University Cybersecurity Policies in Türkiye: A Managerial Feasibility Assessment

Abstract

This inquiry gauges the workability of university cybersecurity policies in Türkiye from an administrative standpoint. To achieve this, an extensive document review and policy analysis was conducted, scrutinizing national cybersecurity strategy documents, higher education statutes, and the specific information security policies, guidelines, and strategic plans of selected institutions. The study's sample comprises public and foundation universities, chosen to reflect a diversity of geographical locations and institutional magnitudes. Data extracted from these documents underwent a thematic analysis, being subsequently appraised against the dimensions of governance structures, organizational roles, human resource capacity, budgetary and technical infrastructure, risk management, and awareness. A fundamental disconnect is apparent. The findings show that while a general cybersecurity framework is established in university policies and regulations, its practical execution suffers from substantial deficiencies. Specifically, anemic commitment from top management, weak institutional coordination, the circumscribed employment of specialized personnel, and the absence of sustainable awareness programs emerge as conspicuous problems. The research posits that cybersecurity in academia cannot be viewed as a purely technical domain; it must be treated as an intrinsic component of institutional governance. Consequently, managerial capacity requires significant reinforcement, a greater congruence between stated policies and day-to-day practices must be achieved, and institutional structures need to be reconfigured for closer harmony with national cybersecurity strategies.

Keywords: Computer Security; Universities; Policy Making

Introduction

Higher education is now digital. The swift evolution of information and communication technologies has inexorably migrated the educational, research, and administrative processes of higher learning institutions into networked environments, where student affairs, academic personnel procedures, financial transactions, research initiatives, distance learning platforms, library services, and official correspondence are increasingly managed via online systems. This transformation creates immense opportunities. It also, however, fundamentally alters the character and severity of threats present in cyberspace, making universities a prime target for cyber-attacks. The obligation to protect personal data, intellectual property, confidential research findings, and the continuity of institutional standing elevates the strategic weight of cybersecurity policies within these academic settings.

The architecture of a university possesses unique attributes when compared to conventional state bodies or private-sector firms. Cybersecurity management is rendered exceedingly complicated by a confluence of factors: open campus designs, a deeply heterogeneous user base, numerous stakeholders sharing common networks, a prevailing culture of open information access rooted in academic freedom, and the simultaneous operation of diverse software and hardware across the same infrastructure. Students, faculty, administrators, visiting scholars, and even outside parties engage with the university's information architecture under varied authorization levels. This condition escalates both user-originated risks and the necessity for robust administrative control systems.

In recent years, consonant with nationwide digitalization policies and e-government applications in Türkiye, a considerable body of national strategy documents, action plans, and regulatory instruments has been formulated for the sphere of information security and cybersecurity in public entities. National strategies exist. These documents articulate a spectrum of objectives and protective measures aimed at critical infrastructures, public organizations, and the education sector, while concurrent data protection legislation stipulates precise obligations related to information security. However, how these policies and goals

How directives formulated at the national level are translated into concrete university practices is a central question. The manner in which they are mirrored in institutional structures and the specific impediments encountered during implementation represent issues that demand detailed examination from a management viewpoint.

In many universities in Türkiye, cybersecurity is often misconstrued. It is frequently perceived as an affair associated principally with the technical activities of information technology units, which causes significant difficulties in approaching it as a comprehensive management domain that should be seamlessly integrated with governance, strategic planning, risk management, and institutional decision-making processes. The successful preparation, approval, updating, and internalization of institutional information security policies by all stakeholders is an endeavor that calls for not just technical knowledge and skills but also a potent mixture of institutional leadership, organizational coordination, dedicated resource allocation, and robust monitoring–evaluation mechanisms. Consequently, the practicability of cybersecurity policies extends well beyond being a simple matter of technological infrastructure or product selection, becoming profoundly interconnected with an institution’s managerial capacity and its prevailing culture.

From a managerial point of view, multiple factors determine policy workability. The significance accorded to the issue by top management, the incorporation of a cybersecurity perspective within decision-making mechanisms, the lucidity of roles and responsibilities, the qualitative and quantitative sufficiency of human resources, available budgetary opportunities, the function of internal audit and reporting processes, coordination among different parties, and overall cybersecurity awareness are all determinative components. Policies on paper are not enough. The degree to which these policies are woven into institutional functioning, the ways they are interpreted and put into action by relevant units, and the efficacy of audit and feedback loops are absolutely essential for comprehending the disparities between policy and practice.

Many efforts have been made in Turkish universities. Despite the implementation of various projects, training programs, and technical measures in the cybersecurity sphere, studies concentrating on the managerial dimension of these initiatives remain conspicuously limited. There exists a particular requirement for systematic and comparative analyses concerning the substance of policy documents, institutional organizational configurations, the division of responsibilities, alignment with strategic plans, and the linkage with national strategies. For this reason, assessing the feasibility of cybersecurity policies in universities from a managerial perspective is a significant undertaking for revealing the current situation, identifying inherent strengths and weaknesses, and indicating areas that necessitate improvement.

This study will evaluate policy feasibility. It aims to appraise the practicability of cybersecurity policies in universities in Türkiye using a managerial framework predicated on document review and policy analysis. National strategy documents and legislation, concurrently with the information security policies, cognate regulations, and strategic documents of selected universities, will be meticulously scrutinized to produce findings about governance structures, organizational roles, human resources, budget, technical infrastructure, risk management, and awareness dimensions. By this method, the investigation will move past the mere confirmation of cybersecurity policies in universities to instead debate their operational viability and the primary managerial challenges met in practice, culminating in the development of recommendations for the field.

Literature Review

In the post-COVID-19 era, academic interest has surged. Cybersecurity and information security in higher education have attracted escalating scholarly attention, a phenomenon that has occurred particularly as universities have quickened their digital transformation across teaching, research, and administration. Recent review and rapid-review studies establish that higher education institutions (HEIs) are structurally vulnerable.

Open network architectures expose higher education institutions to cyberthreats. Their diverse user populations and decentralised governance arrangements create a unique vulnerability profile; as a consequence, cybersecurity demands consideration not simply as a technical predicament but as a profound institutional risk and a genuine public policy matter (1–3,13).

Cyber incidents targeting HEIs are escalating. Sectoral and national reports confirm a discernible surge in both the recurrence and severity of these attacks. The UK Cyber Security Breaches Survey, for one, offers a stark illustration, revealing that educational bodies report a higher probability of identifying breaches over a year than typical businesses, an environment where ransomware and credential-theft events have proliferated alarmingly in recent times (3,12). Similar patterns are materializing in other jurisdictions. Indeed, universities there confront amplified threats to personal data, proprietary research findings, and their foundational reputations, which firmly establishes the higher education sector as an integral element within national cybersecurity ecosystems (1,2,18,19).

The academic focus remains narrow. Investigations concentrating on HEIs suggest that cybersecurity scholarship is often confined to a technology-first perspective, affording comparatively scant consideration to the interlocking dimensions of governance, overarching strategy, and the formulation of policy (2,10,13). Effective policy execution depends on many factors. Institutional-level strategic documents consistently affirm that the successful enactment of cybersecurity policies is contingent upon unwavering top-management dedication, streamlined internal coordination, unambiguous delineation of roles and duties, judicious resource distribution, and the sustainment of ongoing training and awareness initiatives (2,5,6,9,13,21).

Technical defences alone are insufficient. Recent scholarly work makes it plain that cybersecurity within HEIs cannot be exclusively circumscribed by technical defence mechanisms; instead, it must be buttressed by solid governance structures, rigorous maturity evaluations, and thoughtful policy architecture. Research constructing maturity models for universities, which are predicated on standards like ISO/IEC 27001 and ISO/IEC 27014, puts forward a systematic appraisal of information security controls, the incorporation of risk-based methodologies, and the formulation of improvement roadmaps synchronized with institutional development stages (8,9,11,16). A careful equilibrium is required. University-centric cybersecurity frameworks emerging from various national settings also direct attention toward the risk appraisal of academic information systems, the preservation of essential operational continuity, and the complex challenge of reconciling academic liberty with stringent security imperatives (4,7,9,16,21).

The human factor is pivotal. More recent inquiries into this element within HEIs reveal that the cybersecurity cognizance of students and personnel forms an indispensable defensive stratum against the pervasive threats of credential theft, phishing campaigns, and social-engineering subterfuge. Both narrative and empirical scholarship contends that sustained, institutionalized training and awareness initiatives—those engineered to fundamentally remold organizational culture instead of merely offering sporadic seminars—correlate with diminished incident frequencies and mitigated breach expenditures, whereas institutions devoid of such systematic programs continue to be asymmetrically vulnerable (4,5,14,19).

The situation in Türkiye is complex. Regarding the Turkish setting, recent evaluations of national cybersecurity strategies suggest that Türkiye's strategic papers correspond generally with international good practice in their breadth and aims, but concurrently expose deficiencies requiring attention in organizational configurations, the demarcation of duties, and the articulation of sector-specific functions (10,11,17). Capabilities are uneven. Examinations of Türkiye's national cybersecurity maturity, conducted with ENISA's National Capabilities Assessment Framework, show potent capacities in multiple domains while simultaneously pinpointing vulnerabilities in supply-chain security, emergency preparedness, and particular aspects of governance (11). A research gap persists. Nevertheless, a conspicuous void exists in systematic, comparative scholarship that rigorously links the responsibilities allocated to HEIs in national strategic plans with the real-world managerial and technical competencies of these universities, a connection established only through meticulous examination of institutional policies and documents (10,17).

A singular focus fails. The collective body of literature persuasively argues that confronting the cybersecurity challenge in universities exclusively through the application of technical controls, rigid adherence to standards, or isolated user awareness campaigns is an altogether inadequate strategy. On the contrary, national

Strategies, institutional governance structures, maturity levels, human resources, and budgeting are all interlinked. They must be considered as mutually reliant management dimensions, and this study consequently offers a contribution to this nascent field by appraising the workability of cybersecurity policies in Turkish universities through a document- and policy-analysis methodology predicated on a managerial framework.

Methodology

Research Design

The research design is qualitative. Its entire analytical foundation rests exclusively upon national policy and strategy papers alongside official university documentation, an approach focused on the managerial viability of cybersecurity directives within Türkiye's higher education institutions, which by its nature obviates any requirement for ethics committee dispensation since no human subjects were involved.

Data Sources

Two principal categories of documentation form the evidentiary basis for this inquiry:

1. National-level documents
   - National cybersecurity strategy and action plans,
   - Core legislation and guidance documents on personal data protection,
   - Regulations and decisions related to information security and cybersecurity in higher education,
   - Strategy documents, guidelines and reports published by relevant public bodies.
2. University-level documents
   - Information security / cybersecurity policies,
   - Personal data protection notices and commitments,
   - Relevant regulations, procedures and instructions,
   - Institutional strategic plans,
   - Internal control and risk management documents.

Purposeful sampling defined the sample. Ultimately, twenty universities were selected for inclusion, a cohort carefully constructed to represent a spectrum of geographical areas, a mix of public and foundation ownership, and a range of institutional scales measured by student population and programmatic breadth, all contingent upon the public availability of their information security documents. To maintain the integrity of the blind peer review process, the universities are coded as U1–U20 in the analysis.

Data Collection

We sourced documents from official websites. This process involved first pinpointing and retrieving all currently operative national-level documents from the online portals of pertinent ministries and regulatory bodies, followed by a methodical survey of the selected universities' websites to gather institutional records, concentrating specifically on the webpages for IT departments, distance education centers, strategic planning offices, and rectorates. All materials were archived digitally. They were then categorized by their year of publication, the nature of the institution (public or foundation), the document class (such as policy, regulation, or strategic plan), and their overall purview.

Data Analysis

Content and thematic analysis were employed. The analysis proceeded through the following stages:

* All documents were read multiple times to achieve a comprehensive familiarity,
* Open codes were generated for passages pertaining to the dimensions of governance, organisational structure, human resources, budget and infrastructure, risk management and awareness,
* Similar codes were aggregated into sub-themes and overarching themes,
* National-level and university-level documents were compared across themes to discern convergences, lacunae, and disparities, including dissimilarities between public and foundation universities and between institutions of different scales.

The entire analytical process was iterative. This meant that codes and themes underwent continual review and refinement as the examination of the documents proceeded, ensuring a more robust final interpretation.

Ethical Considerations and Limitations

The study used only public documents. All institutional names were anonymized with codes in the final report. A primary constraint of this work is its exclusive reliance on documentary evidence, which necessarily omits the perspectives that might have been gathered from interviews or focus groups with university administrators and personnel, although this specific design was chosen deliberately to permit a methodical and comparative examination of policy language and organizational frameworks.

FINDINGS

This investigation appraised information security and cybersecurity policies, along with internal statutes,

The study interrogated strategic plans and internal control and risk management documents from Türkiye's public and foundation universities, appraising the administrative viability of their cybersecurity postures. Findings are organized thematically across several domains, encompassing governance and organisational structure, policy substance and breadth, human resources and capabilities, fiscal and technical infrastructure, risk mitigation and incident reaction, consciousness-raising and training initiatives, and conformity with national strategies and legal mandates.

Governance and Organisational Structure

Universities broadly regard cybersecurity as an institutional priority. Policies frequently articulate that the defense of information assets is foundational for maintaining the continuity of educational, research, and administrative workflows, a position exemplified by Istanbul University-Cerrahpaşa's policy which not only connects security to institutional reputation but also confirms its senate backing and promises procedural action against any infringements. Ankara University's policy is built on TS EN ISO 27001. It delegates information security management to the IT department and related coordinating bodies, assigning a pivotal function to risk management and the rigorous, ongoing observation of process efficacy to ensure consistent operational standards.

Certain institutions formalize their approach. They explicitly mandate the creation of information security commissions or management system teams, which are then charged with duties ranging from policy formulation and implementation oversight to direct reporting to senior leadership. The policies from Ankara Medipol University and Istanbul Medipol University detail a particularly clear governance model where the rectorate maintains final authority, yet the IT department, an information security commission, and a security manager jointly supervise processes and advance perpetual refinement. This collaborative structure is far from universal. Indeed, in many other cases, the function of senior management is circumscribed to simple ratification and generalized backing, failing to describe in any substantive detail their obligations for strategic guidance, accountability, and horizontal cybersecurity coordination. What emerges is a picture of governance systems that, while established, are frequently skewed toward IT-centric, technical concerns, betraying a significant variance in institutional maturity.

Policy Content and Scope

The core principles are confidentiality, integrity, and availability. Most university policy documents construct their information security architecture upon this foundation, with institutions such as Istanbul Bilgi University and Bursa Uludağ University defining their primary aim as the safeguarding of all informational assets, services, and procedures from internal and external menaces and concurrently affirming that compliance with legislation and pertinent standards is a non-negotiable part of this mission.

Policy specificity differs greatly. Some university documents contain unambiguous operational stipulations covering the definition and cataloging of information assets, authorization for access based on roles and duties, password intricacy and replacement schedules, backup and disaster recovery protocols, log administration, network partitioning, and the application of cloud services, an approach exemplified by Bursa Uludağ University's policy, which formally declares its establishment of a TS ISO/IEC 27001-compliant management system, its commitment to periodic reviews, and its adherence to continuous improvement as a foundational tenet.

Other policies remain vague. These documents often depend on sweeping declarations, such as asserting that "necessary technical and administrative measures shall be taken" or that "relevant legislation shall be complied with," yet they conspicuously omit the granular procedures required for actual execution. The frequency of policy review also appears inconsistent.

The units tasked with updates are not consistently defined. While certain institutions assert that their policy will be reassessed at least once a year or following statutory changes, a significant portion provides only an effective date, offering no description whatsoever of the requisite monitoring or revision mechanisms. This practice is deeply concerning. In a rapidly evolving threat environment, it raises serious questions regarding the durable alignment of policy with practice.

Human Resources and Competencies

Cybersecurity responsibility rests with IT. The evidence shows a strong concentration of accountability within information technology departments, where technical staff are typically assigned the full spectrum of duties from network security and server administration to user account management and backup operations. Some institutions formalize these roles. For instance, policies at Ankara Medipol University and Istanbul Medipol University delineate the information security manager's remit, which encompasses tracking security objectives, formulating improvement suggestions, and assessing internal audit findings. Nevertheless, a widespread issue across numerous institutions is the failure to distinctly segregate strategic, administrative, and educational duties from purely technical functions, a problem compounded by policy texts that give only superficial consideration to user behavior and the broader organizational culture.

Investigations into the elements shaping IT risk management outcomes consistently demonstrate that the effectiveness of information security processes is profoundly dependent on executive-level backing, comprehensive user education, a supportive organisational ethos, and attention to human elements. Without these, risk management falters. Corroborating this, scholarship examining cybersecurity consciousness among university employees in Türkiye reveals that comprehension is not uniform, instead showing marked variations between academic and administrative staff that correlate with their specific roles and professional backgrounds. These results compel a broader approach; human resource and competency planning must therefore expand its scope far beyond just the technical teams to encompass and properly engage every single user group within the university.

Budget and Technical Infrastructure

IT investment is broadly defined. Institutional strategic plans and internal control papers usually conceptualize information technology expenditures through the lens of network hardware, server and storage capacity, end-user devices, and various software licenses. Cybersecurity budgets are often unmentioned. Interestingly, those universities possessing ISO 27001 certification which have also made public their implementation of an information security management system are more inclined to specify investments in firewalls, intrusion detection systems, robust backup architectures, disaster recovery facilities, and endpoint security, explicitly connecting these expenditures to their wider institutional ambitions for digital transformation.

Technical policies vary in detail. A select group of institutions meticulously articulates specifics such as network segmentation strategies, wireless access protocols, conditions for VPN and remote connections, defined log retention schedules, stipulations for cloud service engagement, and precise security prerequisites for agreements with external suppliers. Others remain vague. This observable disparity in documentation implies that the sophistication of a university's cybersecurity framework is contingent upon its unique institutional capabilities and declared strategic imperatives.

Risk Management and Incident Response

Some universities have risk frameworks. The analysis demonstrates that these institutions have instituted formal structures for managing information security risks, characteristically incorporating goals such as the systematic identification and appraisal of such risks, the diminution of their effects on operational continuity, and the assurance of conformity with legal and contractual requirements. Certain policies stipulate that risk assessment activities will be performed at regular intervals, and that determinations of risk appetite and

Acceptance thresholds are to be established. Concurrently, technical and administrative controls will be enacted to mitigate discovered risks. Incident response protocols also demonstrate considerable institutional variance. Numerous universities stipulate procedures that encompass incident classification, designated reporting conduits, responsible teams, and the precise steps for documenting and communicating such events. The policy of Istanbul University-Cerrahpaşa, for instance, expressly declares that information security incidents are subject to monitoring and that sanctions will be levied where appropriate. In sharp contrast, incident management at other institutions is often confined to broad pronouncements that the relevant unit will take necessary actions, lacking granular specifications for post-incident root-cause analysis, corrective measures, or functional coordination with national incident response frameworks.

Evaluations of Türkiye’s national cybersecurity strategies show notable advancements. While substantial progress in legal and organizational arrangements has been recorded, persistent obstacles endure concerning implementation, the allocation of resources, technical proficiency, and inter-agency coordination. The deficiencies identified in risk management and incident response processes at the university level can be plausibly interpreted as symptomatic reflections of these more extensive systemic issues playing out within the higher education domain.

Awareness and Training Activities

Most policies accentuate awareness and training. They are foundational elements of information security. Universities consequently pledge to apprise their constituencies of pertinent legislation, industry standards, and internal protocols, while also disseminating regulations for appropriate conduct and actively soliciting the reporting of suspicious emails, malicious software, and social engineering attacks. A case in point is the policy of Istanbul Bilgi University, which affirms that the institution is committed to furnishing requisite training and resources on information security and that internal audits, combined with management review meetings, will be employed to bolster the perpetual refinement of the system.

The documents, however, exhibit inconsistency in stipulating whether training activities are compulsory, the frequency of their delivery, the degree to which they are customized for distinct cohorts, and the methods by which their efficacy is ascertained. Empirical inquiries into digital data protection and personal cybersecurity consciousness among university staff in Türkiye reveal that a median level of awareness prevails, although pronounced variations exist contingent upon an individual's role, age, professional experience, and educational attainment. These determinations point to an urgent need to transmute general policy pronouncements on training into focused, quantifiable, and enduring initiatives.

Alignment with National Strategies and Legislation

Adherence to Law No. 6698 is a guiding tenet. University policies and regulations frequently posit compliance with this statute on the Protection of Personal Data and its associated secondary legislation as a core principle. Indeed, a great many institutions expressly declare that personal data processing activities are obliged to align with national data protection law, higher education statutes, and other germane regulations. The ambit of university information security policies exhibits a general congruence with the components articulated in Türkiye's national cybersecurity strategies, which include confidentiality, integrity, availability, operational continuity, the safeguarding of critical infrastructures, and national and international cooperation.

Concurrently, a disconnect persists. Studies examining the historical evolution and substance of Türkiye's cybersecurity strategies demonstrate that while these frameworks are substantially harmonious with international best practice regarding their scope and objectives, formidable implementation and coordination impediments endure. Disparities in the timeliness of policies, divergent approaches to risk management and incident response at the university level, and the inclusion of references to antiquated national strategy documents in some institutional regulations, all suggest that the congruence between national cybersecurity policies and higher education institutions remains irregular and necessitates considerable reinforcement.

DISCUSSION

The evidence from this inquiry is clear. It demonstrates that information security and cybersecurity policies in

While Turkish universities formally define their cybersecurity posture through official documentation, the managerial workability and sophistication of these frameworks exhibit a profound variance across institutions. A critical examination of these policies against the backdrop of national cybersecurity strategies and established international practices makes manifest conspicuous deficiencies, especially concerning governance frameworks, execution pathways, personnel, and risk mitigation.

In the realm of governance and organizational design, information security is overwhelmingly perceived as a technical problem. IT departments and ISMS teams are central to policy formulation and execution, while the rectorate and senior leadership's involvement is frequently circumscribed by mere approval and nominal backing. This approach is misaligned with the broader scholarly consensus on information security governance, which contends that genuine effectiveness is contingent upon its deep integration with enterprise-wide risk management and strategic planning, buttressed by assertive leadership and unambiguous ownership from the highest echelons of management. From this vantage point, current structures in Turkish universities attest to some technical progress, but managerial ownership and complete institutional integration are still lacking.

Policy content is inconsistent. While a majority of institutions formally subscribe to the foundational tenets of confidentiality, integrity, and availability—positioning information asset protection as a primary goal—the granularity of their operational directives within policy documents diverges dramatically. Certain institutions have articulated meticulous policies and procedures furnishing explicit direction for asset inventories, access controls, password protocols, backup and disaster recovery plans, log administration, and cloud computing, thus attaining a greater congruence with international benchmarks; conversely, others address these domains with only sweeping generalities, blurring the lines between policy and procedure and failing to delineate responsibilities with sufficient clarity. Such dissimilarity severely hobbles the practical application of policies and impedes the pursuit of a uniform security standard.

The human resources dimension presents a familiar pattern. Cybersecurity duties are principally consolidated within IT departments, and despite a reasonably sophisticated technical capability, the pivotal elements of organizational culture and user conduct in relation to information security are afforded scant consideration in policy. Empirical inquiries into cybersecurity consciousness among Turkish university personnel confirm that comprehension levels fluctuate according to an individual's professional function, age, tenure, and educational background, necessitating bespoke, recurrent, and quantifiable training regimens to mitigate these variances. Our analysis shows that such programs are frequently referenced only superficially in institutional texts. They lack clear specification of scope, frequency, or evaluation criteria. This omission constitutes a profound shortcoming in the administration of human-factor vulnerabilities.

Regarding fiscal and technical frameworks, a subset of universities has attained a commendable degree of sophistication, evidenced by ISO 27001 certifications, substantial capital injections into network and endpoint defenses, and the institution of robust disaster recovery mechanisms. However, dedicated funding is rare. The prevailing practice of subsuming security-related outlays within general IT budgets creates a condition where immediate operational exigencies can easily eclipse forward-thinking, strategic commitments to cybersecurity. This observation resonates with national-level appraisals, which likewise find that although strategic blueprints are ambitious in their aims and breadth, persistent difficulties endure in their actual execution, the allotment of resources, and the cultivation of requisite capabilities.

On the matter of risk management and incident response, certain institutions have instituted

While universities possess frameworks to identify, assess, and monitor information security risks, their incident-handling processes are often less mature. Post-incident analysis and organisational learning seem particularly underdeveloped. National cybersecurity strategies do call for institutional response teams and national-level coordination, yet the specific linkages between university-level procedures and these more expansive national mechanisms are frequently not delineated with clarity inside institutional documents. This ambiguity can seriously impede effective response and subsequent learning when major cyber incidents occur.

The review of awareness and training activities reveals a telling pattern. Policies consistently affirm the necessity of user awareness. However, these declarative commitments frequently fail to manifest as systematic, institution-wide educational programmes. Scholarly work on digital data protection and the personal cybersecurity cognizance of university staff makes it plain that user behaviour fundamentally conditions the attack surface, confirming that policy documents alone are profoundly inadequate for ensuring protection without the scaffolding of continuous instruction, guidance, and periodic reminders. The outcomes of this investigation affirm a chasm between the rhetorical focus on awareness and the tangible architecture and execution of training initiatives.

Concerning congruence with national strategies and legislation, most universities make express mention of the Law No. 6698 on the Protection of Personal Data and associated regulations. Their institutional policies also generally mirror the core objectives of Türkiye’s national cybersecurity strategies. A problem persists, though. Certain policy texts continue to cite obsolete versions of national strategy documents or neglect to fully assimilate recent legislative amendments, which indicates that robust mechanisms for guaranteeing ongoing alignment between national directives and institutional paperwork are not yet wholly refined.

This inquiry's primary constraint is its singular dependence on document analysis. Deeper comprehension of how policies are actually interpreted, put into practice, and experienced could have been achieved through interviews, surveys, or focus groups with university administrators, information technology personnel, and end-users. Notwithstanding this methodological boundary, the research adds to the existing scholarship by concurrently scrutinizing both national-level strategic frameworks and institutional policies, thereby presenting a comprehensive evaluation of the governance, human resource, risk management, and awareness facets of cybersecurity within Turkish higher education.

CONCLUSION AND RECOMMENDATIONS

This investigation has demonstrated that Turkish universities have formally constituted information security and cybersecurity policies. These cover governance, content, human resources, risk management, and awareness. Nevertheless, the degree of managerial viability and maturity exhibits considerable heterogeneity among the institutions. The results suggest a specific condition: while the technical frameworks are present in many universities, there is a clear demand for methodical enhancements in areas ranging from top management proprietorship and the precise demarcation between policies and procedures to risk and incident management, budget appropriation, and the very architecture of training programs.

Therefore, several actions are advisable. Universities should embed information security within their corporate risk management and strategic planning activities; they must also fortify governance structures at the rectorate and senior administrative echelons, enrich policy texts with concrete, implementable particulars, designate dedicated resources and budgets specifically for cybersecurity, and construct mandatory, quantifiable awareness and training programs customized for disparate professional roles. Furthermore, new mechanisms ought to be instituted to make certain that any updates in national cybersecurity strategies and legislation are methodically reflected in institutional documents, and subsequent scholarly inquiry should augment document analysis with qualitative and quantitative methods involving managers, technical staff, and users to probe the nexus between policy and practice with more granular detail.

Acknowledgements

We extend our sincere appreciation to the university officials and the information technology personnel, whose direct support in accessing institutional records and in providing specific elucidations proved foundational to the progression of this inquiry. We are also indebted to our colleagues for their perceptive critiques.