Int. J. Inf. Secur. manuscript No.
(will be inserted by the editor)

Cybersecurity Training and Healthcare: the AERAS Approach

Fulvio Frati · Georgiana Darau · Nikolaos Salamanos · Pantelitsa Leonidou · Costas Iordanou · Dimitrios Plachouris · Efstratios Syrmas · Evangelos Floros · George Nikitakis · George Spanoudakis · Konstantinos Kalais · Stella Tsichlaki · Ernesto Damiani · George C. Kagadis · Jihane Najar · Michael Sirivianos

Received: date / Accepted: date

Abstract Cyber ranges have gained significant importance in cybersecurity training in recent years, and they are still playing a role of paramount importance, thanks to their ability to give trainees hands-on experience with real-world exercises. This paper presents the motivation and objective of the AERAS project, including a thorough analysis of data from adhoc interviews and surveys specifically designed and administered for the project's goals. AERAS aims to apply the cyber range concept to the critical healthcare sector. The AERAS platform will be a virtual cyberwarfare solution that will simulate the operation and effects of security controls and offer hands-on training on their development, assessment, use, and management.

1 Introduction

Cyber ranges have gained increasing importance in cybersecurity training in recent years. Still, it is paramount since it gives trainees hands-on experience in real-world exercises.

High-quality cyber ranges can recreate for users the experience of responding to a simulated cyber-attack by replicating the working environment, the organizational network, and the deployed attack [5]. Cyber ranges are increasingly deployed in critical assets to improve cybersecurity preparedness and awareness in critical environments. One of the pre-

George Nikitakis · George Spanoudakis
Sphynx Analytics Ltd, 108, Nicosia Business Centre, 33 Neas Engomis, 2409 Nicosia, Cyprus, E-mail: g.nikitakis@sphynx.ch, spandoudakis@sphynx.ch

George C. Kagadis · Dimitris Plachouris · Efstratios Syrmas
3DMI research group, Department of Medical Physics, University of Patras, 26504, Rion, Greece, E-mail: gkagad@gmail.com, dim.plachouris@gmail.com, esyrmas@gmail.com

Georgiana Darau · Jihane Najar
AEGIS, 25 Humboldt Str, Braunschweig, Germany, E-mail: g.darau@aegisresearch.eu, jnajar@aegisresearch.eu

Fulvio Frati · Ernesto Damiani
Computer Science Department, Università degli Studi di Milano, via Celoria 18, 20133 Milano, Italy, E-mail: fulvio.frati@unimi.it,ernesto.damiani@unimi.it

Costas Iordanou · Konstantinos Kalais · Pantelitsa Leonidou · Nikolaos Salamanos · Michael Sirivianos
Cyprus University of Technology, 30 Arch. Kyprianos Str., 3036 Limassol, Cyprus, E-mail: kostas.iordanou@cut.ac.cy, ki.kalais@edu.cut.ac.cy, pl.leonidou@edu.cut.ac.cy, nik.salaman@cut.ac.cy, michael.sirivianos@cut.ac.cy

Evangelos Floros · Stella Tsichlaki
University General Hospital of Heraklion, Leof. Panepistimiou, Iraklio 71500, Greece E-mail: efloros@pagni.gr, stsichlaki@gmail.com

dominant is the healthcare sector, whose government expenditure in EU-28 reached 7.1% of EU GDP, exceeding other critical sectors. However, such a level of investment is not reflected in the same level of investment in cybersecurity training and awareness.

As technology use in healthcare grows, so do cyber-attacks. Personal health information (PHI) and e-health records (EHRs) stored in healthcare organizations are of incredible value to cybercriminals, as they contain personal information (e.g., social security numbers and insurance information) that can be easily used for fraudulent purposes or sold for profit. Also, risks are too high with medical devices, especially smart wearable devices, and implants (e.g., drug infusion pumps, defibrillators), which interact with the physical world and affect patient health directly.

In this challenging context, the AERAS project, funded by the EC under the Horizon 2020 Marie Skłodowska-Curie Research and Innovation Staff Exchange Evaluations, is designing and developing its solution. The Consortium is aimed at developing a realistic and rapidly adjustable cyber range platform for systems and organizations in the critical healthcare sector to effectively prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk, critical cybersystems and organizations against advanced, known, and new cyber-attacks, and reducing their security risks. The platform will be a virtual cyberwarfare solution enabling the simulation of the operation and effects of security controls and offering hands-on training on their development, assessment, use, and management. In this paper, we want to put forward our ideas, describe the motivation leading our research activities, and propose a reference architecture that can satisfy its challenging objectives.

The paper is organized as follows. Section 2 provides an overview of the role of cyber ranges in cybersecurity training. Then, Section 3 describes the importance of cybersecurity training in the healthcare sector, presenting the results of a study the AERAS Consortium carried out to lay down the basis of the platform requirements. finally, Section 4 presents the AERAS approach and reference architecture, and Section 5 draws our conclusions.

2 Cybersecurity Training with Cyber Ranges

Recent works [10] describe platforms to train trainees for known and new cyber-attacks by adapting to the continuously evolving threat landscape and examining if the trainees transfer the acquired knowledge to the working environment. In the same way, commercial products like Cyberbit Cyber Range[1] supply a training/simulation platform for the instantiation and management of hyper-realistic training centers, while the AIT Cyber Range[2], provided by the Austrian Institute of Technology, offers a virtual environment of flexible simulation of critical IT systems.

Several high-level commercial and public cyber ranges are available on the market. To name some, the Virginia Cyber Range[3] supplies a cloud-hosted virtual environment for training students in handling cybersecurity events. At the same time, the Michigan Cyber Range[4] focuses on strengthening the State's cyber defenses by providing one of the largest unclassified, network-accessible cybersecurity training platforms, while the National Cyber Range (NCR)[5] provides the ability to conduct realistic cybersecurity testing, evaluation (T&E) and training.

Looking at the private sector, the Italian Aerospace, Defence, and Security Company Leonardo provides a multipurpose operational environment that aims to create realistic operational training scenarios using best-of-breed

[1] https://www.cyberbit.com/

[2] https://cyberrange.at/

[3] https://virginiacyberrange.org/

[4] https://www.merit.edu/cyberrange

[5] https://www.peostri.army.mil/national-cyber-range-ncr

technologies for Infrastructure-as-Code provisioning, cloud management, software-defined networking[6].

Moreover, many projects funded by the European Commission under the Horizon 2020 Framework Program also provided high-quality cyber range platforms. THREAT-ARREST [6] marshaled modern training methods (i.e., emulation, simulation, serious gaming, and fabrication of realistic synthetic data) to enhance the learning experience for trainees. SPIDER cyber range [9] replicated a customized 5G network, enabling the execution of cyber-exercises that take advantage of hands-on interaction in real-time, the sharing of information between participants, and the gathering of feedback from network equipment, as well as the development and adaptation of advanced operational procedures. CYBERWISER cyber range platform [1] provided a multipurpose virtual environment where organizations can test critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their strategic information, services, and assets. Ukwand et al. [12] documented cyber range and test-bed platforms, characterizing them by type, technology, threat scenarios, applications, and the scope of attainable training. The analysis has been enriched by a taxonomy developed to provide a broader comprehension of the future environments.

Finally, Somarakis et al. [11] describe the link between Cyber Range training and Assurance, introducing a model-driven approach that facilitates the generation of ad-hoc training scenarios based on a comprehensive model-based description of the organization and its security posture. Cybersecurity training through Cyber Range has also been exploited for critical environments. In [7], authors describe the Cyber Arena environment, which puts together ICT architectures of two or more organizations, enterprises' business as well as enterprise interdependences of ICT architecture and business, modeling internet and cloud architectures at different tier levels, to achieve the capability for complex training environment in the cybersecurity domain.

3 Cybersecurity Training in the Healthcare Sector

Recent reports reveal gaps in healthcare infrastructure, training, and investment in cybersecurity. The EU Agency for Cybersecurity (ENISA) conducted the "Cyber Europe 2022" [2] exercise, highlighting the need for increased investment in healthcare cybersecurity. With over 900 participants, the exercise emphasized the growing challenges of cyber-attacks, necessitating more frequent local-level testing to enhance cybersecurity resilience in healthcare organizations.

According to ENISA's Threat Landscape 2022 report [3], the healthcare sector ranked sixth among targeted sectors, comprising 7.2% of cyber-attacks. It trailed behind public administration and government, digital service providers, the general public, services, and financial / banking services. Cyber-attacks in healthcare had a more significant social impact, mainly due to incidents involving the disclosure of private patient data or the unavailability of appointment booking services. These incidents had higher social implications than digital, economic, physical, and reputational impacts.

The findings of the NIS Investments 2022 report [4] show a majority (64%) of healthcare organizations are currently utilizing connected medical devices or Internet of Medical Things (IoMT) devices, with an additional 19% planning to deploy them in 2022. However, concerning is the fact that 38% of these organizations have deployed connected devices without implementing any security controls, rendering them vulnerable to cyber-attacks. The healthcare sector has experienced the highest percentage of significant security incidents from exploiting software and hardware vulnerabilities. Approximately 60% of respondents reported current usage of a Digital Health Cloud Platform or Solution, while around 30% planned

[6] https://shorturl.at/hvzAY

to adopt such a solution in the near future. Regarding cybersecurity awareness training programs, the report highlighted that 60% of healthcare organizations provide training for non-IT staff, but only 22% offer dedicated training. Surprisingly, 33% of healthcare organizations do not provide cybersecurity training for their non-IT staff.

To further explore and collect information regarding the needs and requirements for the AERAS platform, we conducted qualitative and qualitative surveys using interviews and questionnaires.

3.1 Interviews with the physicians

Healthcare organizations' cyber systems are exposed to various cyber-attacks and have become appealing targets for cybercriminals since they can reveal sensitive information. Healthcare professionals have varying access levels to the organization's data and systems. As a result, they must be aware of the current dangers and, where applicable, be prepared to respond and manage cyber security issues.

Cybersecurity is crucial for the healthcare system since the organization must secure patients' safety and privacy while ensuring patient care delivery effectiveness. To have robust cybersecurity protection, the institution must have performant technologies that protect its digital network and promote awareness among staff to engage in secure practices when managing patient data. Therefore, to create a platform that fulfills the objectives of healthcare stakeholders, it is necessary to understand their needs and requirements based on their perceptions of how cybersecurity risk management and cybersecurity training will be more effective.

The use of qualitative research as a first step in assessing the healthcare domain's cybersecurity situation was a tremendous opportunity, as it allowed for an in-depth understanding of the needs and expectations of healthcare staff. We performed extensive face-to-face interviews with physicians from EU countries about data access needs in a healthcare setting and cybersecurity training expectations. This enabled us to collect in-depth information about the expectations of non-IT experts about cybersecurity in the healthcare domain.

The qualitative study included interviews and focus groups with clinicians from several European countries. The study was designed as a semi-open interview in which the doctors were asked questions on *Data Access Needs* and *Cybersecurity Training Expectations*. Depending on the participant, the interviews lasted between 12 and 40 minutes. The study had 27 participants, six from Greece, nine from Romania, and 12 from France. In terms of demographics, there were 14 female and 13 male participants. Participants ranged in age from 24 to 67 years old, with a mean age of 39. Physicians came from different medical specialties, including general medicine, radiology, dermatology, ORL, accident and emergency, ophthalmology, and others. Figure 1 and Table 1 depict the distribution of the study participants.

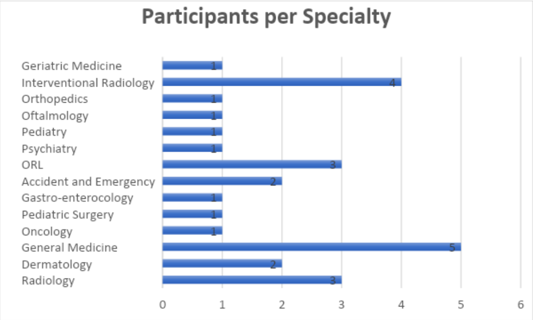


Fig. 1: Interviewed Participants per Medical Specialty

Doctors' requests for access to patient data have been examined, as well as technical challenges in the actual work environment to assess the current state of the healthcare domain. The interviewed physicians provided valuable insight into the types of patient personal information they handle daily, how they communicate with other healthcare colleagues, how

Table 1: Participants Socio-Demographic Information

Country	**no. Participants**	**Gender**		**Mean**	**Mean Work Exp.**
		Female	**Male**	**Age**	**(in years)**
Greece	6	1	5	39	12
Romania	9	6	3	33	7
France	12	7	5	43	16
ALL	27	14	13	39	12

and where they share patient private information, and what technical problems they may encounter daily.

3.1.1 Insights regarding Data Access Needs

Medical workers handle sensitive patient information regularly, including name, address, phone numbers, social security numbers, medical history, and socio-demographic data. Respectively, 66% of the physicians polled stated that they regularly share patient information inside and outside the hospital. Patient information must be shared among colleagues or other external health institutions for various reasons, including collaboration with specialists, thorough investigations, or simply seeking advice from another peer.

When asked how they communicate with other health professionals or share patient personal information, interviewees said they utilize internal hospital platforms or dedicated medical software and email, phone, fax, or paper files. Approximately half (48%) of the doctors polled stated that they utilize and communicate with colleagues digitally via a specific medical platform that is entirely secure via encrypted means. These platforms, however, are primarily local and limited to hospitals or city departments. Furthermore, nearly half of the clinicians polled (48%) said they consult or discuss patient information with peers using paper files. Some doctors indicated using personal emails or devices to communicate patient data in some situations. The choice of an unsecured mode of communication is motivated by time constraints and the availability of communication tools on personal devices (PCs, smartphones). The institution's internal platforms do not allow contact with other less secure media than the one they use, which impedes speedy and effective communication with colleagues.

Table 2 gives an overview of the communication means physicians use during their work, as emerged from the analysis. Additionally, the doctors interviewed stated that they frequently encounter *technological issues* while working on dedicated platforms and laptops. Respectively, 66.6% of physicians said the system or computer they work on often gets stuck or crashes. The clinicians have mentioned the following issues:

- PC or platform gets stuck;
- program crashes;
- programs work slowly;
- programs too big for the available infrastructure;
- slow speed;
- information gets lost, not sent, or received;
- software gives errors;
- old infrastructure and technological equipment;
- slow Wi-Fi connection;
- lack of technology equipment in some places (countryside mostly);
- can't access certain information;
- can't correct information if introduced incorrectly in the system, which requires help from the IT specialists for changing;

Table 2: Summary of Means of Peer-Communication

Means of communication	Benefits	Disadvantages
Internal Platform/Private Office Platform	– Highly secured platforms using encrypted means of share	– Platforms used locally (specific to each hospital or city) – Impossibility of sending information to another platform
Medical Files – Paper wise	– No need for costly technology infrastructure – Already in use – More accessible than digital versions	– Information gets lost, or paper deteriorates easily – Incomplete medical patients' file – Difficulty sharing patient information efficiently and fast
Email	– Professional emails: secure ways – Fast and accessible way of communication – Accessibility of individual or unit emails, separate emails	– Personal emails or devices: unsecure means of communication – Sometimes, there is a lack of individual employee emails, so we need to use a common unit email that has open access to everybody
Phone – verbal communication	– Fast and efficient communication	– Sharing only minimal information about the patient

3.1.2 Insights regarding Cybersecurity Training Requirements

It is critical to train medical workers in best practices for the institution's cybersecurity to ensure high-level cybersecurity for the health system as there is no one-size-fits-all approach to medical personnel training because humans are complex beings, the training/course should be tailored to the needs and expectations of the intended audience. The interviewed clinicians provided great insights into their cybersecurity training preferences and expectations.

When asked if cybersecurity matters in healthcare, one doctor stated, *"We know cybersecurity is important, but nobody told us why."* More than 90% of participants said that they want to take a cybersecurity course because they believe it is essential and useful to understand what cybersecurity is, what risks it entails for the healthcare system, and how to engage in best practices to protect patients and themselves. In terms of the material that doctors would like to see in such a course, they would like to see an introductory course that includes tips and tricks on what to do and what not to do at work to be secure.

According to their recommendations, the course should be kept as brief as possible, similar to a mini-course. Another critical consideration is whether the training should be deemed professional or personal time. They said they would expect more doctors to attend if the training was considered work time rather than personal time. Participants proposed several lengths for the course, including 1-3 hours, 3-5 days, one week, and one weekend. Almost half of the participants said the course should be repeated if significant updates become available. Other participants suggested that the course be repeated every six months, every year, or every two to four years.

Respectively, 70% of the participants mentioned that they would prefer to take such a course in person, with live participation, since they believe it is more dynamic and involved. It allows them to interact with the trainer/s more easily. However, other participants suggested the online format would be more convenient for doctors' busy schedules. In addition to the previously provided information on the content and format of a cybersecurity course for medical personnel, it is crucial to highlight that cybersecurity training should include themes on ethics, biased data, and how to interpret results accurately. Furthermore, training should be outcome-driven, ensuring that participants develop new abilities rather than simply learning for the sake of learning.

All physicians stated that they would like to be notified if there is a security breach in the healthcare system on the devices that doctors use. They would like to receive an alert message on the device indicating what is going on, what is not working, and who to contact, as well as a phone number to call for additional assistance. Furthermore, they stated that they would like to be able to do something to stop the security breach. Therefore, they would like to receive a notification with easy instructions, such as debranching the device, closing windows, or simply not touching it anymore.

Furthermore, 70.3% of physicians stated that they would like to have simulated trials of confirmed cases of security breach scenarios. They believe it should be part of the cybersecurity training course, and it might be helpful to test their understanding and how they react in a real-world scenario. Some participants suggested that these simulations should be similar to emergency scenarios for fires or terrorist attacks because they are just as essential. In terms of frequency, physicians stated that such simulation trials should be received just once a month or every 3-4 months to avoid disrupting their everyday activities. On the other hand, it was suggested that, instead of simulations, a test can be given from time to time to assess understanding of what to do in an emergency, and if they pass five times in a row, the test can be given less frequently.

"The simulations should not be too frequent because then you get used to them and not pay attention to it," explains one of the doctors interviewed. From a psychological standpoint, several techniques may increase or decrease pro-security behavior. According to studies, user behavior may improve cybersecurity management by employing tactics such as introducing unique polymorphic security warnings, rewarding and penalizing good and bad cyber behavior, or encouraging users to consider the long-term effects of their actions [8].

3.2 Online Survey with Healthcare stakeholders

The online survey aimed to investigate healthcare stakeholders' cybersecurity risk management and training requirements on a larger scale. It targeted personnel within the healthcare industry, including hospital administrators, IT staff, and medical professionals (doctors, nurses) handling sensitive patient information.

The survey covered various aspects, including anonymized demographic information, data access needs, existing cybersecurity training programs, security protocols, security monitoring systems, and cybersecurity training requirements. All participants responded to the demographic questions, while non-IT experts responded to questions related to cybersecurity training programs. IT experts exclusively responded to questions concerning security protocols, security monitoring systems, and cybersecurity training requirements.

By December 2022, 44 responses were collected: 17 from Greece, ten from the Republic of Cyprus, five from Italy, four from France, four from Romania, and one from Germany. Most participants fell within the age group of 20-60. The age group of 31-40 had the highest number of participants. The participants represented various health-related positions (see Figure 2), with doctors comprising the most

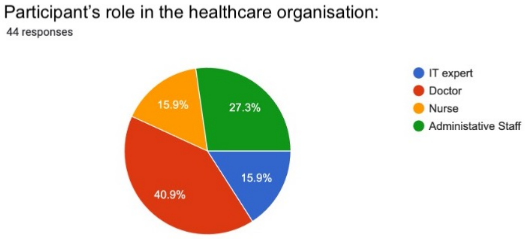


Fig. 2: Questionnaire participants per role in healthcare organization

significant proportion (approximately 41%), followed by administrative staff and nurses, each accounting for around 27%, and IT experts constituting approximately 16% of the participants.

Assessing Cybersecurity Threat Awareness in the Healthcare Industry
50% of the participants responded that they are aware of cybersecurity threats, showing confidence among healthcare personnel. Having 25% of the respondents answer with lower values (1 and 2) in the awareness scale may incline the need for more training and education in the healthcare industry to gain experience and increase the level of cybersecurity threat awareness among staff. Due to self-reported data and a small sample size, it is crucial to consider that the results may not be accurate. For this reason, we cannot generalize the results to the entire healthcare industry.

Data Access Information
The survey results on Data Access Needs revealed that approximately 47% of participants indicated that all listed roles, including doctors, nurses, administrative staff, and IT employees, have access to medical data. Additional roles, such as social workers and transporters, were also mentioned by some participants. However, only one participant said the practice of granting data access based on the medical specialty or position of the personnel. Most participants (around 84%) reported using online platforms as the primary method for accessing medical data, followed by paper files, email, and phone calls. Regarding patients accessing medical reports, the most common practice mentioned was through paper files, email, online platforms, and phone calls.

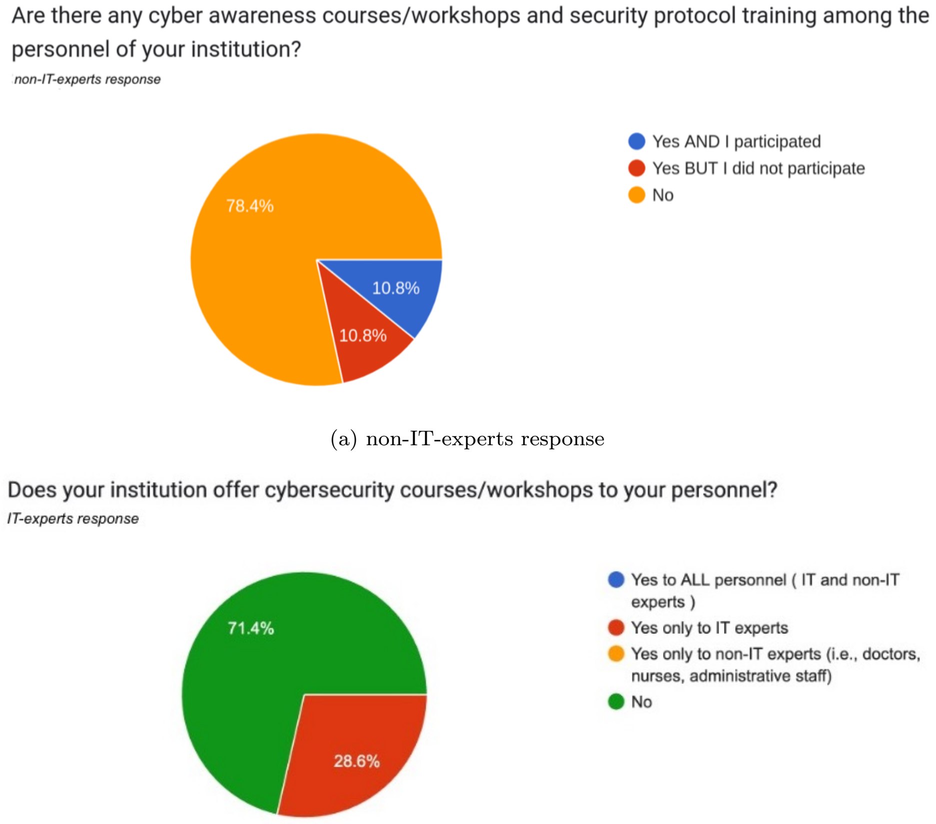
Cybersecurity training and education
This section of the questionnaire focused on non-IT expert participants, aiming to gather information about the presence and attendance of cyber-awareness training in their organizations. Figure 3a displays the responses, indicating that the majority of respondents answered *"NO,"* suggesting a lack of cyber-awareness training within their institutions or a lack of awareness about such training opportunities.

Additionally, 10.8% of participants mentioned that their organization offers cyber-awareness courses or workshops and security protocol training, but they did not participate. The reasons for non-participation remain unknown, as the training may not be mandatory for all personnel. Another 10.8% of non-IT expert participants (4 out of 37) reported attending cyber-awareness courses or workshops and security protocol training.

Participants who received cyber awareness training provided valuable insights into the current state of cybersecurity training in the healthcare sector. The training was primarily conducted by in-house IT experts rather than external security organizations. The topics covered in these workshops and seminars focused on data breaches, malware/viruses, phishing, and various attacks. Attendance was mandatory for personnel with access to medical data and systems, including doctors, nurses, administrative staff, and IT experts. Participants' evaluations varied regarding cybersecurity training sessions' assessment methods and frequency. The responses suggested a neutral level of satisfaction with the adequacy of the training in addressing cybersecurity topics and meeting their specific needs.

Health Organization Security Protocols and Controls

This section focuses on gathering insights from IT experts (7 out of 42 participants).



(a) non-IT-experts response

(b) IT-experts response

Fig. 3: Questionnaire results: Current state of Cyber Awareness courses in the healthcare organizations

All IT experts confirmed that their personnel are equipped with institutional emails, indicating organizations' interest in implementing robust and secure cybersecurity measures for email communications.

Regarding cybersecurity coverage, the primary defenses mentioned by participants are aimed at mitigating data breaches, malware, phishing, Man-in-the-Middle (MITM) attacks, and Distributed Denial-of-Service (DDoS) attacks. To prevent such cyber threats, healthcare organizations employ various tools and software, including firewalls, antivirus programs, encryption, Watchguard, email filters, penetration testing, Virtual Private Networks (VPNs), and public-key infrastructures (PKIs). Furthermore, it is vital to consider the most common causes of system downtime in healthcare organizations, with human error being the predominant factor at 85.7%.

Network failure, hardware/software malfunctions, security vulnerabilities, outdated hardware, natural disasters, and cybersecurity threats contribute to system failures.

Security Monitoring System
When surveyed about the presence of a cybersecurity monitoring system, approximately 43% of IT experts responded negatively, while around 29% were uncertain, and another 29% confirmed its existence.

Moreover, the results indicate that healthcare organizations do not fully utilize cybersecurity monitoring systems. In-depth exploration with participants who reported having such systems revealed concerns about performance, indicating possible shortcomings in implementation, configuration, scalability, compatibility, and user interface. The participants stressed the need for improvements to enhance the effectiveness and functionality of their organizations' cybersecurity monitoring systems.

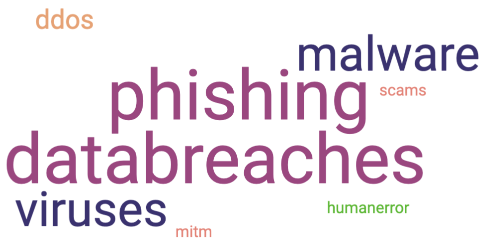


Fig. 4: Word Cloud of Cybersecurity topics for healthcare personnel training

Cybersecurity Training Requirements When queried about training provisions within their organizations, most IT experts (71.4%) responded negatively, as depicted in Figure 3b, indicating a limited scope of training initiatives.

IT experts identified vital threats such as data breaches, malware/viruses, phishing, DDOS attacks, MITM attacks, and human errors, serving as foundational topics for such training (see Fig. 4). Continuous security monitoring enables the updating of this list. IT experts underscored the significance of cybersecurity training for all healthcare personnel with access to organizational data and systems.

Evaluation methods employed after cybersecurity training varied among the IT expert participants. A combination of practical tests or simulations was favored, while written / multiple-choice questions were less preferred. This multifaceted approach enables a comprehensive assessment of employees' abilities and identifies areas for improvement.

The results show that written or multiple-choice tests are considered the most relevant to evaluate understanding of theoretical concepts and regulations like GDPR[7] and HIPAA[8], while simulations offer realistic scenarios to gauge staff members' ability to detect and respond to cyber threats. Practical tests in controlled environments resembling employees' daily routines can further assess their proficiency.

The IT experts favored evaluating trainees' scores based on correct answers (85.7%) and answer statistics (57.1%), with completion time receiving the most minor support. When considering the optimal frequency of cybersecurity training, participants favored annual sessions (42.9%), followed by every six months (42.9%) and monthly (28.6%) intervals.

3.3 Findings

A thorough understanding of what the end users need is critical for the successful creation of any system, and in this specific case, in the definition of technical requirements and reference architecture of AERAS. An understanding of the needs of users is crucial from the beginning of the process of building a new training system since it serves as the foundation for system design and verification. Users are individuals with diverse socio-demographic characteristics. Therefore, their requirements from a system are sure to differ.

As previous research and the current conducted studies' results show, cybersecurity awareness and learning the best practices to keep all information secure is an essential element for the end-users of any device, especially in a healthcare organization that stores so much personal data. As indicated by clinicians, due to stress, time pressure, and work overload, the medical personnel might not give much

[7] General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[8] Health Insurance Portability and Accountability Act, https://www.hhs.gov/hipaa/index.html

attention to security practices when handling patients' personal information, or they might not even be aware of all the risks. There is a need to train the employees of an institution or company to educate them about cybersecurity: risks, challenges, and best practices to engage in. Educating employees about cybersecurity systems used in their daily work can only drive the company's efficiency and productivity and the safe adoption and use of such systems. However, our survey results show that raising cybersecurity awareness among healthcare personnel is not a priority for their organizations. The existing cybersecurity training is not systematic and does not satisfy the cybersecurity needs of the fast-changing digitalization era.

As there is no *one-size-fits-all* approach to medical personnel training, the training course should be tailored to the needs and expectations of the intended audience, in this case, the preferences and expectations regarding cybersecurity training of the medical personnel. The elements that the clinicians want to learn about in a cybersecurity course are:

- How to do the work securely;
- How to know that the patient's information is secure;
- How to handle critical data;
- What are the risks of not using a secure program, and what are they exposing themselves to;
- What to do and not to do while working with patient-sensitive data in a digital format;
- How to share, transfer, and securely store patient information;
- Know basic information about the protection programs;
- How to keep information secure and anonymous;
- How to react in real case scenarios;

Furthermore, even if they are not security professionals, medical personnel should be ready to handle a security breach situation that may occur in the healthcare system on the equipment they often use. However, because they are not security professionals, the procedures they must do during an emergency should be presented briefly and straightforwardly. As a result, medical workers wish to know/see the following information about the impacted devices:

- Message on the device with:
  - what it is happening;
  - what it is not working;
  - who to contact, as well as the phone number to call;
- Simple instructions that need to be done to protect the device:
  - debranch the PC;
  - close windows;
  - simply not touch the PC anymore;
  - or the program closes by itself;
- Similar to anti-virus programs or notifications (e.g., an emergency alert sent by the government on the phone as an SMS):
  - Red alert in the middle of the screen to be obvious;
  - An exclamation mark indicating DANGER;
  - Written in simple words, non-technical language, and in the language of the country, not only English;

Furthermore, a training campaign cannot omit information regarding configuring the security mechanisms or spreading awareness of what the organization adopts regarding cybersecurity controls. The IT experts who participated in our study mentioned a list of security controls that are already in use:

- firewalls;
- antivirus programs;
- encryption;
- Watchguard;
- email filters;
- penetration testing;
- virtual private networks;
- public key infrastructures.

Additionally, the following topics are of high importance to be part of a cybersecurity training curriculum:

- data breaches;
- malware/viruses;
- phishing;
- DDOS attacks;
- MITM attacks;
- human errors.

The training must be obligatory for all healthcare personnel with access to data and systems and must be aligned with the trainee's role in the organization. There must be different levels of difficulty based on the expertise of the trainee.

Our survey findings validate that cultivating cybersecurity awareness within healthcare organizations is best achieved through hands-on practice with cybersecurity instead of theoretical seminars. In a protected environment, the trainees can interact with simulated, similar to their organization's systems, to be exercised and prepared to react to actual cybersecurity incidents. The combination of theoretical and practical exercises has shown to be the preferred evaluation method for the trainees' performance assessment. The frequency of the cybersecurity training can vary from organization to organization. However, our survey shows that having the training annually or every six months is a good compromise regarding the busy nature of the work of healthcare personnel.

The results of the questionnaire and the surveys lead us to a good understanding of the actual healthcare cybersecurity training landscape, laying the first basis and objectives of the AERAS platform. First, the platform should be easy to use and come directly to the point without wasting trainees' working time. The user interface should be clear and easily reachable from any device, giving trainees the freedom to access when and from where they are available. Then, the training should be easily tailored to the organization's needs. Even if the training requirements are similar for the whole healthcare sector, each organization has specific requests and gaps the training needs to fill. For this reason, the configuration of the system and the training course should be flexible and adaptable to any specific situation.

Finally, the organization should quickly reflect and monitor the training results. A continuous monitoring system should be in place to identify cybersecurity weaknesses and monitor the increased awareness of trainees to threats after and during the execution of exercises. Furthermore, the system should follow the evolution of the trainees' cybersecurity knowledge, allowing them to adapt the complexity and content of the exercises to the actual preparedness of the trainees.

4 The AERAS Approach

In the following, we draw up the principles of the AERAS reference platform and provide a list and a high-level description of the tools we expect to equip the platform with to satisfy the needs emerging from the analysis described in Section 3.

To comply with the needs that emerged from the questionnaires and interviews, as described in Section 3, the AERAS reference architecture has been designed as a set of macro-areas and single components better to manage any specific aspects of the integrated framework. Figure 5 overviews the overall platform with macro-areas and components.

In particular, the architecture is composed of the following macro-areas:

Training Tools, including all the components that manage the front-end and direct interactions with the trainers and trainees, the collection and evaluation of training results, and the description of the CRST models.

Cyber Range Tools, managing the storing, creation, deployment, and orchestration of the virtual environment composing the cyber range, including emulated and simulated components.

Assurance Tools, including all the functionalities to create, store, and manage the CRSA models and the facilities for the risk estimation and threats assessments.

Cyber-System Continuous Monitoring Aggregator, comprising the tools dedicated to assessing the Pilot's cybersecurity profile and monitoring the security landscape's evolution while the training activities run or after their conclusion.

Then, each macro-area has been specified in the set of tools that realize them, as described in Figure 5. For each of them, a short description of their functionalities and scope is provided in the following.

Visualization, which incorporates the front end of the AERAS platform, provides trainees, trainers, and admin with a user interface that allows each user category to access the relevant information and training environments. Trainees can access the training contents and the virtual training environment, trainers can see the progress of trainees associated with them and assign courses, and the admin can configure the overall system.

CRST Models, storing the CRST models that provide information and configuration about the training programs created and configured.

Programme Adaptor, that is in charge of raising warning and alert on the level of difficulty of training activities concerning the results of the trainees on this specific activity.

Performance Evaluator, that evaluates the trainees' performance after completing the assigned training activities.

Progression engine, service component dedicated to monitoring trainees' activities within the virtual environment; the Programme Adaptor and Performance Evaluator will consume data from the component to rate trainees' work.

Resource Pool, storing and managing the images of the virtual environments that are instanced by the Cyber System Emulator and accessed by the trainees to complete the training activities.

Cyber System Emulator, service module that is dedicated to the instantiation of the virtual environments and the creation of the virtual channel used by the trainees through the Visualization to access them; the Emulator will use data from CRSA Models to configure the virtual machines.

Training Orchestrator, service module dedicated to the orchestration of the initialization of the virtual environment, integrating the emulated and simulated elements specified in the CRSA and CRST models, providing and configuring the proper connection between them.

Cyber System Simulator, service component that will create and manage the simulated activities; they will be created following the specification included in the CRSA Model. The Simulator will inject simulated events directly into the emulated component to simulate, for example, attacks and realistic situations the trainees should cope with and find solutions.

CRST Programme Generator, a service module combining information from the CRSA and CRST models to configure and trigger a virtual training environment. The model will be translated in a different format if needed by the Emulator and Simulator components.

CRSA Model, component that stores and manages the CRSA Models provides facilities to access and use them by the other platform modules.

CRSA Model Editor, that guides the admin in creating and maintaining the CRSA Models, with specific sections for each CRSA sub-model, providing facilities to help users fill them.

Cyber System Real-time Risk Evaluator, service module that evaluates the overall risk profile of the Pilot, using and providing inputs from/to the assets described in the CRSA Models.

Threat Assessor, similarly to the Cyber System Real-time Risk Evaluator, the component analyses the Pilot concerning the threats described in the CSLA Threat and Incidents Submodel, providing input on the overall cybersecurity profile of the Pilot.

Training Performance Monitor, a service module that takes in input the performance of the trainees executing the training activities and the changes in the overall Pilot's cybersecurity profile, looking for a correlation between the two to give evidence on the effectiveness of

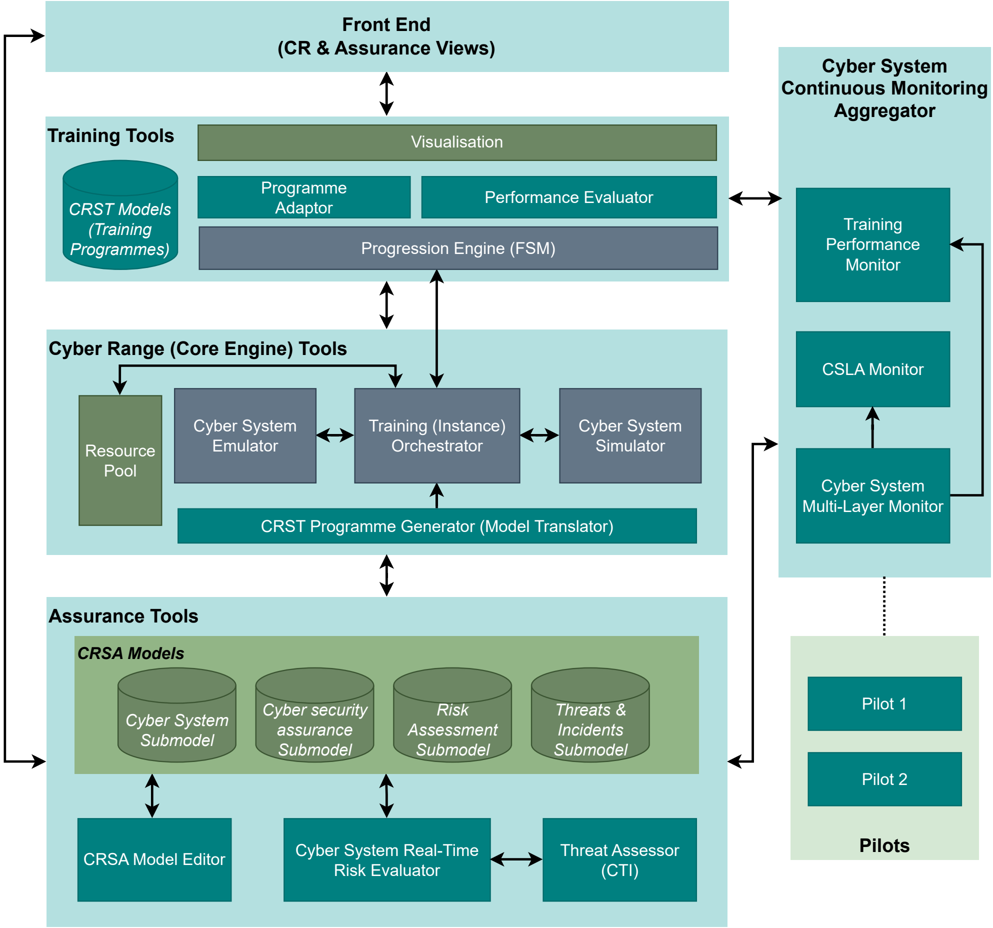

Front End
(CR & Assurance Views)
Training Tools
CRST Models (Training Programmes)
Visualisation
Programme Adaptor
Performance Evaluator
Progression Engine (FSM)
Cyber Range (Core Engine) Tools
Resource Pool
Cyber System Emulator
Training (Instance) Orchestrator
Cyber System Simulator
CRST Programme Generator (Model Translator)
Assurance Tools
CRSA Models
Cyber System Submodel
Cyber security assurance Submodel
Risk Assessment Submodel
Threats & Incidents Submodel
CRSA Model Editor
Cyber System Real-Time Risk Evaluator
Threat Assessor (CTI)
Cyber System Continuous Monitoring Aggregator
Training Performance Monitor
CSLA Monitor
Cyber System Multi-Layer Monitor
Pilot 1
Pilot 2
Pilots

Fig. 5: AERAS high-level proposed architecture.

the platform in improving the general knowledge and application of the course's topics.
CSLA Monitor takes as input the formalization of Pilot's Cybersecurity SLAs, verifies their satisfaction (or not), supplying inputs Cyber System Multi-Layer Monitor.
Cyber System Multi-Layer Monitor, that verifies and keeps monitoring the overall cybersecurity profile of the Pilot, giving input to the Training Performance Monitor; trends detected by the component are essential to the validation or the AERAS approach.

The team is now focused on selecting the best-fitting technologies that could be exploited to reach the ambitious goals of the AERAS framework. In particular, the Cyber System Emulator module is the core component that will drive the design of the other modules. As described in Sec. 2, many frameworks have been examined, but all lacked important properties like availability, community support, and documentation, which made them not indicated to be included in the framework.

The analysis has been extended, and the cyber range framework Kypo[9] [13], recently released as open source, has been selected as the best candidate to be included. Kypo has been engineered to enable the creation of complex virtual networks with full-fledged operating systems and network devices. Kypo is

[9] https://crp.kypo.muni.cz/

also full-model based, allowing us to adopt our approach fully. In parallel, the team is now designing the adaptation of Kypo models to AERAS-specific CRSA and CRST models.

The next steps will include integrating assurance monitoring tools of the Cyber System Continuous Monitoring Aggregator area, considering the specific peculiarities of the Kypo framework and the installation and validation in the pilot sites.

5 Conclusions

This paper analyzed the need for solid cybersecurity training in the healthcare sector. In the context of the European project AERAS, we administered a survey with one-to-one interviews and a questionnaire to analyze the needs and requests of people working in the sector, whose qualitative and quantitative results are well-described in the text. Furthermore, the data gathered by the study have been used to elicit the requirements and to define the reference architecture of AERAS.

The proposed architecture has been presented, designing a framework that can adapt to the different cases and needs that emerged during the interviews. The project aims to supply trainees and trainers with a cyber range infrastructures and a set of tools that can be easily adapted to the different training needs and that can continuously monitor the assurance status of the adopting organization to evaluate the effectiveness of training activities and the enforcement of the cybersecurity concepts subject of the courses.

The analysis carried out in Sec. 2, followed by the research in Sec. 3, allowed us to understand the gaps to be filled in the specific case of cybersecurity training in healthcare. The AERAS framework will supply trainees and trainers with a comprehensive environment to satisfy their needs for tailored courses and a quick and *no-frills* interface that will drive them directly into the teaching phase.

Declaration Statements

Conflict of Interest Statement: The authors declare no conflicts of interest related to this research.

Funding Statement: This work has been partly funded by the European Commission within the H2020 MSCA project AERAS (Grant No. 872735).

Compliance with Ethical Standards: The authors received ethical approval to conduct this study from the Ethics Committee of the University of Milan. Additionally, all data collection procedures for non-personally identifiable information were approved by the Data Protection Officers of the AERAS project beneficiaries.

This study involved the administration of questionnaires and interviews with human subjects. The study adhered to ethical principles, and participants' consent was obtained before involvement. The authors ensured that all participants were informed about the nature of the study, their participation was voluntary, and their responses were kept confidential and anonymous.

Research Data Policy and Data Availability Statements: The questionnaire responses and interview data collected for this study were anonymous and kept confidential to ensure participants' privacy. We will submit the anonymized data supporting this research's findings to a public archive after publication.

References

1. Basile, M., Dini, G., Varano, D.: CYBERWISER.eu: Innovative cyber range platform for cybersecurity training in industrial systems. Electronic Communications of the EASST **79** (2020). DOI 10.14279/tuj.eceasst.79.1114.1065. URL `http://dx.doi.org/10.14279/tuj.eceasst.79.1114.1065`
2. ENISA: Cyber europe 2022: After action report. `https://www.`

enisa.europa.eu/publications/cyber-europe-2022-after-action-report. Accessed: 15 Dec. 2022

3. ENISA: ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. Accessed: 01 Dec 2022
4. ENISA: NIS investments 2022. https://www.enisa.europa.eu/publications/nis-investments-2022. Accessed: 30 Nov. 2022
5. Ferguson, B., Tall, A., Olsen, D.: National cyber range overview. In: 2014 IEEE Military Communications Conference, pp. 123–128 (2014). DOI 10.1109/MILCOM.2014.27
6. Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Braghin, C., Damiani, E., Koshutanski, H., Tsakirakis, G., Hildebrandt, T., Goeke, L., Pape, S., Blinder, O., Vinov, M., Leftheriotis, G., Kunc, M., Oikonomou, F., Maglio, G., Petrarolo, V., Chieti, A., Bordianu, R.: The THREAT-ARREST cyber range platform. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 422–427 (2021). DOI 10.1109/CSR51186.2021.9527963
7. Karjalainen, M., Kokkonen, T.: Comprehensive cyber arena; the next generation cyber range. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 11–16 (2020). DOI 10.1109/EuroSPW51379.2020.00011
8. Moustafa, A.A., Bello, A., Maurushat, a.: The role of user behaviour in improving cyber security management. Front Psychol. **12** (2021). DOI 10.3389/fpsyg.2021.561011. URL https://pubmed.ncbi.nlm.nih.gov/34220596/
9. Rebecchi, F., Pastor, A., Mozo, A., Lombardo, C., Bruschi, R., Aliferis, I., Doriguzzi-Corin, R., Gouvas, P., Alvarez Romero, A., Angelogianni, A., Politis, I., Xenakis, C.: A digital twin for the 5g era: the spider cyber range. In: 2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 567–572 (2022). DOI 10.1109/WoWMoM54355.2022.00088
10. Smyrlis, M., Somarakis, I., Spanoudakis, G., Hatzivasilis, G., Ioannidis, S.: CYRA: A model-driven cyber range assurance platform. Applied Sciences **11**(11) (2021). DOI 10.3390/app11115165. URL https://www.mdpi.com/2076-3417/11/11/5165
11. Somarakis, I., Smyrlis, M., Fysarakis, K., Spanoudakis, G.: Model-driven cyber range training: A cyber security assurance perspective. In: Computer Security, pp. 172–184. Springer International Publishing (2020)
12. Ukwandu, E., Farah, M.A.B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., Bellekens, X.: A review of cyber-ranges and test-beds: Current and future trends. Sensors **20**(24) (2020). DOI 10.3390/s20247148. URL https://www.mdpi.com/1424-8220/20/24/7148
13. ČELEDA, P., ČEGAN, J., VYKOPAL, J., TOVARŇÁK, D.: Kypo - a platform for cyber defence exercises. In: STO-MP-MSG-133: M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. Munich (Germany): NATO Science and Technology Organization, pp. 1–12. NATO (2015)