future internet

MDPI

Review

A Systematic Review of Cybersecurity Risks in Higher Education

Joachim Bjørge Ulven † and Gaute Wangen *,†

Deptment of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU—Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway; joachiu@stud.ntnu.no

* Correspondence: gaute.wangen@ntnu.no

† These authors contributed equally to this work.

Abstract: The demands for information security in higher education will continue to increase. Serious data breaches have occurred already and are likely to happen again without proper risk management. This paper applies the *Comprehensive Literature Review (CLR) Model* to synthesize research within cybersecurity risk by reviewing existing literature of known assets, threat events, threat actors, and vulnerabilities in higher education. The review included published studies from the last twelve years and aims to expand our understanding of cybersecurity's critical risk areas. The primary finding was that empirical research on cybersecurity risks in higher education is scarce, and there are large gaps in the literature. Despite this issue, our analysis found a high level of agreement regarding cybersecurity issues among the reviewed sources. This paper synthesizes an overview of mission-critical assets, everyday threat events, proposes a generic threat model, and summarizes common cybersecurity vulnerabilities. This report concludes nine strategic cyber risks with descriptions of frequencies from the compiled dataset and consequence descriptions. The results will serve as input for security practitioners in higher education, and the research contains multiple paths for future work. It will serve as a starting point for security researchers in the sector.

Keywords: cybersecurity; higher education; university; review; risk; asset; threat; vulnerability

Citation: Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet* **2021**, *13*, 39. https://doi.org/10.3390/fi13020039

Academic Editor: Georgios Kambourakis

Received: 27 November 2020

Accepted: 28 January 2021

Published: 2 February 2021

1. Introduction

Universities and academic institutions have become lucrative targets for cyber-attacks and have already suffered multiple high impact incidents [1,2]. Academic institutions manage large amounts of valuable research, and sensitive personal data, which makes them an attractive target for cyber-criminals, espionage, and hacktivists [3]. The threat landscape consists of everything from opportunists seeking financial gain, to heavily funded state-sponsored actors who intend to steal trade secrets. Furthermore, the free flow of workforce and annual rotations of new students, guest, and employees also adds to the universities' information security (infosec) challenges. Even though academic institutions face substantial infosec risk at their institutions, the initiative of implementing infosec measures varies [4–6]. There are several cultural issues to resolve, such as balancing security measures with the academic openness and free flow of information that institutions are trying to promote [7]. Collaboration and information sharing with other researchers, both inside and outside the university is a security challenge, perhaps unseen in different industries. The interconnectivity in universities continue to increase, and the attack surface grows proportionately. Cybersecurity issues are now moving towards the board room in academia, where the traditional openness and sharing culture is being challenged by organized criminal groups such as *The Silent Librarian Campaign* [8–10]. Academia has published thousands of articles researching cybersecurity, while the HE sector itself often leaves the cybersecurity issue for the technicians to fix [5].

The best practice defines infosec risk management within the scope of assets, threats, vulnerabilities, and events [11,12]. However, identifying these within an organization can be challenging as information assets are continuously created, processed, and stored. Secondly, cyberspace's threat environment is continually changing, where new methods and tools make it is hard to identify, evaluate, and map harmful attacks to an organization. Finally, changes in organizational structure can unveil novel unaccounted vulnerabilities. Universities and higher educational (HE) institutions are regularly conducting teaching, development and research which greatly benefits society. Companies in both the private and public sector are also investing vast amounts of resources in research and development at the HE institutions (HEI). All of which is worth protecting, and as the topic grows in importance, a study of the sector's cybersecurity risks is timely. Therefore, the purpose of this article is to review the existing literature, generalize knowledge about cybersecurity risks, and study the security trends in HE. This research addresses the following research questions (RQ) for HE:

1. What are the key information assets and the associated Key Performance Indicators in HE?
2. Which are the most frequent threat events in HE?
3. Who are the common threat agents?
4. What are the most common vulnerabilities?
5. Which are the most common risks?

We address these topics using the systematic literature review method. This study does not venture into risks from violating laws and regulations given that these are region and country specific. Neither does this paper discuss or propose risk control and mitigation mechanisms in depth. The key findings of this paper is an overview of assets, threats, and vulnerabilities in HE. The article also discusses the industry's common risks at an organizational level, with generic risk management strategies. The implications are common risks HEI should mitigate, and a call for more research within these areas. The paper is written for both academics researching cybersecurity and practitioners working actively with security in HEI.

The remainder of this paper has the following structure:

- Section 2 presents the study context and provides the reader with the background knowledge, properties of the HEI, and previous work within the field.
- Section 3 describes the *Comprehensive Literature Review Model* approach of this paper.
- Section 4 provides a summary of the included and reviewed literature.
- Section 5 presents the literature review results on the information assets and key performance indicators and answers RQ 1.
- Section 6 presents the results from the literature review on cyber threats events and answers RQ 2.
- Section 7 presents the results from the literature review on threat agents and answers RQ 3.
- Section 8 presents the results from the literature review on vulnerability and answers RQ 4.
- Section 9 presents an analysis of HEI's cybersecurity risks together with a discussion of consequences as an answer to RQ 5.
- Section 10 discusses the research questions, implications, and potential future work.
- Section 11 concludes the work.

2. Background and Previous Work

In this section, we first define the terms necessary to understand the content of this paper. Furthermore, we describe some of the essential characteristics of typical of HE which distinguishes them from traditional industry and business. Lastly, we present previous work within cybersecurity in HE.

2.1. Terms and Definitions

This paper assumes that the reader is familiar with common infosec terminology, furthermore, the terms *infosec* and *cybersecurity* are used interchangeably in this paper. Infosec is the preservation of the confidentiality, integrity, and availability of information [13]. This also includes the technology that houses and transfers that information through various protection mechanisms such as policy, training and awareness programs and technology [14] (p. 5). However, infosec is not exclusively limited to these three characteristics; there are also critical characteristics such as processes, including privacy, identification, authentication, authorization, and accountability to consider. When we refer to *risk management* in this paper, we refer to the full process of managing risks, being more specific, continuously identifying, reviewing, treating and monitoring risks to achieve risk acceptance [11,12]. A common approach to infosec risk is to divide it into assets, threats, and vulnerability [11,12], commonly referred to as *the three-factor model* in risk analysis. There are several ways to conduct an infosec risk assessment (ISRA). Still, the majority share the similarity of first, identifying valuable assets in an organization, before identifying threats that might potentially cause harm to these assets [12]. The final step before risk analysis is identifying and evaluating vulnerabilities present in the organization. Risk is then an event caused by the threat exploiting a vulnerability to harm an asset. This event has an associated consequence and likelihood [11,12].

Primary *assets* are either information or business processes considered valuable by an organization [11], including buildings, equipment, personnel, organization reputation, business documents and other tangible and intangible assets. An asset can be logical, such as a Web site, software information, or data; or an asset can be physical, such as a person, computer system, hardware, or other tangible objects. Information assets, on the other hand, is *"an asset that collects, stores, processes, or transmits information, or any collection, set, or database of information that is of value to the organization."* [14] (p. 320) Related to assets in this paper are Key Performance Indicators (KPI) which is defined as *"a measurable value which explains the effectiveness of an institution and how it is achieving key objectives" [15].* KPIs can be used to track progress on specific business objectives and can aid and evaluate if an organizations business strategy is sufficient. A *threat* is a *"potential cause of an unwanted incident, which may result in harm to a system or organization"* [11]. The terms *threat source* and *threat* are commonly used interchangeably, even though the two terms are technically distinct [14]: *Threat* might also describe treat source. While a threat agent is *"The specific instance or a component of a threat"*. This paper distinguishes between the threat agent and event.

A vulnerability is a *"weakness of an asset or control that can be exploited by one or more threats"* [11]. Vulnerabilities are instrumental in determining current and residual risk after control measure implementation.

The results presented in this paper builds on Joachim Ulven's master's thesis submitted in 2020 [16], which evaluated risks facing HEI and the Norwegian University of Science and Technology.

2.2. What Separates HE from Classic Industry?

Two important tenets of HE are *academic freedom* and *openness*, both of which are being universal for most of the sector. Academic freedom is defined by Encyclopædia Britannica as *"the freedom of teachers and students to teach, study, and pursue knowledge and research without unreasonable interference or restriction from the law, institutional regulations, or public pressure."* While the other tenet, *openness*, is commonly described as an overarching concept or philosophy that is characterized by an emphasis on transparency and collaboration [17,18]. That is, openness refers to "accessibility of knowledge, technology and other resources; the transparency of action; the permeability of organizational structures; and the inclusiveness of participation [18]. In practice, this means that academics enjoy intellectual freedom, free from the constraints of short-term deadlines typical for the industry counterpart. Freedom

of choice to pursue and research ideas is primarily limited by the ability to secure funding and resources.

HE serves an essential societal function charged within research, development, and education. Academic research is mostly collaborative and team-work oriented, both cross-disciplinary and multilateral. Autonomy, individuality, and freedom of choice characterize the HE environment, with few restrictions regarding collaboration and knowledge dissemination. These properties differ from industry, where trade secrets are common and often vital to thrive in business. While HE is highly focused on research and development, much research is done for learning and seldom for immediate profit. HE goals tend to be long-term which also leads to a difference in pace between industry and academia. An essential aspect of HE is that research careers are often individual, and the likelihood of receiving recognition for achievements is more significant than in industry.

In contrast to cybersecurity's emphasis on secrecy, the academic environment thrives upon openness, building on a tradition of trust, information exchange, and discussion [7]. Therefore, typical characteristics of universities are to be open and including, meaning few physical perimeters and that strong access control is uncommon [5]. HE is also characterized by the yearly enrollment of new students and temporary staff and visiting researchers. Faculties often operate autonomous entities and build their own IT networks designed to support research, development, and teaching activities [5,6]. The networks are often locally managed with a low degree of centralized control [5].

2.3. Previous Work on Information Security in HE

Our literature review identified several research papers within infosec at HE, but not relevant for our Comprehensive Literature Review (CLR). This section provides the reader with examples of such papers. In 2003, Adams and Blanford [7] studied security in online learning and discuss the trade-off between security and availability. The authors were maybe the first to have an in-depth discussion on the security culture of (North American) academia and tensions with the traditional security departments. An inspiration for our paper was conducted by Whitman and Mattord in 2016 [19] who mapped cybersecurity threat agents, events, and risks for generic industry.

We did not discover any previous literature reviews of cybersecurity risks in HE. The closest we found was a literature review of infosec management present in HE by Bongiovanni [1], which presented literature regarding risk management frameworks and standards, infosec policies, sociotechnical holistic approaches, technical solutions, cyber-behaviors, culture and awareness, and governance. Another review paper authored by Chen and He [20] surveys security risks and protection mechanisms posed to online learning. The findings primarily consist of technical attacks and mitigating controls.

Beaudin [21,22] discusses the legal implications of data breach in HE when storing student data and cybersecurity regulation under state and federal law. Hussain et al. [23] specifically considers the risks among online social networking in HE in Malaysia, focusing on cybersecurity risk towards lecturers. A similar study focuses on cybersecurity risks facing academic libraries [24].

There has also been conducted multiple phishing and social engineering studies of students and faculty in HE, for example, Diaz et al. [25] and Cuchta et al. [26], both documenting a high level of susceptibility to phishing attacks in academia. Related to phishing-attacks, Dadkhah [27] reviews cyber-attacks in scholarly publishing, such as the fraudulent call for papers, and reviews attackers strategies employed to fool scholars. Additionally, Teixeira da Silva [28] researched the issues and costs of spam emails in academia. Wangen et al. conducted a root cause analysis of physical security issues in a University College [29]. Kashiwazaki [30] provides a case study of a data leak incident occurring on a Japanese University. The author offers an insight into how the incident occurred and the possible countermeasures to implement. Liu et al. [31,32] investigates the correlation between IT Centralization, outsourcing and cybersecurity breaches in U.S.

The authors find that both centralized IT and outsourcing are associated with fewer security breaches.

Dar [33] outlines and discuss key infosec challenges within HE. He proposes a framework for managing them for ensuring sustainability, growth, and development. Similarly, in their book, Luker and Petersen [34] outlines key challenges and solutions for computer and network security in HE. In his 2010 book chapter, Custer [35] also provides an extensive theoretical analysis of the infosec threats, data assets, and the risks in HE with challenges and solutions. While Custer cites some incident statistics for HE, the cited online source is no longer available and verifiable, and not included in the review.

3. Method

A literature study is a review of the existing literature surrounding a particular research topic. The literature study in this paper follows the seven-step *Comprehensive Literature Review model* [36]. The process is grouped into three main phases: *Exploration phase*, *Interpretation phase* and *Communication phase*. The applied CLR method is described in Table 1.

Table 1. The three phases of the Comprehensive Literature Review (CLR), from the book [36] (p. 56).

Exploration Phase
Step 1: Exploring beliefs and topics
Step 2: Initiating the search
Step 3: Storing and organizing information
Step 4: Selecting/Deselecting information
Step 5: Expanding the search to include one or more MODES (Media, Observation(s), Documentation, Expert(s), Secondary Data)
Interpretation Phase
Step 6: Analyzing and synthesizing information
Communication Phase
Step 7: Presenting the CLR report

3.1. Exploration Phase

The exploration phase consists of five steps with the purpose of exploring the topic gathering information. Step 1 is *Exploring beliefs and topics* to gather an initial understanding. We conducted step 1 by acquiring knowledge through informal interviews with experts working in the Norwegian sector to achieve first-hand knowledge of threats that may exploit vulnerabilities to abuse valuable information assets. It was essential to identifying valuable information assets that were relevant to strategic objectives at HE. In step 2, *Initiating the search*, we applied the results from these interviews provided a holistic overview of the topics and highly relevant keywords for searching further literature. We acquired the academic papers, dissertations, and books from online academic databases such as ACM Digital Library, Google Scholar, ScienceDirect, Scopus, Researchgate and Springer Link. White papers and technical reports were acquired from Google search.

3.1.1. Search Terms and Strategy

For step 3 (*Storing and Organizing information*) and 4 (*Selecting/Deselecting information*), we used combinations of the identified keywords as strategy when searching for literature. The keywords and possible combinations were:

- For researching assets: *Information assets* or *KPI* and *higher education* or *university* or *academia* or *education sector*
- For researching threats: *Cyber* or *Information* and *Threats* or *Threat intelligence* and *higher education* or *university* or *academia* or *education sector* and *breach*
- For researching vulnerabilities: *Vulnerabilities* or *Vulnerability* and *higher education* or *university* or *academia* or *education sector*

- For researching risk: *Cyber* or *Cyber attacks* or *Information* and *Security risk* or *risk* and *higher education* or *university* or *academia* or *education sector*

We recorded the findings and archived them locally. In step 5, *Expanding the Search to include one or more MODES (Media, Observation(s), Documentation, Expert(s), Secondary Data)*, we also chose to review the references of the relevant academic papers to find more relevant studies to include. The method encourages adding additional sources (MODES) when there is a scarcity of primary sources. We, therefore, decided to open up for including all types of literature relevant to the topic, including webpages from academic institutions, books, technical reports, vendor statistics, and white papers.

3.1.2. Inclusion and Exclusion Criteria

The main inclusion criteria for this study is to include previous studies of cybersecurity in HE in the context of risk management. The literature published during 2008–2020 was taken into consideration for inclusion in the search criteria. The detailed inclusion criteria for the search are:

- Academic studies that describe information security risk assessment or management in HE.
- Academic studies of either assets, KPI, threats, vulnerabilities, or risk in HE.
- White papers, technical reports, thesis, or websites dedicated to either topic. For these sources:

We applied qualitative scrutiny on the latter literature category to focus on high quality sources. Articles are excluded on the following criteria:

- Literature not written in either English or Norwegian
- Studies that do not focus on risk related topics faced by the academic industry (e.g., papers on cybersecurity education [37,38], legal issues [21,22], or issue specific topics in HE [26,39].
- Studies published in the year 2000 or older.
- We have restricted the inclusion of reports from security vendors to those either containing empirical data sorted on HE or containing expert insights.
- We have not included news reports and articles.

3.2. Interpretation Phase

The second phase of the literature review depict the *interpretation* of the extracted information, and consists of step 6, *Analyzing and Synthesizing Information*. The literature search might accumulate a large number of results and the majority of the work will be to investigate potential information and literature. We ranked the results according to bias, prioritizing academic sources over books, technical reports, and white papers. Books generally receive less review by experts before publication and are primarily created for financial gain when compared to scientific literature. Technical reports, white papers, and the likes are usually created by companies seeking financial gain. Though, they can contain legitimate data, they might be written to promote or advertise a service. The literature study gathered and synthesized data on information assets based on KPIs, statistics of threats, and vulnerabilities currently present at HEI.

3.3. Communication Phase

The final step is presenting the comprehensive literature review report and is primarily a communication phase. The phase illustrates how results from the previous steps shall be presented and disseminated. Our primary approach has been to categorize findings within common topics with references. Furthermore, we have summarized the key findings at the end of each analysis to answer the research questions.

Section 4 contains a description of the reviewed literature where we summarize and categorize the literature findings. The findings relating to general ”Valuable information assets,“ “Threats events,” “Threat agents,” and “Vulnerabilities,” are presented and sum-

marized in the subsequent sections. Finally, we apply the CURF framework [12] to frame the identify, discuss, and communicate the most prominent cyber risks in HE.

4. Description of Included Literature

This section provides a brief overview of the referenced literature sorted in categories. We have reviewed 75 different literature sources, including academic papers and MODES, of which, we chose to include 18 academic articles and 14 unique MODES (19 total MODES). The MODES consists mainly of white papers, technical reports, bachelors thesis, and websites. The findings within each category are broadly sorted within the assets, threat, and vulnerability paradigm. However, the papers addressing all three categories are placed in a risk-category and presented at the end of each subsection. The findings are summarized in Table 2.

Table 2. Overview of referenced research sorted on publication type, topics, country, and publication year.

Source	Reference	Publication	Topics	Country	Year
Academic Literature	Ballard [40]	Ph.D. Thesis	Asset/KPI	USA	2013
	Asif & Searcy [41]	Journal article	Asset/KPI	Saudi-Arabia & Canada	2013
	Ncube & Garrison [2]	Journal article	Threat	USA	2010
	Pinheiro [42]	Conference article	Threat	Portugal	2020
	Al-Janabi & AlShourbaji [43]	Journal article	Vulnerability	Middle east	2016
	Metalidou et al. [44]	Journal article	Vulnerability	Greece	2014
	Nyblom et al. [45]	Conference article	Vulnerability	Norway	2020
	Yilmaz & Yalman [4]	Journal article	Vulnerability	Turkey	2016
	Rezgui & Marks [46]	Journal article	Vulnerability	UAE	2008
	Ismail & Widyarto [47]	Conference article	Vulnerability	Malaysia	2016
	Noghondar et al. [48]	Conference article	Vulnerability	Norway & Switzerland	2012
	Kim [49]	Journal Article	Vulnerability	USA	2013
	Wangen [9]	Conference article	Risk	Norway	2019
	Singar & Akhilesh [50]	Book chapter	Risk	India	2020
	Kwaa-Aido & Agbeko [51]	Journal article	Risk	Ghana	2018
	Itradat et al. [52]	Journal article	Risk	Kingdom of Jordan	2014
	Mello [53]	Ph.D. Thesis	Risk	USA	2018
MODES	Fawcett. QUT [54]	Website	Asset	Australia	2020
	FireEye Inc. [3]	White paper	Threat	USA	2016
	Ringdalen et al. [55]	Bachelors thesis	Threat	Norway	2018
	CyberEdge group [56,57]	White paper	Vulnerability	International	2018-19
	Wangen et al. [58]	Technical report	Vulnerability	Norway	2019
	Ellestad et al. [59]	Bachelors thesis	Vulnerability	Norway	2019
	FireEye Inc. [5]	White paper	Risk	USA	2015
	Chapman [8]	Policy Note	Risk	UK	2019
	NCSC [10]	Technical report	Risk	UK	2019
	Grama [60]	White paper	Risk	USA	2014
	UNIT [6]	Technical report	Risk	Norway	2019
	Verizon [61–64]	Technical report	Risk	USA	2017-20
	Hackmageddon [65,66]	Website	Risk	International	2018-19
	Giszczak et al. [67]	White paper	Risk	USA	2016

4.1. Included Academic Literature

Our literature search did not reveal any prior research on assets for HE in relations with ISRA. However, in his doctoral thesis, Ballard [40] identifies the most valuable key performance indicators (KPI) in HE. He analyzed the content of the system portfolios submitted from 34 HEI and identified 2139 different KPI's related to these institutions. Ballard created 24 categories or "Areas Measured" for covering the KPI themes of his work. Additionally, Asif and Searcy [41] researched KPIs and performance tracking in HEI. They

propose a structured framework for this purpose which contains a hierarchical listing of said KPIs.

While there is much academic literature regarding cyber threats, the findings were scarce regarding threats facing HE. Ncube and Garrison [2] analyzed data breach reports at universities and colleges in the U.S. The data was obtained from the Privacy Rights Clearinghouse (PRC), gathered between 2005–2009, and contained 290 incident records from 165 US universities. (Privacy Rights Clearinghouse https://privacyrights.org/ (Visited 28 January 2021)) In 2020, Pinheiro [42] conducted a literature review on the cyber threats on educational institutions. While the paper is informative, the sources for the study are primarily white papers and technical reports.

The literature search revealed more academic sources on vulnerability in HE with some geographic diversity. Security awareness and knowledge is a reoccurring theme: Al-Janabi and AlShourbaji [43] conducted a study of cybersecurity knowledge and awareness in the Middle East's educational environment. The study involved a questionnaire with 760 participants, including personnel from academic staff, researchers, undergraduate students, and employees within HE environments. Metalidou et al. [44] conducted a study to investigate the association and cause of lack of awareness and other human factors regarding threats to computer security in HE. The study included 103 employees, namely teachers, administrators and working post-graduate students from the academic society in Athens, Greece. Rezgui and Marks [46] conducted an interpretive case-study to unveil the infosec awareness in HE in a developing country, mainly in the United Arabic Emirates. Ismail and Widyarto [47] conducted a content analysis and case study to cover the development process of infosec policy in HE in Malaysia. The study uncovered several causes of infosec vulnerabilities in HEI in Malaysia.

Of the broader approaches to vulnerability, we found Nyblom et al. [45], which combined a root cause and socio-technical analysis the determine the causes of compromised passwords at a Norwegian University. The study utilized technical analysis combined with an online questionnaire targeting respondents who had their accounts compromised ($n = 72$) to determine the probable root causes. Yilmaz and Yalman [4] conducted a comparative analysis of the infosec effort at six universities in Turkey, based on infrastructure, operation, application, information, policy and human-based infosec. The authors use the risk term liberally, but the research scope is limited to vulnerability and compliance analysis at these universities. Noghondar [48] discuss the possible causes of data leaks in HE, focusing specifically on the human aspect vulnerabilities. The authors also propose controls to address said vulnerabilities. Kim [49] surveyed infosec security awareness and attitudes of 85 undergraduate students in a U.S. college. The author found that the majority in the sample had a decent understanding of infosec topics.

Our literature search revealed few papers specifically on risk in HE—the paper by Wangen [9] proposes a method to categorize, quantify, and risk analyze an infosec incident register. The article includes a case study data analysis of 550 cybersecurity incidents from a Norwegian University's Security Operations Center between November 2016 and October 2017. Wangen discusses assets, threats, and vulnerabilities at the University as a part of the risk analysis. Another paper specifically on HE's risks is the paper by Singar and Akhilesh [50], which discusses risks and potential cybersecurity management measures in HE. However, the article is not based on a dataset and is lacking adequate sourcing and citations. Kwaa-Aido and Agbeko [51] is an inquiry into the information systems security in a Ghanaian University. The authors use a survey to poll 180 respondents regarding typical security issues faced by the University. Itradat et al. [52] present a case study of an infosec management system (ISMS) implementation at a Jordanian University. The paper centers on the ISMS process and on the key findings within the predefined risk categories with treatments. The analysis has a high level of technical granularity. It mainly focuses on servers and sites, while the remainder is a description of which best-practice security measures from the ISO/IEC 27001 and 27002 should be implemented.

In her thesis, Mello [53] survey data breach records from universities in all of the U.S. states. She investigates the hypotheses whether larger universities are more susceptible to data breaches and if universities with more financial resources are more vulnerable to a data breach. The study includes breach records for U.S. HE from 2005–2017 also collected from the PRC (https://privacyrights.org/ (Visited 28 January 2021)) combined with data from College Scorecard Data from 1996–2016. The data includes universities from all the American states and the combined data resulted in 604 records of HE breaches.

4.2. MODES

While the academic literature was scarce, our search revealed some white papers, technical reports, and websites addressing the issues. We have applied scrutiny of these sources for inclusion regarding their credibility.

For assets in HE, the Queensland University of Technology (QUT) stood out as the most credible source with a formal and updated information asset inventory at their institution available at their website [54].

On cyber risks facings HE, the FireEye security vendor report *Cyber Threats to the Education Industry* represents one of the more credible and targeted technical reports [3]. We also included the 2018 and 2019 versions of the *Cyber Defense Report (CDR)* published by the US consulting firm CyberEdge group [56,57]. The report is an annual survey with 1200 participants from 17 countries and maps the cybersecurity perception among IT security professionals in 19 different industries.

There were three studies conducted at the same Norwegian University: On cyber threats produced in HE, Ringdalen et al. [55] is a bachelor thesis from 2018 that applied threat agent profiling using open source intelligence techniques targeting the University. The study provides a detailed description of the characteristics and capability of threat actors prominent to the institution. Furthermore, on vulnerabilities in HE, Wangen et al. [58] is a technical report which studies unrecorded security incidents at the Norwegian University using an online questionnaire (n = 597). The study builds on and is complementary to the dataset in Wangen [9]. Finally, Ellestad et al. [59] is a bachelor thesis from 2019 which surveyed the infosec culture at the University IT department. 137 individuals participated in the survey, and it uncovered some vulnerabilities, but a severe limitation was that it did not include faculty members.

On cybersecurity risk, we found several credible sources: Grama [60] researched infosec risks in HE as a response to the EDUCAUSE HE infosec Council call to attribute data breaches in HE (https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/about-heisc (Accessed: 2 May 2020)). The data presented in the technical report was also gathered from the PRC dataset from 2005–2013. Another technical report from FireEye [5] addresses some challenges and infosec risks within the HE industry. According to Google Scholar, the Policy Note by Chapman [8] from 2019, is becoming a frequently cited source for cybersecurity in HE. Chapman is the head of the JISC SOC, a sector SOC for multiple UK universities, and carries some authority in his publication. The Policy Note describes SOC statistics and outlines common assets, threats, and vulnerabilities seen by UK universities. Another credible UK source from 2019, was the technical report published by The UK National Cyber Security Centre (NCSC) [10]. The report addresses the HE cyber threat and contains overarching assessments of assets, threat actors, attack vectors, and risks.

Similar to the NCSC report and Chapman, The Norwegian Directorate for ICT and joint services in higher education and research (UNIT) published a technical report paper regarding the state of infosec in Norwegian HE [6]. The study documented the results from interviewing representatives from 21 of the state-owned universities, accompanied by incident data from the sector SOC. The report addressed several potential risks and vulnerabilities that were relevant to the universities in Norway.

We have included some additional sources with less credibility on cyber risk in HE—Verizon Inc. publishes the annual *Data Breach Investigation Report* [61–64] which

illustrates data breaches and security incidents that occurred in the biggest industries, including the educational industry. The parts specifically concerning HE span 2–4 pages and address typical incidents, threats, and risks occurring in US universities. Similarly, Hackmageddon [65,66] is a website that collects public reports on global cybersecurity attacks and converts them into timelines and graphs. This website creates statistics for four different industry categories, including "Education". The Hackmageddon website also manages statistics both for attack type and possible motivation of these attacks. Finally, Giszczak et al. [67] is a white paper from a US consulting firm. The document evaluated the specific cyber risks for HEI, including common causes and costs of a breach, and potential mitigating measures. However, data sources and references are not properly described in this document.

5. Assets in HE

Giszczak et al. [67] write that *"Colleges and universities collect data from donors, trustees, board members, alumni, students, parents, applicants, faculty, staff, medical patients, consumers, and vendors. The type of data they collect and maintain is widespread, including sensitive research, financial, medical, employment, personal, and tax data. Colleges and universities also are not only institutions of HE – they are financial institutions, medical institutions, and retail establishments, and subject to the state, federal and international regulations related to those industries"*. Universities have a broad asset portfolio given the diversity of HE business. The asset value is relative and changes according to life span, threat picture, context, legal requirements, and other conditions. HE shares the unique characteristic that it produces large quantities of research data and sensitive data about students and employees.

The Queensland University of Technology (QUT) has created a formal inventory of possible information assets at their institution, Table 3. The Table contains a compressed list of information assets depicted from the list from QUT. It is included to provide the reader with insight into a modern HE institution's diverse information asset portfolio. When the researchers asked the technical and non-technical staff at the Ghanaian University which IT assets required protection, the results showed that *Student records*, *Internet connectivity*, *Financial records*, *Admin records*, *Student laptops*, and *Research data* ranked in that order was the most valuable assets [51]. However, other stakeholders might rank the value differently. The remainder of this section first outlines the literature findings regarding HE's information asset groups before outlining KPIs and summarizing the findings.

5.1. Research Information and Data

Research data is a broad term, but the University of Leeds defines it as *"any information that has been collected, observed, generated or created to validate original research findings"* (https://library.leeds.ac.uk/info/14062/research_data_management/61/research_data_management_explained (Visited 1 December 2020)). Research data can appear in many formats, primarily digital, but also non-digital. Although the value of research data differs, there are examples of longitudinal studies spanning decades, in which the data is irreplaceable. Some research data may be strictly confidential, while other data only requires control of integrity or high availability. Examples of research data are scientific data, academic knowledge, raw data, analysis results, and scientific publications [6]. Additionally, this category may include assets such as research management data, contracts, intellectual property, patents, and funding information [54]. Kwaa-Aido and Agbeko [51] discuss assets in the context of a Ghanaian University and highlights politically and commercially sensitive research data and personally identifiable information (PII) as core assets managed at the University. Furthermore, FireEye [5] lists enterprise, research, and third-party data as key assets. Examples of the latter are research data received from industry partners. As another kind of third-party data, Giszak et al. [67] add "Government data" to the list, referring to situations where universities cooperate with the government on research projects. Research data were mentioned in the majority of the reviewed sources, summarized in Table 4.

Table 3. Compressed table from Queensland University of Technology (QUT) inventory of information assets [54].

Category	**Information Assets from Queensland University of Technology**
Student information	- Personal/sensitive information (e.g., name, e-mail, address) - Admission details - Class registration information - Student financial information - Student results (e.g., exam results) - Records of student support services - Student communications platforms - Study records of course completion and achievements
Learning and teaching information	- Curriculum information - Information associated with curriculum - Online learning information - Course information - Exam information - Library learning resources - Meta data about resources
Research information	- Research management data (e.g., resources, business and industry engagement) - Research results and publications - Contract management - Intellectual property (patent) - Funding information
Facilities management information	- Campus infrastructure information - Security infrastructure
Financial management information	- General corporate finance information - Management information regarding budget, costing, pricing and report
Governance, strategy and policy information	- Committees management data - Meetings schedules - Legislative documents - Audit and risk management - Strategy documents
IT support information	- Communication and collaboration information - Infrastructure information - Identity and access information (e.g., username and password) - Technology procurement information - Technology support information
Human resources information	- Staff and employee records - Recruitment information - Records of Health, Safety & Environment
Alumni information	- Records of personal detail - International partner agreement information - Partnership
Market and Media	- Websites - Market management information - Intranet - Social media information

Table 4. Proposition of the most valuable information assets based on KPI. References for each asset is listed in the right column.

KPI	Critical Information Assets	Reference
Enrollment & Graduation	Student PII and records	[5,6,9,10,40–42,50,51,53,54,67]
	Learning and teaching information	[40,41,50,54]
	Financial management information	[5,6,9,40–42,50,53,54,67]
Stakeholder satisfaction	Sensitive Research information/data and IP	[5,9,10,40–42,50,51,54,67]
	Government and Third-party data	[5,67]
Employee & HR	Employee & Student PII	[5,9,10,40–42,50,51,54,67]
	Administration details	[40,41,50,51,54,67]
	User and administrator accounts	[6,8,9,45,53,58,65,66]
IT Supporting services	Bandwidth and Internet Connection	[6,9,10,51]
	Computing power and resources	[6,9,10,52]
	Communication systems and data	[6,10,52,53]

5.2. Student and Employee Personal Identifiable Information (PII)

Pinheiro writes that Universities *"store thousands of pieces of information from each student, teacher and staff member. Bank accounts, addresses, school transcripts and other valuable data"* [42]. Additionally, PII processed in HE can include information about applicants, students, employees, guests, alumni and participants in research projects [6]. Several of the information assets are reoccurring in the review, such as PII, research data, and student records. Singar and Akilesh [50] propose the following assets as critical for cybersecurity: Students' PII such as email id, contact number and financial information, and records. Admission, examination, and administration details, together with employee PII. Lastly, the authors describe financial data as a critical asset. FireEye [5] lists PII and distinguishes health and medical information from PII as they are handled at student health centers. FireEye also adds law enforcement data as a part of the assets that must be protected, as *"many schools have their own forces that keep records on students who run into trouble on campus"*. NCSC [10] writes that bulk PII (Personal Identifiable Information) on staff and students are typical targets of a cyberattack. Mello [53] conducted an in-depth analysis of the type of data records lost in her breach investigation. The results illustrate the diversity of the University PII portfolio Figure 1. PII about both students and employees are processed for multiple purposes at the University, and Table 4 shows that PII is mentioned in most of the reviewed sources.

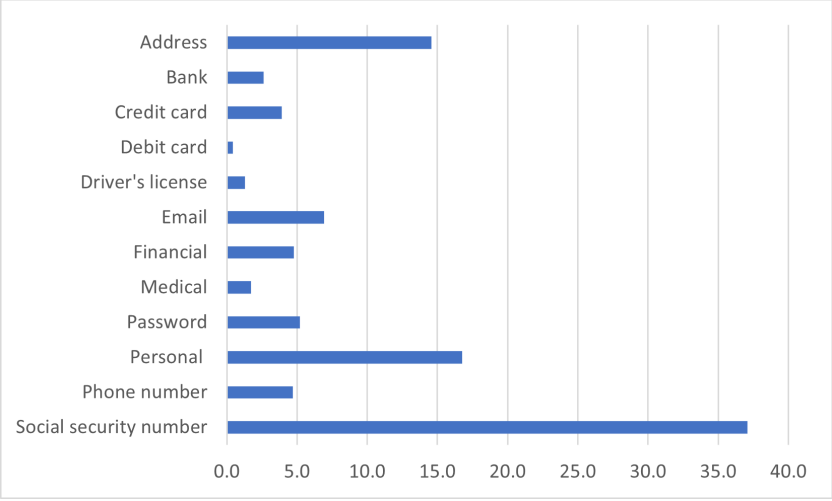

Figure 1. Overview of breached data record types (*y*-axis) and percentages (*x*-axis) from Mello [53], approximate $n = 1150$.

5.3. Student Records

The Kwaa-Aido and Agbeko study ranked student records as the most valuable information asset at the University [51], and Ballard's KPIs rank in Table 5 scores *Graduation measures* highest. The records are crucial for the student production process as they document and describe student performance. There should be strict security requirements for ensuring both the confidentiality and integrity of the records. For example, the reputational damage of an attack on integrity could be devastating as untrustworthy records could make student testimonies worthless. Student records are grouped with PII in Table 5.

Table 5. The top 10 KPI categories ranked by critically by Ballard [40] (p. 120).

KPI Category in HE	Score by %
Graduation measures	100
Stakeholder satisfaction	100
Employee & HR	97
Enrollment	94
Retention	94
Financial	88
Student success	88
Student engagement	85
Strategic planning	82
Admission	76

5.4. Learning, Teaching, and Exam Information

This asset category contains the information needed to conduct the teaching activities, examples are information about the curriculum, course, exam, and learning resources [54]. These information assets can usually be replicated, however the confidentiality of exam information is critical.

5.5. Financial Management Data

Many universities have large budgets and handle a lot of finances. Transactions are diverse and include acquisitions of research equipment, software, IT equipment, furniture, and facilities, to name a few. The universities also manage payment of employees and contractors. Furthermore, several HEI accepts and store banking and credit card information for tuition, and other fees [5]. Financial data is considered a critical asset by most reviewed literature, Table 4.

5.6. Infrastructure, Computing Power and Resources

The modern universities manage an extensive portfolio of systems, infrastructure, computing power and resources. Assets specifically mentioned are digital infrastructures, such as computer networks, supercomputers, sensor networks, research databases, laboratory instruments and equipment [6,10,52]. The analysis in Wangen [9] documents several venues for abusing IT assets: Servers and network resources can be abused as a staging point to conduct attacks. This issue was evident from the number of brute-force and scanning attacks launched from the University network in his dataset. Bandwidth capacity was recruited in outgoing DDoS attacks against third parties. The bandwidth was also exploited for file-sharing in violation of copyright laws. University resources were also abused in hosting illegal content [5]. Computing power and resources are also lucrative in mining for cryptocurrencies [58].

5.7. User and Administrator Accounts

Tightly coupled with access to infrastructure, user and administrator accounts are the asset that provides access to the University infrastructure and resources. There are several venues for abusing credentials, and they are a popular target for attackers [58]. According

to Nyblom et al. [45], HEI credentials are harvested and traded, abused in phishing and spamming, and used to gain access to resources. The Silent-librarian campaign is an example of the latter, where company accesses was abused to mine resources that are only available through university contracts [8,9]. Using legitimate network credentials also adds credibility to new attempts of CEO frauds, phishing, and ransomware [6].

5.8. Communication Data

The universities are dependent on digital communication and the academic community is dependent on email for communication, both internally and externally. NCSC describes emails as an information asset typically targeted by advanced attackers [10]. Emails are also part of the list provided in Mello [53], Figure 1.

5.9. Examining KPIs in HEI

As seen in Table 3 from information assets from QUT, universities are managing a vast variety of information assets. Interesting categories for ISRA such as "Student information", "Learning and teaching information", "Research information" are among them. However, we wish to identify the most critical and valuable information assets in HEI, which can be done by either examining the organization's mission statement to determine essential assets or explore the KPIs. Asif and Cory [41] explain that KPI in HEI needs to be developed through review and adaptation of the institution's mission and core academic processes. All dimensions of HE, including research, teaching, and service to the profession, must be considered. Therefore, KPI in HEI can be anything from the number of research points the institutions achieve to the number of students completing their studies. The paper from Asif and Cory [41] provides a comprehensive list of KPI in HE based on an extensive literature study, Table 6. The list of KPIs in HE provided includes KPIs in academic processes like research performance, teaching performance, service performance and financial performance.

Table 6 shows that there are many types of KPI in HEI. Ballard [40] ranked the most valuable KPIs by analyzing the content of the system portfolios submitted from 34 HEI. He identified 2139 different KPIs related to these institutions. Ballard created 24 categories or "Areas Measured" for covering. The list in Table 5 illustrates the top 10 ranked KPIs by Ballard [40] (p. 120).

As seen in Table 5 the list provided by Ballard [40] manage to rank KPI in HE based on their value. Even though some the KPI categorize or "Areas Measured" attained similar scores, the top four KPI categorize were related to "Graduation measures", "Stakeholder satisfaction", "Employee & HR" and "Enrollment".

5.10. Critical Information Assets in Higher Education

By combining the presented Tables 3–5 with the reviewed literature on infosec risk, we propose the mission-critical assets and KPIs in Table 4. Table 4 categorizes information assets together with citations in the literature, listed in the right column. We found a high agreement among the reviewed sources on important assets in HE. Most sources mentioned student information, financial information, research data, and employee information as critical information assets. Student PII and records are the most frequently mentioned in the literature, together with financial management and sensitive research data. In some cases, the universities also have student health centers that store information [5]. These assets will require extra protection. Other information assets that might be included are learning and teaching information, such as curriculum information, exam information, general corporate finance information, research management data (e.g., resources, business and industry engagement) and government data. Additionally, the universities manage infrastructure resources that are interesting to attackers, such as computing power and resources, bandwidth capacity, and hosting. It is rather unlikely that the generic university will view student laptops as their property as proposed by Kwaa-Aido and Agbeko, but practices might vary.

Table 6. Key performance indicators (KPI) in higher education (HE) from Asif and Cory [41] (p. 993).

Academic Processes	KPI
Research performance indicators	Number of research publications Number of research projects Number of patents Number of monographs Number of spin-offs from main research stream Number of patents addressing local needs % of faculty winning academic grants Number of technology projects Number of research projects addressing local needs % of faculty attending conferences and seminars Research impact
Teaching performance indicators	Students and other stakeholder satisfaction Employer satisfaction with graduates skills Number of students completing the program Student progression rate Dropout rate (Number of dropouts/No. of students enrolled) Median score of students % of students with a particular GPA Course rating – median evaluation of the course by students Graduates employment rate
Service performance indicators (university, profession, and community)	Number of academic programs designed Participation in curriculum development Participation in academic committees Students counseling Community service
Financial performance	*Revenues* Income generated from research projects Income generated from consultancies Income generated from spin-offs/patents Sponsorship's/endowments Income generated from tuition *Expenses* Total teaching and research cost % of budget allocated to the research

6. Cyber Threat Events in HE

Threat events or attacks are acts committed by threat agents to gain access to assets. These agents might utilize a wide range of attack methods to gain access to systems in higher education. The following sections will present sources of literature which illustrates an overview of the most common attacks and threat events to HEI. We start with publications on SOC statistics and follow with publications data breaches before summarizing the findings.

6.1. University SOC Statistics

We found one peer reviewed data source describing statistics collected directly from the University SOC [9]; a technical report from the UK sector SOC [8] and the Norwegian [6] HE sector CERTs. The data set provided by Wangen [9] contains an analysis of 550 infosec incidents from a Norwegian University SOC in 2016–2017. The incident analysis contains a correlation of incident causes and outcomes. As seen in Figure 2, there are 12 major cause classifications, but the majority of incidents are caused by "Social engineering" attacks,

"Compromised Asset", and "Compromised Users". Furthermore, "Vulnerable assets" and "Policy violations" also represent more than 50 each of the 550 incidents. In the analysis the author finds that 99 of the social engineering attacks against the University have negligible consequences.

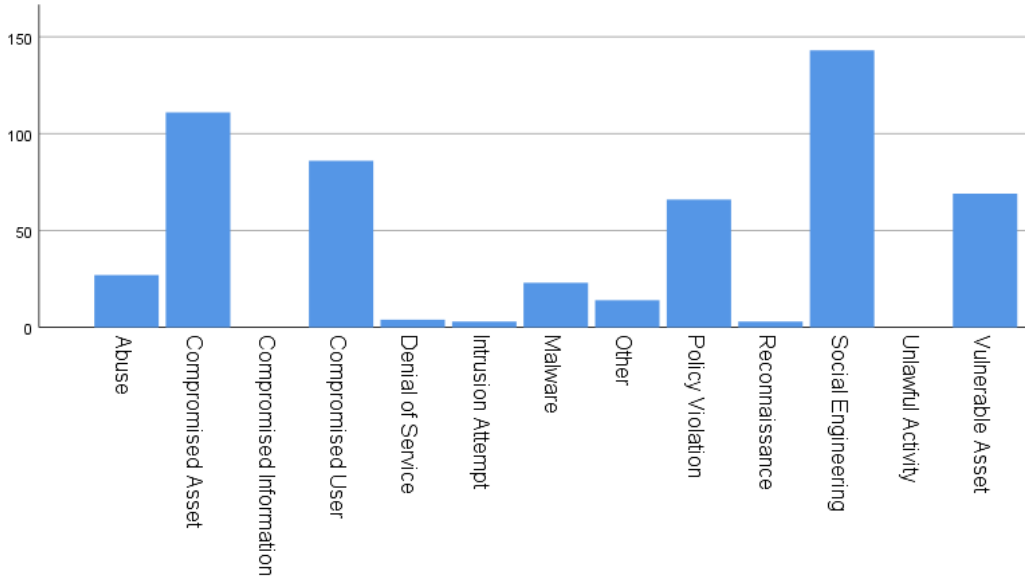

Figure 2. Incident causes in the Norwegian University SOC, histogram from Wangen [9].

Chapman [8] writes that the UK Jisc SOC handled approximately 6100 incidents or queries in 2018. The incident classification is available on a timeline in the Policy Note, and although the authors do not apply the same incident classification, the statistics are comparable to those in Figure 2. Considering the incidents from Jisc SOC, it seems that there was a wave of "Compromise" in January and February 2018 as the primary cause of incidents, but this becomes a minor contributor to incidents for the remaining year. "Malware" and "Copyright" are two significant contributors all throughout the year. Furthermore, Chapman comments on the statistics that students and other users are continuously committing Denial of Service (DoS) attacks towards each other on the network.

Furthermore, the UNIT technical report [6] contains statistics from the Norwegian University Network (UNINETT) CERT, which has a similar role to the Jisc SOC in the UK. The statistics contain 965 incidents, where 682 is caused by "Vulnerable assets", followed by the categories "Compromised asset" and "Scanning" both of which have caused 95 incidents. While not written explicitly, the statistics also show DoS attacks as a consistent cause of incidents. Neither Jisc SOC or UNINETT CERT provides the numbers for their statistics.

The three SOC statistics included in our paper were all collected between 2016–2018 but are quite different using various classifications. While there are some similarities, such as "Malware" and "Copyright" in Wangen [9] and Chapman [8], these are barely visible in the UNINETT CERT data. There are also other major differences, such as for the Norwegian SOC, "Social engineering" is the major category, while it seems negligible for both the Jisc SOC and UNINETT CERT.

6.2. Publications on Data Breaches and Threat Events

The analysis of the PRC data on breaches at universities and colleges in the US from 2005–2009 by Ncube and Garrison [2] applied broad categorization of incidents. As seen in Table 7, "Hacker" incidents are the most frequent. The authors defined the category "Hacker" as *"unauthorized remote computer break-ins"*. These incidents make out 38% of the total 290 recorded incidents. Other frequent incidents were "Exposed" (28%) which the authors defined as *"unprotected data that may be publicly accessible and includes records*

exposed in an e-mail, regular mail, online and through disposal.", and "Stolen" which refers to stolen equipment.

Table 7. Table from Ncube and Garrison [2] (p. 33), of the number of incidents per year.

Type	2005	2006	2007	2008	2009	TOTAL
Stolen	9	15	16	21	12	**73**
Hacker	38	20	16	14	22	**110**
Insider	1	1	0	3	1	**6**
Exposed	5	13	25	28	12	**83**
Missing	1	5	6	6	0	**18**
Total	**54**	**54**	**63**	**72**	**47**	**290**

Kwaa-Aido and Agbeko [51] polled their participants regarding cyberattacks, and found that the most common cyber threat in the Ghanaian University was "Malware", with only 14.5% of the participants reporting that they had never suffered a malware incident. 63% of the respondents reported never to have been targeted by online fraud, scams or phishing attacks. About 70% reported never to have suffered identity theft, impersonation, or password theft.

Furthermore, two of the included literature sources also use the PRC Chronology of Data Breaches and classifications for their analysis: Grama [60] included 562 reported breaches at 324 unique institutions in the US between 2005 to 2013, n = 551. 63% of all breaches were reported from doctoral level institutions, making up approximately 7% of all US institutions. As previously described, Mello enriched the same dataset from 2005–2014 with findings additional analysis, but retaining the same classifications, n = 604. A comparison of these results is presented in Table 8. Although, all three sources emerge from PRC, the categorization is different in Table 7 than in Table 8.

The largest proportion of the reported breaches in the Table fell into the "Hacking/malware" classification, which accounts for 36% and 39% of all breaches, similar to the findings by Ncube and Garrison [2]. Grama reports that these breaches were outside parties accessing records via direct entry, malware, or spyware. The second largest category of reported breaches was the result of "Unintended Disclosures", which is similar to the "Exposed" category proposed by [2]. Finally, the third-largest proportion was caused by the loss of a portable device, which is similar to "Stolen" and "Missing " in Table 7. "Payment Card Fraud" was the least likely data breach classification seen among the reported breaches at higher education institutions [53,60]. Only one breach was classified with this tag, which occurred in 2012. Furthermore, Grama writes that potential direct financial costs of a data breach in higher education could include legal representation, fines, and the expense of notifying affected individuals. He continued to address that organizations like higher education might face, losses in reputation and consumer confidence. Defacement and reputational consequences could result in a loss of alumni donations and even a reduction in the number of students choosing to apply to or attend the institution.

We have included the annual *Data Breach Investigation Report* by the commercial vendor Verizon from 2017–2020 [61–64]. The Verizon 2020 report found 819 and 228 confirmed data disclosures in the educational service. For 2019, 382 incidents with 99 were confirmed data disclosures; 2018 had 292/101, and 2017 had a 455/73 ratio. The numbers are broken down in the "Industry comparison" where Verizon categorizes the incidents in "Actions". The Table 9 illustrates breaches occurring in the year 2017, 2018, 2019 and 2020 systematized into six categories with the corresponding distribution.

Table 8. Incident statistics from Grama (n = 551) and Mello (n = 604), both applying the Privacy Rights Clearinghouse (PRC) data for analysis.

Incident	Description	Grama [60]	Mello [53]
Payment Card Fraud (CARD)	Fraud involving debit and credit cards that is not accomplished via hacking	0%	0%
Unintended disclosure (DISC)	Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail or other.	30%	29%
Hacking or malware (HACK)	Electronic entry by an outside party; data loss via malware and spyware.	36%	39%
Insider (INSD)	Intentional breach of information by someone with legitimate access (e.g., an employee or contractor)	3%	3%
Physical loss (PHYS)	Lost, discarded, or stolen non electronic records, such as paper documents.	5%	5%
Portable device (PORT)	Lost, discarded, or stolen portable devices (e.g., laptop, PDA, smartphone, portable memory device, CD)	17%	16%
Stationary device (STAT)	Lost, discarded, or stolen stationary electronic device such as a computer or server not designed for mobility.	7%	6%
Unknown or other (UNKN)	Breaches that do not fit into the above categories or where a root cause has not been determined.	1%	1%

Table 9. Number of security beaches in HE sorted by action and year from Verizon Data Breach Investigation reports 2017–2020 [61–64].

Threat Events(Action)	2017	2018	2019	2020	Sum
Error	19	16	37	66	138
Hacking	43	46	42	85	216
Malware	26	14	16	39	95
Misuse	5	3	9	7	24
Physical	2	8	1	7	18
Social	32	41	38	61	172
Total number of breaches	127	128	143	265	663

Table 9 shows that *"Hacking"* is again the most frequent data breach action, closely followed up by the *"Social"* and *"Errors"* categories. The least frequent action relating to data breaches in the educational industry is *"Physical"* action, which had only one case in 2019, according to [63]. The 2019 edition also proposed a taxonomy of *patterns* associated with the incidents in HE. The *pattern* can be viewed as a cause of incident, and the two major causes are *Miscellaneous errors* on 35% and *Web application attacks* 24%. The former is defined as *"Incidents in which unintentional actions directly compromised a security attribute of an asset"* (p. 25), and the latter *"Any incident in which a web application was the vector of attack."* (p. 25). However, *Privileged misuse*, *Cyber-espionage*, *Lost and Stolen assets*, and *Crimeware* together make up 20% of breaches. A major category, *"Everything else"*, caused 20% of incidents, of which a 28% were estimated to have been caused by phishing attacks. Similar patterns were also present at the top of the 2017 and 2018 edition.

We have compiled the Hackmageddon 2018–2019 statistics [65,66] for the "Education" category in Table 10, n = 202. The histogram is sorted on 11 different threat events with frequencies. The results show *"Malware/PoS Malware"* is the most frequent cyber-attack in the educational industry. Other frequent attacks were *"Account Hijacking"* and *"Unknown"*. The least frequent threat events were *"Brute-Force"*, *"Vulnerability"*, *"Malicious Script Injection"*, and *"SQL injection"*. However, Hackmageddon.com (Visited 28 January 2021) usually relies on *attack submission*. Classification of attacks can therefore be subjective, and the amount of work regarding follow-ups and fact-checking is unknown. When comparing the

findings to previously presented results in this literature review, the Hackmageddon.com (Visited 28 January 2021) incidents are all domain of technical automated detection.

Table 10. Statistics from Hackmageddon.com (Visited 28 January 2021) [65,66] of attacks (threat events) for the "Education" category, 2018 (n = 74) and 2019 (n = 128).

Attacks (Threat Events)	2018	2019
Malware/PoS Malware	16	71
Account Hijacking	30	26
Unknown	20	20
Targeted Attacks	4	4
Vulnerability	1	2
Brute-Force	0	2
DDoS	2	0
Defacement	0	1
Malicious Script Injection	0	1
Malicious Spam	0	1
SQLi	1	0
Total	**74**	**128**

6.3. Threat Event Summary

The literature study unveiled six distinct sources of literature relating to the threat events, including 4 Verizon reports. Ncube and Garrison [2], Wangen [9], Chapman [8], and Mello [53] and Grama [60] specified their data set as exclusively from HEI. Verizon [61–64] and Hackmageddon [65,66] address threats from the educational industry as a category. Table 11 summarizes our findings of threat events ranked by occurrence per source. Chapman [8] only provided the histogram without exact numbers, the ranking is approximate and the numbers cannot be discerned from his figures.

Table 11. The rank of the threat events present in the educational industry according to the literature.

Source	Wangen [9]	Chapman [8]	UNIT [6]	Ncube [2]	Mello [53]	Verizon [61–64]	Hackmag. [65,66]
Coll. Year	2017	2018	2018	2005–2009	2005–2014	2017–2020	2018–2019
1	Soc.Eng. (26%)	Malware	Vuln. assets (70%)	Hacker (38%)	HACK (39%)	Hacking (33%)	Malware (43%)
2	Comp. asset (20%)	Copyright	Comp. asset (10%)	Exposed (28%)	DISC (29%)	Social (26%)	Account Hij. (27%)
3	Comp. user (16%)	Compromise	Scanning (10%)	Stolen (25%)	PORT (16%)	Error (21%)	Unknown (19%)
4	Vuln. asset (12%)	DoS	Comp. system	Missing (6%)	STAT (5%)	Malware (14%)	Targeted Att. (4%)
5	Copyright (12%)	Unauth. use	DDOS	Insider (2%)	PHYS (5%)	Misuse (4%)	Vulnerability (2%)
6	Abuse (5%)	Scanning	Spam		INSD (3%)	Physical (3%)	Brute-Force (1%)
7	Malware(4%)	Phishing	Query		UNKN (1%)		DDoS (1%)
8	Other (5%)	Other	Other		CARD (0%)		Other (2%)
n	550	∼6100	965	290	604	663	202

Despite different classifications it seems that *Hacking*, *Malware*, and *Social engineering*-attacks appears to be the most occurring threat events in HE. *Hacker*, *Hacking* and *Hacking and Malware* are the dominating events in Table 11. The *Hacking* are at the top in Ncube and Garrison (38%) [2], Grama (36%) [60], and Verizon (33%) [61–64]. *Hacking* is not a category in the three first columns, however, they contain related threat events, such as *Compromised asset* [6,9] and *Compromise* [8]. Social engineering tops the statistics (26%) in Wangen [9], while malware tops the statistics in Chapman [8] and in Hackmageddon (35%) [65,66]. This can be attributed to the rising of malware and ransomware describes in the paper from Singar and Akhilesh [50]. Table 11 also illustrates that "Error", "Misuse" and

"Unintended disclosure" are also occurring frequently in educational institutions, which can be attributed to human errors in HEI. Other threat events like: "Physical loss", "Stolen", "Insider", and "Defacement" are also present threats in educational institutions but occur in minor quantities. However, these events can cause loss of confidential information. Copyright violations was only present in the SOC data but caused a substantial percentage of incidents.

7. Threat Agents in HE

Methods like VPN, proxy servers and compromised systems all help the threat agent in obfuscating his true identity making attribution notoriously hard [68]. There are billions of people using the internet, and a threat agent can range from a state-sponsored group with intentions of stealing information, to a curious "script kiddie". However, identifying the threat agents and their capabilities is a vital part of understanding the risk landscape [12]. While attack vectors and methods frequently change, the threat groups employing them and their motives stay relatively static. The majority of reviewed sources discuss threat events, but not who is behind them. A threat assessment does not require exact attribution to be useful [69], but understanding the motivation, capacity, capability, and frequency of adversaries is enough to build a good threat model [12].

7.1. Who Targets HEI?

Hackmageddon.com (Visited 28 January 2021) creates statistics on the different infosec threats in the industry; they also create statistics on the possible motivation behind these attacks. Table 12 illustrates the number of breaches in HE categorized by threat agents in 2018 [65] and 2019 [66]. *"Cyber Crime"* is listed as the most frequent threat agent in the educational industry. The Hackmageddon data shows that the majority of threat agents attacking HE is seeking financial gain and are primarily cybercriminals of various capacities and capabilities. Other motives addressed by Hackmageddon.com (Visited 28 January 2021) include *"Cyber Espionage"* and *"Hacktivism"*.

Table 12. Threat agents from 2018 and 2019, reported by Hackmageddon.com (Visited 28 January 2021).

Threat Agents (Motivation)	2018	2019
Cyber Crime	70	122
Cyber Espionage	3	5
Hacktivists	1	1
Total	74	128

FireEye [3,5] writes that due to the amount of valuable information stored on school networks, HE will likely face different cyber threats from multiple threat agents. This issue, coupled with the ability to launch operations on other targets from the school networks makes HE an attractive target. The FireEye report also highlights a challenge for administrators at educational institutions to secure school networks due to the number of users and the constant need for internal and external users to access and share information. The Verizon Data Breach reports [61–64] briefly discuss threat actors, but primarily classifies them as either internal or external. The following sub-sections will summarize the most common threat agents described in the reviewed literature.

7.2. Cyber-Crime and Enterprise-Like Criminals

According to FireEye, one of the most pressing threat agents facing HE is *Enterprise-like cybercriminals* or data thieves seeking to steal and profit from sensitive personal and financial information from student, faculty and staff [3]. Organized criminals constitute actors who are motivated by their financial gain and profit. When they attack, the intention is to steal assets which can be monetized easily [55]. The different groupings of cyber-criminals have very different abilities and frequency.

The NCSC [10] is clear on the threat agents facing the UK universities—*Cyber-crime* and *Nation States* looking to steal personal data or intellectual property. *Organized cyber-crime* is mentioned by Chapman [8] as another significant player, being behind both sophisticated and non-sophisticated social engineering attacks. Wangen points to a poorly secured university infrastructure being leveraged by criminals and opportunists in DDoS attacking others. FireEye describes this abuse as *Infrastructure hijackers* aiming to tap into the university's vast resources, such as hosting and bandwidth [5]. Wangen [9] writes that accesses to the University-owned resources was the most attractive assets for the attackers within the time frame. Combined with frequent social engineering campaigns, he deduced that attacking the university's generic motive was financial, as the typical targets were usernames and passwords, financial data, and other resources. He points to *cyber-criminals* using low-cost social engineering attacks as the most frequent threat agent.

Cyber-crime is the most frequently mentioned threat agent in the reviewed literature for HE: Verizon points to *Ransomware* as the top malware infection (80%), and *Financial gain* as the primary motive behind incidents (92%) in HE in 2020 [64]. Table 12 shows cybercrime being attributed 95% of the reported incidents.

7.3. Nation States and Advanced Persistent Threats (APT)

As one of the most severe threat agents to HE, *Nation state-backed actor*s and *Advanced persistent Threats* (APT) are frequently trying to gain access to sensitive intellectual property [3,5,6,55]. State actors can both be foreign states' intelligence services and private actors operating on behalf of foreign states [70]. Besides, foreign intelligence services can target HE to acquire knowledge and technology (cyber espionage). To be defined within this category, the threat agent must have resources available to work methodically over time, often for months or even years, and are primarily motivated by political, economic, military, security and technological ambitions [69].

Typical state-sponsored groups are the Iranian *Silent Librarian Campaign* [8–10]. Chapman also describes a North Korean group, named *Stolen pencil*, who targeted academics specifically. Regarding sophisticated attacks, Wangen et al. [58] documents the persistence of espionage and attempts of illegal data extraction for a small percentage of the respondents. Verizon lists *Espionage* as the motive behind 3% of the recorded incidents in 2020 [64].

7.4. Human Errors

Human error can cause incidents in many ways, for example, through sloppy data handling and negligent security routines. In Ncube and Garrison [2], the *Exposed* category is defined as *"publicly accessible and includes records exposed in e-mail, regular mail, online and through disposal"*, and makes out 5% of the incident causes. *Unintended disclosure* was the cause of 30% of the data breaches documented in the PRC data [53,60]. The survey by Wangen et al. [58] documents that 30% of the surveyed population knew of physical control guideline violations, 11% knew of PII leaks, and 4.7% knew of incidents caused by poorly managed physical documents. Verizon lists *Convenience* as the motive behind 5% of the recorded incidents in 2020 [64].

7.5. Internal and External Opportunists

The opportunists are attackers with minimal resources but are looking for opportunities both from inside and outside the network [55]. For example, script kiddies are typical opportunists who use scripts or programs developed by others to attack computer systems, networks and deface websites by exploiting known vulnerabilities [69]. Their goals are essentially self-assertion for status and sometimes for profit. They are more arbitrary in their approach compared to professional actors. Internally, many students test their knowledge inside the University network, causing events, both unintentional and intentional. DDoS cause a portion of the incidents from the JANET; Chapman [8] attributes many of the DDoS attacks to *disgruntled students* and *staff* due to the timings of

the attacks. Illegal file sharing and copyright infringement is also a widespread problem on the University network [9], labelled as "Policy violations" in Table 2. Furthermore, exploitation of computing resources in cryptocurrency mining for personal gain on the university network is documented in Wangen et al. [58]. Verizon lists *Fun* as the motive behind 5% of the recorded incidents in 2020 [64].

7.6. Chaotic Actors and Hacktivists

Chaotic actors use illegal means over the Internet to promote a stance, ideology or a political agenda [55,69]. Typically, hacktivists will try to deface and disrupt websites, as a method of protest or way to call attention to a cause [3]. Table 12 from Hackmageddon shows Hacktivists causing one incident, while UNIT describes an anecdote where hacktivists defaced a HE institution website with political propaganda [6]. DDoS is a common method to cause service disruption. Exposure to hacktivism is linked to the type of research conducted at the University, for example, research conducted on animals will typically be targeted by chaotic actors. Verizon lists *Ideology* as the motive behind 2% of the recorded incidents in 2020 [64].

7.7. Insiders

The University is a very large and complex organization with many employees and several students. The insider is someone that is dissatisfied or otherwise holds a grudge against leaders, the organization, or others [55]. According to Ncube and Garrison [2], an *"Insider involves misuse of access/authority of computer usage by an employee or former employee."* The motive is revenge and the aim is often to create as much harm as possible. Since they often act alone, they have low capacity, but have high capacity with knowledge and access to systems, weaknesses and values, or as Potter puts it [69]: "They are as well resourced as you let them be." Insider attacks were the cause of 1% of attacks in Ncube and Garrison [2] and 3% in Grama [60]. Verizon lists *Grudge* as the motive behind 2% of the recorded incidents in 2020 [64].

7.8. A Summary of the Threat Agents Facing HE

We propose the generic HE threat model with references in Table 13 built on common practice [12,69]. We have linked the actors to motivations, intentions, and threat events in the Table. By reviewing the sources, we found a high degree of agreement that the primary threat agents are (i)*"Cyber-crime and enterprise-like criminals"*, which can be groups or individuals in it for financial gain. This category is mentioned by all the sources who discuss threat agents. (ii) *State-sponsored Cyber Espionage"*, who can be state-sponsored groups tasked with information gathering and espionage. The latter can also be classified as *Advanced Persistent Threats*. Their motivation is to steal classified and valuable information. Additional threat agents mentioned in the literature are cyberstalkers looking to exploit HE infrastructure to hide their activity and pursue their victims [5], and competitors looking to gain an unfair advantage [55]. Students looking to gain an unfair advantage is a threat specific to HEI that should also be considered in various scenarios.

Table 13. Proposed generic threat model for HE, sorted on threat, motivation, intention, events, and likelihood assessment.

Threat	Motivation	Intention	Threat events	Citations
Cyber-crime	Financial	Unauthorized access, Deny Access Infrastructure hijack	Malware, Hacking, Social engineering, Abuse, Botnets, Stolen Credentials. Fraud	[2,5,8–10,55,61–66]
State sponsored espionage	Intelligence, Political	Unauthorized access, Data gathering	Sophisticated attacks: Social engineering, Tailored malware, Persistent access, credential harvesting	[5,6,8–10,55,58,61–66].
Human errors	Carelessness	N/A	Data loss, Data leakage	[2,58,60–64]
Opportunists	Self-assertion, Fun	Exploitation, Infrastructure hijack	Hacking, Copyright violations, DDoS	[8,9,55,58]
Chaotic actors Hacktivists	Ideology, Political	Damage reputation, Sabotage	DDoS, Spear-phish, Website hacking	[5,55,61–66]
Insider	Grudge	Sabotage	Rights abuse, Physical destruction, Data leakage, Denial of Service	[2,8,55,60–64]

8. Vulnerabilities in HE

While Table 2 lists several papers within the "vulnerability" category, it is also the most complex and challenging to describe and quantify. We can induce vulnerabilities that are not directly discussed in the literature. For example, considering the SOC statistics in Chapman [8], the extensive occurrence of DoS attacks indicates an exploitable infrastructure, but it is not explicitly mentioned.

For the presentation of results, we use simplified vulnerability categories from ISO 27005:2018 [11]: (Section 8.1) Administrative (personnel and organization), (Section 8.2) Technical (including hardware, software, and network), and (Section 8.3) Physical (Site). While several more vulnerabilities can be inferred from the literature, our approach is to highlight the most frequently mentioned issues.

8.1. Administrative and Cultural Vulnerabilities in HE

The vulnerabilities within the administrative and cultural domain are well documented and discussed within the literature. Reoccurring topics are security awareness in HE, and academic culture in clash with cybersecurity requirements.

8.1.1. Information Security Awareness and Knowledge

The constant influx of students each year makes it challenging to uphold infosec awareness in higher education. Security awareness in HE was a well-covered area of literature. 33% of all cyber breaches in 2018 utilized social engineering attacks according to Verizon [63], closely followed by "Miscellaneous errors". Al-Janabi and AlShourbaji [43] also document a lack of infosec knowledge and awareness within the educational environment in the Middle East. The study conducted at TEI in Athens had similar findings [44]: The root cause of low infosec awareness in higher education correlated to lack of motivation to follow security procedures. A lack of general knowledge about attacks, users' risky belief, users' risky behavior, and inadequate use of technology, all correlated with a lack of awareness in higher education.

For the Turkish universities, the authors concluded that *"the human factor directly affects every stage"* of infosec work at HEI [4]. Furthermore, the findings underpinned infosec awareness as needing to be present within the top-level management, and for adapting the ISO/IEC 27001 framework. To support these findings, the study from UAE concluded that the low levels of security awareness have a direct relationship with how the faculty views and values the University's information system assets [46]. Finally, the study by Itradat et al. concludes that one of two primary vulnerabilities is inadequate infosec security awareness for the organization personnel [52]. Besides, this issue leads to a misalignment between the information system goals and the institution's strategic mission and objectives.

Furthermore, Wangen et al. [58] found that 60% of the respondents participating in the survey did not know how to report a security incident at the Norwegian University.

Additionally, the study documented a low awareness of infosec issues. Supporting this finding, the root cause analysis conducted at the same University identified low awareness as one of the primary root causes of account compromise [45]. Additionally, low information availability and insufficient security training were both highlighted as key contributors to the problem.

One of the key findings from the UNIT report was the lack of infosec awareness and knowledge [6]. A lack of practical competencies relating to infosec was a reoccurring topic in the report with frequent violations of infosec policies. While Singar and Akhilesh [50] provide a well-known argument that cyber-security managers focus more on technical solutions rather than focusing on the absence of cyber-security awareness among end-users. Furthermore, the authors make the point that cyber-security awareness at HEI in developing countries are more absent than in developed countries.

Vulnerability to social engineering attacks is tightly coupled with security awareness and knowledge, and social engineering attacks represent one of the most frequent attack vectors towards HE [8–10]. Wangen et al. [58] found that the University averaged one security incident per day caused by social engineering. 48% of the survey participants had experienced tailored attacks, and 22% knew about cases where they or their co-workers had fallen victim to such attacks.

8.1.2. Insufficient Information Security Management

Bongiovanni [1] argues that security management is a highly under-investigated topic. UNIT [6] found that several of the surveyed institutions had implemented or where in the process of implementing infosec management systems. However, these were mainly not operationalized due to lack of personnel, resources and limited knowledge of practical infosec and privacy work. We can assume that institutions with smaller security budgets do not invest in security management systems. Additionally, few institutions had contingency plans to restore operations of systems or IT-infrastructure; neither did they know which systems were critical for operations. The six surveyed Turkish universities also scored poorly on aspects within security management, for example, five of them did not have sufficient data classification policies which is a cornerstone of security management. Additionally, all were missing appropriate disposal routines [4]. The case study of the Jordanian University concluded that *"information systems are facing real possible dangerous security breaches due to the presence of a huge number of different kinds of vulnerabilities in their information systems"* [52]. Moreover, the authors write that they assume *"most of Jordanian universities have similar IT setup,"* and they conclude missing ISMS as one of two primary vulnerabilities.

Poor information security management can make the organization vulnerable within several areas: Industrial espionage and illegal data extraction is documented as reoccurring events within the Norwegian university [58]. Not having defined appropriate security policies to address these issues will leave the organization uncertain regarding what is allowed and not. Furthermore, both Chapman [8] and Wangen [9] document copyright and policy violations as significant contributors to incidents. Clarity of both the security policy and the possibility for sanctioning violations are key elements of this vulnerability. Additionally, when polled about security leaks and routines, 11% of the employees at a Norwegian University said that knew about occurrences of data leaks of PII within the five previous years [58]. The same report also documents weak data handling routines. Security management in terms of policy, guidelines, and routines are vital to prevent sloppy data handling. All must be tailored to support the organization's mission.

8.1.3. Insufficient Risk Management and Communication

Appropriate risk management is at the center of all infosec work [11]. FireEye writes that when faced with the balance between openness and mitigating cybersecurity risks, universities often err on the side of openness [5]. In the security compliance check of the Turkish universities, all of the participants were found severely lacking in both vulnerability

(weakness) management and software development security [4], the compliance check of the Jordanian University produced similar results [52]. UNIT reported that while some risk assessments were being conducted, comprehensive risk management was not implemented on any of the surveyed universities [6]. A significant issue was that there was no follow up on identified and planned risk treatments. Furthermore, Nyblom et al. [45] points to insufficient risk reporting and communication channels as critical vulnerabilities in the analyzed university. The UNIT report [6] also found that the GDPR had sparked an initiative to map PII within the universities. However, there was still a lack of overview of sensitive research data and other mission-critical data. This finding did not necessarily indicate that all research data had insufficient secure storage; however, the report addressed that it was unclear regarding the details of how data was secured.

8.1.4. Missing Management Support, Resources, and Finance

Chapman [8] states in his Policy Note that "*Cyber risk cannot be delegated away from the governing body and the executive management needs to be held accountable for ensuring that informed and appropriate decisions are being made which meet or exceed the expectations of any organization's stakeholders – and the law*". This is reflected in Ismail and Widyarto [47], were one interview subject said: "We can't do anything without their [management] authorization they have to support us in implementing information security in the organization." There is a tight connection between management support and financing and resources, and a lack of which can be a root cause of several vulnerabilities in HE. Ismail and Widyarto's case studies unveiled that colleges and universities in Malaysia had insufficient resources to adapt and implement sufficient security policies, caused by limited finical budgets allocated to information security. FireEye [5] also cites financial challenges as present in western HEI, writing that "*The central IT department's share of research grant money is often not enough to secure the data from that research. Despite this mismatch, central IT is still tasked with providing the right level of network security controls*". FireEye points to that it is simply not enough funding to do the job and that most schools cannot afford to hire the experts they need to fill critical security roles. Resulting in an inability to detect, prevent, and respond to attacks. Additionally, CyberEdge [57] claimed that the educational industry suffers the biggest IT security skills shortage among the 19 surveyed different industries. Approximately 91.3% of the participants from HE experienced a shortage of qualified IT security talents, an increase of 4% from the 2018 report [56]. The UNIT report [6] also documented lacking human security resources and capacity, where 19 of the 21 interviewed institutions described insufficient investments in human infosec and privacy personnel to meet the sector demand. Pinheiro [42] also highlights the HE industry as under-funded within information security. He argues that limited budgets for information technology infrastructure cause a high vulnerability in HE, where security investments lose out to equipment needed for school and labs.

8.1.5. Openness, Attitude and Culture

Academic freedom, openness, and transparency are strong norms in higher education, but these values might generate conflict when confronted with cybersecurity requirements [7]. One of the challenges addressed by FireEye is attitude and *cultural resistance* to security measures [5]. FireEye writes that universities might be reluctant to incorporate any changes that may impede research. Security tools, or anything similar, that can limit access to information or communication might be undesirable. It can, therefore, be challenging to implement security controls to protect valuable information. This issue between academia and the security department is named the *"clash of cultures"* by Adams and Blandford [7], which can lead to the circumvention of security mechanisms caused by low usability and largely blame the HE security departments for not appropriately accommodate the needs of the faculty and students.

Ringdalen et al. [55] illustrate how the academic openness culture can be exploited through a spear-phishing experiment: The authors targeted the University's security

department and exploited the openly available information shared by the University to profile the targets. The small-scale experiment succeeded in tricking all of the targets that were uninformed of the attack vector. NCSC also criticizes information availability as a vulnerability that can be exploited in social engineering [10]. Nyblom et al. [45] point to cultural issues regarding low tolerance for security requirements and low loyalty to administrative decisions as key contributors to inadequate security at the social level of the University.

8.1.6. Password Security

Good password hygiene is vital to protect information. However, the number one cause of hacks was the use of stolen credentials in 2018 according to Verizon [63], and password stuffing attacks was the number one attack vector against HE in 2019 [64]. Password stuffing is an attack-type that exploit lists of known usernames and passwords to obtain unauthorized access. When examining the password security at the six Turkish universities, the authors found various practices [4]: all of the participants were severely lacking in password policies for regular and remote users. In comparison, all password policies needed improvement to become compliant. One of the leading causes of security incidents at the Norwegian university was compromised user accounts [9,58]. The findings from the socio-technical root cause analysis in Nyblom et al. [45] supports the Verizon findings: the primary root-causes of compromised passwords were password reuse across multiple services, weak password strength, and low generic awareness. Singar and Akilesh also describe password problems as prominent in HE [50]. Academic accounts get exploited by malicious actors for many purposes, such as harvesting research articles, industrial espionage, and leveraging the university infrastructure to attack third parties [8–10].

8.2. Technical Vulnerabilities in HE

Technical vulnerabilities will vary from one HE institution to the next depending on systems in use and current architecture. The following summarizes the generic findings about the topic for HE, whereas several are tightly connected to the administrative vulnerabilities.

8.2.1. Bring Your Own Device (BYOD)

Bring your own device is the standard for HE, where both students and employees connect their privately-owned devices to the network [50]. BYOD problems occur when the network has an inappropriate security architecture, and poorly implemented access control mechanisms. Typically, trust and authorization in the network will be lacking, meaning that when a person's device is authenticated on the network, it obtains access to most or all of the resources without adequate security mechanisms in place. Security zones are either weak or non-existent, and BYODs roam the network. Singar and Akhilesh [50] discuss the implications of BYOD in HE: Protection against devices that are infected with viruses, primarily through downloading unauthorized content and accessing malicious websites and bringing the compromised device inside the network.

FireEye [5] describes a few of the implications, such as no patch-level awareness for the devices in the network; devices can enter the network being unpatched for months or years, and administrators cannot force patching. Both FireEye, and Singar and Akhilesh argue that in most cases, central IT cannot take responsibility for the security of personal BYODs. Poor network oversight leads to the problem that campus IT has no way of knowing which devices should and should not be connected to the network. Furthermore, FireEye writes that these issues *"add up to massive endpoint environments with little or no control over device-level security"* [5]. They point to the lack of device registrations and basic protection mechanisms which means that anyone can connect to the university network. Problems with BYOD are enhanced technical support, network overload and security issues.

8.2.2. Data Acquisition, Storage, Processing, and Transfer

FireEye found that one of the primary problems is that each academic department or unit is often responsible for storing, processing, and securing its data [5]. This finding is also supported in the UNIT report, which addressed that the personnel had low knowledge of security policies, especially regarding secure research data storage [6]. 5% also knew about data leaks caused by improper data storage in the survey at the Norwegian university [58]. Technical controls for data storage and communication was also missing at the Turkish universities [4]. There are at least two dimensions to this problem: The policies and guidelines must adequately describe proper data management for both administrative tasks and research. Furthermore, the technical systems must be user-friendly and scaled adequately secure to handle sensitive data and be described in the policy. Given the problem described by FireEye on university network security, leaving the employees to create their own data management systems, for example, for research projects, allows for a lot of variance in security measures and is a major vulnerability.

8.2.3. Missing Best Practice Technical Security Controls

Yilmaz and Yalman [4] found that the Turkish universities scored high on the maturity modeling, but they also found various degrees of technical compliance within the control domains. The previously mentioned password security policies scored the worst, together with vulnerability management. Only one University had intrusion detection systems in place at the time. Itradat et al. [52] found that the Jordanian University was lacking in several technical controls. FireEye also comments on this issue for US universities [5], writing that they lack threat intelligence regarding events and log data. Missing network monitoring prevents efficient incident detection and response, as it will be very challenging to detect and respond without appropriate tools. Additionally, FireEye comments that, for those who have implemented network monitoring, the university network traffic is so diverse that they will be flooded with low-level alerts, preventing efficient response. The UNIT report also addressed that some institutions had implement mitigation method to limit the damage of a cyber-attack by conducting backups [6]. Considering the statistics in the threat event Section (Section 6), some findings point to missing baseline security measures: A portion of the incidents reported being caused by malware, hacking, and vulnerabilities are likely connected to missing security controls. For example, vulnerable systems should either be patched or hidden behind a firewall. Hacking attacks are also demanding on a hardened security system. More specifically, the Verizon report points to *Web application*-attacks and backdoors accounting for about 90% of all hacking attacks against HE in 2018 [63], indicating poor technical security in web applications. Furthermore, over 75% of the recorded incidents targeted servers. There are strong indications of varying technical security in HE.

8.2.4. Vulnerability Caused by Technical and Network Complexity

Pinheiro [42] points to the security challenges in having a complex and distributed IT architecture, and having to secure the different environments at a common university. UNIT found that several Norwegian universities had experienced an increase in technical complexity [6], which made working with infosec and privacy more challenging. The networks in the surveyed HE organizations had developed organically over time and were developed to support research and development activities, not for security purposes. The organic approach has led to large and complex networks that are hard to defend from a security perspective [5]. NCSC writes that *"many university networks contain a collection of smaller, private networks, providing close-knit services for faculties, laboratories and other functions. The freedom this offers is balanced by the challenge it presents to protecting the data and information within"* [10]. FireEye also points to *decentralized and poorly documented networks* as a major challenge in universities [5], and that issue leads to poorly documented networks merged into a single, unsegmented network. Patching an organic network is a challenge, and the statistics show *Vulnerable asset* make up 682 and *Compromised assets* 95 of the handled

incidents in UNIT [6]. Additionally, in Wangen [9], *Vulnerable asset* was the cause of 71 of 550 incidents and *Compromised Asset* as the cause of 107 incidents.

Most of the reviewed sources discuss the occurrence of- and vulnerability to malware and hacking events, Table 11. These threats are typically associated with either technical vulnerabilities or social engineering. For example, Wangen [9] examines the causes of incidents and shows that vulnerable systems are exploited in DoS and amplification attacks. This issue is typically a sign of unpatched and exploitable systems. Similarly, both Verizon reports [63] and Chapman [8] provide statistics that prove DoS attacks as prevalent in HE. Organic networks, combined with unmanaged devices, and poor network segmentation, leads to a large attack surface for the University networks [5]. NCSC writes that *"when [networks] are maintained with minimal central oversight or adherence to security policy, private networks are likely more vulnerable to persistent infection or unauthorized access"*[10]. However, NCSC also points to that there is also opportunity in managing the networks in this manner as the separate "private" networks can be secured differently according to the information they handle. However, having a "loose" security policy regarding network devices creates challenges within configuration management and patching for the central IT services [5].

8.3. Physical Security in HE

Physical security is also an essential aspect of information security as it can lead to hardware loss, espionage, and data theft. The physical security will be very dependent on geographical location and vary from one university to another. However, we found some generic discussion on the physical vulnerabilities on University campuses:

Related to the academic culture being open and inclusive, universities practice very little physical security in general. FireEye writes that there is an obvious lack of physical security on US university campuses as they have no physical access controls [5]. Furthermore, FireEye writes that if they do, they cannot enforce the access control or determine who caused a security incident. We see from the statistics in Table 11 that threat events such as *Stolen*, *Missing*, *Loss of portable/stationary device*, and *Physical* are frequent causes of incidents at the universities. These threat events are all caused by weak physical access control and physical equipment security. Considering the findings at the Turkish universities [4], the six participants score moderately well on when considering physical security, three out of six needs improvement, while the remainder meets best practice.

Digging into the issues regarding of physical access control, Wangen et al. [58] found that a total of 161 out of 532 (30.3%) had lent their access card and given the PIN to others. Furthermore, 9 out of 532 answered that they knew of security incidents directly caused by card lending. Seventeen answered that they had lost devices containing information belonging to the University and one respondent commented that he knew about lab equipment theft, indicating multiple unrecorded incidents.

8.4. Summary of the Vulnerabilities in HE

It may have become evident to the reader that the three "vulnerability domains" are tightly connected, where policy and budget decisions span the whole problem area. For example, the cultural aspects have deep roots in academia and directly impacts management thinking: for example, physical security, where openness is the dominating factor, and security restrictions might be undesirable. Furthermore, a lack of investment in central IT and cybersecurity will lead to fragmented networks with weak segmentation and security control, and not investing in security training will lead to negligent staff with a higher probability of data leaks. However, there are regional differences to consider when we discuss vulnerabilities, for example, the physical security on the surveyed Turkish universities was adequate in some areas [4], while the universities considered by FireEye received a lot of criticism [5].

9. Analysis and Discussion of Cyber Risks and Countermeasures in HE

Grama [60] wrote that potential direct financial costs of a data breach in HE could include legal representation, fines, and the expense of notifying affected individuals. Furthermore, HEI might face a loss in reputation and consumer confidence. Consequences can be quantified in a loss of alumni donations, research grants, partners, or even a reduction in student applicants, following a serious data breach. In this section, we summarize the findings, propose generic risks for HE, and give brief descriptions how they can occur in HE based on the prior findings, summarized in the Tables 5, 11, 13 and 14. The section starts with a frequency and risk analysis of the threat events. The threat events are only ranked based on frequency, but we provide a description of the possible consequences with examples. Countermeasures are briefly discussed in this section, however, for a more in-depth discussion on how to work with generic risk mitigation in HE [33–35], or ISMS implementation methods in HE [4,52], and for risk management [12].

Table 14. Summary over vulnerability classifications, descriptions, and citations.

Classification	Description	Citations
Administrative	Insufficient Security Awareness and knowledge	[4,6,8–10,43–46,50,52,58,61–64]
	Insufficient information security management	[1,4,6,8,9,52,58]
	Insufficient risk management and communication	[4–6,45,52]
	Missing management support, resources, and finance	[5,42,47,56,57]
	Openness, Attitude and culture	[5,10,45,55]
	Password Security	[4,9,10,45,50,58,61–64]
Technical	Bring your own device (BYOD)	[5,50]
	Data acquisition, storage, processing, and transfer	[4–6,58]
	Missing best practice security controls	[4–6,9,52,61–64]
	Vulnerability caused by technical and network complexity	[5,6,8–10,42,61–64]
Physical	Physical security in HE	[5,58]

9.1. Risk Analysis

We have synthesized the data presented in Table 11 for further analysis. However, we left out the data from Chapman because he did not provide the distribution numbers. Besides, we assume that the events recorded in Ncube and Garrison [2] and Grama [60] are subsets of the 604 events analyzed in Mello [53]. Furthermore, the distribution was also missing for the threat events ranked 4–8 in UNIT [6], the remaining 10% in UNIT was categorized as *Other*. Since the threat event categorization is distinct for all the included sources [6,9,53,61–66], we grouped together similar threat events together with a description. The compiled dataset consists of 2984 threat events, Table 15. Although not included in the Table, the results from Chapman [8] shows the most frequent events as malware infections, copyright violations, compromise, and DoS-attacks (Table 11), which means that "Intrusion, malware, and compromise" is likely the most frequent threat event in HE. Furthermore, according to the Chapman-data, both the "Abuse and misuse" and the "DoS/DDoS" categories likely occurs with higher frequency in an HEI than depicted in the Table 15.

An event cause comprises of a threat agent exploiting a vulnerability, and an incident can occur in several ways. Taking the most frequent threat event, "Intrusions, malware, and compromise" (29%), as an example—We start by identifying motivated threat agents (Table 13) and vulnerabilities (Table 14) together with the attack vectors for exploitation. *Missing best-practice security controls*, poor *Password security*, and *Technical and network complexity* all present ways to compromise a network through different attack vectors. *Cybercrime* is the most frequent threat facing HE, and once inside the network, the threat agent will act on their financial motives, for example, by stealing easily marketable information, such as PII, research data, and credential harvesting (Table 5). Another option for the

criminal is to encrypt data with ransomware. The former leads to data leakage and the latter to data and availability loss, as illustrated in Figure 3.

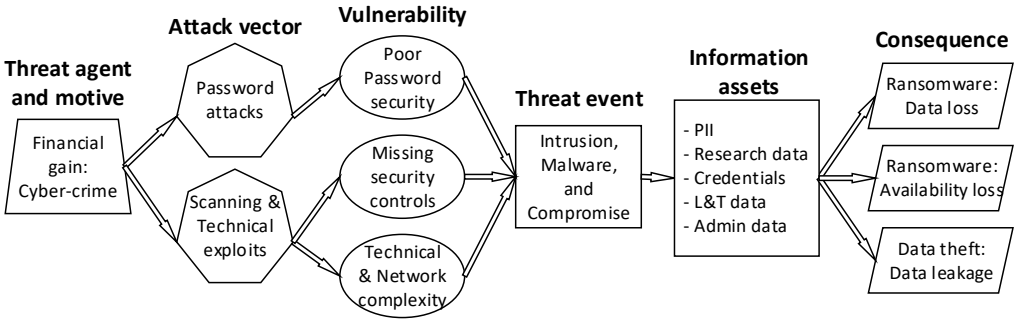

Figure 3. Risk analysis combining threat agents, vulnerabilities, events, assets, and consequences, for the "Intrusions, malware, and compromise"-events.

Table 15. Categorized and merged threat events from the findings in [6,9,53,61–66], n = 2984.

Threat Event/Incident	Description	Freq.	%
Intrusion, malware, and compromise	Electronic entry by an outside party; data loss via malware, spyware, and hacking. Also includes compromised asset.	864	29.0
Vulnerable assets and scanning	Organizational property that is vulnerable to external and internal attacks, or adversaries scanning for vulnerabilities.	852	28.6
Social Engineering and targeted attacks	Frauds primarily attempted through phishing scams, targeted attacks, and intrusion attempts towards the organization.	324	10.9
Unintended disclosure and error	Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail.	311	10.4
Device or document loss or theft	Lost, discarded, or stolen devices (e.g., laptop, PDA, PC, smartphone, portable memory device, CD, hard drive) or stolen non-electronic records such as paper documents.	187	6.2
Unknown or other	Breaches that do not fit into the other categories or where a root cause has not been determined.	165	5.5
Account hijack/Compromised user	A compromised user is when the username and password of an account get compromised.	142	4.8
Abuse and misuse	Law or policy violations through abuse and misuse of Infrastructure for copyright infringement, illegal hosting, cryptomining, etc.	117	3.9
Insider attacks	Intentional breach of information by someone with legitimate access.	17	0.6
DoS/DDoS	Denial of service (DoS) occurs when a service or asset becomes unavailable.	6	0.2

Table 16 proposes a generic connection between threat events, vulnerabilities, threat agents, assets, and consequences for all the threat events. The second most frequent event is "Vulnerable assets and scanning" with 28.6% of incidents. This threat event is directly connected to technical vulnerabilities, such as missing best practice controls and complexity. However, technical vulnerabilities often occur due to missing maintenance and patching, and as such, can be connected to the vulnerabilities highlighted in the administrative domain, such as insufficient infosec management combined with missing resources and financing for security work. While a poorly secured system can be exploited in many ways, the results document that HEI assets are frequently exploited in different kinds of *Abuse and Misuse*.

"Social engineering and targeted attacks" are attacks designed to exploit weaknesses in security awareness and knowledge. However, these attacks are common to most sectors and industries [61–64]. What stands out in HE, is that social engineering attacks are eased by the openness and information sharing in HEI [55]. Cyber-criminals typically conduct Social engineering attacks for financial gain. Phishing-attacks is a large contributor to account hijacks in HEI [9,45]. We associate "Unintended disclosure and errors" with vulnerabilities such as insufficient security awareness, insufficient security management, and the security culture. Furthermore, inappropriate systems for data handling can also contribute to the problem on a technical level. "Device or document loss or theft" is

typically associated with physical security violations or poor security routines, where equipment is left unattended or unsecured.

Table 16. Vulnerability, threat, asset, and consequence analysis of the top threat events.

Threat Event/Incident	Vulnerability	Threat	Asset	Consequence
Intrusion, malware, and compromise	Missing security Controls Security awareness Security culture Password security BYOD Missing security controls Complexity	Cyber-crime State sponsored esp.	Info assets. for example: PII Research data Credentials Financial data IT supporting ser.: Bandwidth Comp. resources Comm. systems	Data loss Data leakage Availability
Vulnerable assets and scanning	Missing resources and finance Missing security controls Complexity	Cyber-crime State sponsored esp. Opportunists	IT supporting ser.: Bandwidth Comp. resources Comm. systems	Abuse/Misuse Availability loss
Social Engineering and targeted attacks	Security awareness Security Culture Missing security controls	Cyber-crime State sponsored esp.	Info assets, for example: PII Research data Credentials Financial data	Fraud Data leakage
Unintended disclosure and error	Security awareness Insufficient security management Security culture Data acquisition, storage, processing, transfer	Human errors	Info assets	Data leakage Integrity loss Availability loss
Device or document loss or theft	Insufficient security management Physical security in HE	Human errors Criminals Opportunists	Physical devices Physical Documents	Hardware loss Data loss
Account hijack Compromised user	Security awareness Password security	Cyber-crime State sponsored esp.	Credentials	Data leakage Data loss Abuse/Misuse
Abuse and misuse	Insufficient security management Security culture Missing security controls	Opportunists Insiders	IT resources, for example: Bandwidth Comp. power Hosting Subscriptions	Abuse/Misuse Availability loss
Insider attacks	Insufficient security management Missing security controls	Insiders	Info assets IT resources	Data leakage Data loss Integrity loss Availability loss
DoS/DDoS	Insufficient security management Missing resources and finance Missing security controls Complexity	Cyber-crime Opportunists Hacktivists	IT resources	Availability loss

Nyblom et al. [45] researched the root causes of 72 compromised users at a Norwegian university, and found that users re-using their university password caused 42% of the reviewed incidents. Other common causes were weak passwords (25%), malware infections (19%), and successful phishing attacks (10%); these causes are typically associated with security awareness and password security routines. "Abuse and misuse" make out 3.9% of the incidents, and happens when employees and students exploit University resources for personal gain or amusement. These incidents are typically a result of insufficient security management with scant consequences of policy violations, and missing security controls for both prevention and detection. Insider-attacks seemingly occur at a low frequency in HE, but they can have severe consequences as the threat agent will have capacities to cause much damage. With both a diverse workforce and a high-turnover, it is hard to reduce malicious insiders' probability. However, the key element in mitigating the consequences of insider-attacks is to limit the access of the threat through the implementation of the *least privilege* and *separation of duties*-principles. Finally, denial of service attacks targeting HEI is uncommon in the compiled dataset (0.2%). Chapman describes DoS attacks as popular among students and employees, but these are not statistics.

In the following sub-sections, we will describe the possible consequences of the described risks, together with examples of publicly known incidents. We leave it to the reader to determine which outcome is the most severe.

9.2. Data Leaks

Data leaks are often the focus in cybersecurity, and severe incidents have already occurred [1,5]. We identified several valuable information assets in HE that needs protection, notably both student and employee PII, passwords, financial information, and research data, were all frequently mentioned. Targeted attacks by state-sponsored espionage and cyber-crime aim for such information, Table 13. Espionage can aim to map the organization and obtain a technological advantage. Organized crime will primarily look to sell obtained information for financial gain. The most common attack vector in HE is social engineering in spear-phishing emails and other hacking attacks, exploiting the weak security culture or technical security. The attacker will likely install malware for persistent access once inside the network, Table 11. An example of a persistent hacking attack hit the Australian National University targeting and extracting student and employee PII over multiple years (https://www.abc.net.au/news/2019-06-04/anu-data-hack-bank-records-personal-information/11176788 (Visited 1 November 2020)). There are also publicly known industrial espionage attacks targeting universities, such as against the Norwegian University of Science and Technology where the perpetrators extracted information illegally and shared it with another nation (https://www.ntnu.no/nyheter/en/two-employees-are-charged-with-contributing-to-data-breaches/ (Visited 1 November 2020)). The constant influx of new students, external guest and employees does also present the potential risk of opportunist and unfaithful servants in the HE environment. Foreign intelligence services have also been known to target vulnerable employees from their home country in the academic environment [70].

Additionally, the results document that data leaks can occur in multiple ways. Unintended disclosure can be caused by, for example, human error combined with poorly documented data handling routines and security management, both in the research and administrative processes. Weakly configured systems can leak data publicly. Hacktivists are a threat for universities working with politically controversial material, which can gather sensitive data and release it for political gain.

Countermeasures: Implementing sufficient information security strategies to academic institutions might mitigate data leakage. The doctoral thesis from Compton [71] addresses that University data custodians should implement, promote, and monitor comprehensive information security strategies to protect university PII and minimize the adverse effects of a data breach. These strategies, including training, monitoring and new defensive technologies, while implementing positive social change, include potential leadership awareness and culture.

9.3. Data Loss

Irrecoverable data loss is a dreaded risk. Ransomware encrypts data and demands a ransom to decrypt it. Ransomware can enter the network via different channels, for example, phishing emails, software vulnerabilities, BYOD, and other hacking attacks. Ransomware attacks are particularly severe when networks are poorly segmented, as the attacker can, manually or automatically, traverse significant parts of the network unhindered and encrypt data. Furthermore, if the information is not backed up, or the backups are poorly protected, ransomware can lead to irrevocable data loss. Multiple universities have already ended up paying the ransom in the face of a data loss caused by ransomware. In 2020 alone, known cases include Maastricht University paying 250 thousand Euro in January (https://nltimes.nl/2020/01/24/maastricht-univ-paid-eu250k-ransomware-hackers-report (Visited 1 November 2020)), University of California paying 1.14 million dollars in June (https://www.bbc.com/news/technology-53214783 (Visited 1 November 2020)), and the University of Utah paying 457 thousand dollars in August (https://attheu.utah.

edu/facultystaff/university-of-utah-update-on-data-security-incident/ (Visited 1 November 2020)). Consider the asset lists in Tables 4 and 5, how much did it cost to produce these assets and how much should be spent on adequate protection? There is also no guarantee that the attackers will restore data upon received payment.

Countermeasures: Adapting a sufficient information security framework to minimize the information security risk at an academic institution is essential. Yilmaz and Yalman [4] highlights in their paper that university that had adapted the ISO/IEC 27001 were more successful in counteracting data loss and information security risks. Data loss can also occur through human or system error combined with inadequate security routines and backup. Taking backup is a well-known security measure that is easily overlooked. For example, all of the Turkish Universities had backup, but only one of six had tested restoration from backup [4].

9.4. Financial Fraud

The findings document *cyber-crime* as the main threat actor for academia. Primarily motivated by financial gain, this actor infiltrate systems and routines looking for financial and transaction data for exploitation. Fraud is conducted mainly through social engineering, looking to exploit weak security routines or low-security awareness. Criminals can also leverage extortion techniques to coerce universities and employees into paying money. A popular attack vector is hijacking acquisition processes through social engineering and sending false invoices to the target. This attack technique succeeded tricking, for example, the University of Tromsø into paying 1.2 million Euro (https://uit.no/nyheter/artikkel?p_document_id=659434 (Visited 1 November 2020)).

Countermeasures: A potential countermeasure for financial fraud is implementing sufficient security policies and awareness training in the organization. The paper from Rezgui and Marks [46] highlight several recommendations to implement information security awareness training in higher education. These recommendations include information security awareness campaigning, training users on information system security best practices, practice reward and punishment and continuous evaluate and readjust, to name a few.

9.5. Loss of Service Availability

Universities are high availability organizations considering services such as the internet connection, email systems, and digital libraries. For most universities, core processes will immediately suffer if critical services become unavailable. Weak risk management regarding not identifying essential systems and not making contingency plans is a significant vulnerability in HE. Under-staffing when operating security-critical systems is also a vulnerability, especially when personnel is unaware of its critically. Random errors can cause prolonged downtime and service level reduction if the HE institution is missing the appropriate workforce to restore the system quickly.

A large attack surface means many targets for both hacking and DoS attacks. The possibilities for sabotage are many—Intentional DoS attacks can cripple parts of a poorly protected institution's IT service delivery. Hacking attacks can cripple and shut down servers. Random errors can also lead to critical incidents in systems supporting IT communication, such as email. Furthermore, the Corona-pandemic in 2020 forced the HE sector to digitize. This development increased the requirements of IT-system availability to conduct core functionality, such as teaching.

Countermeasures: Potential countermeasures for mitigating loss of availability can include conducting backups, updating and patching programs, and implementing incident response and management policies [42,72]. Identifying and prioritizing mission-critical systems is essential when planning for redundancies and business continuity.

9.6. Abuse and Misuse of University Infrastructure and Resources

4% of the incidents in Table 15 and copyright violations is ranked the number two incident cause in Chapman [8]. Universities possess a broad range of computing resources,

hosting opportunities, subscriptions, and bandwidth. The review results show that these assets can be abused by threat agents ranging from non-malicious to worst-case scenario. Several sources mention *The Silent librarian campaign* where cybercriminals exploited compromised University accounts to steal thousands of research articles. Both criminals and insiders look to exploit University computing resources for cryptojacking for financial gain (mining for cryptocurrency using resources they do not own) [58]. Another severe risk from weak security controls occurs when the University infrastructure is abused by criminals as a stepping stone to attack third parties. Typically, they either hide the attacker's true identity or masquerade the attack as legitimate traffic between the University and the target. The resources can also be abused for cyberstalking [5].

More benign types of abuse are copyright violations caused by illegal hosting and downloading on University networks. Our results show that these violations are commonplace in HE.

Lastly, our results have documented large amounts of DDoS attacks occurring on the University networks. Again, this can be a relatively benign activity, for example, when students attack each other for fun, but can also be very serious when vulnerable network resources are leveraged by criminals to attack third parties.

Countermeasures: A centralized IT governance could potentially mitigate abuse of infrastructure and resources at HE. The papers from Liu et al. [31,32] investigates the correlation between IT centralization, outsourcing and cybersecurity breaches in U.S. The authors found that both centralized IT and outsourcing are associated with fewer breaches. This was due to the establishment of uniform control and organization-wide security policies, better strategic alignment, and well-defined accountability. In addition, centralized IT governance facilitates universal compliance with security protocols, resulted in better security information sharing, raised awareness of security issues, and enhanced coordination between business units. The white paper from FireEye [5] does also highlight several recommendations to counter abuse. The paper recommends implementing two-factor authentication, segmenting networks, implementing incident response plans, recording data traffic, and increasing communication flow.

9.7. Integrity Loss in Key Assets

One of the most critical information assets managed at the university is student records and the finishing diplomas. The incentive is obvious for students to hack and illegitimately change their grades for the better. However, a large-scale incident with changed exam grades and a loss of integrity in issued diplomas would be critical. Untrustworthy diplomas would be devastating for most HEI. Furthermore, integrity attacks on research data sets to sabotage competitors is also a likely scenario. Universities are also responsible for various payments and invoicing. Consider the possibility of such information being wrong, and either paying the wrong employee or billing the wrong recipient. Integrity risks are also present in HEI.

Countermeasures: Identify the assets with mission-critical integrity and risk manage them appropriately. Implement proper infosec management, including access control, backup functionality, and integrity checks.

10. Limitations and Future Work

Our findings correspond to the findings in the recent review article by Bongivionni [1] who also documented a scarcity of sources within his surveyed topics for HE. Following the review method [36], we chose to add Norwegian sources to enrich the data set. This choice might have skewed the results towards risks faced by European universities, but the majority of findings where already from Europe and the US. Eight sources were from outside US and Europe, and two studies were international. Future studies should aim to validate or reject our findings for their local universities.

10.1. Future Work within HE Risk Management

The amount of empirical studies featuring information assets in higher education was quite limited. We identified one relevant academic resource [40], which was not written for risk assessment purposes and thus did not feature a holistic and adequate representation of the information assets featured in a HE institution or a ranking said assets. While multiple sources mentioned critical assets in their description, for example, Table 5 illustrates a vastly more complex picture than that listed in the reviewed risk literature. The level of value these information assets possess, can also be disputed. The reason for this might be the complexity of quantifying information assets in higher education. A call for more studies to examine the value of information assets in higher education would be beneficial, both for the HE security community and researchers. As modern HEI can be considered as enterprises, one can research comparisons with industry who have similar enterprise systems and expand the understanding.

The literature search identified peer reviewed sources researching infosec vulnerabilities in HE. While there is room for more research, the most saturated area was *cybersecurity awareness* in HE (Table 14). However, significant effort should be put into improving security awareness in HE, through both research and training. Raising awareness and discussing the issues highlighted in our research is a start. It is also likely that cybersecurity will become a competitional advantage in future research grant applications, especially within the STEM disciplines.

One paper focused on comparative analysis of compliance to technical security mechanisms [4]. In this study, the six surveyed universities scored high on security maturity and were probably well ahead of the average HE institution within infosec and not representative. Nevertheless, this was an interesting study which yielded interesting results. A path for future work is to conduct similar maturity modeling studies of international universities to expand the knowledge and increase security compliance.

Other topics regarding vulnerabilities in HEI were either absent or not specifically described in the academic papers, but documented in technical reports and white papers instead. This issue might be caused by the sensitivity level and possibility of reputational loss in HE by going public with this information. Only FireEye [5] and UNIT [6] attempted to provide a holistic overview of the vulnerabilities in HEI. Generally, academia should be more willing to publish vulnerability and incident data for researchers. More empirical studies of security vulnerabilities in HE would be beneficial. Cloud security in HEI was also an area with scarce information.

We also researched threat agents in this study and proposed a generic threat model for HE. More research and understanding of the threat landscape will allow for better security decision-making when planning for research and administrative tasks.

10.2. Critique of Incident Statistics

The amount of white papers and technical reports depicting information security threats in higher education was also scarce. However, these white papers and technical reports have weak sources as they are usually referencing news articles and other media regarding the events.

We also found the number of reported events in several of the white papers and technical reports highly questionable, considering for example, the 2019 Verizon data breach report where $n = 99$ for HE [63] or the Hackmageddon numbers with $n = 74$ for 2018, and $n = 174$ for 2019. The data provided in Ncube and Garrison [2] is 11 years old and only contains 290 incidents collected over 5 years from multiple universities. Comparing these numbers to the $n = 550$ for one year of data collected at one university [9], approximately 6100 from JANET [8], or the $n = 965$ from the UNIT report [6] confronts us with a two-fold problem: Firstly, it is highly likely that there is incomplete and biased data combined with under-reporting in the previously mentioned commercial reports. Where the latter may be caused by local detection capacity which is a major component in incident management. Herein also lies the problem of the reports provided by the commercial security companies:

The data is highly biased towards the security company's tasks, privileges, and detection capacities within the client's networks. Another limitation is that these capacities are often of a technical kind, such as intrusion detection systems and centralized anti-malware solutions. This technical bias is evident in the statistics from Hackmageddon, Table 10, and Verizon, Table 9, both of which primarily reporting only about attacks detectable by such means. The second part of the problem with the incident statistics is that there is no unified approach to neither defining what a security incident is nor how to classify it. Our findings clearly document the ambiguity in the reporting of security incidents. Consider the incident classifications documented in Tables 7, 9 and 10, Figure 2. While the vocabulary is similar, the reporting is different from source to sources. This problem leads to a level of incomparably of the reported data and is also discussed extensively by Wangen [9]. HE needs to agree on an incident classification to allow for data comparison and aggregation.

Furthermore, there is are interesting differences in the sector CERT/SOC data and the data published directly from the Norwegian University, but the data is to scarce to draw any conclusions. Both HE sector and University CERTs and SOCs should be encouraged to publish more statistics directly to the scientific community.

10.3. Scarcity of Sources

The findings in this paper was limited by a scarcity of reliable sources, and we have already argued the need for more studies. The U.S. studies Ncube and Garrison [2], Grama [60], and Mello [53] all reference the PRC as the primary data source. The Policy Note with incident data from JANET by Chapman [8] is currently becoming one of the most cited sources within the topic according to Google Scholar. However, the Policy Note is neither an academic paper nor does it contain proper explanations of how the statistics was gathered and treated. We interpret this trend towards that cybersecurity in HE is in high need of reliable data and peer reviewed research to advance. The most dominant literature regarding cybersecurity in HE consist of risk management and other proposed security frameworks, and is lacking in epistemology. HE is in need of research and empirical studies regarding information security assets, threats, vulnerabilities, and risk. A research path would be validation studies of the findings presented in this paper.

11. Conclusions

While the amount of research papers on cybersecurity is growing extensively, our findings show that empirical research on security practices within HE itself is severely lacking. The question still remains if HE wants to leave this crucial area to commercial security vendors? Our results call for more empirical research within HE cybersecurity risks. The HE sector SOCs and CERTs should be more willing to share incident data with the community and work towards a common incident classification framework for reporting. Maturity modelling and baseline studies are also promising research paths for improving the knowledge base of security practice in academia.

Despite being compiled from sources with varying credibility, the sources largely agreed on the following for HE: The most valuable assets managed in academia are PII on students and employees, financial data, research data, IP, student grades, and administration details. The most frequent threat events were intrusion, malware, and other forms of compromise. Vulnerable assets and scanning were also frequent causes of incidents. Social engineering attacks and unintended disclosures are also frequent occurrences in HE. Organized crime, state-sponsored espionage, and human errors were the most prominent threat agents in higher education. These threats can exploit vulnerabilities in the HEI's administrative, technical, and physical domains, such as the lack of information security knowledge and awareness, or the missing best-practice security controls. By combining the literature review findings, we proposed a generic analysis for nine high-level cybersecurity risks common to HE. The consequences of these risks were discussed in six broad categories: *Data leakage*, *Data loss*, *Financial fraud*, *Loss of availability*, *Abuse*, and *Attacks on*

data integrity. Strategic countermeasures to said risks are only superficially addressed in this work.

The primary conclusion of this systematic review is that more research is needed within the area. Our findings highlight several focus areas within infosec in HE that practitioners can use for strategic infosec work in HE. Furthermore, our findings have also brought new knowledge on cybersecurity risk in HE.

Author Contributions: Conceptualization, J.B.U. and G.W.; Background, J.B.U. and G.W.; methodology, J.B.U.; formal analysis, J.B.U. and G.W.; investigation, J.B.U. and G.W.; resources, J.B.U.; Data curation, J.B.U. and G.W.; writing–original draft preparation, J.B.U. and G.W.; writing–review and editing, J.B.U. and G.W.; visualization, J.B.U. and G.W.; supervision, G.W.; project administration, J.B.U. and G.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not Applicable, the study does not report any data.

Acknowledgments: The authors acknowledge the help provided by Einar Snekkenes, Stian Husemoen, and the NTNU risk assessment team. The authors also thank the anonymous reviewers for their invaluable comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CERT	Computer Emergency Response Team
CLR	Comprehensive Literature Review
DoS	Denial of Service
GDPR	General Data Protection Regulation
HE	Higher Education
HEI	Higher Education Institutions
infosec	Information security
ISMS	Information security management system
ISRA	Information Security Risk Analysis/Assessment
IT	Information Technology
KPI	Key Performance Indicators
MODES	Media, Observation(s), Documentation, Expert(s), Secondary Data
NCSC	National Cyber Security Centre
PII	Personal Identifiable Information
PRC	Privacy Rights Center
SOC	Security Operations Center
STEM	Science, Technology, Engineering, and Mathematics
UNIT	The Norwegian Directorate for ICT and joint services in higher education and research
QUT	Queensland University of Technology

References

1. Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education. *Comput. Secur.* **2019**, *86*, 350–357. [CrossRef]
2. Ncube, C.; Garrison, C. Lessons learned from university data breaches. *Palmetto Bus. Econ. Rev.* **2010**, *13*, 27–37.
3. FireEye, Inc. Cyber tHreats to the Education Industry. White Paper, 2016. Library Catalog. Available online: www.fireeye.com (accessed on 28 January 2021).
4. Yilmaz, R.; Yalman, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. *TEM J.* **2016**, *5*, 180–191.
5. FireEye, Inc. Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do about It. White Paper, 2015. Library Catalog. Available online: www.fireeye.com (accessed on 28 January 2021).
6. Unit-Department for ICT and Joint Services in Higher Education and Research. Technical Report, 2019. Available online: https://www.regjeringen.no/contentassets/f464322e9623456dabe220571dfab8f6/unit-okonomiseminar_2019.pdf (accessed on 28 January 2021).

7. Adams, A.; Blanford, A. Security and Online Learning: To Protect and Prohibit. In *Usability Evaluation Of Online Learning Programs*; IGI Global: Hershey, PA, USA, 2003; pp. 331–359.
8. Chapman, J. How Safe Is Your Data? Cyber-Security in Higher Education. *HEPI Policy Note*, April 2019.
9. Wangen, G. *Quantifying and Analyzing Information Security Risk from Incident Data*; Graphical Models for Security; Albanese, M., Horne, R., Probst, C.W., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 129–154.
10. NCSC. *The Cyber Threat to Universities*; Technical Report; UK National Cyber Security Centre: London, UK, 2019.
11. *ISO/IEC 27002:2013 Information Technology–Security Techniques–Information Security Risk Management*; Standard; International Organization for Standardization: Geneva, Switzerland, 2018.
12. Wangen, G.; Hallstensen, C.; Snekkenes, E. A framework for estimating information security risk assessment method completeness. *Int. J. Inf. Secur.* **2017**. [CrossRef]
13. *ISO/IEC 27002:2013 Information Technology–Security Techniques–Code of Practice for Information Security Controls*; Standard; International Organization for Standardization: Geneva, Switzerland, 2014. Available online: https://www.iso27001security.com/html/27002.html (accessed on 28 January 2021).
14. Whitman, M. *Management of Information Security*; Cengage Learning, Inc.: Boston, MA, USA, 2018; ISBN 9780357691205.
15. Ahmed, A.E.A.; Badawy, M.; Hefny, H. Exploring and Measuring the Key Performance Indicators in Higher Education Institutions. *Int. J. Intell. Comput. Inf. Sci.* **2018**, *18*, 37–47.
16. Ulven, J. High level information security risk in higher education. Master's Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2020.
17. Peter, S.; Deimann, M. On the role of openness in education: A historical reconstruction. *Open Prax.* **2013**, *5*, 7–14. [CrossRef]
18. Schlagwein, D.; Conboy, K.; Feller, J.; Leimeister, J.M.; Morgan, L. "Openness" with and without Information Technology: A Framework and a Brief History, 2017. Available online: https://journals.sagepub.com/doi/pdf/10.1057/s41265-017-0049-3 (accessed on 28 January 2021).
19. Whitman, M.; Mattord, H. Threats to Information Protection-Industry and Academic Perspectives: An annotated bibliography. *J. Cybersecur. Educ. Res. Pract.* **2016**, *2016*, 4.
20. Chen, Y.; He, W. Security risks and protection in online learning: A survey. *Int. Rev. Res. Open Distrib. Learn.* **2013**, *14*, 108–127. [CrossRef]
21. Beaudin, K. The Legal Implications of Storing Student Data: Preparing for and Responding to Data Breaches. *New Dir. Institutional Res.* **2017**, *2016*, 37–48. [CrossRef]
22. Beaudin, K. College and university data breaches: Regulating higher education cybersecurity under state and federal law. *J. Coll. Univ. Law* **2015**, *41*, 657–693.
23. Hussain, H.S.; Din, R.; Khidzir, N.Z.; Daud, K.A.M.; Ahmad, S. Risk and Threat via Online Social Network among Academia at Higher Education. *J. Physics: Conf. Ser.* **2018**, *1018*, 012008. [CrossRef]
24. Ajie, I. A Review of Trends and Issues of Cybersecurity in Academic Libraries. *Libr. Philos. Pract.* **2019**, 1–20. Available online: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5803&context=libphilprac (accessed on 28 January 2021).
25. Diaz, A.; Sherman, A.T.; Joshi, A. Phishing in an Academic Community: A Study of User Susceptibility and Behavior. *arXiv* **2018**. arXiv: 1811.06078.
26. Cuchta, T.; Blackwood, B.; Devine, T.R.; Niichel, R.J.; Daniels, K.M.; Lutjens, C.H.; Maibach, S.; Stephenson, R.J. Human Risk Factors in Cybersecurity. In Proceedings of the 20th Annual SIG Conference on Information Technology Education, Tacoma, WA, USA, 3–5 October 2019; pp. 87–92.
27. Dadkhah, M.; Borchardt, G.; Maliszewski, T. Fraud in Academic Publishing: Researchers Under Cyber-Attacks. *Am. J. Med.* **2017**, *130*, 27–30. [CrossRef] [PubMed]
28. Teixeira da Silva, J.; Alkhatib, A.; Tsigaris, P. Spam emails in academia: Issues and costs. *Scientometrics* **2020**, *122*, 1171–1181. [CrossRef]
29. Wangen, G.; Hellesen, N.; Torres, H.; Brækken, E. An empirical study of root-cause analysis in information security management. In Proceedings of the SECURWARE 2017-The Eleventh International Conference on Emerging Security Information, Systems and Technologies. International Academy, Research and Industry Association (IARIA), Rome, Italy, 10–14 September 2017.
30. Kashiwazaki, H. Personal Information Leak in a University, and Its Cleanup. In *Proceedings of the 2018 ACM SIGUCCS Annual Conference*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 43–50. [CrossRef]
31. Liu, C.W.; Huang, P.; Lucas, H.C. *Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. SSRN Scholarly Paper ID 2850178*; Social Science Research Network: Rochester, NY, USA, 2019.
32. Liu, C.W.; Huang, P.; Lucas, H. IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the US Higher Education 2017. Available online: http://penghuang.com/WordPress/wp-content/uploads/2021/01/IT-Centralization-Security-Outsourcing-and-Cybersecurity-Breach.pdf (accessed on 28 January 2021).
33. Dar, W.M. Cyber Security Challenges on Academic Institutions and Need For Security Framework Towards Institutional Sustainability Growth and Development. *i-Manag. J. Inf. Technol.* **2015**, *5*, 1.
34. Luker, M.A.; Petersen, R.J. *Computer and Network Security in Higher Education*; Jossey-Bass: San Francisco, CA, USA, 2003.
35. Custer, W.L. Information security issues in higher education and institutional research. *New Dir. Institutional Res.* **2010**, *2010*, 23–49. [CrossRef]

36. Onwuegbuzie, A.J.; Frels, R. *Seven Steps to a Comprehensive Literature Review: A Multimodal and Cultural Approach*; Sage: Thousand Oaks, CA, USA, 2016; pp. 48–64.
37. Bishop, M. Academia and Education in Information Security Four Years Later. Available online: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=E3FBD07A58F3919A670717FF93B9F419?doi=10.1.1.9.5820&rep=rep1&type=pdf (accessed on 28 January 2021).
38. Orozova, D.; Kaloyanova, K.; Todorova, M. Introducing Information Security Concepts and Standards in Higher Education. *TEM J.* **2019**, *8*, 1017–1024.
39. Johal, J.; Ward, R.; Gielecki, J.; Walocha, J.; Natsis, K.; Tubbs, R.; Loukas, M. Beware of the Predatory Science Journal: A Potential Threat to the Integrity of Medical Research. *Clin. Anat.* **2017**, *30*. [CrossRef]
40. Ballard, P.J. Measuring Performance Excellence: Key Performance Indicators for Institutions Accepted into the Academic Quality Improvement Program (AQIP). PhD Thesis, Western Michigan University, Kalamazoo, MI, USA, 2013.
41. Asif, M.; Searcy, C. A composite index for measuring performance in higher education institutions. *Int. J. Qual. Reliab. Manag.* **2014**. Available online: https://www.emerald.com/insight/content/doi/10.1108/IJQRM-02-2013-0023/full/html?fullSc=1&fullSc=1 (accessed on 28 January 2021).
42. Pinheiro, J. Review of cyber threats on Educational Institutions. In Proceedings of the Digital Privacy and Security Conference 2020, Porto, Portugal, 15 January 2020; p. 43.
43. Al-Janabi, S.; AlShourbaji, I. A Study of Cyber Security Awareness in Educational Environment in the Middle East. *J. Inf. Knowl. Manag.* **2016**, *15*, 1650007. [CrossRef]
44. Metalidou, E.; Marinagi, C.; Trivellas, P.; Eberhagen, N.; Giannakopoulos, G.; Skourlas, C. Human factor and information security in higher education. *J. Syst. Inf. Technol.* **2014**, *16*, 210–221. [CrossRef]
45. Nyblom, P.; Wangen, G.B.; Kianpour, M.; Østby, G. The Root Causes of Compromised Accounts at the University. In *Proceedings of the 6th International Conference on Information Systems Security and Privacy*; SciTePress: Setubal, Portugal, 2020; pp. 540–551. [CrossRef]
46. Rezgui, Y.; Marks, A. Information security awareness in higher education: An exploratory study. *Comput. Secur.* **2008**, *27*, 241–253. [CrossRef]
47. Ismail, W.; Widyarto, S. A Formulation and development process of information security policy in higher education. In Proceedings of the 1st International Conference on Engineering Technology and Applied Sciences, Afyonkarahisar, Turkey, 21–22 April 2016.
48. Noghondar, E.R.; Marfurt, K.; Haemmerli, B. The Human Aspect in Data Leakage Prevention in Academia. In *ISSE 2012 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2012 Conference*; Reimer, H., Pohlmann, N., Schneider, W., Eds.; Springer Fachmedien Wiesbaden: Wiesbaden, Germany, 2012; pp. 137–146._14. [CrossRef]
49. Kim, E. Information Security Awareness Status of Business College: Undergraduate Students. *Inf. Secur. J. A Glob. Perspect.* **2013**, *22*, 171–179. [CrossRef]
50. Singar, A.V.; Akhilesh, K. Role of Cyber-security in Higher Education. In *Smart Technologies*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 249–264.
51. Kwaa-Aidoo, E.K.; Agbeko, M. An Analysis of Information System Security of a Ghanaian University. *Int. J. Inf. Secur. Sci.* **2018**, *7*, 90–99.
52. Itradat, A.; Sultan, S.; Al-Junaidi, M.; Qaffaf, R.; Mashal, F.; Daas, F. Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. *Jordan J. Mech. Ind. Eng.* **2014**, *8*, 102–118.
53. Mello, S. Data Breaches in Higher Education Institutions. In *Honors Theses and Capstones*; University of New Hampshire: Durham, NH, USA, 2018.
54. Fawcett, D. Information Asset Register. 2020. Available online: https://www.qut.edu.au/about/governance-and-policy/information-asset-register (accessed on 1 October 2020).
55. Ola, F.R.; Lasse, S.; Sebastian, B.W.; Arne, M.L. Trusselprofilering og Etterretning i åpne kilder. Bachelor's Thesis, NTNU Open Gjøvik, Trondheim, Sweden, 2018.
56. Group, C. 2018 Cyberthreat Defense Report. White Paper, 2018. Library Catalog. Available online: https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf (accessed on 28 January 2021).
57. Group, C. 2019 Cyberthreat Defense Report. White Paper, 2019. Library Catalog. Available online: https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf (accessed on 28 January 2021).
58. Wangen, G.; Brodin, E.Ø.; Skari, B.H.; Berglind, C. Unrecorded Security Incidents at NTNU 2018 (Mørketallsundersøkelsen ved NTNU 2018). Bachelor's Thesis, NTNU Open Gjøvik, Trondheim, Sweden, 2019.
59. Ellestad, J.N.; Lilja, M.L.; Gustad, A.G.; Skuggerud, E.S. Sikkerhetskultur ved NTNU. Bachelor's Thesis, NTNU Open Gjøvik, Trondheim, Sweden, 2019.
60. Grama, J. Just in Time Research: Data Breaches in Higher Education. *EDUCAUSE* **2014**. Available online: https://library.educause.edu/~/media/files/library/2014/5/ecp1402-pdf.pdf (accessed on 28 January 2021).
61. Verizon. 2017 Data Breach Investigations Report. White Paper, 2017. Library Catalog. Available online: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf (accessed on 28 January 2021).
62. Verizon. 2018 Data Breach Investigations Report. White Paper, 2018. Library Catalog. Available online: https://admin.govexec.com/media/vz_assets/2018_dbir_public_sector_final.pdf (accessed on 28 January 2021).

63. Verizon. 2019 Data Breach Investigations Report. White Paper, 2019. Library Catalog. Available online: https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf (accessed on 28 January 2021).
64. Verizon. 2020 Data Breach Investigations Report. White Paper, 2020. Library Catalog. Available online: https://itb.dk/wp-content/uploads/2020/07/verizon-data-breach-investigations-report-2020.pdf (accessed on 28 January 2021).
65. Hackmageddon. 2018: A Year of Cyber Attacks, 2019. Library Catalog. Available online: www.hackmageddon.com (accessed on 28 January 2021).
66. Hackmageddon. 2019 Cyber Attacks Statistics, 2020. Library Catalog. Available online: www.hackmageddon.com (accessed on 28 January 2021).
67. James, J.G.; Dominic, A.; Paluzzi, S.A.K. *Pass or Fail? Data Privacy and Cybersecurity Risks in Higher Education*; White Paper; McDonald Hopkins: Chicago, IL, USA, 2016.
68. Wangen, G. The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information* **2015**, *6*, 183–211. [CrossRef]
69. Potter, B. Practical Threat Modeling. *Login* **2016**, *41*, 59–63. Available online: https://www.usenix.org/system/files/login/articles/login_fall16_11_potter.pdf (accessed on 28 January 2021).
70. Norwegian Police Security Services(PST). Annual Threat Assessment 2020. White Paper, 2020. Library Catalog. Available online: www.pst.no (accessed on 28 January 2021).
71. Compton, Y.R. Obstacles With Data Security: Strategies From Carolina Universities. Ph.D. Thesis, Walden University, Minneapolis, MA, USA, 2020.
72. Maia, D.V.A. Cyberattacks across academic organisations: Analysis of attacks and guidelines to improve defence. In Proceedings of the 11th International Conference on System Safety and Cyber-Security (SSCS 2016), London, UK, 11–13 October 2016. [CrossRef]