TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Ketevan Jebisashvili 202487IVSB

An E-learning Module on Cybersecurity Risk Awareness for Healthcare Personnel: a Case Study of Georgia

Bachelor's thesis

Supervisor: Kaido Kikkas, PhD

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Ketevan Jebisashvili 202487IVSB

Küberturvalisuse riskiteadlikkuse e-õppemoodul tervishoiutöötajatele: Gruusia juhtumiuuring

Bakalaureusetöö

Juhendaja: Kaido Kikkas

Tallinn 2023

Author's declaration of originality I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Ketevan Jebisashvili

Abstract

This paper presents a case study of Georgia's healthcare organizations and their implementation of a multimedia learning program for healthcare IT security training. The authors applied Mayer's principles of multimedia learning to design an effective and engaging program that addressed the specific needs and risks of the healthcare industry. The program was developed in accordance with the ISO 81001 standard for healthcare security risk management, utilizing a risk-based approach to identify, analyze, evaluate, treat, and monitor security risks. Through a survey of healthcare professionals, high-risk areas were identified, and risk treatment options such as implementing antivirus software, establishing password management policies and procedures, and providing training on recognizing security breaches were developed and implemented. The effectiveness of the program was monitored and reviewed to ensure that the identified risks were being addressed and that desired outcomes were being achieved. In summary, the case study demonstrates the importance of incorporating multimedia learning principles and a risk-based approach to healthcare IT security training, and provides valuable insights for other healthcare organizations looking to enhance their security posture.

This thesis is written in English and is 37 pages long, including 6 chapters, 4 figures

and 1 table.

Annotatsioon

See artikkel tutvustab juhtumiuuringut Gruusia tervishoiuorganisatsioonidest ja nende poolt tervishoiu IT-turbekoolituse multimeediaõppeprogrammi rakendamisest. Autorid rakendasid Mayeri multimeediaõppe põhimõtteid, et koostada tõhus ja kaasahaarav programm, mis käsitleb tervishoiutööstuse spetsiifilisi vajadusi ja riske. Programm töötati välja vastavalt tervishoiu turvariskide juhtimise standardile ISO 81001, kasutades turvariskide tuvastamiseks, analüüsimiseks, hindamiseks, käsitlemiseks ja jälgimiseks riskipõhist lähenemist. Tervishoiutöötajate küsitluse kaudu selgitati välja kõrge riskiga valdkonnad ning töötati välja ja rakendati riskide käsitlemise võimalusi, nagu viirusetõrjetarkvara juurutamine, paroolihalduspoliitika ja protseduuride kehtestamine ning turvarikkumiste äratundmise koolitus. Programmi tõhusust jälgiti ja vaadati üle, et tagada tuvastatud riskidega tegelemine ja soovitud tulemuste saavutamine. Kokkuvõttes näitab juhtumiuuring multimeedia õppimise põhimõtete ja riskipõhise lähenemisviisi kaasamise tähtsust tervishoiu IT-turbekoolitusse ning annab väärtuslikku teavet teistele tervishoiuorganisatsioonidele, kes soovivad oma turvalisust parandada.

See lõputöö on kirjutatud inglise keeles ja on 37 lehekülge pikk, sealhulgas 6 peatükki, 4 joonist ja 1 tabel.

List of abbreviations and terms

CERT	Computer Emergency Response Team
EHR	Electronic Health Records
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
HIPAA	The Health Insurance Portability and Accountability Act
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
UTM	Urchin Tracking Module

Table of contents

List of Figures

List of Tables

1. Introduction

The purpose of this research is to raise awareness towards healthcare industry workers. According to the World Healthcare Organisation (WHO) digital technologies are becoming an inseparable part of medical organisations[1]. With this ongoing trend, cyberattacks are becoming a more frequent issue in companies that provide medical care. Due to the sensitivity of data patients share, It is crucial to educate employees about common threats.

A case study for this research will be Georgia. Since this country does not have its own standards specifically for this reason, neither does it fall in GDPR scope, ISO 81001 standard will be used to back up the research modules. This standard specialises in health software and health IT systems security and is applicable to all organisations and people whose work is related to the field. It is very important to understand that research groups are independent employees from different hospitals or universities, so organisation specific implementation can't be conducted.

The thesis will try to answer the following questions: Is e-learning module a good approach to raise cybersecurity awareness in industry and what are the most successful instructional design methodologies and content elements?

1.1 Problem Statement

In 2008, After the 2008 Russo-Georgian war Georgia received various cyberattacks on air, sea and land domain[2]. One of the most notable cyberattacks was the distributed denial-of-service (DDoS) attack on Georgian government and media websites. This involved overwhelming the websites with traffic to make them inaccessible to users. The attack affected websites such as the president's website, the Ministry of Foreign Affairs, and several news outlets. It was after this war that Georgia decided to take action over their cyber defence systems.

Sadly, there is no cybersecurity training provided to healthcare employees in Georgia. Only financial organisations get this type of training as the public considered it the most targeted industry.

This problem is encountered worldwise. According to a study 70% of healthcare workers in Europe reported not receiving any type of related training at the workplace[3] . This increases risks of cyberattacks and patient data breaches, which in this industry puts people's health in danger.

2. Background

Following section will provide background information about mission-critical healthcare infrastructure and cybersecurity importance regarding it. It also provides a brief overview of the current situation in Georgia and importance of standards. Lastly, related work will be analysed.

2.1 Mission-Critical Healthcare Infrastructure

Mission critical infrastructure is all about organisations and institutions that are essential for common welfare and where disruptions or interruptions can lead to deficiencies to public safety, scarcities in supplies, breaches of data security, or other very serious outcomes. The vital equipment, facilities, and systems that are necessary for giving patients prompt and efficient medical care are referred to as mission-critical healthcare infrastructure.Due to a number of reasons, including the high value of healthcare data on the black market, the increasing use of EHRs, and the predominance of outdated and vulnerable technology in the healthcare sector, healthcare is one of the most frequently targeted by cyberattacks. According to CheckPoint Research in 2022, there were 1,463 weekly cyberattacks against healthcare organisations worldwide making it the third most attacked sector[4]. Connected medical devices can cause serious consequences if exploited. Cynerio's research report suggests that in a typical hospital, more than half of

the connected devices have serious risks. Most important are IV pumps (38% of a hospital's IoT footprint). The safety of patients could be compromised by almost 3/4 of IV pumps' vulnerabilities[5].

2.2 Security and privacy concerns in healthcare industry.

In the research paper "Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations" [6] authors suggest the idea of "You are only as safe as your 'weakest' person". Authors also highlighted several key challenges that healthcare organisations face when it comes to cybersecurity. The authors noted that healthcare organisations are prime targets for cyber attacks due to the sensitive nature of the data they hold, including patient health information (PHI) and personally identifiable information (PII). They argued that healthcare organisations must adopt a proactive approach to cybersecurity, rather than relying on reactive measures, to address these challenges effectively.

The literature emphasizes that healthcare organizations face trade-offs when it comes to cybersecurity. For example, implementing measures to enhance privacy may cause delays in completing referrals, while the financial and resource costs of cybersecurity measures may be significant. To address these challenges, it is suggested that healthcare organizations adopt a portfolio approach to managing IT projects and prioritize their use of resources accordingly.

Another concern in deciding on HIT risk trade-offs is the idea of "hiding in the bell curve," which suggests that organizations may not want to be too far ahead or behind their peers in meeting regulatory requirements. It is unlikely that being in the middle of the peer group will disadvantage an organization competitively or attract unwanted regulatory attention.

The literature suggests that healthcare organizations should take a comprehensive approach to cybersecurity rather than dealing with threats on a case-by-case basis. This approach involves viewing security in the context of processes rather than relying solely on technological fixes. The CERT Resilience Management Model is cited as an example

of a comprehensive approach to cybersecurity, which involves evaluating process areas throughout the organization and establishing a governance structure over each process to ensure adequate planning, training, financing, and other factors to achieve required resilience.

The literature review also revealed that healthcare organisations face several specific privacy and security concerns, such as ransomware attacks, insider threats, and the risks associated with the use of mobile devices and social media. To address these concerns, the authors suggested several best practices for healthcare organisations to improve their security posture, including implementing strong access controls, conducting regular risk assessments, and ensuring that all employees receive comprehensive cybersecurity training. The article suggested that training employees in are of the appropriate and cautionary use of handheld devices. is very important and

The study A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures by Fotios Gioulekas [3] suggested that 70% of ICT personnel in European healthcare industries admitted of not getting any cybersecurity trainings and identified main reason of not having security handling and incident response departments in the workplace. They also suggested that lack of ICT staff is the main reason for not having the trainings and found the pattern between the number of IT personnel and awareness of healthcare workers in hospitals. The implementation and deployment of security awareness programs, along with training procedures, have been identified as a necessity for healthcare institutions to combat cybersecurity threats effectively. This assertion is supported by the findings of a study that showed that 76% of non-ICT personnel in healthcare institutions agreed that following the hospitals' security policies would help them perform their job better.

The study's results were communicated to the institutions' management, and proactive and reactive cybersecurity measures were implemented during the COVID-19 crisis. The management allocated a certain budget to procure or upgrade cybersecurity systems and software, such as antivirus databases and UTM firewalls with IDS/IPS. A specialised workshop was conducted with the support of ENISA for the ICT staff, which was reinforced in several cases. Additionally, in-house awareness campaigns for non-ICT employees about anti-phishing or anti-social engineering were periodically

conducted. Those who dealt with sensitive data and processes participated in GDPR related seminars.

The study's authors plan to revisit the updated cybersecurity measures and strategies and re-perform an extensive assessment to re-evaluate the new level of cybersecurity awareness and personnel readiness. The study emphasises the importance of taking a proactive approach to cybersecurity by implementing security awareness programs and training procedures in healthcare institutions. The results demonstrate that such measures can lead to increased personnel readiness and improved performance, and can also help institutions to combat cybersecurity threats effectively.

2.3 Role of standards in healthcare industry

In their work “The landscape of cybersecurity vulnerabilities and challenges in

healthcare: Security standards and paradigm shift recommendations” Authors Kitty Kioskli [7], Theo Fotis and Haralambos Mouratidis talk about cybersecurity vulnerabilities and attacks that the healthcare sector faces. The authors also explore the potential of using living labs and healthcare domain standards to address these vulnerabilities and challenges. Specifically, the paper discusses the need for a comprehensive approach to cybersecurity in healthcare that incorporates best practices and standards. It talks about several standards in industry including ISO 81001, which purpose is defined as “to adpot a coordinated approach on security and safety of healthcare devices”. According to research ISO/IEC 81001-1 emphasises the significance of information transfer as a product that goes through a cycle from the manufacturer to the implementer, integrator, and finally, the user. The standard aims to harmonise definitions and simplify terms in this cycle as much as possible. This information includes configuration, usability, and risk, all necessary to maintain and transfer ownership of the product.

In the paper “Threat Modeling Methods in the Medical Device Industry: An Integrative Literature Review” [8] author praises ISO 81001’s threat modelling paragraph and it’s

contribution to the risk management process by identifying potential threats to the software and infrastructure, which can cause risks to the users and environment using the software.

The research “Risk management in academic medical device research environment” by Viivi Lankinen [9] indicates that ISO 81001 focuses on ensuring the safety, effectiveness, and security of health software and IT systems. It covers various types of health software, including software as a part of medical devices, software as a part of specific health hardware, software as a medical device, and software-only products for other uses. Its primary aim is to enhance the information security of health software by establishing specific activities and tasks throughout the software life cycle processes.

IEC 81001-5-1 is essential because health software is increasingly becoming an integral part of healthcare delivery, and the security risks associated with it are also increasing. The standard provides a framework for ensuring the security and effectiveness of health software through a systematic approach. By integrating TRA into the risk management system, it enables organisations to identify and mitigate potential security threats proactively.

Thus, in relation to thesis, Training healthcare workers on standards such as IEC 80001-1 and IEC 81001-5-1 can help to ensure that they are aware of the necessary steps to manage risks associated with medical devices and health IT systems. By understanding the standards and their requirements, healthcare workers can better incorporate medical devices into IT networks and develop and maintain health software in a safe, effective, and secure manner.

2.4 Georgia’s cybersecurity strategy

Georgia has a strong focus on cybersecurity and has implemented several initiatives to improve its cybersecurity standards. In 2021, the country launched its 3rd Cybersecurity Strategy, which aims to enhance the country's cybersecurity capacity, protect critical infrastructure, and promote a secure digital environment [10].

The strategy focuses on developing a comprehensive legal framework for cybersecurity, improving coordination between government agencies and private sector stakeholders, promoting cybersecurity education and awareness, and developing a national incident response capability.

In addition to the strategy, Georgia has also established the Cyber Security Bureau, a government agency responsible for cybersecurity policy and incident response. The Bureau works closely with other government agencies and private sector organisations to develop and implement cybersecurity policies and initiatives.

ISO 81001-1 is a fairly new standard as it was finalised in 2021. While these standards have been adopted at national and international levels, there is limited research on their effectiveness in improving the safety, security, and effectiveness of health IT systems. In particular, as these standards are fairly new, there is a lack of literature on their implementation and impact on the healthcare industry.

In the case of Georgia, a country that has been undergoing rapid modernization in the healthcare industry, there is a lack of resources available for implementing these standards and ensuring the security of health IT systems. There is also a dearth of research on the challenges and opportunities for implementing these standards in a country like Georgia, which is still grappling with the impact of the COVID-19 pandemic on its healthcare infrastructure. In addition, there are few e-learning modules or training resources available to healthcare workers in Georgia on how to incorporate these standards into their practice, indicating a need for further investment in education and capacity building in this area. Overall, there is a significant gap in the literature on the implementation and impact of these standards in the context of Georgia, highlighting the need for further research and investment in this area.

Main reason the country struggles with training workers in the country is financial problems within the country. Although it is considered to be an upper middle income country [11], it still struggles to fund cybersecurity training. For comparison, a similar size high income country can be taken - New Zealand, with a population of 5 million [12]. Georgia’s current GDP is 28B USD while New Zealand’s is 252B USD [13]. Which gives New Zealand more budget to finance training of the population. In

practice it is conducted by Cyber Security Skills Taskforce, which was funded with $257 million in launching year - 2016 [14].

2.5 Related Work

An analysis of the online materials reveals that there are several e-learning module research in the healthcare industry, Upon conducting an extensive review of the available academic literature, it was found that no e-learning module on healthcare cybersecurity with Georgia as a case study was identified. There is evidence of numerous e-learning modules being developed and utilised in various countries around the world to educate healthcare professionals on cybersecurity best practices. However, the lack of an e-learning module specifically focused on healthcare cybersecurity with Georgia as a case study highlights the need for more tailored and localised e-learning solutions. The research conducted on Korean and Malaysian study group conducted that this type of modules motivated 54.1 % of participants were motivated to learn more about the subject [15]. The other paper concludes that cybersecurity awareness doubled after study group completed the learning module. It has to be noted that none of the researches were based on ISO 81001 standard but their goal was to rise awareness and minimise cyber security breaches in industry.

The “Cybersecurity Training in the Healthcare Workforce – Use of the ADDIE Model” purposes the new effective model for the training [16]. The instructional design process typically comprises five interrelated phases: **A**nalysis, **D**esign, **D**evelopment, **I**mplementation, and **E**valuation. These phases involve identifying the learning objectives, determining the most effective approach to learning, creating the learning materials, integrating them into real-world contexts, and assessing the outcomes and effectiveness of both the learning materials and the instructional design process itself. In short, the five phases of the instructional design process involve analysing, designing, developing, implementing, and evaluating the learning materials and process. During the workshop, participants were provided with critical information regarding potential cyber attacks, as well as the reasoning behind specific actions they should take to mitigate such attacks. By highlighting the benefits of certain actions, the workshop aimed to help participants develop a deeper understanding of how their decision-making

processes can impact cybersecurity and encourage them to make safer choices. In summary, the workshop not only explained the nature of cyber attacks but also emphasised the importance of taking proactive measures to prevent them.
The literature highlights the significant role of healthcare workers in influencing the strength of cybersecurity in healthcare organisations. It is essential to acknowledge that all healthcare workers have a duty to ensure that cybersecurity measures are in place and adhered to, given that there are approximately 59 million healthcare workers worldwide. As a result, all healthcare workers require cybersecurity training programs that can improve learning outcomes regardless of their role.

Numerous medical care associations have perceived the significance of giving network safety training to their workers and have made their own instructional classes. For example, the UK National Health Service (NHS) sent off the 'Keep I.T. Classified' crusade in 2019 to teach their representatives on key network safety dangers, for example, phishing, cell phone dangers, and social designing.

Many healthcare organisations have recognized the importance of providing cybersecurity training to their employees and have created their own training courses. For instance, the UK National Health Service (NHS) launched the ‘Keep I.T. Confidential’ campaign in 2019 to educate their employees on key cybersecurity threats such as phishing, mobile device risks, and social engineering. The campaign was successful in increasing general awareness of cybersecurity in the organisation. However, the literature suggests that there is still a lack of cybersecurity training content specifically designed for nursing practices and students.

Study found out that motivation and confidence are of utmost importance when it comes to education, as they are key factors that significantly contribute to the success of any training program, and best way to increase this factor is to give them real life examples which will aid their willingness to learn.

Literature research has concluded that e-learning cybersecurity training is very rare and if it exists, it’s primarily provided to IT specialists and not industry workers. For that reason the industry lacks materials to prevent major breaches. Normally, within these

sectors IT specialists are a very small percentage of total industry workers and major breaches are mostly caused by people who don’t come from such backgrounds. For all these reasons it is very important to train people within industry and raise awareness.

3. Methodology

A risk-based approach can assist in identifying and prioritising the most important assets and systems that need to be protected in healthcare organisations. By concentrating on the areas that are most susceptible to attack and implementing targeted controls to lower those risks, this approach can assist organisations in allocating their resources effectively[4]. (“Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks - Check Point Software”)

In general, a risk-based strategy is a key component of a healthcare organisation's cybersecurity strategy. Employing this strategy enables healthcare organisations to proactively identify and reduce potential risks, safeguard vital infrastructure, and guarantee the confidentiality, integrity, and availability of patient data.

The research methodology consisted of five main steps. First, a risk assessment was conducted using a survey specifically designed for healthcare professionals. The survey aimed to identify and prioritize the risks associated with health software and health IT systems safety, effectiveness, and security. Second, the identified risks were mapped with ISO standards, including IEC 81001-1 and 81001-5-1, to ensure compliance with international standards. Third, an e-learning module was developed with specific learning objectives and appropriate instructional material. An evaluation plan was also created to assess the effectiveness of the module. Fourth, the module was implemented and sent to the study group, which consisted of healthcare professionals. Feedback from the learners was collected in the form of a survey, and possible areas for future development were identified. Finally, the findings were recorded and presented, demonstrating how well the e-learning module worked to increase the knowledge and comprehension of health software and health IT systems among healthcare workers. It

should be mentioned that the study was carried out in Georgia, a nation with few resources and little written material on protecting the healthcare sector.

After conducting the risk assessment and mapping identified risks with ISO standards, the author utilized Mayer's principles of multimedia learning to guide the development of the e-learning module. To do this, interactive learning materials had to be developed, including case studies, quizzes, and films that were matched to the precise learning goals noted in the risk assessment.

The author developed an evaluation plan that includes a survey to gauge learner satisfaction and information retention in order to guarantee the module's efficacy. After the module had been implemented, a survey was given to the study group, and the results were analyzed to determine how the module had affected the learners' knowledge and understanding of the effectiveness, security, and safety of health software and IT systems.

The survey also asked participants to list areas in which they felt the module could be improved upon in the future. This allowed the authorto gather insights into how the module could be improved and tailored to better meet the needs of healthcare professionals in Georgia.

The evaluation plan aimed to assess the effectiveness of the e-learning module in improving learners' knowledge and understanding of health software and health IT systems safety, effectiveness, and security. The survey used to collect feedback from the learners included questions about the module's design, content, and relevance to their work. It also assessed the learners' level of satisfaction with the module and their confidence in applying the acquired knowledge to their daily practice.

The research methodology was designed to address the specific challenges and limitations faced by healthcare professionals in Georgia when it comes to securing health software and health IT systems. By utilising a risk-based approach, mapping identified risks to international standards, and incorporating Mayer's principles of multimedia learning into the development of the e-learning module, the author was able to create an effective training tool that could help healthcare professionals in Georgia better understand and mitigate cybersecurity risks in their industry.

4. Developing the e-learning module

Research was conducted in several steps: risk assessment which was important to identify the risks, mapping risks to standards and developing a module on relevant topics.

4.1 Risk assessment

Total of 27 medical workers were asked to complete a questionnaire about their daily work routines and basic cybersecurity practices. The purpose of the questionnaire was to gain insight into the current cybersecurity practices within the healthcare industry and identify areas for improvement. The questionnaire covered topics such as password management, data backup procedures, and software update practices. The responses were analyzed to identify areas of concern and potential risks. The table 1 shows answers about questionary questions.

The first set of questions in the survey was designed to assess the basic understanding of cybersecurity concepts among the medical workers. This was important because it helped to identify the areas where the workers lacked knowledge and where the training module should focus on. It is crucial for healthcare professionals to have a fundamental understanding of cybersecurity concepts as they deal with sensitive patient data that must be kept confidential and secure.

By ensuring that healthcare workers have a basic understanding of cybersecurity concepts, they can better identify potential security risks and take steps to mitigate them. This can include using secure passwords, recognizing phishing attempts, and reporting suspicious activities. Without this basic knowledge, healthcare workers may unknowingly put sensitive data at risk.

Therefore, the first set of questions in the survey was essential to assess the current level of knowledge among medical workers regarding basic cybersecurity concepts. This information helped to shape the content and delivery of the training module to ensure that workers have a solid foundation in cybersecurity before moving on to more advanced topics. Survey results are illustrated in Figure 1.

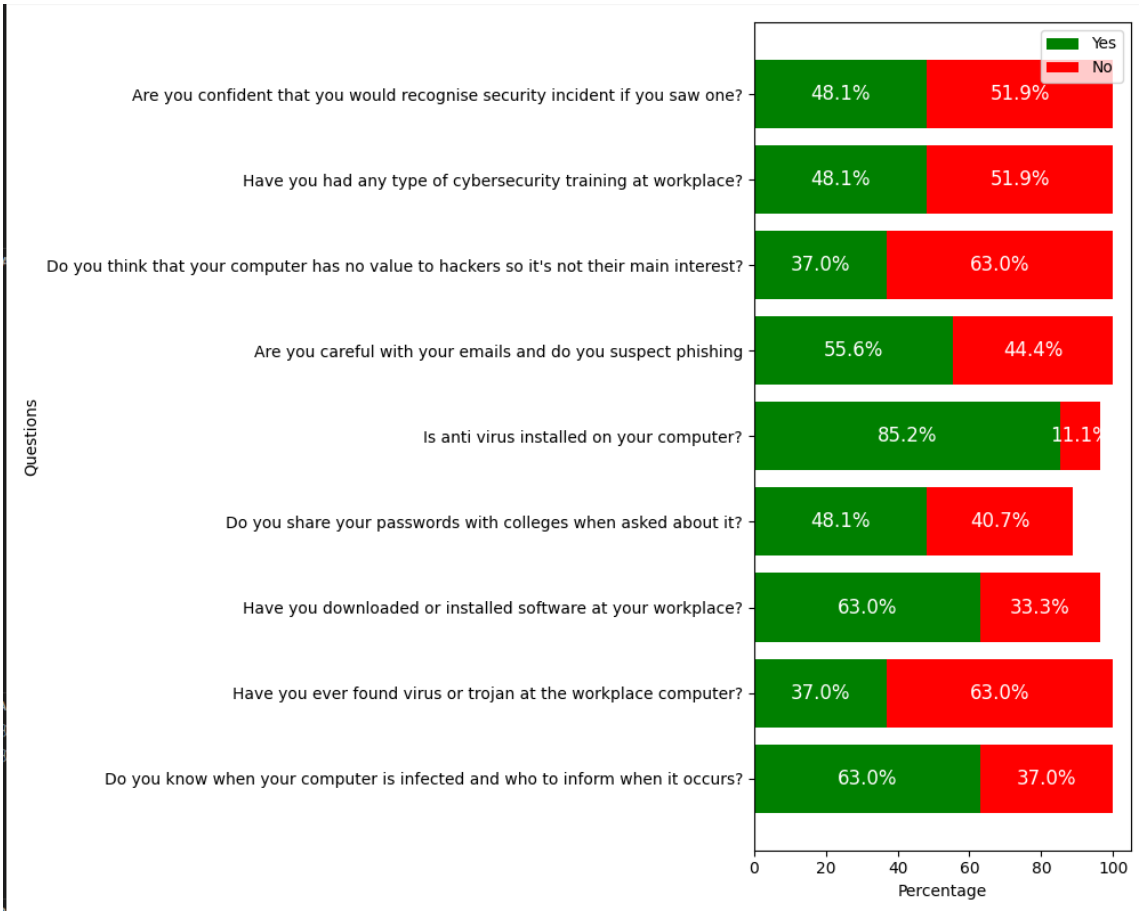

Figure 1. Survey 1 questions and answers.

The survey helped the author identify general level and awareness of individuals and key areas to focus while developing the module. For example, a module about anti virus necessity does not need much resources (85.2% of survey participants have it already installed) but a lot of workers don't follow necessary password protocols (48.1%) so much more attention to it is needed. After the survey author decided to develop module with heavy resources in areas of virus detection, how to recognise security breach, password management and steps and cautions in case of incidents.

4.2 Mapping risks to ISO 81001:5 standards

The International Organization for Standardization (ISO) has developed standards for various industries, including the healthcare industry. ISO 81001:5 is a standard for the application of risk management for IT networks incorporating medical devices[17]. This standard provides guidance on the development and implementation of risk management processes and is applicable to all types of healthcare organizations.

1. Risk identification
2. Risk analysis
3. Risk evaluation
4. Risk treatment
5. Risk monitoring and review

This steps were linked to survey questions which resulted to following analysis:

Risk Identification - The risks related to virus detection, recognizing security breaches, and password management were identified through a survey of healthcare professionals. The survey asked questions related to the participants' awareness of these risks and their practices for managing them.

Risk Analysis - The identified risks were analysed to determine the likelihood and impact of each risk on the healthcare IT system. The analysis revealed that virus detection and password management were high-risk areas, while recognizing security breaches was a moderate-risk area.

Risk Evaluation - Based on the analysis, the risks were evaluated to determine the level of risk and prioritise risk treatment options. The evaluation revealed that virus detection and password management required immediate attention, while recognizing security breaches could be addressed through ongoing monitoring and training.

Risk Treatment- Risk treatment options were developed and implemented to address the identified risks. This included implementing antivirus software, establishing password management policies and procedures, and providing training on recognizing security breaches.

Risk Monitoring and Review - The effectiveness of the risk treatment options was monitored and reviewed to ensure that the identified risks were being addressed and that the desired outcomes were being achieved. This involved developing chapters on ongoing monitoring of the healthcare IT system and regular review of the risk

The analysis revealed that virus detection and password management were high-risk areas, while recognizing security breaches was a moderate-risk area. This analysis was used to develop and implement risk treatment choices, such as installing antivirus software, creating password management policies and procedures, and offering security breach awareness training.

In order to make sure that the risks that had been identified were being handled and that the expected results were being obtained, the effectiveness of these risk treatment methods was afterwards assessed and monitored.This involved ongoing monitoring of the healthcare IT system and regular review of the risk management framework.

By applying the risk management process outlined in ISO 81001:5, healthcare organizations can take a proactive approach to cybersecurity and better manage the risks associated with their IT systems. This approach helps to ensure that patient data remains secure and that the organization is better protected against cyber threats.

4.3 Developing the module

It was discovered during the creation of the mission-critical cybersecurity training e-learning module that a general cybersecurity training component was required in order to have a thorough understanding of cybersecurity. While the mission-critical healthcare

infrastructure cybersecurity was the module's main focus, it was also crucial to take into account the larger context of cybersecurity and the connections between the two topics.

Because many of the same concepts and procedures apply to both types of cybersecurity, there should also be a general cybersecurity training component. For instance, both kinds of cybersecurity education call for a comprehension of how to safeguard against dangers like malware, phishing, and insider threats.

Additionally, both types of training require knowledge of best practices for password security, email security, and data privacy.

In order to effectively protect mission critical healthcare infrastructure, it is necessary to have a strong foundation in general cybersecurity principles. Without a comprehensive understanding of general cybersecurity, it is difficult to fully appreciate the importance of mission critical cybersecurity training and the risks associated with not implementing it. By providing both general and mission critical cybersecurity training, learners are able to develop a holistic understanding of cybersecurity and the risks associated with it.

Furthermore, including a general cybersecurity training component in the e-learning module provides learners with the knowledge and skills necessary to protect not only mission critical healthcare infrastructure, but also their personal devices and information. This is particularly important given the increasing prevalence of cyber attacks and the need for individuals to be able to protect themselves against such attacks and also from the survey results that were gathered prior to development.

The development process of the e-learning module followed the ADDIE model (Analysis, Design, Development, Implementation, and Evaluation). The ADDIE model is a systematic instructional design process that involves five phases, which includes the analysis of learning needs, design, development, implementation, and evaluation.

The Analysis phase involved identifying the learning needs of healthcare professionals, which were gathered through a literature review, and consultation with subject matter

experts. Based on the identified learning needs, the learning objectives were developed, which formed the basis for the instructional design of the e-learning module.

The Design phase involved the application of Mayer's principles [18] to the design of the e-learning module. The coherence principle was applied by ensuring that the content was organized in a logical manner and was easy to follow. The contiguity principle was applied by presenting relevant visual and auditory information simultaneously. The modality principle was applied by using both text and visual aids to present information. The redundancy principle was applied by avoiding unnecessary information, and the personalization principle was applied by providing feedback and interactivity to enhance the engagement of the learner.

the use of Mayer's multimedia theory was an important component of e-learning module design, as it helped us create an effective and engaging learning experience for the healthcare professionals. By incorporating both visual and auditory elements in the presentation, it was aimed to reduce the cognitive load of the learners and improve their understanding and retention of the information. Table 1 highlights key principles of the theory.

Table 1. Mayer’s multimedia theory

Principle	**Description**
Multimedia Principle	People learn better from words and pictures than from words alone.
Modality Principle	People learn better when information is presented in the form that matches the sensory system that is best suited for processing it.
Redundancy Principle	People learn better from graphics and narration than from graphics, narration, and on-screen text.

Coherence Principle	People learn better when extraneous material is excluded rather than included.
Signalling Principle	People learn better when cues are added to highlight the organization and structure of the essential material.
Spatial Contiguity Principle	People learn better when corresponding words and pictures are presented near rather than far from each other on the page or screen.
Temporal Contiguity Principle	People learn better when corresponding words and pictures are presented simultaneously rather than successively.
Personalization Principle	People learn better when words are in conversational style and virtual coaches are used rather than formal style.
Segmenting Principle	People learn better when a multimedia lesson is presented in learner-paced segments rather than as a continuous unit.
Pre-Training Principle	People learn better from a multimedia lesson when they know the names and characteristics of the main concepts.
Multimedia Design	People learn better when multimedia design is user-centered, task-centered, and context-centered.

The multimedia pictures were used in almost all pages to keep the learner's attention to text, for multimedia and redundancy principle. There was no timer used neither in modules nor quiz , as they are fully self-paced. For pre-training principle all the IT terms had definitions, so they would not confuse learners. It was made sure that the

navigation between chapters were easy and accessible in an ordered and non-ordered way, from within chapters and from the toolbar. One possible example is Figure 2.

Figure 2. disaster recovery practices chapter from module

The Development phase involved the creation of the e-learning module. The e-learning module was developed using an authoring tool that allowed the integration of multimedia, interactive features, and assessments.

The module has following chapters:

1. Importance of cybersecurity
2. Scope of ISO 81001:5
3. Data privacy and security
   - 3.1. Risks associated with data breaches
   - 3.2. Strategies to protect patient data
   - 3.3 Conclusion
4. Common Cybersecurity Threats in Healthcare
   - 4.1. Ransomware attacks
   - 4.2. Phishing attacks
   - 4.3. Malware attacks

4.4 Insider threats

4.5. Conclusion

5. Best practices for managing passwords
   5.1. Creating strong passwords
   5.2. Managing passwords securely
   5.3. Multi-Factor Authentication
   5.4. Conclusion
6. Email security
7. Mobile device security
8. Mission critical healthcare infrastructure
9. Ensuring data security and integrity
10. Disaster recovery planning
    10.1. Risk assessment
11. Mission critical healthcare infrastructure examples and recommendations

The chapters in this study that address the major issues in the healthcare sector were carefully chosen. A significant standard for managing cybersecurity risks in healthcare organizations, ISO 81001:5, is covered in the first chapter, which also emphasizes the significance of cybersecurity in the healthcare industry.

The second chapter addresses data security and privacy, a crucial issue in the healthcare industry. In order to keep patients' trust and uphold legal requirements, it provides a thorough analysis of the risks connected to data breaches and approaches to protecting patient data.

All of the common cybersecurity risks that the healthcare industry encounters are covered in the third chapter, including ransomware, phishing, malware, and insider threats.

This chapter's goals are to increase reader understanding of the most common cyberthreats and provide strategies for avoiding and dealing with them.

The fourth chapter provides best practices for managing passwords, which is one of the most basic and critical aspects of cybersecurity. Strong password creation, secure

password management, multi-factor authentication, and other techniques to increase password security are all covered.

The fifth chapter focuses on mobile device and email security, two issues that the healthcare sector is concerned about. It offers instructions on how to protect mobile devices and email communications to stop illegal access to sensitive data.

The sixth chapter focuses on mission-critical healthcare infrastructure, which includes the vital equipment, facilities, and systems that are necessary for giving patients prompt and efficient medical care. This chapter provides examples and recommendations for ensuring the security and integrity of mission-critical healthcare infrastructure.

The seventh chapter covers disaster recovery planning, which is a critical component of cybersecurity in healthcare. It offers instructions on how to evaluate risks, create disaster recovery plans, and test those plans to make sure they work.

The decision to include these chapters was made after a thorough examination of the state of cybersecurity in the healthcare sector and the unique requirements of healthcare professionals. The chapters go over the most important areas of worry and offer helpful advice on how to avoid cyberattacks and safeguard sensitive data.

The research paper aims to promote cybersecurity awareness and encourage the implementation of best practices in the healthcare industry.

The e-learning module was designed to cover various cybersecurity topics relevant to the healthcare sector, including the importance of cybersecurity, ISO 81001:5, data privacy and security, common cybersecurity threats, best practices for managing passwords, email security, mobile device security, and disaster recovery planning.

Additionally, the module includes a specific focus on mission-critical healthcare infrastructure to ensure data security and integrity. This section covers topics such as risk assessment, disaster recovery planning, and examples and recommendations for mission-critical healthcare infrastructure.

The Implementation phase involved the delivery of the e-learning module to the target audience. The e-learning module was published as google sites to allow access to healthcare professionals.

The Evaluation phase involved the assessment of the effectiveness of the e-learning module in promoting learning outcomes. The evaluation was carried out through a pre- and post-test, which assessed the knowledge gained by the learners before and after completing the e-learning module. The final assessment is solely for learners to check their learnt skills and data from it was not collected. The feedback from the learners was also collected through a survey to evaluate the usability, engagement, and overall effectiveness of the e-learning module.

5. Findings and Recommendations

After learners finished the module they were asked to complete a survey which would aid assessment of the e-learning module's usefulness, level of involvement, and overall efficacy. They were given 8 statements and responses ranged from (1-disagree to 5-agree). The survey's results are visualised in Figure 3.

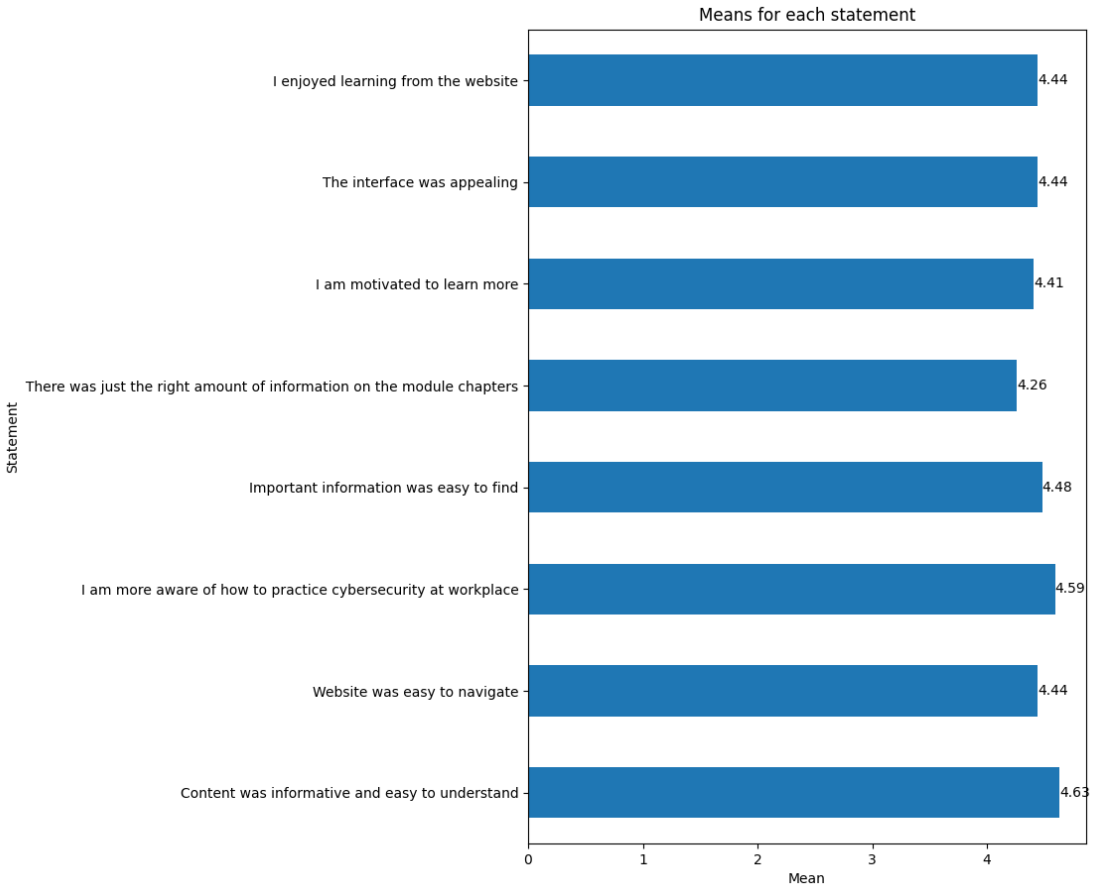

Figure 3. Survey 2 questions and answers

Based on the results, it appears that the learners found the e-learning module to be effective and informative. The mean scores for all of the statements were above 4, indicating that the learners generally agreed with the statements.

The learners found the website easy to navigate, with a mean score of 4.44. This is important as it can impact their overall experience and engagement with the material.

The statement 'I am more aware of how to practice cybersecurity at workplace' had the highest mean score of 4.59, indicating that the learners felt they gained valuable knowledge from the module.

The statement 'There was just the right amount of information on the module chapters' had a mean score of 4.26, which suggests that the learners felt that the module did not overload them with too much information, but still provided enough information to be effective.

The learners were also motivated to learn more, with a mean score of 4.41. This is a positive result as it indicates that the learners were engaged with the material and interested in continuing their cybersecurity education.

The interface was found to be appealing with a mean score of 4.44. This is important as it can impact the learners' engagement and overall experience with the material.

Finally, the learners enjoyed learning from the website, with a mean score of 4.44. This suggests that the module was well-received and enjoyable to use.

The results suggest that the e-learning module was effective in teaching cybersecurity concepts and engaging the learners.

Learners were also asked if they would like to have similar trainings in workspace or educational institutions where majority of them said yes as shown in Figure 4.

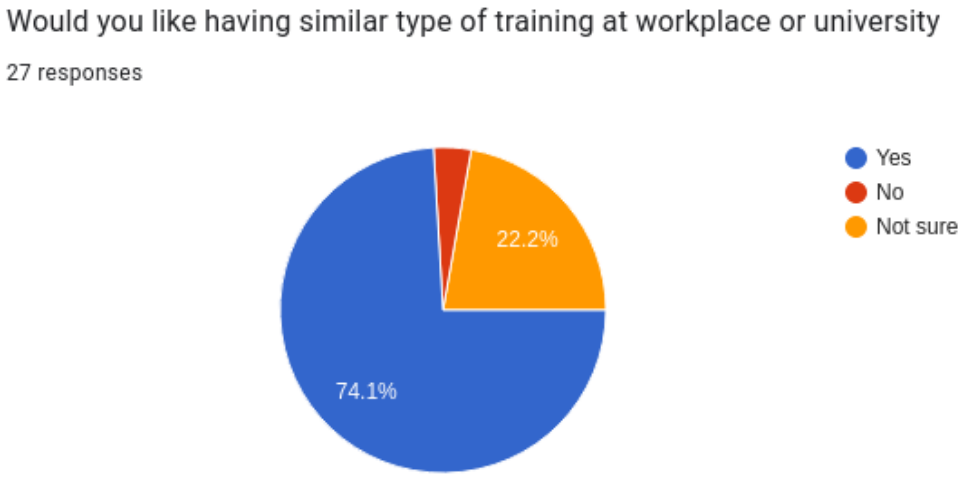

Figure 4. Learner's answer on getting professional training

Based on the positive feedback received from the learners, it is recommended that similar cybersecurity training modules should be provided to employees in their respective workplaces. This can help in creating a culture of cybersecurity awareness and promote safe online practices in the workplace. The training can be customised to suit the specific needs of the organisation and can be made mandatory for all employees. The feedback received from the learners can also be used to improve the content and delivery of the training modules. In conclusion, providing cybersecurity

training to employees can be an effective way to prevent cyber-attacks and protect sensitive information.

Continuous training for healthcare professionals in cybersecurity is crucial because cyber threats are constantly evolving. Attackers are continually developing new techniques and tactics to exploit vulnerabilities in healthcare systems, and healthcare professionals must stay up-to-date with the latest developments in cybersecurity to keep pace with these threats. Without continuous training, healthcare professionals may not be aware of the latest cybersecurity risks and may not know how to respond appropriately to an attack.

Moreover, healthcare professionals are frequently targeted by cybercriminals because they have access to sensitive patient data. This data is valuable on the black market, and cybercriminals are continually looking for new ways to steal it. Training healthcare professionals in cybersecurity helps to reduce the likelihood of data breaches by educating them on how to identify and respond to potential threats. It can also help to create a culture of cybersecurity awareness within healthcare organisations, where all staff members are trained to recognize potential cyber threats and take appropriate action to mitigate them.

Continuous training in cybersecurity can also improve the efficiency and effectiveness of healthcare organisations. Cybersecurity incidents can disrupt operations and cause downtime, which can be costly for healthcare organisations. By training healthcare professionals in cybersecurity, organisations can reduce the likelihood of incidents occurring, minimising the risk of downtime and ensuring that critical systems and services remain operational.

6. Summary

The study employed a risk-based approach, which involved conducting a risk assessment survey and mapping identified risks to international standards. The construction of the e-learning module, which comprised interactive and captivating learning content suited to specific learning objectives, was also guided by Mayer's principles of multimedia learning. To determine the effectiveness of the module, an assessment plan was put into place, and input from the students was gathered via a survey. The outcomes showed that the e-learning module was successful in raising learners' knowledge and comprehension of the security, efficacy, and safety of health software and IT systems. The study offers insightful information on how to create e-learning modules that can be tailored for healthcare personnel in order to raise cybersecurity awareness within the healthcare sector.

Mayer's principles of multimedia learning emphasise the importance of creating interactive and engaging learning material that includes a combination of text, images, audio, and video. By following these principles, the e-learning module was tailored to the specific learning objectives identified in the risk assessment, and designed to be flexible and adaptable for different types of healthcare professionals. This approach turned out to be effective according to participant’s feedback.

Overall, the e-learning module is a good and efficient way to raise cybersecurity awareness in employees. It is highly customizable and interactive. E-learning modules can be updated and revised as new threats and risks emerge, which means that employees can engage in continuous learning to stay up-to-date on the latest cybersecurity best practices.

References

1. On Primary Health Care (2018). World Health Organisation (WHO)
2. Hollis D. (2011) Cyberwar Case Study: Georgia 2008 . Small Wars Journal
3. Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., et al. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. Healthcare, 10, 327.
4. Check Point Research Team. (2023, January 5). Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. [Online]. Available https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ [Accessed 4 April 2023]
5. Cynerio. Research Report: The State of Healthcare IoT Device Security 2022
6. Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. Journal of medical systems, 44(5), 98.
7. K. Kioskli, T.Fotis & H. Mouratidis. (2021) The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. In Proceedings of the 16th International Conference on Availability, Reliability and Security
8. Lechner, N. H., Strahonja, V., & Stapić, Z. (n.d.). Threat Modeling Methods in the Medical Device Industry: An Integrative Literature Review. Faculty of Organization and Informatics, University of Zagreb, Pavlinska 2, 42000 Varaždin, Croatia.
9. Lankinen, V. (2022). Risk Management in Academic Medical Device Research Environment: Case mTMS Prototype. Tampere University.
10. Healthtech staff. (2018) A Risk-Based Security Approach Helps Healthcare Protect Data Beyond HIPAA. [Online]. Available https://healthtechmagazine.net/article/2018/03/risk-based-security-approach-helps-healthcare-protect-data-beyond-hipaa [Accessed 4 April 2023]
11. The World by Income and Region. (2021) The World Bank [Online]. Available

https://datatopics.worldbank.org/world-development-indicators/the-world-by-income-and-region.html [Accessed 11 May 2023]

12. Population Clock. New Zealand Government Statistics. [Online]. Available https://www.stats.govt.nz/topics/population [Accessed 11 May 2023]
13. International Monetary Fund (April 2023). World Economic Outlook Database. [Online]. Available https://www.imf.org/en/Publications/WEO/weo-database/2023/April/ [Accessed 11 May 2023]
14. A. Adams (November 2016). The official website of the New Zealand Government [Online]. Available https://www.beehive.govt.nz/release/cyber-security-skills-taskforce-established [Accessed 11 May 2023]
15. Neo, M., Park, H., Lee, M.-J., Soh, J.-Y., & Oh, J.-Y. (2015). Technology acceptance of healthcare e-learning modules: A study of Korean and Malaysian students' perceptions. TOJET: The Turkish Online Journal of Educational Technology, 14(2), 181.
16. Pears, M., & Konstantinidis, S. (2021, May). Cybersecurity Training in the Healthcare Workforce – Use of the ADDIE Model. In IEEE Global Engineering Education Conference (EDUCON) (pp. 1-5). IEEE. doi: 10.1109/EDUCON46332.2021.9454062
17. ISO 81001-5-1:2019. (2019). Health software and health IT systems safety, effectiveness, and security -- Part 5-1: Security and privacy requirements. Geneva, Switzerland: International Organization for Standardization.
18. Mayer, R. E. (2009). Multimedia learning (2nd ed.). Cambridge University Press

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Ketevan Jebisashvili

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "An E-learning Module on Cybersecurity Risk Awareness for Healthcare Personnel: a Case Study of Georgia" , supervised by Kaido Kikkas

    1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

    2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

    [11.05.2023]

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.