Advances in Reliability, Safety and Security, Part 4 – Kołowrocki, Dąbrowska (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-16-6 (printed), ISBN 978-83-68136-03-6 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Risk Management In Higher Education: Recent Developments And Challenges

Eivind Lorentzen Styr, Marie Røyksund, Terje Aven

University of Stavanger, Stavanger, Norway

Abstract

Risk management in higher education and research institutions has received little attention in the risk science literature, although, in practice, there has been an increased awareness of these institutions' potential risks. The handling of the COVID-19 pandemic in universities and colleges and different cases involving academic espionage and cybercrime demonstrate the need for systematic and prudent risk management in the higher education sector. However, implementing more robust risk management regimes in such an environment could hamper other goals and values typically associated with higher education and research, such as knowledge-sharing, collaboration, and the principle of academic freedom. This paper explores recent trends and developments relevant to higher education risk management and discusses related challenges. The aim is to provide new insights that will contribute to improved risk management in the higher education sector, building on current risk science principles. Finally, we make some recommendations for future work.

Keywords: higher education, risk management, risk assessment, digital transformation, technology development, national security

1. Introduction

There has been growing attention on the potential risks in higher education and research (HE) in recent years. The academic environment represents the forefront of knowledge development and innovation, making HE institutions more exploited to threats from state intelligence and cybercrime (PST, 2023). This development is closely related to the vast digitalization of this sector in the past few years and the geopolitical situation the world is currently facing (Wang et al., 2023). The risk landscape is becoming more complex due to emerging trends such as changes in societal dynamics, technological advancements, and the impact of globalization. Globalization has been identified as a critical factor contributing to large-scale cascading events, including global pandemics (Aven and Zio, 2021).

On the positive side, the developments provide new opportunities in how universities, colleges, and research institutions can be organized and managed. For example, the introduction of various digital tools changed teaching during COVID-19, and the use of the home office has been more common due to easily accessible cloud services. Digitalization in the HE sector has made interconnectivity and collaboration with foreign academic institutions more effective through digital communication mediums and contributed to new business models (Asheim, 2023). However, while digitalization is crucial for effective social and economic resource utilization, it also introduces new vulnerabilities and challenges for risk management. According to Ulven and Wangen (2021), the vulnerabilities are mainly linked to greater digital exposure and attack surface to the outside world. The combination of high-value assets, such as sensitive technology and research areas, and a low level of cybersecurity is one of the main reasons that the HE sector is an attractive target for cyberattacks and espionage (Chin, 2023). A recent report evaluating HE in 31 countries shows that the rate of cyberattacks against this sector increased by about 50% in 2022 compared with previous years (Sophos, 2022). Another report shows that 92% of the HE institutions in Great Britain had identified breached cybersecurity attacks in 2021-2022. These attacks range from phishing attacks (97%), impersonating emails (79%), viruses (59%), distributed denial-of-service (35%), takeover accounts (26%), hacking of bank accounts (18%), ransomware (18%), and several other forms of cyberattacks (Department for Digital, Culture, Media & Sport, 2022).

The risks of academic espionage and illegal knowledge transfer are also issues that HE and research institutions must deal with. For instance, in the National Threat Assessment 2023, the Norwegian Police Security Service (PST) has pointed to research and education institutions as vulnerable intelligence targets in respect of the illegal transfer of knowledge to countries which Norway does not have security cooperation (PST, 2023). Furthermore, in the latest version of the National Threat Assessment (PST, 2024), PST elaborates on the current threats to academic environments. Collaboration among researchers has been identified as a significant concern or risk factor for potentially transferring knowledge illegally (and most often unintentionally). The report also highlights that research and technological developments, in addition to political and business connections, will make Norway more vulnerable to threats from various state-enforced intelligence agencies in the coming years. The National Threat Assessment reports have contributed to increased attention and awareness among higher education and research institutions in Norway in the past few years. To prevent illegal transfer of knowledge, the Norwegian Export Control Regulations require HE and research institutions to assess and evaluate the risks of illegal transfer of knowledge and to establish strategies to avoid such incidents. All the above examples demonstrate the need to establish and develop appropriate risk management strategies at higher education and research institutions, including information security measures to protect critical information values, as well as to protect the well-being of students and employers.

However, implementing stronger risk management regimes in an academic environment could conflict with other goals and values typically associated with research and innovation, such as international collaboration and the principle of academic freedom. For instance, how should HE institutions balance international scientific exchanges ("openness") and the protection of national security, as well as complying with the export control regulations? It is challenging to establish a justifiable and acceptable safety level in this context, and guidance is needed. Recent reviews on risk management in higher education show that this topic has received little attention in the research literature, although the number of studies has increased in recent years (Khaw and Teoh, 2023). Most of the research focuses on enterprise risk management, performance risk management in HE institutions, and information security (Bongiovanni, 2019). Studies that involve issues on how to describe, understand, and handle the risks in higher education and research are, however, not sufficiently addressed in the literature.

In this paper, we provide an overview of some of the main developments and trends that have an impact on HE institutions' risk management by using the Norwegian higher education sector as a case. We argue how concepts, approaches, and methods described in the risk science literature can contribute new insights that will improve risk management in higher education and research, including suitable strategies for decision-making when balancing conflicting concerns. The paper is structured as follows: Section 2 contains a description of the Norwegian HE case that forms the basis for the discussion. Section 3 describes a few of the identified developments and challenges and discusses the implications for risk management in higher education and research. Finally, Section 4 concludes the paper.

2. Overview of higher education and its risk management strategies

In the following, we will give a short introduction to the Norwegian higher education sector and its work with risk and security management and emergency preparedness.

2.1 Roles and responsibilities

The Norwegian higher education sector includes about 30 public and private universities and university colleges. In 2022, nearly 300,000 students enrolled at these institutions[1]. As in most countries, universities and colleges vary in size, organization, and geographic location. Some institutions have their campus located within the city center and thus close to, e.g., emergency services, while others are in provinces, characterized by scenic and wilder environments and longer distances. All higher education and research institutions in Norway are instructed by the Ministry of Education and Research to work systematically with risk management, including developing risk management systems, performing risk assessments, and establishing emergency preparedness plans that involve both intentional and unintentional events (NMER, 2021; Internal Control Regulations, 1997). However, it is relevant to mention that only public universities and university colleges are obligated to meet these requirements. The private institutions are encouraged to follow the same principles and establish a prudent risk management system as described in the governmental guidelines (NMER, 2021); however, these institutions are formally regulated only by the Internal Control Regulations, 1997. This means that the Ministry of Education and Research does not have a responsibility to follow up the private university colleges in the same way as it

[1] The indicator report 2022, published by the Norwegian Research Council. Accessed: https://www.forskningsradet.no/indikatorrapporten/indikatorrapporten-dokument/menneskelige-ressurser/utdanning/

does the public institutions, with a few exceptions. However, in Norway, public and state institutions often collaborate to find good solutions and best practices, including in issues concerning risk management practices.

Traditionally, HSE-related topics have often dominated risk assessments, e.g., related to safe working (and learning) conditions, accidents, and fire prevention. However, in recent years, there has been an increased awareness and acknowledgment that academic institutions should be more concerned with protecting their (information) values from criminal actors, resulting in a greater focus on cybersecurity, national security, and export control. For instance, according to the 2019 version of the Norwegian Security Act, public educational institutions now must establish a security organization that involves specific security roles and responsibilities, in addition to implementing a system of security management, including assessment and protection of critical values relevant to national security interests.

The Ministry of Education and Research has issued different governmental documents to explain in more detail its expectations of institutions` work with different areas of risk management, such as information security & privacy, national security & export control, and civil protection & emergency preparedness (NMER, 2020; NMER, 2021). Such governmental documents follow from the Ministry´s responsibility to clarify roles, identify risks, and implement risk-reducing measures within their sector, as well as set objectives for and coordinate how their sector works with civil protection and emergency preparedness[2]. Moreover, the Ministry has assigned safety- and security-specific tasks and responsibilities to different directorates and organizations. The goal is to improve academic institutions` risk management and to strengthen the knowledge base for the Ministry's decision-making and sector management. For instance, the Norwegian Directorate for Higher Education and Skills (DHES) is responsible for collecting and establishing an overview of the education sector's risk levels, as well as developing different guidelines[3]. As part of this responsibility, they have published annual risk-level reports on information security in higher education in the past few years, including recommendations for further work (DHES, 2023).

Another example of actors involved in safety and security work in higher education in Norway is the National Council for Civil Protection and Emergency Preparedness, appointed by the Ministry of Education and Research in 2017. The Council is voluntary and organized with sixteen representatives from the (higher) education sector at large, both public and private institutions, aiming to develop and share experiences and best practices on issues related to safety and security work (NMER, 2021). Finally, 33 universities, colleges, and research institutions in Norway have collaborated to develop "sikresiden.no" ("On the safe side"), which is a web application designed to offer user-friendly guidance and training to prepare for and handle different emergencies. The content is specifically tailored to students and staff at universities and colleges. The basic idea is to cooperate and share resources that empower institutions to carry out activities and meet regulatory requirements more collectively.

2.2 Status of the academic institutions´ risk management practices

Risk management in higher education in Norway has received greater attention for several reasons. In parallel with regulatory developments, different events have demonstrated the need to understand and prepare for the potential risks of today. For instance, handling the COVID-19 pandemic was challenging for the education sector.

According to the Ministry´s requirements, institutions must establish emergency preparedness plans that include pandemic diseases as part of the systemic risk management. A review published in early 2020 confirmed that, with a few exceptions, nearly all institutions had developed such documents (Norwegian National Audit Office, 2020). However, the repercussions of COVID-19 became far more severe than described in most plans, and institutions had to develop many new routines and practices involving teaching, exams, and the use of home offices for students and staff. All universities and university colleges had to close their campuses for longer periods, establishing infection control measures and online teaching during the pandemic (NOU, 2022). In the aftermath of COVID-19, the evaluations have concluded that the quality of online teaching and the exam results on a national level were better than could be expected. However, many students reported that they struggled during this time, both physically and mentally. The motivation to learn and study was reduced, and a large group of students were isolated from both family and friends (NOU, 2022). It was difficult for universities and university colleges to meet these challenges besides offering online teaching and supervision. The institutions have, however, reported that, as an emergency preparedness organization, they learned a lot from handling the COVID-19 situation. The question is whether they will manage to transfer the experience and knowledge from COVID-19 to other areas and emergencies. It is a common challenge to establish a mutual understanding of the

[2] Instructions for the Ministry's work with safety (2017).

[3] In 2023, the Norwegian Directorate for Higher Education and Skills (DHES), in collaboration with the Research Council of Norway, published guidelines and tools for responsible international knowledge cooperation.

risk potential in an organization during a crisis. To be able to do so, it is necessary to build an organization with personnel that have competence in risk, as well as conducting risk assessments that contribute to risk-informed decision-making.

With that in mind, the same 2020 audit review investigated how higher education institutions comply with other regulatory requirements for civil protection and emergency preparedness. An interesting finding is that only 6 out of 21 reviewed institutions met the requirements related to risk- and vulnerability assessments, including documentation of such assessments and additional action plans to reduce high and medium-high risks (Norwegian National Audit Office, 2020). Moreover, all institutions have developed emergency preparedness plans and nearly all have organized mandatory crisis management exercises. The study shows, however, that more than half of the institutions do not adequately evaluate and update the emergency preparedness plans according to the requirements.

In 2020, the Ministry published a policy for information security and privacy in higher education and research that emphasizes institutions´ responsibility to work systematically to protect information values, including developing risk management systems (NMER, 2020). According to the annual risk reports published by the DHES, public universities and colleges have improved their efforts on cybersecurity in recent years, for example, by strengthening the Information- and Communication Technology (ICT) departments and implementing stronger protection solutions, such as Two-Factor Authentication (2FA). The number of data breaches reported by educational institutions reduced by 30 percent compared to the previous year (DHES, 2023). The risk report emphasizes that risk awareness has increased in the past few years, although cyber risk is still considered to be high in the higher education sector. However, a recent review performed by the Norwegian National Audit Office (2024) concludes that, although institutions have implemented relevant information security systems and plans in the past few years, the operationalization of the plans is still lacking. Similarly, the report reveals that the Ministry´s efforts and use of policy instruments related to information security are deficient.

3. Recent challenges and developments – implications for risk management practices

This chapter addresses the changing risk landscape in higher education and research. First, we elaborate on the challenges mentioned in the introductory part, followed by a discussion on some recent developments that could contribute to improved risk understanding and risk management practices in this sector.

3.1 Emerging risks and threats in higher education and research

The ongoing digital transformation in society is arguably one of the trends with the highest impact on the education sector, as it influences how we organize, communicate, collaborate, and work (Xu et al., 2018; Díaz-García et al., 2022). However, moving to digital systems and solutions introduces new vulnerabilities and risks, such as cyberattacks, social engineering, and human errors (Ulven and Wangen, 2021). The risks related to digitalization and cybersecurity were considered the highest threats to the education sector in 2023 (PWC, 2023). In recent years, several universities have experienced internet service shutdowns due to cyberattacks (e.g., Coffey, 2023; Collier, 2022; Gatlan, 2020), including Norwegian higher education institutions.

In 2020, one of the northern universities in Norway was attacked by a well-organized hacker group. Several scientists linked to Arctic research activities received infected emails, which gave unauthorized access to some IT systems for a period. Investigations concluded that the threat actors probably operated on behalf of state intelligence services (Lie, 2022). Another example from Norway is a zero-day exploit at one of the university colleges in 2021 related to a server patch. Fortunately, this incident was quickly identified and handled by IT personnel, who were able to limit the consequences by shutting down the email services (Tønnesen, 2021). In the latter example, experts concluded that the system was not compromised. However, such attacks often create organizational uncertainties and interfere with daily tasks, e.g., temporarily blocked access to emails and calendars, in addition to potentially large economic consequences. According to a report from IBM Security (2023), the average cost of a data breach in the education sector in 2023 was 3.7 million dollars. In the Norwegian HE sector, some of the biggest vulnerabilities regarding digitalization risks and information security are: a lack of competence and organizational routines, technical vulnerabilities with security liabilities, a lack of human capacity to work with this topic, and a lack of digital safety culture (Norwegian Directorate for Higher Education and Skills, 2023). The vulnerabilities related to digitalization clearly state a need for higher competence and knowledge of the new risks and threats this sector is facing.

Another trend influencing risk management in higher education is rapid technological advancements related to, e.g., artificial intelligence, machine learning, robotics, nuclear physics, oil and gas, energy, biotechnology, cybersecurity, etc. These innovations are typically developed in an academic environment or as a collaboration between industrial actors and scientific communities. International collaboration is considered essential to solving many of the significant challenges in today´s society (Ingierd, 2022). According to Hrynkiv (2022), there is, however, a growing competition between industries and among states to gain information about technologies that could give, for instance, military advantage. This situation makes universities and research institutions more vulnerable to cyberattacks and industrial- or state-sponsored espionage (PST, 2023; NSM, 2023).

In Norway, greater attention has been given to risk management in higher education related to national security in the past few years. Both the Security Act and the Export Control Act require a risk-based approach to protect the interests and security of the nation and to reduce the possibility of illegal transfer of knowledge. The Ministry of Education and Research also focuses more on these issues in its dialogue with institutions. Universities and colleges are expected to identify and assess the critical values relevant to national security interests and sensitive technologies that can have both civilian and military applications, i.e., emerging technologies with a so-called dual-use potential (PST, 2023). The export of such knowledge to countries with which Norway does not have security cooperation is strictly regulated. Other Western countries have similar regulations and practices, intending to hinder the development of, e.g., weapons of mass destruction and other military activities. It is, however, challenging for educational institutions to find and establish proper risk management activities to comply with national security regulations and export control, while at the same time continuing to be in the lead in exploring and developing new technologies. In the changing risk landscape, institutions must gain a good understanding of the risks and establish suitable risk management practices to balance the need for openness and protection. We will further touch upon these issues in the coming chapters.

3.2 Development of a new guideline document in risk- and vulnerability assessment

For many years, risks in the HE sector have been associated with “well-known” risks, such as fire safety, lab safety, accidents, pandemics, natural hazards, and technical failure, in addition to worst-case scenarios related to crime and violence, e.g., school-shootings. The risks associated with digitalization, technological advancements, and academic espionage, however, are relatively new, generally less understood, and, at the same time, carry large uncertainties and vulnerabilities. This development challenges the approaches and methods typically used for assessing and evaluating risks in higher education, as illustrated by the Norwegian case.

All universities and colleges in Norway must perform overall risk and vulnerability assessments that include both safety and security risks. As mentioned in section 2.2., institutions struggle to comply with these requirements. In 2022, the National Council for Civil Protection and Emergency Preparedness (2022) published new guidance in risk- and vulnerability assessment, aiming to support the higher education institutions in assessing and handling risks. The guideline document was developed in close cooperation with risk researchers at the University of Stavanger and builds on principles and concepts recently discussed in the risk science literature. The risk assessment method described is tailored to the higher education sector and aligns with the typical steps in the ISO 31000 standard in risk management (ISO, 2018), i.e., 1) scope, context, criteria, 2) risk assessment, and 3) risk treatment. However, compared to the ISO standard, the guideline introduces some new ideas that involve the method for assessing and characterizing risk, in particular. We will now briefly explain some of the methodological pillars as described in the guidance document.

Firstly, the suggested risk assessment method builds on the uncertainty-based risk perspective, where risk can be understood as consequences, C, and associated uncertainty, U, for short denoted (C,U). This risk understanding aligns with recommendations by the Society for Risk Analysis (SRA, 2015; 2017) and related research (see e.g., Aven and Renn, 2009; Flage et al., 2014; Aven and Thekdi, 2022). The most common way to express uncertainty is to use probability. However, as described in the guideline document, many find it difficult to evaluate probability when performing risk- and vulnerability assessments in higher education, especially for low-probability and high-consequence events. The guideline document therefore recommends using pre-defined probability intervals to express uncertainties. As an example, an analysis group is asked to assess the probability that event A will happen over one year. The analysis group states that the probability is 10%-50%, which expresses the group´s degree of belief that the event will occur. The interpretation is that the probability is the same as randomly drawing a red ball from an urn of 100 balls of which 10, 11, ... or 50 are red (Aven and Thekdi, 2022).

However, in line with the risk science literature, the guideline also emphasizes the importance of looking beyond probability when assessing and describing risk, by making additional evaluations of the knowledge supporting the probability judgments. The guideline document makes concrete suggestions on performing and documenting strength-of-knowledge (SoK) considerations as part of the risk assessment, building on the work of Aven and Flage (2018), as referred to in Aven and Thekdi (2022). It is recommended that the following five criteria (National Council for Civil Protection and Emergency Preparedness, 2022) be evaluated:

- the assumptions that the probability is based on are considered to be highly reasonable and credible;
- there is good access to reliable and relevant data/information;

- there is agreement in the analysis group (among the experts);
- there is a good understanding of how the event can occur and develop, inter alia, through the modeling of phenomena and processes;
- the information (knowledge) that the probability is based on is thoroughly reviewed, particularly in terms of potential surprises ("black swans" / "unknown known").

An overall evaluation of all the criteria may result in either:

- strong knowledge – if all the relevant criteria are met; or
- moderate strong knowledge – if most of the relevant criteria are met; or
- moderate weak knowledge – if most of the relevant criteria are not met; or
- weak knowledge – if none of the relevant criteria are met.

According to the risk- and vulnerability guideline, the evaluation of SoK should be conducted and documented for all the assessed events and communicated as an integrated part of the risk assessment.

A second point worth mentioning is that the guideline developed by the Norwegian National Council for Civil Protection and Emergency Preparedness in Higher Education (2022) also emphasizes the importance of addressing potential surprises when identifying hazards and threats. This means exploring in detail various issues that could provide insights about:

- events that are unknown by the risk analysts but known to others ("unknown known");
- events that are known but not believed to occur (low probability); or
- deviations in assumptions, i.e., an event can occur as the assumptions supporting the assessment turn out to be wrong.

It should be noted that it is relevant to consider both typical "security-risks" and "safety-risks" in the process of identifying events that are worthy of further assessment. A similar focus on potential surprises is seldom found in other, comparable standards and guidelines on risk assessment, although it is thoroughly described in current risk science literature; see, e.g., Aven and Thekdi (2022). Finally, the guideline document challenges the use of risk matrices showing only consequence and probability, by suggesting various alternatives to visualizing and communicating the risk assessment results. For instance, in line with the risk science literature, it presents a risk matrix that illustrates consequence, probability, and the strength-of-knowledge (SoK) supporting the assessments for each consequence category. The SoK evaluations are illustrated by different bubble sizes, similar to those suggested in Amundrud and Aven (2012). The smaller the bubble, the weaker the knowledge supporting the assessments and vice versa. However, a limitation of such risk matrices is the lack of demonstration of the possible outcomes of an event. For instance, event A could potentially lead to more severe consequences that are not shown in the matrix. A third option is therefore suggested in the guideline document: using a matrix that shows only a fixed consequence category, for instance, severe outcome (e.g., one or more fatalities). The strength-of-knowledge evaluations (X-axis) associated with the probability assignment (Y-axis) are mapped for each of the assessed events. The main idea is to give the decision-maker an improved risk understanding by emphasizing the importance of considering the knowledge supporting the probability assessment when describing risk.

3.3 Some reflections on risk management implications

A changing risk landscape in higher education and research raises some interesting issues. From a governmental perspective, it challenges the established risk regulation regime and regulatory practices. As illustrated by the Norwegian case, the increased focus on information security, national security, and the prevention of illegal transfer of knowledge, in academic milieus traditionally characterized by international cooperation and transparency, creates new dilemmas. How should universities and colleges balance protection and knowledge-sharing, and what is considered the right security level? The regulations currently place the responsibility for handling these questions on individual educational institutions, as they apparently can best identify and assess the (information) values and vulnerabilities they possess. However, these institutions do not have deep insights into ongoing threats and the potential threat actors, which makes it difficult to describe and understand the risks properly. Strengthening the knowledge foundation that decisions are built on requires clear guidance from the security authorities beyond the Annual Threat Assessments that are made publicly available.

In the past few years, there has been a growing interaction and dialogue between the Norwegian Police Security Service (PST) and educational institutions, which benefits both parties. Universities and colleges become more aware of the risks associated with, e.g., research and technology developments, and thus can better protect their values. Similarly, the authorities learn about the uniqueness of academia, e.g., their role in building democratic competence among students and the importance of developing new knowledge, including international collaborations. Too much securitization in higher education could potentially conflict with these core values, such as freedom of expression and equality, as well as hampering academic freedom. Circling back to the questions about balance and security levels, we argue that the authorities should take on a more proactive and leading role on behalf of all institutions in expressing their expectations concerning national security and not leave it to the individual university or college to find the proper security level. The educational institutions should instead focus on developing risk management systems and practices, including performing quality risk assessments to support communication and decision-making. Moreover, mastering risk management requires trained risk personnel and, in general, a clear understanding of fundamental risk concepts and principles at all organizational levels.

As described in Section 2.3., attempts are made to establish a common approach to risk assessment and management in Norwegian higher education, building on contemporary risk science knowledge. The method suggested covers both safety and security risks. In preparing this paper, however, it became clear that there appears to be some confusion among the institutions regarding how to include security problems in existing risk management systems and processes. The tendency is for security management to become a separate activity, which is unfortunate. One explanation is that many practitioners are used to assessing security risks through the triplet, values, threats, and vulnerability (Amundrud et al., 2017; PST, 2023) and thus find it problematic to use probabilities due to a lack of solid information and knowledge supporting the estimates (Heyerdahl, 2022). However, as argued by Aven (2023), ignoring the uncertainty (usually expressed by probability) and knowledge aspect of risk could lead to serious mischaracterization of risk and, ultimately, wrong decisions and incorrect use of resources.

4. Concluding remarks

This paper has addressed some recent trends, challenges, and developments that may influence risk management in higher education and research. It has been a goal to bring risk science knowledge into the discussion and contribute new insights to improve risk management practices. The Norwegian higher education sector is used for illustration purposes.

We have identified and discussed two trends: the digital transformation of academic institutions and rapid technological advancement, which both increase the risks of cyberattacks and espionage. Information security, national security, and prevention of the illegal transfer of knowledge have consequently become more relevant to universities and colleges. This situation introduces new challenges related to risk characterizations and risk acceptance. The latter also involves the dilemma of balancing protection and other values typically associated with the academic context. In the paper, we conclude that the government should be clearer on its expectations of institutions when it comes to finding the proper security level. Concerning risk assessments, different methods are frequently used to assess security and safety risks. However, as shown in the paper, it is possible and recommended to apply frameworks that cover all types of risk. One example of such a framework is the Norwegian guidance on risk and vulnerability assessment, developed for universities and colleges. The same guideline document introduces a new and alternative risk matrix that illustrates a fixed consequence category together with probability and strength of knowledge. The Norwegian Ministry of Education and Research refers to this guidance in its policy document on risk management. However, the extent to which it has impacted the educational institutions` risk assessment and management practices at this point is not clear.

Finally, working on this paper has demonstrated the relevance of higher education and research as an application area within risk science. Only a few studies on risk management in higher education are referred to in the literature, covering topics such as information security and enterprise risk management. Hence, there is a potential for exploring and generating new knowledge through both empirical and conceptual work, using higher education as a case.

References

Amundrud, Ø., Aven, T. 2012. A practical guide on how to present and visualize the result of risk and vulnerability analyses in a societal safety and security context. European Safety and Reliability Conference 2012.Curran.

Amundrud, Ø., Aven, T., Flage, R. 2017. How the definition of security risk can be made compatible with safety definitions. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 231(3), 286–294. https://doi.org/10.1177/1748006X17699145

Asheim, H. 2023. Strategy for digital transformation in the higher education sector. Available at: https://www.regjeringen.no/en/dokumenter/strategy-for-digital-transformation-in-the-higher-education-sector/id2870981/ Accessed: December 2023

Aven, T. 2023. On the gap between theory and practice in defining and understanding risk. Safety Science, 168, 106325. https://doi.org/10.1016/j.ssci.2023.106325

Aven, T., Flage, R. 2018. Risk assessment with broad uncertainty and knowledge charactericatons: An illustrating case study. In. T. Aven and E. Zio (eds.), Knowledge in Risk Assessments. New York: Wiley, 3-26.

Aven, T., Renn, O. 2009. On risk defined as an event where the outcome is uncertain. Journal of Risk Research 12, 1-11.

Aven, T., Thekdi, S. 2022. Risk Science: An introduction. Routledge, Taylor & Francis Group.

Aven, T., Zio, E. 2021. Globalization and global risk: How risk analysis needs to be enhanced to be effective in confronting current threats. Reliability Engineering & System Safety, 205, 107270. https://doi.org/10.1016/j.ress.2020.107270

Bongiovanni, I. 2019. The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Chin, K. 2023. Why is the education sector a target for cyber attacks? Available at: https://www.upguard.com/blog/education-sector-cyber-attacks Accessed: November 2023

Coffey, L. 2023, September 25. Hackers Accessed Data of Up to 230,000 at University of Michigan. Available at: https://www.insidehighered.com/news/quick-takes/2023/10/25/hackers-access-data-230k-university-michigan Accessed: November 2023

Collier, K. 2022, September 5. Illinois college, hit by ransomware attack, to shut down. Available at: https://www.nbcnews.com/tech/security/ransomware-attack-covid-combine-shutter-illinois-college-rcna24905 Accessed: November 2023

Department for Digital, Culture, Media & Sport. 2022. Official Statistics. Educational institutions findings annex—Cyber Security Breaches Survey 2022. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022 Accessed: November 2023

DHES (The Norwegian Directorate for Higher Education and Skills.) 2023. Informasjonssikkerhet og personvern i høyere utdanning og forskning. Available at: https://hkdir.no/rapporter-undersokelser-og-statistikk/informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning Accessed: November 2023

Díaz-García, V., Montero-Navarro, A., Rodríguez-Sánchez, J.-L., Gallego-Losada, R. 2022. Digitalization and digital transformation in higher education: A bibliometric analysis. Frontiers in Psychology, 13, 1081595. https://doi.org/10.3389/fpsyg.2022.1081595

Flage, R., Aven, T., Zio, E., Baraldi, P. 2014. Concerns, challenges, and directions of development for the issue of representing uncertainty in risk assessment. Risk Analysis, 34(7), 1196–1207. https://doi.org/10.1111/risa.12247

Gatlan, S. 2020, May 7. Ruhr University Bochum Shuts down servers after ransomware attack. Available at: https://www.bleepingcomputer.com/news/security/ruhr-university-bochum-shuts-down-servers-after-ransomware-attack/ Accessed: November 2023

Heyerdahl, A. 2022. Risk assessment without the risk? A controversy about security and risk in Norway. Journal of Risk Research, 25 (2), 252–267.

Hrynkiv, O. 2022. Export controls and securitization of economic policy: Comparative analysis of the practice of the United States, the European Union, China, and Russia. Journal of World Trade, 56(Issue 4), 633–656. https://doi.org/10.54648/TRAD2022026

IBM Security. 2023. Cost of a data breach report 2023. Available at: https://www.ibm.com/downloads/cas/E3G5JMBP Accessed: November 2023

Ingierd, H. 2022, July 20. Mellom sikkerhet og akademisk frihet [Between security and academic freedom. (In Norwegian only)]. Available at: https://khrono.no/mellom-sikkerhet-og-akademisk-frihet/703867 Accessed: December 2023

Internal Control Regulations 1997. Available at: https://lovdata.no/dokument/SFE/forskrift/1996-12-06-1127 Accessed: November 2023

ISO 2018. ISO 31000 Risk Management. www.iso.org/iso-31000-risk-management.html

Khaw, T. Y., Teoh, A. P. 2023. Risk management in higher education research: A systematic literature review. Quality Assurance in Education, 31(2), 296–312. https://doi.org/10.1108/QAE-04-2022-0097

Lie, T. 2022, February 28. NRK: Russland sto bak hackerangrep mot UiT. [NRK: Russia was behind the hacker attack against UiT. (In Norwegian only)] Available at: https://www.khrono.no/nrk-russland-sto-bak-hackerangrep-mot-uit/665879 Accessed: November 2023

National Council for Civil Protection and Emergency Preparedness. 2022. Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren. [Guide to risk and vulnerability assessment for the higher education sector (In Norwegian only)] Available at: https://www.uis.no/nb/det-teknisk-naturvitenskapelige-fakultet/veileder-i-risiko-og-sarbarhetsanalyser-for Accessed: November 2023

NMER (Norwegian Ministry of Education and Research). 2020. Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. [Policy for information security and privacy in higher education and research (In Norwegian only)] Available at: https://www.regjeringen.no/contentassets/cfb4f2cc8f744cb2acf6d0df4027df7d/rundskriv-f-04-20.pdf Accessed: November 13, 2023

NMER (Norwegian Ministry of Education and Research). 2020. Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. [Policy for information security and privacy in higher education and research (In Norwegian only)] Available at: https://www.regjeringen.no/contentassets/cfb4f2cc8f744cb2acf6d0df4027df7d/rundskriv-f-04-20.pdf Accessed: November 13, 2023

Norwegian National Audit Office. 2020. Underskelse av samfunnssikkerhet og beredskap ved statlige universiteter og høyskoler. [Review of societal safety and emergency preparedness at state universities and colleges. (In Norwegian only)] Available at: https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-samfunnssikkerhet-og-beredskap-ved-statlige-universiteter-og-hoyskoler/ Accessed: November 13, 2023

Norwegian National Audit Office. 2024. Informasjonssikkerhet i forskning innenfor kunnskapssektoren [Information security in research within the higher education sector (In Norwegian only)] Available at: https://www.riksrevisjonen.no/globalassets/rapporter/no-2023-2024/informasjonssikkerhet-i-forskning-innenfor-kunnskapssektoren.pdf. Accessed: January 18, 2024.

Norwegian National Council for Civil Protection and Emergency Preparedness in Higher Education 2022. Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren. [Guide to risk and vulnerability analyses for the knowledge sector (In Norwegian only)] Available at: https://www.uis.no/nb/det-teknisk-naturvitenskapelige-fakultet/veileder-i-risiko-og-sarbarhetsanalyser-for Accessed: November 2023

NOU. 2022:5. Myndighetenes håndtering av koronapandemien – del 2 (In Norwegian only). Available at: https://www.regjeringen.no/contentassets/d0b61f6e1d1b40d1bb92ff9d9b60793d/no/pdfs/nou202220220005000dddpdfs.pdf Accessed: April 2024

NSM. 2023. Risiko 2023. The Norwegian National Security Authority. https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf Accessed: November 2023

PST. 2023. National threat assessment 2023. Norwegian Police Security Service. Available at: https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/ Accessed: November 2023

PST. 2024. Nasjonal trusselvurdering (In Norwegian only). Available at https://pst.no/globalassets/2024/ntv2024/nasjonal-trusselvurdering-2024_uuweb.pdf Accessed: April 2024

PWC. 2023. Managing risk in higher education. Higher education sector risk profile 2023. Available at: https://www.pwc.co.uk/government-public-sector/education/documents/higher-education-sector-risk-profile-2023.pdf Accessed: December 2023

Sophos. 2022. The state of ransomware in education 2022. Available at: https://assets.sophos.com/X24WTUEQ/at/pgvqxjrfq4kf7njrncc7b9jp/sophos-state-of-ransomware-education-2022-wp.pdf Accessed: November 2023

SRA. 2015. Glossary Society for Risk Analysis. Available at: www.sra.org/resources. Accessed: April 2024

SRA. 2017. Core Subjects of Risk Analysis. Available at: www.sra.org\/resources. Accessed: April 2024

Tønnesen, E. 2021, March 10. Oppdaget uregelmessigheter. E-post ute av spill i to dager. [NRK: Email out of action for two days. (In Norwegian only)] Available at: 2023https://www.khrono.no/oppdaget-uregelmessigheter-e-post-ute-av-spill-i-to-dager/561841 Accessed: November 2023

Ulven, J. B., Wangen, G. 2021. A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), Artikkel 2. https://doi.org/10.3390/fi13020039

Wang, K., Li, B., Tian, T., Zakuan, N., Rani, P. 2023. Evaluate the drivers for digital transformation in higher education institutions in the era of industry 4.0 based on decision-making method. Journal of Innovation & Knowledge 8(3), 100364. https://doi.org/10.1016/j.jik.2023.100364

Xu, L. D., Xu, E. L., Li, L. 2018. Industry 4.0: State of the art and future trends. International Journal of Production Research 56(8), 2941–2962. https://doi.org/10.1080/00207543.2018.1444806