World Journal on Educational Technology: Current Issues
e-ISSN 1309-0348

Volume 18, Issue 1, (2026) 76-87

https://un-pub.eu/ojs/index.php/wjet/index

# Corporate Policy Integration for Cybersecurity in Education: A Model Structure for Higher Education Institutions

**Serkan Yaman**[a1], Istanbul Aydin University, Istanbul, Türkiye, serkanyaman@aydin.edu.tr https://orcid.org/0000-0001-5916-5131
**Ebru Yaman**[b], Istanbul Aydin University, Istanbul, Türkiye, ebruyaman1@aydin.edu.tr https://orcid.org/0009-0009-3641-7135

**Suggested Citation:**

Yaman, S., & Yaman, E. (2026). Corporate policy integration for cybersecurity in education: A model structure for higher education institutions. *World Journal on Educational Technology: Current Issues, 18*(1), 76-87. https://doi.org/10.18844/wjet.v18i1.9980

Received on August 2, 2025; revised on December 12, 2025; accepted on January 12, 2026.
Selection and peer review under the responsibility of *Prof. Dr. Huseyin Uzunboylu*, University of Kyrenia, Cyprus


**Abstract**

Higher education institutions, standing at the forefront of digital transformation, have become primary targets for cyber attackers on a global scale due to the massive personal data, strategic academic research, financial records, and large-scale network infrastructures they host. Unlike traditional corporate structures, the fact that higher education institutions are founded on the principles of "academic freedom" and "open access to information" brings unique challenges to the construction of cybersecurity architecture. Viewing cybersecurity merely as a technical IT issue in these institutions remains insufficient in today's complex threat landscape. Therefore, integrating technical measures into corporate governance processes, legal requirements, and academic culture is a necessity. The primary objective of this research is to develop a sustainable and holistic "Cybersecurity in Education" model structure suitable for the dynamic nature of higher education institutions. The study centers on the perspective of Cybersecurity Program students who are in the process of professionalization and are being cultivated within the technical core of this field. Synthesizing the students' technical vision with institutional needs will ensure that the proposed model is both technologically valid against current threats and practically applicable. The methodological framework of the research is built upon the "case study" design, a qualitative research method. Data was collected through a semi-structured interview form divided into three main categories. As a result of the content analysis of the collected data, it was determined that the greatest risk factor threatening corporate security is "user unawareness." To ensure the balance between academic freedom and security and to manage BYOD (Bring Your Own Device) risks, the necessity of "Network Access Control (NAC)," "isolated research networks (Sandbox)," and anomaly detection systems was emphasized. Within the scope of emergency and business continuity, redundant server architectures and DDoS protection systems stood out; while it was determined

* ADDRESS FOR CORRESPONDENCE: **Serkan Yaman**[a1], Istanbul Aydin University, Istanbul, Türkiye, serkanyaman@aydin.edu.tr

that to spread the cybersecurity culture throughout the institution, policies must be supported by gamification, phishing simulations, and practical laboratory training. In light of these findings, a three-dimensional model proposal consisting of technical, administrative, and human layers has been developed. This model, in which legal obligations such as the KVKK (Personal Data Protection Law) are transparently integrated into technical processes, is expected to guide decision-makers, IT departments, and strategy development units in higher education institutions. This study not only provides a security guide but also presents an original theoretical framework for making cybersecurity an integral part of educational processes.

**Keywords:** Cybersecurity in Education, Higher Education Institutions, Corporate Policy, Cybersecurity Model, Cyber Resilience.

## 1. INTRODUCTION

The past decade has witnessed a tectonic shift in the perception of cybersecurity education and corporate security paradigms. Once considered the technical responsibility of a limited group of IT professionals or a few dedicated educators, the phenomenon of cybersecurity has now moved to the forefront of national and international policies, geopolitical conflicts, and corporate strategic planning (Austin, 2020). In this new era where technological disruption and political threats are rapidly accelerating, the global cybersecurity talent shortage places immense pressure on organizations and states regarding workforce development and infrastructure resilience policies. Higher education institutions, in particular, positioned at the very center of digital transformation, find themselves at the heart of increasing domestic and international cyber dependency and parallel organized cyber threats due to the massive amounts of personal data, intellectual property, patents, and critical research infrastructures they host (Thakur, 2016). This situation clearly demonstrates that for universities, cybersecurity no longer means merely protecting hardware assets; it means sustaining the existential integrity, reputation, and knowledge production capacity of the institutions.

The cybersecurity architecture and infrastructure management in higher education institutions possess a much more complex and unique nature compared to traditional corporate structures, government agencies, and industrial systems (Schneider, 2013). While a commercial enterprise or a government office can strictly secure itself with rigid access restrictions, isolated systems, and closed-loop networks; universities are inherently built upon the principles of “academic freedom,” “transparency,” “information sharing,” and “cross-border global collaboration.” When this innovative and open vision is combined with tens of thousands of students, academics, researchers, and guest users integrating into campus networks with their own personal smartphones and computers (BYOD – Bring Your Own Device), it significantly blurs the physical and logical boundaries of the corporate network, making centralized control of network traffic almost impossible. The primary goal of cybersecurity policies and education in universities is not to create a closed box by restricting access to information; rather, it is to guarantee the free circulation of information within a secure, flexible, and resilient ecosystem. Therefore, higher education institutions must strike that fine, delicate, and difficult-to-manage balance between data security requirements and the usability and freedom of academic systems (Stiawan, 2010).

On the other hand, an examination of traditional approaches in the literature reveals a tendency to define cybersecurity primarily through technology-based skills, next-generation firewalls, complex encryption algorithms, and software patch solutions for many years. Today, however, this narrow and one-dimensional perspective has given way to the reality that cybersecurity is not merely a technical hardware or software issue. Cybersecurity is an incredibly complex, multidimensional, and socio-technical problem area that intertwines user privacy, digital ethics, corporate governance, policy-making, human behavior, and systems engineering (von Solms & Futcher, 2018). A cybersecurity infrastructure that relies solely on technical

measures, is not synchronized with human behavior and administrative policies, and fails to educate users (students and staff) about risks cannot survive in today's sophisticated threat environment—especially against phishing, ransomware, and social engineering attacks. National and international frameworks mandate the integration of strategic best practices into the organizational culture and the centralization of the "human factor" in planning cybersecurity awareness and enhancing the resilience of critical infrastructures (NIAC, 2009; NICE, 2012). In this context, on the new social terrain of security in cyberspace, the integrated repositioning of education, technology, and policy-making processes is an inevitable academic necessity (Singh, 2017).

### *1.1. Purpose of the Study*

The primary purpose of this study is to develop a sustainable, inclusive, and holistic "Cybersecurity in Education" model that is fully compatible with the dynamic, decentralized, and open structure of higher education institutions. Going beyond providing institutions with a purely technical IT framework, this study proceeds from the premise that cybersecurity is a multi-layered and "human-centric" phenomenon (von Solms & Futcher, 2018); it aims to establish a rational and practically applicable balance between academic freedom, the fundamental philosophy of universities, and the information security imperatives of the modern age. Within this main theoretical framework, the sub-objectives of the study are detailed as follows:

- To holistically analyze the human-centric security vulnerabilities arising from the "unawareness of users" (students, academic, and administrative staff) in higher education institutions and the general risk perception of the institution against internal/external threats, in the context of increasing levels of cyber dependency (Thakur, 2016).
- To evaluate and resolve the management challenges and technical risks posed to information security by multiple and personal device usage habits (BYOD), which eliminate the traditional boundaries of the corporate network, without violating the university's principles of uninterrupted access to information (CERT, 2020).
- To ensure an interdisciplinary "corporate policy integration" that combines hardware and software security measures in the network infrastructure with existing legal requirements (e.g., KVKK/GDPR compliance, intellectual property laws), national standards, and university administrative rules (NICE, 2012).
- To move beyond theoretical policy documents that merely remain on shelves; providing an actionable model architecture that will prevent any interruption in education and research processes during crises (including steps for business continuity, disaster recovery, and emergency planning) and build a permanent, sustainable "cybersecurity culture" throughout the institution.

## 2. METHOD AND MATERIALS

### *2.1. Research Model*

In order to conduct an in-depth and comprehensive examination of the cybersecurity policies, educational frameworks, and human-centric risk factors within higher education institutions, this research adopted a "case study" design, which is a prominent qualitative research approach. A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, particularly when the boundaries between phenomenon and context are not clearly evident. The fundamental rationale for selecting this

specific methodological design is that the complex, multi-layered relationship between the philosophy of "academic freedom" in higher education and the strict imperatives of "cybersecurity" embodies a deep socio-technical structure that cannot be adequately measured or understood through purely quantitative metrics. As von Solms and Futcher (2018) emphasize, cybersecurity must be viewed not solely as a technical discipline, but as a comprehensive socio-technical problem area that requires qualitative exploration of human behaviors, ethics, and corporate governance. Within the scope of this study, the existing cybersecurity ecosystem of a higher education institution and the security perceptions of the individuals operating within this ecosystem were evaluated within the framework of a "holistic single-case design." The interactions between technical requirements, administrative policies, and user behaviors were analyzed in detail, recognizing that cybersecurity education in universities requires a unique pedagogical and structural approach compared to traditional corporate environments (Schneider, 2013). This qualitative framework allows the researcher to capture the nuances of cyber dependency and the resulting vulnerabilities at an institutional level (Thakur, 2016).

### *2.2. Participants*

The study group for this research was determined using the "criterion sampling" technique, which is a purposive sampling method that enables the collection of in-depth, information-rich data in qualitative research. In line with the objectives of the study, the primary criterion for participant selection was that the individuals must possess both theoretical and applied technical education in the field of cybersecurity, and they must actively use and experience the network infrastructure of a higher education institution. Consequently, the study group consists of Cybersecurity Program students who are being cultivated in the "technical core" of cybersecurity, are in the process of professionalization, and stand as prospective experts and future workforce professionals. The critical shortage of global talent places immense pressure on national policy and workforce development (Austin, 2020); thus, capturing the perspectives of these future experts provides invaluable insights into the efficacy of current educational and security policies (Li, 2021). The participants' advanced technical knowledge base ensured that they could evaluate corporate cybersecurity vulnerabilities—such as Bring Your Own Device (BYOD) risks, infrastructure inadequacies, and the integration of legal obligations—from a highly analytical perspective, rather than that of an average end-user. Furthermore, their status as active members of the institution allowed them to provide an "insider" and critical viewpoint regarding the practical applicability of administrative policies and the delicate balance required to maintain academic freedom without compromising critical infrastructure resilience (NIAC, 2009).

### *2.3. Data Collection Tools*

The primary data collection tool utilized in this research was a "Semi-Structured Interview Form," which was developed by the researcher following a comprehensive review of the relevant literature and consultations with field experts. Semi-structured forms offer the researcher the opportunity to collect systematic data around pre-determined themes while simultaneously allowing participants the flexibility to express their unique experiences, observations, and original ideas in detail. Aligned with the sub-objectives of the research and the best practices for planning a cybersecurity workforce and framework (NICE, 2012), the form consists of open-ended questions designed across three main axes:

- Corporate Risk and Threat Perception: This section evaluates the fundamental elements that make higher education institutions highly attractive targets for cyber attackers—such as valuable research data, extensive personal information, and financial records. It also questions the greatest risk factors

threatening corporate security, particularly focusing on the dichotomy between technical infrastructure inadequacies and the human factor, such as user unawareness and a lack of institutional cyber hygiene.

- Model Components and Implementation: This section addresses the complex challenge of establishing a delicate balance between academic freedom (unrestricted internet access for research) and cybersecurity. It probes how institutions should manage the immense risks created by tens of thousands of personal devices (BYOD) on the corporate network and investigates the necessary emergency and business continuity scenarios required to prevent the disruption of educational processes during a cyberattack.
- Policy and Future Recommendations: The final section seeks concrete, actionable recommendations to ensure that security rules do not remain merely as written documents. It explores strategic steps and tangible methods—such as gamification, interactive phishing simulations, continuous education, and strict auditing—to foster a sustainable "cybersecurity culture" that is embraced as a way of life by both staff and students across the institution, addressing the geopolitical and social challenges of modern cyber education (Austin, 2020).

### *2.4. Data Collection Process*

The data collection process was conducted in strict adherence to research ethics and protocols. Prior to their participation, all individuals were provided with preliminary information regarding the primary purpose of the study. They were assured that the data collected would be used exclusively for the scientific development of this research paper and would not be utilized for any commercial or administrative purposes. Furthermore, in accordance with the principle of anonymity, participants were guaranteed that their personal identities would remain completely confidential. The semi-structured interview forms were administered asynchronously through secure, structured digital platforms. This digital and asynchronous method was deliberately chosen to allow participants ample time to think deeply about the questions, reflect on their technical knowledge, and accurately incorporate complex technical terminology into their written responses without feeling any time pressure. This approach facilitated the free and detailed expression of comprehensive policy recommendations and technical observations. The raw data obtained from these forms were digitally recorded without any alteration or intervention, rendering them ready for the subsequent analysis phase (Selvaraj, 2012).

### *2.5. Data Analysis*

The qualitative data obtained from the study were analyzed using the "content analysis" method. The fundamental objective of content analysis is to identify concepts and relationships that can explain the collected data, grouping similar data within the framework of specific themes to organize them in a manner that is comprehensible to the reader. Given the socio-technical complexities of cybersecurity (von Solms & Futcher, 2018), this systematic analysis process was carried out in four main stages:

- Coding of Data: The responses provided by the participants were read line by line. Important words, phrases, and technical expressions that form the conceptual framework of the research (e.g., phishing simulations, Network Access Control, redundant servers, legal compliance, user unawareness) were identified using a free coding approach.

- Finding Themes: The semantic relationships between the generated codes were carefully examined to derive broader, overarching categories and themes that reflect common characteristics (e.g., Technical Layer, Administrative Layer, Human Layer).
- Organizing Data According to Codes and Themes: The participants' views were placed into this systematic thematic framework, and the internal consistency of the findings was rigorously checked.
- Interpretation of Findings: The data, now structured within the thematic framework, were interpreted to construct the architecture of the proposed "Cybersecurity in Education Model," which is the main objective of the study. The findings were then reported and corroborated by the relevant literature. To ensure the reliability of the analysis process, the relationships between the codes and themes were reviewed by a second domain expert, and inter-coder reliability was confirmed (Scott-Hayward, 2015).

## 3. RESULTS

This section presents the results of the content analysis of the qualitative data obtained through semi-structured interview forms from the study group participants, who receive technical education in the field of cybersecurity. The participants' technical and critical observations regarding the university network infrastructure, administrative policies, and user behaviors have been structured under three main sub-headings (themes) in line with the primary objectives of the study.

### *3.1. Corporate Risk and Threat Perception*

The research findings indicate a strong technical consensus on why higher education institutions constitute a primary center of attraction for cyber attackers. According to the data derived from the participants' statements, the fundamental elements that make universities open targets are grouped into three main categories: Firstly, innovative projects at the patent stage and strategic "research/R&D data"; secondly, "comprehensive personal data pools" containing the health, identity, and contact information of tens of thousands of students and staff; and thirdly, "financial records" where high-budget grants and tuition payments are managed. The increasing cyber dependency at both domestic and international levels heightens the criticality of protecting these extensive data repositories (Thakur, 2016). However, when participants were asked about the source of the greatest security vulnerability within the institution, an overwhelming majority emphasized the "human factor" and "user unawareness" rather than hardware or technical infrastructure inadequacies. Consistent with the literature indicating that cybersecurity must be approached as an intricate socio-technical problem rather than a purely technical discipline (von Solms & Futcher, 2018), participants noted that even the most advanced, next-generation firewalls could be breached due to a single unaware user (student or administrative staff) clicking on a phishing email or utilizing weak passwords (Wallach, 2002). The students expressed that while the technological infrastructure in universities is generally at a sufficient level, the digital literacy and cyber hygiene levels of the individuals using this technology remain critically low, which constitutes the largest vulnerability in the corporate risk map.

### *3.2. Balance of Academic Freedom and Security*

The conflict between the principle of "unrestricted access to information"—the fundamental philosophy of higher education institutions—and strict cybersecurity requirements emerged as one of the themes where participants generated the most extensive solutions. The unique and inherently open environment of

universities necessitates a specialized approach to cybersecurity education and infrastructure management that differs significantly from rigid corporate or government networks (Schneider, 2013). Participants argued that internet access cannot be completely restricted to avoid hindering academic research and collaboration; however, this freedom must not degenerate into uncontrolled chaos that threatens the institution's digital assets. The greatest challenge highlighted in maintaining this delicate balance is the BYOD (Bring Your Own Device) culture, which refers to thousands of students and staff connecting to the campus network with their personal, unmanaged smartphones and computers. Participants consider the integration of artificial intelligence-supported "Network Access Control (NAC)" systems mandatory to detect and isolate malicious traffic anomalies within the network dynamically. Furthermore, to protect the main backbone while preserving academic freedom, logically segmenting the network (VLAN configurations) was highly recommended. For instance, the broad "guest/campus networks" connected by students, the "isolated research networks (Sandbox)" utilized by researchers, and the "critical data networks" accessed by administrative staff must be completely isolated from one another (Alvarez-Valdes, 2016). Thus, a potential ransomware infection occurring on an open network endpoint (such as a student's personal laptop) will be physically and logically prevented from spreading to the institution's core academic databases.

### *3.3. Model Components and Corporate Implementation*

When examining the necessary components to transform cybersecurity from a mere IT procedure into a sustainable corporate model, the concepts of "business continuity" and "cultural transformation" came to the forefront. These qualitative findings strongly align with federal recommendations for enhancing the resilience and rapid recovery capabilities of critical infrastructures against complex disruptions (NIAC, 2009). Participants stipulated that "Disaster Recovery" scenarios must be strictly integrated into corporate policy to ensure that vital processes such as exams, course registrations, and administrative operations are not interrupted during a cyberattack (e.g., a massive DDoS attack or a data wiping incident). In this context, it was stated that data must be instantaneously mirrored to servers in a different geographical location utilizing redundant server architectures and secure cloud backups.

On the other hand, it was heavily emphasized that a holistic "cybersecurity culture" must be built across the entire institution so that security policies do not remain solely as legal texts or compliance forms (such as GDPR/KVKK consent documents) on paper. Drawing parallels to the established best practices for planning a cybersecurity workforce and implementing effective awareness programs (NICE, 2012), the concrete and innovative solutions proposed by the participants include the following:

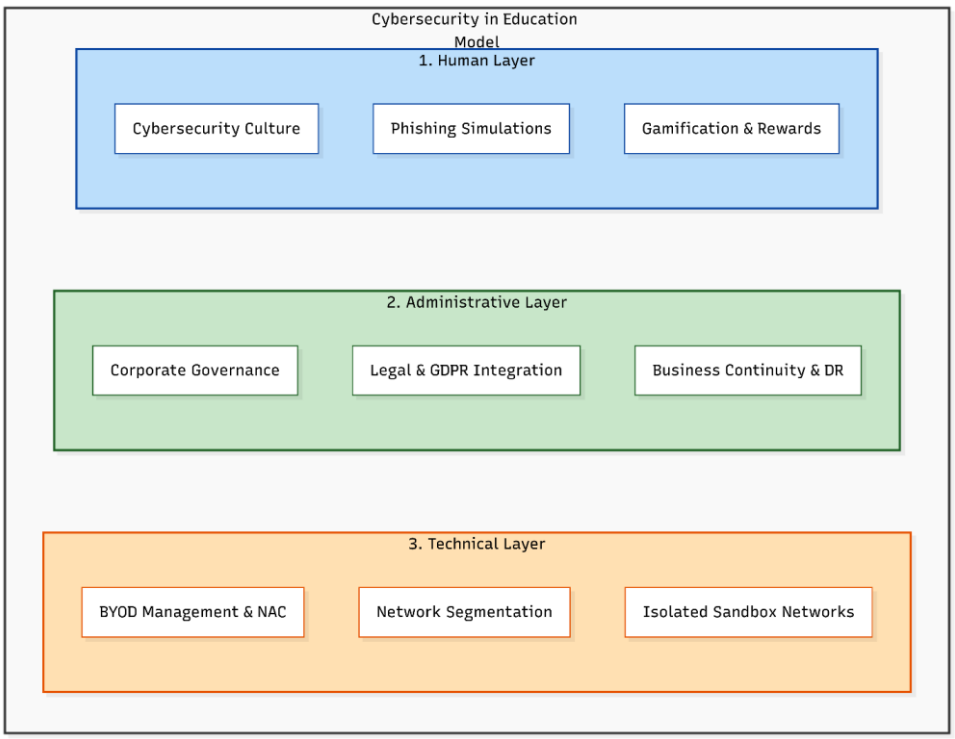
- Gamification and Reward Systems: Transforming security training from tedious theoretical texts into interactive, competition-based modules. Rewarding students and staff who adhere to security rules or actively report vulnerabilities with academic or administrative incentives. This proactive strategy directly responds to the urgent need for new pedagogical approaches in cybersecurity education amidst global talent shortages and escalating threats (Austin, 2020).
- Phishing Simulations: Periodically sending harmless, simulated attack emails to institution staff and students to empirically measure their awareness levels, and providing immediate, applied micro-training to users who fall for the trap.
- Legal and Practical Integration: Integrating legal obligations, such as personal data protection laws, into technical processes from the network architecture's design phase (Privacy by Design).

Furthermore, participants highlighted that presenting real attack scenarios (hacker practices) to students in interactive cyber laboratory environments is necessary to bridge the gap between theoretical knowledge and practical defensive reflexes.

These findings clearly demonstrate that ensuring cybersecurity in higher education institutions requires a holistic model structure where technical intelligence, administrative policies, and human behaviors are continuously synchronized, rather than relying solely on passive hardware investments.

**Figure 1**

*The proposed Cybersecurity in Education Model, illustrating the integration of human, administrative, and technical layers.*




## 4. DISCUSSION

The findings of this study clearly demonstrate that cybersecurity in higher education institutions, which are at the center of digital transformation, is not merely about establishing a hardware-based defense line; rather, it requires the management of a complex socio-technical ecosystem where human factors, administrative policies, and technology are heavily intertwined. The data obtained from the research show a strong parallelism with current theoretical approaches in the literature (von Solms & Futcher, 2018), which argue that cybersecurity has ceased to be a purely technical engineering problem and has transformed into a multidimensional discipline encompassing privacy, ethics, human behavior, and corporate governance. In particular, the technical and administrative criticisms obtained from the perspective of students, who will be

the cybersecurity experts of the future, prove that there are significant gaps in adapting current security paradigms to the unique and flexible structure of universities.

One of the most striking results emerging from the research is that the primary factor threatening corporate information security is not defined as technical infrastructure deficiency or inadequate software investments, but overwhelmingly as the "human factor" and "user unawareness." Considering what a critical center of attraction higher education institutions are at the level of national and international cyber dependency due to the massive research data and personal information they host (Thakur, 2016), it is understood that defense strategies relying solely on firewalls are highly unsustainable. The reality emphasized by the participants, that "even the strongest system can collapse with a single user clicking on a phishing email," indicates that cybersecurity education and awareness should no longer be the primary responsibility of IT experts alone, but of all campus stakeholders. This situation directly coincides with the thesis emphasized by Austin (2020) that the global cybersecurity talent shortage and increasing geopolitical threats force institutions to invest not only in technology but also in "workforce development and new education policies."

On the other hand, the study has opened up for in-depth discussion the structural conflict (paradox) between the principles of "academic freedom" and "open access to information," which are the building blocks of higher education institutions, and the strict requirements of "cybersecurity." Unlike traditional commercial companies or closed government institutions, the cybersecurity architecture and education in universities must have a much more flexible, innovative, and unique nature (Schneider, 2013). The connection of thousands of students and staff to the campus network with their personal and unmanaged devices (BYOD) blurs network boundaries, rendering traditional perimeter security models dysfunctional. The AI-supported Network Access Control (NAC) mechanisms and logical network layering (VLAN, Sandbox isolated networks) proposed by the participants to manage this chaos stand out as the most rational solutions that can protect the main data backbone without restricting the freedom of academic research.

Finally, one of the most critical discussion points of the study is the necessity that cybersecurity within the institution should not remain merely a written regulation or a legal compliance document (such as KVKK/GDPR consent texts), but instead be transformed into a living "cybersecurity culture." The gamification-supported training, interactive phishing simulations, and reward mechanisms suggested by the participants aim to ensure that employees and students participate in security processes not as passive spectators but as active defenders. Such applied and innovative awareness strategies are perfectly aligned with the fundamental framework provided by the National Initiative for Cybersecurity Education (NICE, 2012) to plan the cybersecurity workforce and integrate best practices into corporate culture. Furthermore, the necessity of disaster recovery and business continuity scenarios to prevent the interruption of education and examination processes in the event of a potential destructive cyberattack (e.g., DDoS or ransomware) integrates with macro-level national policy recommendations (NIAC, 2009) aimed at increasing the resilience of critical infrastructures. In conclusion, cyber resilience in higher education institutions will only be possible by integrating legal requirements, technical architecture, and human-centric education models under a single, unified corporate policy.

## 5. CONCLUSION

With the acceleration of digital transformation, higher education institutions have become one of the primary targets of cyber threats due to the critical academic data, extensive personal information pools, and

massive network infrastructures they host. This research has clearly demonstrated that the innovative, transparent, and "open access to information" culture that forms the foundation of universities cannot be managed with rigid and restrictive traditional cybersecurity paradigms. The findings prove that current cybersecurity processes have evolved beyond being merely a hardware-based defense line into a complex socio-technical ecosystem that integrates human behaviors, administrative policies, and technological infrastructure.

One of the most striking results of the study is the determination that the greatest threat to corporate information security is the "human factor" and "user unawareness" rather than technical infrastructure inadequacy. In particular, the connection of thousands of students and staff to the campus network with their personal and unmanaged devices (BYOD) eliminates the logical boundaries of the network and increases corporate vulnerabilities. In this context, to establish the delicate balance between academic freedom and cybersecurity, it was concluded that network traffic must be securely managed through AI-supported network access control (NAC) systems and isolated logical network layers (VLAN, Sandbox), rather than restricting information.

Consequently, the holistic "Cybersecurity in Education Model" proposed specifically for the dynamic structure of higher education institutions aims to remove cybersecurity from being solely the responsibility of an IT department. For institutions to gain cyber resilience, it is imperative that legal requirements (e.g., KVKK/GDPR) are transparently integrated into the technical architecture, and that business continuity and disaster recovery scenarios against potential destructive attacks are included in corporate policies. Beyond all these structural steps, to ensure that security rules do not remain solely on paper, a sustainable "cybersecurity culture" supported by proactive methods such as gamification, applied training, and interactive phishing simulations must be built. Only in this way can higher education institutions protect their existential integrity and safely sustain their academic knowledge production processes against the sophisticated threats of the modern age.

## 6. RECOMMENDATION AND FUTURE DIRECTIONS

Based on the findings of this research and the developed "Cybersecurity in Education Model," the fundamental recommendations for decision-makers, IT managers in higher education institutions, and future researchers in this field are presented below.

### *6.1. Corporate and Technical Recommendations*

- Policy Integration and Governance: Cybersecurity in universities must cease to be merely a technical sub-branch left to the initiative of IT Departments; a centralized "Corporate Cybersecurity Governance Committee" should be established with the participation of all stakeholders, such as the Rectorate, Strategy Development, Legal Counsel, and Student Affairs. This committee must place legal obligations, such as the Personal Data Protection Law (KVKK/GDPR), at the center of the processes.
- Bring Your Own Device (BYOD) Management and Network Segmentation: Artificial Intelligence-supported Network Access Control (NAC) systems must be implemented immediately to protect the campus network without restricting academic freedom. The network hierarchy must be physically or logically (VLAN) segmented into layers; the networks used by students, academic

researchers (Sandbox networks), and administrative staff must be isolated from each other to prevent lateral movement risks.

- Proactive Training and Culture Building: Instead of standard and tedious legal consent texts, cybersecurity training should be redesigned using "gamification" techniques. Periodic, unannounced "phishing simulations" must be organized for institution staff and students, and instant, interactive micro-trainings must be assigned to users who exhibit vulnerabilities. Furthermore, academic or administrative reward mechanisms should be developed for stakeholders who comply with cybersecurity rules.
- Business Continuity and Disaster Recovery: To prevent the collapse of exam and course registration systems during a potential ransomware or DDoS attack, geographically backed-up server architectures and cloud-based disaster recovery scenarios must be integrated into the institution's emergency action plans.

### *6.2. Future Directions*

This research is a qualitative case study conducted with a specific study group. Future research testing the three-dimensional model (technical, administrative, and human) proposed in this study across broader populations will significantly contribute to the literature. Accordingly:

- It is recommended that the developed model be supported by comparative quantitative (survey-based) research by applying it in public and foundation universities of different scales.
- Longitudinal studies can be conducted to measure the impact of gamification-supported cybersecurity training on students' long-term security reflexes.
- Finally, there is a need for specific research to examine the effects of next-generation, personalized social engineering attacks generated by Generative AI tools targeting higher education institutions.

**REFERENCES**

Alvarez-Valdes, R., Belenguer, J. M., Benavent, E., Bermudez, J. D., Muñoz, F., Vercher, E., & Verdejo, F. (2016). Optimizing the level of service quality of a bike-sharing system. *Omega, 62,* 163–175. https://econpapers.repec.org/scripts/redir.pf?u=https%3A%2F%2Fdoi.org%2F10.1016%252Fj.omega.2015.09.007;h=repec:eee:jomega:v:62:y:2016:i:c:p:163-175

Austin, G. (2018). Cybersecurity in China: The next wave. Springer.

CERT. (2020). Continuous diagnostics and mitigation (CDM). Retrieved from https://www.us-cert.gov/cdm/home

Li, W., & Zhu, H. (2021, June). Research on comprehensive enterprise network security. In 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC) (pp. 1–6). IEEE. https://doi.org/10.1109/ICEIEC51955.2021.9463823

National Infrastructure Advisory Council (NIAC). (2009). Critical infrastructure resilience final report and recommendations. Department of Homeland Security.

National Initiative for Cybersecurity Education (NICE). (2012). Best practices for planning a cybersecurity workforce (White Paper Version 2.0). Department of Homeland Security, Cybersecurity Education Office.

Yaman, S., & Yaman, E. (2026). Corporate policy integration for cybersecurity in education: A model structure for higher education institutions. *World Journal on Educational Technology: Current Issues, 18*(1), 76-87. https://doi.org/10.18844/wjet.v18i1.9980

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy, 11*(4), 3–4. https://doi.org/10.1109/MSP.2013.84

Scott-Hayward, S., Natarajan, S., & Sezer, S. (2015). A survey of security in software defined networks. IEEE Communications Surveys & Tutorials, 18(1), 623–654. https://doi.org/10.1109/COMST.2015.2453114

Selvaraj, C., & Anand, S. (2012). A survey on security issues of reputation management systems for peer-to-peer networks. *Computer Science Review, 6*(4), 145–160. https://doi.org/10.1016/j.cosrev.2012.04.001

Singh, B., & Goel, R. (2019). MCMC estimation of multi-component load-sharing system model and its application. *Iranian Journal of Science and Technology, Transactions A: Science, 43*(2), 567–577. https://doi.org/10.1007/s40995-018-0527-7

Thakur, K. (2016). Literature review – Cyber dependency at a domestic and international levels (Cyber Discussion Paper, No. 2). University of New South Wales, Canberra.

von Solms, S., & Futcher, L. (2018). Identifying the cybersecurity body of knowledge for a postgraduate module in systems engineering. In L. Drevin & M. Theocharidou (Eds.), Information security education – Towards a cybersecure society (pp. 133–145). Springer.

Wallach, H. (2002). Efficient training of conditional random fields (Doctoral dissertation, University of Edinburgh).