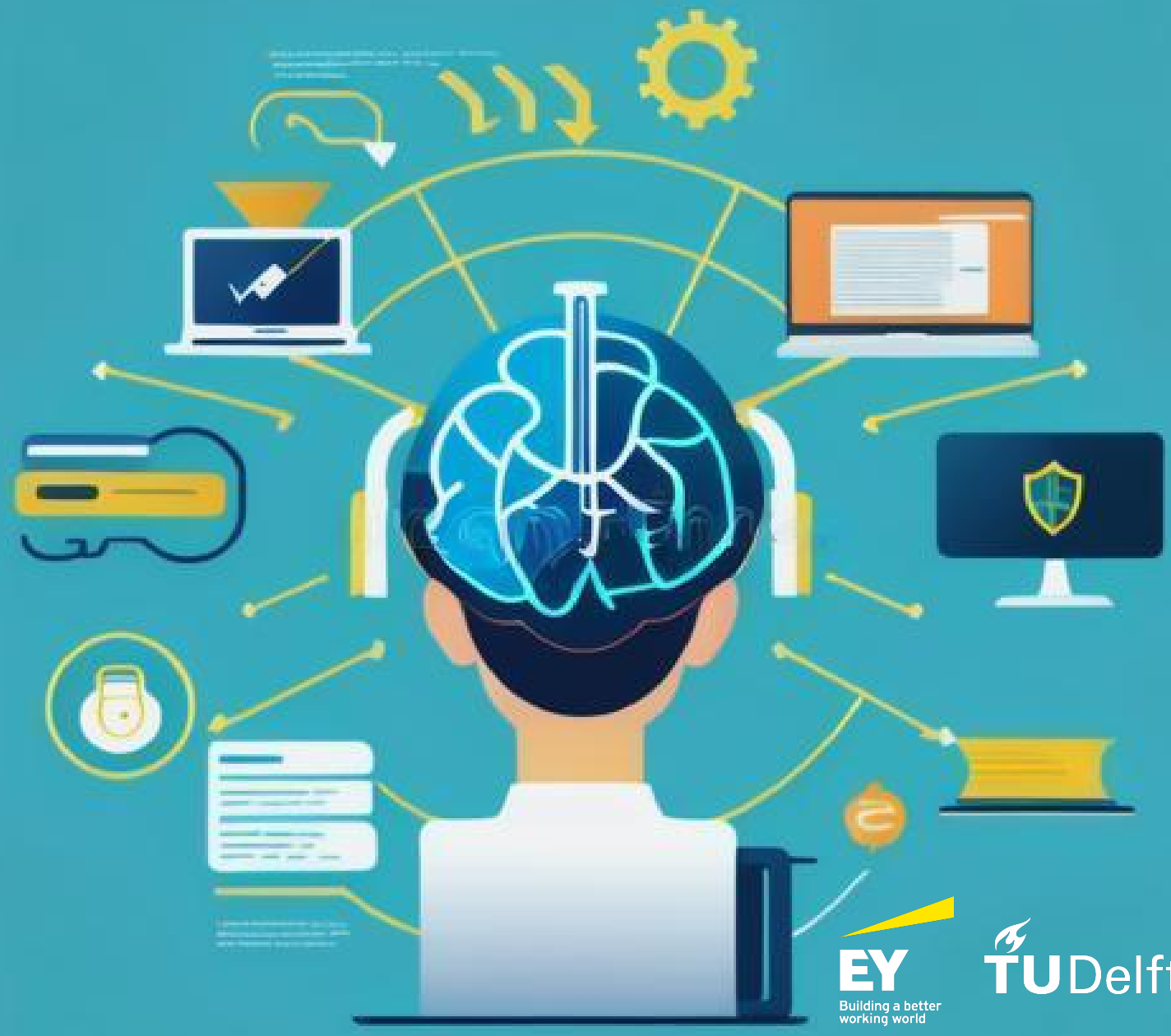
The Cyber Shield: Uniting Forces for Knowledge Security in Universities

A Comprehensive Investigation into the Path to Fortifying Knowledge Protection in Dutch Universities

J.S.Bissumbhar



EY Building a better working world

TU Delft

The Cyber Shield: Uniting Forces for Knowledge Security in Universities

A Comprehensive Investigation into the Path to Fortifying Knowledge Protection in Dutch Universities

By

J.S. Bissumbhar

in partial fulfilment of the requirements for the degree of

Master of Science
in Engineering and Policy Analysis

at the Delft University of Technology,
to be defended publicly on Monday October 30, 2023, at 11:00 AM.

Supervisor:	Prof. dr. ir. P.H.A.J.M. van Gelder	TU Delft
Thesis committee:	Dr. J.M. Duran	TU Delft
	Dr. S. Parkin	TU Delft
	M. Gijzen	Ernst & Young
	D. Rutten	Ernst & Young

TU Delft

Preface

It is with great pleasure and a sense of accomplishment that I present this master's thesis for the Master's degree of Engineering and Policy Analysis at the Delft University of Technology. This research delves into the factors influencing universities in implementing cybersecurity standards/measures within their policies to ensure knowledge security. The ultimate aim is to alleviate these barriers by introducing essential cybersecurity measures to mitigate and prevent cyber threats.

I would like to express my sincere gratitude to my thesis committee, composed of my three supervisors from the university, Mr. van Gelder, Mr. Parkin, and Mr. Duran. Their guidance, expertise, and support have been instrumental in shaping this research. I am also deeply appreciative of my mentors from Ernst & Young, Maik Gijzen and Daan Rutten, who provided insights and practical guidance during my internship. Finally, I would like to extend my heartfelt thanks to my family and friends for their unwavering encouragement, understanding, and support throughout this academic journey.

It is my hope that this research contributes to the advancement of knowledge security in universities and inspires further dialogue and action within the academic community and beyond. May this thesis serve as a catalyst for change, fostering a culture of cybersecurity and ensuring the resilience of our educational institutions.

Josephine S. Bissumbhar
Delft, October 2023

Contents

Abstract

In a rapidly evolving digital landscape, where information is the currency of progress, universities play a vital role in fostering innovation, research, and knowledge dissemination. However, this invaluable role also exposes universities to significant cybersecurity challenges. Cybersecurity is an increasingly important topic for organisations in all sectors, including universities. As repositories of valuable research data and other sensitive information, universities are attractive targets for cyber attacks.

Addressing these challenges is crucial not only to protect intellectual property and sensitive data but also to maintain the trust and integrity of academic institutions. Despite the importance of cybersecurity for universities, there is a lack of research on how to effectively implement cybersecurity policies and practices in this context. The lack of a standardised approach to cybersecurity can leave universities vulnerable to cyber threats and hinder the sharing of best practices. This study is expected to identify key challenges and measures for cybersecurity policy in Dutch universities. It will provide insights into the implementation of effective cybersecurity policies and contribute to the development of an approach to cybersecurity in the higher education sector. The research question is: *"How should the cybersecurity policies of Dutch universities be designed to mitigate cyber threats to ensure knowledge security?".*

To accomplish this research, a multidimensional approach was adopted. Extensive literature review provided a foundation for understanding cybersecurity standards and cyber ethics, while interviews were conducted with various Dutch universities to gain insights into their experiences and perspectives. Additionally, a comprehensive survey was administered to students and staff members of Dutch universities, enriching the study with diverse viewpoints. This work aligns with the objective of examining the quality of decision-making concerning grand societal challenges within the context of their socio-economic and political environments. It aspires to inform decision-makers in the public (policy) domain or at the intersection of the public and private spheres. By shedding light on the barriers faced by universities in implementing cybersecurity norms, this research aims to contribute to the ongoing discourse on securing knowledge assets in the face of emerging cyber threats. The thesis is structured as follows: it begins with an introduction that provides a comprehensive overview of the topic, delineating the problem at hand and outlining the proposed approach. Subsequently, the literature review section presents the findings of the extensive research conducted, exploring various subjects such as cybersecurity standards and cyber ethics, among others. The expected outcomes of this study are an overview of current cybersecurity challenges for Dutch universities, an understanding of the opinions and experiences of university staff and students, and recommendations for developing and implementing cybersecurity policies for Dutch universities.

Nomenclature

ATPs	Advanced Persistent Threats
CSAN	Cyber Security Assessment Netherlands
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
GDPR	General Data Protection Regulation
HRA	Higher Education and Scientific Research Act
IP	Intellectual Property
IoT	Internet of Things
ISMS	Information Security Management System
NSCS	National Cyber Security Centre
NIST	National Institute of Standards and Technology
SDR	Socially Desirable Responding
TU	Technical University
UNL	Universities of the Netherlands

Introduction

In recent years, there has been a marked increase in cyber attacks targeting universities globally, driven by the allure of obtaining valuable intellectual property, groundbreaking research data, and personal information. The UK's National Cyber Security Centre (NCSC) has identified the education sector, notably universities and research institutions, as principal targets for cybercriminals (National Cyber Security Centre, 2021). Given the rapidly evolving nature of these threats, academic institutions are in a race not just to safeguard their technical infrastructure but also to protect their invaluable knowledge assets. Despite their diligent efforts, the complex intricacies of these cyber challenges have raised pertinent questions: Are current defensive measures sufficient, or is there a need for specialized support and resilience measures to further fortify academic realms?

Maastricht University's experience in 2019 serves as a sobering example. They fell victim to a ransomware attack in which hackers encrypted the university's computer systems and demanded a ransom to make the data accessible again. The university ended up paying €197,000 to the hackers to recover the files (Digitale Overheid, 2020). Following suit in 2020, the University of Amsterdam was subjected to a DDoS attack, crippling essential online services for several days (NOS, 2021).

Dutch universities, renowned for their avant-garde research and innovation, are not impervious to the escalating cybersecurity challenges. Such incidents accentuate the vulnerability even of top-tier institutions, suggesting that amidst the burgeoning complexity of cyber threats, these institutions might necessitate specialized support or resilience measures. Numerous factors obstruct the seamless integration of essential safeguards into their policy framework. Addressing these impediments is crucial to stave off cyber threats and bolster knowledge security within the academic sphere. The European Union Agency For Cybersecurity (2021) underscores the burgeoning recognition of the imperative for robust cybersecurity policies. A more holistic, systematic approach is indispensable to ensure the availability, integrity, and confidentiality of information. Universities are urged to espouse a multi-faceted approach to cybersecurity, encompassing technical, organisational, and human dimensions (Kraemer et al., 2009).

In today's ever-evolving digital landscape, there is a heightened risk associated with knowledge security. Iv-Ho (2022) delineates knowledge security as an expansive concept that goes beyond mere technical defenses. It encompasses the overarching safeguarding of an institution's intellectual property, which includes its scientific knowledge, research outcomes, and innovations. With the steady increase in sensitive and valuable digital information that universities develop, utilize, and store, the associated risks become more pronounced. These risks not only pose threats to day-to-day operations but also jeopardize the achievement of strategic goals. The primary objective of ensuring knowledge security is to prevent pivotal technology and nationally strategic knowledge from falling into precarious hands. Recognizing this, one of the cardinal duties of the Dutch government is to fortify national security, as stated by the Ministerie van Onderwijs, Cultuur en Wetenschap (2022). To this end, additional funds have been earmarked by the government to bolster knowledge security within universities, as reported by Ad Valvas (2022).

The multifaceted nature of a university's IT infrastructure, coupled with varying degrees of cyber threat awareness among its users and the ever-evolving cyber threats, creates a nuanced and complex cybersecurity landscape. Reinforcing this sentiment, Dijkgraaf, the Minister of Education, Culture, and Science, underscored the imperative of recruiting the right talent and fostering expertise as pivotal areas requiring investment (Ad Valvas, 2022).

World-class higher education and science cannot exist without international cooperation and scientific talent from around the world (Nationale Leidraad Kennisveiligheid, 2022). The basic principle is therefore "open where possible, protect where necessary". Academic freedom and scientific integrity are core values that form the foundation of science in the Netherlands. Open science within Europe is the norm. The cybersecurity of universities is a crucial component in ensuring the security of academic research, which is necessary for addressing global grand challenges such as climate change, health, and food security. Protecting research data and other sensitive information from cyber attacks is essential to maintaining the integrity of scientific research, which is a key driver of global progress. Laws and regulations address the threats (SURF, 2021). However, ethical dilemmas arise when cooperating countries do not respect applicable fundamental rights and regulations (Nationale leidraad kennisveiligheid, 2022).

To uphold the reputation and confidentiality of the university, it's pivotal to recognize the current vulnerabilities in IT management systems, as highlighted by assessments like those by Iv-Ho (2022) and AIVD & MIVD (2017). These systems, as they stand, fall short in offering adequate resistance to advanced cyber threats. Addressing this, government parties, including Bakker (2022), advocate for a systematic and comprehensive risk analysis conducted by impartial external audit firms. Such a thorough approach ensures the identification of risks from both expected and "unexpected" angles. In pursuit of enhanced security and fostering a culture of security consciousness, the Universities of the Netherlands (UNL) is poised to collaborate with external experts. Ultimately, the synergy between administrators, policymakers, managers, and cybersecurity professionals will dictate the success and effectiveness of the selected security strategy (AIVD, 2021).

Grounded in this context, the pivotal research question is formulated:
"How should the cybersecurity policies of Dutch universities be designed to mitigate cyber threats to ensure knowledge security?"
The primary objective of this study is to dissect the factors that influence the effective implementation of Cyber Security standards within Dutch universities. By delving into the root causes of these challenges, this research seeks to provide actionable insights and recommendations. Policymakers and Cyber Security experts can then utilize these findings to craft guidelines and interventions tailored to promote the adoption of best practices across academic institutions.

The subsequent section delves into a synthesis of the literature review, encapsulating discussions on the myriad of cyber threats, frameworks, prevailing laws and regulations, and the cyber ethics embedded within policy analysis. Insights garnered from interviews with Cyber Security professionals, as well as survey responses from university affiliates, will be unpacked to accentuate their comprehension and viewpoints on Cyber Security practices in

academic settings. This investigation culminates in formulating policy recommendations tailored to fortifying the cybersecurity landscape and safeguarding knowledge within universities.

Theoretical Framework

To answer the main research question, the following sub-questions will be considered:

1. What cybersecurity standards apply to Dutch universities and how is this reflected in current cybersecurity policies?
2. What factors stimulate or prevent universities from implementing Cyber Security standards and measures?
3. What legal and ethical issues play a role in drafting and implementing cybersecurity policy for Dutch universities?
4. What experiences and opinions do employees at Dutch universities have with regard to safeguarding knowledge security?

The ultimate aim of this theoretical odyssey is to shed light on how we can leverage theory to fortify the cybersecurity resilience of universities against an array of ever-escalating threats.

Cyber threats

Given the nature of the cyber threat landscape, it has become increasingly important for these institutions to adopt and enforce robust cybersecurity standards (Von Solms & Van Niekerk, 2013). The Netherlands is renowned for its high level of internet connectivity and advanced digital infrastructure, which, while beneficial, also places Dutch institutions, including universities, at risk of cyber threats (Van der Meulen, 2016). The greatest fear when it comes to knowledge and information security arises from cyber threats. Defined as malicious activities aimed at exploiting weaknesses in information systems, networks, and technologies, cyber threats put institutions like universities in jeopardy, causing financial harm and damaging their reputation. The risks that these knowledge institutions face have the potential to breach the integrity, confidentiality, and availability of their systems and data. Cyber threats can adopt various forms, including but not limited to phishing attacks to advanced persistent threats (APTs), malware, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, ransomware, and threats related to Internet of Things (IoT) devices. All of which can profoundly impact knowledge and information security, leading to data breaches, reputational damage, financial loss, and other adversities.

Phishing attacks

Phishing attacks aim to trick users into revealing sensitive information, often under the guise of a trustworthy entity. Universities are particularly susceptible to phishing attacks due to their diverse user base, with varying levels of cyber threat awareness. Attackers often impersonate university administrators, fellow students, or trusted external organisations, seeking to obtain login credentials or other sensitive data from unsuspecting students and staff (Hadnagy & Fincher, 2015). These attacks exploit human error, making them a preferred method for cybercriminals (Heartfield & Loukas, 2018). The diverse user base in universities, consisting of students, faculty, and staff, can significantly increase the potential for successful phishing attempts (Jagatic, Johnson, Jakobsson, & Menczer, 2007). This emphasizes the importance of user awareness and education as a primary defence line against such attacks (Kumaraguru et al., 2007). Solutions like multi-factor authentication and artificial intelligence-based phishing detection systems could substantially decrease the impact of phishing attempts within the university environment (Burnett & Feamster, 2019).

Advanced Persistent Threats (ATPs)

APTs are a category of cyber threats wherein unauthorised users gain access to a network and remain undetected for an extended period. APT actors focus on establishing a long-term presence in their targets' systems to steal sensitive information (Tankard, 2011). Universities are attractive targets for APTs due to the valuable intellectual property they house. Tankard's (2011) paper discusses APTs as long-term intrusions into network systems designed to steal sensitive information. Machine learning and artificial intelligence can be leveraged to improve intrusion detection systems and mitigate the impact of APTs.

Malware

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. Various forms of malware, such as viruses, worms, and trojans, pose substantial threats to universities. These malicious programs can disrupt operations, damage systems, and lead to data loss (Kaspersky Lab, 2017).

DoS and DDoS attacks

DoS attacks aim to make a system, service, or network unavailable to its intended users. In a DDoS attack, the assault comes from multiple sources, making it difficult to counter (Yu et al., 2014). Universities, reliant on their networks for teaching, research, and administrative purposes, can suffer significant disruption from such attacks. Yu et al. (2014) discuss the considerable disruption that DoS and DDoS attacks can cause, given universities' reliance on their networks. The authors suggest that cloud-based solutions can provide universities with robust and flexible defences against these attacks.

Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or data until a sum of money (ransom) is paid. Given the valuable data that universities hold and their reliance on digital systems, they are prime targets for such attacks (Cimpanu, 2019). Cimpanu's (2019) piece rightly asserts that universities are prime targets for ransomware attacks due to the valuable data they hold and their reliance on digital systems. The author suggests preventative measures and contingency plans, such as regular system backups and ransomware-specific response protocols. However, the article falls short in discussing the psychological and social engineering aspects of ransomware attacks, which often involve manipulating users into opening malicious emails or files.

IoT-related threats

With increasing numbers of IoT devices used in universities, new cyber threats have emerged. These devices, often with insufficient security measures, can provide attackers with easy entry points to gain access to university networks (Roman et al., 2018).

Cybersecurity Frameworks

In an era where cyber threats are a constant concern, Dutch universities have turned to national and international cybersecurity standards to fortify their defence systems.

Several cybersecurity frameworks are available for organisations to design and implement security strategies, assisting them in better management of security risks, and enhancing their overall security. However, these frameworks do not escape criticism due to their inflexibility and limited focus on human aspects of cybersecurity. It's essential to acknowledge that no framework is flawless, and organisations should select a framework that best aligns with their specific needs and objectives.

The cybersecurity measures adopted by Dutch universities largely follow the guidelines set out by the National Cyber Security Centre (NCSC). The NCSC, under the purview of the Ministry of Justice and Security, plays a key role in setting the national cybersecurity guidelines (Gootjes, Van De Weerd, & Tellegen, 2016). Dutch

universities are encouraged to follow the NCSC's guidelines, which include a focus on risk management, the development of secure IT infrastructures, and the enforcement of stringent access controls (Verhoeven, 2019). The NCSC also provides guidelines on the reporting of cybersecurity incidents to facilitate nationwide tracking and response (NCSC, 2017).

In addition to the NCSC guidelines, Dutch universities often refer to international cybersecurity standards such as the NIST Cybersecurity Framework and the ISO/IEC 27001.

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST) in the United States, provides organisations with a structured methodology to manage security risks. The framework encompasses five core functions: identify, protect, detect, respond, and recover (National Institute of Standards and Technology, 2014). While the focus remains on improving the security of critical infrastructure, its applications can extend to other organisations as well. ISO 27001, an international standard for information security, outlines a structured approach to manage information security risks. The framework is widely applicable and can be used in different types of organisations, irrespective of size or sector. The ISO/IEC 27001 is a globally recognized standard that provides guidelines for the establishment, implementation, and maintenance of an information security management system (ISMS). CIS Controls, developed by the Center for Internet Security, includes a structured approach to security risk management. The framework is based on a list of 20 best practices that organisations can use to enhance their security.

The implementation of these standards is evident in the cybersecurity policies of Dutch universities. For instance, many universities have adopted risk management approaches to cybersecurity, as advised by the NCSC, the ISO/IEC 27001, and the NIST Framework (Verhoeven, 2019). Universities have also enforced more rigorous access controls, aligning with the NCSC's guidelines.

The organisation SURF, a collaborative information and communication technology (ICT) platform for Dutch higher education and research institutions, has emerged as a vital influencer within the realm of cybersecurity in the Netherlands. It extends beyond just providing a cooperative framework for ICT facilities; SURF is instrumental in defining and setting the cybersecurity maturity levels for universities and other higher educational institutions.

Establishing a cybersecurity maturity level provides a clear, structured, and measurable approach to understanding an organisation's current cybersecurity status and offers a pathway for future improvements. The SURF's maturity model evaluates universities on numerous aspects including policy, technology, human aspects, and governance, thereby providing a comprehensive overview of the institution's cybersecurity posture (SURF, 2020). For Dutch universities, adhering to the SURF cybersecurity maturity model holds significant importance. Firstly, it aids in identifying strengths and weaknesses in their cybersecurity policies and practices, enabling targeted efforts to address identified vulnerabilities. Secondly, it promotes an awareness culture among all stakeholders (students, faculty, and administration), underscoring the collaborative role everyone plays in cybersecurity. Additionally, it supports compliance with various cybersecurity laws and regulations, including GDPR and the Higher Education and Scientific Research Act, as the model includes measures related to data protection and privacy. Furthermore, a study by Van Brakel & Chis (2018) revealed that there is a direct correlation between the maturity level of an institution's cybersecurity framework and its overall reputation. Thus, aligning with SURF's maturity model also benefits universities in terms of enhancing their reputation, fostering trust among students, staff, and collaborators, and potentially attracting more funding and partnerships. Moreover, the continuous evolution of the model ensures that it keeps

pace with the dynamic nature of cyber threats, thereby providing Dutch universities with a robust, relevant, and up-to-date framework to navigate their cybersecurity journeys. In essence, the SURF maturity model provides a vital tool for Dutch universities to ensure they are equipped to manage and mitigate the cybersecurity risks they face in an increasingly digitised educational landscape.

Laws and regulations

When implementing cybersecurity measures, Dutch universities grapple not only with technical challenges, but also with complex legal and ethical considerations. These issues can influence the scope, design, and execution of cybersecurity policies (Kabay, 2010).

Laws and regulations are of paramount importance in safeguarding knowledge and information security. Governments have implemented various laws and regulations aimed at the protection of critical infrastructure, personal data, and intellectual property. Dutch universities operate under a legal framework defined by both Dutch and European Union (EU) legislation.

The General Data Protection Regulation (GDPR), implemented by the EU, has wide-ranging implications for data protection and cybersecurity. Introduced in 2018, the GDPR is a revolutionary privacy law implemented by the European Union, focusing on protecting and empowering all EU citizens' data privacy. The GDPR emphasises consent, transparency, and accountability. It obliges universities to process personal data securely, disclose the reason behind data collection, and restrict its usage to those purposes only. Breaching these regulations can result in severe financial penalties. The GDPR has profoundly impacted how organisations manage data, prompting the need for significant changes to information systems, processes, and policies (Greenleaf, 2018). Universities, as processors of vast amounts of personal data, must ensure that their cybersecurity measures comply with GDPR requirements, including those pertaining to data breach notification, data subjects' rights, and data minimisation principles (Voigt & Von dem Bussche, 2017).

Moreover, Dutch law mandates that cybersecurity measures should not infringe upon the rights of individuals. This means that universities must strike a balance between ensuring network security and respecting the privacy rights of students, staff, and researchers (Van der Meulen, 2016).

In the Netherlands, universities must comply with an array of laws and regulations related to cybersecurity policies.

- Higher Education and Scientific Research Act (HRA):

The Dutch HRA stipulates that universities have an obligation to maintain an adequate level of information security and privacy protection. It emphasises the importance of having well-structured security and privacy policies detailing the measures universities take to secure data. As with the GDPR, compliance with the HRA is crucial to prevent financial penalties and reputational damage (De Hert & Papakonstantinou, 2016).

- Cyber Security Assessment Netherlands (CSAN):

The CSAN is an annual report issued by the Dutch National Cyber Security Center (NCSC) that provides insights into cybersecurity threats and developments. Universities are encouraged to use this document as a guideline to improve their cybersecurity practices. Despite not being a mandatory requirement, the CSAN provides valuable information for improving cybersecurity resilience and response (National Cyber Security Centre, 2019).

- Government Information Security Baseline:

The Government Information Security Baseline outlines the measures Dutch municipalities should take to secure their data. Although initially developed for municipalities, it also serves as a valuable guideline for universities to develop their own security policies. The baseline ensures that organisations adhere to the same standard of data protection, thereby enabling a uniform

approach to information security across the country (Van den Berg & Van den Hoven, 2013).

- Network and Information Systems Security Act:

Introduced by the Dutch government in 2018, the Network and Information Systems Security Act aims to enhance the security of network and information systems across the country. The law requires vital providers, including universities, to implement appropriate measures ensuring their network and information systems' continuity and reporting any cybersecurity incidents to the government. The law contributes to a more resilient and secure digital society by increasing the responsibility of critical organisations in managing cyber threats (Dutch Ministry of Justice and Security, 2018).

These regulations' implementation and compliance can significantly vary based on each university's organisational structure, culture, and resources. Furthermore, as the cybersecurity landscape is continually evolving, these regulations should not be considered as a final destination but rather an ongoing journey towards achieving information security resilience (Shackelford et al., 2019).

Building upon these pivotal observations, we understand that the quest for cybersecurity in the higher education sector is far from static. The digital ethics – a field concerning the study of how we should act in the digital realm and the kind of people we should become (Tavani, 2013) – a vital aspect of this journey. As we pivot from a focus on adherence to cybersecurity regulations and standards, we now turn our attention towards the role of ethics in cybersecurity, highlighting its indispensable role in framing responsible behaviour in the digital world, particularly within the context of higher education.

Cyberethics

Ethics play a pivotal role in policymaking, requiring policymakers to consider the ethical and moral implications of their policy choices, and the potential impact of their decisions on individuals and society at large. Policymakers should align with ethical principles such as justice, autonomy, non-injury, and confidentiality.

Research studies have indicated that ethical considerations in policy making lead to better decision-making and reduced probability of unwanted consequences. For instance, a study by Hillman and Wollman (2016) showcased that the application of ethical principles in policy making can contribute to developing more inclusive policies and curtailing social inequality. A similar study by Hudson and McLean (2021) concluded that the incorporation of ethical principles in policy making can enhance the safety and security of citizens.

Policymaking and risk analysis are vital elements of cybersecurity governance. Policymakers must contemplate the ethical implications of cybersecurity policy decisions, ensuring that such policies do not infringe upon individual rights, including privacy and freedom of expression. Risk analysis aids policymakers in identifying potential threats and vulnerabilities, enabling the formulation of effective risk mitigation strategies.

Ethical considerations in cybersecurity revolve around questions of privacy, freedom of information, and the boundaries of defensive measures. Universities must grapple with how to protect their systems and data while still maintaining their commitment to openness and the free exchange of ideas (Kabay, 2010). Another ethical question arises in the context of "active defence" measures or "hacking back". While such actions might be effective in deterring attackers, they raise important ethical concerns and can potentially lead to legal repercussions (Rowe, 2010). Policymakers must consider the ethical and moral implications of their policy choices, and be aware of the potential impact of their decisions on individuals and society as a whole. It is therefore important for policymakers to be guided by ethical principles such as justice, autonomy, non-injury, and confidentiality. Justice means

that policies should be fair and equal to all parties involved and that the interests of all affected parties are weighed when making decisions. Autonomy means that people should be free to make their own choices and that their personal freedom and dignity should be respected. Non-harm means that policies should not cause harm to individuals or society as a whole. Confidentiality means that personal data and privacy are protected and that there is transparency about the processing of personal data.

Scientific studies have shown that policymakers who are guided by ethical principles make better decisions and that there is less chance of unwanted side effects. For example, a study by Hillman and Wollman (2016) showed that applying ethical principles in policy making can help develop more inclusive policies and reduce social inequality. Another study by Hudson and McLean (2021) concluded that applying ethical principles in policy making can help improve the safety and security of citizens.

Overall, it can be argued that policymakers should be aware of the ethical implications of their decisions and strive to develop policies that are in line with ethical principles. This can help increase citizens' trust in government and can contribute to achieving positive outcomes for society as a whole.

Protection of privacy

One of the significant ethical considerations when implementing a cybersecurity policy is the protection of privacy. Universities handle vast amounts of sensitive and personal information, such as student records, employee details, and research data, which may be targeted by cyber threats. While it is imperative for universities to safeguard this data, they must also respect individuals' privacy rights (Bennett, 2016). Universities may need to monitor network traffic to detect and prevent cyber attacks. However, indiscriminate surveillance can infringe on privacy rights. Therefore, universities must strike a balance between ensuring security and respecting privacy, adhering to regulations such as the General Data Protection Regulation (GDPR) (Hugl, 2011).

Privacy, in a broad sense, is the right to be left alone, or freedom from interference or intrusion (Westin, 1967). In the context of digital privacy, this principle extends to the realm of digital data, encompassing the rights and expectations of individuals to control their personal information collected, used, and stored in digital formats (Solove, 2008).

Universities are confronted with intricate digital privacy issues. The various data types are subject to different legal and ethical norms surrounding their use and disclosure, requiring a nuanced approach to their management (Daries et al., 2014). The need for robust cybersecurity policies in universities arises from the necessity to protect this vast pool of sensitive data from external threats, such as hackers, and internal threats, such as inadvertent data breaches by staff or students (Chen et al., 2019). Such policies often require a certain level of surveillance and control, such as monitoring network traffic or access to certain data (Zimmer, 2010).

The key ethical challenge here lies in the potential conflict between maintaining security and respecting privacy rights. Overly intrusive security measures might be effective in preventing data breaches but can infringe on the privacy rights of individuals (Bambauer, 2014). Indiscriminate surveillance, for instance, could lead to "chilling effects" on academic freedom, as individuals might self-censor or avoid certain research topics for fear of surveillance (Penney, 2017). Similarly, aggressive data collection for security purposes could violate the principle of data minimization, which is enshrined in privacy regulations such as the GDPR (Hugl, 2011).

Universities must, therefore, carefully craft their cybersecurity policies to balance the need for data protection with respect for individuals' digital privacy rights. This could include adopting a principle of least privilege (only granting access permissions necessary for a role), implementing robust data

anonymization techniques for research, and ensuring transparency in their data collection and use practices (Tavani, 2011).

In essence, digital privacy should not be seen as an obstacle to security, but rather as an integral part of a comprehensive and ethical cybersecurity policy. Universities have a duty to protect not only their data assets but also the privacy rights of their community members.

Fair access

Fair access represents another crucial ethical issue. Fair access, as the term suggests, refers to the equitable distribution of resources and opportunities, ensuring that every individual has the same chance to use and benefit from them (Bahl, 2020). In the context of a university, fair access means ensuring that every student, faculty member, and staff has equal opportunity to access and use the university's digital resources, including but not limited to educational materials, research tools, online platforms, databases, and networks (Weller, 2014). Unequal access to these resources may lead to disparities in educational opportunities, contradicting the university's mandate to provide an equitable learning environment.

When drafting cybersecurity policies, universities should aim to protect digital resources without unnecessarily limiting access to them. A balance should be maintained between security measures and ensuring that the university community has adequate and equitable access to digital resources (Johnson, 2015).

The responsibility for ensuring fair access in a university typically lies with multiple entities. The university administration plays a significant role in setting policies that promote fair access and allocating resources accordingly. Information technology (IT) departments are often responsible for implementing these policies and maintaining the systems that provide access to digital resources. Faculty members, for their part, can help ensure fair access by designing and delivering their courses in ways that do not unnecessarily limit the availability of materials or opportunities based on students' digital access (Seale, 2013).

Academic freedom is fundamentally about the freedom to teach, learn, and conduct research without undue restriction. Ensuring fair access to digital resources is directly related to upholding academic freedom. If access to educational resources and research tools is unequal, it can inhibit the ability of certain students or faculty members to learn, teach, or conduct research effectively, thus undermining academic freedom (Karran, 2007). For example, if a university's cybersecurity policy restricts access to certain digital resources or online platforms in an effort to mitigate cyber threats, it could inadvertently limit academic freedom by hindering access to educational materials or tools needed for research. On the other hand, a lack of adequate security measures could also undermine academic freedom by leaving digital resources vulnerable to cyber attacks that disrupt access or damage the integrity of the resources (Taddeo & Floridi, 2018). Therefore, universities must carefully balance the need for cybersecurity with the principle of fair access to uphold academic freedom. They should aim to protect digital resources from cyber threats without unduly limiting access to those resources. This might involve, for example, implementing role-based access controls that limit access based on a user's role without completely blocking access to necessary resources, or providing alternative access options in cases where certain security measures might limit access (Johnson, 2015).

Responsible Use

Responsible use pertains to how students, faculty, and staff use university resources, including its network and digital assets. Universities must foster an environment that encourages ethical and responsible use of these resources (Siponen, 2000). The cybersecurity policy should outline acceptable use policies (AUPs) that define the do's and don'ts regarding the use of the university's IT resources. This can help mitigate the risk of

insider threats, both intentional and accidental.

"Responsible use" is a term often used in the context of information technology (IT) and refers to the proper and ethical usage of digital resources such as software, hardware, networks, and data (Siponen, 2000). In a university setting, responsible use pertains to how students, faculty, and staff use the institution's digital resources and network. This involves following rules and guidelines set forth by the university in the form of acceptable use policies (AUPs). These policies often outline behaviours that are allowed and disallowed when using the institution's IT resources, aiming to mitigate potential cybersecurity risks from both intentional and accidental misuse (Sasse, Brostoff, & Weirich, 2001).

Furthermore, responsible use extends to cyber hygiene practices, like maintaining strong, unique passwords, not sharing account credentials, being mindful of phishing attempts, and ensuring that personal and university devices are properly secured and updated. Universities should take proactive steps to foster a culture of cybersecurity by continuously educating their community members about their roles and responsibilities in maintaining cybersecurity (Furnell, 2014).

Cybersecurity education and awareness are key to promoting responsible use. Universities need to continuously educate their community members about their roles and responsibilities in maintaining cybersecurity (Furnell, 2014).

Intellectual property

Universities are intellectual powerhouses, producing a plethora of research findings and scholarly works. Protecting this intellectual property (IP) is another significant ethical consideration when formulating a cybersecurity policy. Cyber threats such as data theft, corporate espionage, and plagiarism can compromise the university's IP (Vacca, 2005).

Intellectual property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce. In a university setting, IP often includes research findings, scholarly works, course materials, and proprietary university technologies (Vacca, 2005). Protecting this IP from cyber threats like data theft, corporate espionage, and plagiarism is a significant ethical consideration when formulating a cybersecurity policy.

The cybersecurity policy should provide clear guidelines on protecting IP, including secure storage and transmission of research data, and respect for copyright laws and licensing agreements. It's also crucial to emphasise the adherence to academic integrity standards and professional ethics, including avoiding unauthorised use or dissemination of scholarly works. Violations of these guidelines can have serious consequences, such as disciplinary action, legal penalties, or damage to the university's reputation (Gopal & Sanders, 1997).

Safety and security

The primary purpose of a cybersecurity policy is to ensure the safety and security of the university's digital assets. This includes securing the university's network, systems, data, and user accounts from cyber threats. But it also includes the physical security of the devices used to access these resources.

The concept of safety and security in the context of a cybersecurity policy can be broken down into two components. The first is digital security, referring to the protection of the university's digital assets—its network, systems, data, and user accounts—from cyber threats. This involves measures like using firewalls, encryption, intrusion detection systems, and regularly updating and patching systems to prevent attacks and unauthorised access (Bishop, 2003). However, in their quest to secure their systems and data, universities should not overlook the safety of individuals. This can include physical safety, like the threat of violence related to cyberstalking, and psychological safety, like

ensuring that the university's digital environment is free from harassment and abuse (Clement, 2017). The second component is physical and psychological safety. This aspect involves safeguarding the devices used to access digital resources and ensuring the well-being of individuals in the university community. For instance, physical safety might involve measures to protect against theft of devices or protecting individuals from potential threats like cyberstalking. Psychological safety includes ensuring the university's digital environment is free from online harassment, bullying, and other forms of abuse, which can be achieved by enforcing strict anti-harassment policies and providing support systems for affected individuals (Clement, 2017).

Digital privacy and academic freedom arguably hold the most significant importance in the context of drafting and implementing a cybersecurity policy in universities. Both these factors intertwine deeply with the university's mandate to uphold the rights of individuals and to foster a free and equitable learning environment (Pritchard, 2016).

Academic freedom

Academic freedom is a guiding principle of higher education that assures faculty and students can pursue scholarly inquiry without fear of interference or retribution (Karran, 2007). It encompasses the freedom to conduct research, teach, publish, and engage in discourse, unbounded by political, social, or institutional constraints. Academic freedom is vitally connected to the pursuit of knowledge and truth, forming the backbone of university existence (Fish, 2014). However, the digital age, with its cyber threats and security needs, adds a complex layer to maintaining this freedom.

Cybersecurity policies can, at times, encroach on academic freedom if they become overly restrictive, limiting access to certain information or imposing surveillance that hinders the free exchange of ideas (Bambauer, 2014). Conversely, the absence of a proper cybersecurity infrastructure could expose academics to threats that may result in self-censorship due to fear of reprisal, thereby stifling academic freedom (Taddeo & Floridi, 2018). Protecting academic freedom, therefore, is crucial. Cybersecurity policies must find a balance that enables secure academic discourse and protects the academic ecosystem without undermining academic freedom (Cate, 2015). In essence, cybersecurity measures should be tools that safeguard academic freedom rather than suppress it (Schober, 2020).

Academic freedom refers to the principle that scholars and researchers should have the freedom to pursue and disseminate knowledge without undue interference or censorship. It is the cornerstone of intellectual growth and critical inquiry within universities. When it comes to cybersecurity policies, academic freedom is paramount because it ensures that scholars can explore controversial or unconventional ideas, engage in open discourse, and challenge established norms without fear of reprisal or restriction.
Academic freedom requires universities to create cybersecurity policies that strike a delicate balance between protecting sensitive data and allowing for free and open exchange of ideas. Policies should aim to prevent data breaches and unauthorised access to research data while preserving the right of researchers to access, share, and publish their findings without unnecessary obstacles. This may involve implementing robust security measures, such as data encryption, access controls, and secure collaboration platforms, to safeguard intellectual property and research integrity.

Digital Privacy

Digital privacy addresses the ethical concerns surrounding the collection, use, and dissemination of personal data in the digital domain (Solove, 2011). Universities handle extensive personal and sensitive data, and the potential for privacy breaches or misuse of this data is a significant concern.

While universities adopt cybersecurity measures to protect against digital threats,

these measures can often infringe on individual privacy. Strategies like monitoring network traffic and electronic communications can prevent cyber threats, but these also intrude into individuals' privacy, creating an ethical quandary (Zimmer, 2010). Hence, universities need to craft cybersecurity policies that respect privacy rights while safeguarding data.

Respecting digital privacy extends beyond regulatory compliance, such as adhering to GDPR. It is essential for fostering trust within the university community, encouraging open exchange of ideas, and ensuring the integrity of research and academic practices (Tavani, 2011; Nissenbaum, 2009). Therefore, universities must strive to balance the dual imperatives of data security and privacy protection.

Digital privacy, as articulated by Westin (1967), is the freedom from unwarranted interference or intrusion, extending to personal data in the digital realm (Solove, 2008). In universities, this principle applies to the vast array of sensitive data managed by the institution, including personal data from students, faculty, and employees (Daries et al., 2014). Protecting this data is essential, yet measures taken to ensure this protection must not infringe on the privacy rights of individuals (Bennett, 2016). Intrusive surveillance or aggressive data collection may not only violate privacy regulations such as GDPR but also potentially limit academic freedom by creating a 'chilled' environment, discouraging research into certain areas for fear of surveillance (Penney, 2017).

Academic freedom, on the other hand, is the freedom to teach, learn, and conduct research without undue restriction. It is integral to the university's mission to foster intellectual growth and discovery (Karran, 2007). Without fair and equitable access to digital resources, this freedom is compromised, and the potential for learning and innovation is hindered (Weller, 2014). Hence, cybersecurity measures must be balanced so as not to limit access to the resources needed for education and research (Johnson, 2015).

For instance, a restrictive cybersecurity policy might inhibit the sharing of research findings or scholarly works, limiting the spread of knowledge within the academic community. Similarly, a lack of adequate security could leave resources vulnerable to cyber threats that disrupt access, undermining the ability to learn, teach, and conduct research effectively (Taddeo & Floridi, 2018).

Developing a cybersecurity policy involves balancing the need for security with respect for ethical values. Dutch universities must consider the ethical issues related to the protection of privacy, fair access, responsible use, intellectual property, and safety and security when drafting and implementing their cybersecurity policies. The importance of academic freedom and digital privacy in shaping cybersecurity policies in universities cannot be overstated. They are fundamental to the core academic mission and need to be preserved in the face of digital threats. Striking a balance between security measures and these principles is a delicate but essential task that universities must undertake.

Digital privacy concerns the protection of individuals' personal information and their right to control how it is collected, stored, and used in the digital realm. In the context of cybersecurity policies for Dutch universities, digital privacy is a vital ethical issue due to the vast amount of personal and sensitive data that universities collect and process. This includes student records, research data, and personal information of faculty and staff. Respecting digital privacy necessitates the implementation of strong data protection measures and adherence to relevant legal frameworks such as the GDPR. Cybersecurity policies should outline clear guidelines on data collection, storage, access, and disclosure practices to ensure that individuals' privacy rights are upheld. Policies should also address issues such as obtaining informed consent, anonymization or pseudonymization of data where appropriate,

and providing individuals with control over their own personal information.

Protecting digital privacy not only fosters trust between universities and their stakeholders but also safeguards individuals' autonomy and dignity. It allows students, researchers, and faculty members to engage in academic pursuits without the fear of their personal information being exploited or misused. By prioritising digital privacy in cybersecurity policies, universities can create a safe and secure environment that respects the privacy rights of all individuals involved.

These legal and ethical considerations can significantly impact how cybersecurity measures are implemented in Dutch universities. Moreover, the necessity to respect privacy rights can limit the scope of monitoring and surveillance measures that universities can employ. On the ethical side, the commitment to academic freedom might constrain the stringency of access controls and the extent of data encryption in universities' systems (Kabay, 2010).

Cybersecurity functions as the backbone of information and knowledge security, presenting itself as a vital counterforce against the significant risk cyber threats pose to institutions and nations. Structural methodologies in addressing these risks are given shape through cybersecurity frameworks, requiring policymakers to meticulously ponder the ethical consequences tied to cybersecurity policy decisions. Legal frameworks and regulations become crucial tools to bolster knowledge and information security. The comprehension of the nuances of knowledge and information security, cyber threats, cybersecurity frameworks, policymaking ethics,, and laws, and organisations and governments in devising robust cybersecurity strategies to shield knowledge and intellectual property.

Methodology

The research design consists of three core components: a comprehensive literature review, expert interviews with cybersecurity-related personnel from Dutch universities, and an anonymous survey disseminated among university staff and students.

Research Approach

The research question necessitated a mixed-methods approach, combining both quantitative and qualitative techniques to glean in-depth and multi-faceted insights. The employed methods included literature research, expert interviews and a survey offering a comprehensive perspective on cybersecurity policies within Dutch universities (Creswell & Plano Clark, 2017).

The iterative research approach enabled a continual refinement of the research, facilitating adjustments to the research questions and methods based on findings (Wynn & Eckert, 2017). An iterative research approach refers to a research process where the data collection and analysis are interlinked. As new information or insights are gained during the research process, these are used to refine the research questions or to inform subsequent data collection (Wynn & Eckert, 2017). This flexible approach allows researchers to incorporate new knowledge and adapt their research methods in response to emerging patterns or themes. This way, the findings are continually refined and the validity of the research is enhanced. The semi-structured interviews allowed for flexibility in data collection, enabling the addition of further questions to gain more comprehensive insights (McIntosh & Morse, 2015).

Data Collection

Literature Review

A meticulous review of existing literature was performed to establish the current knowledge base on cybersecurity implementation in universities. This review entailed the examination of academic papers, reports, and relevant policy documents sourced from reputable journals and institutional websites.

Key databases such as IEEE Xplore, Google Scholar, and Scopus were scoured using pertinent keywords, including "Cyber Security," "knowledge security," "universities," and "implementation challenges" (Booth et al., 2016).

Interviews with Cyber Security Personnel

Cybersecurity personnel, specifically Chief Information Security Officers (CISO) and Information Security Officers (ISO) from various Dutch universities, were interviewed in a semi-structured format (Appendix A.2: Interview Questions), and data collected were securely stored. The participants were chosen based on their expertise and roles in developing and implementing cybersecurity policies within their respective institutions. The interviews were designed to explore the firsthand experiences and perspectives of these experts regarding the challenges faced in implementing Cyber Security standards and measures. Open-ended questions allowed respondents to elaborate on their insights, experiences, and any suggested approaches to improve knowledge security through Cyber Security measures.. The interview data will be transcribed verbatim and analysed thematically to derive meaningful patterns and common themes related to the research questions.

Survey for University Staff and Students

An online survey was designed and disseminated to staff and students from various Dutch universities to gather a broader understanding of cybersecurity awareness and knowledge of security practices. The survey was designed to be fully anonymous, ensuring candid responses from participants. Recruitment of participants was carried out through multiple channels, including university websites for staff emails and personal networks, as well as social media platforms like Instagram, LinkedIn, and Facebook.

The survey comprised both closed-ended and open-ended questions (Appendix B.1: Questionnaire questions), and data collected were securely stored. The closed-ended questions were used for quantitative analysis and were designed to assess the respondents' awareness of Cyber Security policies and their opinions on the challenges faced by universities in implementing these measures. The open-ended questions allowed participants to provide additional insights and suggestions, and the responses to these questions will be manually analysed for thematic content.

Data Analysis

The collected data underwent a rigorous analysis process. For interviews, a thematic analysis was conducted to identify patterns and themes in the responses (Braun & Clarke, 2006). Thematic analysis is a qualitative method used for identifying, analysing, and interpreting patterns of meaning ('themes') within data (Braun & Clarke, 2006). This approach allows researchers to see and make sense of collective or shared meanings and experiences. Thematic analysis is flexible in terms of research framework and can provide a rich, detailed, yet complex account of data. Survey data were processed using Google Forms, where the quantitative data were analysed via descriptive statistics and the qualitative data underwent manual thematic analysis (Evans, 2018).

To integrate quantitative and qualitative findings, a triangulation method was utilised. This approach allows the analysis of a single concept or variable from multiple perspectives, ensuring a comprehensive picture of the research subject (King et al., 1995; Marks, 2007). Triangulation refers to the use of multiple methods or data sources in qualitative research to develop a comprehensive understanding of phenomena (Marks, 2007). Triangulation can increase the credibility and validity of research results as the multiple methods or perspectives keep in check the biases that may come from using one particular method, analyst, or source.

Validity and Reliability

Reliability and validity, key aspects of any research methodology, were considered throughout the study. Validity and reliability are key aspects of quality control in research. Validity refers to how well a method investigates what it purports to investigate (Scholte & Douma, 1999). This encompasses the accuracy and truthfulness of the findings. Reliability refers to the consistency and dependability of the research findings, and is concerned with the replicability of the research (Scholte & Douma, 1999). If research is reliable, the same study conducted under the same circumstances should produce similar results. These factors together provide assurance that the research findings are sound and accurately reflect the reality they claim to represent.

The reliability and validity of literature depend on the quality of the literature sources and the accuracy of the analysis. It is important to ensure a comprehensive and diverse selection of sources, such as scientific articles, reports, and policy documents, and to critically assess them for relevance, reliability, and validity. It is important to ensure that the experts interviewed are experts in cybersecurity, universities, and knowledge security and to carefully analyse the views and recommendations they share. In addition, it is essential to ensure that the sample of the survey is representative of the target population.

Ethical Considerations

This research adhered to stringent ethical guidelines to protect participant rights and confidentiality. All participants provided informed consent (Appendix A.1: Informed consent form that needed to be completed by the interviewees), and data collected were securely stored and utilised exclusively for research purposes.

The methodology combined a range of approaches to deliver a comprehensive perspective on cybersecurity implementation within Dutch universities. This methodological design allowed for the generation of in-depth insights, leading to robust recommendations for improving cybersecurity measures.

Results

The results are organised and presented according to the type of question, which allows for an efficient analysis and understanding of the data. Each section provides a summary of the results, which offer insights into the prevailing perceptions, beliefs, and attitudes towards cybersecurity among the respondents. It is worth noting that the findings should be interpreted with consideration of the respondents' diverse backgrounds and experiences. For those who are interested in a more granular examination of the responses, a detailed description is provided in Appendix A and B.

Reflection Cyberethics

This section will reflect on the ethical considerations outlined in the literature review. The aim is to provide a comprehensive analysis of potential guidelines based on these considerations that could be integrated into policy frameworks.

Privacy

It's abundantly clear that the complex relationship between cybersecurity and privacy presents universities with a significant moral dilemma. Taking inspiration from the core Dutch values of transparency, consensus-driven decision-making, and a steadfast commitment to the well-being of its people, universities in the Netherlands must proactively develop a strategy that goes beyond reactive measures and addresses upcoming challenges with foresight.

- *Uniform Cybersecurity Protocol:* Universities in the Dutch context, whether they operate independently or as part of a larger academic consortium, should consider creating a collaborative cybersecurity plan. This approach ensures consistency in

addressing cyber threats while also accommodating the specific needs of each institution.

- *Transparant Data-Handling:* Following the Dutch tradition of openness, academic institutions must be clear in explaining their approaches to data collection, retention, and use. Every stakeholder, including students, faculty, and external partners, deserves clarity, not confusion.
- *Inter-University Collaboration:* Dutch academic institutions, known for their collaborative tendencies, should actively promote knowledge sharing about digital privacy complexities. This could take the form of regular scholarly gatherings or a centralized digital platform.
- *Privacy Audits:* Routine privacy assessments should be implemented to gauge the effectiveness of data protection measures. These audits should include internal evaluations and third-party reviews to comprehensively evaluate existing systems.
- *Engage the Academic Community:* Fostering dialogue within the academic community is essential. Incorporating the concerns and wisdom of scholars can provide valuable insights for policy development.
- *Dedicated Ethical Committees:* It's crucial to establish specialized groups that focus on the ethical aspects of managing digital information. These entities should provide guidance in shaping policies, ensuring that privacy considerations are not overshadowed by security concerns.

Within the broader context, Dutch academic institutions demonstrate varying levels of cybersecurity maturity. Some universities may be pioneers, seamlessly integrating cutting-edge technological approaches, while others may just be starting their cybersecurity journey. Regardless of their positions, a steadfast commitment to privacy is paramount. Thus, the challenge lies not only in implementing robust security measures but also in aligning these efforts with an unwavering respect for individual privacy rights.

In conclusion, the key is not whether universities can reconcile cybersecurity with privacy, but how effectively they can strike this balance. For Dutch academic institutions, the solution lies in collaborative partnerships, complete transparency, and an unwavering commitment to respecting the sacred nature of individual privacy.

Fair Acces

The thoughtful discussion surrounding equitable access to digital resources within university settings provides deep insights into the ethical challenges that arise from integrating technology into education. The Netherlands, with its commitment to egalitarianism and equal opportunities, faces challenges that are both technologically complex and culturally ingrained.

- *Inclusive Digital Design:* Universities should strive to promote an "inclusive digital design" approach, carefully creating digital interfaces and tools with a keen awareness of user diversity and capabilities.
- *Continuous Education & Training:* It is essential for academic institutions to continually educate and train both students and staff in emerging digital tools, ensuring maximum utility for the entire academic community.
- *Regular Evaluation:* Periodic assessments of digital resource access and usage patterns can reveal hidden disparities or obstacles.
- *Clear Policy Communication:* Institutions must clearly communicate any access restrictions due to security requirements and proactively provide alternative access options when possible.
- *Inter-Departmental Collaboration:* Collaboration between technology departments and academic faculties is essential to ensure that cybersecurity strategies do not inadvertently hinder educational pursuits.

- *Stakeholder Feedback:* Establishing a responsive feedback channel that allows the academic community to share their experiences with digital resources is of paramount importance.

Responsible Use

The importance of wisely utilizing IT resources within academic environments is undeniable. As technology becomes an integral part of academic pursuits, mastering the ethical use of these tools becomes an essential skill for all members of the academic community.

- *Policy on Responsible Use:* Every academic institution must establish a comprehensive policy outlining the principles of responsible IT asset usage, regularly updating it to keep pace with technological and societal changes.
- *Education & Training:* It's crucial to continually provide education and training on responsible usage norms and potential risks associated with digital recklessness.
- *Promotion of Cyber Hygiene:* Institutions should lead in promoting the importance of cyber hygiene practices, such as timely software updates, strong password protocols, and cautious avoidance of suspicious online activities.
- *Feedback Mechanisms:* Establishing mechanisms that empower students and faculty to voice concerns related to digital tool usage can help identify and address misconceptions or challenges.
- *Ubiquitous Responsibility:* From new students to experienced faculty to administrative staff, everyone should understand their crucial role in strengthening the institution's digital defenses.

Intellectual Property

Protecting intellectual property (IP) within academic institutions is of utmost concern. Given the increasing incidents of cyberattacks aimed at obtaining valuable data and research findings, safeguarding IP should be a top priority for Dutch universities. The importance of research and scholarly contributions can be immeasurable, and potential misuse or loss could have far-reaching academic and economic implications.

- *Robust Storage and Transfer:* Universities should implement advanced security measures for storing and transferring research data and other forms of IP.
- *Education and Awareness:* Researchers, students, and staff should receive regular training on best practices for safeguarding their intellectual creations and understanding the scope and significance of IP.
- *Legal Protections:* Universities must actively pursue patents, copyrights, and other legal protections for their intellectual assets.
- *Collaboration with External Entities:* Clear agreements must be crafted when collaborating with industries or other external entities, ensuring rights and responsibilities regarding IP are protected.
- *Monitoring and Enforcement:* Proactive monitoring of university IP resources usage can help swiftly detect potential breaches. Clear policies and procedures should be in place for addressing infringements, including possible legal actions.

Regarding Dutch universities' stance on IP protection, a proactive approach is imperative. It's not only pivotal to safeguard the invaluable intellectual contributions of the academic community but also vital to uphold standards of academic integrity and ethics.

Safety & Security

Ensuring the safety and security of digital assets within universities is undeniably crucial. However, in light of the intricate and ever-evolving digital milieu, the concept of safety within a university setting must encapsulate both digital and the physical and

psychological facets of safety. Dutch universities, given their eminent role in the academic and research ecosystem, bear a unique responsibility to maintain this multi-dimensional approach to safety.

- *Comprehensive Digital Security:* Universities should instate a multi-layered cybersecurity infrastructure, encompassing not merely firewalls and encryption but also advanced threat intelligence and response mechanisms.
- *Physical Security of Devices:* Strict protocols must be in place for safeguarding devices accessing university networks. This includes measures against theft and routine updates to preempt security vulnerabilities.
- *Ensuring Psychological Safety:* Universities should strive to cultivate a digital environment devoid of online harassment, bullying, and abuse. This calls for not just technological solutions but a zero-tolerance policy against such behavior, backed by educational initiatives.
- *Education and Awareness:* Continuous training and consciousness-raising are essential for students and staff alike. They should be cognizant of not only potential cyber threats but also the psychological and physical risks arising from their digital actions.
- *Support Systems:* Robust support mechanisms are indispensable for those targeted by cyber threats, bullying, or harassment. This ranges from technical assistance to counseling services.

In terms of their stance on safety and security, Dutch universities should adopt a holistic approach. It's not merely about safeguarding data and systems but ensuring the overall well-being and safety of their community. The academic mission of universities can only thrive in an environment where digital, physical, and psychological safety is assured.

Academic Freedom

In the world of academia, the principles of freedom in research and education are of paramount importance. Universities should provide a haven for open thought, critical examination, and independent research. Nevertheless, in this digital era, where cybersecurity is a prominent concern, preserving academic freedom becomes more complex.

- *Preservation of Freedom:*Universities must ensure that their cybersecurity policies do not jeopardize academic freedom. This means that policies should not impose unnecessary restrictions or surveillance that could hinder free thought and open debate.
- *Balance between Security and Freedom:* While universities need to shield their digital assets from cyber threats, they must ensure that such measures don't undermine academic freedom. This demands a judicious consideration of which security protocols are initiated and how they're deployed.
- *Transparency and Dialogue:* Universities should be forthright and transparent about their cybersecurity measures, involving faculty and students in decision-making to ensure academic freedom remains at the forefront.
- *Education on Cybersecurity and Academic Freedom:* Universities should offer educational programs and training that explore the relationship between cybersecurity and academic freedom. This will help the academic community understand how these two concepts can mutually reinforce each other.
- *Robust Support and Response:* Should breaches or threats arise that jeopardize academic freedom, robust response mechanisms and support networks should be at the ready to assist affected individuals and preserve academic integrity.

At the heart of the academic mission lies a dedication to the free exchange of ideas and independent inquiry. As Dutch universities endeavor towards digital security, their focal point must remain the protection and amplification of this fundamental academic value. Cybersecurity should be perceived as an instrument serving academic freedom, not as an impediment.

Digital Privacy

In today's digital era, privacy is of paramount importance. As the significance of data and the technologies processing it continues to grow, universities face the challenge of protecting the privacy of their community members while also safeguarding sensitive information.

- *Informed Consent:* As universities amass personal data, they must ensure unequivocal, informed consent from the concerned parties. This dictates that students, faculty members, and employees be precisely apprised of what data is collected and for what purpose.
- *Data Minimization and Protection:* Cybersecurity policies should champion data minimization, where only essential data is collated and processed. Moreover, robust encryption measures and other security practices should be employed to guard this data.
- *Transparency and Access:* Universities should lucidly convey their data processing practices, and individuals should have facile access to their own data. Clear protocols should also be established for data correction or deletion.
- *Balance between Security and Privacy:* While warding off cyber threats is imperative, security measures shouldn't result in unwarranted invasions of privacy. This implies that practices like extensive network monitoring must be judiciously applied, striking a balance with individual rights' respect.
- *Education and Awareness:* Universities should commit to training and awareness initiatives on digital privacy and cybersecurity. This enables members of the academic community to be conscious of their rights and responsibilities in the digital landscape.

The academic community relies on an open and secure ambiance for learning and research. In an era marked by escalating digital threats and privacy concerns, it's paramount for Dutch universities to take a proactive role in safeguarding the digital rights and freedoms of their community. A well-considered cybersecurity policy that centers on digital privacy is essential for maintaining trust and fostering academic excellence.

Interview Analysis

In the study at hand, a rigorous six-step process was employed to conduct the thematic analysis of the interviews, as prescribed by Braun and Clarke (2006). This robust approach ensures the depth and breadth of participants' insights are adequately captured, and that the emerging themes are thoroughly grounded in the data.

In the initial familiarisation phase, the interview transcripts were read and reread exhaustively to gain a comprehensive understanding of the data. This immersion in the data allows for the identification of nuanced details and aids in the formulation of insightful initial observations (Guest, MacQueen, & Namey, 2012). After that, the generating initial codes stage involves the systematic creation of descriptive codes that encapsulate interesting and research question-relevant features of the data. The coding process is a fundamental building block of qualitative data analysis, as it organises the data into meaningful and manageable segments (Saldana, 2016). Upon completing the initial coding, these

codes were reviewed, and patterns of broader meaning were sought. By grouping related codes, potential themes began to surface. This stage is pivotal for transitioning from a fragmented understanding to a more synthesised interpretation of the data (Nowell, Norris, White, & Moules, 2017). To ensure the preliminary themes accurately represented the collected data, a stringent review against the full dataset was undertaken. This occasionally necessitated refining, merging, or creating sub-themes to better reflect the nuances in the data (Braun, Clarke, & Weate, 2016). Each theme was then carefully analysed to capture its essence, allowing for the formulation of clear definitions and apt names. The main idea behind this step is to provide coherent and distinct identities for each theme, contributing to the clarity of the results section (Braun & Clarke, 2006). Lastly, a detailed write-up of the thematic analysis was performed. For each identified theme, evidence from the dataset was provided in the form of illustrative quotes. The analysis was conscientiously tied back to the research question and existing literature, providing an enriched understanding of the study's context and findings (Nowell et al., 2017). Through the systematic and iterative process outlined above, the thematic analysis ensures a transparent, replicable, and trustworthy interpretation of the qualitative data derived from the interviews.

The tables below show how the interviewed universities responded to these factors:

- Limited Resources: Universities often have limited resources and budgets to implement Cyber Security measures. This may mean that they are unable to purchase the necessary technologies or hire staff needed to implement and maintain Cyber Security measures.
- Complexity: Cyber Security is a complex field with different technologies and methodologies that change regularly. It can be difficult for universities to keep up with the latest developments and understand the complexity of Cyber Security.
- Culture: There may be a culture of nonchalance toward Cyber Security within universities. There may be a lack of understanding of the risks of cyber threats and the value of protecting data and systems.
- Lack of priority: Cyber Security can sometimes be considered a secondary priority compared to other operational or educational activities of the university. This may result in insufficient resources and priority being given to cyber security measures.
- Human factor: Cyber Security requires not only technological solutions, but also awareness, training and involvement of staff. It can be a challenge to involve all staff, students and researchers within the university in implementing and enforcing cyber security measures.

Cyber ethics as it relates to universities deals with the moral issues and responsibilities arising from the use of technology and digital resources within the academic community. This includes:

- Protection of privacy: Universities have a responsibility to protect the privacy of students, employees and researchers. This means they must take appropriate technical and organisational measures to protect personal data from unauthorised access, loss or theft.
- Fair Access: Universities must ensure that their technology and digital resources are available to all students, staff and researchers in a fair and equal manner. This means a commitment to digital inclusion and accessibility for all.
- Responsible use: Universities should encourage students, staff and researchers to use technology and digital resources responsibly. This means integrating ethical considerations into their education and

research and establishing guidelines for the use of technology.
- Intellectual property: Universities have a responsibility to protect intellectual property and ensure that students, staff and researchers comply with copyright and other intellectual property laws.
- Safety and Security: Universities have a responsibility to secure their technology and digital assets against cyber-attacks and other threats. This means taking appropriate technical and organisational measures to ensure the integrity, confidentiality and availability of their data and systems.

As mentioned, two questions were asked during the interview that asked the interviewee to estimate by level of both influence and priority. The various universities interviewed offered diverse assessments regarding the factors influencing the implementation and enforcement of cybersecurity policy. Notably, culture was the sole factor universally considered by all universities as posing (significant) hindrance. Interestingly, TU3 did not perceive equitable access as a factor in cyber ethics. All the universities interviewed assigned the highest priority to the safety and security factor.

These findings suggest a broad consensus on the importance of safety and security in shaping cybersecurity strategies. However, the range of views on other factors indicates a complex interplay of influences in the management of cybersecurity within these institutions. It also underscores the unique contextual challenges each university faces in prioritising and addressing cybersecurity concerns. The detailed insights from each interview offer a comprehensive perspective on the multifaceted nature of cybersecurity policy implementation in the academic sector.

Table 1 - Influencing factors cybersecurity policy

	Highly restrictive	Restrictive	No influence	Stimulating	Highly stimulating
Limited Resources	X	XXXX	X		X
Complexity	XX	XXX	XX		
Culture	XXXXX	XX			
Priority		XX		XXXX	X
Human factor	XXXX			XX	X

Table 2 - Cyber ethics factors

	1 - Highest priority	2	3	4	5 - Lowest priority
Protection of privacy	XXXXX	X	X		
Fair Access	XXXX	XX			
Responsible Use	XX	XXXX	X		
Intellectual property	XXXX	XX	X		
Safety and security	XXXXX XX				

Legend

	TU1
	O1
	O2
	TU2
	TU3
	O3
	O4

In addition, these are the key findings from the interviews, clustered by theme:

Table 3- Thematic Analysis

	TU1	O1	O2	TU2	TU3	O3	O4
Cyber Security challenges	Phishing attacks	Phishing attacks	Hacks	Phishing attacks Ransomware Giftcard scam	Hack of supplier	Hackers Pentests Scans Red-teams	Phishing attacks Long term spyware
Cyber Security standards	SURF ISO270001 TU specific ISO framework	SURF ISO270001 NIST CIST Security by Design / Default	SURF ISO270001 Information-security policy	SURF ISO270001 NEN7510	SURF NBA Framework NIST	SURF ISO270001 NIST Own framework	SURF ISO270001
Awareness and training	No mandatory training E-learning Newsletter, Brightspace	Awareness program Awareness office	Awareness program Mandatory training for staff	Newsletter Student and staff portal	Awareness campagne	Phishing simulations	No mandatory training Online training for staff
Collaboration and partnerships	Collaboration between universities is useful	Collaboration between universities is useful Collaboration with NSCS	Collaboration between universities is useful	Collaboration between universities is useful Collaboration with NSCS	Government should decide a minimum base-line Collaboration between universities is useful	Collaboration between universities is useful	Collaboration between universities is useful Sharing of policies and measures Collaboration with NSCS
Influencing factors	University politics	Human attitude	Autonomy of faculties Culture and human behaviour	Students are stimulating Faculties are independent which is hampering	Culture Technical delay Democratic decision model	Awareness Open science	Government is stimulating Not willing to change is hampering

	TU1	O1	O2	TU2	TU3	O3	O4
Cyber ethics	Ethics department	Privacy and security Knowledge security Fair access - levels of assurance	X	Ethical board of faculties Collaboration with lawyers	Monitoring and testing against privacy	No ethical objections	Ethical research Privacy department
Future directions	CIS controls Create more awareness	Training by onboarding Create more awareness Security Office Change the culture	Recruit knowledgeable people Developing with the attacks Create more awareness Change the culture	Create more awareness Implement new policy	Gain more knowledge about cyber security Increase base-line Being ambitious in growing maturity Create more awareness	Increase security posture Access policy distinction (priviledge and non-priviledge) Create more awareness	Offline training by onboarding Centralisation of policy - overarching approach - combining forces New cloud services Create more awareness

Interview Results

This section presents the results of the interview analysis. The process of thematic analysis, as proposed by Braun and Clarke (2006), was employed to rigorously examine and distil the interview data into salient themes. The six-step procedure from initial familiarisation to a comprehensive write-up, allowed for an in-depth exploration and presentation of the participants' perspectives. It ensured a transparent, replicable, and trustworthy interpretation of the qualitative data.

The first section discusses the responses to two interview questions that asked participants to assess influence and priority levels related to cybersecurity policy implementation. This is followed by the presentation of additional influential factors identified by the respondents. The final section covers themes related to cyber ethics, as these issues are critical to the academic community's use of technology and digital resources.

Influence and Priority Assessment

Universities showed varying perceptions of the factors influencing the implementation and enforcement of cybersecurity policies. All universities, however, identified the aspect of culture as posing a significant hurdle. Surprisingly, TU3 did not identify equitable access as a factor within cyber ethics. Overall, the safety and security factor was accorded the highest priority by all the universities.

This consensus on safety and security underscores its central role in shaping cybersecurity strategies. The diversity of

viewpoints on other factors highlights a complex web of influences in managing cybersecurity. These factors also indicate the unique challenges each university confronts when addressing cybersecurity issues. Limited resources, complexity, culture, priority, and the human factor were identified as significant influencers on the execution of cybersecurity policies. Each of these factors represents different challenges to universities, ranging from financial constraints and technical complexity to issues with staff awareness and training. Themes around the protection of privacy, fair access, responsible use, intellectual property, and safety and security were identified in relation to cyber ethics. Universities have diverse responsibilities in these areas, which include not only securing digital assets but also promoting ethical behaviour within the community.

Thematic Analysis: Key Findings

The thematic analysis of the interviews was conducted using a rigorous six-step process as proposed by Braun and Clarke (2006). The results derived from the process, highlight key findings across seven identified themes: Cybersecurity Challenges, Cybersecurity Standards, Awareness and Training, Collaboration and Partnerships, Influencing Factors, Cyber Ethics, and Future Directions.

A predominant issue across all universities was the threat of phishing attacks, further emphasising the ever-present nature of this cybersecurity concern. TU1, O1, and TU2 all mentioned phishing attacks as one of their main cybersecurity challenges. O2, on the other hand, cited hacks as their primary cybersecurity issue. TU3 highlighted a unique case of supplier hacking, reflecting the interconnected vulnerabilities that come with digital partnerships. O3 and O4 reported a broader spectrum of challenges, including hackers, pentests, scans, and red-teams. O4 also pointed out the issue of long-term spyware, demonstrating the diverse array of threats universities face.

Cybersecurity standards adopted by the universities show the concerted efforts to standardise security practices and comply with international norms. All universities were found to have implemented SURF and ISO27001. Notably, TU1 mentioned using a TU specific ISO framework, showing an institution-specific adaptation of a standard approach. TU2 employed a broad suite of standards, including SURF, ISO27001, and NEN7510. TU3 employed the NBA Framework, along with SURF and NIST. O3 employed its own framework, in addition to SURF, ISO27001, and NIST, indicating a customised strategy. O4 strictly adhered to SURF and ISO27001.

Across universities, the emphasis on awareness and training was highly evident. TU1, for instance, highlighted the absence of mandatory training, instead relying on e-learning and newsletter updates. In contrast, O1 and TU2 exhibited a more structured approach to awareness, with the implementation of formal awareness programs and mandatory training for staff. O3 and O4 also showed efforts to foster awareness through online training for staff and phishing simulations, respectively.

The critical role of collaboration and partnerships in enhancing cybersecurity emerged as a common theme. Almost all universities indicated that collaboration between universities is useful, emphasising the importance of sharing knowledge and practices within the academic sector. Specific collaborations with NSCS were mentioned by O2, TU2, and O4.

The interviews unearthed a multitude of influencing factors that shape the cybersecurity landscape within these universities. The nuances were highlighted by responses ranging from the influence of university politics and the attitude of individuals at TU1 and O1, respectively, to the implications of culture and human behaviour at TU2. TU3 cited technical delays as a barrier, while O3 pinpointed the effects of open science as an influencing factor.

The importance of ethical considerations was underscored across all universities. TU1, O1, and TU2 cited the existence of specific departments or policies, such as an ethics department or privacy and security regulations. TU3 mentioned monitoring and testing against privacy, highlighting a proactive approach. O3 showcased a collaborative approach, with the involvement of lawyers in ethical matters.

Finally, the interviews highlighted the envisioned future directions in terms of cybersecurity for the universities. A common theme was the emphasis on creating more awareness, as indicated by TU1, O2, TU2, and O4. Other directions included implementing new policies (TU1), recruiting knowledgeable people (O1), increasing baseline security (TU3), and distinguishing access policies (O3).

In summary, these thematic findings highlight a shared recognition of the importance of cybersecurity among the universities, along with their unique challenges and approaches. Despite the commonalities, there are clear distinctions in how each institution experiences and navigates their cybersecurity landscape, shaped by their unique contexts, resources, and institutional cultures.

Comparison Technical and Other Universities

Technical Universities, by their very nature, possess a concentration on technical, engineering, and science disciplines. This distinction might influence their approach, resources, and perspectives on matters such as cybersecurity, setting them apart from institutions with a more generalized or humanities-centric curriculum. TU's might possess different financial, infrastructural, and human resources dedicated to technical endeavors, including cybersecurity. Understanding how these resources are allocated and utilized can shed light on potential disparities in cybersecurity readiness and infrastructure.

Each type of institution might have evolved its unique institutional culture, reflecting in its strategies and priorities. Clustering universities by these categories helps in discerning overarching patterns, strategies, or deficiencies prevalent within each group. By segmenting the universities, one can derive more granular insights, reducing the potential noise or outliers that might emerge if all universities were treated as a homogenous entity. This refined granularity can, in turn, lead to more actionable insights and recommendations tailored for each cluster. When communicating findings, especially to policy-makers or institutional leaders, having a clear differentiation can make recommendations more palatable and actionable. It allows for a nuanced discussion on what might work best for each type of institution, respecting their inherent differences and strengths. In essence, clustering results by differentiating Technical from Other Universities not only accentuates the unique challenges and strengths of each group but also ensures that any subsequent actions or recommendations are both relevant and tailored, enhancing the efficacy of potential interventions.

The 4TU.Federation is a collaborative alliance among the Netherlands' four premier technical universities: TU Delft, Universiteit Twente, TU Eindhoven, and Wageningen University. Together, they aim to fortify their national and international standing, ensuring the cultivation of skilled engineers and technologists, conducting globally recognized and socially pertinent research, and fostering collaborations between research institutions and industries. (4TU.Federation)

In the preceding sections, we have delineated the findings from interviews with both Technical Universities (referred to as TU) and other universities (referred to as O). The thematic outcomes reveal shared insights as well as distinct elements in their approach to cybersecurity. The contrasts between the Technical Universities (TUs) and the Other (O) universities, as illuminated by the interview outcomes, can be characterized

based on their perceptions, strategies, and challenges related to cybersecurity:

Perception of Cybersecurity Challenges

- Phishing Attacks: Whilst both TUs and Os recognize the peril of phishing onslaughts, it is specifically pinpointed as a primary concern by TU1, O1, and TU2. Conversely, O2 places a heightened emphasis on hacking incidents.
- Unique Challenges: TU3 has broached a specific issue pertaining to supplier hacking, possibly suggesting their expansive digital collaboration networks. The Os convey a more comprehensive range of challenges, as indicated by O3 and O4, ranging from hacker incursions to penetration tests and spyware.

Strategy and Standardization

- Standard Implementation: Even though all universities have adopted SURF and ISO27001, TUs exhibit a predilection for customization with more variance and adaptation. For instance, TU1 has employed a TU-specific ISO framework, while TU3 integrated the NBA Framework alongside SURF and NIST.
- Awareness and Training: TUs display more heterogeneity in their approach to training. TU1, for instance, predominantly relies on e-learning modules, while TU2 has instituted formal training curriculums. The Os, as exemplified by O1, manifest a more structured approach, mandating specific trainings.

Collaboration and Partnerships

Both TUs and Os recognize the quintessential value of collaboration. However, explicit partnerships with NSCS are predominantly cited by TU2, O2, and O4, suggesting a possibly more profound engagement of technical universities with national cybersecurity initiatives.

Influencing Factors

TUs underscore a gamut of both technical and cultural determinants influencing cybersecurity, such as institutional politics in TU1 and technological lags in TU3. The Os, conversely, like O1, emphasize individualistic attitudes and broader institutional determinants like the concept of open science championed by O3.

Ethics in Cybersecurity

TUs portray a more nuanced and occasionally proactive stance on ethics, with structures like specific ethical departments in TU1 and surveillance against potential privacy infringements in TU3. The Os tend to embrace a more collaborative tactic, as seen in O3, involving legal experts in ethical deliberations.

Both technical and other universities underscore the paramountcy of cybersecurity; however, their methodologies, perceptions, and challenges differ considerably. Technical universities, owing to their inherent nature, seem to embody a more adaptive and occasionally anticipatory posture, whereas the other universities lean towards standardization and concerted collaboration. These variances mirror their unique institutional cultures, priorities, and resources.

Questionnaire Analysis

In total, 88 students or staff members have responded to the questionnaire of which 80 percent are students and 20 percent are employees. By having the option to answer the survey question in the language of choice, the result is that 78,9% of the respondents answered in Dutch, the remaining 21,1% answered in English. The outcomes of the survey are analysed by classifying them based on the type of question—multiple choice, Likert scale, and open-ended questions. This process allows for a streamlined, systematic, and comprehensive interpretation of the collected data, thus enhancing the validity and reliability of the results.

Multiple-choice questions

Multiple choice questions provide a set of predetermined answers to choose from, thus facilitating a quantitative analysis. The results can be presented in the form of percentages or frequencies, offering insights into the preferred choices among respondents.

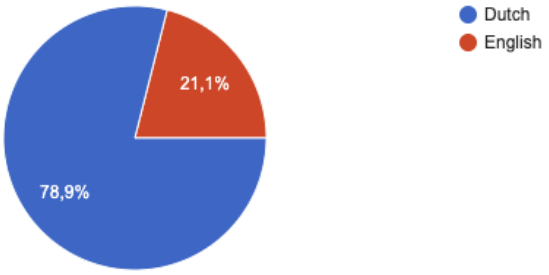


Figure 1 - Percentage of Language

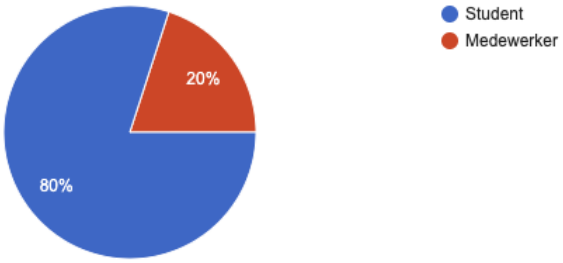


Figure 2 - Percentage of type responde

Table 4 - Multiple-choice answers questionnaire

Question	Conclusion
Which Dutch university are you affiliated with ?	Most of the respondents were affiliated with TU1. It is a diverse group but not every university has a respondent.
Have you ever personally experienced your data or information being compromised or stolen at the university?	Two-thirds have never had experience with stolen information.
Are you aware of the current policies and guidelines of your university regarding knowledge security and cyber security?	The majority say they are not aware of the current policy.
What factors do you see as influential in the implementation and compliance of cybersecurity measures at the university?	The majority see human factor as influencing factor
Are you aware of what is considered sensitive information within your university and what is not?	The majority of respondents are not aware of what is considered sensitive information.
Do you believe that sufficient resources and support have been provided to students and employees to help them deal with Cyber Security issues?	53.3% indicate that enough resources and support have been made available.
Do you think your university has enough resources and expertise to effectively implement Cyber Security?	More than half feel that the university has insufficient resources and expertise at its disposal.
Has the university provided you with sufficient information about cyber security and knowledge security?	Only one-third feel they are sufficiently informed about cybersecurity and knowledge security.
Has the university provided training or guidelines for cyber security and knowledge security?	Currently, two-thirds have no training or guidelines.
Would you be interested in participating in training or workshops on cyber security to enhance your knowledge and skills in this area?	80% are willing to participate in training or workshops to improve skills.
Do you believe that mandatory training on Cyber Security should be offered to students and employees at your university?	More than 90% think mandatory training should be offered.
Would you feel safer if the university took additional measures to enhance cyber security?	Nearly 90% would feel safer if the university took additional measures to improve cybersecurity.

Likert-scale questions

Likert-scale specifies the level of agreement or disagreement (Barua, 2013). In other words, if one chooses 1, the respondent strongly disagrees with the statement and if one chooses 5, the respondent strongly agrees with the statement.

Likert scale questions, on the other hand, assess the level of agreement or disagreement with a particular statement. These questions are typically structured as a five or seven-point scale, with one end representing strong disagreement and the other strong agreement (Allen, I., & Seaman, C. A., 2007). The responses can be analysed both individually, to capture specific attitudes or perceptions, and collectively, to gauge general trends or consensus. According to Boone and Boone (2012), Likert scale data can be analysed using both descriptive and inferential statistical methods, with mean scores often used to compare groups or conditions.

Table 5- Likert-scale answers questionnaire

Question	Conclusion
To what extent do you believe Cyber Security standards/measures should be a priority for Dutch universities?	The majority think cyber security should be a very high priority. 13.3% still say very low priority.
To what extent do you think your university invests adequately in Cyber Security?	More than 50% give this an average score.
To what extent are you aware of the urgency of Cyber Security and the potential consequences of a breach in the security of sensitive information?	26.7% have little or no awareness of the urgency and implications of cyber security.
How skilled do you consider yourself and other students/staff in recognizing and reporting possible security incidents or suspicious activity?	Two-thirds consider themselves moderately proficient.
How confident do you feel in your knowledge of cyber security and taking measures to ensure knowledge security?	40% give this a score 2 of confidence. No one is very unsure. The other three scales contain 20% of participants.
How willing are you to participate in Cyber Security training if it is offered?	40% percent are very willing to participate in training. 26.7% give this both scores 2 and 3. No one is unwilling.

Open questions

Open-ended questions allow participants to respond in their own words. These responses offer qualitative insights into participants' thoughts, feelings, and experiences. Such data can be analysed through thematic analysis or other qualitative data analysis methods (Braun & Clarke, 2006).

The open-ended queries yielded several findings:

1. The majority of respondents demonstrated an astute awareness of the myriad types of online threats. The range of answers was wide, with predominant concerns centred around phishing attacks and data breaches.
2. Numerous students and staff members were uninformed about the university's current investment in cybersecurity. A few indicated that the university actively engages in cybersecurity measures, noticeable through regular password update reminders and monthly communication emails. However, most respondents were oblivious to the resources and support extended to assist in navigating cybersecurity issues.
3. The majority of participants claimed to adopt a vigilant role, reporting potential cyber threats. Conversely, many appeared indifferent to the importance of secure data handling when working with confidential information. A minority reported data anonymization practices and prioritised secure storage locations.
4. According to students and staff, while there is expertise available, it remains underutilised, impeding knowledge transfer.
5. While a portion of respondents could not pinpoint specific obstacles to cybersecurity policy implementation, others highlighted culture and the human element as significant barriers. The accompanying rationale was a lack of understanding of potential consequences, unawareness, and ignorance.
6. The respondents suggested that the university could provide straightforward information, conduct workshops, training sessions, or even courses offering credit points. Hiring proficient staff to articulate guidelines more clearly could foster increased awareness and promote a more open community.
7. Suggestions to which the students and staff were open included mandatory campaigns/seminars, transparent policies, and threat identification training, for instance, by disseminating decoy phishing emails.

Analysis Student vs. Staff

Google Forms is a renowned tool for collecting responses to surveys and questionnaires. However, it lacks innate functionality to segregate responses based on demographic or other distinctive characteristics such as 'student' or 'staff'.

The responses harvested from Google Forms were transitioned to an Excel spreadsheet. This transition facilitates a more intricate analysis of the data, given that Excel stands as a potent instrument for data scrutiny. Should the survey incorporate a query where respondents identified their status (be it student or staff), Excel's filtering mechanisms or other analytical methods can be employed to study the responses of these two cohorts distinctly. Upon exporting the responses into Excel, the feedback from students and staff was discerned and examined separately, thus illuminating the distinctions between the two groups.

Questionnaire Results

This section presents the results from the survey conducted to assess the awareness, understanding, and practices related to cybersecurity within the Dutch universities. The analysis was carried out by categorising the responses based on the type of question—multiple-choice, Likert scale, and open-ended.

The majority of respondents were associated with TU1, providing a diverse yet not fully representative sample of all Dutch universities. The prevalence of personal experience with data compromise was relatively low, with two-thirds of respondents reporting no such incidents.Regarding policy awareness, the majority of respondents indicated unfamiliarity with their university's current guidelines and policies related to knowledge and cybersecurity. This extends to the specific classification of sensitive information, with most respondents expressing unawareness of what constitutes sensitive information within their university context. The human factor emerged as a predominant influence in implementing and complying with cybersecurity measures, as identified by most respondents. Regarding the provision of resources and support, 53.3% of respondents believed that the university has provided adequate assistance for dealing with cybersecurity issues. However, more than half of the respondents felt that the university lacked the necessary resources and expertise for effective cybersecurity implementation. The analysis reveals a lack of sufficient information and training on cybersecurity, with only a third of respondents feeling adequately informed and two-thirds stating that they had not received any training or guidelines. However, a significant interest in participating in training or workshops was expressed, with 80% of respondents indicating a willingness to enhance their knowledge and skills. Additionally, over 90% of respondents endorsed the idea of mandatory cybersecurity training for students and employees, and nearly 90% would feel safer if additional measures were taken by the university to improve cybersecurity.

Likert scale responses were analysed to gauge the level of agreement or disagreement with specific statements related to cybersecurity.

The majority of respondents strongly agreed that cybersecurity should be a high priority for Dutch universities, although 13.3% considered it to be of very low priority. More than 50% of respondents felt that their university's investment in cybersecurity was average. Awareness of the urgency of cybersecurity and the potential consequences of a security breach varied, with 26.7% of respondents expressing little to no awareness. Self-perception of skill in recognizing and reporting security incidents was moderate among two-thirds of the respondents. Confidence in their knowledge of cybersecurity was rated as '2' by 40% of respondents, with no respondent feeling very unsure. On the topic of participation in cybersecurity training, 40% were very willing, while no one expressed unwillingness.

Open-ended responses offered insights into the respondents' thoughts and experiences. Most respondents demonstrated an acute awareness of various online threats, with primary concerns around phishing attacks and data breaches. However, awareness of the university's efforts and investment in cybersecurity was notably low. Respondents claimed to adopt vigilant behaviours such as reporting potential cyber threats, but a lack of secure data handling practices was evident. Barriers to implementing cybersecurity policy were largely attributed to the human element and culture, while expertise was perceived as underutilised. Respondents suggested various measures for improvement, including providing clear information, conducting workshops and training, and hiring skilled staff. Respondents were open to initiatives such as mandatory campaigns or seminars, transparent policies, and threat identification training.

Comparison Students and Staff

The survey's results delineate a distinct discrepancy in cybersecurity awareness and engagement between the staff and students within the university.

Foremost, the staff's feedback revealed a pronounced proficiency in understanding the intricacies of cybersecurity. Each staff member exhibited a comprehensive grasp of the institution's policies and guidelines pertaining to knowledge protection and cyber resilience. They unanimously attributed the human element as a significant determinant in cyber vulnerabilities, suggesting that human behavior might, at times, supersede technological shortcomings in influencing cyber risks. Notably, challenges were particularly accentuated in the HR sector, primarily concerning the safeguarding of student and employee data. Staff's recognition of these challenges highlights their instrumental role in not only being vigilant but also in fostering this vigilance within the broader university community.

On the subject of sensitive information, every staff respondent demonstrated a thorough understanding of what the institution classified as such. This deep-seated familiarity is a testament to the institution's efficacious endeavors in keeping its staff well-versed. The findings also indicate the provision of training to the staff, and a unanimous inclination among them to partake in further such sessions. Their unanimous advocacy for mandatory cybersecurity training underscores their commitment to fortifying the university's cyber environment.

To further bolster cybersecurity measures, staff proffered several recommendations. These spanned from instituting a robust contingency framework and amplifying VPN utilization to instating a more stringent access control regime. Additionally, there was a strong call for the provision of clear, role-specific guidelines and modular courses to enhance comprehension and implementation.

Conversely, the student population displayed a less nuanced understanding of cybersecurity. This disparity was palpable in areas such as policy awareness, where the majority of students indicated a lack of familiarity as opposed to the almost universal awareness among staff. Similarly, concerning the classification of sensitive information, the majority of students were found wanting in their understanding, while staff exhibited a comprehensive grasp. Both demographics, however, converged on the centrality of the human factor in cybersecurity compliance.

Further disparities arose when addressing resources and support. A majority of students felt underserved in terms of institutional resources and cybersecurity expertise. While staff responses did not overtly express this sentiment, the depth of their feedback suggested that they might have better access or visibility to available resources.

In essence, while the staff emerges as well-versed and deeply integrated within the university's cybersecurity framework, students appear to navigate with a lesser degree of information and resources. This gap in comprehension and commitment between the two core demographics underscores the imperative for the university to redouble its efforts. By adopting a more holistic approach that addresses this disparity, the institution can ensure a universally informed, vigilant, and cyber-resilient academic milieu.

Conclusion and recommendations

This chapter coalesces the diverse threads of inquiry that have pervaded our discourse. Drawing from the tapestry of insights uncovered, this section endeavors to directly address and provide answers to the posited sub-questions. Through a meticulous synthesis of the findings, we aspire to not only culminate our exploration but also proffer salient recommendations that emanate from the same.

Cybersecurity standards

What cybersecurity standards apply to Dutch universities and how is this reflected in current cybersecurity policies?

Cybersecurity Standards Adopted by Dutch Universities:

- National Cyber Security Centre (NCSC) Guidelines: The NCSC, overseen by the Ministry of Justice and Security, is pivotal in shaping national cybersecurity standards. Dutch universities widely incorporate its guidelines which focus on:
    - Risk management. Development of a secure IT infrastructure.
    - Enforcement of rigorous access controls.
    - Reporting of cybersecurity incidents for nationwide tracking.
- NIST Cybersecurity Framework: Developed by the National Institute of Standards and Technology (NIST) in the U.S., this framework provides a systematic methodology to manage security risks and is characterized by its five core functions: identify, protect, detect, respond, and recover.
- ISO/IEC 27001: A globally recognized standard, it offers a structured approach to managing information security risks, highlighting the initiation, implementation, and maintenance of an information security management system (ISMS).
- CIS Controls: Developed by the Center for Internet Security, it provides a systematic approach to managing security risks, emphasizing 20 best practices for improved security.
- SURF's Cybersecurity Maturity Model: This model evaluates universities on aspects such as policy, technology, human aspects, and governance. Compliance with this model is significant as it assists universities in identifying vulnerabilities, promotes cybersecurity awareness, ensures compliance with various laws, and enhances the university's overall reputation.

Dutch universities have strategically blended national guidelines, primarily from the NCSC, with recognized international standards like NIST and ISO/IEC 27001, further enriched by the adoption of SURF's Cybersecurity Maturity Model, illustrating a comprehensive and adaptive approach to fortify their digital landscapes against evolving cyber threats. The maturity of the involved universities have integrated risk management into their cybersecurity strategies, as advocated by NCSC, ISO/IEC 27001, and NIST. Stringent access controls, reflecting the guidelines of NCSC, have been adopted across universities. TU1 utilizes a specific TU adaptation of the ISO framework.
TU2 employs a combination of standards including SURF, ISO27001, and NEN7510. TU3 integrates the NBA Framework, along with SURF and NIST. O3, while using SURF, ISO27001, and NIST, also employs its own distinctive framework. O4 adheres strictly to SURF and ISO27001. Besides, with SURF's maturity model, universities gain an understanding of their cybersecurity posture. This aids in strengthening weak areas, fosters a culture of cybersecurity awareness, and supports alignment with laws like the GDPR and the Higher Education and Scientific Research Act. Institutions see a direct correlation between the maturity level of their cybersecurity framework and their overall

reputation, further motivating adherence to these standards.

In summary, Dutch universities have incorporated a blend of national and international cybersecurity standards, showing a holistic and comprehensive approach. While they primarily adhere to guidelines set by NCSC, there's a prominent role played by international standards like NIST and ISO/IEC 27001. The adoption of SURF's Cybersecurity Maturity Model also indicates the priority placed on continual evaluation and improvement in cybersecurity measures. This multifaceted approach signifies the dedication of Dutch universities to safeguard their digital landscapes against evolving cyber threats.

Influencing factors

What factors stimulate or prevent universities from implementing Cyber Security standards and measures?

Factors influencing the implementation of cybersecurity standards and measures within Dutch universities are multifaceted, reflecting the intricate mesh of organisational, technical, and human elements inherent to academic institutions.

Limited resources present a significant challenge, as universities often grapple with the dilemma of allocating budgets between academic activities and cybersecurity. This constraint can hinder their ability to acquire advanced technologies and skilled personnel necessary to enhance their cyber defenses.

The complexity of cybersecurity adds an additional layer of challenge. As technologies and methods evolve rapidly, universities may find it difficult to keep up with the latest advancements. The dynamic nature of cybersecurity requires not only technical expertise but also a deep understanding of its many intricacies.

The prevailing culture within universities can have both positive and negative effects. On one hand, some academic institutions may not take cybersecurity seriously due to a lack of understanding about the potential cyber threats and the importance of protecting data. This casual attitude can make cybersecurity a lower priority, possibly overshadowed by other operational or educational activities. On the other hand, factors like university politics and the autonomy of faculties can also influence cybersecurity practices. For example, this autonomy can unintentionally lead to a fragmented approach to cybersecurity, with each faculty following its own path, potentially resulting in inconsistencies.

Additionally, the human factor remains pivotal. Beyond the sophisticated technological tools lies the challenge of fostering awareness, instilling training, and securing the active participation of the vast tapestry of university stakeholders, from staff and students to researchers. This human-centric approach becomes even more imperative given the intricacies of university politics, individual attitudes, and the democratic decision model that underscores the governance in such institutions.

However, amid these challenges, there are also positive factors at play. The spirit of open science, the proactive approach of some universities regarding ethical considerations, and active government support act as catalysts. Additionally, students often play a crucial role in advocating for cybersecurity, emphasizing the importance of strong defenses. This combination of influencing factors, both hindering and propelling, ultimately shapes the cybersecurity stance of Dutch universities. The responsibility rests on these institutions to navigate this complex terrain, finding a balance between challenges and opportunities, in order to establish a resilient and robust cybersecurity framework.

Legal and ethical issues

What legal and ethical issues play a role in drafting and implementing cybersecurity policy for Dutch universities?

Legal and ethical considerations are closely intertwined when it comes to developing and implementing strong cybersecurity policies for Dutch universities. These educational institutions face a significant challenge, not only in keeping up with the ever-changing digital landscape but also in meeting the stringent requirements set by both Dutch and European Union legal frameworks.

The European Union's General Data Protection Regulation (GDPR) plays a pivotal role in this discussion. Introduced with the commendable aim of strengthening data privacy for EU citizens, its profound impact resonates throughout organizational structures. Universities, which hold extensive personal data, face the challenging task of ensuring strict compliance with GDPR. This regulation emphasizes the key principles of consent, transparency, and accountability, necessitating not only a technological transformation but also an organizational culture aligned with these principles. Compliance entails clear justifications for data collection, rigorous data protection measures, and ensuring that data usage aligns with its stated purpose. The financial consequences of non-compliance underscore the urgency of integrating these principles into the core of institutional practices.

The legal framework for Dutch universities becomes more comprehensive when considering domestic laws. The Dutch Higher Education and Scientific Research Act (HRA) emphasizes the responsibility of universities to establish strong digital defenses, manifested in carefully crafted security and privacy policies. The Cyber Security Assessment Netherlands (CSAN) offers guidance, although it is not mandatory, to help universities enhance their cybersecurity resilience.

Additionally, regulations like the Network and Information Systems Security Act push critical institutions, including universities, into an era where digital resilience is of utmost importance. This requires both robust protective measures and transparent incident reporting. The ever-evolving nature of cybersecurity means that compliance with these regulations is not just a destination but an ongoing journey.

However, within this complex legal framework, powerful ethical considerations are deeply intertwined. The emerging field of digital ethics prompts us to reflect deeply on our moral values in an increasingly digitized world. Universities, as centers of knowledge and innovation, stand at the forefront of these ethical discussions. Their mandate goes beyond mere legal compliance. Preserving privacy, ensuring fair and equal access to digital resources, promoting a culture of responsible technology use, steadfastly protecting intellectual property, and maintaining a strong commitment to digital safety and security are the pillars of their ethical responsibility. This comprehensive duty underscores the need for universities to take a holistic approach, incorporating ethical considerations into their core, from educational methods to research practices.

Universities' perspectives provide a fascinating insight into the intersection of these legal and ethical dimensions. There is a unanimous agreement on the importance of safety and security, demonstrating a shared commitment to protecting the digital realm. However, differing views on other aspects, such as culture and equitable access, highlight the distinct challenges that each institution faces. This diverse array of shared and individual challenges, shaped by unique institutional cultures, resources, and experiences, underscores the need for a customized approach to cybersecurity. At the same time, the emphasis on ethical considerations, whether through dedicated departments or collaborative efforts with legal experts, reinforces the idea that cybersecurity is not only about technological defenses but also about moral integrity.

In essence, as Dutch universities navigate the digital era, they find themselves walking a fine line. On one side, they are bound by strict legal requirements, and on the other, they are guided by deep ethical commitments. The interplay between these two imperatives will define the path of their cybersecurity journey in the years ahead.

Experiences Staff & Students

What experiences and opinions do employees at Dutch universities have with regard to safeguarding knowledge security?

Employees at Dutch universities, as presented by the survey results, provide a multidimensional perspective on the state of knowledge security within these institutions.

Firstly, while most respondents associated with TU1 had not experienced a direct compromise of their data, their overall awareness of the institution's cybersecurity policies and guidelines was wanting. This unfamiliarity extended to understanding what constitutes sensitive information, a foundational aspect of any cybersecurity protocol. It's evident that while technical breaches might not be rampant, the perceptual and informational gaps pose significant vulnerabilities. This lack of familiarity and understanding suggests that universities may not be effectively communicating their cybersecurity strategies and policies or that the information provided is not accessible or clear to all university members.

The human factor was recurrently identified as a significant influence on the implementation and adherence to cybersecurity measures. This aligns with global cybersecurity insights which posit human error as a primary vulnerability. This perception also ties in with the emphasis on the cultural aspect, hinting that behavioural nuances and entrenched habits might hinder optimal cybersecurity practices.

On the matter of resources and expertise, the narrative is dual-faceted. While over half the respondents felt that the university has been somewhat supportive in offering cybersecurity resources, an equally significant majority believed that there's a dearth of necessary resources and expertise for effective cybersecurity practices. This dichotomy underscores a potential misalignment between the resources provided by universities and the actual needs or expectations of their employees. Furthermore, the expressed interest in training, both from a reception and advocacy standpoint, underscores the collective appetite for more informed and actionable cybersecurity practices.

The Likert scale analysis further deepens this narrative. A significant majority, while considering cybersecurity as a priority, feel that the university's investment in the area is merely average. There's a variance in the perceived urgency and consequences of cybersecurity breaches, and the majority's moderate self-perception of skill in recognising and reporting security incidents points towards an environment where cybersecurity awareness is perhaps not optimal but not entirely neglected.

Insights from the open-ended responses lay bare the nature of threats that employees are most concerned about: phishing attacks and data breaches, both of which are predominantly human-centric vulnerabilities. Their emphasis on the human factor and cultural barriers aligns with this concern. The feedback provided, focusing on clearer information, workshops, hiring skilled staff, and more, paints a picture of employees who are acutely aware of the challenges and are proactively suggesting remedies.

The comparison between students and staff crystallises the state of cybersecurity within the university from a demographic standpoint. Staff, understandably owing to their roles and longer tenure within the institution, demonstrate a more comprehensive grasp of cybersecurity protocols and the institution's approach towards it. Their understanding of

the nuances, evident awareness of the role of human behaviour, and their advocacy for mandatory training suggests a demographic that is not just informed but also invested in enhancing the cybersecurity posture of the university.

Students, on the other hand, depict a less informed and less engaged demographic. Their lack of familiarity with policies and what constitutes sensitive information, juxtaposed against the staff's deeper understanding, delineates a clear need for targeted awareness and training campaigns.

In conclusion, employees at Dutch universities, both staff and students, demonstrate varying degrees of engagement and understanding of knowledge security. While the staff emerges as a demographic that is deeply informed and actively engaged, students, who arguably represent the future of the institution, present a clear opportunity for universities to enhance their cybersecurity outreach and training. The overarching sentiment suggests that while Dutch universities have made strides in safeguarding knowledge security, there's an evident need for more targeted and effective communication, training, and resource allocation to ensure a comprehensive and universally resilient cybersecurity framework.

Conclusion

"How should the cybersecurity policies of Dutch universities be designed to mitigate cyber threats to ensure knowledge security?"

By embracing a holistic and comprehensive approach, encompassing technical, human, and organizational facets, Dutch universities can effectively mitigate cyber threats, ensuring the security of their knowledge repositories and upholding their reputation in the academic world.

Policy Proposition
Cybersecurity policy in Dutch Universities

The recent surge in cyberattacks targeting academic institutions has unveiled the vulnerabilities inherent to Dutch universities. Given the paramount importance of universities as hubs of knowledge and their reliance on digital technologies, there is an urgent imperative to bolster cybersecurity measures to safeguard the integrity of academic data and research. This policy proposal has been crafted to provide a holistic approach to cybersecurity in higher education, ensuring a secure digital milieu for both students and staff.

Objective:
To devise a comprehensive cybersecurity framework for Dutch universities, targeting the mitigation of cyber threats and safeguarding academic knowledge integrity.

Target Audience:
This policy proposal has been specifically crafted for Dutch universities. It is designed with the understanding that while the primary beneficiaries are the universities themselves, its broader impact will resonate with a multitude of stakeholders. University leadership, academic staff, students, IT and cybersecurity departments, as well as external collaborators and research partners, all stand to gain from its successful implementation. Additionally, policymakers concerned with the larger implications of cybersecurity in higher education will find valuable insights within this proposal. By bolstering digital defenses and cultivating a culture of cybersecurity, the entire academic community in the Netherlands will be better positioned against potential threats, ensuring the safeguarding of academic data and the continuity of academic endeavors.

Proposed Policy Measures:

1. Standardization and Frameworks:

- Mandatory Adoption: All universities are required to adhere to the NCSC guidelines as well as the stipulations of the GDPR.
- Flexible Integration: Based on institutional needs and infrastructure, supplementary standards like NIST, ISO/IEC 27001, CIS Controls, and SURF's Cybersecurity Maturity Model may be incorporated.
- Uniformity: There should be a pursuit of a consistent strategy across all faculties to avert fragmentation of cybersecurity policies.

2. Financial and Technical Support:

- Budget Allocation: Universities should designate a specific budget for cybersecurity, prioritizing both technological and human-centric facets of security.
- Technological Enhancements: Invest in cutting-edge cybersecurity technologies and tools to proactively address threats.

3. Awareness and Training:

- Compulsory Training: Implement mandatory cybersecurity training sessions for all staff and students to augment awareness and proficiency.
- Communication Strategy: Design a lucid and accessible communication strategy to educate staff and students on cybersecurity protocols, risks, and best practices.

4. Legal and Ethical Considerations:
- Compliance Team: Constitute a compliance team to ensure all cybersecurity initiatives align with national and EU regulations, notably the GDPR and the Higher Education and Scientific Research Act.
- Ethical Council: Contemplate establishing an ethics council focused on digital ethics, ensuring that cybersecurity measures incorporate ethical considerations.

5. Feedback and Continuous Evaluation:
- Feedback Mechanism: Establish channels for staff and students to share feedback and concerns pertaining to cybersecurity.
- Annual Review: Undertake annual cybersecurity evaluations to ascertain the efficacy of the policy and pinpoint areas for enhancement.

Dutch universities stand at the nexus of knowledge and technology. It is thus paramount for them to roll out an avant-garde cybersecurity policy that's both proactive and adaptive, taking into account both technological and human dynamics. By investing in the right technology, fostering training and awareness, and underpinning solid legal and ethical foundations, Dutch universities can fortify themselves against cyber threats and secure their intellectual treasury.

Discussion

This study has provided a comprehensive analysis of the state of cybersecurity in Dutch universities, the application of national and international cybersecurity standards, legal and ethical considerations, as well as recommendations for future action. These findings have broad implications for both academia and industry. In academia, these insights can foster discussions on the balance between information sharing and knowledge safety. They can also inform university policies and guidelines on cybersecurity, enabling the creation of more secure academic environments. In the business sector, especially for companies collaborating with universities on research and development projects, understanding the security landscape is crucial. Companies can use these findings to assess their risks and adapt their own cybersecurity measures when engaging with universities.

Despite its contributions, this study has several limitations. First, it primarily relies on publicly available literature, which means that more recent developments in cybersecurity threats and countermeasures may not be included. Second, the study is limited to a generic discussion of Dutch universities, without delving into specific institutions or disciplines. Cybersecurity needs may vary significantly across different institutions and academic disciplines, and these nuances are not captured in this study.

Given these limitations, several future research directions are suggested. First, empirical studies examining specific cybersecurity strategies employed by individual Dutch universities could provide more nuanced and actionable insights. Second, future research could focus on the intersection between cybersecurity and specific academic disciplines, such as digital humanities or data-intensive sciences, which might have unique cybersecurity needs. Lastly, longitudinal studies could shed light on how cybersecurity threats and countermeasures evolve over time, informing the development of more dynamic and adaptable cybersecurity strategies.

Additionally, this study will rely on self-reported data from interviews and surveys, potentially introducing response biases. Some research methods, such as expert interviews and surveys, can be time-consuming to conduct, especially when it comes to reaching a representative sample of the target population. Besides, surveys rely on participants' personal opinions and experiences, which can lead to subjectivity and limitations in generalising results, such as social desirability bias, response bias, and sample bias. In any research endeavor, particularly those relying on self-reported data from participants, it is imperative to consider the potential for response bias, notably in the form of socially desirable responding (SDR). Socially desirable responding refers to the tendency of respondents to answer questions in a manner that would be viewed favorably by others, often leading to an over-reporting of 'positive' behaviors or under-reporting of 'negative' or undesirable behaviors. Given the nature of this study, which delves into the realm of cybersecurity awareness and practices, there is a possibility that participants might overstate their knowledge or compliance with security guidelines to align with perceived institutional or societal expectations. Such biases could skew the results, painting a rosier picture of cybersecurity preparedness than might actually be the case. It's crucial to recognize this limitation when interpreting the data and drawing conclusions, and it underscores the importance of implementing multiple methods of data collection or validation when assessing such subjective areas of inquiry.

To address these limitations, the study will employ various strategies, such as ensuring anonymity, using multiple data sources, and employing a representative sample. Regarding interviews, finding suitable experts on cybersecurity, universities, and knowledge security can be difficult, especially if they are unavailable due to work commitments or other reasons.

In addition, it could be possible that universities are not willing or able to share their policy documents and cybersecurity practices due to security or confidentiality issues, which can make it difficult to get a complete picture of Dutch universities' policies.
The results of the study may be applicable only to the Dutch context and may not be fully generalizable to other countries or institutions. While the study will focus on Dutch universities, the findings may have implications for academic institutions globally, considering the shared nature of cybersecurity challenges. However, due to the ever-evolving nature of cybersecurity threats, the conclusions drawn from this research are subject to the information available up to the time of the study.

Furthermore, the study relies on existing data sources such as policy documents, cybersecurity reports, and academic literature, which may have inherent limitations, such as bias, inconsistency, and incompleteness. To mitigate these limitations, the study will conduct a rigorous review of the data sources and use multiple sources to triangulate findings.

Despite these limitations, the study aims to address the research question and contribute to the understanding of the cybersecurity policy landscape of Dutch universities. By acknowledging the limitations, the study can improve the validity and reliability of its findings and provide actionable recommendations for policymakers. While the challenge of ensuring knowledge safety and cybersecurity in Dutch universities is complex, it is an essential endeavour. Through continued research and dialogue, universities, businesses, and policymakers can work together to create more secure digital landscapes for the pursuit of knowledge.

References

Ad Valvas (2022, December 14). 2,8 miljoen extra naar kennisveiligheid universiteiten. Advalvas. https://www.advalvas.vu.nl/nieuws/28-miljoen-extra-naar-kennisveiligheid-universiteiten

AIVD (2021, June 2021). Cyberaanvallen door statelijke actoren: zeven momenten om een aanval te stoppen. Algemene Inlichtingen- en Veiligheidsdienst. AIVD. https://www.aivd.nl/documenten/publicaties/2021/06/28/cyberaanvallen-door-statelijke-actoren---zeven-momenten-om-een-aanval-te-stoppen

AIVD & MIVD. (2017). Bent u zich bewust van de risico's van cyberspionage? Ministerie van Binnelandse Zaken en Koninkrijksrelaties (AIVD) & Ministerie van Defensie (MIVD). https://integraalveilig-ho.nl/wp-content/uploads/Bentuzichbewustvanderisicosvancyberspionage22mei2017.pdf

Allen, I. E., & Seaman, C. A. (2007). Likert scales and data analyses. Quality Progress, 40(7), 64-65.

Bahl, R. W. (2020). Fair access to infrastructure services: The role of governance. In Infrastructure governance and finance (pp. 37-54). Routledge.

Bakker, M. (2022, September 15). Regeringspartijen willen strenger toezicht op aanpak kennisveiligheid door universiteiten. ScienceGuide. https://www.scienceguide.nl/2022/09/regeringspartijen-willen-strenger-toezicht-op-aanpak-kennisveiligheid-door-universiteiten/

Bambauer, D. E. (2014). Ghost in the network. University of Pennsylvania Law Review, 162, 1011.

Bennett, C. J. (2016). Privacy advocates, privacy law and the surveillance society. Surveillance & Society, 4(1/2), 132-138.

Bilge, L., & Dumitras, T. (2012). Before we knew it: an empirical study of zero-day attacks in the real world. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 833-844).

Bishop, M. (2003). Computer security: Art and science. Addison-Wesley.

Boone, H. N., & Boone, D. A. (2012). Analyzing likert data. Journal of extension, 50(2), 1-5.

Booth, A., Sutton, A., & Papaioannou, D. (2016). Systematic approaches to a successful literature review (2nd ed.). Sage Publications.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Braun, V., Clarke, V., & Weate, P. (2016). Using thematic analysis in sport and exercise research. In Routledge handbook of qualitative research in sport and exercise (pp. 191-205). Routledge.

Burnett, S., & Feamster, N. (2019). Making sense of cybersecurity: a simple guide to protecting your business from cyber attacks, data breaches, and online criminals.

Cate, F. H. (2015). Principles of Internet Policy. Law & Contemporary Problems, 79, 1.

Chen, S., Ramamurthy, K., & Wen, K. (2019). Protecting against network intrusions. In Cybersecurity in China (pp. 95-110). Springer.

Cimpanu, C. (2019). Ransomware: An executive guide to one of the biggest menaces on the web. ZDNet. https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/

Clement, A. (2017). Disconnected: Youth, new media, and the ethics gap. MIT Press.

Clement, A. (2017). The Snowden revelations and the networked individual. Surveillance & Society, 15(2), 347-353.

Creswell, J. W., & Plano Clark, V. L. (2017). Designing and conducting mixed methods research (3rd ed.). Sage Publications.

Daries, J. P., Reich, J., Waldo, J., Young, E. M., Whittinghill, J., Ho, A. D., ... & Chuang, I. (2014). Privacy, anonymity, and big data in the social sciences. Communications of the ACM, 57(9), 56-63.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, 32(2), 179-194.

Digitale Overheid. (2020, June 16). Inspectie: Universiteit Maastricht was niet goed voorbereid op ransomware-aanval. Digitale Overheid. https://www.digitaleoverheid.nl/nieuws/inspectie-universiteit-maastricht-was-niet-goed-voorbereid-op-ransomware-aanval/

Dutch Ministry of Justice and Security. (2018). Network and Information Systems (Security) Act. https://wetten.overheid.nl/BWBR0040638/2019-04-21

Evans, S. (2018). Theme development in qualitative content analysis and thematic analysis. Journal of Nursing Education and Practice, 8(5), 100-110.

European Union Agency For Cybersecurity. (2021). Raising awareness of cybersecurity: A Key Element of National Cybersecurity Strategies. ENISA.

Fish, S. (2014). Versions of academic freedom: From professionalism to revolution. University of Chicago Press.

Furnell, S. (2014). Cybersecurity culture: Counteracting cyber threats through organizational learning and training. In E. Alkhalifa (Ed.), Security and privacy assurances in advancing technology (pp. 1-16). IGI Global.

Gopal, R. D., & Sanders, G. L. (1997). International software piracy: Analysis of key issues and impacts. Information Systems Research, 8(4), 380-397

Greenleaf, G. (2018). Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. Privacy Laws & Business International Report, 147, 10-13.

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). Applied thematic analysis. Sage.

Hadnagy, C., & Fincher, M. (2015). Phishing dark waters: The offensive and defensive sides of malicious emails.

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-real-time-sensor framework. Computers & Security, 73, 50-67.

Hillman, A. L., & Wollmann, H. (2016). Ethical issues in policymaking.

Hudson, D., & McLean, C. (2021). Ethics and public policy: A philosophical inquiry. Routledge.

Hugl, U. (2011). Reviewing person's value of privacy of online social networking. Internet Research, 21(4), 384-407.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94-100.

Iv-Ho, P. (2022, February 16). Kennisveiligheid - Platform Integrale Veiligheid Hoger Onderwijs. Platform Integrale Veiligheid Hoger Onderwijs. https://integraalveilig-ho.nl/thema/kennisveiligheid/

Johnson, D. G. (2015). Computer ethics. Prentice Hall Press.

Johnson, M. (2015). Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare. CRC Press.

Kabay, M. E. (2010). Legal and ethical aspects of cybersecurity. In Cyber Warfare and Cyber Terrorism (pp. 309-314). IGI Global.

Karran, T. (2007). Academic freedom in Europe: A preliminary comparative analysis. Higher Education Policy, 20(3), 289-313.

Kaspersky Lab. (2017). What is malware? And how to protect against it. Kaspersky. https://usa.kaspersky.com/resource-center/threats/malware-classifications

King, N., Horrocks, C., & Brooks, J. (1995). Interviews in qualitative research. Sage Publications.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & security, 28(7), 509-520.

Kritzinger, E., & Smith, E. (2018). Cyber security education in higher education institutions. International Journal of Information and Computer Security, 10(2-3), 189-207.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2007). School of phish: a real-word evaluation of anti-phishing training. SOUPS.

Marks, L. (2007). Triangulation: A democratic approach to mixing methods. Qualitative Research in Psychology, 4(2), 135-146.

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. Global Qualitative Nursing Research, 2, 2333393615597674.

Ministerie van Onderwijs, Cultuur en Wetenschap. (2022, April 1). Wat is kennisveiligheid? Loket Kennisveiligheid. https://www.loketkennisveiligheid.nl/kennisveiligheid

National Cyber Security Centre. (2019). Cyber Security Assessment Netherlands. https://english.ncsc.nl/publications/cyber-security-assessments/2019/cyber-security-assessment-netherlands-csan-2019

National Cyber Security Centre. (2021). Annual Review 2021 : Making the UK the safest place to live and work online. In National Cyber Security Centre. https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf

Nationale Leidraad Kennisveiligheid. (2022, January). Veilig internationaal samenwerken. Rijksoverheid. https://open.overheid.nl/documenten/ronl-05d0f839b62c8ad96fa1bd3ca8d3f487c6f5c7d6/pdf

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

NOS. (2021, 17 februari). Cyberaanval op UvA en HvA: “Toegang derden tot ict-systemen”. https://nos.nl/artikel/2369091-cyberaanval-op-uva-en-hva-toegang-derden-tot-ict-systemen

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International Journal of Qualitative Methods, 16(1), 1609406917733847.

Penney, J. (2017). Chilling effects: Online surveillance and Wikipedia use. Berkeley Tech. LJ, 31, 117.

Pritchard, M. S. (2016). Responsible stewardship of IT resources. In L. Floridi (Ed.), The Cambridge handbook of information and computer ethics (pp. 197-214). Cambridge University Press.

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698. https://doi.org/10.1016/j.future.2016.11.009

Rowe, N. C. (2010). The ethics of cyberweapons in warfare. International Journal of Technoethics (IJT), 1(1), 20-31.

Saldana, J. (2016). The coding manual for qualitative researchers. Sage.

Schober, J. (2020). Cybersecurity and freedom on the internet. Journal of Cyber Policy, 5(1), 81-96.

Scholte, W., & Douma, J. (1999). Inleiding in de psychologie. McGraw-Hill.

Seale, J. (2013). E-learning and disability in higher education: Accessibility research and practice. Routledge.

Shackelford, S. J., Proia, A., Martell, B. S., & Craig, A. (2019). Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices. Texas International Law Journal, 50(2), 305-346.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41.

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Solove, D. J. (2011). Nothing to hide: The false tradeoff between privacy and security. Yale University Press.

SURF (2020). Cybersecurity Framework for Higher Education Institutions. Retrieved from https://www.surf.nl/en/knowledge-base/2020/cybersecurity-framework-for-higher-education-institutions.html

SURF (2021, November 8).SURF Informatieveiligheidsbeleid. https://www.surf.nl/files/2022-07/211108-surf-informatieveiligheidsbeleid-versie-1.2-def.pdf

Taddeo, M., & Floridi, L. (2018). Regulating artificial intelligence and robotics: Ethics by design in a digital society. Contemporary Issues in Law, 14(1), 129-148.

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. Network Security, 2011(8), 16-19. https://doi.org/10.1016/S1353-4858(11)70086-1

Tavani, H. T. (2011). Ethics and technology: Controversies, questions, and strategies for ethical computing. Wiley.

Vacca, J. R. (2005). Computer forensics: Computer crime scene investigation. Charles River Media.

Van Brakel, R., & Chis, A. (2018). Higher Education and the Cybersecurity Skills Gap: An analysis of the cybersecurity skills gap in the higher education sector and a proposal for an educational model to address this gap. Journal of Computer and Information Systems, 61(2), 132-140. DOI: 10.1080/08874417.2018.1517766

Van den Berg, B., & Van den Hoven, J. (2013). ICT and Value Sensitive Design. In P. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.), ICT and Society (pp. 67-72). Springer.

Van der Meulen, R. (2016). The Dutch approach to threats in the digital domain. International Journal of Cyber Warfare and Terrorism (IJCWT), 6(2), 39-46.

Verhoeven, J. (2019). Cyber security in higher education: adaptation of the Dutch NIST Cyber security framework by universities. International Journal of Cyber-Security and Digital Forensics, 8(4), 345-358.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). A Practical Guide, 1st Ed., Cham: Springer International Publishing.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102.

Weller, M. (2014). The battle for open: How openness won and why it doesn't feel like victory. Ubiquity Press.

Westin, A. F. (1967). Privacy and freedom. Atheneum.

Wynn, D., & Eckert, C. (2017). Perspectives on iteration in design and development. Research in Engineering Design, 28(2), 143-167.

Yu, S., Tian, Y., Guo, S., & Wu, D. (2014). Can we beat DDoS attacks in clouds? IEEE Transactions on Parallel and Distributed Systems, 25(9), 2245-2254. https://doi.org/10.1109/TPDS.2013.2295806

Zimmer, M. (2010). Surveillance, privacy and the ethics of vehicle safety communication technologies. Ethics and Information Technology, 12(2), 137-149.

4TU.Federatie. (z.d.). TU Delft. https://www.tudelft.nl/over-tu-delft/strategie/samenwerking-universiteiten/4tufederatie#:~:text=De%20TU%20Delft%2C%20Universiteit%20Twente,als%20internationaal%2C%20verder%20te%20versterken.

Appendices

Appendix A: Interview

This appendix provides an in-depth explanation of the interview methodology employed in this study. It outlines the preparation for the interviews, the structure and design of the questions, and the technique used for recording and transcribing the interviews. The appendix also details the approach taken for the analysis of the interview data, including the steps involved in coding and thematic analysis. By including this information, the goal is to provide transparency and facilitate a thorough understanding of the processes that led to the research findings.

Appendix A.1: Informed Consent

Prior to participation in the interviews, all interviewees were presented with a clear and thorough informed consent form, following the ethical guidelines for research. The consent form highlighted the objectives and methods of the study, emphasising the voluntary nature of participation and their right to withdraw at any point, without facing any consequences. The form further clarified that their responses would be anonymized, ensuring that no identifiable information would be linked to the data used in the final report. Only after providing written consent did the interviewees participate in the research. This approach ensured transparency, respect for the participants' autonomy, and adherence to ethical standards throughout the research process.

Please note that there has been a change in the schedule of the researcher's thesis period. As per the initial plan, the thesis period was expected to end in July 2023. However, it has been extended and will now conclude in August 2023 (Informed Consent Form - Point 5).

You are invited to participate in the research titled 'An Investigation of Influencing Factors Which Potentially Hamper Universities in the Adoption of Cyber Security Standards in Their Policy to Ensure Knowledge Security'. This research is conducted by Josephine Bissumbhar, a Master's student at TU Delft and a graduate intern at Ernst & Young.

The goal of this research is to elucidate these factors by providing recommendations for the implementation of necessary cyber security measures to limit and prevent cyber threats. It will take approximately 60 minutes. The data will be used for processing the practical application of cyber security policy of Dutch universities in the study. You are asked to answer questions, estimate factors at certain levels, and share your own experience/opinion based on experience and expertise.

As with any online activity, the risk of a data breach exists. Attempts will be made to keep your answers confidential and minimise the risks by anonymizing the data where necessary.

Your participation in this research is entirely voluntary, and you can withdraw at any time without giving a reason. You are free not to answer questions.

Principal Investigator:
Josephine Bissumbhar
j.s.bissumbhar@student.tudelft.nl

Responsible Researcher:
Pieter van Gelder
p.h.a.j.m.vangelder@tudelft.nl

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
A: GENERAL AGREEMENT – RESEARCH GOALS, PARTICIPANT TASKS AND VOLUNTARY PARTICIPATION		
1. I have read and understood the research information dated [DD/MM/YYYY], or it has been read to me. I have had the opportunity to ask questions about the research, and my questions have been answered to my satisfaction.	☐	☐
2. I voluntarily participate in this research, and I understand that I can refuse to answer questions and can withdraw from the study at any time, without having to give a reason.	☐	☐
3. I understand that my participation in the research involves the following: - Audio recording for transcription purposes, facilitating easier analysis of the interview. After transcription, the audio recording will be destroyed. - During the interview, written notes are taken of the main points of the answer to the question. - As far as possible, efforts are made to minimise the personal data collected.	☐	☐
4. I understand that my participation in the research is not compensated.	☐	☐
5. I understand that the researcher's thesis period ends in July 2023.	☐	☐
B: POTENTIAL RISKS OF PARTICIPATING (INCLUDING DATA PROTECTION)		
6. I understand that my participation entails the following risks: - Potential digital and/or physical/mental discomforts as a result of participation in the research. I understand these risks are minimised by: - Prior to participation, the nature of the research will be discussed, and whether the interview takes place physically or mentally. - Participants have the right to stop the research at any time, without giving a reason. - The researcher will be available for questions and any concerns from the participants during and after the research.	☐	☐

7. I understand that my participation means that personal identifiable information and research data are collected, with the risk that I can be identified from this. - The existence of personally identifiable information can lead to unintentional disclosure of sensitive data, which can harm the participant's privacy. - In the event that the collected information is made public, participants may run the risk of their personal or professional reputation being harmed. - If personally identifiable information falls into the wrong hands, it can lead to identity theft or fraud. Personally identifiable information will be anonymized or pseudonymized to reduce the chance of re-identification.	☐	☐
8. I understand that under the General Data Protection Regulation (GDPR), some of this personally identifiable research data is considered sensitive, namely: - Data can be collected and processed that relate to potential criminal activities with the respective university as the target. - It is possible that data is collected on the political views of the participants.	☐	☐
9. I understand that the following steps are taken to minimise the risk of a data breach, and my identity is protected in the following ways in case of a data breach: - Anonymous data collection: To minimise the risk of identification, data are collected anonymously at the participant's request. This means that no direct personally identifiable information will be linked to the collected data. - (Pseudo-) anonymization or aggregation: If necessary, the collected data are pseudonymized or aggregated. This means that personally identifiable information is replaced with a unique code or that data are grouped together so that individual identification is no longer possible. - Transcription: The audio files that are collected are transcribed into text. This can help further reduce identifiable information and protect the privacy of the participants.	☐	☐
10. I understand that the personal information that is collected about me and can identify me, such as name, position, and any background information will not be shared at my request.	☐	☐
11. I understand that the personal data that is collected about me will be destroyed when I indicate that I want this.	☐	☐

C: RESEARCH PUBLICATION, DISSEMINATION AND APPLICATION		
12. I understand that after the research, the (anonymized) information will be used for: - The researcher's thesis report. Possibly the research results will be shared with interested interviewees. - It is possible that the research results will be published. This can contribute to the broader knowledge in the field and inform the scientific community about the findings.	☐	☐
13. I give permission to quote my answers, ideas, or other contributions in resulting products.	☐	☐
14. I give permission to use my name, position, and respective university for quotes in resulting products.	☐	☐
D: (LONGTERM) DATA STORAGE, ACCESS AND REUSE		
15. I give permission for the (anonymized) data that are collected about me to possibly be archived in the TUDelft Repository so that they can be used for future research and education.	☐	☐

Signatures

_____	_____	_____
Participant's name	Signature	Date

I, the researcher, declare that I have correctly read the information and consent form to the potential participant and, to the best of my ability, have ensured that the participant understands what he/she is voluntarily agreeing to.

_____	_____	_____
Participant's name	Signature	Date

Contact information of the researcher for further information:

Josephine Bissumbhar
j.s.bissumbhar@student.tudelft.nl

Appendix A.2: Interview Questions

Each interview conducted in this research adhered to a predefined procedure to ensure consistency and uphold ethical standards. Initially, the informed consent was verbally confirmed by the interviewees at the onset of the conversation. Subsequently, a written version of the informed consent statement was sent to the interviewees to ensure they were thoroughly informed about the nature and objectives of the research. Next, the nature and purpose of the thesis was explained to the participants, emphasising the value of their contribution towards developing a deeper understanding of the research topic.

Every interview was structured in three segments. The first segment comprised introductory questions designed to comprehend the background and context of the interviewees. These questions enabled us to gain a clear understanding of their experiences and perspectives. The second segment of the interview was the main section, where the core research questions were discussed. These questions aimed to elicit detailed and thorough responses that illuminate the central themes of my thesis. The third and final segment of the interview was dedicated to concluding questions, where the interviewee's opinion took centre stage. Here, the participants had the opportunity to freely express their views and beliefs about the subject. These closing questions served to fully comprehend and document the interviewee's thoughts, which was critical for the qualitative analysis of the data.

The pre-formulated questions for the interview are shown below. Please note that during the interview, there is always the possibility to delve deeper into a specific topic or supplement the provided structure based on the flow of conversation. The aim is to foster a comprehensive understanding and ensure we cover all relevant aspects of the subject matter.

A) Introductory Questions

1. Could you provide some information about yourself and your role?
2. Has University X ever experienced a cyber attack or unwanted transfer of knowledge?
3. How is the Cyber Security department within University X structured?
    a. Is it a separate department?
    b. Part of the IT department?
4. What role do the university's executives play in promoting Cyber Security and safeguarding knowledge protection?
5. Who is the decision-making party regarding which policy changes/measures need to be taken (who decides what is the priority) and on what basis is this decision made?
    a. Who within the university is ultimately responsible for compliance with the Cyber Security policy and thus for the safeguarding of knowledge security?

B) Main Part

6. What do you consider to be the trends and developments in the field of Cyber Security that are relevant for Dutch universities?
7. What are the current cybersecurity standards applicable to Dutch universities and how are these reflected in the current cybersecurity policy of University X?
8. What are the potential costs and benefits of implementing Cyber Security standards and measures for the university?
9. What is the budget?
   What are the potential (financial) consequences for universities if they do not take adequate Cyber Security measures?
10. What influencing factors (either encouraging or inhibiting) affect universities in implementing Cyber Security standards and measures?
11. How do the following factors play a role in the introduction or compliance with Cyber Security measures?

	Highly restrictive	Restrictive	No influence	Stimulating	Highly stimulating
Limited Resources					
Complexity					
Culture					
Priority					
Human factor					

12. What resources are available to the university to assist them in implementing Cyber Security standards and measures?
13. Are there challenges that the university faces in complying with cybersecurity standards and policy?
    a. If so, which ones?
    b. Technical and technological challenges?

14. What legal issues are involved in drafting and implementing cybersecurity policy for Dutch universities?
    a. Legislation and regulation
15. Does the cyber policy take into account cyber ethics?
    a. If so, in what way?

16. How do you prioritise the following cyber ethics topics?

	1 - Highest priority	2	3	4	5 - Lowest priority
Protection of privacy					
Fair Access					
Responsible Use					
Intellectual property					
Safety and security					

17. Are students and employees involved and made aware of the importance of Cyber Security and knowledge protection? If so, how?

C) Concluding questions

18. Would a collaboration between universities help in addressing common challenges in the field of Cyber Security?
    a. If so, how?
19. Would collaboration between universities and external parties, such as government agencies or industry experts, promote the implementation of Cyber Security standards? SURF?
20. Cyber Security policy University X:
21. In short, how can the university ensure that the likelihood of cyber attacks is minimised and knowledge security is safeguarded?
22. Is the Cyber Security policy publicly accessible?

Appendix A.3:Interview Transcriptions

The transcription and translation process followed for the interviews is conducted as part of this research study. The original interviews were held in Dutch and were audio-recorded with the explicit permission of the interviewees, as granted through the informed consent process. In order to maintain the integrity and accuracy of the responses, the first step was to transcribe the Dutch audio recordings verbatim. This transcription process was performed meticulously to ensure that all details were accurately recorded and the essence of the responses was preserved. Following this, to make the data accessible to a broader audience and to fit within the context of this English-language report, the transcriptions were translated into English. This translation was carried out with utmost care to retain the original meaning and nuances of the interviewee responses, adhering to the principle of 'equivalence of meaning' rather than literal word-for-word translation. Please note that while every effort has been made to ensure the accuracy of these translations, some minor discrepancies may inevitably occur due to the inherent complexities of language translation.

The transcripted interviews are available upon request for those interested.

Appendix B: Questionnaire

This appendix offers a comprehensive elucidation of the survey methodology utilised in the current research. It delineates the formulation of the survey questions, the selection and recruitment of participants, and the procedure used for collecting and processing the responses. Additionally, it details the strategy adopted for the analysis of the survey data, including the statistical techniques used. The purpose of this appendix is to promote transparency and enable a deeper understanding of the steps that led to the outcomes of this research.

Appendix B.1: Survey questions

These are the questions outlined for the survey. Please note that there is an option for participants to indicate their preferred language for completion, with both Dutch and English options available. The objective is to ensure accessibility and comfort for all respondents, allowing them to provide their insights in the language they are most comfortable with.

1. Are you a student or an employee at a Dutch university ?
    a. Student
    b. Employee
2. Which Dutch university are you affiliated with ?
    a. Delft University of Technology
    b. Erasmus University Rotterdam
    c. Utrecht University
    d. Leiden University
    e. Maastricht University
    f. Eindhoven University of Technology
    g. Wageningen University & Research
    h. University of Amsterdam (UvA)
    i. University of Groningen
    j. Vrije University of Amsterdam
    k. University of Twente
    l. Tilburg University
    m. Other
3. What do you consider the biggest threat to the security of your university in terms of Cyber Security?
4. Have you ever personally experienced your data or information being compromised or stolen at the university?
    a. Yes
    b. No
5. Are you aware of the current policies and guidelines of your university regarding knowledge security and cyber security?
    a. Yes
    b. No
6. How do you think your university handles cyber security and ensures knowledge security?
7. What factors do you see as influential in the implementation and compliance of cybersecurity measures at the university?

    a. Limited resources
    b. Complexity
    c. Culture
    d. Lack of priority
    e. Human factor
    f. None of all
    g. Other
8. To what extent do you believe Cyber Security standards/measures should be a priority for Dutch universities?
    a. High priority (1) - Low priority (5)
9. To what extent do you think your university invests adequately in Cyber Security?
    a. Sufficient (1) - Insufficient (3)
10. Are there specific sectors or departments within your university where you believe Cyber Security poses a greater challenge?
    a. Yes
    b. No
11. To what extent are you aware of the urgency of Cyber Security and the potential consequences of a breach in the security of sensitive information?
    a. Very aware (1) - Very unconscious (5)
12. What role do you envision for yourself and other students/employees in promoting Cyber Security within your university?
13. How confident do you feel in your knowledge of cyber security and taking measures to ensure knowledge security?
    a. Highly skilled (1) - Not at all proficient (5)
14. Are you aware of what is considered sensitive information within your university and what is not?
    a. Yea
    b. No
15. How do you ensure the security of university data when working with confidential information?
16. Do you believe that sufficient resources and support have been provided to students and employees to help them deal with Cyber Security issues? Explain,
    a. Yes
    b. No
17. Do you think your university has enough resources and expertise to effectively implement Cyber Security? Explain.
    a. Yea
    b. No
18. How confident do you feel in your knowledge of cyber security and taking measures to ensure knowledge security?
    a. Very confident (1) - Very insecure (5)
19. Has the university provided you with sufficient information about cyber security and knowledge security?
    a. Yes
    b. No

20. Has the university provided training or guidelines for cyber security and knowledge security?
    a. Yes
    b. No
21. Would you be interested in participating in training or workshops on cyber security to enhance your knowledge and skills in this area?
    a. Yes
    b. No
22. Do you believe that mandatory training on Cyber Security should be offered to students and employees at your university?
    a. Yes
    b. No
23. How willing are you to participate in Cyber Security training if it is offered?
    a. Extremely willing (1) - Extremely unwilling (5)
24. What measures could your university take to increase the willingness of students and employees to contribute to the security of sensitive information?
25. Would you feel safer if the university took additional measures to enhance cyber security?
    a. Yes
    b. No
26. What do you believe are the most important measures that your university should take to ensure knowledge security and mitigate the threat of cyber attacks?
27. What obstacles do you see in the implementation of Cyber Security standards/measures within your university?
28. What steps could your university take to facilitate the implementation of Cyber Security standards/measures?
29. What do you believe are the key aspects that the policy regarding Cyber Security within your university should focus on?
30. Do you have any suggestions for improving the awareness of Cyber Security among students and employees at your university?
31. Do you have any suggestions for further improvements or initiatives to strengthen Cyber Security at your university?