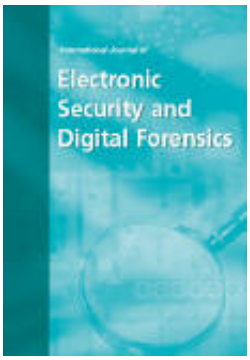


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

Rule of law education for cybersecurity governance in higher education institutions: a framework for policy and practice

Jinyan Xue

DOI: 10.1504/IJESDF.2026.10078386

Article History:

Received:	04 September 2025
Last revised:	23 December 2025
Accepted:	14 February 2026
Published online:	21 May 2026

Rule of law education for cybersecurity governance in higher education institutions: a framework for policy and practice

Jinyan Xue

Shandong Huayu University of Technology,
Marxist Academy,
DeZhou, Shandong 253034, China
Email: jinyanxue3107@outlook.com

Abstract: This study proposes a governance framework that integrates rule of law education into cybersecurity management within higher education institutions (HEIs). By emphasising legal compliance, risk management, and awareness, the framework addresses human and organisational vulnerabilities, thereby enhancing institutional resilience against evolving cyber threats. The growing prevalence of data breaches, ransomware, and human-related risks underscores the critical importance of cybersecurity in HEIs. While prior research has largely concentrated on technical safeguards, limited attention has been given to integrating legal, organisational, and governance dimensions. Adopting a qualitative design, this study employed semi-structured interviews with IT managers, security officers, and policymakers across multiple institutions. Data triangulation and iterative validation informed the framework's development. Findings showed high adoption in quality standards (85%), data privacy (80%), and reporting (75%), with lower levels in risk management (60%) and compliance monitoring (65%). Expert consensus, confirmed through Delphi sessions, yielded Kendall's W scores above 0.78.

Keywords: cybersecurity governance; rule of law education; higher education institutions; HEIs; risk management; compliance; data privacy; quality assurance; QA; institutional strategies; cybersecurity awareness; policy framework.

Reference to this paper should be made as follows: Xue, J. (2026) 'Rule of law education for cybersecurity governance in higher education institutions: a framework for policy and practice', *Int. J. Electronic Security and Digital Forensics*, Vol. 18, No. 9, pp.1–22.

Biographical notes: Jinyan Xue is affiliated with the Shandong Huayu University of Technology, serving in the Marxist Academy, Dezhou, Shandong, China. As a dedicated academic and researcher, her work focuses on interdisciplinary studies integrating social sciences, governance, and contemporary development issues. With a strong commitment to academic excellence, she has contributed to research in areas such as policy analysis, sustainable development, and technology-driven societal transformation. As a corresponding author, she actively engages in scholarly collaborations and international publications, promoting innovative research perspectives. She is committed to fostering critical thinking and advancing research that bridges theory and practical application in higher education.

1 Introduction

Due to the advancement, growth, and accessibility of internet, mobile, and communication technologies, online transactions have grown more widespread. As a result, an increasing amount of digital data is produced and usually kept on servers spread over the globe, a phenomenon known as the cloud. In an attempt to keep this data safe and reduce the possibility of cybercrimes resulting from illicit online activities, those in charge of safeguarding sensitive information, such as bank records, have made large investments in cybersecurity measures. These measures include hiring security experts, developing thorough security policies, implementing cutting-edge security technologies, and continuing education and training of security personnel (Alharbi, 2025). Clients and users remain the weakest link, even if expenditures in security education have produced more secure networks, operating systems, and apps. Because of this, organised cybercriminals are focusing on human factors and investing a lot of money in creating ingenious hacking methods that take advantage of customers' confidence and eagerness to assist in order to acquire their data (Garba and Sirat, 2020). To target gullible people, cybercriminals commonly use strategies including social engineering, online chat rooms, phishing, fraud, cyberbullying, ransomware, and identity theft.

Cyber threats that take advantage of people's mistakes are always changing. This is why people should be the main focus of cybersecurity training and when dealing with cybersecurity issues. More and more, cyberattacks are happening that depend on people making mistakes to get at data. Because of this, users need to be taught what to do in cybersecurity training classes. According to a study (Khader et al., 2021), one reason why more and more people are getting hurt online is that they do not know how it can affect them. Many of the people in schools do not know much about cybersecurity or cybercrime, so it's very important for schools to teach it. This way, they are not easy targets for data breaches and other digital crimes. Students are often cyberattacked because they use many different apps and social media sites every day. Most students do not know much about cybersecurity or how to protect their devices from online threats like scams and bugs. People in Silicon Valley, which is in the US, are known for being very interested in and skilled about technology. Kids who go to school there said that pretty low numbers of people used two-factor authentication and hard passwords (Murphey, 2022).

Even though they knew it wasn't safe, they told everyone at the university sensitive things about themselves. The lack of safety at schools and universities is due to a number of different reasons. It's important to keep in mind that hacks can hurt higher education in more ways than just taking or breaking things. Yes, higher education institutions do store a lot of private data, like records for current and former students, IP connected to research or studies that are not shared with anyone else, and really valuable inventions or ideas. If data is lost or hacked, the agency's reputation may take a big hit, which could put people involved at risk. Second, any cybersecurity event could be very bad because colleges and universities often have systems that many people use and important infrastructure that a city or country counts on (like the core network's internet link hub). Third, the IT systems at many colleges and universities are not as well-organised as those at big companies. This is because each school and department has different tech needs, so it makes sense for them to have separate IT systems. This setup is problematic because it is easy for attackers to get in through its security holes.

Fourth, the different kinds of academic schools have safety problems. More than most businesses, these societies value being open and clear. At first, schools and universities wanted to make their websites and networks available to everyone (Lee, 2021). Finally, the COVID-19 outbreak in 2020 caused a lot of people to start learning and working from home. Since then, more personal devices that colleges do not provide have been able to join to the networks and IT systems of higher education schools. This makes it a lot more important to have good protection. These issues have raised the importance of safety in higher education. The horizon report will publish a new issue about computer security in 2021 as an example of this increased attention. Colleges and universities continue to spend money on people and equipment for cybersecurity. Policymakers and leaders are asking for help from institutional frameworks to focus their resources and fix the problem. At this moment, technology is the main target of cybersecurity research. This means that it is not as helpful for institutional leaders and officials who want to get a better sense of the field as a whole (Cheng, 2022). There are not many general views on safety in higher education schools in magazines that focus on fun activities. Because there is not a lot of research on this subject, this study tries to contribute more knowledge by exploring how colleges and universities manage cybersecurity from a systemic point of view and offering useful information that politicians and leaders of higher education institutions can use to put these strategies into action.

Cybersecurity in OHE is very important because more and more people are using digital tools for teaching, testing, and management. The OHE business has poor cybersecurity, which has led to big outages and data breaches. For example, in 2019 hackers asked for $2 million in Bitcoin as a payment after shutting down Monroe College's tech infrastructure (Ahmed et al., 2021). That year, Hamilton College, Oberlin College, Grinnell College, and the Stevens Institute of Technology were all hit by ransomware, too. Ransomware attacked the University of Utah's College of Social and Behavioural Science in 2020; it wanted $457,000 to unlock the data (Akacha and Awad, 2023). Also, in 2019, hackers got into 27 places in the US, Canada, and Southeast Asia that were working on underwater technology. Some of these schools were Duke, MIT, Penn State, and Washington University, which are all well-respected (Mubin et al., 2024). Ransomware is going after more and more schools. In 2020, UC San Francisco was hit, Howard University was hit in 2021, Lincoln College had to close because of a ransomware attack in 2022, and the University of Manchester had a data breach in 2023. These cases show that schools need strong cybersecurity to protect them from online threats that are always changing.

Here is how this article is structured: Second, we take a look at the relevant literature on rule of law instruction for university cybersecurity administration. 'A framework for policy and practice' describes the suggested technique in Section 3. Section 5 offers the study's final remarks, while Section 4 explains the results and their implications.

1.1 Contribution of the study

By presenting a new paradigm that incorporates rule of law education into institutional cybersecurity practices, this study adds to the literature on cybersecurity governance in higher education. The human and organisational aspects of cybersecurity, including awareness, compliance, and governance structures, are highlighted in this study, in contrast to previous research that has concentrated chiefly on technical measures. The research seeks to address systemic vulnerabilities in HEIs by analysing qualitative data

from cybersecurity experts, IT managers, and higher education leaders in various contexts. The findings are then translated into practical strategies for risk management, compliance monitoring, data privacy, and quality assurance (QA). An additional theoretical and practical contribution of the study is the way it brings together cybersecurity governance with principles of law, organisational learning, and international best practices. The framework promotes a culture of responsibility, openness, and accountability in the digital realm while simultaneously giving higher education administrators and policymakers a practical instrument to make their institutions more resilient to cyber threats. This research fills a significant need in the field by providing a model that can be adjusted to fit different institutional settings, thus bridging the gap between cybersecurity governance and legal education.

2 Literature review analysis

The writing on drone use shows a range of opinions. This study report and the related questionnaire show all three of these points of view: legal, cybersecurity, and economic. The things we studied and the poll results both show many helpful uses for drones.

2.1 Background

Now that computers are not just used in big labs, security has become a big issue. As local and global networks get bigger, so does understanding of connected issues, problems, responsibilities, trends, and cybersecurity. Strang and Vajjhala (2024) suggested a plan to protect all colleges and universities cyber-wise that did not look at how those schools are different or how they work. The plan made sure that the right facts and steps were taken to protect the cybersecurity of HEIs. The method used functional modelling and graphical display of IDEF0 processes to make a high-level context map that would help reach the planned goal. But the study's feature selection process did not improve over time, which is important to look for signs of hacking risk. Using unsupervised machine learning (ML) to look at the chance of hacking breaches in HEIs is one way to find risk signs (Salem et al., 2024). The study is mainly about the ML method and its advantages and disadvantages. It also uses real-world data to compare HEIs. The sample selection process uses a set of 848 records from educational websites that was created by looking at data from US colleges and universities that are open to the public. It was mostly because each college site had its own set of facts that bigger groups made a lot of entries for the study of some college places. There were almost 4,000 things in the collection that were thought to be useful for finding hacking problems. These items included XML embedding's, URLs, and other HTTP scripts. First, purposeful sampling was used to make sure that the average-sized public and private groups from different states were represented properly.

After that, random sampling was used. The levels of protection at the schools in the sample were not very similar. The 'control' function, which showed how risk factors were combined, made it possible to improve cybersecurity in a more focused way. A lot of people still hack when they take classes online, which causes problems with technology and contact between students and teachers. Page et al. (2021) looked into these issues by using a mixed-methods qualitative technique on data collected in two stages from postgraduate students who are full-time online cybersecurity school students.

A class was held to collect qualitative data from a group of postgraduate cybersecurity students. The goal was to find out how much they had learned and how they felt about learning online. Cybersecurity issues are becoming a bigger problem for local governments (Hossain et al., 2024a), but there is not a lot of information about the types of attacks and methods used, the technologies and frameworks that are available, and the specific problems and solutions. The papers that were looked at for this study also showed a lack of academic research, say that only three papers from 2000 to mid- 2021 talked about hacking that happened to local governments. It is clear that rules and strategies for cybersecurity need to be put in place, but according to Chodakowska et al. (2022, p.163), "there has been little research verifying the adopted solutions in practice or analysing actual examples of cybercrime in public entities, especially at the local government level." These days, most studies use a detailed method that focuses on the importance of and variety of cyber threats. These studies do not, however, include theories or evidence-based methods that help people understand cybersecurity problems.

2.2 Selection of nations

The countries chosen for this study have enough cybersecurity rules. There is also enough data for hacking rules and worries in these countries. So, their rules can be used as a guide for making a big plan. These things affected how the selecting process worked. Many people in the US use the internet (AlAhmad et al., 2021). More than 300 million people are already online, and that number is growing every day. Because of this, access to the internet is a basic human right. Because its online business is worth a trillion dollars, this country has strong cybersecurity policies in place. Some of the world's richest and most industrialised nations are in the European Union (EU), and many people in those countries can easily reach the internet. The internet has a lot of different security problems because it is used for so many things. So, the hacking policy is just as broad.

- Over 20 million people use the internet in Australia, and the country hosts a large number of students and tourists every year. Evidently, many people are affected by Australia's cybersecurity legislation, and the nation is striving to create a perfect plan for all kinds of internet users.
- Canada is one of the most cybersecurity-conscious countries due to its 30 million internet users, or 88% of the population. Like many other wealthy nations, it has been the target of major cyberattacks.
- Of all the countries in the world, China has more than a billion people using the internet. Many people will be unable to use many internet services if the biggest e-commerce company in the world does not implement a suitable policy.
- India has more than 600 million internet users, making it the second-largest nation in the world. Despite a relatively low internet penetration rate compared to other countries, the country's IT industry is one of the world's most dynamic. Due to its abundance of legislation covering a wide range of cybersecurity issues, it was also selected.
- One of the fastest-growing economies in Asia is Malaysia's [17]. More people are using the internet there than in most other Asian nations. Over 30 million people in Malaysia have access to the web. Due to the extensive involvement of specialists in

the development of Malaysia's cybersecurity rules, the country has been selected for scrutiny.

For various reasons, we did not include a couple more countries that have sizable populations online and advanced infrastructure (AlAhmad et al., 2021). Countries like South Korea and Japan have a lot of people using the internet, but all the cybersecurity resources there are in Korean or Japanese, so we did not include them in our research.

The internet of things (IoT) and the linking of many gadgets are quickly becoming a reality. Now that device-to-device (D2D) contact has been created, IoT devices, especially edge devices, are more likely to be hacked. To look at traffic as it happens and keep bad traffic from getting through, you need advanced network security. These tools also need to be able to find texts that are bad. We have found a great new way to quickly get new malware and sort it out. This is how we will deal with zero-day viruses. The piece (Lija et al., 2025) discusses the idea of a mixed deep learning (DL) model for finding hacks. The suggestion was based on models using gated recurrent units (GRUs) and long short-term memory (LSTMs). The main goal of the project is to protect data. To keep the information safe, we recommend using hybrid encryption. If someone tries to send illegal material to someone else by email, it will be protected with symmetric encryption and a symmetric key. A secure key that gives the person who gets the message access to the information is usually given to them. Using mixed cryptography (Modi et al., 2025) makes security even better. In this method, the symmetric key is encrypted with asymmetric encryption and sent to the recipient. This way, both the key and the receiver are safe. The encrypted symmetric key is decoded by the person receiving the message, who uses their own private key to do so. The symmetric key is decrypted and then used to safely send the encrypted data about criminals to its target.

In the IoT era, it is important to keep things safe so that all of the systems and gadgets that are linked to each other stay safe. Many experts have worked on making strong classification models that can spot hacks and protect the IoT infrastructure because being able to see these attacks is very important for IoT security. Feature selection is an important part of making good classification models for IoT security. In 2025, Li et al. published a study that looks at all the previous research on feature selection methods for ML-based attack classification models in IoT security that use IoT datasets. The point is to help researchers and practitioners choose the best ways to select features. This study finds 63 primary studies that meet the standards for inclusion after using the PRISMA guidelines to look at data from 1,272 articles published between January 2018 and December 2022.

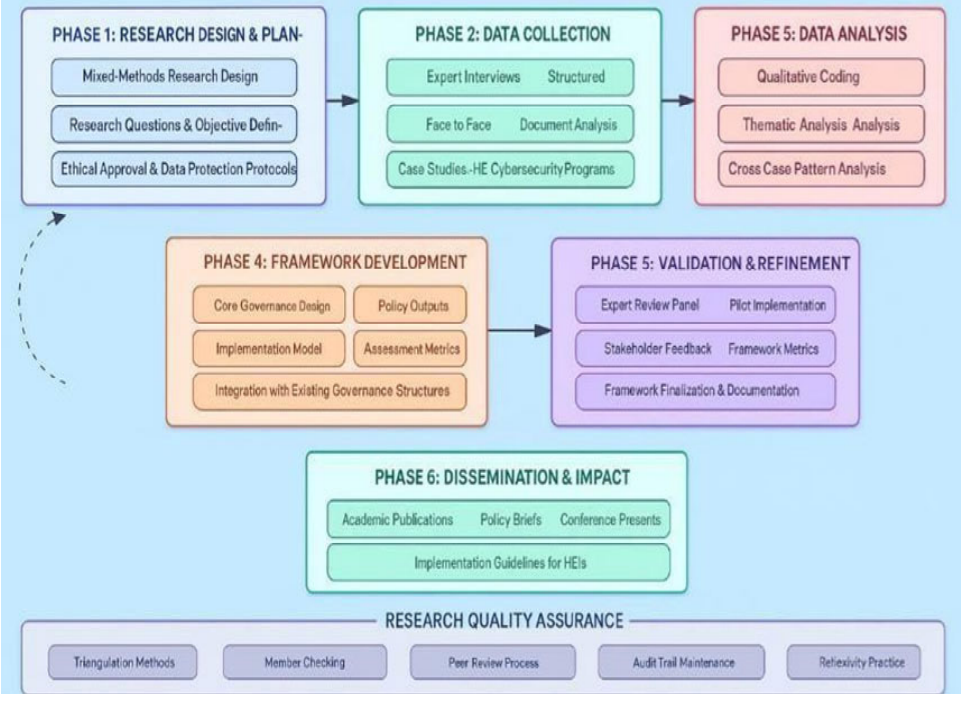
3 Methodology

This study forms and verifies the cybersecurity control structure using three datasets that work with each other. To begin, IT managers and security officers from colleges and universities in Australia and Europe were interviewed in a semi-structured way (N = 23). These talks showed new policy ideas, governance problems, and basic framework rules that are only seen in higher education. Second, a Delphi study with cybersecurity experts from Bahrain's banking sector (N = 25) confirmed the framework's ideas and ranked them. It was decided to go with the banking sector because it has the same needs for managing risk, following rules, and protecting data as colleges and universities. This set

the validation process up with good starting points. Third, baseline evaluations with IT leaders from colleges and universities in Portugal, Germany, Brazil, and Spain (N = 5) (N = 5) studied how useful, practical, and complete the framework was in different types of institutions. This framework is based on the unique realities of higher education schools and uses a triangulated method. It is also checked against well- known rules for cybersecurity control. This makes the structure stricter and more applicable to real-life scenarios.

Research design, data collection, analysis, framework building, validation, and dissemination are the six stages of the research technique shown in Figure 1. Emphasising triangulation, peer review, audit trail maintenance, reflexivity practices, and interaction with governance structures, iterative feedback loops are highlighted. Research QA is also emphasised.

Figure 1 Research methodology framework for rule of law education in cybersecurity governance (see online version for colours)

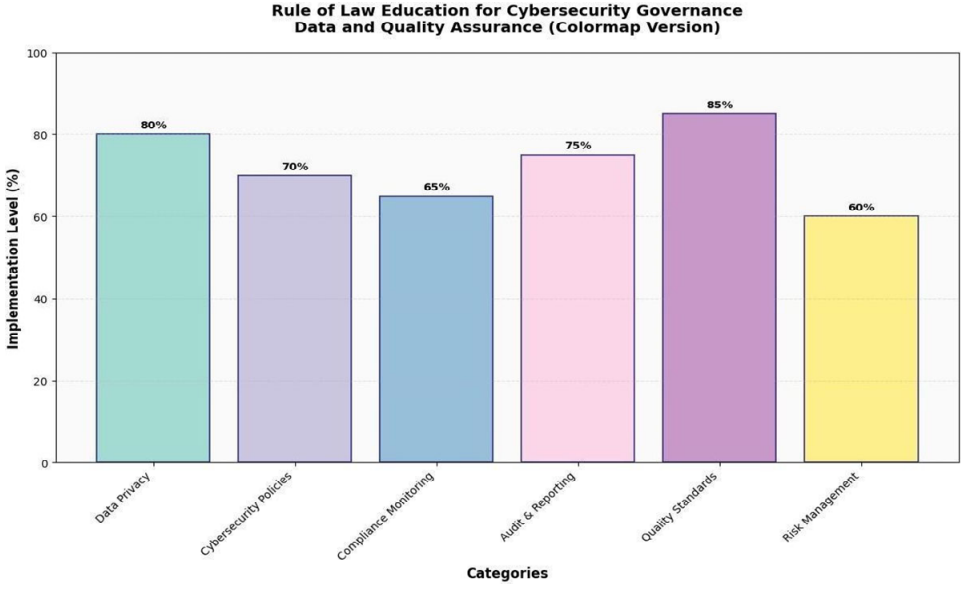


3.1 Data collection

Levels of rule of law education implementation for data and QA cybersecurity governance are shown in the figure. In six critical areas, it shows different levels of adoption. Of the three areas evaluated, 85% have been implemented in quality standards, 80% in data privacy, and 75% in audit & reporting. The following areas have the lowest implementation rates: cybersecurity policies at 70%, compliance monitoring at 65%, and risk management at 60%. As a whole, the graphic shows that standards, privacy, and reporting are essential in cybersecurity governance, but that risk management and

compliance monitoring might use some work to be more balanced and complete. Table 9 shows these implementation metrics in summary form, with priority types based on how often they are used and comments from institutions.

Figure 2 Implementation levels of rule of law education for cybersecurity governance in data and quality assurance (see online version for colours)



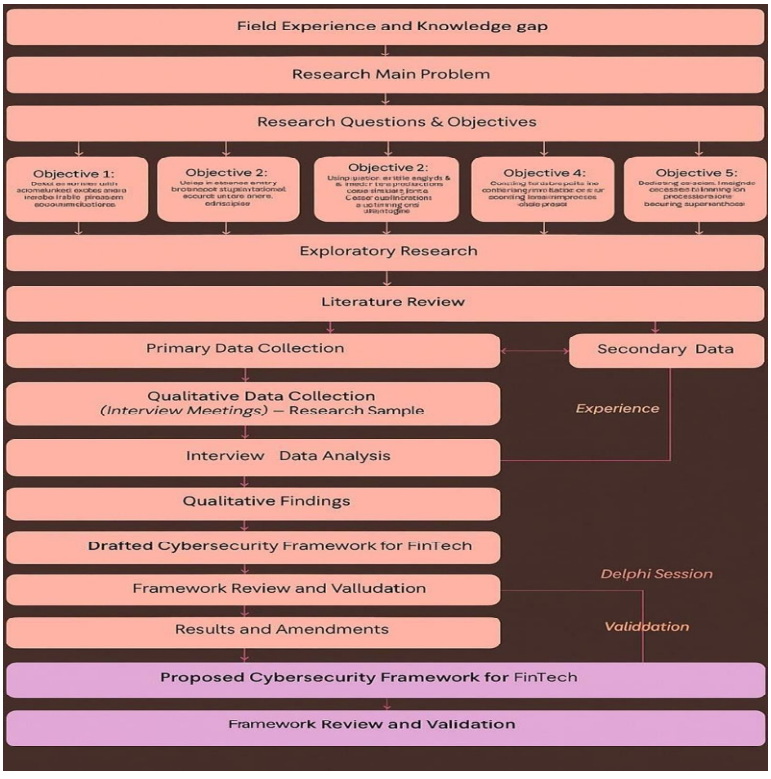
The interviews included all three of the researchers. Researchers chose cybersecurity professionals and senior managers who are actively participating in their organisations' strategic learning efforts to address cybersecurity threats. We utilised a snowball sampling strategy since previous research has shown that personal interactions are a good way to choose the right cases. Informants are contacted through the contact information given by other informants, typically through personal connections and social networks. This process is called the snowball sampling approach. We reached out to different HR and top management individuals in HERS via email and social media. In the email, we explained the research study, why their participation would be valuable, and what they could expect from us if they decided to take part. The case organisation's involvement, however, was entirely optional (Mishra et al., 2022). You may find more details about the people who were interviewed in Table 1. From September 2022 to May 2023, a total of 23 interviews were carried out. Following each interview, the first author obtained the participant's consent before audiotaping and transcribing the interviews. To review and make any necessary revisions, the completed interview transcript was shared with the appropriate interviewee.

The interviewee's approval allowed for the use of the final transcription in subsequent analyses. The variety of cybersecurity threats that surfaced during significant crises, the organisational responses to these threats, and the interviews mainly focused on these dangers and how they prompted learning. To fully grasp the various strategies employed in HERS, we asked you to elaborate on some instances and strategies, among other probing questions.

Table 1 A table describing the interview

Identifier	*Position title*	*Years of experience*
P001	Officer for Security, Chief	11 years
P002	Manager of Data Security	3 years
P003	Manager of it for Seniors	5 years
P004	Analyst of Cybersecurity	9 years
P005	Officer for Security, Chief	9 years
P006	Manager of Strategy	6 years

Figure 3 A step-by-step guide to creating a fintech cybersecurity framework (see online version for colours)



In order to achieve its goals, this study employs a qualitative methodology. A wide variety of forms may be taken by this method, depending on the field of study. Gaining a deeper understanding of the collected data and providing unambiguous conclusions is the main objective of this strategy. Interviews were scheduled with important individuals from Bahraini financial institutions and fintech firms to obtain qualitative data that may be used for future research purposes. We investigated the rules that the Central Bank of Bahrain issued to the banks in the country about cybersecurity. The results of these studies will guide the development of a research tool that uses interviews to examine the main features of a cybersecurity framework for financial technology in Bahrain. Examining the methodological approaches is an integral part of solving the research

problem since it allows us to test the theoretical cybersecurity measures. We decided that the best approach to take in this study was the research 'onion' strategy that Saunders, Lewis, and Thornhill came up with. A number of researchers have made use of this to better comprehend the many components of the research process. Each layer of this onion represents a distinct approach to study, including a philosophy, strategy, options, technique, timeline, tool, and process for collecting data.

By looking at how companies usually function, this kind of study primarily focuses on real practices. Silverman argues that the research issue is best addressed using a case study approach since it enables researchers to thoroughly examine a process, event, or activity with a limited sample size. Consequently, to understand the cyber-related problems in Bahrain's financial industry, the study employed an exploratory qualitative methodology. Because of this, we were able to answer the study question using the qualitative data in a thoughtful and significant way. Comparing data from different sources allowed us to define and assess the consistency and accuracy of the findings; this was made possible by the qualitative method. The research plan and design are shown in Figure 1.

Table 2 Background about educational institutions

No.	*Nation*	*IT governance model*	*Control type*	*Institution size*	*IT staff count*	*Primary orientation*
1	Netherlands	Federal	Public	Very large	100–300	Teaching
2	Netherlands	Centralised	Public	Medium	100–300	Research
3	Brazil	Federal	Public	Very large	50–99	Research, teaching, community
4	Brazil	Federal	Public	Very large	100–300	Research, teaching, community
5	Israel	Federal	Public	Very large	100–300	Research, teaching, community

3.2 Data analysis

In order to discover both current and future ITG practices, 10 institutions in five different countries (Israel, Portugal, the Netherlands, Spain, and Brazil) were interviewed using a semi-structured interview format. Although a convenience sample was still used to choose colleges based on their availability for the study, a range of criteria were used to minimise contextual bias, including institutional size, culture, strategy, structure, and procedure. Table 2 provides some details regarding these establishments.

Higher education institutions' chief information officers (CIOs), information technology coordinators, and directors – those typically in charge of all things IT – were interviewed for this study. Each interview is about 1.5 hours long. Every interview, whether conducted in person or by Skype when that was not an option, was video recorded. One way the researcher got in touch was by searching the institution's IT website for the name, email, and phone number of the CIO or another IT decision-maker (Mahmood, 2024). After that, the individual was contacted via email to go over the study goals and interview purposes, along with an invitation to fill out a questionnaire that would serve as a roadmap for the interview. To make sure that everyone who participated

in the interview understood what each ITG practice meant, we also supplied a booklet with definitions of the practices. Myers and Newman's suggestions for reducing social dissonance in research informed the development of the interview and questionnaire (2007, pp.16–17). The interviewers were also confronted with documents, observations, the IT website, and the study of IT strategic plans to make sure they were aware of and confident in their replies. Specifically, the interview was structured around a four-part questionnaire that asked the following:

1 general institution-related questions

2 interviewee-specific questions

3 enquiries evaluating the efficacy and simplicity of execution (using a five-point Likert scale)

4 questions allowing respondents to propose new practices, with a focus on university settings, and to rank the ten most essential practices (AlBenJasim et al., 2024).

The purpose of asking the same question twice for all 46 activities (Table 2) was to gather more detailed information about each practice. Using Microsoft Excel, we examined the data and tallied the occurrences of each mechanism. The qualitative data were also transcribed and analysed using the program 'NVIVO.' Structure, process, and relational were the three primary pre-defined categories used to code the data. Respondents were also given the chance to fill in gaps in the practices section by sharing their own experiences. In order to interpret the respondents' suggestions for new practices, the data were coded primarily using three categories: structures, processes, and relational mechanisms. 'We are in an open environment' is one such quote. You get my point. When compared to industry, universities are unique. Here, we can try out several approaches and see what works best; if something goes wrong, it won't affect the company overall.

Table 3 Essential tenets for every candidate

Structure type	*Org 1*	*Org 2*	*Org 3*	*Org 4*	*Org 5*	*Org 6*	*Org 7*	*Org 8*	*Org 9*	*Org 10*	*Count*
IT strategy committee	1	6	1	1	7	–	1	1	1	1	9
IT governance framework	–	–	3	6	8	–	3	–	2	10	6
IT governance officer/function	–	–	–	2	–	10	8	–	3	–	4
Business & IT relationship managers	–	10	10	9	–	4	–	–	–	–	4
IT steering committee	10	–	4	4	–	–	–	–	–	–	3
Governance roles integrated in duties	–	–	–	–	–	–	–	2	–	3	

However, this is just not doable in the business world because of the imperative of operational efficiency..." placed in the processes section at the 'test and experiments

possibility' made selective code. For every practice that the interviewers suggested, the identical approach was taken. The study of the data revealed eight practices. Each interviewee ranked ten practices from one (most essential) to ten (least significant), as shown in Table 3.

3.3 Data and quality assurance

To be effective, a company's decision-making process needs to be quick and precise. Information can originate from a wide variety of places, depending on the industry and kind of business. Some European HEIs had trouble gaining access to data until the past decade. Among other things, they investigated data gaps at 12 European universities and proposed solutions for collecting and vetting data from a variety of national sources. While some nations' national statistical organisations gathered information from universities centrally, others relied on data obtained directly from colleges. This highlighted problem with data transparency. Concerning the data's credibility, the writers also noted issues with its consistency and quality. Higher education institutions may find it tough to collect and analyse accreditation key performance indicator data. It might be challenging to guarantee data accuracy and consistency when the data is dispersed across many systems (Bianchi et al., 2021). Data privacy, security, and access permission management are not without their difficulties, particularly when dealing with sensitive data. Furthermore, institutions frequently face challenges due to budget limits and limited resources when it comes to data administration and reporting.

Jacob states that descriptive, predictive, diagnostic, and prescriptive data analytics are the four main categories. Keeping track of known or suspected connections is the most prevalent strategy employed in descriptive analytics. In order to find bottlenecks, diagnostic analytics use metrics such as quality process cycle times. Measurements that centre on forecasting the future include trend analysis and the application of trend rules to SPC data. These days, analytics are more directive. Common characteristics include self-sufficiency, error detection, and directions for modifying the outcome or resolving issues. Using typical quality settings and conventional data, analytics operations of a descriptive, diagnostic, and predictive nature can be done with the help of ML/AI. Many HEIs encounter considerable challenges when trying to make strategic decisions because of the complexity of measuring and analysing massive amounts of data. Data analytics, according to Nguyen, Gardner, and Sheridan, enable HEIs to discover the crucial instructional practices that boost their efficiency. There are three main approaches to data analysis in HEIs, according to the authors:

- Data mining for education: analytics like these centre on students and how they learn. This method improves learning outcomes by collecting data on students and their learning profiles in addition to course materials and analysing it descriptively.
- Analytics in the classroom: this strategy helps teachers identify the most effective ways to improve their lessons by combining descriptive and predictive analytics. Using data mining in the classroom: using analytics to make sense of unstructured data, this approach seeks to better understand students and educational systems. The enterprise level is the only appropriate place to run the quality management system; lower levels are ineffective. At its core, value chain development is an organisation's commitment to quality, since it permeates all operational and managerial aspects of

> the value chain. Before they are linked, these processes should be synced, and the software should be automated, says Jacob.

This will allow the high-value workers to focus on innovation and improving traditional quality methods, rather than the mechanics of execution. Although there has been an uptick in the number of organisations using integrated systems, the author claims that only over 10% of businesses have made the switch. Modern companies' disconnected core processes have caused delays in installing high-quality technology that enables systems to become autonomous. This technology is a necessity for adopting an integrated system. Therefore, businesses should coordinate their quality processes so that software can automate them. Once a business's quality procedures are standardised and automated, they can be seamlessly connected with other systems and operations. An increase in collective analytics and learning would lead to a steady improvement in system autonomy with this kind of link. The system's central database is utilised to track quality indicators, and reports can be generated at the university or organisational unit level. The incorporation of preexisting data from databases of separate organisational divisions is a key feature of the system. A further essential quality is the ability to record information for which no digital copy currently exists.

A university-level subsystem for data integration implements features for obtaining, cleaning, and loading a central data warehouse. The data warehouse stores information about programs, courses, students, and faculty. Also included in the statistics on faculty members are the outcomes of student questionnaires that are used to assess the quality of instruction. This data is examined and displayed using programming tools that are based on the application of business knowledge. Multiple surveys are providing quality indicators. It is much easier to have the data ready when needed if these surveys are automated and integrated with current systems. When automating quality-related processes or undergoing a digital transition, these measures are crucial. The success of these endeavours depends critically on getting the surveys into the correct systems via a well-defined procedure that guarantees the correct response rate. There are around nine surveys about various aspects of Prince Sultan University, such as students, staff, services, etc. These components were integrated into the preexisting system using an appropriate method to mandate a specific rate of response.

4 Results and findings

In response to increased cybersecurity threats, the organisation implemented new rules, as described in the Triple- loop learning topic, during the height of the HERS crisis. The creation of novel OL rules and procedures is known as deuteron or triple-loop learning. There is a main subtheme within the theme: one piece of strategic data is the introduction of new policies and processes. Following up on the theme's investigation, we found that during a big crisis at HERS, we were able to keep our employees safe by updating our strategic information and implementing new organisational procedures. Critical data regarding the amount of implementation, efficacy, and ease of implementation was provided by the questioned individuals in order to understand the context of IT governance in their universities. The selection of the ten most critical practices relied heavily on this data. The respondent also acquired the meaning of each mechanism, which allowed them to reevaluate and prioritise their university's actual IT governance

architecture. The number of people who have listed that specific mechanism as very important is reflected in the 'frequency' column. 'process management office,' 'dashboard,' and 'engagement between IT and academia' were among the additional practices proposed, along with the chosen ones.

4.1 Important strategic data – the implementation of novel policies and procedures

Because of the increased cybersecurity risks during the COVID-19 pandemic, the higher education institutions that participated put into place in five new policies. This is an example of triple-loop organisational learning. These planned actions and the places and ways they were used are summed up in Table 4.

Table 4 Summary of new cybersecurity policies implemented

Policy name	*Core features*	*Implementation context*	*Primary stakeholders*
Zero-trust policy	You must use multi-factor login; ongoing verification process Trust is not given by default	Remote work transition during COVID-19	All staff and students
Access control policy	Data access based on role; official data request steps; security approval levels	Data breach mitigation; remote access vulnerabilities	IT administrators; department heads
Meet-and-greet policy	Virtual meetings every week, open channels of contact, and working together to solve problems	COVID-19 pandemic; distributed workforce	All employees; management
Chatbot application	Reporting incidents any time of the day or week, contact across departments, and quick responses	Remote operation requirements	IT support; all end- users
Device usage policy	Security rules for BYOD; protection needs for endpoints; compliance tracking	Personal device proliferation	All network users

The study found these rules to be very similar: they prioritise ongoing verification over perimeter-based security, they make it easier to work from home, they improve communication channels for quick incident response, and they include user awareness in technical controls.

Representative participant insights include:

- Zero-trust implementation: zero trust means that everyone is not believed by default. 'Even with valid credentials, we require additional verification through personal ID confirmation' (C002).
- Rapid reporting mechanism: 'our portals' chatbot helps us report cyber problems faster'.
- Data access governance: the policy has been changed so that staff can't get to all info. 'Security administrators make sure that only people who are allowed to see the data they need can get to it' (C012).

These policy changes are the first fully documented complete cybersecurity countermeasures for higher education institutions during times of crisis. In the next step, a group of 25 cybersecurity and fintech experts from Bahrain's banking industry at NGN Mallis International confirmed that the framework was correct through Delphi workshops.

4.2 Delphi rounds

Twenty-five experts in hacking and banking each took part in two Delphi validation rounds. Frameworks were rated on Likert scales in the first round, and results based on agreement that led to the ordering of frameworks by value in the second round. Table 5 shows the changes in the rankings over time in both games.

Table 5 Delphi session rounds for principal ranking and prioritisation within the framework

Principle area	*Round 1 mean*	*Round 1 SD*	*Rank (R1)*	*Round 2 mean*	*Round 2 SD*	*Rank (R2)*
Risk management	2.00	1.118	1	1.76	0.831	1
Regulation and governance	2.56	1.685	2	2.12	1.269	2
Capacity development and awareness	3.36	1.655	3	3.32	1.345	3
Secure service implementation	3.88	1.364	4	3.48	1.194	4
Adoption of best practices	4.32	1.464	5	5.08	0.954	5
Engagement with third parties	4.88	1.130	6	5.20	1.000	6

4.3 Statistical analysis

The optimal number of rounds in a Delphi session is still unknown; however, it has been observed that more rounds may result in lower answer rates. While there are numerous ways to look at the data, descriptive statistics are a typical way to validate the data that is obtained at each round of the Delphi method. This study makes use of more sophisticated techniques, such as Kendall's W, which provide a way to assess changes across Delphi rounds. To compare and evaluate expert responses, the Delphi method uses descriptive statistics. The responses were quantified using a Likert scale that went from 1 to 5. After that, we utilised Kendall's W coefficient to find out how concordant the feedback was and how much convergence the Delphi rounds had produced. To find out how much people agree based on rank correlation, researchers use Kendall's coefficient of concordance (W), a non-parametric statistic. To review, the following is the definition of Kendall's W: form raters assign ratings to n subjects ranging from 1 to n, and S is the squared deviation of ratings.

$$W = \frac{12S}{m^2\left(n^3 - n\right)} \tag{1}$$

According to Schmidt, Kendall's W, a measure of agreement, is a scale from 0 to 1. A score of 0 indicates full agreement and a score of 1 complete dissent, as shown in Table 6.

Table 6 Reasoning behind Kendall's W-coefficient

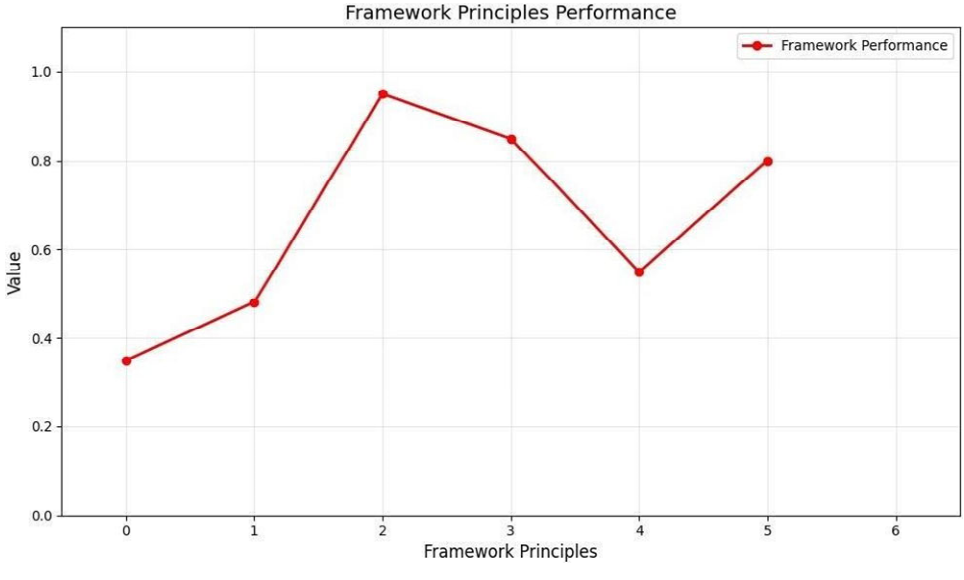
W value	*Description of consensus*
0.00	No consensus observed
0.10	Very weak level of consensus
0.30	Moderate level of consensus
0.60	Strong consensus achieved
1.00	Complete consensus

The calculated degrees of consensus (W) are displayed in Table 7, second column. Each set of controls (principles) had W values of 0.78, 0.55, 0.91, 0.84, and 0.32 according to Kendall's W coefficient interpretation, indicating that the participants were at high levels of agreement with the ranking of the framework's controls.

Table 7 Indicators of agreement level (W)

S. no.	*Principle area*	*W score*
1	Awareness and capacity building	0.3208
2	Governance and regulation	0.4574
3	Risk management	0.8379
4	Secure service implementation	0.5546
5	Collaboration with third parties	0.9086
6	Adoption of best practices	0.7832

Figure 4 Cybersecurity framework development for financial technology innovations: a case study of Bahrain (see online version for colours)



The W values were higher than 0.55 in five of six main areas, which shows that there was moderate to strong agreement in these cases. The highest level of agreement (W = 0.9086) was found in collaboration with third parties, and a moderate level (W = 0.3208) of agreement was found in awareness and capacity building. This means that this area needs to be changed to fit the unique situation.

4.4 Framework evaluation across institutional contexts

4.4.1 Evaluation methodology and criteria

The framework was tested at a basic level in four institutions in Portugal, Germany, Brazil, and Spain, which had different types of government and sizes (Table 9). Evaluation used five factors (Table 8): how complete it was, how easy it was to use, how well it matched up with practice, how consistent it was internally, and how detailed it was.

Table 8 Assessment Tool for IT governance practices' foundation

No.	*Criterion*	*Reformulated statement*
1	Completeness	The framework includes all essential practices required for effective IT governance in higher education institutions
2	Ease of use	The set of practices is clearly explained, user-friendly, and can be implemented in universities with minimal effort
3	Alignment with practice	The proposed framework reflects realistic solutions and supports the appropriate selection of IT governance practices.
4	Internal consistency	The framework applies consistent terminology, is clearly articulated, and is supported by theoretical justification
5	Level of detail	Each mechanism in the framework provides adequate detail to guide IT governance processes in universities

4.4.2 Evaluation outcomes all evaluators (N = 5) confirmed the framework's

- Completeness: encompasses essential ITG practices for diverse HEI contexts
- Ease of use: clearly articulated with implementable guidelines, though requiring context-specific adaptation
- Alignment with practice: reflects realistic solutions applicable across institutional maturity levels
- Internal consistency: demonstrates consistent terminology and theoretical justification
- Level of detail: provides adequate guidance while allowing institutional flexibility.

4.4.3 Geographic and institutional variations

Table 10 synthesises implementation challenges and recommendations by geographic region. Common challenges across all institutions included: human resource limitations (4/5 evaluators) – organisational culture resistance

to change (3/5 evaluators) – budget constraints for comprehensive implementation (5/5 evaluators) – variable IT governance maturity levels (4/5 evaluators).

- European institutions (Portugal, Germany, Spain): stressed how difficult it is to work with partners and old tools. Governance groups that are suggested for phased adoption.
- Latin American context (Brazil): cultural change is needed, and so is shared infrastructure control. It is suggested that government policies be changed in ways that consider what is happening in the area.

All of the evaluators said that for the project to work, the institution would have to adapt to its culture, finances, level of management support, and level of governance maturity.

Table 9 The Evaluation provides information regarding the interviews

No.	*Country*	*University size and IT staff*	*Position*	*Education and professional background*
1	Portugal	Large (50–99 employees) IT	Director of IT Services	Holds a Master's degree in Computer Science, with more than 20 years in IT and over 5 years in a senior director role
2	Germany	Extra-large (100–300 IT employees)	Chief Information Officer (CIO)	PhD holder with 30+ years of IT expertise; also serves as a full professor and active researcher
3	Portugal	Large (24–50 employees) IT	IT Technical Coordinator	Master's in Computer Science, more than 13 years in IT, with notable experience in IT governance and academic research
4	Brazil	Extra-large	(100–300 IT employees)	CIO and Consultant PhD in Information Technology and Business, over 40 years in academic IT, 20+ years in governance leadership, and consultancy for multiple universities
5	Spain	Extra-large	(100–300 I	

Table 10 Institutional context and implementation challenges by region

Region	*Institution size*	*Primary challenges*	*Recommended focus areas*
Portugal	Large (24–99 staff)	Budget is small; old technology; staff is not trained in all areas	Capacity building, incremental upgrades, and phased execution
Germany	Extra-large (100–300)	Federal rule; policy alignment; stakeholder coordination	Communication methods; clearer governance; committees that work across departments
Brazil	Extra-large (100–300)	Cultural adaptation; infrastructure spread; resource differences	Making decisions based on the area, working together at the federal level, and sharing resources
Spain	Extra-large (100–300)	System integration; resistance to change; complicated coordination	Interoperability rules, trial projects, and involvement of stakeholders

4.5 Digital transformation and quality assurance

The digital revolution has altered the goals and standards for QA in education, as well as the methods used to assess the efficacy of instructors. This leads to a digital shift in QA in education, which incorporates new elements. The following features are included in these changes: Objectives, ranging from a singular set to a variety of them. In this digital era, talents with a diverse set of abilities are in high demand. Because of this, we need to shift our attention from the old standard QA goals in education, which were for kids to acquire knowledge, to their holistic development, which encompasses developing their skills and values. Grades and early warning systems are among the many operations. Following an evaluation of the effectiveness of instruction delivery and student learning, QA in education often comprises optimising QA operations. QA in education can now evaluate these and other factors with the use of real-time data on student learning, instructional delivery, course implementation, and other subjects made possible by artificial intelligence prediction technology and big data. These, in turn, provide analyses of broad patterns and presentations on the current status of education. They can serve as a signal for potential danger because of this.

Things that are either scattered or integrated: Analytics based on unstructured data from all of an enterprise's systems replace analytics based on structured data from a single information system in QA learning and teaching objects after the digital revolution. Many departments focus solely on their own areas of responsibility in the initial QA system, and information is fragmented, and links lack meaningful relationships. However, these issues do not arise in a digitally modified QA system because all QA components are integrated systematically. Complete and balanced coverage of standards, as opposed to incomplete and biased coverage: due to the increasing multidimensionality of quality goals and the digitisation of measurement and statistics, the standards for QA in education have expanded to encompass the whole educational process and all aspects of instructional objectives, rather than focusing on just a subset of these – the evolution of standardised and sampling-based approaches to evaluating classroom instruction's quality. Typically, a small subset of students, instructors, and academic programs is assessed at the end of each semester or quarter under the old system of QA in education.

Poor management of assessment feedback time and erroneous assessment findings lead to inadequate impact on instruction. In contrast, data-driven intelligent teaching assessment permits standardised and full-scale quality evaluation by improving the efficiency of measuring, assessing, and giving feedback. Transitioning from closed to an open form of evaluating teaching quality: The previous evaluation process, which involved the transmission of data between multiple assessors, was costly, inefficient, and had minimal transparency. The idea of data sharing and the promotion of digital technology have opened the door for more items and more people to join the digital age. Multiple parties can conduct evaluations using the same database. This also makes it easier for groups both inside and outside the university to communicate and work together. The review process becomes more accessible, transparent, and participatory as a result. Figure 5 shows the potential benefits to educational settings of automating data collection methods and consolidating data onto a single platform. Educational services can be delivered more effectively by facilitating the integration of learning and reducing communication barriers. One more way to make education better is to use dashboards and alerts to keep an eye on key performance indicators (KPIs).

Figure 5. Actions taken and their impact on SDG (see online version for colours)

5 Conclusions

The importance of incorporating the rule of law principles into cybersecurity governance plans by higher education institutions is highlighted by this study. While technical safeguards are still necessary, the results show that a comprehensive framework is needed to protect institutional assets in the long run. This framework should priorities organisational learning, capacity building, and legal compliance. The suggested framework places an emphasis on raising awareness to encourage staff and students to take an active role in cybersecurity, improving data and QA processes, and bolstering risk management. Heterogeneous information technology infrastructures and cultural openness can be mitigated if HEIs implement the suggested policies, which include access control legislation, compliance monitoring, and zero-trust designs. Furthermore, the report emphasises the importance of ensuring that governance procedures are in line with global standards for protecting intellectual property, research integrity, and personal data. Lastly, incorporating cybersecurity governance into the broader framework of rule of law education helps encourage a culture of accountability and resilience in the face of evolving cyber threats, therefore reducing institutional risks.

Funding

Dezhou Research Center for Ideological and Political Education.

Declarations

All authors declare that they have no conflicts of interest.

References

Ahmed, S., Taqi, H.M.M. and Sankaranarayanan (2021) 'Evaluation of flexible strategies to manage the COVID-19 pandemic in the education sector', *Global Journal of Flexible Systems Management*, December, Vol. 22, Suppl. 2, pp.81–105.

Akacha, S.A-L. and Awad, A.I. (2023) 'Enhancing security and sustainability of e-learning software systems: a comprehensive vulnerability analysis and recommendations for stakeholders', *Sustainability*, Vol. 15, No. 19, p.14132, DOI: 10.3390/su151914132.

AlAhmad, A.S. et al. (2021) 'Mobile cloud computing models security issues: a systematic review', *J. Netw. Comput. Appl.*, Vol. 190, No. 2021, p.103152.

AlBenJasim, S. et al. (2024) 'Development of a cybersecurity framework for FinTech innovations: Bahrain as a case study', *Int. Cybersecur. Law Rev*., December, Vol. 5, No. 4, pp.501–532.

Alharbi, T. (2021) 'Assessment of cybersecurity awareness among students of Majmaah University', *Big Data Cogn. Comput*., 10 May, Vol. 5, No. 2, p.23.

Bianchi, I.S., Sousa, R.D. and Pereira, R. (2021) 'Information technology governance for higher education institutions: a multi-country study', *Informatics*, MDPI, Vol. 8, No. 2, p.2021.

Cheng, E.C.K. (2022) 'Institutional strategies for cybersecurity in higher education institutions', *Information*, 12 April, Vol. 13, No. 4, p.192.

Chodakowska, A., Kańduła, S. and Przybylska, J. (2022) 'Cybersecurity in the local government sector in Poland: more work needs to be done: more work needs to be done', *Lex Localis-Journal of Local Self-Government*, Vol. 20.1, No. 2022, pp.161–192.

Garba, A. and Sirat, M.B. (2020) 'Cyber security awareness among university students: a case study', *Sci. Proc. Ser*., 1 January, Vol. 2, pp.82–86.

Hossain, S.T. et al. (2024a) 'Cybersecurity in local governments: a review and framework of key challenges', SSRN 4631885.

Hossain, S.T. et al. (2024b) 'Local government cybersecurity landscape: a systematic review and conceptual framework', *Applied Sciences*, Vol. 14.13, No. 2024, p.5501.

Javed, Y. (2023) 'Case study on sustainable quality assurance in higher education', *Sustainability*, Vol. 15, p.8136, https://doi.org/10.3390/su15108136.

Khader, M., Karam, M. and Fares, H. (2021) 'Cybersecurity awareness framework for academia', *Information*, 12 October, Vol. 12, No. 10, p.417.

Lee, I. (2021) 'Cybersecurity: risk management framework and investment cost analysis', *Bus. Horiz*., 1 September, Vol. 64, No. 5, pp.659–671.

Li, J., Othman, M.S., Hewan, C. and Yusuf, L.M. (2025) 'IoT security: a systematic literature review of feature selection methods for machine learning-based attack classification', *International Journal of Electronic Security and Digital Forensics*, Vol. 17, Nos. 1–2, pp.60–107, DOI: 10.1504/IJESDF.2025.143475.

Lija, A.V.K., Shobana, R., Misbha, J.C. and Chandrakala, S. (2025) 'IoT security using deep learning algorithm: intrusion detection model using LSTM', *International Journal of Electronic Security and Digital Forensics*, Vol. 17, Nos. 1–2, DOI: 10.1504/IJESDF. 2025.143479.

Mahmood, S. (2024) 'Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: an organisational learning perspective', *Information*, Vol. 15, p.106, https://doi.org/10.3390/info15020106.

Mishra, A. et al. (2022) 'Cybersecurity enterprises policies: a comparative study', *Sensors*, Vol. 22.2, No. 2022, p.538.

Modi, R., Jammoria, A.S., Pattiwar, A., Agrawal, A. and Raja, S.P. (2025) 'Secure system to secure crime data using hybrid: RSA-AES and hybrid: blowfish-triple DES', *International Journal of Electronic Security and Digital Forensics*, Vol. 17, Nos. 1–2, pp.194–232, DOI: 10.1504/IJESDF.2025.143472.

Mubin, O. et al. (2024) 'Tracking ChatGPT Research: Insights from the literature and the web', *IEEE Access*, Vol. 12, No. 2024, pp.30518–30532.

Murphey, D. (2022) 'A history of information security', *IFSEC Global* [online] https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/ (accessed 20 February 2022).

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E. and Chou, R. (2021) 'The PRISMA 2020 statement: an updated guideline for reporting systematic reviews', *bmj*, 29 March, Vol. 372.

Salem, M. et al. (2024) 'Evaluating the effectiveness of online cybersecurity program in higher education', *2024 IEEE Global Engineering Education Conference* (*EDUCON*), IEEE.

Strang, K.D. and Vajjhala, N.R. (2024) 'Exploring cybersecurity risks in higher education environments with machine learning', *2024 4th International Conference on Pervasive Computing and Social Networking* (*ICPCSN*), IEEE.