hygiene is.

In the case of the “Cybersecurity Training” risk category, as shown in Error: Reference source not found, the controls C1 and C2 related to the analysis and filling of skills gap could be used only in the “Mitigation” risk strategy because the employee group probably lacks basic cybersecurity skills (e.g., selecting a strong password) and has limited knowledge about cybersecurity. On the other hand, the controls C7 and C8 related to training for identifying social engineering attacks (e.g., in person, over the phone, or through phishing emails) and conducting mock social engineering exercises (e.g., fake phishing emails sent out by the organisation’s IT department) are recommended in both “Mitigation” and “Reduction” risk strategies. This is because social engineering is probably the most serious threat that the healthcare workforce needs to defend against. Again, the frequency (i.e., monthly, or weekly vs. quarterly or monthly), the content level (e.g., baseline phishing emails for beginners vs. more sophisticated phishing emails with email address spoofing), and the target audience are adapted according to the risk strategy.

For these two risk categories listed in Error: Reference source not found, the “Monitoring” risk strategy may include mild controls, e.g., C12 and C17 for discussing cybersecurity in internal meetings and assigning a cybersecurity champion in the team/department to monitor the situation; or in the case of the “Cybersecurity Training” risk category the strategy may include training on identifying and reporting incidents (i.e., C11) other than social engineering attempts. This is because for this risk strategy, the employee group can be assumed to have adequate knowledge of social engineering attacks, how to recognise, to defend against them, and inform their IT department; thus, the focus should be on different types of suspicious events or behaviours. In addition, for the “Cybersecurity Training” risk category, the “Monitoring” risk strategy may also include nudges (e.g., to encourage updating more often and choosing stronger passwords for their accounts) because this risk strategy assumes some level of awareness and basic knowledge of the underlying threats and nudges aim to motivate desirable cybersecurity behaviours to further reduce the associated risk.

Finally, for the “Checking” and “Acceptance” risk strategies, where the corresponding risk can be considered tolerable, the recommended controls include mainly acknowledging and rewarding desirable and “good-example” behaviours by individuals or teams within the healthcare organisation, as well as celebrating cybersecurity event occasions.

Table 8: Indicative mapping of controls to risk strategies for the risk categories of all employee groups

Risk Category	Risk Strategy				
	Mitigation	Reduction	Monitoring	Checking	Acceptance
Cyber Hygiene	C3, C4, C5, C12, C13	C3, C4, C12, C13, C17	C12, C13, C17	C16, C17, C18, C19	C16, C18, C19
Cybersecurity Awareness	C3, C5, C11, C12	C3, C5, C11, C12, C17	C11, C12, C17	C16, C17, C18	C16, C18
Data Privacy/ Protection Awareness	C4, C5, C11, C13	C4, C5, C11, C13, C17	C11, C13, C17	C16, C17, C19	C16, C19
Cybersecurity Training	C1, C2, C7, C8, C11	C7, C8, C11, C12, C17	C11, C12, C14, C17	C14, C16, C17, C18	C16, C18
Data Privacy/ Protection Training	C1, C2, C9, C10	C9, C10, C11, C13, C17	C11, C13, C15, C17	C15, C16, C17, C19	C16, C19
Communication Channels	C3, C4, C5	C3, C4, C5, C17	C14, C15, C17	C14, C15, C17	-
Secure connection and use of devices	C3, C4, C5, C6, C9, C10	C3, C4, C5, C6, C9, C10, C17	C10, C14, C15, C17	C14, C15, C16, C17, C18, C19	C16, C18, C19

Example application of the proposed risk-based survey analysis approach

In the following, we provide an example application of the proposed risk-based approach to demonstrate in a simple way how it works in practice. In this example, we consider the Administrative employee group at one of the CUREX partner healthcare organisations.

First, the risk category is given with the corresponding number of questions in Error: Reference source not found. The types of these specific questions are agreement (i.e., questions 3 and 4) and awareness – YES/NO/I don’t know (i.e., question 2). “Re” represents the number of responses for each case and “Marks” represents the corresponding mark.

Table 9: Example application of the proposed risk-based survey analysis approach

Risk Category	Survey Questions	Total Questions	Agreement	Re	Marks	YES/ NO/ DON’T KNOW	Re	Marks
Cyber Hygiene	2, 3, 4	3	Strongly Agree	9	1	Yes		1
			Agree	11	2			2

			Can't Say	2	3	Don't know		3
			Disagree	6	4			4
			Strongly Disagree	2	5	No	15	5

Thus, the first step is the collection of the responses and rating them, using the scoring system from 1 to 5, for this risk category. Next, we calculate the risk marking by multiplying Re with Marks. Then, we sum them all up and we multiply the result with the corresponding RF.
Following, we give the risk calculation of the above example.
Risk Marking = ((9 x 1) + (11 x 2) + (2 x 3) + (6 x 4) + (2 x 5) + (15 x 5)) x RF ≈ 16 ϵ [15 – 19], where RF= 5/(3 x 15)

The risk marking, which is rounded to a whole number, is 16. By using the risk evaluation matrix, this risk marking shows that the risk is "**Medium-High**" and the corresponding risk strategy is "**Reduction**"; see Table 3. In this case, the recommended controls to address and manage the risk related to Cyber Hygiene (see Error: Reference source not found) include C3, C4, C12, C13, C17, where the controls C3 and C4, related to the cybersecurity and data privacy awareness programs respectively, can be implemented quarterly or monthly with intermediate level content.

Application of the exploratory Cyber Hygiene methodology
This section presents the results of applying the exploratory methodology to the CUREX healthcare organisations (hospitals and research institutes) including the survey demographics, the risk-based analysis of the survey responses, and our observations. For anonymising the survey results and findings, the names of the three Healthcare Organisations (HO) have been randomised and replaced by HO1, HO2, and HO3. The analysis of the results is performed with regards to three different aspects. Specifically, in the following sections we first present the survey demographics and then report a sample of the results with general remarks and discussion regarding the following Dimensions (D):

- D1 – Healthcare Organisation (HO2)
- D2 – Employee Group (Medical/Clinical)
- D3 – Risk Category (Cybersecurity Awareness)

Survey Demographics
The demographics of the survey respondents of the three CUREX healthcare organisations are listed in Error: Reference source not found including the employee groups, the population size, the total number of responses, and the confidence interval for HO1, HO2, HO3 respectively.
As we observe in Error: Reference source not found, in some cases the total number of responses is much smaller compared to the population size. As a result, the confidence interval for some of the employee groups is not small enough.
Table 10**: Survey demographics for the Healthcare Organisations in the CUREX project**

	HO1			**HO2**			**HO3**		
	Population	**Responses**	**Confidence Interval (95%)**	**Population**	**Responses**	**Confidence Interval (95%)**	**Population**	**Responses**	**Confidence Interval (95%)**

Administrative	278	15	24.66	24	16	14.45	78	16	21.98
Medical/ Clinical	1437	29	18.02	2730	178	7.1	554	70	10.96
Executive/ Security	88	16	22.29	12	3	51.18	-	-	-
IT/ Technical	12	11	8.91	5	2	60.01	-	-	-

Note that for the last organisation (HO3), there are no responses for the Executive/Security and the IT/Technical groups, therefore these are not included in the above table.

Analysis of results D1 – Healthcare organisation

In the following, Figure 3 illustrates the results of the application of the risk-based approach in our CH methodology for the risk categories pertaining to all employee groups at the HO2.

In Figure 3, the x-axis represents the risk categories, while the y-axis represents the risk evaluations as Low (1), Low-Medium (2), Medium (3), Medium-High (4), and High (5). According to the risk evaluation matrix, these risk evaluations point to specific risk strategies and associated controls to manage the underlying risks.

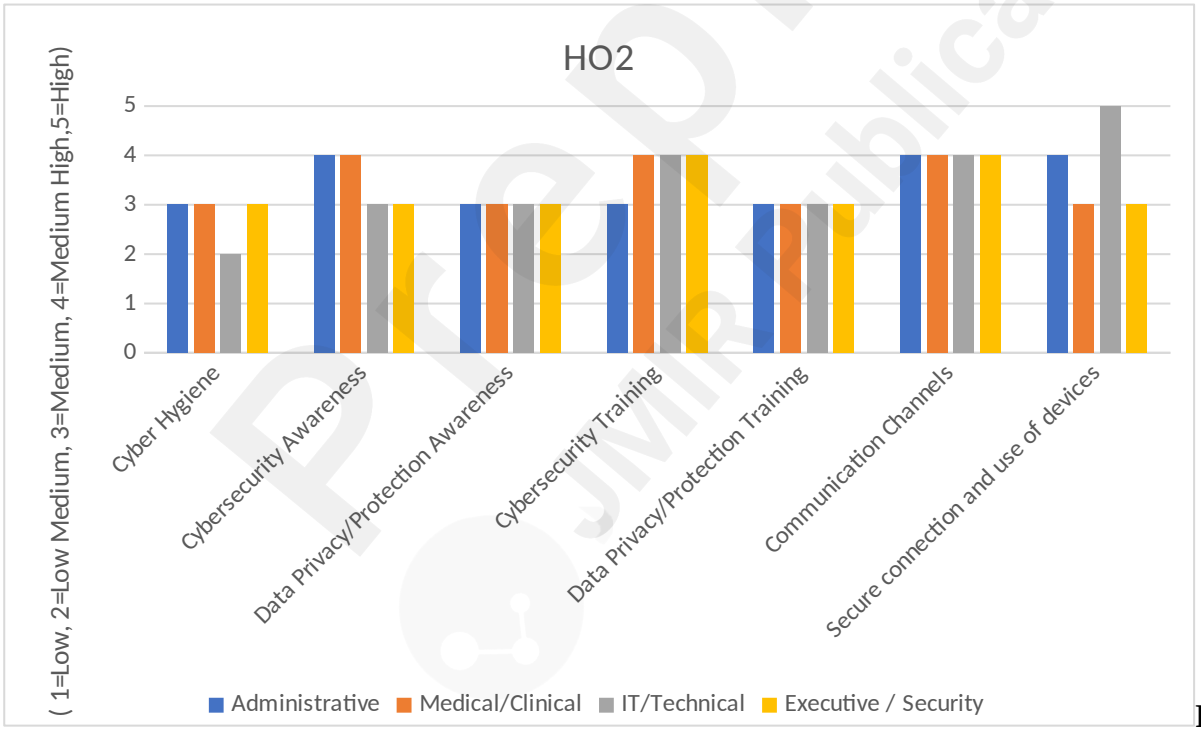

Figure 3 - Findings for all employee groups at HO2

Results for all employees in Figure 3, indicate that the risks are mostly Medium and Medium-High with risk strategies being “Monitoring” and “Reduction”, respectively. Findings for the IT/Technical group imply that employees have high awareness on Cyber Hygiene since the risk for the corresponding category is Medium-Low. In contrast, this group demonstrates high risk for the risk category “Secure Connection and use of devices”, which means that controls should be applied to properly manage this risk compared to the other three employee groups. Specifically, based on Error: Reference source not found in order to address this risk, the controls C3, C4, C5, C6, C9, and C10

need to be customized with respect to their frequency and content (if applicable) and then targeted to this specific group as shown in Table 11.

Table 11 **- Subset of Human-Centric Controls for the IT/Technical group at HO2**

No	Control title	Implementation level	
		Frequency	**Content level**
C3	Implement a Cybersecurity Awareness Program	Monthly or Weekly	Beginners
C4	Implement a Data Privacy Awareness Program	Monthly or Weekly	Beginners
C5	Update Awareness Content Frequently	Monthly or Weekly	N/A
C6	Train Workforce on Secure Authentication	Monthly or Weekly	Beginners
C9	Train Workforce on Sensitive Data Handling	Monthly or Weekly	Beginners
C10	Train Workforce on Causes of Unintentional Data Exposure	Monthly or Weekly	Beginners

Analysis of results D2 – Employee group

In Figure 4, survey findings are presented for the Medical/Clinical employee group at HO1, HO2, and HO3. Similar to the previous graph, the x-axis represents the risk category of the corresponding employee group, and the y-axis represents the risk evaluation.

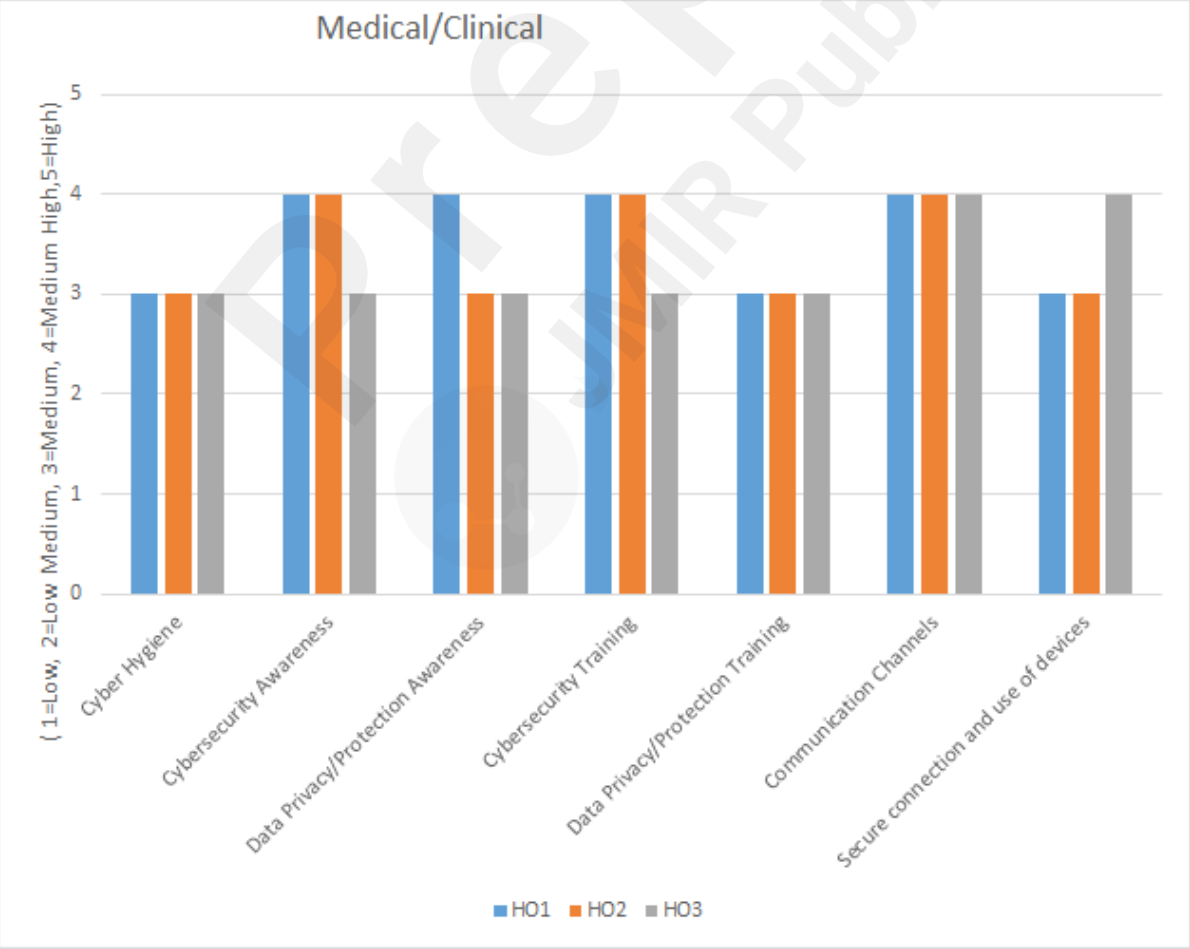

Figure 4 - Findings for the Medical/Clinical employee group at the CUREX healthcare organisations

Findings for this employee group show that "Cyber Hygiene" and "Data Privacy/Protection Training" risk categories have the lowest risk with Medium size, which need to be monitored with mild controls. In contrast, the "Communication Channels" risk category has the highest risk since this employee group across all three CUREX HOs has reached a Medium-High risk. For this risk, the corresponding controls are C3, C4, C5, C17 which need to be applied on a quarterly or monthly basis with intermediate level content for the employees to be able to follow the communication channels and absorb the awareness messages. Moreover, the HOs could consider using additional channels for conveying the cybersecurity and data privacy messages, e.g., channels that are preferable by the employees and are not currently in use. As a last observation, employees at the HO3 show lower risks compared to the HO1 and HO2, since most of their risks are Medium level.

Analysis of results of D3 – Risk Category

The bar chart in Figure 5presents findings for the three CUREX HOs with respect to the "Cybersecurity Awareness" risk category pertaining to all employee groups.

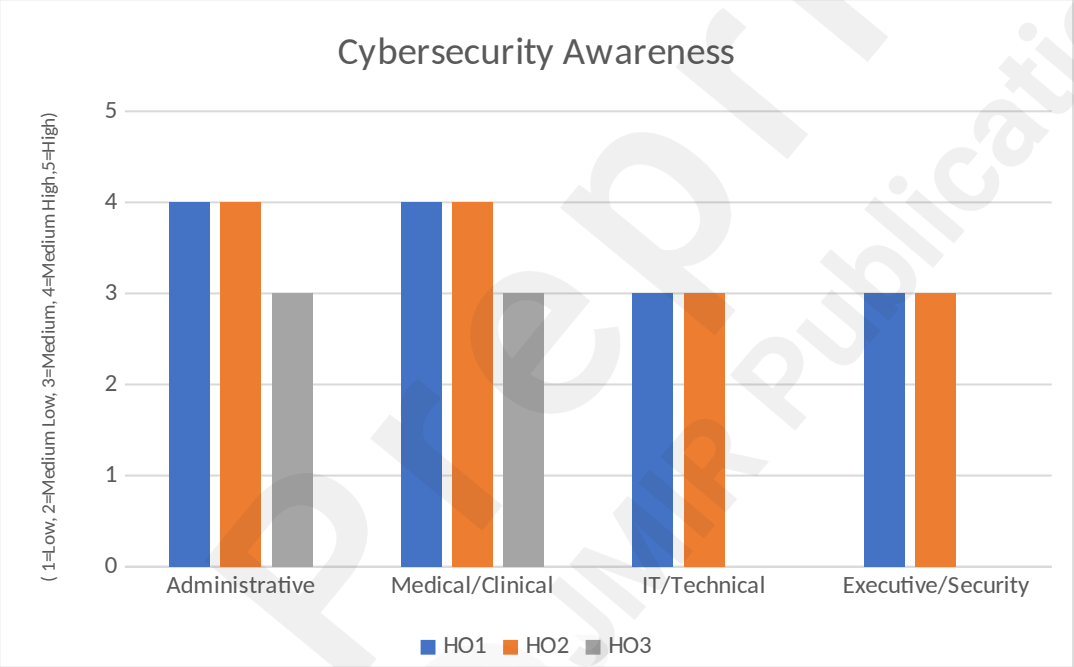

Figure 5 - Findings for the 'Cybersecurity Awareness' risk category at the CUREX Healthcare Organisations

The "Cybersecurity Awareness" risk category seems to have relatively high evaluation for all employees across the CUREX HOs. Specifically, the risk is Medium-High at the HO1 and HO2 for the Administrative and Medical/Clinical personnel. The rest of the risk evaluations are Medium level. The Medium-High risks point to the "Reduction" risk strategy, where the controls include C3, C5, and C11, which need to be applied every month or quarter with intermediate level for the awareness and training content, as well as the controls C12, and C17 for motivating desirable cybersecurity behaviours (Error: Reference source not found).

Limitations

The research presented in this paper had been carried out across three healthcare organisations. Therefore, the development of the cyber hygiene controls is based on the limited feedback gathered

from the study participants. Additionally, as the study period coincided with the COVID-19 pandemic, the responses obtained have been limited in number as outlined in Error: Reference source not found, i.e., 356 respondents. On average, HO1, HO2 and HO3 had 29%, 34%, and 17% respective responses completed from the overall population. Among the four employee groups, the Medical/Clinical group is represented with 2%, 6% and 12% respectively across the healthcare organisations. It is important to note the two employee categories in HO3 were not available to participate in the research study. Yet, the inclusion of three different healthcare organisations brings together different perspectives on cybersecurity and data privacy, as experienced by different personnel in the healthcare sector, and paves the way for a Cyber Hygiene methodology to recommend targeted human-centric controls. The future work of the study could lead to the analysis of increased responses from geographically diverse group of healthcare organisations to further validate the proposed cyber hygiene controls. We also plan to monitor the application of the recommended controls (i.e., step 5 in Figure 1) at a specific HO and run the CH survey again after some time to confirm that the situation in terms of cybersecurity and data privacy awareness has improved.

Comparison with Prior Work

Regarding the literature review, the findings in [32] suggest that the knowledge about cyber hygiene is not the same among different age groups and older users tend to have more secure habits. In the proposed approach, instead of considering the age of the employees we instead consider the role of different employees leading to the identification of four employee groups in healthcare organisations that have different background and needs regarding Cyber Hygiene; not so much because of their age, but because of the nature of their work and daily tasks. Considering the findings in [33] and [34] related to the use of rewards for encouraging and motivating employees to adopt desirable behaviours, targeted motivation and reward controls are included in the pool of candidate human-centric controls that are recommended to address specific risks. Finally, as phishing emails (and in general social engineering) have been recognised in [32], [33], [34], and [35] as a serious threat, the proposed methodology focuses on this aspect. The survey questionnaire includes questions for different employee groups related to this popular form of social engineering attacks, as well as specific controls including training the workforce on identifying social engineering attacks and conducting mock social engineering exercises.

Conclusions

In this paper, a novel concept for improving the cyber hygiene perception and behaviour of four key employee groups within healthcare organisations has been proposed. The value of the proposed exploratory survey-based CH methodology has been demonstrated through its application to three HOs, who participated in the study in the context of the H2020 CUREX project. In particular, the proposed CH methodology relies on a survey questionnaire to achieve a deep understanding of the needs and gaps of different healthcare employee groups. It then employs a risk-based approach to quantify the risk associated with various human-related cybersecurity and data privacy threats, identifies the proper strategies for addressing various risks, and recommends subsets of human-centric controls for managing each risk.

Acknowledgements

The research work leading to the publication was supported by European Union’s Horizon 2020 research and innovation programme under grant agreement no. 826404—CUREX project. The work of C.L. and E.A. has been partially supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE) and from the Republic of Cyprus through the Deputy Ministry of Research, Innovation and Digital Policy.

Conflicts of Interest

None declared.

Abbreviations
CH: Cyber Hygiene
IT: Information Technology
WHO: World Health Organisation
EHR: Electronic Health Records
HSE: Health Service Executive
IoT: Internet of Things
BYOD: Bring Your Own Device
TPB: Theory of Planned Behaviour
CISO: Chief Information Security Officer
CSO: Chief Security Officer
DPO: Data Privacy Officer
GDPR: General Data Protection Regulation
USB: Universal Serial Bus
HO: Healthcare Organisation

Appendix: Survey questionnaire
The questions of the survey are included in this appendix.
Legend
- o **Indicates a single-answer question**
- ☐ **Indicates a multiple-answer question**

1. What is your role in the organisation?
   - o Administrative (e.g., administration manager, secretary, reception, call centre, human resources, etc.)
   - o Medical/Clinical/Research (e.g., department/unit manager, doctor, nurse, researcher, etc.)
   - o IT/Technical (e.g., IT manager, IT staff, software developer, etc.)
   - o Executive/Security (e.g., Director, Sub Director, Hospital Manager, Chief Information Officer, Chief Data/Information Security Officer, Data Protection Officer, etc.)

2. Are you familiar with the term Cyber Hygiene?
   - o Yes
   - o No

3. To what extend do you agree with the following description of Cyber Hygiene?
   (1 = I strongly disagree | 5 = I strongly agree)

   Cyber Hygiene refers to activities that users and computer system administrators can undertake to improve their cybersecurity while online.

   1 2 3 4 5

4. To what extend do you agree with the following description of Cyber Hygiene?
   (1 = I strongly disagree | 5 = I strongly agree)

Cyber Hygiene, in analogy to personal hygiene, refers to simple routine measures that any employee can take to minimise the risks from cyber threats.

◉ 1 ○ 2 ○ 3 ○ 4 ○ 5

5. How familiar are you with the General Data Protection Regulation (GDPR)?
(1 = I have never heard of GDPR | 5 = I have in-depth knowledge of GDPR)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

6. Which of the following statements best describes what the GDPR is?
   - o A new legal framework relating to the collection, storage and usage of personal data, which applies to any organisation based in the EU doing business with EU citizens
   - o A new legal framework aimed at companies operating online in the EU, stipulating how and when companies are able to collect personal data
   - o An update on the EU Data Protection Act 1998, which means personal data can only legally be collected and stored by companies that are certified in accordance with the GDPR regulations

7. Who is responsible for monitoring data protection in your business?
   - o Senior management
   - o Legal department
   - o IT managers
   - o All users of data within the workplace
   - o Other. Please specify:_____
   - o I do not know

8. Which of the following cybersecurity and data privacy threats are you aware of? (Select all that apply)
   - ☐ Social engineering
   - ☐ Ransomware
   - ☐ Loss or theft of hardware
   - ☐ Insider, accidental, or intentional data loss
   - ☐ Attacks against smart medical devices
   - ☐ Other. Please specify:_____
   - ☐ None of the above

9. Have you received any training by your organisation on cybersecurity?
   - o Yes. Please note frequency (e.g., Weekly, Monthly, Quarterly, etc.): _____
   - o No

10. Have you received any training by your organisation on data privacy?
   - o Yes. Please note frequency (e.g., Weekly, Monthly, Quarterly, etc.): _____
   - o No

11. Have you heard of any cybersecurity incident <u>outside</u> your organisation (e.g., from the news, etc.)?

- o Yes
- o No

12. Have you heard of any data privacy incident outside your organisation (e.g., from the news, etc.)?
    - o Yes
    - o No

13. Have you ever personally experienced any cybersecurity incident inside your organisation?
    - o Yes
    - o No

14. Have you ever personally experienced any data privacy incident inside your organisation?
    - o Yes
    - o No

15. Is there a procedure in place in your organisation, in case you face a cybersecurity threat?
    - o Yes
    - o No
    - o I do not know
    - o Only for specific threats. Please specify: _____

16. Is there a procedure in place by your organisation, in case that you face a data privacy threat?
    - o Yes
    - o No
    - o I do not know
    - o Only for specific threats. Please specify: _____

17. How often do you consider cybersecurity during your daily work?
    (1 = Never | 5 = In every daily activity)
    1 2 3 4 5

18. How often do you consider data privacy during your daily work?
    (1 = Never | 5 = In every daily activity)
    1 2 3 4 5

19. How often do you manage personal data (i.e. of patients, clients)?
    - o Never
    - o Rarely
    - o Daily
    - o Weekly
    - o Monthly

20. How would you rate your knowledge about matters of cybersecurity?

(1 = I have no knowledge | 5 = I am an expert)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

21. How would you rate your knowledge about matters of data privacy?
(1 = I have no knowledge | 5 = I am an expert)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

22. Which communication channels are currently used in your organisation to raise awareness on cybersecurity and data privacy?

(Select all that apply)

- ☐ Emails
- ☐ Corporate Intranet
- ☐ Articles
- ☐ Videos
- ☐ Online training
- ☐ In-person training
- ☐ Information sessions during staff meetings
- ☐ Other. Please specify: _____
- ☐ I do not know

23. Which communication channels would you prefer to learn about cybersecurity and data privacy in your organisation?

(Select all that apply)

- ☐ Emails
- ☐ Corporate Intranet
- ☐ Articles
- ☐ Videos
- ☐ Online training
- ☐ In-person training
- ☐ Information sessions during staff meetings
- ☐ Other. Please specify: _____
- ☐ I do not know

24. How often do you interact with your organisation's IT department or local IT manager?

(1 = Never | 5 = Daily)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

25. Do you personally use remote connection (e.g., Virtual Private Network – VPN) to access your organisation's corporate network?

- o Yes
- o No
- o I do not know

If yes:

- How often do you do this over public access networks (e.g., public Wi-Fi hotspots)? (1 = Never | 5 = Daily)

  ○ 1 ○ 2 ○ 3 ○ 4 ○ 5
- I am cautious about using public wireless networks.
  (1 = I strongly agree | 5 = I strongly disagree)

  ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

26. Does your organisation provide public Wi-Fi access to patients and visitors?
    - o Yes
    - o No
    - o I do not know

27. Is there a Bring Your Own Device (BYOD) policy in your organisation?
    - o Yes
    - o No
    - o I do not know

    If yes:
    - Did you receive any special training or instructions on this?
      - o Yes
      - o No
      - o I do not know
    - I am conscious about protecting my mobile devices and their contents. (1 = I strongly disagree | 5 = I strongly agree)

      ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

28. Are employees allowed to plug in personal USB storage devices on workplace PCs and machines?
    - o Yes
    - o No
    - o I do not know

References

[1] D. Z. and A. V. Berumen, “Digital technologies: shaping the future of primary health care,” *WHO/HIS/SDS/2018.55*, 2018. https://www.who.int/docs/default-source/primary-health-care-conference/digital-technologies.pdf (accessed Dec. 2022).

[2] J. MS and K. JP, “Cybersecurity in Hospitals: A Systematic, Organizational Perspective.,” *J. Med. Internet Res.*, vol. 20, no. 5, p. e10059, 2018, [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/29807882/.

[3] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville, “How can organizations develop situation awareness for incident response: A case study of management practice,” *Comput. Secur.*, vol. 101, p. 102122, 2021, doi: https://doi.org/10.1016/j.cose.2020.102122.

[4] H. Alami *et al.*, "Digital health: Cybersecurity is a value creation lever, not only a source of expenditure," *Heal. POLICY Technol.*, vol. 8, no. 4, pp. 319–321, 2019.
[5] M. S. Jalali and J. P. Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective.," *J. Med. Internet Res.*, vol. 20, no. 5, p. e10059, May 2018, doi: 10.2196/10059.
[6] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward.," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.
[7] S. Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, 2020.
[8] W. CM, C. R, and C. K, "Cybersecurity Risks in a Pandemic.," *J. Med. Internet Res.*, vol. 22, no. 9, p. e23692, 2020, [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/32897869/.
[9] E. Šípková, "Ireland's Health Service Executive ransomware attack (2021)," 2021.
[10] S. J. T. Chopra, "Hackers shut down system for booking COVID-19 shots in Italy's Lazio region," 2021.
[11] T. A. Wani, A. Mendoza, and K. Gray, "Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature," *JMIR mHealth uHealth*, vol. 8, no. 6, pp. e18175–e18175, Jun. 2020, doi: 10.2196/18175.
[12] L. A. Saxon, N. Varma, L. M. Epstein, L. I. Ganz, and A. E. Epstein, "Factors Influencing the Decision to Proceed to Firmware Upgrades to Implanted Pacemakers for Cybersecurity Risk Mitigation.," *Circulation*, vol. 138, no. 12. United States, pp. 1274–1276, Sep. 2018, doi: 10.1161/CIRCULATIONAHA.118.034781.
[13] S. Nifakos *et al.*, "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," *Sensors*, vol. 21, no. 15, 2021, doi: 10.3390/s21155119.
[14] J. MS, B. M, W. D, and S. G, "Why Employees (Still) Click on Phishing Links: Investigation in Hospitals.," *J. Med. Internet Res.*, vol. 22, no. 1, p. e16775, 2020, [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/32012071/.
[15] J. L. Kamerer, D. McDermott, J. L. Kamerer, and D. McDermott, "Cybersecurity: Nurses on the Front Line of Prevention and Education," *J. Nurs. Regul.*, vol. 10, no. 4, pp. 48–53, 2020.
[16] R. Heartfield, G. Loukas, and D. Gan, "You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks," *IEEE Access*, vol. 4, pp. 6910–6928, 2016.
[17] R. Wash and M. M. Cooper, "Who Provides Phishing Training? Facts, Stories, and People Like Me," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, 2018, pp. 1–12.
[18] HHS, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, 2019. [link, accessed Dec. 2022]
[19] ENISA, Review of Cyber Hygiene practices, December 2016. [link, accessed Dec. 2022].
[20] ENISA, Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, December 2018. [link, accessed Dec. 2022].
[21] ENISA, Smart Hospitals – Security and Resilience for Smart Health Service and Infrastructures, November 2016, [link, accessed Dec. 2022].
[22] D. Liveri, et al., "Security and Resilience in eHealth. Security Challenges and Risks" ENISA, 2015. [link, accessed Dec. 2022]
[23] ECSO, HEALTHCARE SECTOR REPORT Cyber security for the healthcare sector, March 2018.
[24] CIS, Cyber Attacks: In the Healthcare Sector [link, accessed Dec. 2022]
[25] 2021 HIMSS Healthcare Cybersecurity Survey [link, accessed Dec. 2022]
[26] SecureHospitals project, D2.2: Current perceptions and trends on cybersecurity in hospital

[27] Creative Research Systems, Your Complete Survey Software Solutions Since 1982.
[28] “CIS Critical Security Controls v7.1.” https://www.cisecurity.org/controls/v7 (accessed Jun. 30, 2022).
[29] “CUREX Project.” https://curex-project.eu/ (accessed Dec. 2022).
[30] “PANACEA 2nd End User Workshop | Session 7: Secure Behaviour Nudging Tool.” https://www.youtube.com/watch?v=x2_VBRM9fro (accessed Dec. 2022).
[31] “PANACEA project.” https://www.panacearesearch.eu/ (accessed Dec. 2022).
[32] A. A. Cain, M. E. Edwards, and J. D. Still, “An exploratory study of cyber hygiene behaviors and knowledge,” *J. Inf. Secur. Appl.*, vol. 42, pp. 36–45, 2018, doi: https://doi.org/10.1016/j.jisa.2018.08.002.
[33] D. Ashenden and D. Lawrence, “Can We Sell Security like Soap? A New Approach to Behaviour Change,” in *Proceedings of the 2013 New Security Paradigms Workshop*, 2013, pp. 87–94, doi: 10.1145/2535813.2535823.
[34] A. Vishwanath *et al.*, “Cyber hygiene: The concept, its measure, and its initial tests,” *Decis. Support Syst.*, vol. 128, p. 113160, 2020, doi: https://doi.org/10.1016/j.dss.2019.113160.
[35] M. Muthuppalaniappan LLB and K. Stevenson, “Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health,” *Int. J. Qual. Heal. Care*, vol. 33, no. 1, p. mzaa117, Aug. 2021, doi: 10.1093/intqhc/mzaa117.