TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Nadezda Semjonova 221871IVCM

Cybersecurity Culture in Academia: the case of Tallinn University of Technology

Master's Thesis

Supervisor: Kaido Kikkas
PhD

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Nadezda Semjonova 221871IVCM

Küberturbekultuur akadeemilises keskkonnas Tallinna Tehnikaülikooli näitel

Magistritöö

Juhendaja: Kaido Kikkas
PhD

Tallinn 2024

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: Nadezda Semjonova

12.05.2024

Abstract

The digital transformation of education presents immense opportunities for global connectivity and collaboration, yet it also brings forth unprecedented cybersecurity challenges. This thesis examines the imperative of cultivating a strong cybersecurity culture within academia, with a specific focus on Tallinn University of Technology. The research problem focuses on the lack of emphasis on cybersecurity culture within higher education institutions, despite its significant impact on institutional security.

A quantitative survey was administered to undergraduate students enrolled in the School of Information Technologies to assess the existing cybersecurity culture and formulate specific guidelines for enhancing it within academic settings. The study delved into defining cybersecurity culture, identifying optimal measurement methods, and highlighting the benefits of cultivating a resilient cybersecurity culture. Analysis of the responses revealed that students are more engaged when university leadership supports cybersecurity initiatives. Cybersecurity behaviour among Cybersecurity Engineering students improves with more related courses. Disparities in responses emphasize that the cybersecurity culture at IT College is stronger compared to other departments. There is common dissatisfaction with scarcity of cybersecurity activities and a lack of awareness regarding security policies and procedures.

This thesis claims that Tallinn University of Technology can strengthen its cybersecurity culture by leveraging insights from the methodologies, findings, and proposed guidelines presented in this study. Furthermore, universities globally can undertake similar initiatives to enhance their cybersecurity practices. This promotes the exchange of best practices and encourages a collaborative effort to nurture a resilient cybersecurity culture in academia. Therefore, this research not only enhances knowledge in the field but also acts as a catalyst for positive developments in cybersecurity education and practices within academic institutions.

This thesis is written in English and is 99 pages long, including 7 chapters, 11 figures and 12 tables.

Annotatsioon

Hariduse digitaalne ümberkujundamine pakub tohutuid võimalusi ülemaailmseks ühenduvuseks ja koostööks, kuid toob kaasa ka enneolematuid küberjulgeoleku väljakutseid. See lõputöö uurib tugeva küberjulgeolekukultuuri kasvatamise vajalikkust akadeemilistes ringkondades, keskendudes eelkõige Tallinna Tehnikaülikoolile. Uurimisprobleem keskendub küberturvalisuse kultuuri vähesele rõhuasetusele kõrgkoolides, hoolimata selle olulisest mõjust institutsionaalsele julgeolekule.

Infotehnoloogiakoolis osalenud bakalaureuseõppe üliõpilastele viidi läbi kvantitatiivne uuring, et hinnata olemasolevat küberjulgeolekukultuuri ja sõnastada konkreetsed juhised selle tõhustamiseks akadeemilises keskkonnas. Uuringus käsitleti küberturvalisuse kultuuri määratlemist, optimaalsete mõõtmismeetodite väljaselgitamist ja vastupidava küberjulgeolekukultuuri kasvatamise eeliste esiletõstmist. Vastuste analüüsist selgus, et üliõpilased on rohkem kaasatud, kui ülikooli juhtkond toetab küberturvalisuse algatusi. Küberturvalisuse inseneri üliõpilaste küberturvalisuse käitumine paraneb seotud kursustega. Vastuste erinevused rõhutavad, et IT Kolledži küberturvalisuse kultuur on teiste osakondadega võrreldes tugevam. Üldine on rahulolematus küberjulgeolekualaste tegevuste nappuse ning turvapoliitika ja -protseduuride vähese teadlikkusega.

Käesolevas lõputöös väidetakse, et Tallinna Tehnikaülikool saab tugevdada oma küberturvalisuse kultuuri, kasutades ära selles uuringus esitatud metoodikatest, leidudest ja pakutud juhistest saadud teadmisi. Lisaks saavad ülikoolid üle maailma teha sarnaseid algatusi oma küberturvalisuse parandamiseks. See soodustab parimate tavade vahetamist ja julgustab koostööd tegema, et arendada akadeemilistes ringkondades vastupidavat küberjulgeolekukultuuri. Seetõttu ei suurenda see uurimus mitte ainult valdkonna teadmisi, vaid toimib ka küberjulgeolekualase hariduse ja tavade positiivsete arengute katalüsaatorina akadeemilistes asutustes.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 99 leheküljel, 7 peatükki, 11 joonist, 12 tabelit.

List of abbreviations and terms

AI	Artificial Intelligence
BIT	Business Information Technology
CE	Cybersecurity Engineering
COVID-19	Coronavirus Disease 2019
DoSpeRT	Domain-Specific Risk-Taking
GDPR	General Data Protection Regulation
HD&P	Hardware Development and Programming
HSM	Heuristic Systematic Model
ISC	Information Security Culture
ITSA	IT System Administration
ITSD	IT System Development
MBTI	Myers-Briggs Type Indicator
PMT	Protection Motivation Theory
US	United States

Table of contents

List of figures

List of tables

1 Introduction

Digital technologies allow connecting people, knowledge, and things around the world, they help to share concerns, challenges and unite human beings to solve global health, financial, or climatic crises. The digital transformation of traditional education is one of the pillars of the future to create a more united society, and all future generations will become a part of it. Along with the benefits of digitalization of educational systems, there are risks and challenges that must be addressed before the transition is sustainable. A critical area of scrutiny lies in the careful examination of the behaviors and attitudes towards cybersecurity exhibited by young individuals and the subsequent impact of these factors on overall security.

1.1 Motivation

Technological advancements have created revolutionary changes in the way young people behave and interact in many areas of their lives, including socialization, interpersonal communication, sleep habits, participation in sports, and academics. Many social problems are exacerbated by digital life and create complex relationships through the use of technology and media.

With the gradual or total digitization of old educational paradigms, greater consideration needs to be given to the associated security risks. Considering that educational institutions bear the primary responsibility for the security and welfare of their students, it is imperative that they use cutting edge pedagogical methodologies, make use of technical resources, and develop long-lasting and effective cybersecurity strategies.

The author is concerned for the well-being and preparedness of the younger generation as they navigate the complexities of the digital age. In today's rapidly evolving technological landscape, young people are not only heavily reliant on digital tools and platforms for various aspects of their lives but also increasingly vulnerable to cybersecurity threats and risks. From online communication and social media interactions

to academic pursuits and personal data management, the digital realm presents a myriad of challenges and potential pitfalls for the youth. Recognizing the critical role that educational institutions play in shaping the attitudes, behaviors, and skills of young individuals, the author advocates for a proactive approach to cybersecurity within academia.

By fostering a strong cybersecurity culture, educational institutions can empower students with the knowledge, skills, and attitudes necessary to navigate the digital landscape safely and responsibly. This not only ensures the security and integrity of educational environments but also equips students with essential life skills that will serve them well in an increasingly digitized world. Moreover, a robust cybersecurity culture will help students protect themselves from online crimes, bullying, threats, and other digital dangers. Additionally, it will prepare them for their professional futures by instilling confidence and competence in navigating the digital environment, thereby enhancing their employability and success in the digital age. Ultimately, the author envisions a future where young people are not only adept at leveraging technology for positive purposes but also resilient in the face of cybersecurity challenges, safeguarding their well-being and contributing to a safer and more secure digital society.

1.2 Research Problem

This work underscores the critical need for Educational Institutions to assess and foster a robust cybersecurity culture, especially in light of the increasing vulnerability to cybercrime, notably ransomware attacks [1]. Such attacks pose a substantial threat, resulting in significant financial losses and reputational damage.

As a key outcome, this thesis will develop a methodology for evaluating cybersecurity culture and identifying existing security indicators in Educational Institutions, offering a unified approach to address security risks stemming from human behaviour across academic settings. While technological advancements alone have not yielded significant cybersecurity improvements, understanding and shaping human behaviour towards cybersecurity is crucial. Despite this, cybersecurity culture remains largely overlooked in Higher Educational Institutions, with little research or development in this area. This thesis aims to bridge this gap by evaluating Tallinn University of Technology's current cybersecurity culture and contributing to tailored guidelines for academic institutions.

The practical implications of this research lie in the potential transformation of existing cybersecurity culture based on gathered data, paving the way for stronger security practices and heightened awareness among students and faculty.

1.3 Research Question

The primary objective of this study is to establish a comprehensive definition of cybersecurity culture, serving as a foundational guide across various dimensions. The secondary goal is to identify an optimal research methodology and strategy as a benchmark for scholars engaged in cultivating a robust cybersecurity culture. The ultimate aim is to evaluate the impact of the chosen approach within the selected educational institution on the transformation of cybersecurity culture.

Thus, the main research questions are:

[RQ1] How to define the cybersecurity culture?

[RQ2] What are the most reliable methods for evaluating cybersecurity culture in Educational Institutions?

[RQ3] How do educational programmes and initiatives at Tallinn University of Technology contribute to the development of cybersecurity skills and awareness among students, and how does this impact the overall cybersecurity culture?

1.4 Scope and Goal

The primary goal of this research is to systematically assess and analyze the prevailing cybersecurity culture within an academic context. The study specifically aims to compare cybersecurity awareness and behavior among undergraduate students across various programs at the Tallinn University of Technology, with a focus on the School of Information Technologies. By examining and comparing the cybersecurity culture of these different academic programmes and examining the differences between first-year students and those students who have already spent one, two, or more years at university, the study aims to draw meaningful conclusions. The overreaching objective is to contribute valuable insights that can inform strategies for enhancing cybersecurity awareness and fostering a robust cybersecurity culture within educational institutions.

Ultimately, the goal is to promote a safer digital environment for students and stakeholders in academia.

This study is constrained by certain limitations. While it aims to establish a set of guidelines explicitly crafted for an academic institution, the implementation and subsequent analysis of these guidelines fall outside the purview of the study. Therefore, additional research efforts by subsequent student researchers may be possible to assess progress and determine the appropriate level of cybersecurity culture.

1.5 Novelty

Due to the failure of relying primarily on technological advances to improve cybersecurity, interest in the significance of human behaviour in this area has increased dramatically over the past several years. Understanding how cybersecurity culture affects security is in high demand in businesses, academia, and other sectors and requires a lot of research and practical assessments.

While there has been considerable research on organizational cybersecurity culture in the business environment, such as the studies by Batteau (2011) [2], Lancey (2016) [3], AlHogail (2015) [4], Da Veiga (2016) [5], Ioannou (2019) [6], Tolah (2019) [7], which focus on corporate settings, and numerous studies assessing cybersecurity knowledge in academia, like those by Zheng (2018) [8], Witsenboer (2022) [9], Hongbo (2023) [10], the specific exploration of cybersecurity culture within academic institutions remains largely under-researched.

The insufficiently explored and frequently overlooked domain of social behaviour, collective values, beliefs, and attitudes among individuals regarding cybersecurity exert a substantial influence on institutional security, particularly within Educational Institutions.

COVID-19 caused substantial changes in educational institutions as well as a very rapid digitization of the entire planet. Since the shift to digital education is underway, it is critical to do it with the fewest security risks possible. Thus, today more than ever, the imperative lies in cultivating a robust cybersecurity culture among the youth to enhance their security awareness and preparedness for the future.

2 Background

To comprehensively grasp the essence of cybersecurity culture, it is imperative to delve into its background, which involves analysing various elements such as the digital landscape, existing literature, and prevailing practices. By scrutinizing the digital landscape, including emerging technologies, threats, and vulnerabilities, we gain insights into the evolving nature of cybersecurity challenges. Additionally, examining existing literature provides a foundation for understanding key concepts, theoretical frameworks, and empirical findings related to cybersecurity culture. Moreover, exploring real-world case studies and best practices offers practical insights into how organizations approach cybersecurity and foster a culture of security. Through this multifaceted analysis, we can uncover the underlying dynamics shaping cybersecurity culture and identify areas for improvement and innovation in promoting cyber resilience.

2.1 Literature Review

This chapter presents a literature review that is conducted to find relevant works on cybersecurity culture, frameworks, and assessment mechanisms in academia and organizations. Definitions, measurements, and guidelines for creating a robust cybersecurity culture are identified based on the research explored in the literature review.

2.1.1 The Current State of Cybersecurity Domain

In 2022 and 2023, Estonia experienced a marked escalation in cyber threats, with the number of incidents reaching 2,672 and 3,314 respectively [11]. The years saw a significant rise in Distributed Denial-of-Service (DDoS) attacks, which not only increased in frequency but also in complexity, reflecting their use as tools in cyber warfare and foreign policy [12]. The impact of these attacks extended beyond disruption, with a notable incident in 2023 severely affecting Estonia's train ticketing services for nearly a day. Additionally, the period witnessed sophisticated phishing operations and dangerous ransomware attacks [13]. In addition, cyber fraud surged, causing financial losses upwards of 8.3 million euros, with tactics ranging from phishing emails to Business Email Compromise (BEC) schemes [11]. These developments underscore the growing

sophistication of cyber threats and the urgent need for strengthened cybersecurity measures in Estonia.

In 2023, ransomware attacks in US reached unprecedented levels, predominantly driven by phishing tactics, resulting in financial losses exceeding one billion dollars [14].

Furthermore, as of 2024, the cybersecurity domain is experiencing a substantial transformation surged by two prominent elements: the escalating influence of artificial intelligence (AI) and the persistent consequences of geopolitical tensions. With the ability to empower both defenders and adversaries in cybersecurity efforts, AI is emerging as an effective instrument. While security professionals utilize AI to devise inventive countermeasures against ever-changing threats, cybercriminals capitalize on its functionalities to coordinate increasingly sophisticated assaults. In the meantime, ongoing geopolitical conflicts persistently exert a substantial influence over the cybersecurity landscape, impacting cyber operations across various sectors worldwide, including businesses, governments, public administrations, and academia.

2.1.2 Existing Studies on Cybersecurity Culture

Numerous studies have delved into cybersecurity culture; however, the precise definition of "cybersecurity culture" remains elusive, leading to ambiguity regarding its scope and components. Furthermore, some frameworks and assessment tools have been devised for organizational contexts, and they are not well suited for this research purposes due to their limitations and lack of practical applicability.

Previous studies have examined the definition of “information security culture” or “security culture”, with one notable contribution made by Da Veiga in 2008, titled “Cultivating and Assessing Information Security Culture” [15]. However, consensus on a definitive definition is not agreed upon. As such, this study aims to analyse existing definitions and develop a comprehensive “Cybersecurity culture” definition that encompasses the various perspectives in the field.

Given the absence of specific research on cybersecurity culture within academia, the search also encompassed research papers focusing on organizational contexts, and focused on literature that contains terms such as "cybersecurity culture", "information security culture" and "security culture". The systematic literature review titled "Developing a Cybersecurity

Culture: Current Practices and Future Needs" served as a guiding framework and reference point for the existing literature search [16]. In addition to the initial 58 research papers identified in the systematic review, the search was expanded from 2010 to 2023, resulting in the identification of 8 additional papers through repeated process. The complete list of these research articles is available in the Table 1.

Table 1. Existing Literature [16]

Paper ID	Author , Year	Research	D	PA
P1	Alfawaz et al. (2010)	Information security culture: A behaviour compliance conceptual framework [17]		
P2	Da Veiga and Eloff (2010)	A framework and assessment instrument for information security culture [18]	x	x
P3	Lacey (2010)	Understanding and transforming organizational security culture [19]		x
P4	Lim et al. (2010)	Embedding information security culture emerging concerns and challenges [20]		
P5	Sánchez et al. (2010)	Security Culture in Small and Medium-Size Enterprise [21]		
P6	Van Niekerk and Von Solms (2010)	Information security culture: A management perspective [22]		
P7	Batteau (2011)	Creating a culture of enterprise cybersecurity [2]	x	
P8	Alnatheer et al. (2012)	Understanding and measuring information security culture in developing countries: case of Saudi Arabia [23]		x
P9	Hassan and Ismail (2012)	A conceptual model for investigating factors influencing information security culture in healthcare environment [24]		
P10	Olivos (2012)	Creating a security culture development plan and a case study [25]		
P11	Shahibi et al. (2012)	Determining factors influencing information security culture among ICT librarians [26]		x
P12	AlHogail and Mirza (2014a)	A proposal of an organizational information security culture framework [27]		

P13	AlHogail and Mirza (2014b)	A framework of information security culture change [28]		
P14	Astakhova (2014)	The concept of the information-security culture [29]	x	
P15	D'Arcy and Greene (2014)	Security culture and the employment relationship as drivers of employees' security compliance [30]		x
P16	Da Veiga and Martins (2014)	Information security culture: A comparative analysis of four assessments [31]		x
P17	Lopes and Oliveira (2014)	Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises [32]		x
P18	Reid et al. (2014)	From information security to cyber security cultures [33]		
P19	Reid and Van Niekerk (2014)	Information security culture: A general living systems theory perspective [34]		
P20	AlHogail (2015a)	Design and validation of information security culture framework [35]		x
P21	AlHogail (2015b)	Cultivating and assessing an organizational information security culture; an empirical study [36]	x	x
P22	Alnatheer (2015)	Information security culture critical success factors [37]		
P23	AlKalbani et al. (2015)	Organisational security culture and information security compliance for e-government development: The moderating effect of social pressure [38]		
P24	Da Veiga (2015)	The influence of information security policies on information security culture: Illustrated through a case study [39]		x
P25	Da Veiga and Martins (2015)	Improving the information security culture through monitoring and implementation actions illustrated through a case study [40]		x

P26	Greig et al. (2015)	An ethnographic study to assess the enactment of information security culture in a retail store [41]		x
P27	Lim et al. (2015)	Information security culture: Towards an instrument for assessing security management practices [42]		x
P28	Martins and Da Veiga (2015)	An Information security culture model validated with structural equation modelling [43]		x
P29	Sherif et al. (2015)	An Identification of Variables Influencing the Establishment of Information Security Culture [44]		
P30	Da Veiga (2016a)	A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument [5]	x	x
P31	Da Veiga (2016b)	Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study [45]		x
P32	Hassan and Ismail (2016)	Information security culture in healthcare informatics: A preliminary investigation [46]		
P33	Santos-Olmo et al. (2016)	The importance of the security culture in SMEs as regards the correct management of the security of their assets [47]		
P34	Hayden (2016)	People-Centric Security: Transforming Your Enterprise Security Culture [3]	x	x
P35	Tang et al. (2016)	The impacts of organizational culture on information security culture: a case study [48]		x
P36	Da Veiga and Martins (2017)	Defining and identifying dominant information security cultures and subcultures [49]		x
P37	Gcaza et al. (2017)	A general morphological analysis: Delineating a cyber-security culture [50]	x	
P38	Hassan et al. (2017)	Information security culture in health informatics environment: A qualitative approach [51]		x

P39	Masrek et al. (2017)	Information security culture for Malaysian public organization: a conceptual framework [52]		
P40	Da Veiga (2018)	An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture [53]		x
P41	Masrek et al. (2018a)	Assessing the information security culture in a government context: The case of a developing country [54]		x
P42	Masrek et al. (2018b)	The development of an information security culture scale for the Malaysian Public organization [55]		x
P43	Mokwetli and Zuva (2018)	Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa [56]		x
P44	Nævestad et al. (2018)	Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security [57]		x
P45	Ioannou et al. (2019)	Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination [6]	x	x
P46	Marotta and Pearlson (2019)	A culture of cybersecurity at Banca Popolare di Sondrio [58]	x	
P47	Nasir et al. (2019b)	A dimension-based information security culture model and its relationship with employees' security behaviour: A case study in Malaysian higher educational institutions [59]		x
P48	Nel and Drevin (2019)	Key elements of an information security culture in organisations [60]		x
P49	Patrascu (2019)	Promoting Cybersecurity Culture Through Education [61]		
P50	Ruhwanya and Ophoff (2019)	Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania [62]		

P51	Tolah et al. (2019)	A Comprehensive Framework for Understanding Security Culture in Organizations [63]	x	x
P52	Van't Wout (2019)	Develop and maintain a cybersecurity organisational culture [64]	x	x
P53	Alshaikh (2020)	Developing cybersecurity culture to influence employee behaviour: A practice perspective [65]		
P54	Blythe et al. (2020)	Human cyber risk management by security awareness professionals: Carrots or sticks to drive behaviour change? [66]		x
P55	Da Veiga et al. (2020)	Defining organisational information security culture—Perspectives from academia and industry [67]	x	x
P56	Govender et al. (2020)	A Framework for the Assessment of Information Security Risk, the Reduction of Information Security Cost and the Sustainability of Information Security Culture [68]		
P57	Nasir et al. (2020)	Information Security Culture for Guiding Employee's Security Behaviour: A Pilot Study [69]		x
P58	Schneider et al. (2020)	A Practical Guideline for Developing a Managerial Information Security Awareness Programme [70]		
P59	Wiley et al. (2020)	More than the individual: Examining the relationship between culture and Information Security Awareness [71]		x
P60	Georgiadou et al. (2020)	A Cybersecurity Culture Framework for Assessing Organization Readiness [72]		
P61	Gioulekas et al. (2022)	A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures [73]		x
P62	Crawley (2022)	8 Steps to Better Security: A Simple Cyber Resilience Guide for Business [74]		
P63	Tarun (2022)	Building a Culture of Security [75]		

P64	Mitrovic et a. (2023)	Towards Building Cybersecurity Culture in TVET Colleges in South Africa [76]		
P65	Yulianto et al. (2023)	Ransomware Resilience: Investigating Organizational Security Culture and Its Impact on Cybersecurity Practices against Ransomware Threats [77]		
P66	Thembakazi et al. (2023)	Towards a Cybersecurity Culture Framework for Mobile Banking in South Africa [78]		

2.1.3 Definitions of Information Security, Cybersecurity, and Security Culture

Upon thorough analysis, it becomes apparent that only 11 research articles delve deeply into defining security culture. The selected papers listed in Table 2 will undergo an in-depth examination for this research.

Table 2. Literature with definitions for review.

Paper ID	***Author , Year***	***Research***	***D***	***PA***
P2	Da Veiga and Eloff (2010)	A framework and assessment instrument for information security culture [18]	x	x
P7	Batteau (2011)	Creating a culture of enterprise cybersecurity [2]	x	
P14	Astakhova (2014)	The concept of the information-security culture [29]	x	
P21	AlHogail (2015b)	Cultivating and assessing an organizational information security culture; an empirical study [36]	x	x
P30	Da Veiga (2016a)	A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument [5]	x	x
P34	Hayden (2016)	People-Centric Security: Transforming Your Enterprise Security Culture [3]	x	x
P37	Gcaza et al. (2017)	A general morphological analysis: Delineating a cyber-security culture [50]	x	

P45	Ioannou et al. (2019)	Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination [6]	x	x
P46	Marotta and Pearlson (2019)	A culture of cybersecurity at Banca Popolare di Sondrio [58]	x	
P51	Tolah et al. (2019)	A Comprehensive Framework for Understanding Security Culture in Organizations [63]	x	x
P55	Da Veiga et al. (2020)	Defining organisational information security culture—Perspectives from academia and industry [67]	x	x

Table 3. Three available definitions.

Definitions of culture	**Studies**
Cybersecurity Culture definition	P30, P37, P45, P46
Information Security Culture definition	P2, P14, P21, P34, P51, P55
Security Culture Definition	P7

In 2020, in the research paper "Defining Organizational Information Security Culture – Perspectives from Academia and Industry", the authors concluded that there is no single definition of information security culture [67]. They looked at several definitions and structures and found that there are a couple of works that are dominated by academic concepts, but the factors that define an ideal information security culture are inconsistent. The research's concept of the comprehensive definition put out by the authors was extended by an analysis of both internal and external elements. According to their definition, management support, consistent training, and adherence to security policies all contribute to the development of an information security culture that is ultimately in line with the organization's mission and fosters trust and integrity. Their study emphasizes the value of an information security culture in businesses and the part that employee behaviour plays in safeguarding processed data [67].

In the research paper "The concept of the information-security culture ", ISC is defined as encompassing more than just enforced policies or implemented technologies. It

represents a deeply ingrained ethos that must permeate all levels of an organization. The study outlines that a robust information security culture is characterized by the proactive engagement of employees, from top management to front-line staff, in secure practices. This involves regular training and awareness programmes that keep security at the forefront of organizational operations. The analysis also emphasizes the dynamic nature of information security culture, noting that it should evolve in response to changing security landscapes and emerging threats. Additionally, the impact of organizational structure on the effectiveness of an information security culture is considered, with open communication channels and a non-punitive approach to reporting security incidents highlighted as vital components [29].

In an empirical study "Cultivating and assessing an organizational information security culture; an empirical study", AlHogail provides a nuanced definition of information security culture as "The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in [an] organization with the aim of influencing employees' behaviour to preserve information security". The study underscores that human behaviour often constitutes the weakest link in the security chain. It asserts that organizations must prioritize understanding and influencing employees' behaviour to ensure information security, as the effectiveness of security measures hinges largely on employees' actions or oversights. The research highlights the inadequacy of solely focusing on technical security aspects, stressing the need for equal attention to human interaction with the system [36].

Information security culture was also defined by A. Da Veiga and J.H.P. Eloff in 2010 as the attitudes, assumptions, beliefs, values, and knowledge that stakeholders and employees use to engage with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artifacts and creations that become part of the way things are done in the organization to protect its information assets. This information security culture changes over time [18].

An important characteristic of culture is that it tends to be invisible, functioning just below our conscious awareness of its influence. The author of "People-Centric Security" highlights security culture from a people-centric perspective, putting humans at the centre of the whole security challenge and emphasizing how important it is for people to solve

problems rather than how they cause them. Security culture is part of all organizational cultures, and most industries will have multiple information security cultures because not all employees have the same views and assumptions about what security should be [3]. The author acknowledges that emphasizing technology alone will always be futile and that emerging human behaviour has always conquered security. Therefore, it's crucial to comprehend why people act in a certain way and make an effort to explore all of the potential alternatives, not just those that might seem straightforward or anticipated.

The new definition of information security culture was presented in 2019 in the research paper “A Comprehensive Framework for Understanding Security Culture in Organizations”. “The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in [an] organization with the aim of influencing employees’ behaviour to preserve information security” [63]. The meaning of it is that in order to avoid actions that could pose hazards to the security of information assets or IT systems, information security culture defines human behaviour while engaging with IT systems. Rather than merely dictating employee behaviour, a culture that promotes appropriate security behaviour through values, knowledge, and assumptions is very successful. When employees are aware of, comprehend, and take the appropriate safeguards, adopting security policies in the conventional cycle is more effective when there is a proper information security culture.

Enhancing organizational security culture involves fostering a positive environment that guides employees to adhere to policies, reducing the risk of harmful information interaction through knowledge, skill development, and secure behaviour [63] [79]. In A Comprehensive Framework for Understanding Security Culture in Organizations, the authors acknowledge that it is preferable to have a culture that encourages safe behaviour through knowledge and values than to have rules that only dictate how staff members should act. According to numerous studies, a corporate security culture can influence people to behave as "human firewalls" in situations where acting appropriately is expected [79].

As literature on cybersecurity culture expands in a last decade, discerning terminology differences becomes crucial. While cybersecurity culture and information security culture are seen as distinct yet related concepts, they are often conflated in academic discourse. And only few studies explicitly explore the disparities between information security and

cybersecurity culture. Gcaza, von Solms, and van Vuuren in the research paper "A general morphological analysis: delineating a cyber-security culture" [50], highlight the lack of a clear definition for cybersecurity culture and underscoring the importance of clarifying related terms to mitigate ambiguity. Cybersecurity culture is defined as the collective values, beliefs, attitudes, and behaviours of individuals within an organization regarding cybersecurity practices and protocols. The research suggests that cybersecurity culture encompasses not only technical aspects such as implementing security measures and protocols but also the human element, including awareness, training, and adherence to security policies. It emphasizes the importance of fostering a culture where all members of the organization understand the significance of cybersecurity and actively contribute to maintaining a secure environment. The analysis also highlights the role of organizational leadership in promoting and sustaining a strong cybersecurity culture by setting clear expectations, providing adequate resources, and cultivating a climate of accountability and continuous improvement in cybersecurity practices [50].

The internet, while providing various benefits, presents security and privacy threats such as exposure of personal information, unauthorized access, intellectual property theft, industrial system failures, and network disruptions. In 2016, Adele Da Veiga, defined cybersecurity culture by looking at industrial psychology and using the definition of information security culture as well as organizational culture. In this research article, cybersecurity culture is defined as the intentional and unintentional manner in which cyberspace is utilized at four levels, namely the international, national, organizational, or individual level, which either promotes or inhibits the safety, security, privacy, and civil liberties of individuals, organizations, or governments [5].

In Marotta and Pearlson's research paper "A culture of cybersecurity at Banca Popolare di Sondrio" [58] and in Huang and Pearlson's article "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture" (2019) [80], the distinction is made between information security culture and cybersecurity culture. While information security culture focuses on adhering to policy, cybersecurity culture extends beyond mere compliance to encompass personal commitment to safeguarding organizational cyber safety. Within this paper, organizational cybersecurity culture is defined as "the beliefs, values, and attitudes that drive employee behaviours to protect and defend the organization from cyber-attacks" [58].

The authors in the research paper “Cybersecurity Culture in Computer Security Incident Response Teams” define cybersecurity culture as referring to the procedures established by an organization for all of its employees, guiding their course of action in all situations involving data integrity, whenever they are in the line of duty [6]. Therefore, creating a cybersecurity culture begins with the creation of policies that instruct personnel who handle data on how to respond in various circumstances.

The article “Creating a culture of enterprise cybersecurity” defines another terminology “Security Culture” as a composite of mind-set, social connections, and nuanced behaviours within an organization that influence how security policies are implemented and adhered to [2]. Security culture, similar to safety culture in high-reliability organizations like aviation and nuclear power, involves consistent training, robust communication, and a shared understanding of risks. It encompasses the responsibility of individuals and teams to maintain security measures, such as updating anti-virus software and managing access through identification and authentication processes. Security culture also involves making informed decisions about trust and security trade-offs, balancing openness and restriction to safeguard organizational assets while promoting a proactive and informed approach to potential security threats. This culture supports a framework where errors are openly discussed and learned from, enhancing overall security through collective vigilance and improvement [2].

2.1.4 Existing Measuring Instruments

Ensuring the effectiveness of cybersecurity culture hinges on accurate measurement. To craft a robust measurement plan aligned with specific goals, it's vital to first identify existing evaluation tools. Quantitative data mining stands out as a prevalent method for assessing cybersecurity culture, with surveys or questionnaires emerging as the most effective instruments for this purpose. Moreover, it's prudent to reevaluate the cybersecurity culture periodically, especially after implementing any changes or enhancements to the safety programme. This reassessment allows for the examination of how the adjustments and advancements have influenced cybersecurity culture, aiding in the refinement of strategies for greater efficacy.

The authors of “A Framework and Assessment Instrument for Information Security Culture” created a questionnaire using the Information Security Culture Framework and

statistical analysis of the survey results. An empirical study was conducted at a South African firm that performs audit and consulting assignments and employs over 3,000 people. The concept evaluation tool created in an earlier study by the Professor Adele Da Veiga served as the foundation for the development of the assessment tool [81]. To ensure content validity, the concept evaluation instrument was updated with the Information Security Culture Framework components and changed based on the validity and reliability tests completed in the earlier research [18]. For each of the three information security behavioural tiers (organizational, group, individual), there were 85 statements in the final improved assessment tool, covering every Information Security Culture Framework component. The poll received a total of 1085 responses from employees, which is a sufficient sample. The results show that the proposed theoretical framework in this study can be accepted, and there is a good fit between the Information Security Culture Framework and the empirical evidence. The author concludes that the proposed framework and assessment tools can provide guidance to security professionals in building a strong security culture.

The methodology used in the research paper "A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument" is based on three components. The first is the definition of a cybersecurity culture; the second is the development of a cybersecurity measurement tool; and the third is an assessment of the validity of the cybersecurity culture model. The author suggests the development process for the questionnaire to measure cybersecurity culture. The questionnaire should include eleven dimensions, such as information asset management, information security policies, user management, information security programmes, information security leadership, information security management, trust, training and awareness, privacy perception, and cybersecurity in practice [5]. It is important to validate the developed measurement tool, and this can be done through various statistical analyses. This study can be used to standardize a technique for measuring cybersecurity culture from a national, organizational, academic, and individual point of view.

Saudi Arabia served as the location for the Areej Alhogali case study. To get comprehensive data, a questionnaire and interviewing techniques were combined. The questionnaire consists of two parts, such as demographic information (age group, education, job level) and information security culture structure parameters (strategy, technology, organization, people, environment, change management) [36]. The

interviews were conducted through field visits and telephone conversations, but for ethical reasons, the data from these interviews is confidential and not included in the research work. The use of change management concepts and the degree of information security culture are positively correlated, according to the research. This emphasizes the significance of change management in establishing a strong information security culture [36].

The primary technique of data collection for the article “A Comprehensive Framework for Understanding Security Culture in Organizations” was one-on-one interviews. Four segments made up the interview questions, with the first one covering participants' general characteristics and demographics. The second section contained open-ended questions about security practices used by organizations and how staff members are trained in compliance with security regulations [63]. Due to the confidential nature of the interview information, the participants refused to record it. According to the conclusions of the author, the analysis data provided insight into the security practices and behaviour patterns of employees in the field of security. The interview has the drawback of being anonymous and thus confidential, making it unsuitable for further re-examinations and comparative analysis as a method of data collection.

The author of “People-Centric Security” suggests two evaluation methods that can be used in combination or separately: the first is a survey, and the second is value metrics. The diagnostic survey consists of 10 questions that relate to the core business of the organization, with 4 sub-questions that correlate to the concept of the Competing Security Culture Framework and associate with a specific security culture (trust, autonomy, process, compliance) [3]. The value metrics include 25 measures, and each result of a specific metric is associated with a key value behaviour of the FORCE (Failure, Operations, Resilience, Complexity, Expertise) Model. Such a survey is used to determine how an organization's behaviour is consistent with a high-assurance security programme. In this study, the author presents one of the most comprehensive works on security culture, however, it requires practical implementation and validation.

To research the cybersecurity culture in computer security incident response teams, the authors employed an online questionnaire [6]. In total, 25 participants responded to the questionnaire from 23 different countries across the United States of America, Europe, Asia, Australia, and Africa. Sensitive information was gathered, handled with

confidentiality, and instantly made anonymous. The questions were divided into a number of categories to perform analysis and identify challenges and best practices [6]. The research discovered a number of problems, all of which are connected to human factors. Building a sense of trust and teamwork among the staff should be the first priority for any organization, as they concentrate on addressing the challenges and performing their duties.

The authors of "Defining Organizational Information Security Culture: Perspectives from Academia and Industry" analyse various questionnaires to understand the pros and cons of different types of questions. The following questions were analysed: open-ended, background, and questions on the Likert scale [29]. The efficiency of initiatives to create and foster an information security culture within an organization or academia heavily depends on perceptions of the concept's parameters and the factors that affect this process. The theoretical value of this research lies in the understanding of the notion of information security culture and the system of external and internal factors influencing its state.

2.1.5 Research Gap

An exploration of the research literature concerning cybersecurity culture within academic institutions uncovers a notable gap. This deficiency underscores the lack of specialized measuring tools, a clearly outlined methodology, and a comprehensive analysis tailored to the unique educational environment. As a result, the absence of these elements hinders the capacity to accurately evaluate and improve cybersecurity practices within educational settings.

Existing evaluation tools are often generic and not designed to capture the unique aspects of cybersecurity behavior, attitudes, and awareness that pertain to students, faculty, and administrative staff. The diversity of roles within educational institutions means that a one-size-fits-all approach to measurement may overlook critical nuances in how different groups perceive and prioritize cybersecurity.

In addition, there is no specific research methodology that has been universally adopted for studying cybersecurity culture in educational settings. Research tends to borrow methodologies from corporate settings or IT environments, which may not align with the

educational context. For instance, educational institutions have specific regulatory requirements, stakeholder expectations, and cultural values that differ markedly from those of business organizations. The lack of a tailored methodology means that research may fail to address these unique factors effectively, leading to interventions that are less impactful or inappropriate.

Furthermore, the absence of detailed analysis in the existing literature is a critical shortfall. Studies often do not go beyond identifying the presence of cybersecurity policies to analyzing their efficacy or the depth of their integration into the daily lives of those within the institution. Without such analysis, it is challenging to understand the real-world implications of policies and practices on fostering a robust cybersecurity culture.

Addressing these gaps requires a concerted effort to develop measurement tools that are specific to the educational sector, encompassing its diverse stakeholders and their particular needs. Additionally, a dedicated methodology for studying cybersecurity culture within academia needs to be formulated—one that considers the organizational structure, pedagogical goals, and possible vulnerabilities of educational environments. Finally, a more nuanced analysis of existing data will enable a deeper understanding of how cybersecurity culture manifests in educational institutions, leading to more effective and targeted interventions.

2.2 Definitions

In this chapter, the author introduces a novel definition of cybersecurity culture grounded in fundamental principles and aspects. By delving into various dimensions of cybersecurity behaviour, attitudes, and practices, the aim is to construct a comprehensive understanding of what constitutes a robust cybersecurity culture.

2.2.1 Understanding Culture

To formulate a comprehensive definition of cybersecurity culture, it is essential to grasp the concepts of organizational culture and academic culture. Organizational culture encompasses a wide array of values, norms, beliefs, and practices that shape how an organization functions internally and externally. It encompasses elements such as leadership approaches, communication strategies, decision-making protocols, and employee interactions [82]. This overarching culture permeates all aspects of

organizational functioning, including cybersecurity practices. It embodies the organization's core values, traditions, customs, and social dynamics across its operations. Furthermore, organizational culture indirectly influences cybersecurity through its impact on employee conduct, leadership styles, and communication channels.

However, cybersecurity culture addresses a specific aspect of organizational culture—the organization's approach to cybersecurity. It examines how cybersecurity is integrated into the organization's overall culture and how it influences employee beliefs, attitudes, behavior, practices and decision-making regarding security. It focuses on how individuals perceive and prioritize cybersecurity, their awareness of security risks, and their adherence to security policies and procedures. A strong cybersecurity culture is essential for enhancing security posture and mitigating cyber threats effectively. It fosters a security-conscious mindset among employees, promotes adherence to security policies, and facilitates collaboration and communication on security-related issues.

On the other hand, educational institutions, such as universities and colleges, distinguish themselves from traditional organizational cultures found in businesses and companies in several key ways. Unlike businesses, which prioritize profitability and market competitiveness, educational institutions focus primarily on academic excellence, teaching, and research. While organizational cultures often feature hierarchical structures with clear lines of authority, academic cultures may have more decentralized decision-making processes, allowing faculty and students greater participation in governance. Academic cultures prioritize values such as knowledge, learning, and intellectual inquiry, promoting academic freedom, critical thinking, and diversity of thought. Additionally, educational institutions prioritize relationships with students, faculty, researchers, and the academic community, whereas businesses prioritize relationships with customers, shareholders, and external stakeholders.

Therefore, cybersecurity culture within educational institutions refers to the collective mindset, values, and behaviors shared among faculty, staff, and students, shaping their approach to safeguarding digital assets and information systems against cyber threats. It encompasses a proactive commitment to cybersecurity education, awareness, and best practices, fostering a collaborative and vigilant environment. Educational institutions prioritize the integration of cybersecurity principles into curriculum, policies, and procedures, empowering individuals to become responsible digital citizens and guardians

of institutional data security. This culture promotes a continuous learning ethos, adapting to evolving technologies and emerging threats, while emphasizing the importance of collaboration, communication, and shared responsibility in maintaining a resilient cybersecurity posture.

2.2.2 Cultural Transformation

Cultural transformations within organizations are a well-documented phenomenon. While many corporations rely on diverse studies to enact the necessary changes in organizational culture, educational institutions also offer notable examples of such cultural shifts.

Culture within academia is a dynamic interplay of various factors. Institutional values and mission guide priorities such as research, teaching, and community engagement, shaping the behaviors of faculty, staff, and students. Leadership styles and decision-making processes influence organizational culture, with transparent, collaborative leadership fostering positivity. Academic disciplinary cultures, distinct in methods and norms, vary between departments. Student-led initiatives and activism advocate for diversity and inclusion, contributing to a vibrant campus culture. Technological advances facilitate new forms of collaboration and communication, influencing teaching and research practices. Increasing globalization and cultural diversity enrich academic environments, fostering multicultural interactions. Together, these factors shape the unique culture of each academic institution.

For example, MIT has a rich history of successful cultural transformation, known for fostering a unique environment where innovation and creativity flourish. This prestigious institution has not only been a pioneer in technological research but also in cultivating a distinctive culture that encourages unconventional thinking and problem-solving. Over the years, MIT has transformed its culture from a purely academic institution into a dynamic hub that merges the rigor of science with the creativity of engineering and technology.

Hacker culture at MIT (Massachusetts Institute of Technology) emerged through a combination of factors, including the institution's emphasis on technical prowess, its collaborative academic environment, and the influence of pioneering individuals [83].

In the 1950s and 1960s, MIT's proximity to cutting-edge technology companies and research institutions fostered an atmosphere of innovation and experimentation. Students and faculty were encouraged to explore new ideas and push the boundaries of technology [84].

One key influence was the Tech Model Railroad Club (TMRC), founded in the late 1940s. This club served as a gathering place for students interested in electronics and computing. Members of the TMRC tinkered with model trains and built elaborate control systems, honing their skills in programming and problem-solving [85].

Another significant factor was the arrival of early computer systems on campus, such as the TX-0 and the PDP-1, in the late 1950s and early 1960s. These machines provided students with unprecedented access to computing power and sparked a wave of experimentation in programming and software development [86].

The growing popularity of hacker culture can be attributed to the MIT community's constant commitment to discovery and collaboration. To stretch the boundaries of technological possibility, students engaged in collaborative project work, code sharing, and friendly competition.

The term "hacker" itself originally had positive connotations at MIT, referring to individuals who were skilled programmers and problem solvers. These hackers valued ingenuity, creativity, and the pursuit of knowledge [87].

Over time, the Hacker culture at MIT evolved and spread beyond the campus, influencing the development of the wider hacker community. Today, hacker culture continues to thrive, characterized by a spirit of curiosity, collaboration, and innovation.

Furthermore, MIT has promoted a culture of “mens et manus” or “mind and hand”, which emphasizes the importance of practical application of knowledge [88]. This philosophy has created an environment where theoretical knowledge meets practical implementation, making it fertile ground for innovation. The institute has been instrumental in fostering an ecosystem that supports startups and technological entrepreneurship. Students and faculty alike are motivated to push the boundaries of their fields, leading to groundbreaking developments that have a worldwide impact.

2.2.3 Proposed Definition

Drawing from the wealth of existing literature and the comprehension of culture, it becomes evident that cybersecurity culture comprises two fundamental aspects: the individual and the collective [80]. Figure 1 illustrates the components that constitute these dimensions.

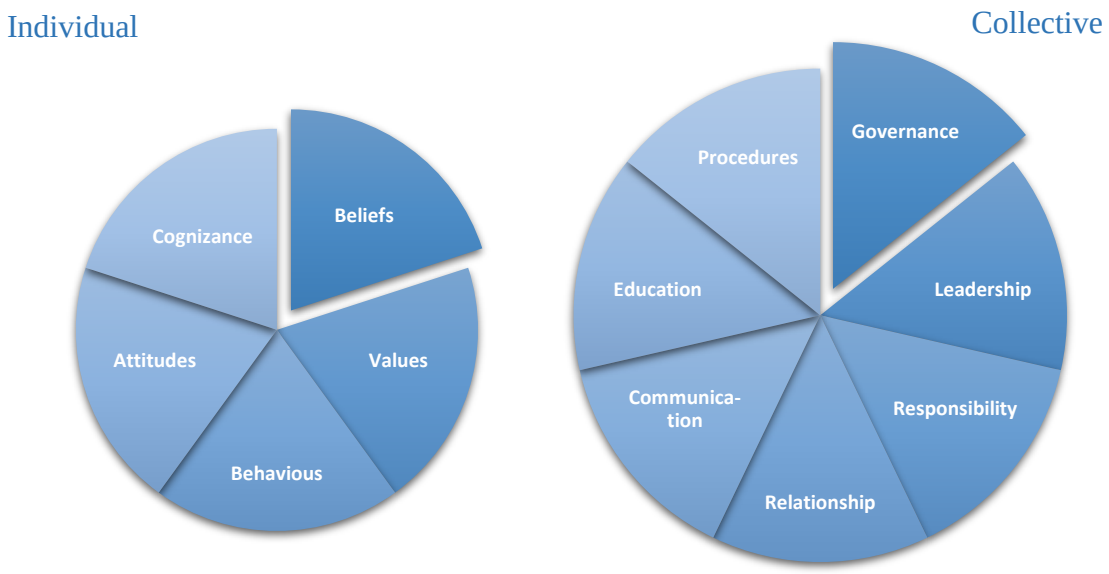

Figure 1. Individual and Collective components.

In a robust cybersecurity culture, both individual and collective components play pivotal roles in establishing a secure operational environment [89]:

Beliefs - These represent the personal convictions held by individuals about the importance of cybersecurity, and it directly influencing how they engage with security measures.

Values - Personal principles that guide individuals in prioritizing and addressing cybersecurity within their daily actions and decisions.

Behaviours - The specific actions and habits demonstrated by individuals concerning cybersecurity, such as adhering to secure password protocols and remaining vigilant against phishing.

Attitudes - The general mindset or disposition individuals hold towards cybersecurity practices, policies, and adherence within their organization [89].

Cognizance - The cognitive processes, including knowing, thinking, judging, remembering, problem solving [90], and understanding an individual possesses regarding cybersecurity risks, potential threats, and necessary preventative actions.

Governance - The frameworks and policies an organization implements to guide the execution and control of cybersecurity strategies and measures.
Leadership - The role of organizational leaders in setting a tone and culture that prioritizes cybersecurity through their actions, decisions, and the support they provide to cybersecurity initiatives [91].
Responsibility - The shared accountability among all members to uphold cybersecurity protocols and respond proactively when issues emerge [91].
Relationships - The interactions among different organizational stakeholders (employees, management, IT teams) that influence the effective implementation and sustainability of cybersecurity policies.
Communication - The mechanisms for distributing and discussing cybersecurity-related information within the organization to ensure widespread awareness and readiness.
Education - Organized awareness programmes aimed at enhancing the cybersecurity skills and knowledge of all members within an organization [91].
Procedures - The defined steps, polices and guidelines for managing cybersecurity issues, ensuring a uniform and effective response to security incidents.
Practices - The routine activities and standardized practices conducted to maintain and boost the organization's defense against cyber threats.

Cybersecurity culture is a multifaceted concept encompassing both individual and collective elements within an organization, industry, or academic institution. By incorporating these vital components, the author has put forth the following definition of cybersecurity culture:

"Cybersecurity culture refers to the overall mindset, beliefs, behaviours, and practices concerning cybersecurity landscape. It encompasses both individual attitudes towards cybersecurity and collective efforts to promote security awareness, implement best practices, and effectively respond to cyber threats. In essence, cybersecurity culture reflects the organization's commitment to prioritizing and maintaining robust cybersecurity measures as an integral part of its operations and values".

3 Methodology

Assessing cybersecurity culture within educational institutions requires active involvement from students and extensive support from the academic community, including the Student Counselling Office, deans, and all programme managers. The original research aimed to encompass all undergraduate programmes at Tallinn University of Technology, comprising over 7,000 students across 44 programmes spanning five schools, including the School of Economics, School of Science, Estonian Maritime Academy, School of Engineering, and School of Information Technology. Unfortunately, the required support from the leadership of various departments for this research was not provided. Certain aspects of this behaviour are being analysed in the subsequent analysis section, and solutions to address these issues are also being provided later in this research.

However, the author chose to move forward with the research, concentrating exclusively on the School of Information Technologies, where it was more positively received, although not universally so. The analytical scope encompassing all undergraduate students within the School of Information Technologies, which consists of six programmes. Among these are three programmes offered by the IT College: IT Systems Administration, IT Systems Development, and Cybersecurity Engineering, the latter being the only one taught in English. Additionally, the Department of Software Science offers programmes in Business Information Technology and Informatics, while the Department of Computer System provides the Hardware Development and Programming programme.

Currently, more than 10,000 students are enrolled at Tallinn University of Technology, with over 10% of them being international students from nearly 100 different countries [92]. Approximately 70% of these students are undergraduates, with around 700 enrolled in the School of Information Technologies.

A quantitative research method was chosen to gather objective data reflecting broad characteristics of cybersecurity culture. This method allowed for data collection from a large sample size, enabling the identification of general trends and areas of strength and vulnerability within the student body's cybersecurity practices. By employing probability voluntary response sampling, a structured survey was distributed among undergraduate

students at School of Information Technologies. The assessment was conducted among first-, second-, and third-year students, allowing for a detailed evaluation of progress over time. A comparative analysis conducted to identify the impact of the university's cybersecurity culture on students and identify any observed changes. Cross-programme comparisons was used to determine the differential impact of cybersecurity culture transformation across different academic programmes. The survey was disseminated to Programme Managers and their assistants, who then facilitated its distribution among their students via email. Over a span of two weeks, the survey garnered a total of 110 responses. With this sizable dataset, the analysis is poised to offer tangible insights into the effectiveness of the university in nurturing a culture of cybersecurity among its students throughout their academic journey.

The survey was made using SurveyLegend online platform, paid “Business Version” because it is suitable by all privacy characteristics and features for this particular research. The data analysis was conducted using Life Analytics, an integrated programme provided by SurveyLegend. Initially, individual responses were examined, followed by exporting the data to Excel to identify correlations between various answers within the dataset. Additionally, the author utilized pie charts and graphs generated by the platform to enhance the visual representation of the data. Prior to analysis, the dataset was prepared and cleaned by removing blank entries and identifying any outliers.

The survey comprised 41 questions meticulously designed to capture a wide array of data. It encompassed four parameter questions aimed at gathering basic information such as the student's study programme, academic year, age group, and employment status. Additionally, there were thirty-five questions employing a 5-point Likert Scale System, one Multiple Choice Question, and one Open-Ended Question. The author opted for the Knowledge of Action Likert-type scale response anchors, omitting the "neutral" option as it was deemed incongruent with the research objectives [93]. The absence of a neutral option ensured that respondents provided definitive answers, as neutrality could imply indifference toward certain security aspects, which was not conducive to the study's objectives.

The methodology for this research was developed from a combination of existing works, including “Cultivating and assessing an organizational information security culture: an empirical study" by AlHogail [36], “A framework and assessment instrument for

information security culture" by A. Da Veiga and J.H.P. Eloff [18], and "Scaling the Security Wall: Developing a Security Behaviour Intentions Scale (SeBIS)" by Serge Egelman and Eyal Peer [94]. These studies provided valuable insights and frameworks for evaluating cybersecurity culture, which were adapted and integrated into the methodology for this research. Additionally, the author made necessary modifications and adjustments to tailor the methodology specifically for research in the educational sector.

3.1 Platform and Privacy

Several criteria were established for the survey to ensure strict compliance with data protection standards. First, the survey platform servers were required to be located within the European Union to align with the General Data Protection Regulation (GDPR), which sets guidelines for the collection and processing of personal information of individuals within the EU. The survey itself was designed to anonymize responses, ensuring that no personal data was collected, and that all data was securely stored only for a limited duration necessary for the research. To further adhere to privacy regulations, a consent statement was incorporated into the survey. This statement informed participants that by submitting their responses, they were consenting to the processing and analysis of their data in accordance with GDPR guidelines, emphasizing transparency and the protection of participant privacy.

The platform selected for the survey was SurveyLegend, based in Sweden, renowned for its robust compliance with the General Data Protection Regulation (GDPR) and a strict privacy policy [95]. This choice was made after careful consideration of various other platforms, including SurveyPlanet [96], LimeSurvey [97], PollForAll [98], and Forms.app [99]. These alternatives were evaluated but ultimately did not meet the stringent selection criteria required for this project. Some of these platforms hosted servers outside of the European Union, primarily in the US, which raised concerns regarding data sovereignty and privacy. Additionally, others lacked the necessary flexibility in their tools to tailor the survey specifically for a student demographic, making them less suitable. Thus, SurveyLegend [100] stood out as the best option, providing both the security and adaptability required to effectively conduct the survey within educational

institutions. However, to access all the features, the author opted for the "business" subscription.

The privacy note displayed on the survey's welcome page reads as follows: “SurveyLegend platform is GDPR compliant [101]. The survey created with anonymous features enabled, where IP-address, location information, technical information about browser, operating system or device are not collected and the answers received are used in a generalized form for research purposes. We request the following personal information: the programme you're enrolled in, your current academic year, and your age group. The data is securely stored until the end of this year, when research period is over and then permanently deleted. Data will not be transferred to any third party. By filling out this survey you agree that we will process provided data”.

To ensure privacy preserving, several measures were implemented in the survey design. Personal identifiers such as names, emails, and IP addresses were not requested. Additionally, no location data or technical information regarding browsers, operating systems, or devices was collected. To maintain anonymity, respondents were grouped into age categories (e.g., under 24, 25-30, 31 and above), and no data regarding gender or nationality was solicited. The survey posed questions regarding the respondents' academic status and programme enrolment. These included inquiries about the year of their academic programme registration and the specific programme in which they were currently enrolled. These measures were taken to enhance privacy and confidentiality throughout the survey process.

3.2 Survey Development

The survey questions were meticulously crafted, drawing from various research sources to ensure broad applicability and sufficient variability among respondents. One such example is the inclusion of questions related to security behaviour, inspired by the Security Behaviour Intentions Scale (SeBIS) [94]. This scale consists of 16 items organized into four sub-domains: password generation (such as the creation of strong passwords and use of password management tools), system updates (ensuring software is kept up to date), device security (such as locking devices), and proactive awareness (considering security alerts and taking action accordingly) [94]. These security questions underwent thorough evaluation, being tested multiple times to ensure their applicability,

reliability (using Cronbach's alpha), and factor analysis (using Bartlett's test). This process involved continuous refinement based on feedback from 500 participants. Moreover, this questionnaire holds promise for correlation with various psychometric tests to enhance its validation.

Table 4. Security Behaviour Intentions Scale evaluation [94].

#	***Device Securement (28.47% of variance explained; λ = 4.555)***	**μ**	**σ**
	I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	3.20	1.559
	I use a password/passcode to unlock my laptop or tablet.	3.78	1.525
	I manually lock my computer screen when I step away from it	2.63	1.343
	I use a PIN or passcode to unlock my mobile phone.	3.21	1.733
#	***Password Generation (12.95% of variance explained; λ = 2.071)***	**μ**	**σ**
	I do not change my passwords, unless I have to.	2.65	1.091
	I use different passwords for different accounts that I have.	3.75	1.037
	When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.	3.31	1.096
	I do not include special characters in my password if it's not required	3.30	1.292
#	***Proactive Awareness (8.36% of variance explained; λ = 1.337)***	**μ**	**σ**
	When someone sends me a link, I open it without first verifying where it goes	4.01	1.014
	I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar	3.17	1.077
	I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).	3.69	1.102
	When browsing websites, I mouseover links to see where they go, before clicking them.	3.69	1.027
	If I discover a security problem, I continue what I was doing because I assume someone else will fix it	4.08	0.976
#	***Updating (6.77% of variance explained; λ = 1.082)***	**μ**	**σ**

	When I’m prompted about a software update, I install it right away	3.07	1.035
	I try to make sure that the programmes I use are up-to-date	3.78	0.890
	I verify that my anti-virus software has been regularly updating itself	3.55	1.228

The final survey is composed of 41 questions, designed to capture a comprehensive range of data. It includes four parameter questions that gather basic information such as the student's study programme, academic year, age group, and employment status. The bulk of the survey, 35 questions, employs a 5-point Likert scale with “Knowledge of Action” ranging from “never” to “always” without “neutral” ensuring participants provide responses that reflect their level of engagement [93]. These questions are aimed at assessing specific areas such as security behaviour, awareness, proactiveness, the university's contribution to security education, and the students' satisfaction with their cybersecurity education. The responses provided in the survey, were numerically coded from 1 to 5, corresponding to the intensity or frequency of the behaviour being assessed. This conversion allowed for a quantitative analysis of the data, facilitating statistical examination and comparison across different variables. By assigning numerical values to the qualitative responses, author gained deeper insights into the prevalence and consistency of cybersecurity-related behaviours among the participants.

Additionally, there is one multiple-choice question that explores the primary sources from which students receive their cybersecurity information and news. Finally, the survey includes an open-ended question, providing students with the opportunity to express their opinions and provide qualitative insights into their experiences and perceptions regarding cybersecurity.

3.3 Methods of Data Analysis

The survey was prepared in both Estonian and English to accommodate the diverse linguistic preferences of the students. Consequently, it necessitated an initial analysis of both surveys separately, followed by merging the data to gain a comprehensive understanding of the results.

The data analysis was conducted using Life Analytics, an integrated programme provided by SurveyLegend. Initially, individual responses were examined, followed by exporting

the data to Excel to identify correlations between various answers within the dataset. Additionally, the author utilized pie charts and graphs generated by the platform to enhance the visual representation of the data. Prior to analysis, the dataset was meticulously prepared and cleaned by removing blank entries and identifying any outliers.

The responses provided in the survey, ranging from "never" to "always," were numerically coded from 1 to 5, corresponding to the intensity or frequency of the behaviour being assessed. This conversion allowed for a quantitative analysis of the data, facilitating statistical examination and comparison across different variables. By assigning numerical values to the qualitative responses, researchers gained deeper insights into the prevalence and consistency of cybersecurity-related behaviours among the participants.

As the survey was administered in two languages, the data in the charts display responses from English-speaking students in English and those from Estonian-speaking students in Estonian. Additionally, some students from Estonian programmes opted to submit their survey responses in English and vice versa.

- 16 students took part in the survey in English, with one incomplete response; hence, a total of 15 submissions were received.

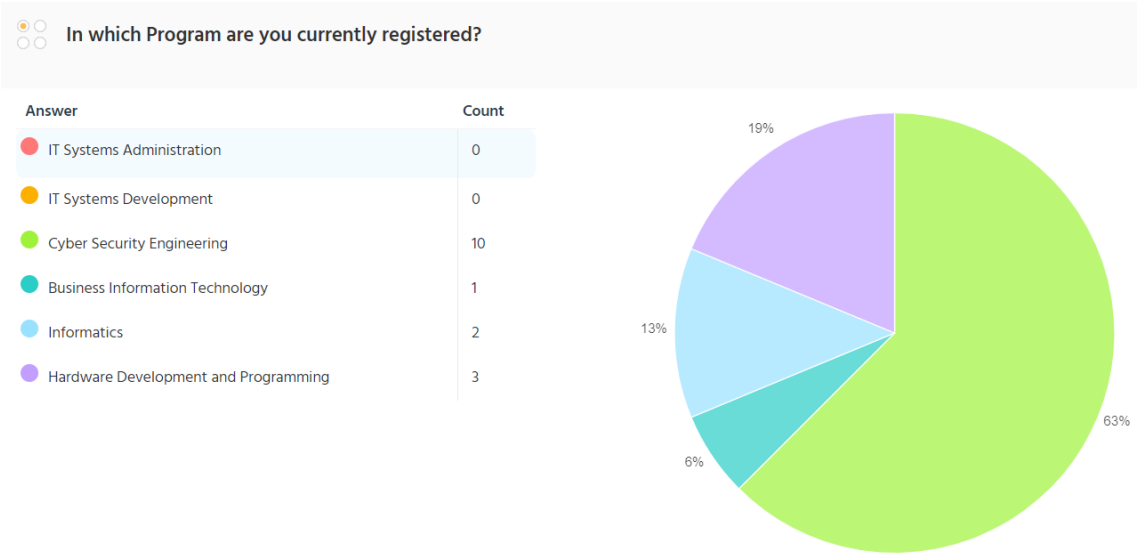

Figure 2. Submitted answers in English.

- 94 students took part in the survey in Estonian, with four incomplete responses; hence, a total of 90 submissions were received.

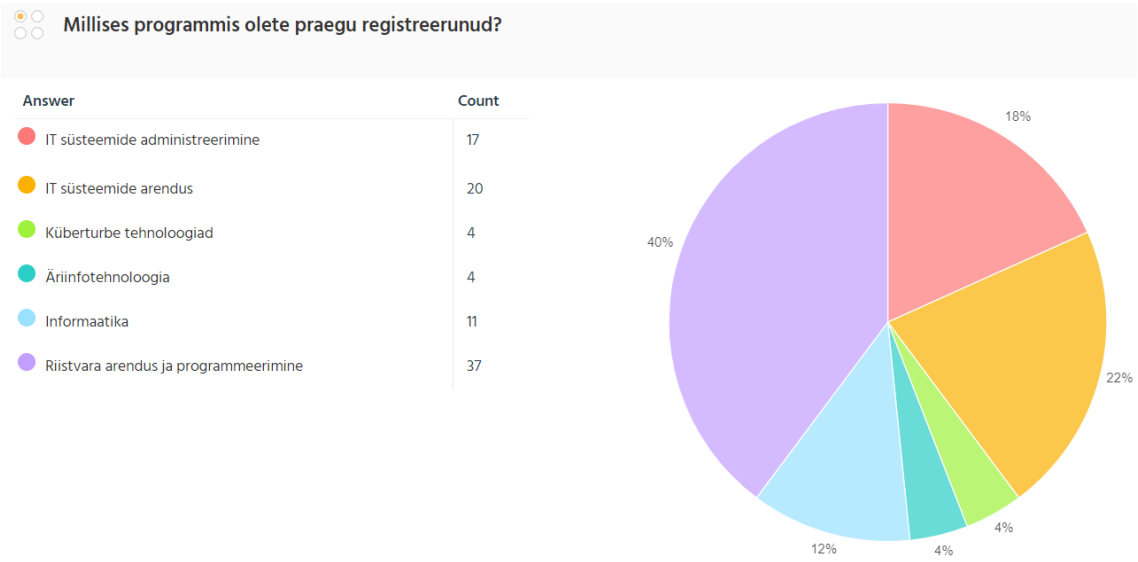

Figure 3. Submitted answers in Estonian.

A total of 110 students participated, with five incomplete responses, resulting in 104 submissions received.

There are 25 students participated from the first year of studies, 58 from the second, 17 from the third, 5 from the fourth, and 4 from the fifth year of studies or more.

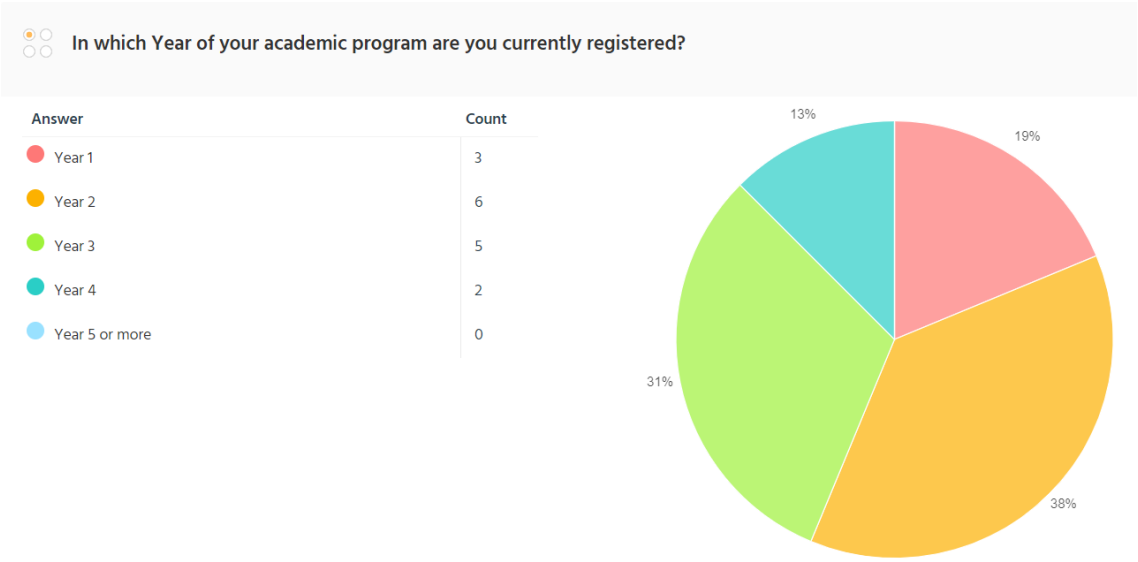

Figure 4. Academic year of the programme (English survey).

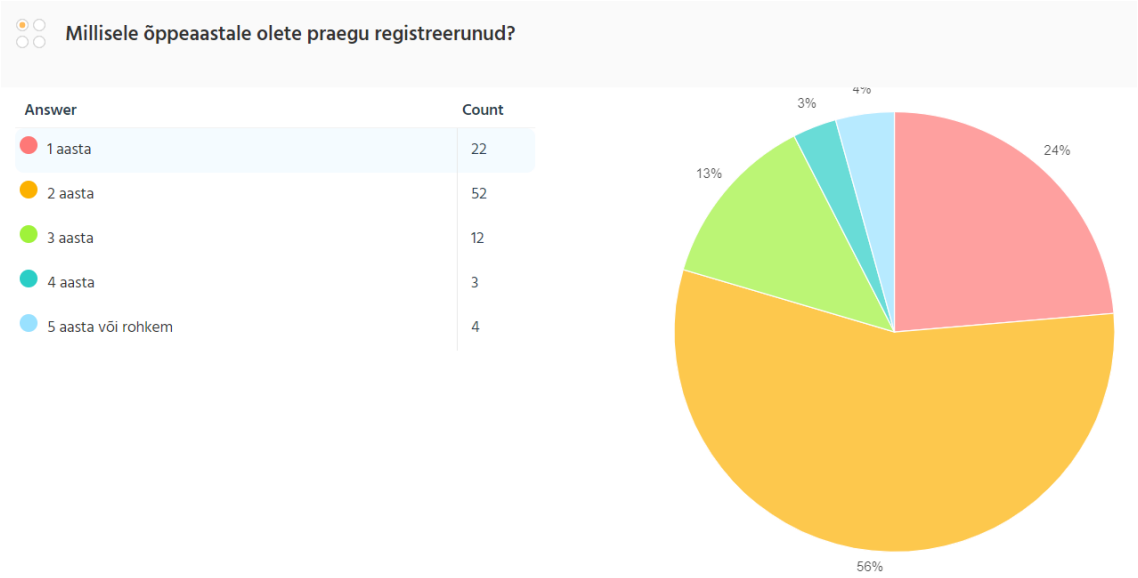

Figure 5. Academic year of the programme (Estonian survey).

Among the participants, second-year students were notably the most engaged, followed by first-year students, and then third-year students. Each programme included in the study typically requires 180 ECTS credits and is anticipated to be finished within three years. However, occasionally, various circumstances may prolong the duration for students to complete their programme requirements.

Table 5. Percentage of students based on academic year.

Answer choices	Count	Percentages
Year 1	25	22.94%
Year 2	58	53.21%
Year 3	17	15.60%
Year 4	5	4.59%
Year 5 or more	4	3.67%

After reviewing the submission results, considering the time spent answering questions, and identifying invalid answers, 8 responses were eliminated from the initial 110, resulting in 102 clean datasets suitable for analysis.

4 Analysis

This chapter aims to analyse the survey data to formulate strategies and guidelines tailored for fostering a strong cybersecurity culture within academic environment. The author utilized charts from SurveyLegend and Pivot Tables in Excel to identify correlations between survey questions, shedding light on different aspects of students' cybersecurity culture.

4.1 Online Habits

Investigating the internet usage habits of students was an integral part of this research. It was essential to ascertain the primary devices they used, and the amount of time spent online to grasp the potential cyber risks they may be exposed to. Utilizing descriptive statistics allowed to explore connections between variables like employment status, online duration, and other behavioural trends, offering valuable insights into their cybersecurity environment.

Table 6. Estimated time spent online.

Parameter	Daily	n	%	1y	2y	3y	4y	5+y	Working
Online Time	1-2 hours	0	0	-	-	-	-	-	-
	3-4 hours	16	15.69%	2	11	2	-	1	43.75%
	5-6 hours	31	30.39%	5	21	3	1	1	41.93%
	7-8 hours	29	28.43%	9	12	4	3	1	37.93%
	9-10 hours	26	25.49%	7	13	6	-	-	42.30%

- Among students spending 9 to 10 hours online daily, 25.49% fall into this category. Further breakdown reveals that 26.9% of first-year students, 50% of second-year students, and 23.07% of third-year students are within this group. 42.30% of the students are currently employed, and the time they spend online may also include work-related activities, depending on the nature of their job.

- 28.43% of students dedicating 7 to 8 hours to online activities each day, approximately 31.03% of those in their first academic year, 41.37% in their

second, and 13.79% in their third, 10.34% and 3.44% in their fourth and fifth year respectively. 37.93% of these students are employed, which is lower than the percentage of students who spend less than 7 hours per day online or more than 9 hours.

- 30.39% of students spending 5 to 6 hours on the internet daily, with 16.66% being first-year students, 67.74% second-year, 9.67 third-year students, and 3.22% fourth and fifth-year students. 41.93% of students are employed, which is also closer to the average of employed students.

- 15.69% of students are online daily for 3 to 4 hours, which represents the smallest percentage among the different time brackets. The breakdown is as follows: 12.5% are first and third-year students, 68.75% are second-year students, and 6.25% are fifth-year students. The highest percentage, 43.75%, of employed students spend the least amount of time online.

The preferred device among students is the Laptop/PC, constituting 59.80% of usage among both the age group of 24 years or younger and the age group of 31 years or older. Following closely is the smartphone, with a usage rate of 39.22% among those aged 24 years or younger and the age group of 25 to 30 years old. On the other hand, the Tablet is the least favoured device, accounting for only 0.98% of usage among individuals aged 31 years or older.

Table 7. The main device used for online activities for various age groups.

Parameter	**Item**	**n**		**%**
Main Device	Smartphone	40		39.22%
		Age:	n	
		24 or less 25 -30 31 or +	33 4 3	
	Tablet	1		.98%
		31 or +	1	
	Laptop/PC	61		59.80%
		Age:	n	
		24 or less 25 -30	51 3	

		31 or +	7	

Understanding students' employment status is crucial for researching cybersecurity culture as it provides insights into their time management strategies, online behaviour, and exposure to security threats. Employed students may allocate their time differently, impacting their engagement in online activities and cybersecurity practices.

In total, 41.17% of students are currently employed while pursuing their university studies. Primarily, students in their fourth and fifth years are engaged in employment, constituting the highest proportion. Following closely are second-year students, with 43.85% holding jobs, while approximately 30% of first and third-year students are also balancing work alongside their academic commitments.

Table 8. Employment status of students.

Employment	**n**		**%**	**Total by year**
Working	42		41.17%	
	1 year 2 year 3 year 4 year 5 year	7 25 5 2 3	16.66% 59.52% 11.90% 4.76% 7.14%	30.43% 43.85% 33.33% 50% 100%
Not Working	60		58.82%	
	1 year 2 year 3 year 4 year 5 year	16 32 10 2 0	26.66% 53.33 16.66% 3.33% 0	

Understanding the situation and tailoring cybersecurity awareness programmes to accommodate the needs and experiences of employed students can enhance the effectiveness of these initiatives in promoting a culture of cybersecurity among the student population.

4.2 Cybersecurity Behaviour and Awareness

In this study, cybersecurity behaviour was categorised into several subcategories, each offering unique insights into the overall security posture of the participants. These categories include Information Security Behaviour, which delves into how individuals handle and protect sensitive data; Cyber Hygiene, which focuses on everyday habits and practices that contribute to online safety; Proactive Awareness, examining the level of vigilance and preparedness against potential threats; Software Updates, addressing the diligence in keeping software and systems up-to-date to mitigate vulnerabilities; Password Security, assessing the strength and management of passwords for secure access; and Device Security, examining measures taken to safeguard devices against unauthorized access.

Table 9. Behaviour Scale, by year and programme.

School	Prog	#		Dev. Sec.	Pwd. Sec.	Proact. Awar.	Soft. Upd.	Cyber Hyg.	I. Sec. Beh.	Total
		Y.	n	Mean (<= 20)	Mean (<=15)	Mean (<=30)	Mean (<=10)	Mean (<=15)	Mean (<=15)	%
IT College	IT System Admin.	1y	8	17.3	11.87	14.75	8.25	12	7.25	11.33
		2y	6	18	10.33	13.66	7.66	13.33	5.66	10.96
		3y	1	13	11	8	8	12	7	10.2
		4y	0	-	-	-	-	-	-	
		5y	0	-	-	-	-	-	-	
	IT System Development	1y	4	17.7	10.25	15.25	7.5	11.75	6.25	10.69
		2y	7	17.8	11	13.57	7.42	12.28	6.85	11.07
		3y	4	15.2	10.75	13.75	8	9.75	6.5	10.04
		4y	1	15	7	10	8	11	7	9.6
		5y	2	17.5	10.5	13	8	7.5	6.5	10
	Cybersecurity Engineering	1y	2	18	9.5	17	9	10.5	6	10.6
		2y	4	16.5	11.75	13	7.75	11	6.75	10.75
		3y	4	17.2	11	15.25	7.75	12.5	7	11.09
		4y	2	16.5	12	13	7.5	12	7	11
		5y	0	-	-	-	-	-	-	

Department of Software Science	Business Information	1y	3	16.3	9	14.66	7	9.66	4.33	9.25
		2y	1	20	12	11	9	15	8	12.8
		3y	1	20	9	14	6	13	8	11.2
		4y	0	-	-	-	-	-	-	
		5y	0	-	-	-	-	-	-	
	Informatics	1y	6	15	7.66	16.16	7	9.83	4.33	8.76
		2y	3	14.3	9	15.66	8.33	12.66	7.66	10.39
		3y	2	11	7	17	3.5	11	6	7.7
		4y	1	13	7	18	3	7	2	6.4
		5y	1	18	12	10	8	15	9	12.4
Department of Computer System	Hardware Dev. and Programming	1y	0	-	-	-	-	-	-	
		2y	36	15.1	9.61	14.08	6.58	10.94	5.22	9.49
		3y	3	12.6	9	16.66	6	8.66	5.66	8.38
		4y	0	-	-	-	-	-	-	
		5y	0		-	-	-	-	-	

To assess Device Security habits, participants were presented with a series of questions probing various aspects of their behaviour. These inquiries delved into actions such as enabling automatic screen locking on computers to prevent unauthorized access after periods of inactivity, manually locking computer screens or room doors when stepping away, utilizing PINs or passcodes to unlock mobile phones, and employing biometric authentication methods such as fingerprints or facial recognition for mobile phone access. These questions aimed to gauge individuals' adherence to security measures regarding their devices, encompassing both personal computers and mobile phones. The highest results in device security behaviour, at 18.76%, were attained by students from Business Information Technology (BIT), followed by Cybersecurity Engineering (CE) students at 17.05%. Subsequently, ITSA and ITSD students achieved close percentages of 16.1% and 16.64% respectively, while Informatics and HD&P students demonstrated the lowest rates, recording 14.26% and 13.85% respectively.

To evaluate the strength of password security practices, participants were asked a series of questions. These queries delved into behaviours such as the propensity to change passwords even in the absence of requirements, the diligence in updating passwords for different accounts, the adoption of unique passwords for each account, and the effort to craft robust passwords surpassing minimum criteria when establishing new online

accounts. Students enrolled in ITSA and CE programmes exhibit the highest levels of password security behaviour, with 11.06%. Following closely are students from ITSD and BIT, with 9.9% and 10% respectively. Subsequently, HD&P students demonstrate a rate of 9.30%, while Informatics students show a slightly lower percentage at 8.53%.

To assess proactive awareness habits, participants were presented with a set of questions. These inquiries aimed to measure behaviours such as the tendency to click on links without verifying their destination, reliance on the visual appearance of websites rather than scrutinizing the URL bar, submission of information without confirming secure transmission, cautious inspection of links before clicking, and the response to encountering security issues, including the inclination to overlook them under the assumption that someone else will address the problem. Additionally, participants were queried about their willingness to install unreliable software on their devices. For this behaviour measurement, the percentage is reversed; the lower the percentage, the more secure the behaviour is. ITSA students exhibited the highest level of proactive behaviour at 10.54%, closely followed by ITSD students at 11.7%. CE students displayed proactive behaviour at a rate of 12.12%, slightly higher than BIT students at 12.33%. Conversely, the lowest rates of proactive behaviour were observed among Informatics students at 13.8% and HD&P students at 13.33%.

The survey examined participants' tendencies regarding software updates, gauging their promptness in installing updates and their diligence in ensuring the programmes they use are up-to-date. CE, ITSA, ITSD, and BIT students received the highest percentages, ranging from 7.33% to 8%, while HD&P and Informatics students received the lowest at 5.96% and 6.29%, respectively.

To assess Cyber Hygiene habits, participants were queried on various practices, including checking and removing viruses and malicious software, utilizing built-in antivirus programmes where available, and deleting suspicious emails without reading them. BIT students exhibit the highest percentage in this security habit, with 12.55%, closely followed by ITSA students at 12.44%. Following them are CE students at 11.4% and Informatics students at 11.09%. On the other hand, ITSD students show a percentage of 10.45%, while HD&P students demonstrate the least at 9.8%.

To analyse Information Security Behaviour habits, respondents were queried on their practices regarding security technologies to safeguard confidential information and their usage of automatic backups to ensure the safety of their files. CE students exhibit the highest percentage at 6.68%, closely followed by ITSA students at 6.63% and ITSD at 6.62%. Informatics students demonstrate a percentage of 5.79%, while HD&P students have 5.44%. The lowest percentage is seen among students enrolled in the BIT programme, standing at 4.37%.

Table 10. Students Behaviour by programme and by school.

Programmes	Device Sec	Pwd Sec.	Proact AW	Soft Upd	Cyber Hygiene	Info Sec. Behaviour	Mean by Prog	Mean By Sch.
IT System Admin.	16.1	11.06	10.54	7.97	12.44	6.63	10.84 10.54	10.64 11.45
IT System Develop.	16.64	9.9	11.7	7.78	10.45	6.62	10.27 11.7	
Cybersec. Eng.	17.05	11.06	12.12	8	11.4	6.68	10.83 12.12	
Business Information Technology	18.76	10	12.33	7.33	12.55	4.37	10.60 12.33	9.83 13.06
Informatics	14.26	8.53	13.8	5.96	11.09	5.79	9.07 13.8	
Hardware Dev. and Prog.	13.85	9.30	13.33	6.29	9.8	5.44	8.93 13.33	8.93 13.33

In this study, an interesting aspect is examining the variation in Cybersecurity Behaviour Scale among the three departments within the School of Information Technologies. Notably, the highest overall percentage, indicative of higher security behaviour, is observed in the IT College, boasting a notable 10.64%. This department encompasses three programmes, including ITSA, ITSD, and CE. Following behind is the Department of Software Science, presenting a percentage of 9.83%, housing two programmes, BIT and Informatics. Then, the Department of Computer Systems, hosting the HD&P programme, exhibits the lowest percentage at 8.93%. This comparison sheds light on the differential emphasis on cybersecurity practices across these academic departments.

However, the author acknowledges that students from the Department of Computer Systems, the HD&P programme, displayed notable engagement, with an impressive 38.23% participation rate in the survey. Additionally, their leadership exhibited strong support for the research effort. This underscores a significant commitment to security and a proactive stance toward enhancing cybersecurity culture within the department.

4.3 Dynamics of Cybersecurity Behaviour

Another insightful perspective to explore in this research is the analysis of cybersecurity behaviour across academic years, examining how the behaviour of freshman students evolves throughout their tenure at the university.

Examining the overall statistics on Security Behaviour across all programmes by academic year reveals a subtle decrease in the strength of security behaviour over time. Interestingly, first-year students, who are just beginning their studies, exhibit higher security behaviour compared to third or fourth-year students. There appears to be an exception with fifth-year students, although this could be attributed to a limited number of participants or other factors. However, when considering Proactive Awareness Behaviour, first-year students scored the lowest, while the highest percentage of 12.33% was observed among fifth-year students, followed by second-year students.

Table 11. Students behaviour by academic year.

	Academic Year	Dev. Sec. (mean)	PSW Sec. (mean)	Proact. AW (mean)	Soft. Upd. (mean)	Cyber H (mean)	Info Sec Behaviour (mean)	Total %
ALL PROGRAMS	1 year	16.73	9.91	15.39	7.69	10.95	5.82	10.13 15.39
	2 year	15.87	10.01	13.94	6.94	11.52	5.75	10.01 13.94
	3 year	14.86	9.86	14.93	6.8	10.08	6.53	9.62 14.93
	4 year	15.25	9.5	14.75	6.5	10.5	5.75	9.5 14.75
	5 year +	17.66	11	12.33	8	10	7.33	10.79 12.33

Upon delving deeper into the Behaviour scale by both year and programme, it becomes evident that programmes like HD&P and ITSA exhibit a similar descending trend, with first-year students displaying the highest security behaviour, followed by a gradual

decline in subsequent years. Conversely, ITSD and Informatics programmes depict lower percentages of security behaviour among first-year students, which then improve in the second year before declining again in the third and fourth years of study. Notably, CE programme students demonstrate a consistent upward trend in security behaviour throughout their three academic years.

4.4 Password Management

In the realm of cybersecurity, the method of storing passwords is of paramount importance as it directly correlates with the protection of sensitive information. Utilizing a password manager not only ensures the security of passwords but also enhances convenience by generating strong, unique passwords for different accounts and securely storing them in an encrypted vault [102]. Conversely, resorting to writing down passwords on paper or saving them in an unsecured digital file poses significant risks of exposure to unauthorized individuals, potentially leading to identity theft or data breaches. Furthermore, sharing passwords with others, although seemingly innocuous, can compromise the confidentiality of personal accounts and jeopardize the integrity of sensitive data.

In the evaluation of Password Management habits, students were questioned about their approaches to password storage and whether they intended to share passwords with acquaintances. Additionally, it was vital to ascertain if students utilized specific authentication methods like Uni-ID, ÕIS User or Estonian ID card, Mobile ID, or Smart ID for university environment entry. These inquiries sought to uncover the varied methods students use to organize and safeguard their passwords, providing insights into common practices.

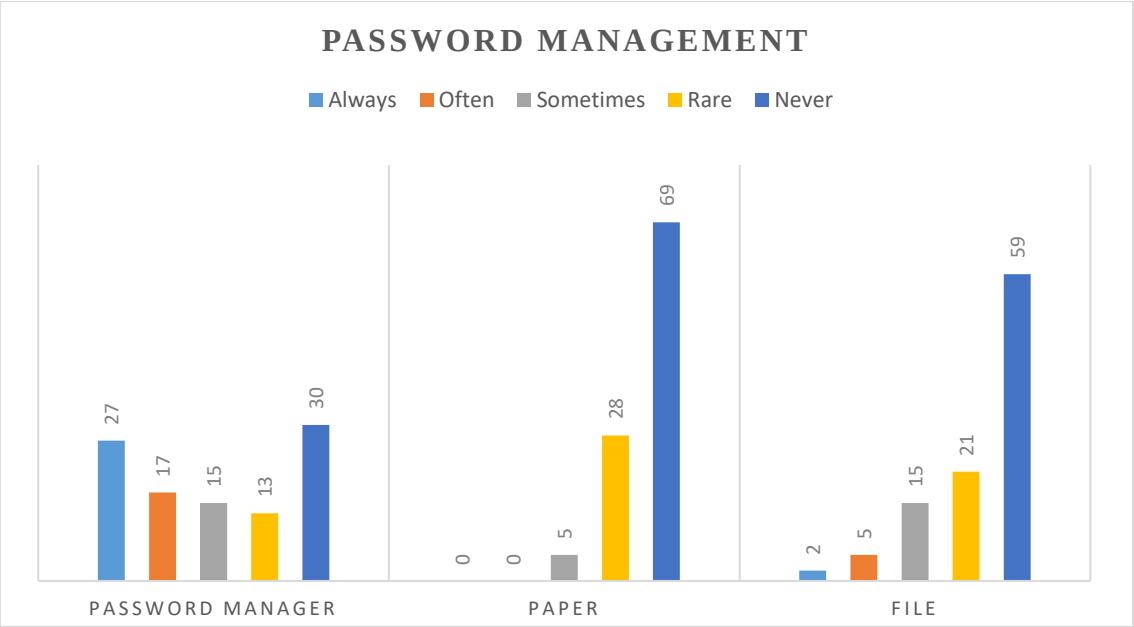

Figure 6. Preferred method for storing passwords (n).

The results showed that the preferred method for storing passwords is using a Password Manager, with 26% of students opting for this method. Conversely, the least favoured approach is writing down passwords on paper, with 67.64% of students indicating that they "never" employ this method.

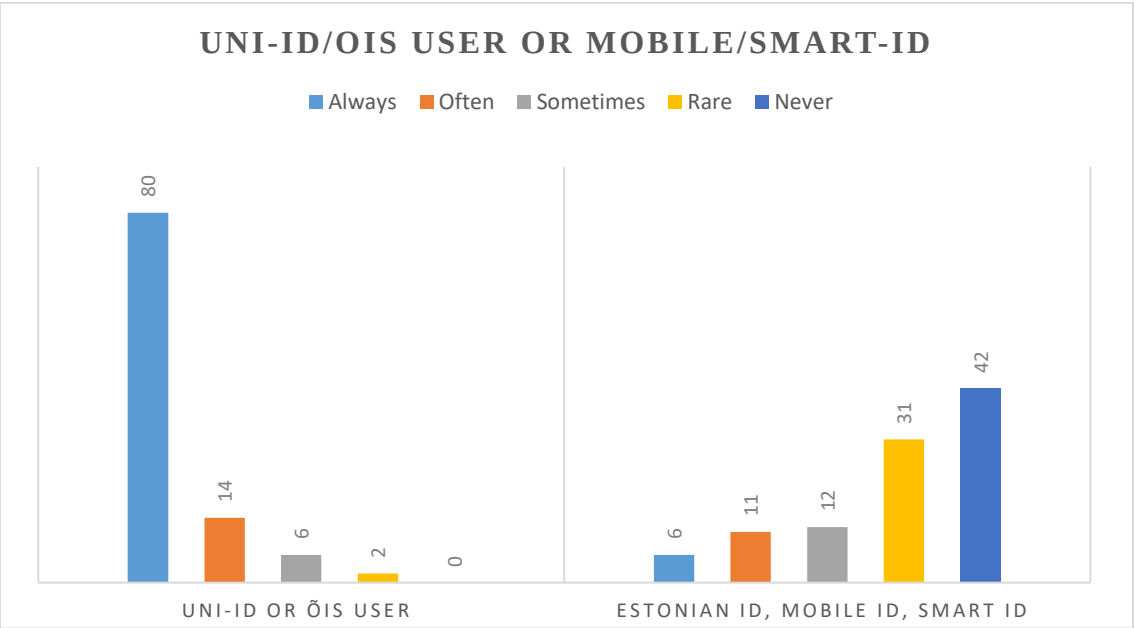

Figure 7. Preferred methods of accessing the university environment.

As for password sharing, the research reveals that none of the students surveyed reported sharing their passwords with anyone. Additionally, a significant majority, comprising

64.70% of respondents, stated that they would never share their passwords. This underscores their commitment to confidentiality and privacy.

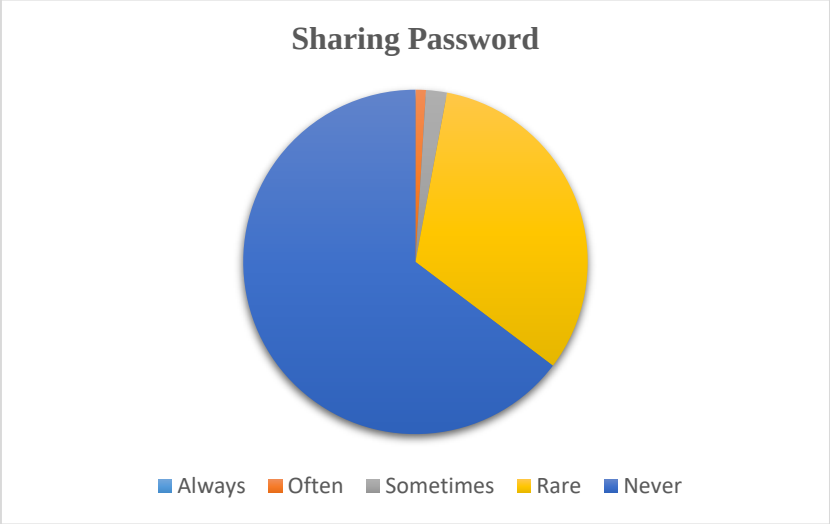

Figure 8. Sharing passwords.

4.5 Cybersecurity Awareness within University

The assessment of Cybersecurity Awareness within the University delves into several aspects, examining students' perceptions and experiences regarding cybersecurity education and support. Students were asked various questions to evaluate their awareness, views, and engagement with cybersecurity practices within the university context. These inquiries included whether students are personally interested in and study cybersecurity laws and regulations. Also, their perception of the university's emphasis on cybersecurity education, awareness of cybersecurity policies and procedures, satisfaction with the training and support provided. Additionally, it was assessed whether any students had reported cybersecurity incidents or concerns to the university's IT department during their studies. These questions aim to elucidate the extent to which students are informed, engaged, and supported in cybersecurity matters, shedding light on potential areas for enhancement and ensuring a proactive approach to cybersecurity culture within the academic community.

The survey questions and corresponding responses are displayed in a bar graph, showing that the majority of students believe that the university “sometimes” or “often” places importance on cybersecurity education. However, responses regarding the university's execution of cybersecurity activities lean towards "sometimes." Similarly, opinions vary

regarding satisfaction with cybersecurity training and support, with responses evenly distributed between "sometimes" and "often." Notably, a significant portion of students indicated "rare" when asked if the university informs about policies and procedures. Additionally, when queried about their awareness of existing policies and procedures, students predominantly indicated "sometimes" or "rare."

Questions:

Q1. I think my university places great importance on cybersecurity education.

Q2. My university carries out cybersecurity education activities.

Q3. I am satisfied with cybersecurity training and support provided by my university.

Q4. The University informing us about our cybersecurity policies and procedures.

Q5. I am aware of the cybersecurity policies and procedures in place at my university.

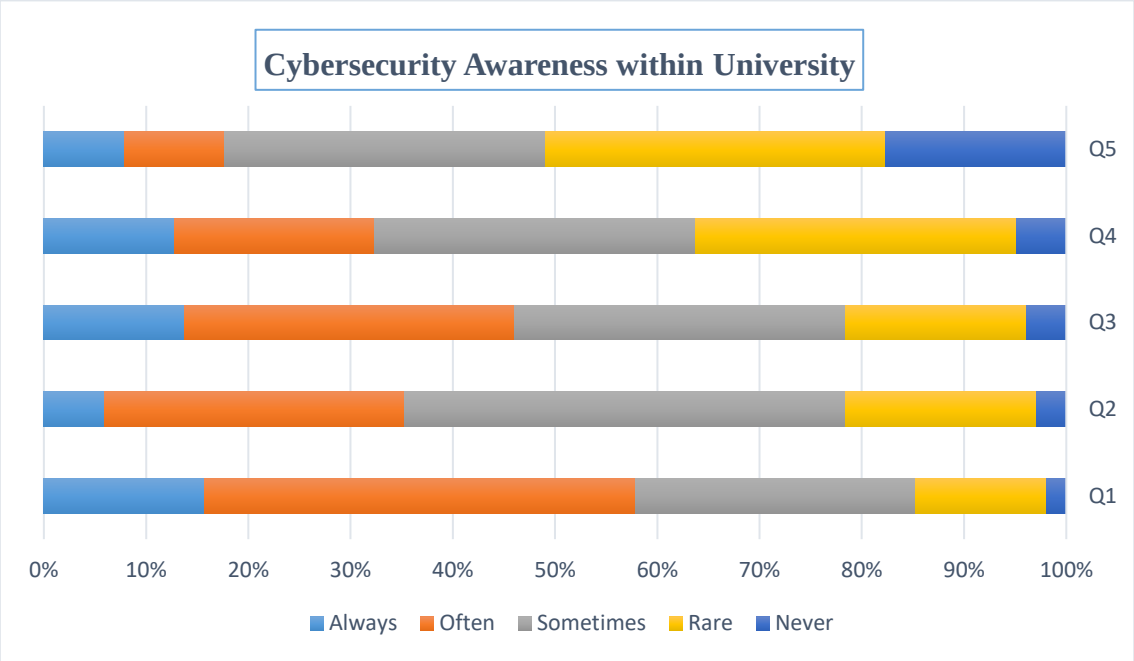

Figure 9. Representation of answers from Q1 to Q5 on Cybersecurity Awareness in University.

Additionally, understanding whether students have reported cybersecurity incidents or concerns to the university's IT department is crucial for several reasons. Firstly, it provides insights into the effectiveness of the university's cybersecurity infrastructure and policies. If students are reporting incidents, it suggests that they are aware of security issues and are proactive in addressing them, indicating a robust cybersecurity culture within the institution. Conversely, a lack of reported incidents could either mean that students are unaware of how to report, perceive severity of incidents or that there are gaps in the reporting process, highlighting areas for improvement.

Based on the results, it appears that BIT students have never reported any incidents, while HD&P and ITSA students are the most proactive in reporting their concerns to the IT Department of the university. Further analysis may be needed to understand the underlying reasons behind these variations and to identify potential strategies for encouraging reporting among all student groups.

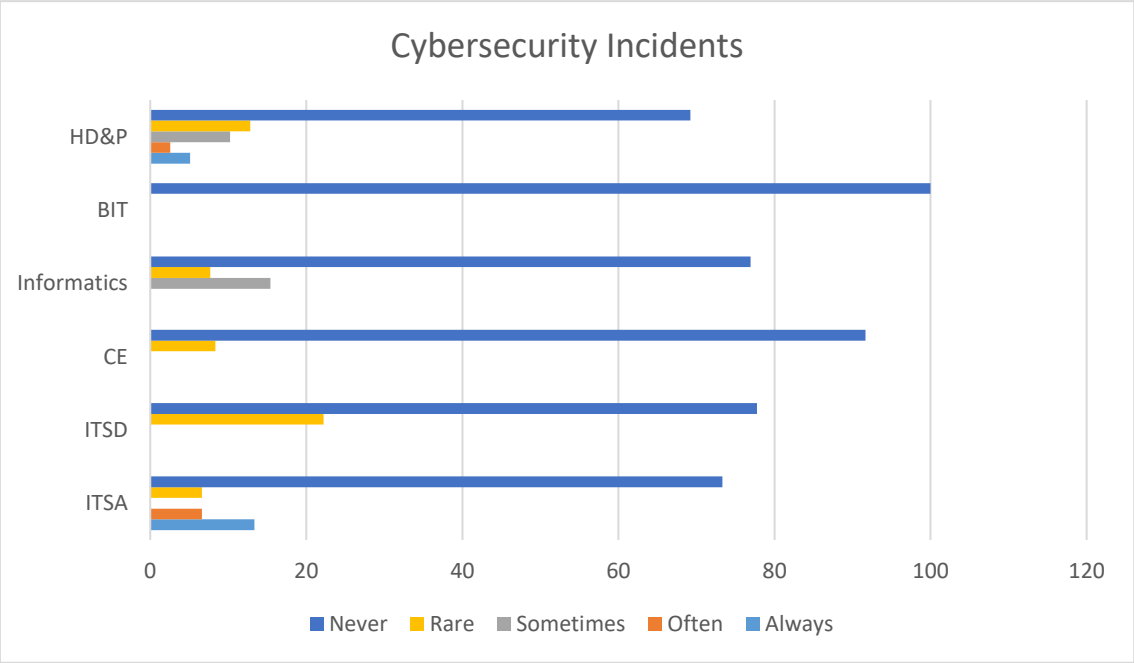

Figure 10. Reported cybersecurity incidents or concerns by the programme.

To gain insight into the factors influencing students' cybersecurity culture, the author sought to identify the sources from which students acquire knowledge about best cybersecurity practices. Students were asked to indicate the information sources they relied on, with the option to select multiple choices. By exploring the diverse range of sources students utilize to enhance their cybersecurity knowledge, the author aims to uncover the multifaceted nature of cybersecurity awareness and education among students.

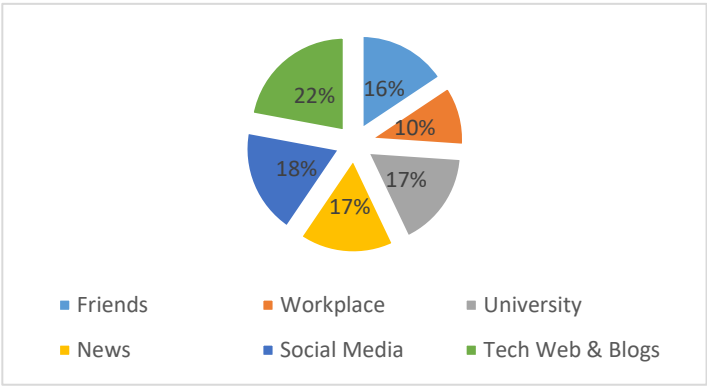

Figure 11. Sources of cybersecurity best practices information.

Table 12. Sources of cybersecurity best practices information.

Source	n	%
Friends	51	15.69%
Workplace	34	10.46%
University	55	16.92%
News	54	16.61%
Social Media	59	18.15%
Tech Web & Blogs	72	22.15%

According to the collected data, Technical Websites and Blogs emerge as the primary information source for students, closely followed by Social Media Platforms, with the University ranking third. Conversely, the workplace is identified as the least utilized source of information among all enrolled students.

Furthermore, the author aimed to gather students' perspectives and preferences regarding cybersecurity by posing an open-ended question: "What additional resources or support would you like to see in terms of cybersecurity education?" The subsequent responses obtained are highly valuable as they indicate that students dedicated time to reflect on and articulate their thoughts (in original form):

- There could be more seminars on cybersecurity.
- More activities, such as practical seminars or conferences related to cybersecurity.
- More practical ways to use tools for pentest, or at least some Bs degree subjects for pentestation, recon, and the like. The only subject that really helped me at work was the master's degree programme.
- A stronger and stricter fundamental basis - the content must be understood.
- Breeding offensive capability; The dangers of IoT
- The basics of cybersecurity are mandatory for everyone!
- Seminars, trainings, lectures
- Practical lessons on attacks and application protection from a development perspective

4.6 Comparison of Curriculum

Comparing students' curricula helps in understanding the emphasis placed on cybersecurity education within different academic programmes. Variations in curriculum can indicate the level of importance given to cybersecurity across disciplines. Therefore, a table detailing the curriculum of all undergraduate programmes within the School of Information Technology was compiled (see Appendix 5) to reveal any gaps or inconsistencies in cybersecurity education.

The curriculum for Hardware Development and Programming (IACB17/24), consisting of 180 ECTS credits, as outlined in the "Standard Study Plan", includes only one dedicated course on cybersecurity (Foundations of Cybersecurity (ITI0216). This course is typically offered to students during their 6th semester of studies. While there are additional courses available in the first year, such as Programming, Software Project, and Introduction to Information Technology, which may touch upon the importance of cybersecurity, a specific focus on security-related coursework is introduced only in the third year of the programme.

Informatics (IAIB17/24), with a curriculum totalling 180 ECTS credits, as per the "Standard Study Plan", also features only one dedicated course on cybersecurity, titled "Foundations of Cybersecurity (ITI0216)", offered in the 4th semester of students' studies, corresponding to the second academic year. Based on the description, the course aims to equip students with comprehensive knowledge and skills in various aspects of information security. Upon completion, students are expected to grasp general concepts such as the C-I-A triad and basic principles of cryptography, discern security components, and understand common security risks in web applications, including the OWASP Top 10 vulnerabilities. Furthermore, students learn to utilize information security tools like Wireshark and Nmap, apply log management tools such as Splunk and Elastic Stack for security event analysis, and employ different techniques for detecting and analysing malware, enhancing their ability to respond effectively to information security incidents.

In the Business Information Technology programme (IABB17/24), encompassing 180 ECTS credits according to the "Standard Study Plan", the mandatory course "Fundamentals of Information and Cybersecurity (ITB1711)" is situated in the 5th semester, during the third academic year. Based on the course description, upon

completion of this course, students acquire a comprehensive understanding of terminology within the information security domain, distinguishing between various terminologies such as information security, cyber defence, and cyber security. Additionally, they gain insight into the process and life cycle of information security, familiarize themselves with best practices in security management, and grasp the economic dimensions of cybersecurity. Moreover, students become proficient in identifying tools and strategies to optimize information/cybersecurity costs.

In the Administration of IT Systems programme (IAAB17/24), comprising 180 ECTS credits according to the “Standard Study Plan”, there exists one mandatory course, “Data Security and Cryptology (ICA0003)”, in the 3rd semester of students' studies, followed by one elective course, “Security of Computer Networks (ICA0015)”, in the 4th semester, during the second academic year. The description of the course ICA0003 outlines the following learning outcomes: Upon completion of the course, students become acquainted with the fundamental concepts of data security and cryptography, discerning their interrelationships. They acquire proficiency in employing diverse techniques and methodologies to ensure data security across various practical scenarios. Moreover, students develop the capability to utilize modern cryptographic algorithms and protocols at a level essential for practical data securing purposes. Additionally, students gain familiarity with all components of the Estonian national information security infrastructure, including eID solutions, PKI, ISKE, X-road, among others, and demonstrate competence in utilizing them across diverse practical contexts. Furthermore, students are equipped to identify the relationship between data security and practical IT problems, along with typical approaches to addressing them. Lastly, students gain insight into the legal regulations governing common security-related topics, such as eID solutions, personal data protection, digital signature, and risk analysis, within Estonia, the European Union, and globally. In addition, the Security of Computer Networks (ICA0015) elective course in the 4th semester, focuses on equipping students with the necessary skills to secure routers and switches against various known attacks. Essential topics covered include the setup and management of IPsec tunnels, the configuration of firewalls, and the implementation of Virtual Private Networks (VPNs). Through practical exercises and theoretical knowledge, students learn how to fortify network infrastructure to mitigate potential security risks and ensure robust protection against cyber threats.

IT Systems Development (IADB17/24) programme, as outlined in the “Standard Study Plan,” incorporates a single elective course titled “Data Security and Cryptology (ICA0003)” in the 3rd semester of students' studies. Interestingly, this course is also part of the Administration of IT Systems programme curriculum, where it is compulsory. Therefore, while IT Systems Development students have the option to take this course, it is a mandatory component for Administration of IT Systems students. Hence, there are no other courses with a specific focus on cybersecurity offered for students in this programme, indicating that the elective course “Data Security and Cryptology (ICA0003)” serves as the sole opportunity for students.

The Cyber Security Engineering programme, curriculum IVSB17/24 with 180ECTS, as stated in the “Standard Study Plan” offers a comprehensive array of courses focusing on cybersecurity across its three academic years. In the first year, students engage with both mandatory and elective courses tailored to cybersecurity, including the mandatory “Introduction to Cybersecurity (ICS0002)”and the elective “Information Security Risk Management (ICS0035)”. Moving into the second year, students delve deeper into cybersecurity with three mandatory courses: “Security of Computer Networks (ICA0015)”, “Cyber Security Management and Governance (ICS0009)”, and “Social Engineering (ICS0018)”, alongside an elective option, “Cryptography (ICS0026)”. Finally, in the third year, students encounter two mandatory courses, “Secure Programming (ICS0022)” and “Malware (ICS0028)”, complemented by elective choices in “Web Application Security (ICS0027)”and “Computer Forensics (ICS0033)”. This structured curriculum ensures that students receive comprehensive training across various facets of cybersecurity, preparing them for the complexities of the field.

Upon scrutinizing the curricula across different programmes, it becomes evident that, with the exception of Cyber Security Engineering, there exist discrepancies and deficiencies in cybersecurity education. Notably, there is a lack of standardized cybersecurity curricula, even at a fundamental level, across these programmes. Despite all programmes falling within the technical domain of the School of Information Technology, the degree of emphasis on cybersecurity education varies significantly. Consequently, there is a notable absence of a unified security framework, shared principles, and foundational knowledge essential for fostering a robust cybersecurity culture.

5 Proposed Guidelines

The author suggests the implementation of the following guidelines based on the collected data:

1. The emphasis should be placed on leadership. It is essential to align the leadership with cybersecurity initiatives as new security policies cannot be effectively introduced without their understanding and support. Leaders need to comprehend the rationale behind new systems and grasp the significance of cybersecurity, including the repercussions of neglecting best practices. Therefore, leadership should undergo awareness training and stay informed about developments in the cybersecurity domain. By setting an example and adhering to newly established security protocols, they can effectively safeguard the educational environment.

2. The university should conduct a comprehensive analysis of the security landscape, encompassing not only students from all schools but also all levels of leadership, including deans, programme managers, their assistants, and all other employees involved in the educational process.

3. The university should assess its current management and consider potential alterations, especially given the shift towards a more digital educational landscape, necessitating individuals who are flexible and forward-looking.

4. By understanding the current security landscape, the university should develop comprehensive procedures and policies that cover all cybersecurity aspects and are applicable to all stakeholders. This involves crafting robust guidelines for data protection, network security, access control, incident response, and awareness training. These policies should be designed to address potential vulnerabilities, mitigate risks, and promote cybersecurity culture throughout the academic community. Furthermore, these policies must be introduced and communicated to all students and employees to ensure their familiarity and accessibility.

5. Regular security assessments and audits play a pivotal role in ensuring the ongoing effectiveness and relevance of these policies. By conducting these assessments, the university can gauge its security preparedness and identify any potential vulnerabilities or shortcomings in its existing measures. This proactive

approach not only helps validate the effectiveness of implemented policies but also enables the institution to uncover and address any gaps in its security posture.

6. Moreover, instituting well-defined protocols for incident reporting and response mechanisms is essential for ensuring prompt and efficient management of security incidents, thereby mitigating their potential impact on university operations. These protocols should be communicated to all students and employees of the university to ensure widespread awareness and understanding. Also, regular practice drills for reporting can help familiarize individuals with the reporting process, ensuring they know who to contact and providing them with assurance that their reports will be followed up on and resolved in a timely manner. This proactive approach not only promotes a culture of transparency and accountability but also strengthens the university's overall cybersecurity culture.

7. The university should develop foundational mandatory cybersecurity courses for all students across programmes to ensure they acquire essential knowledge about current threats, risks, and vulnerabilities. These courses should also cover topics such as phishing, social engineering, and mitigation strategies, aiming to make students comfortable with security concepts and equip them to identify and respond to security incidents effectively. It's imperative that these courses are consistent and taught at least once a year to provide students with repeated exposure and reinforcement of cybersecurity best practices throughout their academic journey. Additionally, the university should regularly host seminars and conferences, inviting experts to speak on a wide range of security topics.

8. The university should establish a dedicated Research Hub for its students. With a student body exceeding 10,000 from diverse backgrounds and nationalities, there's a wealth of perspectives and insights waiting to be tapped. Many students, at some point in their academic journey, will need to conduct research, whether for their thesis work or as part of coursework. Providing access to this extensive pool of opinions and thoughts from fellow students is essential for facilitating research endeavors. To achieve this, a standardized system should be implemented, outlining procedures for creating questionnaires and selecting appropriate platforms for survey distribution. The university could explore partnerships with local companies offering survey services to streamline this

process. By facilitating access to research resources and fostering collaboration among students, the university can enhance the academic experience and promote knowledge sharing within its community.

9. The university should create a Cybersecurity Club, providing a platform for students to share knowledge, collaborate on projects, and develop innovative solutions to enhance security within the academic community. Research has shown that students often learn effectively from their peers, as they are on a similar mental wavelength and can communicate information in a relatable manner [103]. The club's initiatives and innovations should be actively supported and encouraged by the university administration, fostering a culture of creativity and collaboration in addressing cybersecurity challenges.

10. The University should establish and financially support a "Gaming for All" initiative, offering students the opportunity to engage in cybersecurity games and utilize gaming platforms for practicing attack/defense techniques and penetration testing. Platforms such as RangeForce [104], TryHackMe [105] and others, can be integrated into this initiative to provide hands-on experience and practical skills development.

11. The University should foster collaborations with international organizations that issue certifications in various security topics. These certifications serve as tangible proof of students' knowledge and skills in cybersecurity, enhancing their competitiveness in the job market and preparing them effectively for future careers. By supporting students in obtaining these certifications, the university demonstrates a genuine commitment to their professional development, thereby nurturing a culture of trust, support, and appreciation essential for fostering a robust cybersecurity culture.

12. The university should actively promote a cultural transformation aimed at fortifying its security environment, advancing research progression, and elevating its reputation on the global stage as a paragon of strength, security, supportiveness, and innovation. Drawing inspiration from successful cultural transformations like that of MIT, the university can establish itself as a beacon of excellence in academia and beyond.

6 Limitations and Future Research

Unfortunately, due to time constraints, the author was unable to conduct qualitative research through focused interviews with university leadership. Understanding the perspectives of university leaders on the importance of cybersecurity education and their visions for the future, could gather valuable insights for improving cybersecurity practices and fostering a more robust cybersecurity culture within the academic community. The author reached out to them via email, seeking valuable suggestions on the research and requesting support in distributing the survey to student. However, most leaders weren't forthcoming in delving deeper into the current cybersecurity landscape at the university and were reluctant to offer assistance.

The survey was disseminated online via email with the help of programme manager assistants. However, it is conceivable that with greater support from university leadership, a higher participation rate could have been achieved. For instance, in the HD&P programme, when the survey was distributed directly by the programme manager, participation rates were notably higher. If top-level leadership, including Deans, were actively engaged in this research initiative, the survey could potentially be mandated, ensuring a comprehensive response rate from all students.

The survey was limited to students within the School of Information Technologies. Future research endeavours could expand the scope to encompass other schools within Tallinn University of Technology, including the Schools of Economics, Science, Estonian Maritime Academy, and Engineering. Consolidating data from all five schools would facilitate comprehensive comparative analyses across various dimensions. However, given the extensive volume of data and the intricate nature of such an investigation, it may be more feasible as a doctoral research endeavour.

In addition, it would be intriguing to concurrently administer personality traits tests among the students, such as Big Five Inventory or Myers-Briggs Type Indicator (MBTI) [106]. The survey in this research is designed to align with certain behavioural categories that could be correlated with personality traits, providing a deeper understanding of the subject matter. The predictive power of personality traits regarding users' intentions regarding cybersecurity-related behaviour on their computer devices is significant. Certain characteristics, including agreeableness, have been found to be correlated with

victimization rates. On the contrary, there is a correlation between neuroticism and computer anxiety, suggesting that people possessing this characteristic are especially vigilant regarding their security and confidentiality, potentially reducing their vulnerability to social engineering schemes such as phishing [107].

Moreover, with the support of leadership, conducting deeper psychological analyses and testing using frameworks such as the Heuristic-Systematic Model (HSM), Protection Motivation Theory (PMT), and DoSpeRT (Domain-Specific Risk-Taking) [91] in relation to cybersecurity culture could yield valuable insights. Integrating these tests and analyses could significantly enhance the prediction of human behaviour and assist in fostering a robust cybersecurity culture, not only within academia but also on an organizational scale and across industries.

7 Conclusion

The goal of this research was to assess the current cybersecurity culture at Tallinn University of Technology, particularly within the School of Information Technologies, and to propose a set of guiding principles and best practices for developing a robust cybersecurity culture. The author focused on defining cybersecurity culture, and answered RQ1, through a review of existing literature and identifying limitations in current definitions. As a result, a new comprehensive definition of cybersecurity culture was proposed, suitable for both academic and organizational contexts. The following definition of cybersecurity culture is proposed: “Cybersecurity culture refers to the overall mindset, beliefs, behaviours, and practices concerning cybersecurity landscape. It encompasses both individual attitudes towards cybersecurity and collective efforts to promote security awareness, implement best practices, and effectively respond to cyber threats. In essence, cybersecurity culture reflects the organization's commitment to prioritizing and maintaining robust cybersecurity measures as an integral part of its operations and values”.

The author then focused on identifying the most effective methodologies for evaluating cybersecurity culture within educational settings to address RQ2. After careful consideration, it was determined that the optimal approach involves utilizing quantitative research methods alongside anonymized questionnaires. This ensures that respondents feel comfortable providing honest feedback. Moreover, this methodology allows for in-depth analysis, and once the suggested guidelines are implemented, the assessment can be repeated to measure any resulting changes over time.

The analysis of the collected data unveiled several noteworthy insights. Firstly, it became apparent that the highest level of survey participation occurred when there was support from university leadership, indicating that students are more responsive to initiatives spearheaded by their leaders. Additionally, the data showcased a discernible upward trend in cybersecurity behaviour and awareness among students enrolled in the Cybersecurity Engineering (CE) programme. This trend was found to correlate with the number of cybersecurity courses integrated into the CE curriculum, starting from the first semester and persisting throughout the duration of their studies. Another significant finding was the disparity in responses among students from the three schools under scrutiny. Students

enrolled in programmes affiliated with the IT College exhibited the most secure behaviour, as well as more robust awareness and perceptions regarding cybersecurity. Interestingly, the analysis also demonstrates that the influence of other environments, such as work and social circles, on students' cybersecurity culture is not pronounced enough to impact the cybersecurity culture within the university environment.

The collected data also indicates that a significant majority of students feel that the university does not adequately inform them about cybersecurity policies and procedures. Likewise, most students believe that the university does not conduct a satisfactory number of cybersecurity activities, leading to dissatisfaction with the level of support provided by the institution. Furthermore, fewer than 10% of students are convinced that the university places great importance on cybersecurity education.

Therefore, the analysis of collected data answered the RQ 3, and it suggests that within the School of Information Technologies, there seems to be a vulnerability in its cybersecurity culture, largely stemming from a lack of robust support from leadership and inadequate emphasis placed on cybersecurity education and practices. It appears that there's room for improvement in terms of dedicating attention, resources, and effort to bolster security measures, as well as in providing adequate support for students and their cybersecurity needs. Nonetheless, this study highlights the potential for positive change by implementing the proposed guidelines. These recommendations include instituting mandatory cybersecurity courses for all students from the outset of their studies, providing training for leadership and other stakeholders, fostering initiatives like the Cybersecurity Club, Research Hub, and Gaming for All, and conducting regular assessments to track progress in fortifying the cybersecurity culture.

It's also crucial to broaden this study in the future to encompass additional schools within Tallinn University of Technology and other educational institutions such as the University of Tartu and Tallinn University. Given Estonia's advanced technological landscape, prioritizing cybersecurity is paramount, emphasizing the importance of cultivating a cybersecurity culture beginning at the university level.

In concluding this pioneering study on cybersecurity culture within academia, particularly focused on Tallinn University of Technology, it's worth noting the potential impact it can have beyond its immediate scope. As the first of its kind in this domain, this research

serves as a foundational framework that other educational institutions can leverage to booster their own cybersecurity cultures. By extracting insights from the methodologies, findings, and proposed guidelines outlined in this study, universities worldwide can embark on similar journey to fortify their cybersecurity practices. This not only facilitates the sharing of best practices but also fosters a collaborative approach towards cultivating a robust cybersecurity culture across the academic landscape. Thus, this research not only contributes to the advancement of knowledge within the field but also serves as a catalyst for positive change in cybersecurity education and practices within academia.

References

[1] S. McAlmont, “3 big reasons that it’s time for higher education to crack down on cybersecurity,” 2 September 2022. [Online]. Available: https://universitybusiness.com/3-big-reasons-that-its-time-for-higher-education-to-crack-down-on-cybersecurity/. [Accessed April 2024].

[2] A. W. Batteau, “Creating a Culture of Enterprise Cybersecurity,” *International Journal of Business Anthropology*, vol. 2, no. No. 2 (2011), 2011.

[3] L. Hayden, People-centric security: transforming your enterprise security culture, McGraw Hill Professional, 2015.

[4] A. A. Hogail, “Cultivating and Assessing an Organizational Information Security,” *International Journal of Security and Its Applications*, vol. 9, no. No.7, pp. 163-178, 2015.

[5] A. D. Veiga, “A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument,” in *2016 SAI Computing Conference (SAI)*, London, UK, 2016.

[6] E. Stavrou, M. Bada, M. Ioannou, “Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination,” in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Oxford, UK, 2019.

[7] S. Furnell, M. Papadki, A.Tolah, “A Comprehensive Framework for Understanding Security Culture in Organizations,” in *Information Security Education. Education in Proactive Information Security. WISE 2019*, 2019.

[8] T. Robertson, R. Yan, S. Yong Park, S. Bordoff, Q. Chenn, E. Sprissler, Zheng Yan, “Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?,” *Computers in Human Behavior*, vol. 84, pp. 375-382, 2018.

[9] K. Sijtsmaa, F. Scheele, Jacob Willem Abraham Witsenboer, “Measuring cyber secure behavior of elementary and high school,” *Computers & Education*, vol. 186, no. 0360-1315, p. 104536, September 2022.

[10] H. T. Hongbo Guo, “A survey on college students’ cybersecurity awareness and education from the perspective of China,” *Journal for the Education of Gifted Young Scientists*, vol. 11(3), no. 2149-360X, pp. 351-367, September 2023.

[11] B. Oyetunde, “A year of advanced threats and global tensions: Estonia’s cybersecurity scene in 2023,” 9 April 2024. [Online]. Available: https://e-estonia.com/2023-estonia-advanced-cybersecurity-threats/. [Accessed 1 May 2024].

[12] Republic of Estonia Information System Authority, “RIA: The number of cyber attacks in 2022 was a hundred times higher than during the April Unrest,” 2 February 2023. [Online]. Available: https://ria.ee/en/news/ria-number-cyber-attacks-2022-was-hundred-times-higher-during-april-unrest. [Accessed 5 April 2024].

[13] RIA, “Cyber Security in Estonia 2023,” February 2023. [Online]. Available: https://ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf. [Accessed 8 April 2024].

[14] Chainalysis, “Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline,” 7 February 2024. [Online]. Available: https://www.chainalysis.com/blog/ransomware-2024/. [Accessed 15 April 2024].

[15] A. d. Veiga, *Cultivating and Assessing Information Security Culture,* Faculty of Engineering, Built Environment and Information Technology, University of Pretoria, 2008.

[16] J. R. Nurse, M. Bada, S. Furnell, Betsy Uchendu, “Developing a cyber security culture: Current practices and future needs,” *Computer & Security,* vol. 109, no. 102387, 2021.

[17] S. Alfawaz, K. Nelson, K. Mohannak, “Information security culture: A behaviour compliance conceptual framework,” in *Security, Information Aisc, Conference.*, 2010.

[18] J. Eloff, A. Da Veiga, “A framework and assessment instrument for information security culture,” *Computers & Security,* vol. 29, no. 2, pp. 196-207, March 2010.

[19] D. Lacey, “Understanding and transforming organizational security culture.,” *Information Management & Computer Security,* vol. 18, no. 1, March 2010.

[20] A. Ahamd, S. Chang, S. B. Maynard, Joo soon Lim, “Embedding information security culture emerging concerns and challenges,” in *Pacific Asia Conference on Information Systems, PACIS 2010,* Taipei, Taiwan, July 2010.

[21] L. Sanchez, A.S-Olmo, E.F.Medina, M. Piattini, “Security Culture in Small and Medium-Size Enterprise,” in *ENTERprise Information Systems. CENTERIS 2010. Communications in Computer and Information Science,* Springer, Berlin, Heidelberg., 2010.

[22] R. Von Solms, J.F. Van Niekerk, “Information security culture: A management perspective,” *Computers & Security,* vol. 29, no. 4, pp. 476-486, June 2010.

[23] M. A. Alnatheer, *Understanding and measuring information security culture in developing countries: case of Saudi Arabia,* PhD Thesis, Queensland University of Technology, 2012.

[24] Z. I. Noor Hafizah Hassan, “A conceptual model for investigating factors influencing information security culture in healthcare environment,” *Procedia - Social and Behavioral Sciences,* vol. 63, no. 1877-0428, pp. 1007-1012, December 2012.

[25] O. Olivos, “Creating a Security Culture Development Plan and a case study.,” in *International Symposium on Human Aspects of Information Security and Assurance.*, 2012.

[26] M. R. Rashid, M.S. Shahibi, S.K.W.Fakeh, “Determining factors influencing information security culture among ICT librarians,” *Journal of theoretical and applied information technology,* vol. 37, pp. 132-140, 2012.

[27] AlHogail and A. Mirza, “A proposal of an organizational information security culture framework.,” in *Proceedings of International Conference on Information, Communication Technology and System (ICTS),* Surabaya, Indonesia, 2014.

[28] A. Mirza, A. Ahogali, “A framework of information security culture change,” *Computer Science, Business,* 2014.

[29] L. V. Astakhova, “The concept of the information-security culture,” *Scientific and Technical Information Processing,* vol. 41, pp. 22-28, April 2014.

[30] "Security culture and the employment relationship as drivers of employees' security compliance," *Information Management & Computer Security*, vol. 22, no. 5, November 2014.

[31] N. Martins, Adéle Da Veiga, "Information security culture: A comparative analysis of four assessments," in *European Conference on Information Management and Evaluation*, Ghent, Belgium, September 2014.

[32] P. Oliveira, Isabel Lopes, "Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises," in *New Perspectives in Information Systems and Technologies, Volume 1. Advances in Intelligent Systems and Computing, vol 275*, 2014.

[33] R. Reid and J. V. Niekerk, "From information security to cyber security cultures," in *Information Security for South Africa*, Johannesburg, South Africa, November 2014.

[34] R. Reid, J. V. Niekerk and K. Renaud, "Information security culture: A general living systems theory perspective," in *Information Security for South Africa*, Johannesburg, South Africa, 2014.

[35] A. AlHogail, "Design and validation of information security culture framework," *Computers in Human Behavior*, vol. 49, pp. 567-575, August 2015.

[36] A. AlHogail, "Cultivating and assessing an organizational information security culture; an empirical study," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 163-178, 2015.

[37] M. A. Alnatheer, "Information security culture critical success factors," in *12th International Conference on Information Technology - New Generations*, Las Vegas, NV, USA, April 2015.

[38] H. Deng, B. Kam, Ahmed AlKalbani, "Organisational security culture and information security compliance for e-government development: The moderating effect of social pressure," in *Pacific Asia Conference on Information Systems(PACIS)*, 2015.

[39] A. D. Veiga, "The influence of information security policies on information security culture: Illustrated through a case study," in *Human Aspects of Information Security & Assurance*, Greece, Lesvos, June 2015.

[40] N. Martins, Adéle da Veiga, "IImproving the information security culture through monitoring and implementation actions illustrated through a case study," *Computers & Security*, vol. 49, pp. 162-179, March 2015.

[41] A. Greig, K. Renaud and S. Flowerday, "An ethnographic study to assess the enactment of information security culture in a retail store," in *World Congress on Internet Security (WorldCIS)*, Dublin, Ireland, October 2015.

[42] S. B. Maynard, A. Ahmad, S. Cheng, Joo S. Lim, "Information security culture: Towards an instrument for assessing security management practices," *International Journal of Cyber Warfare and Terrorism (IJCWT)* , 2015.

[43] N. Martins, Adéle Da Veiga, "An Information security culture model validated with structural equation modelling," in *Human Aspects of Information Security & Assurance*, Greece, Lesvos, July 2015.

[44] S. Furnell, &. N. Clarke, Emad Sherif, "An Identification of Variables Influencing the Establishment of Information Security Culture," in *Human Aspects of Information Security, Privacy, and Trust* , January 2015.

[45] A. D. Veiga, “Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study,” *Information and Computer Security,* vol. 24, no. 2, pp. 139-151, June 2016.

[46] 2. I. NOOR HAFIZAH HASSAN, “Information security culture in healthcare informatics: A preliminary investigation,” *Journal of Theoretical and Applied Information Technology,* vol. 88, no. 2, June 2016.

[47] L. E. Sanchez, I. Caballero, S. Camacho, E. F.-Medina, Antonio Santos-Olmo, “The importance of the security culture in SMEs as regards the correct management of the security of their assets,” *Information System Security,* July 2016.

[48] M. Li, T. Zhang, Mincong Tang, “The impacts of organizational culture on information security culture: a case study,” *Information Technology and Management ,* vol. 17, pp. 179-186, November 2015.

[49] N. Martins, Adéle da Veiga, “Defining and identifying dominant information security cultures and subcultures,” *Computers & Security,* vol. 70, pp. 72-94, September 2017.

[50] R. v. Solms, M. Grobler, J. Jansen van Vuuren, Noluxolo Gcaza, “A general morphological analysis: Delineating a cyber-security culture,” *Information and Computer Security,* vol. 25, no. 3, July 2017.

[51] N. Maarop, Z. Ismail, W. Z. Abidiin, N. H. Hassan, “Information security culture in health informatics environment: A qualitative approach.,” in *International Conference on Research and Innovation in Information Systems (ICRIIS),* Langkawi, Malaysia, July 2017.

[52] Q. N. Harun, M. K. Zaini, Mohamad Noorman Masrek, “Information security culture for Malaysian public organization: a conceptual framework,” in *4th International Conference on Education and Social Sciences* , Istanbul, Turkey , February 2017.

[53] A. D. Veiga, “An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture,” *Information and Computer Security,* vol. 26, no. 5, November 2018.

[54] Q. N. Harun, N. Z. Sahid, Mohamad Noorman Masrek, “Assessing the information security culture in a government context: The case of a developing country,” *International Journal of Civil Engineering and Technology ,* vol. 9, no. 8, pp. 96-112, August 2018.

[55] Q. N. Harun, M. K. Zaini, Mohamad Noorman Masrek, “The development of an information security culture scale for the Malaysian Public organization,” *International Journal of Mechanical Engineering and Technology (IJMET),* vol. 9, no. 7, July 2018.

[56] T. Z. Moraba Mokwetli, “Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa,” in *International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD),* Durban, South Africa, August 2018.

[57] S. F. Meyer, J. H. Honerud, T.O. Nævestad, “Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security,” in *Safety and Reliability – Safe Societies in a Changing World,* 2018, p. 9.

[58] D. K. Pearlson, Angelica Marotta, *A culture of cybersecurity at Banca Popolare di Sondrio,* A Culture of Cybersecurity at BPS, March1, 2019.

[59] A. Nasir, R.A.Arshar, M.R.ab Hamid, “A dimension-based information security culture model and its relationship with employees’ security behaviour: A case study in Malaysian higher educational institutions,” *Information Security Journal: A Global Perspective,* vol. 28, no. 3, pp. 55-80, 2019.

[60] L. Drevin, Frans Nel, “Key elements of an information security culture in organisations,” *Information and Computer Security,* vol. 27, no. 2, May 2019.

[61] P. Petrisor, “Promoting Cybersecurity Culture Through Education,” in *International Scientific Conference. elearning and Software for Education*, 2019.

[62] J. Ophoff, Zainab Ruhwanya, “Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania,” in *IFIP Advances in Information and Communication Technology,* April 2019.

[63] S. M. Furnell, M. Papadaki, Alaa Tolah, “A Comprehensive Framework for Understanding Security Culture in Organizations,” in *Information Security Education. Education in Proactive Information Security* , June 2019.

[64] C. v. '. Wout, “Develop and maintain a cybersecurity organisational culture,” in *14th International Conference on Cyber Warfare and Security,* Stellenbosch, South Africa, February 2019.

[65] M. Alshaikh, “Developing cybersecurity culture to influence employee behaviour: A practice perspective,” *Computers & Security,* vol. 98, November 2020.

[66] A. Gray, E. Collins, John M. Blythe, “Human cyber risk management by security awareness professionals: Carrots or sticks to drive behaviour change?,” in *HCI for Cybersecurity, Privacy and Trust* , July 2020.

[67] L. V. Astakhova, A. Botha, M. Herselman, Adéle da Veiga, “Defining organisational information security culture—Perspectives from academia and industry,” *Computers & Security,* vol. 92, May 2020.

[68] E. Kritzinger, M. Loock, S.G. Govender, “A Framework for the Assessment of Information Security Risk, the Reduction of Information Security Cost and the Sustainability of Information Security Culture,” *Personal and Ubiquitous Computing* , vol. 25, pp. 927-940, March 2021.

[69] A. Nasir, R. A. Arshah and M. R. A. Hamid, “Information Security Culture for Guiding Employee’s Security Behaviour: A Pilot Study,” in *6th International Conference on Information Management (ICIM)*, London, UK, March 2020.

[70] B. Schneider, P. M. Asprion, S. Androvicsova and W. and Azan, “A Practical Guideline for Developing a Managerial Information Security Awareness Program,” in *AMCIS 2020 Proceedings. INFORMATION SECURITY AND PRIVACY (SIGSEC)*, 2020.

[71] A. McCormac, D. Calic, Ashleigh Wiley, “More than the individual: Examining the relationship between culture and Information Security Awareness.,” *Computers & Security,* vol. 88, no. 101640, January 2020.

[72] S. Mouzakitis, K. Bounas, D. Askounis, Anna Georgiadou, “A Cybersecurity Culture Framework for Assessing Organization Readiness,” *Journal of Computer Information Systems* , vol. 62, no. 3, pp. 1-11, November 2020.

[73] E. Stamatiadis, A. Tzakas, K. Gounaris, A. Georgiadou, A. M.-Psarrou, G. Doukas, Fotios Gioulekas, “A Cybersecurity Culture Survey Targeting Healthcare Critical

Infrastructures," *Cybersecurity and the Digital Health: An Investigation on the State of the Art and the Position of the Actors,* vol. 10, no. 2, February 2022.

[74] K. Crawley, in *8 Steps to Better Security: A Simple Cyber Resilience Guide for Business,* 2022.

[75] R. Tarun, "Building a Culture of Security," in *Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders*, Wiley Data and Cybersecurity, 2022, pp. 29-41.

[76] C. Thakur, S. Palhad, Z. Mitrovic, "Towards Building Cybersecurity Culture in TVET Colleges in South Africa," in *IST-Africa Conference (IST-Africa)*, Tshwane, South Africa, 2023.

[77] B. Soewito, Semi Yulianto, "Ransomware Resilience: Investigating Organizational Security Culture and Its Impact on Cybersecurity Practices against Ransomware Threats," in *International Conference on Informatics Engineering, Science & Technology (INCITEST)*, October 2023.

[78] T. M. Kangapi, E. Chindenga, "Towards a Cybersecurity Culture Framework for Mobile Banking in South Africa," in *IST-Africa Conference (IST-Africa)*, Ireland, 2022.

[79] E. W, "Growing positive security cultures," 18 September 2017. [Online]. Available: https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures. [Accessed 20 April 2024].

[80] K. P. Keman Huang, "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture," in *Proceedings of the 52nd Hawaii International Conference on System Sciences* , Massachusetts Institute of Technology, Cambridge, MA, US, 2019.

[81] J. Eloff, A. DA Veiga, "An information security governance framework. Information Systems Mangement," *Information Security Management,* pp. 361-372, 10 December 2007.

[82] E. H. Schein, "Organizational Culture and Leadership," vol. 2, San Francisco, CA, John Wiley & Sons, 2010.

[83] *Mind and hand book. II(12). Hacking,* Cambridge, MA, US: Massachusetts Institute of Technology, 2023-2024.

[84] "MIT leaves behind a rich history in Tech Square," 17 March 2004. [Online]. Available: https://news.mit.edu/2004/techsquare-0317. [Accessed February 2024].

[85] S. Levy, "The Tech Model Railroad Club," 21 November 2014. [Online]. Available: https://www.wired.com/2014/11/the-tech-model-railroad-club/. [Accessed February 2024].

[86] J. A. McKenzie, "TX-O Computer History. The RESEARCH LABORATORY of ELECTRONICS at the MASSACHUSETTS INSTITUTE OF TECHNOLOGY," June 1999.

[87] B. Yagoda, "A Short History of "Hack"," 6 March 1014. [Online]. Available: https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack. [Accessed February 2014].

[88] MIT, “A brief history of MIT,” [Online]. Available: https://mitadmissions.org/discover/about-mit/a-brief-history-of-mit. [Accessed March 2024].

[89] K. R. Aimee Laycock, “The seven dimensions of security culture,” CLTRe, KnowBe4, 2019.

[90] G. R. VandenBos, *APA Dictionary of Psychology*, American Psychological Association., 2007.

[91] Y. Nikoloudakis, I. Kefaloukos, E. Pallis, E. K. Markakis, DIMITRA PAPATSAROUCHA*, *A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues,* Department of Electrical and Computer Engineering, Hellenic Mediterranean University, 2021.

[92] “TalTech,” Tallinn University of Technology, 2020. [Online]. Available: https://taltech.ee/en/. [Accessed February 2024].

[93] W. M. Vagias, *Likert-type scale response anchors.*, Clemson International Institute for Tourism & Research Development, Department of Parks, Recreation and Tourism Management. Clemson University, 2006.

[94] E. Peer, Serge Egelman, “Scaling the Security Wall. Developing a Security Behavior Intentions Scale (SeBIS),” in *CHI 2015*, April 2015.

[95] “Privacy Policy,” SurveyLegend, 01 May 2018. [Online]. Available: https://www.surveylegend.com/terms-and-privacy/privacy-policy/. [Accessed 3 March 2024].

[96] “A simple and powerful online survey tool,” SurveyPlanet, 2024. [Online]. Available: https://surveyplanet.com/.

[97] LimeSurvey, 2024. [Online]. Available: https://www.limesurvey.org/.

[98] “Online polls made simple,” PollForAll, 2024. [Online]. Available: https://www.pollforall.com/en.

[99] “Online form builder,” Forms.app, 2024. [Online]. Available: Forms.app.

[100] “Start creating responsive polls,” SurveyLegend, 2024. [Online]. Available: https://www.surveylegend.com/.

[101] “General Data Protection Regulation Compliance,” SurveyLegend, February 2018. [Online]. Available: https://www.surveylegend.com/gdpr-compliance/. [Accessed March 2024].

[102] “How to protect your data online by using a password manager,” Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/protecting-your-data-online-password-manager. [Accessed 1 April 2024].

[103] C. I. Nunn, B. J. White, S. L. Williams, M. D. Clark, Bader A. Alomary, “Teachers, Are They Really Needed?,” *Creative Education,* vol. 8, no. 13, October 2017.

[104] “Cyber Readiness For Teams,” RangeForce, [Online]. Available: https://www.rangeforce.com/?utm_source=google&utm_medium=paid-search&utm_campaign=branded&utm_term=rangeforce&utm_campaign=US+-+Branded+Search&utm_source=adwords&utm_medium=ppc&hsa_acc=9894833688&hsa_cam=15045445856&hsa_grp=126117123302&hsa_ad=55538971456. [Accessed March 2024].

[105] “A fun way to learn cyber security,” TryHackMe, [Online]. Available: https://tryhackme.com/. [Accessed March 2024].

[106] MBTI, “Build a foundation for personal and professional growth,” [Online]. Available: https://www.mbtionline.com/en-US. [Accessed March 2024].

[107] S. Flowerday, Edwin Donald Frauenstein, “Susceptibility to phishing on social network sites: A personality information processing model,” *Computers & Security*, vol. 94, July 2020.

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

I, Nadezda Semjonova

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Cybersecurity Culture in Academia: the case of Tallinn University of Technology”, supervised by Kaido Kikkas.
   1.1. 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;
   1.2. 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.

12.05.2024

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.

Appendix 2 – Available Literature

Paper ID	Author , Year	Research	D	PA	DL
P1	Alfawaz et al. (2010)	Information security culture: A behaviour compliance conceptual framework			L1
P2	Da Veiga and Eloff (2010)	A framework and assessment instrument for information security culture	x	x	L2
P3	Lacey (2010)	Understanding and transforming organizational security culture.		x	L3
P4	Lim et al. (2010)	Embedding information security culture emerging concerns and challenges			L4
P5	Sánchez et al. (2010)	Security Culture in Small and Medium-Size Enterprise			L5
P6	Van Niekerk and Von Solms (2010)	Information security culture: A management perspective			L6
P7	Batteau (2011)	Creating a culture of enterprise cybersecurity	x		L7
P8	Alnatheer et al. (2012)	Understanding and measuring information security culture in developing countries: case of Saudi Arabia		x	L8
P9	Hassan and Ismail (2012)	A conceptual model for investigating factors influencing information security culture in healthcare environment			L9
P10	Olivos (2012)	Creating a security culture development plan and a case study			L10
P11	Shahibi et al. (2012)	Determining factors influencing information security culture among ICT librarians		x	L11
P12	AlHogail and Mirza (2014a)	A proposal of an organizational information security culture framework.			L12

P13	AlHogail and Mirza (2014b)	A framework of information security culture change			L13
P14	Astakhova (2014)	The concept of the information-security culture	x		L14
P15	D'Arcy and Greene (2014)	Security culture and the employment relationship as drivers of employees' security compliance		x	L15
P16	Da Veiga and Martins (2014)	Information security culture: A comparative analysis of four assessments		x	L16
P17	Lopes and Oliveira (2014)	Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises		x	L17
P18	Reid et al. (2014)	From information security to cyber security cultures			L18
P19	Reid and Van Niekerk (2014)	Information security culture: A general living systems theory perspective			L19
P20	AlHogail (2015a)	Design and validation of information security culture framework		x	L20
P21	AlHogail (2015b)	Cultivating and assessing an organizational information security culture; an empirical study		x	L21
P22	Alnatheer (2015)	Information security culture critical success factors			L22
P23	AlKalbani et al. (2015)	Organisational security culture and information security compliance for e-government development: The moderating effect of social pressure			L23
P24	Da Veiga (2015)	The influence of information security policies on information security culture: Illustrated through a case study		x	L24
P25	Da Veiga and Martins (2015)	Improving the information security culture through monitoring and implementation actions illustrated through a case study		x	L25

P26	Greig et al. (2015)	An ethnographic study to assess the enactment of information security culture in a retail store		x	L26
P27	Lim et al. (2015)	Information security culture: Towards an instrument for assessing security management practices		x	L27
P28	Martins and Da Veiga (2015)	An Information security culture model validated with structural equation modelling		x	L28
P29	Sherif et al. (2015)	An Identification of Variables Influencing the Establishment of Information Security Culture			L29
P30	Da Veiga (2016a)	A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument	x	x	L30
P31	Da Veiga (2016b)	Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study		x	L31
P32	Hassan and Ismail (2016)	Information security culture in healthcare informatics: A preliminary investigation			L32
P33	Santos-Olmo et al. (2016)	The importance of the security culture in SMEs as regards the correct management of the security of their assets			L33
P34	Hayden (2016)	People-Centric Security: Transforming Your Enterprise Security Culture	x	x	L34
P35	Tang et al. (2016)	The impacts of organizational culture on information security culture: a case study		x	L35
P36	Da Veiga and Martins (2017)	Defining and identifying dominant information security cultures and subcultures		x	L36

P37	Gcaza et al. (2017)	A general morphological analysis: Delineating a cyber-security culture	x		L37
P38	Hassan et al. (2017)	Information security culture in health informatics environment: A qualitative approach.		x	L38 L38 b
P39	Masrek et al. (2017)	Information security culture for Malaysian public organization: a conceptual framework			L39
P40	Da Veiga (2018)	An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture		x	L40
P41	Masrek et al. (2018a)	Assessing the information security culture in a government context: The case of a developing country		x	L41
P42	Masrek et al. (2018b)	The development of an information security culture scale for the Malaysian Public organization		x	L42
P43	Mokwetli and Zuva (2018)	Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa		x	L43
P44	Nævestad et al. (2018)	Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security		x	L44
P45	Ioannou et al. (2019)	Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination	x	x	L45
P46	Marotta and Pearlson (2019)	A culture of cybersecurity at Banca Popolare di Sondrio	x		L46
P47	Nasir et al. (2019b)	A dimension-based information security culture model and its relationship with employees' security behaviour: A case study in Malaysian higher educational institutions		x	L47

P48	Nel and Drevin (2019)	Key elements of an information security culture in organisations		x	L48
P49	Patrascu (2019)	Promoting Cybersecurity Culture Through Education	x		L49
P50	Ruhwanya and Ophoff (2019)	Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania			L50
P51	Tolah et al. (2019)	A Comprehensive Framework for Understanding Security Culture in Organizations	x	x	L51
P52	Van't Wout (2019)	Develop and maintain a cybersecurity organisational culture	x	x	L52
P53	Alshaikh (2020)	Developing cybersecurity culture to influence employee behaviour: A practice perspective			L53
P54	Blythe et al. (2020)	Human cyber risk management by security awareness professionals: Carrots or sticks to drive behaviour change?		x	L54
P55	Da Veiga et al. (2020)	Defining organisational information security culture—Perspectives from academia and industry	x	x	L55
P56	Govender et al. (2020)	A Framework for the Assessment of Information Security Risk, the Reduction of Information Security Cost and the Sustainability of Information Security Culture			L56
P57	Nasir et al. (2020)	Information Security Culture for Guiding Employee's Security Behaviour: A Pilot Study		x	L57
P58	Schneider et al. (2020)	A Practical Guideline for Developing a Managerial Information Security Awareness Programme			L58
P59	Wiley et al. (2020)	More than the individual: Examining the relationship between culture and Information Security Awareness.		x	L59
P60	Georgiadou et al. (2020)	A Cyber-Security Culture Framework for Assessing Organization Readiness			L60
P61	Gioulekas et al. (2022)	A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures		x	L61

P62	Crawley (2022)	8 Steps to Better Security: A Simple Cyber Resilience Guide for Business			L62
P63	Tarun (2022)	Building a Culture of Security			L63
P64	Mitrovic et a. (2023)	Towards Building Cybersecurity Culture in TVET Colleges in South Africa			L64
P65	Yulianto et al. (2023)	Ransomware Resilience: Investigating Organizational Security Culture and Its Impact on Cybersecurity Practices against Ransomware Threats			L65
P66	Thembakazi et al. (2023)	Towards a Cybersecurity Culture Framework for Mobile Banking in South Africa			L66

Appendix 3 - Cybersecurity Culture Survey Questions in English

Answers 5-point Likert scale: Never (1), Rarely (2), Sometimes (3), Often (4), or Always (5)

Parameters to collect:

1. Current Academic Year (choose one)
2. Programme/Degree (choose one)
3. Estimated time spent online daily (1-2, 3-4, 5-6, 7-8, 9-10 hours)
4. Main device used for online activities (laptop, tablet, smartphone)
5. Age Group (24 or less, 25-30, 31 or more)
6. Do you currently have a job? (Yes, No)

Device Security

7. I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
8. When I step away from my computer, I either manually lock my computer screen or lock my room door.
9. I use a PIN or passcode to unlock my mobile phone.
10. I use biometrics (fingerprints or facial features) to access my mobile phone.

Password Security

11. I change passwords even when it's not required.
12. I change my passwords for my accounts (university, email, bank) even when not required)
13. I use different passwords for different accounts that I have.
14. When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.

Password Management

15. I use password manager to store passwords.
16. I write down my passwords on paper.
17. I write all my passwords to a file on the device.
18. I share my passwords with my family/classmates or friends.
19. I use Uni-ID or ÕIS User to access the university environment.

20. To access the university environment, I use an Estonian ID card, Mobile ID or Smart ID.

Proactive Awareness

21. When someone sends me a link, I open it without first verifying where it goes.
22. I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.
23. I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).
24. When browsing websites, I mouseover links to see where they go, before clicking them.
25. If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
26. I install unreliable software on my computer/phone.

Software Updates

27. When I'm prompted about a software update, I install it right away.
28. I try to make sure that the programmes I use are up-to-date.

Cyber Hygiene

29. I check and erase viruses and malicious software.
30. I use built-in antivirus (where applicable).
31. I delete suspicious e-mails without reading them.

Information Security Behaviour

32. I use security technologies to protect confidential information.
33. To ensure the safety of my files, I use automatic backups.

Cybersecurity Awareness within University

34. I, myself study various cybersecurity laws and regulations issued by the government.
35. I think my university places great importance on cybersecurity education.
36. My university carries out cybersecurity education activities.
37. I am satisfied with cybersecurity training and support provided by my university.
38. I am aware of the cybersecurity policies and procedures in place at my university.
39. The University informing us about our cybersecurity policies and procedures.
40. I reported a cybersecurity incident or concern to the university IT department.

Additional Questions

41. Where do you usually get information about cybersecurity best practices? [multiple choice allowed]

    Friends, Workplace, University, News, Social Media, Tech Websites and Blogs.

42. What additional resources or support would you like to see in terms of cybersecurity education? [Open-ended response]

Appendix 4 - Cybersecurity Culture Survey Questions in Estonian

Vastused 5-palline Likerti skaala: mitte kunagi (1), harva (2), mõnikord (3), sageli (4) või alati (5)

Kogutavad parameetrid:

1. Praegune õppeaasta (valige üks)
2. Programm/kraad (valige üks)
3. Hinnanguline iga päev võrgus veedetud aeg (1–2, 3–4, 5–6, 7–8, 9–10 tundi)
4. Peamine võrgutegevuseks kasutatav seade (sülearvuti, tahvelarvuti, nutitelefon)
5. Vanuserühm (24 või vähem, 25–30, 31 või rohkem)
6. Kas teil on praegu töökoht? (Jah ei)

Seadme turvalisus

7. Seadistan arvutiekraani automaatselt lukustama, kui ma seda pikema aja jooksul ei kasuta.
8. Kui ma arvuti juurest eemale astun, siis kas lukustan käsitsi arvutiekraani või lukustan oma toa ukse.
9. Kasutan mobiiltelefoni avamiseks PIN-koodi või pääsukoodi.
10. Kasutan oma mobiiltelefonile juurdepääsuks biomeetrilisi andmeid (sõrmejälgi või näojooni).

Parooli turvalisus

11. Muudan paroole isegi siis, kui seda ei nõuta.
12. Muudan oma kontode (ülikooli, e-posti, panga) paroole isegi siis, kui seda ei nõuta)
13. Kasutan erinevate kontode jaoks erinevaid paroole.
14. Uue veebikonto loomisel püüan kasutada parooli, mis ületab saidi miinimumnõudeid.

Paroolihaldus

15. Kasutan paroolide salvestamiseks paroolihaldurit.
16. Kirjutan oma paroolid paberile.
17. Kirjutan kõik oma paroolid seadmes olevasse faili.
18. Ma jagan oma paroole oma pere/klassikaaslaste või sõpradega.
19. Ülikooli keskkonda pääsemiseks kasutan Uni-ID või ÕIS Kasutajat.

20. Ülikooli keskkonda pääsemiseks kasutan Eesti ID-kaarti, Mobiil-ID-d või Smart ID-d.

Ennetav teadlikkus

21. Kui keegi saadab mulle lingi, avan selle ilma, et kontrolliksin, kuhu see läheb.

22. Ma tean, millist veebisaiti külastan, pigem selle välimuse ja tunde järgi, mitte URL-i riba vaadates.

23. Esitan teavet veebisaitidele, ilma et oleksin eelnevalt kontrollinud, kas see saadetakse turvaliselt (nt SSL, „https://", lukuikoon).

24. Veebisaitide sirvimisel liigutan enne nendel klõpsamist kursorit linkidel, et näha, kuhu need lähevad.

25. Kui avastan turvaprobleemi, jätkan seda, mida tegin, sest eeldan, et keegi teine parandab selle.

26. Installin oma arvutisse/telefoni ebausaldusväärset tarkvara.

Tarkvaravärskendused

27. Kui mul küsitakse tarkvaravärskenduse kohta, installin selle kohe.

28. Püüan jälgida, et kasutatavad programmid oleksid ajakohased.

Küberhügieen

29. Kontrollin ja kustutan viiruseid ja ründetarkvara.

30. Kasutan sisseehitatud viirusetõrjet (kui see on asjakohane).

31. Kustutan kahtlased e-kirjad neid lugemata.

Infoturbe käitumine

32. Kasutan konfidentsiaalse teabe kaitsmiseks turvatehnoloogiaid.

33. Failide ohutuse tagamiseks kasutan automaatseid varukoopiaid.

Küberturvalisuse teadlikkus ülikoolis

34. Mina ise uurin erinevaid valitsuse poolt välja antud küberturvalisuse seadusi ja määrusi.

35. Arvan, et minu ülikool omistab küberjulgeolekualasele haridusele suurt tähtsust.

36. Minu ülikool viib läbi küberjulgeolekualase koolituse tegevusi.

37. Olen rahul oma ülikooli pakutava küberturvalisuse koolituse ja toega.

38. Olen teadlik minu ülikoolis kehtivatest küberjulgeoleku põhimõtetest ja protseduuridest.

39. Ülikool teavitab meid meie küberturvalisuse põhimõtetest ja protseduuridest.

40. Teatasin ülikooli IT-osakonnale küberturvaintsidendist või -probleemist.

Lisaküsimused

41. Kust te tavaliselt saate teavet küberturvalisuse parimate tavade kohta? [lubatud valikvastustega]

Sõbrad, töökoht, ülikool, uudised, sotsiaalmeedia, tehnilised veebisaidid ja ajaveebid.

42. Milliseid täiendavaid ressursse või tuge sooviksite näha küberjulgeolekualase hariduse vallas? [Avatud vastus]

Appendix 5 - Undergraduate Programmes Curriculum in the School of Information Technologies

Hardware Development and Programming (180 ECTS, IACB17/24):

1 Semester	2 Semester
Mandatory subjects: Professional introduction IAS0001 Discrete Mathematics IAX0010 Programming I IAX0583 Side IEE1220 Introduction to Information Technology ITI0101	Mandatory subjects: Software project IAS1410 Computers IAX0043 Programming II IAX0584 Electronics IEE1010 Mathematical analysis I YMX0231
3 Semester	**4 Semester**
Mandatory subjects: Operating systems and their management ICA0001 Schematic engineering project IEE1030 Linear algebra YMX0242 Elective subjects: Academic communication in English HLI0070 Presentations, speeches and discussions in English HLI0080 English is the professional language HLI0091 Algorithms and data structures IAS0090 Automatic control of processes IAS0130 Robot control and software IAS0220 Signals and signal processing IEEE1210 Functions and functional transformations of a complex variable YMX0340	Mandatory subjects: Software engineering IAS0110 Foundations of natural sciences and sustainable development YFX0060 Elective subjects: Automatic control and system analysis IAS0020 Digital systems IAS0150 Basics of computer networks ICA0019 Schematic technique IEE1020 Measuring technique IEE1070 Communication technology IEE1120 Internet of Things MET0330 Higher mathematics II YMX0223 Mathematical analysis II YMX0233 Matlab and numerical methods YMX0262
5 Semester	**6 Semester**
Mandatory subjects: Computers and Systems Project IAS1420 Elective subjects:	Mandatory subjects: Computer Systems Project IXX1530 Basics of business TMJ0130

Philosophy HHF3080 Intellectual property HOE6056 Foundations of law HOX6061 Engineering ethics HPP0300 Basics of sard systems IAS0230 Advanced Computer Networks ICA0020 Sensory IEE1040 Industrial internship (internship) IXX0750 Teaching practice (internship) IXX0760 Modeling of physical processes YFX0050	Elective subjects: Design of digital systems IAX0600 Electromagnetic field engineering IEE1110 **Foundations of Cybersecurity ITI0216** Calculation methods YMX0050 Probability theory and mathematical statistics YMX0252

Informatics (180 ECTS, IAIB17/24)

1 Semester	2 Semester
Mandatory subjects: Basics of computer networks ICA0019 Introduction to Information Technology ITI0101 Basic programming course ITI0102 Professional introduction ITI0105 Discrete Mathematics ITI0401	Mandatory subjects: Operating systems and their management ICA0001 Robot programming ITI0201 A basic programming course ITI0202 Software development project ITI0301 Higher mathematics I YMX0221 Elective subjects: Special programming course ITI0214
3 Semester	**4 Semester**
Mandatory subjects: Computers IAX0043 6.0 Algorithms and data structures ITI0204 Fundamentals of artificial intelligence and machine learning ITI0210 Web application project ITI0302 Logic ITI0402	Mandatory subjects: Databases I ITI0206 **Foundations of Cybersecurity ITI0216** Data mining ITI0217 Probability theory and mathematical statistics YMX0030 Elective subjects: Teaching of expression and argumentation HHM1155 Machine learning applications ITI0219
5 Semester	**6 Semester**
Mandatory subjects:	Mandatory subjects:

Bachelor thesis seminar ITI0218 Foundations of natural sciences and sustainable development YFX0060 Elective subjects: Philosophy and logic HHF1011 Academic communication in English HLI0070 Rights, obligations and responsibilities of internet operators HOE7120 Engineering ethics HPP0300 Robot control and software IAS0220 Platform-specific mobile applications ICD0022 Databases II ITI0207 Logic programming ITI0211 Software development internship (internship) ITI0220 Study methodical work ITI0223 Custom software development project ITI0303 Start-up business TMJ0180 Operational analysis YMR0050	Basics of business TMJ0130 Elective subjects: User interfaces ITI0209 Functional programming ITI0212 Scattered systems ITI0215 Study methodical work ITI0224 Matlab and numerical modelling YMX0261

Business Information Technology (180 ECTS, IABB17/24)

1 Semester	2 Semester
Mandatory subjects: Discrete Mathematics IAX0010 Information Systems Development I: Basic Skills ITB2201 Introduction to the profession and professional self-development ITB2401 Elective subjects: Basics of business TMJ0140	Mandatory subjects: Data processing IDK1615 Information Systems Development II: Development Techniques and Web Applications ITB2202 Processes in the economic environment TET0150 Linear algebra YMX0241

Start-up business TMJ0190	
3 Semester	**4 Semester**
Mandatory subjects: Software architecture and design IDU1550 Information Systems Development III: Distributed Applications ITB2203 Elective subjects: English is the professional language HLI0091 Legal education for IT managers HOE7051 Economic mathematics I TEM0240 Personal finance TER0520 Mathematical analysis I YMX0231	Mandatory subjects: Information Systems Development IV: Business Applications ITB2204 Databases I ITI0206 Basics of financial accounting TAF0070 Elective subjects: Economic mathematics II TEM0250 Probability theory and mathematical statistics YMX0030
5 Semester	**6 Semester**
Mandatory subjects: **Fundamentals of information and cyber security ITB1711** Algorithms and data structures ITI0204 Basics of finance TER0440 Elective subjects: Automatic testing ICD0004 Hybrid mobile applications ICD0018 Design of user interfaces and applications ICM0009 Professional practice (internship) ITB1705 Information Systems Development Team Project: Order ITB1706 Business modelling ITB8813 Databases II ITI0207 Physics for non-physicists NSO0160 Environmental protection and sustainable development YTG0060	Mandatory subjects: Fundamentals of IT management and maintenance ITB1708 Elective subjects: Organization and management HHM1152 Introduction to Cloud Technologies ICA0017 User interfaces ITI0209 Fundamentals of artificial intelligence and machine learning ITI0210 Financial modelling TER0570 Project management TMK2080 Foundations of natural sciences and sustainable development YFX0060

Administration of IT systems (180 ECTS, IAAB17/24)

1 Semester	**2 Semester**
Mandatory subjects:	Mandatory subjects:

Discrete Mathematics IAX0010 Introduction to Information Technology and Hardware ICA0012 Basics of computer networks ICA0019 Introduction to Information Technology ITI0101 Basic programming course ITI0102	Operating systems and their management ICA0001 Linux administration ICA0007 Higher mathematics ICY0030 Business basics and business communication ICY0031 Elective subjects: Ethical, social and professional aspects of IT ICY0004 Business English for IT professionals MLI0008
3 Semester	**4 Semester**
Mandatory subjects: IT infrastructure services ICA0002 **Data security and cryptology ICA0003** Basics of database systems ICA0005 Windows administration ICA0009 Web technologies ICD0007 Elective subjects: Advanced Computer Networks ICA0020 English for IT professionals MLI0007	Mandatory subjects: Support and organization of IT systems in the company ICA0004 Data storage technologies ICA0006 Introduction to Cloud Technologies ICA0017 Scripting languages ICA0021 Elective subjects: **Security of computer networks ICA0015** Advanced Routing ICA0018 Fundamentals of software testing ICD0012 Java ICD0019 Advanced Python ICS0019 Fundamentals of IT management and maintenance ITB1708
5 Semester	**6 Semester**
Mandatory subjects: Oracle: programming languages SQL and PL/SQL ICA0016 Logging and system monitoring ICS0020 Physics for non-physicists NSO0160 Environmental protection and sustainable development YTG0060 Elective subjects: Basics of wireless communication ICA0008	Mandatory subjects: Internship (internship) ICY0017

Container technologies and container orchestration ICA0022 Automatic testing ICD0004 Web applications based on Java ICD0011 Microservices and Container Architecture ICM0014 Basics of research ICY0016	

IT Systems Development (180 ECTS, IADB17/24)

1 Semester	**2 Semester**
Mandatory subjects: Discrete Mathematics IAX0010 Ethical, social and professional aspects of IT ICY0004 Environmental impact and sustainable development ICY0010 Introduction to Information Technology ITI0101 Basic programming course ITI0102 Physics for non-physicists NSO0160 Elective subjects: Economics ICY0019 English for IT professionals MLI0007	Mandatory subjects: Computers IAX0043 Operating systems and their management ICA0001 Basics of computer networks ICA0019 Java ICD0019 Higher mathematics ICY0030 Elective subjects: Advanced Python ICS0019 Logic ICY0025
3 Semester	**4 Semester**
Mandatory subjects: Basics of database systems ICA0005 Algorithms and data structures ICD0001 Web technologies ICD0007 Programming in C# ICD0008 Probability theory and mathematical statistics ICY0006 Elective subjects: **Data security and cryptology ICA0003**	Mandatory subjects: Oracle: programming languages SQL and PL/SQL ICA0016 JavaScript ICD0006 Software engineering ICD0013 Business basics and business communication ICY0031 Elective subjects: Fundamentals of software testing ICD0012 ASP.NET Web Applications ICD0015

Platform-specific mobile applications ICD0022 Microcontroller programming based on Python ICD0023 Philosophy ICY0021 Sets, relations, systems ICY0024	Web applications based on C# ICD0024 Information systems projects and their management ICY0009 Machine learning applications ITI0219
5 Semester	**6 Semester**
Elective subjects: Usability of IT systems ICD0003 Automatic testing ICD0004 Web applications based on Java ICD0011 Hybrid mobile applications ICD0018 Web management environments ICD0020 Development of distributed systems ICD0025 Advanced JavaScript ICD0026	Mandatory subjects: Internship (internship) ICY0017

Cyber Security Engineering (180 ECTS, IVSB17/24)

1 Semester	**2 Semester**
Mandatory subjects: Basics of computer networks ICA0019 Introduction to computer science and computer hardware ICS0001 **Introduction to Cyber Security ICS0002** Basics of programming ICS0004 Social, Professional and Ethical Aspects of IT ICS0006	Mandatory subjects: Electronics methods in information technology ICS0007 Web technologies ICS0008 Basics of research ICS0029 Logic and discrete mathematics ICY0001 Verbal and written communication MLI0003 Elective subjects: Java technologies ICS0014 Python for beginners ICS0015 **Information security risk management ICS0035** Estonian language and culture MLE0010
3 Semester	**4 Semester**
Mandatory subjects: Basics of database systems ICS0012 Linux administration ICS0021	Mandatory subjects: Windows administration ICA0009 **Security of computer networks ICA0015**

Elective subjects: Advanced Computer Networks ICA0020 Programming in C# ICS0010 Probability theory and mathematical statistics ICS0011 Basics of C/C++ ICS0017 **Cryptography ICS0026** Basics of business TMJ0130	**Cyber security management and governance ICS0009** **Social Engineering ICS0018** Elective subjects: Advanced Routing ICA0018 Algorithms and data structures ICS0005 Advanced Python ICS0019 C/C++ for advanced students ICS0025 Functional programming ITI0212
5 Semester	**6 Semester**
Mandatory subjects: IT infrastructure services ICA0002 Logging and system monitoring ICS0020 **Secure programming ICS0022** **Malware ICS0028** Elective subjects: Automatic testing ICS0024 **Web Application Security ICS0027** Machine learning ICS0030 **Computer forensics ICS0033** Statistical and interdisciplinary physics YFX0120	Mandatory subjects: Internship (internship) ICY0017