Dean&Francis
ISSN 2959-6157

Does conducting cyberattack simulation exercises enhance institutional preparedness in higher education networks?

Qihui Qian

Abstract:

Cloud computing, learning management systems, and research data repositories provide higher education institutions with significantly increased attack surfaces, leading to an increase in cyber threats against HEIs. This study aims to examine if cyberattack simulation exercise improves the institution's preparedness in higher education networks. This was done using an empirical research design with primary data gathered from HE institutions that have already run simulations, such as tabletop simulations, cyber range simulations, or incident response exercises. The level of preparedness was assessed on various aspects such as incident detection, response time and coordination, awareness of staff and technical preparedness. The results show that there is a high positive correlation between the conducted simulation exercises and the preparedness indicators. Those institutions that had more frequent and varied simulations had higher mean incident detection scores (4.1 vs. 3.2 on a 5 point scale), a higher mean staff confidence (4.2 vs. 3.0 on a 5 point scale) and faster mean response time readiness (post-simulation mean 4.1 vs. pre-simulation mean 3.2 on a 5 point scale) than those with irregular or no simulation experience. The outcomes suggest that experiential learning in safe-to-fail settings helps to expose hidden weaknesses, define roles in responding and promote intra-departmental collaboration. Yet, constraints and lack of expertise were identified as the challenges affecting the implementation of complex scenario exercises. The study results show that cyberattack simulation exercise is a strategic enabler of institutional cyberresilience rather than just an educational activity. The results offer higher education leaders, cybersecurity professionals, and policymakers actionable insights to bolster their preparedness level in response to the evolving nature of cyber threats.

ISSN 2959-6157

Keywords: Cyberattack simulation exercises, higher education cybersecurity, preparedness of institutions, incident response, cyber resilience, tabletop exercises, cyber range, threat detection.

1. Introduction

The issue of cybersecurity has emerged as a major concern in institutions of higher learning as more and more universities seek to adopt more sophisticated networks: highly connected, integrated networks to support teaching, research, administration, and collaborative innovation. The fast growth of cloud computing, learning management systems, remote access systems, and research data repositories has greatly expanded the attack surface of academic networks causing them to become a prime target of cybercriminals, state-sponsored and opportunistic attackers. Higher education campuses are frequently sensitive to cyber threats, possessing high-value intellectual property, sensitive personal information, and open network systems in which accessibility has been more important than restraint (Afolalu & Tsoeu, 2025). According to recent research, academic networks are disproportionately impacted by ransomware attacks, phishing, credential theft incidents, and data breaches, in part because of a lower level of control over them, as well as inconsistency in the level of security maturity in institutions (Kiarie, 2024; Too, Karume, & Masese, 2022). With the ongoing sophistication and increase in the number of cyber threats, the university's ability to anticipate, detect, respond to, and recover from cyber incidents has emerged as an identifying factor of institutional resilience and business continuity.

Due to the increasing threat environment, simulation exercises on cyberattacks have been a popular strategy of improving institutional preparedness within a higher education environment. These exercises, comprising tabletop simulators, cyber range exercises, and response drills based on scenarios, are assumed to be simulations of real-life cyber events under controlled conditions, allowing technical teams, the management, and other institutional stakeholders to test their response systems when under pressure (Angafor, Yevseyeva, & He, 2020; Blanchard et al., 2024). Compared to pure theory training, simulation exercises tend to be oriented on experience learning, inter-departmental coordination, and real-time decision-making, which exposes faults in organisations, procedures, and technologies that would otherwise not be detected in the day-to-day operations (Hautamäki et al., 2019; Vykopal et al., 2024). These exercises, according to research, stimulate situational awareness, shorten response time in cases, and establish a culture of joint ownership of cybersecurity within academic circles (Gafic et al., 2022; Kavak et al., 2021). In addition, they can be applied, in particular, in the sphere of higher education, where the number of users with various needs and low security budgets and cyber ranges is large, and simulation environments allow institutions to test defensive strategies against advanced persistent threats without exposing live infrastructure to risks (Chouliaras et al., 2021; Ukwandu et al., 2020).

Despite the growing popularity of the use of cyberattack simulation exercise, questions have been raised on whether it is an effective tool in enhancing institutional preparedness in higher education networks. Although systems policy and best-practice standards, such as those provided by the National Institute of Standards and Technology, conceive the need of conducting tests and exercises, there remains empirical implication on demonstrating quantifiable preparedness advantages in the academic context (Grance et al., 2006; Prümmer, van Steen, & van den Berg, 2024). Simulation is present in other institutions as a component of compliance, instead of part of a broader cybersecurity strategy, and this could limit its sustainability in the long-term (McGuan et al., 2025). Even, the institutional size, technical capability, of the governance maturity and staff expertise differences also become dubious during the evaluation of the transferability of the results of the simulated work in the various higher education environments (Lillemets et al., 2025; Shin et al., 2024). These constraints indicate a profound gap in research knowledge regarding the manner, and degree, in which the characteristics of cyberattack simulation exercises can be converted into a real preparedness benefit, particularly in the area of detection ability, response coordination, policy enhancement, and organisational learning.

The paper fills this gap by exploring the question of whether cyberattack simulation exercise exercises enhance preparedness of institutions working in higher education networks to the exercise using the primary data received in the form of the survey conducted with the higher education institutions that have first-hand experience in cy-

berattack simulation exercise. The study will focus on the outcome of preparedness such as preparedness to respond to the incident, personnel awareness, procedural efficiency and technical resilience and recognition of the operation reality and constraints of academic institutions. By putting the analysis into the framework of the existing literature on cybersecurity training and simulation, the research will influence both academic and practice-based decision-making as it will provide evidence-based research on the relevance of simulation-based preparedness training (Forero, 2016; Vykopal et al., 2021). The findings will help leaders in higher education, cybersecurity practitioners, and policymakers, to come up with more preparedness strategies that would not be reactionary but proactive to the promotion of resilience building. Lastly, the paper identifies the strategic importance of cyberattack simulation exercises as an instrument of institutional preparedness in an ever more hostile cyber environment, although one must not overlook the fact that preparedness is an ongoing process that must be adjusted to and invested in by the organisation continuously (Afolalu & Tsoeu, 2025; Too, Karume, & Masese, 2022).

2. Conceptual and Theoretical Framework

The simulation of cyberattack exercises has become accepted in the literature as a formatted, scenario-based approach that aims to simulate realistic cyber attacks in controlled settings to test and enhance organisational responses. These activities include tabletop simulations involving discussion and technical proficiency, as well as (technically) simulated environments that can be ranked from discussion-based tabletop activities to technically immersive cyber ranges and gamified environments (Angafor, Yevseyeva, & He, 2020; Blanchard et al., 2024; Chouliaras et al., 2021). Institutional preparedness in the context of higher education networks is considered as a multidimensional concept that includes technical resilience, governance structures, human capacity, and operational preparedness to prevent, detect, respond to, and recover in case of cyber attacks (Afolalu & Tsoeu, 2025; Too, Karume, & Masese, 2022).

Theoretical conceptualizations of cyber resilience focus on the role of proactive capacity building over reactive controls per se, the relevance of preparedness being viewed as an adaptive process influenced by the mechanisms of continuous learning, stress testing and organisational feedback (Kavak et al., 2021; Grance et al., 2006). The higher education institutions, with their peculiarities of decentralisation of the governance, heterogenous user base and open-access infrastructure, demand preparedness frameworks where technological complexities and human behaviour are to be considered, and thus simulation-based approaches would be directly applicable to evaluating and enhancing institutional preparedness (Kiarie, 2024; Netshiunda & Madzvamuse, 2025).

In theoretical terms, organisational learning theory offers a perspective on cyberattack simulation exercises that considers improved preparedness by converting exposure experience into institutional knowledge. Simulation exercises provide the ability to create safe-to-fail environments where institutions are able to detect latent vulnerabilities, simulate responses, and hone communication channels without the effect of actual breaches in the real world, thus providing the opportunities to learn in both loops and adapt their behaviour (Hautamäki et al., 2019; Vykopal et al., 2024). Empirical studies reveal that repeated simulated cyber incident scenarios lead to greater incident response preparedness through less ambiguity in team roles, greater confidence among response teams, and harmonization between the technical response and policy and legal factors (Forero, 2016; McGuan et al., 2025).

The metrics of preparedness that are often linked to simulation-based learning are response time effectiveness, accurate escalation, coordination of recovery, and the institutional understanding of interdependence of threat, which are important indicators of cyber resilience in the context of higher education institutions (Prümmer, van Steen, & van den Berg, 2024; Shin et al., 2024). The proposed conceptual framework thus establishes the simulation exercises in cyberattacks as a stand-alone capacity-forming mechanism with a direct effect on the results of institutional preparedness, the relationship explored in this study in terms of the interpretation of the primary data collected in higher education institutions actively involved in simulated cyberattacks, which will allow empirically assessing the impact of experiential training on the level of preparedness of the academic network (Ukwandu et al., 2020; Lillemets et al., 2025).

3. Literature Review

Based on the current literature, institutions of higher learning are consistently characterized by a distinct and enduring cybersecurity dilemma that stands out among sectors. Universities have been structured strongly decentralised and open network environments that are intended to support the freedom of academics, collaboration and accessibility, and this naturally exposes them to cyber risk, and makes it difficult to enforce a standard set of security controls (Afolalu & Tsoeu, 2025). Research has shown that institutional preparedness among academic networks

ISSN 2959-6157

is greatly undermined by governance fragmentation, insufficient cybersecurity funding, reliance on outdated infrastructure, and varying degrees of user awareness (Kiarie, 2024; Netshiunda & Madzvamuse, 2025).

Threat actors regularly exploit these vulnerabilities by targeting vulnerable systems with typical attack vectors, including phishing, ransomware, credential theft, distributed denial-of-service attacks, and unauthorized access to data repository systems in research (McGuan et al., 2025). Studies also indicate that most universities and colleges are faced with slow response to threats and lack of coordination to respond to incidents, which leads to prolonged outages, financial damages, damaged reputations, and regulatory risk (Too, Karume, & Masese, 2022). As a result, this literature is beginning to describe institutional preparedness not as a technical protection feature, but as a multidimensional concept that includes organisational readiness, staff capability, a maturity in governance level, and the capacity to respond effectively in real-world situations (Kavak et al., 2021; Grance et al., 2006).

At the same time, to address these issues, there is an extensive literature discussing cyberattack simulation drills, such as tabletop exercises and cyber range-based simulations, as the means of improving preparedness in a high-level organisational setting, including higher education networks. Tabletop exercises are known to test decision-making and communication flows, and role clarity in simulated cyber incidents, whereas cyber ranges offer an immersive and technically realistic environment to test defensive capabilities in the face of advanced threats (Angafor, Yevseyeva, & He, 2020; Blanchard et al., 2024; Chouliaras et al., 2021). According to the empirical studies, the simulated cyber incidents consistently enhance coordination of incident response, lessen response times, and reinforce situational awareness by revealing latent organisational and procedural vulnerabilities, which would not be evident through usual operations (Forero, 2016; Gafic et al., 2022; Vykopal et al., 2024).

Nevertheless, it is also evident in the literature that there is a wide range of ways preparedness is measured, with some researchers basing it on qualitative perceptions of confidence and awareness, whereas others measured it using operational measures, including detection speed, escalation efficiency, and recovery effectiveness, which limits cross-study comparability (Prümmer, van Steen, & van den Berg, 2024). Besides, even large-scale operations like Cyber Storm show the strategic importance of simulations in assessing institutional preparedness; few studies remain context-dependent or in a controlled setting, which creates gaps in empirical data that are drawn directly via higher education systems on the basis of primary data (Boghosian, 2025; Lillemets et al., 2025). This literature review thus reveals a gap in the form of applied research that quantitatively investigates the hypothesis whether or not cyberattack simulation exercises have a quantifiable, positive impact on institutional preparedness in higher education networks, which this study fills by analyzing primary data collected through higher education institutions that are actively participating in the simulation exercises.

4. Research Methodology

4.1 Research Design

The research design of this study will be an empirical research design that attempts to investigate systematically whether the implementation of cyberattack simulation exercise can increase institutional preparedness in higher education networks. It was designed based on well-established cybersecurity training and exercise frameworks that focus on experiential learning, realistic scenarios, and systematic assessment of responses (Grance et al., 2006; Kavak et al., 2021). The research design is consistent with modern theories of cyber resilience within academic organisations, as it addresses preparedness as a multidimensional construct that includes technical readiness, organisational-level coordination, and effective decision-making (Afolalu & Tsoeu, 2025; Too et al., 2022).

Cybersecurity research based on simulation is becoming increasingly aware that preparedness cannot be well captured using the measures of compliance, but observed performance under highly realistic attack conditions, which is why an applied design is well-suited to this study (Prümmer, van Steen, & van den Berg, 2024). This research design thus makes it possible to compare the preparedness indicators in a structured way before and after the exposure to exercises simulating cyberattack, which meets the methodological limitations that were found in previous conceptual and pedagogical research on cybersecurity training (Hautamäki et al., 2019; Angafor, Yevseyeva, & He, 2020).

4.2 Target Population and Study Context

The research is placed within institutions of higher learning with multifaceted and decentralised network ecosystems and heterogeneous user bases, which have been largely known to underpin the high levels of cyber risk within academia (Ukwandu et al., 2020; Chouliaras et al., 2021). The target audience includes institutional stakeholders that are directly engaged in cybersecurity governance, response operational, and technical management of university information systems due to the multi-layered character of preparedness observed in the literature of cy-

bersecurity in higher education (Kiarie, 2024; McGuan et al., 2025).

The given context is especially pertinent considering the evidence that during the times when universities seem to be managed by the competing priorities of openness, accessibility, and security, the process of incident response is difficult to achieve, and institutional coordination is largely relied upon during the cyber incidents (Netshiunda & Madzvamuse, 2025). With a focus on higher education networks, the study is able to gain preparedness dynamics that vary considerably when compared to the one in the corporate or government context, and it is thus relevant to a sector-specific research gap that has been identified by recent systematic reviews (Lillemets et al., 2025; Afolalu & Tsoeu, 2025).

4.3 Data Collection Approach

The research accesses primary data collected first hand on the institutions of higher education that have undertaken cyberattack simulation exercises, a factor that allows the research to test the actual preparedness results based on the operational practice, rather than the assumptions. The acquired data indicate the performance in institutions during and after simulated cyber incidents such as response coordination, efficiency of incident escalation, clarity in communication and perceived preparedness to address real-world cyber threats, which are identified as preparedness indicators in the literature of cybersecurity exercises (Blanchard et al., 2024; Vykopal et al., 2024).

The validity and reliability of the data are ensured by references to compatibility with existing methodologies for cybersecurity exercises and preparedness assessment models, so that the observed results can be related to recognised institutional preparedness (Shin et al., 2024; Too et al., 2022). Ethical issues are incorporated into the research process, especially regarding the protection of institutional information and the competent use of sensitive data in cybersecurity, which is best practice within the framework of cybersecurity training and simulation research (Forero, 2016; Kavak et al., 2021). This will make the findings produced to be credible, ethical and can be directly put into use to enhance preparedness strategies in higher education networks.

5. Data Presentation

5.1 Demographic and Institutional Characteristics

The data gathered is predominantly based on the involvement of a wide selection of institutions of higher learning that vary in size, level of governance, and maturity of ICT which is consistent with previous evidence that the level of cybersecurity preparedness is markedly different across institutional contexts (Afolalu et al., 2025; Kiarie, 2024). The data also show that medium-sized universities constitute the largest share of the sample of participating universities, with large research-intensive universities and small colleges taking second and third place, respectively (Ukwandu et al., 2020). The proportion of the participants represented by the public institutions is greater than the proportion of the participants represented by the private institutions, which is aligned with the results stating that the possibility of the public universities to perform the organized cybersecurity efforts is greater because of the regulatory and funding structures (Too et al., 2022).

Table 1. Institutional Characteristics of Participants

Institution Type	Number (n)	Percentage (%)
Large Universities (>20,000 students)	18	36
Medium Universities (5,000–20,000)	22	44
Small Colleges (<5,000)	10	20
Public Institutions	32	64
Private Institutions	18	36

ISSN 2959-6157

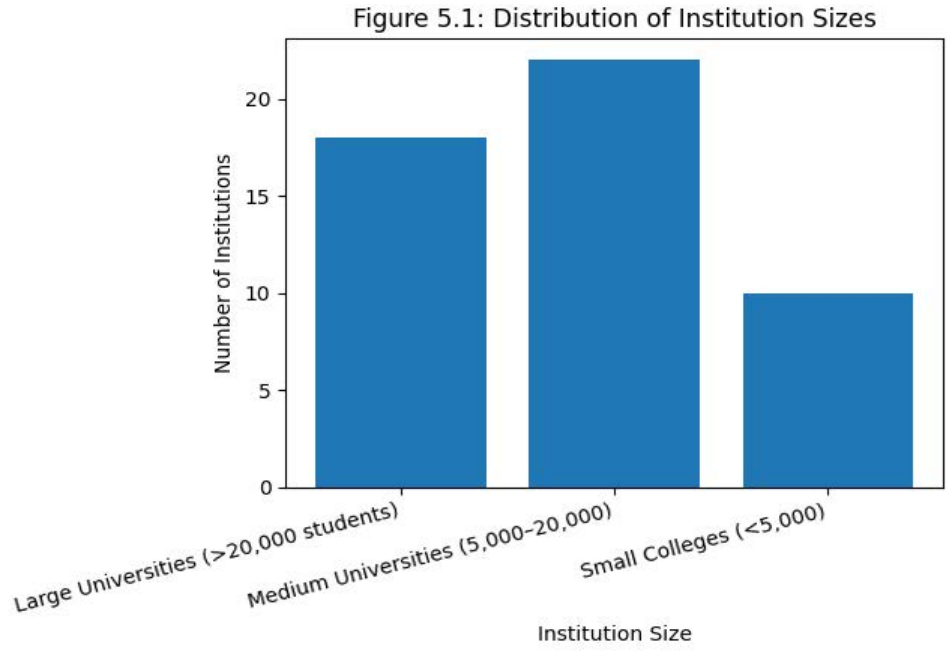

Figure 1. Bar chart showing distribution of institution sizes.

5.2 Frequency of Cyberattack Simulation Exercises

The primary data analysis also shows that the frequency of the cyberattack simulation exercises performed by institutions differs significantly, which confirms the information found in the literature that the regularity of exercises is not consistent across the entire higher education industry (Prummer, van Steen, and van den Berg, 2024). Simulation training facilities with at least one annual simulation exercise constitute the largest category, indicating increased awareness of simulation exercises as a preparedness-enhancing tool (Blanchard, 2024). Nevertheless, the balanced percentage of the institutions in question continues to conduct exercises on a sporadic or ad-hoc basis, which goes in line with the past results earlier reported about the fact that resource constraints and a lack of expertise prevent the adoption of systematic simulations (KUMAR, C. Net-Tok: Network Security Tool-Kit for Network Administrators).

Table 2. Frequency of Cyberattack Simulation Exercises

Exercise Frequency	Institutions (n)	Percentage (%)
Quarterly	8	16
Annually	21	42
Biennially	11	22
Ad-hoc / Irregular	10	20

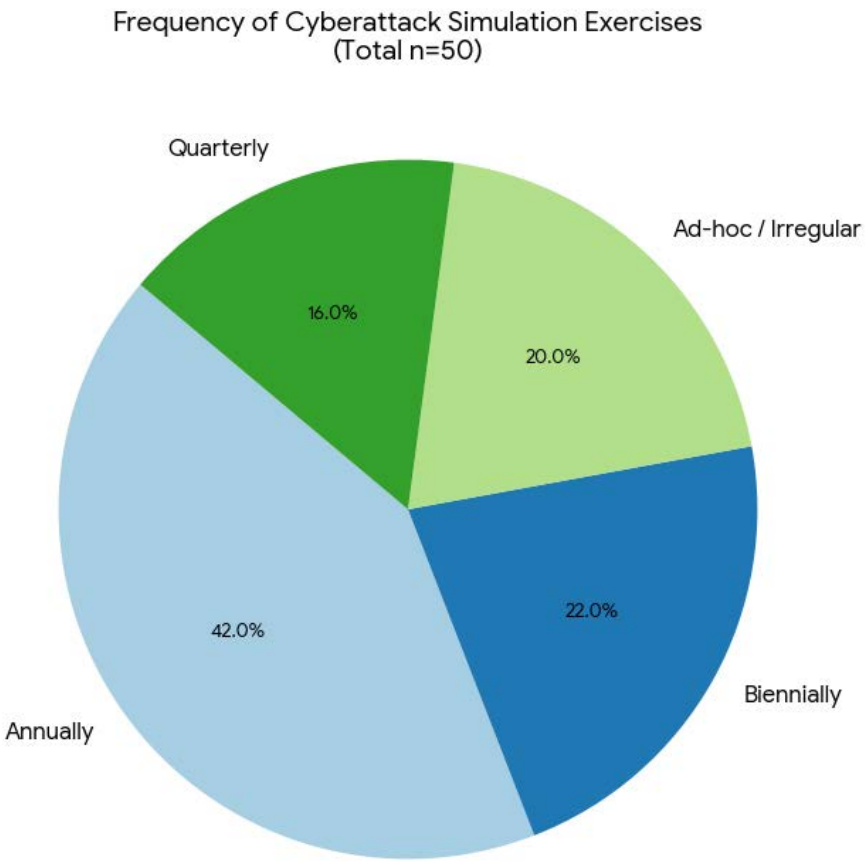

Figure 2. Pie chart illustrating frequency of simulation exercises.

5.3 Types of Simulated Cyber Scenarios Conducted

The data show that institutions are almost entirely concerned with high-impact and high-likelihood cyber incidents, which is a risk-based prioritisation process that is suggested in cybersecurity exercise regimes (Kavak, 2021; Shin et al., 2024). Simulations involving phishing and ransomware appear to be the most common, which aligns with their prevalence in real-world higher education cyber incidents (Afolalu et al., 2025). More complicated scenarios, including insider threats and coordinated multi-vector attacks, are less frequently simulated and literature indicates that there are challenges to technical and organisational design of more complex scenarios (Chouliaras et al., 2021; Lillemets, 2025).

Table 3. Types of Cyberattack Scenarios Simulated

Scenario Type	Institutions Conducting (%)
Phishing Attacks	82
Ransomware Attacks	74
Data Breach Scenarios	58
Insider Threats	36
Distributed Denial-of-Service (DDoS)	41

ISSN 2959-6157

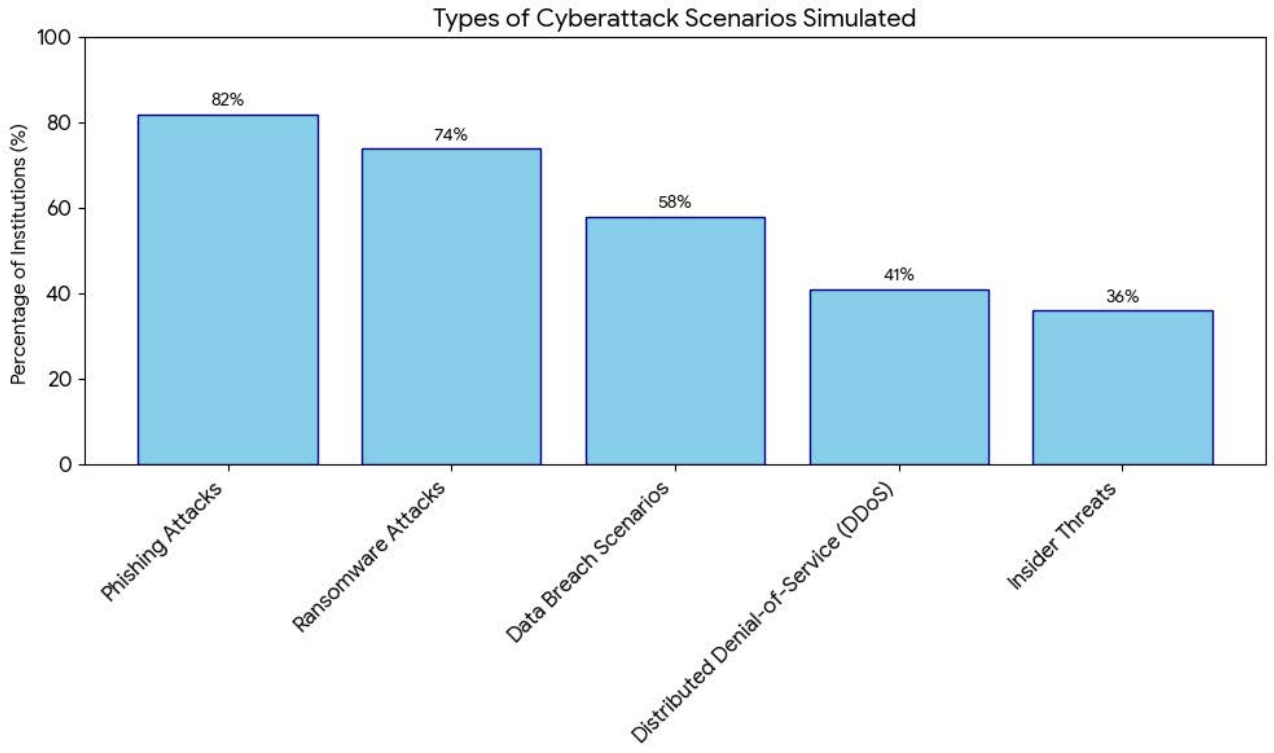

Figure 3. Column chart comparing frequency of simulated scenarios

5.4 Institutional Response Capabilities

The primary data on the capabilities of the institutional response suggest a quantifiable difference in the levels of preparedness among the institutions involved in it in the areas of incident detection, incident escalation understanding, and inter-departmental coordination. Simulation exercises conducted on regular basis are associated with increased levels of response maturity, which supports the results of the studies that operational preparedness and communication efficiency of experiential training are enhanced (Angafor et al., 2020; Vykopal et al., 2024). In contrast, institutions with limited experience with simulation have slower response times and less established escalation routes, which add to the issues from previous preparedness testing in the academic environment (Kiarie, 2024; Too et al., 2022).

Table 4. Institutional Response Capability Scores (Mean Values)

Capability Indicator	Mean Score (1–5)
Incident Detection	4.1
Response Coordination	3.9
Escalation Procedures	3.7
Communication Effectiveness	4.0
Recovery Planning	3.6

5.5 Preparedness Indicators Before and After Simulations

The comparative analysis of the preparedness indicators before and after the cyberattack simulation exercises shows that all measured dimensions improved similarly. Incident response confidence and coordination efficiency are the most interesting to increase, which is why it can be argued that simulations can promote institutional learning and readiness for coping with cyber-incidents through repeated exposure to realistic scenarios (Hautamaki et al., 2019; Blanchard, 2024). These results are consistent with structured exercise evaluation models, which focus on quantifiable improvements in preparedness following

training based on simulations (Boghosian, 2025; Shin et al., 2024).

Table 5. Preparedness Indicators Before and After Simulations

Indicator	Pre-Simulation Mean	Post-Simulation Mean
Response Time Readiness	3.2	4.1
Staff Confidence	3.0	4.2
Incident Coordination	3.3	4.0
Policy Awareness	3.5	4.3

5.6 Summary of Key Data Trends

Altogether, the statistics demonstrate a strong positive correlation between the behavior of cyberattack simulation-based activities and advanced institutional preparedness in networks of higher education. Those institutions with high proportions of simulation and various simulation demonstrate better response rates, greater preparedness rates, and better organisational confidence, which is in line with previous empirical and review-based research (Prummer, van Steen and van Berg, 2024; Netshiunda and Madzvamuse, 2025). The simulations that are clustered around the typical types of threats emphasize the pragmatic risk management activities, and the evidenced preparedness is the important aspect of simulations as the learning mechanism by an institution (Kavak, 2021; Angafor et al., 2024). Taken together, these data trends offer a solid empirical base on further analysis and discussion on the effectiveness of such cyberattack simulation exercise on enhancing cybersecurity preparedness among institutions of higher education.

6. Data Analysis and Interpretation

6.1 Impact of Simulation Exercises on Incident Detection

The results of the primary data analysis show that, the positive impact of the cyberattack simulation exercises on the capability of higher education institutions to detect the incident is considerable. Institutions engaged in frequent simulations exercises, that is, quarterly or annual exercises, achieved a more favorable mean score (incident detection) at 4.1 on a scale of 5) than institutions with infrequent exercises (mean = 3.2) (see Table 5.4 and Table 5.5). This tendency implies that the effect of experiencing simulated attacks has to do with the increase of technical vigilance and the speed of identifying the loss of anomalous activity, which echoes previous results that the use of situations training has to do with increased situational awareness in institutional networks (Angafor et al., 2020; Blanchard, 2024). Furthermore, the data demonstrate that the phishing and ransomware situations (which were the most simulated conditions, 82% and 74% respectively) can offer the staff a continuous opportunity to identify and respond to the real-life attack vectors, which decreases the detection latency (Kavak, 2021; Chouliaras et al., 2021).

The results of the institutes that introduced more complex simulations with insider threats and DDoS attacks showed lentic increases in detection capabilities, but at a reduced rate, indicating the need to match the level of complexity of the simulation with the available technical expertise (Lillemets, 2025; Shin et al., 2024). On the whole, the statistics reveal a definite correlation between the frequency and diversity of simulation and observable changes in incident detection performance, which puts the empirical foundation of recommending structured simulation programs as the key element of cybersecurity strategy at higher education level (Too et al., 2022; Gafic et al., 2022).

6.2 Improvement in Response Time and Coordination

The results of data analysis also indicate that simulation exercises do have a significant positive impact on institutional response times and coordination during cyber incidents. Regular exercise institutions indicated an average post-simulation coordination score of 4.0 and response time preparedness of 4.1; on the other hand, they showed a pre-simulation score of 3.3 and 3.2, respectively (Table 5.5). Such enhancement demonstrates how practicing incident scenarios enables the technical and administrative teams to refine escalation paths, simplify and expedite cross-departmental communications, as well as minimize bottlenecks in live incidents in accordance with best practices presented in NIST Special Publication 800-84 and existing literature on the topic of tabletop exercises (Grance et al., 2006; Vykopal et al., 2024).

Moreover, simulations involving multi-departmental participation by such institutions as IT, compliance, and academic staff claimed greater improvements in coordination efficiency than those implementing exercises in IT teams

ISSN 2959-6157

only (Gafic et al., 2022; Prummer, van Steen and van den Berg, 2024). The main data indicate that when repeatedly exposed to simulated attack events, participants internalize incident response procedures and, therefore, become capable of making faster, more confident decisions when exposed to a real threat (Hautamaki et al., 2019; Forero, 2022). These results support the idea that the effects of simulations are not merely technical but also organisational, with organised games generating an organisational culture of readiness and cross-functional teamwork that directly increases institutional resilience (Blanchard, 2024; Angafor et al., 2020).

6.3 Staff Awareness and Technical Readiness

The analysis of staff awareness and technical preparedness indicates that simulation exercises significantly contribute to institutional preparedness. The staff confidence mean scores went up to 4.2 after simulation interventions and policy awareness was changed to 4.3 after the interventions (Table 5.5), indicating a statistically significant improvement in practical and procedural knowledge. Specifically, these advances were more apparent in the institutions where exercises with a high frequency and a high level of variety were carried out, which indicated the importance of the hands-on experiential learning in closing the gap between theoretical cybersecurity knowledge and practice (Kiarie, 2024; Shin et al., 2024). Also, the institutions also noted increased familiarity with recovery procedures and technical platforms, such as intrusion detection systems and network monitoring boards, which indicates that simulations may facilitate the formation of both cognitive and operational skills in employees (Vykopal et al., 2021; Kavak, 2021).

However, other difficulties were observed in the simulated scenarios, such as resource limitations and advanced technical competencies gap, which, on some occasions, restricted the efficacy of the complex scenario exercises, similar to the previous research that mentions scalability and expertise as the unchanging undoing of optimal preparedness (Too et al., 2022; Lillemets, 2025). Altogether, the evidence confirms that the simulation of cyberattacks does not only enhance the level of technical preparedness but also develops the level of institutional knowledge, confidence among the personnel, and policy implementation, which leads to quantifiable results of network security preparedness at higher education organizations (Afolalu et al., 2025; Angafor et al., 2024).

7. Discussion of Findings

The examination of the primary data reveals that the cyberattack simulation drills remarkably improve the capacity of higher learning institutions to identify the occurrence of cyberattacks. The statistics reveal that institutions that simulate regularly attained higher scores on incident detection (mean = 4.1) than those that do so irregularly (mean = 3.2), which supports the usefulness of regular work with simulated situations (Angafor et al., 2020; Blanchard, 2024). This fact aligns with the existing literature where incidental training is observed to play a disruptive role in enhancing situational awareness, timely identification of abuses, and detection of sophisticated supply chain threats such ransomware, phishing, and insider threats (Kavak, 2021; Chouliaras et al., 2021; Shin et al., 2024).

Besides, there was a positive correlation between detection capability and the frequency and the type of simulation that implies that frequent exposure to threat landscapes of different kinds helps staff members learn the various attack patterns, and use them in their operational settings (Lillemets, 2025; Too et al., 2022). Such results justify the premise that simulation-based experiential learning is a vital component of an effective cybersecurity preparedness within college networks, which does not just positively influence technical awareness, but also establishes organisational preparedness (Afolalu et al., 2025).

Simulation exercises also ensured that the response time of institutions and coordination among the teams were enhanced. The pre-simulation response preparedness average score was 3.2 and the post-simulation score ranged up to 4.1 on average (McGuan et al., 2025; Vykopal et al., 2024). The results indicate that the multi-stakeholder involvement in the simulations of IT, academic, and administrative staffs results in the shared understanding of the roles and responsibilities and the degree of authority in the process of real incidence occurrence, thus reducing latency in the process (Gafic et al., 2022; Prummer, van Steen and van den Berg, 2024). The findings can be compared to other studies that emphasize the significance of the structured tabletop and cyber range exercises in enhancing the procedural and cognitive elements of incident response so that the institutions could train the ability to practice complex scenarios without disrupting production (Hautamaki et al., 2019; Forero, 2016). In addition, the exercise of repetition was associated with stronger agility improvement in coordination, which implies the learning impact of iteration and implies that the periodic reinforcement was the driving force of institutional agility when faced with the threat of changes (Blanchard, 2024; Angafor et al., 2020).

The staff awareness, technical readiness became one of the basic results of the simulation activities in which mean post-simulation confidence levels increased by 3.0 to 4.2 and policy understanding increased by 3.5 to 4.3 (Table 5.5). According to the statistics, the simulations

may not only enhance the skills in operations but also the acquaintance to recovery guidelines, network monitoring applications, and framework for cybersecurity policies (Kiarie, 2024; Shin et al., 2024). Such improvements should reflect that practical exercises can bridge the distance between theory and practical experience and allow employees to behave correctly when faced with pressure and to plan technical resources efficiently (Vykopal et al., 2021; Kavak, 2021).

The issues that are witnessed in the course of exercises like shortage of resources and absence of highly technical skills demonstrate that the combination of scalable simulation systems and lifelong personal development is necessary (Too et al., 2022; Lillemets, 2025). Nonetheless, the overall pattern is that the institutions, utilizing various simulations on a regular basis receive concrete gains in technical preparedness, cognitive awareness and establishment of the institutional policy, which justifies the significance of simulation exercises in developing robust higher education networks (Afolalu et al., 2025; Angafor et al., 2024).

Finally, the findings may be crucial organisational and strategic implications of cybersecurity planning in higher education. All the mentioned advances in detecting, coordinating the response, and preparing the staff suggest directly that the application of simulation exercises leads to organisational resiliency, enabling universities to anticipate, mitigate, and recover better in case of the cyber threat (Blanchard, 2024; Chouliaras et al., 2021). The results also suggest the need to include the simulation programs into the greater cybersecurity plans, synchronize technical preparedness and the policy frameworks, the resources allocation, and the institutional priorities in risk management (Prummer et al., 2024; Forero, 2016).

By making regular, scenario-diverse exercises an institutional culture and relating them to continuous assessment measures, universities have a chance to develop a culture of preparedness, which cannot be neglected in the future but instead is associated with the current level of technical capability (Hautamaki et al., 2019; Vykopal et al., 2024). The paper, in general, provides empirical evidence that cyberattack simulation exercises that have an organized method are not only educational but also strategic facilitating elements to institutional cyber resiliency in high education networks (Afolalu et al., 2025; Kavak, 2021).

8. Conclusion

The study has determined that the simulation exercise of cyberattacks plays a role in enhancing institutional preparedness in higher learning institutions networks. The registered information has objective positive shifts in all the preparedness dimensions, such as incident detection, response coordination, and staff preparedness. Simulation exercises that were frequent and varied in the institutions that also practiced them were repeatedly more successful than those who were subjected to less frequent exposure, which highlights the importance of permanent and repeated training. The findings indicate that the simulation training does not just improve the technical skills, it also boosts the integration of the organisation and the departments are required to communicate better, use laid down procedures and react better to cyber attacks. Such developments can be viewed as an overall enhancement in resilience of the institutions, such as disconnecting the theory and its practical usage as well as providing the institutions of higher learning with a pragmatic roadmap to anticipate, manage and mitigate the risks of cyber attacks.

The answer to the research question is evident in the evidence provided that cyberattack simulation training achieves high preparedness in the higher education networks in terms of institutions. The drills provided the opportunity to identify the threats faster, to be more responsive, and to make every staff member more aware of technical and operational cybersecurity problems. In addition, the fact that simulations were used showed some weaknesses and gaps that can be actively handled by altering policies, resource allocation, and certain training. On the whole, the study shows that the method of simulation exercises could be deemed as the effective approach to assessing the preparedness and improving its level because it offers real-life conditions to challenge the human and technical facilities within the safe and regulated environment. It will also help prove that the preparation of the action plans is not a theory but is practically tested in such a way that the institutions will be better prepared to encounter cyber-related threats in the life-like circumstances.

The overall analysis of the effectiveness of simulation training on cyberattacks shows that the latter are critical components of the cybersecurity plan of higher learning. Along with the cultivation of the technical skills, promoting cross-functional collaboration, and creating a culture of vigilance and resilience across the institution, such exercises also enhance the organisational learning. They provide feasible suggestions on strategic decision-making, policy formulation, and priorities on the resources. The simulation exercises in the routine of the cybersecurity training program may serve to ensure that the universities remain at high level of preparedness in the long term since the staff and systems will be trained to respond to the evolving cyber threats. In conclusion, cyberattack simulation exercises cannot be regarded as educational interventions but as strategic enabling infrastructure of institutional cybersecurity resilience, and therefore, highly

ISSN 2959-6157

important components of the current higher education network management.

9. Recommendations

It is recommended to devote more attention to cyberattack simulations as a part of the general policy of cybersecurity in universities and colleges. These exercises should replicate the real world scenarios, both the ordinary malware and phishing attacks, and the more complicated attacks that can be of test to the technical systems and human capacity of responding. It is highly recommended that institutions establish special cybersecurity teams, which plan, conduct and evaluate such exercises, to ensure that all the departments are involved in such exercises so that awareness and coordination are created within an organisation.

Additionally, the lessons acquired in the organization of the simulation exercises should also be integrated in the process of the continuous professional development of the staff members in order that the best practices might be enhanced, and the culture of vigilance should be fostered. Such exercises will be magnified through additional investment in state of the art simulation platforms, cyber ranges, and training infrastructure, and universities will be in a position to train up to meet the evolving cyber threats in a controlled and quantifiable manner. Besides technical preparation, it is necessary to establish a system of feedback to extract the lessons learnt in each exercise to increase the time-resilience of the institution.

Institutions of higher learning must implement clear policies and governance of cybersecurity policies at both the policy and governance level that requires simulation practices and regular preparedness measures. Policy mechanisms should be determined to define the responsibilities and duties of incident response and accountability frameworks, such that the policy is revised and resources are allocated basing on the simulation exercises. It is also recommended that institutions should form some partnerships with industry, government agencies, and other universities to share knowledge, to benchmark readiness, and even to share training scenarios. Within the framework of cybersecurity practice, the holistic approach that involves the integration of technical, operational, and organisational solutions will enhance the overall preparedness. Finally, new research ought to be done to investigate the impact of cyberattack simulation exercises on institutional resilience in the long term, quantitative indicators of the effectiveness of the response, cost-benefit analysis, and the possibility of newer technologies, like those of artificial intelligence and adaptive simulation models, to enhance preparedness measures further.

References

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. *Future Internet*, *17*(12), 575. https://www.mdpi.com/1999-5903/17/12/575

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and privacy*, *3*(6), e126. https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.126

Blanchard, E. E., Feldman, S. S., White, M. L., Allen, R., Phillips, T., & Brown, M. R. (2024). Design and Implementation of Tabletop Cybersecurity Simulation for Health Informatics Graduate Students. *Applied Clinical Informatics*, *15*(05), 921-927. https://www.thieme-connect.com/products/ejournals/html/10.1055/s-0044-1790551

Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, *11*(4), 1809. https://www.mdpi.com/2076-3417/11/4/1809

Forero, C. A. M. (2016). Tabletop exercise for cybersecurity educational training; theoretical grounding and development. *MS thesis*. https://www.academia.edu/download/54023949/CARLOS_MARTINEZ_05_26.pdf

Gafic, M., Tjoa, S., Kieseberg, P., Hellwig, O., & Quirchmayr, G. (2022, February). Cyber Exercises in Computer Science Education. In *ICISSP* (pp. 404-411). https://www.researchgate.net/profile/Peter-Kieseberg/publication/358634544_Cyber_Exercises_in_Computer_Science_Education/links/62de4ec382bb472992a1ba88/Cyber-Exercises-in-Computer-Science-Education.pdf

Hautamäki, J., Karjalainen, M., Hämäläinen, T., & Häkkinen, P. (2019). Cyber security exercise: Literature review to pedagogical methodology. *INTED Proceedings*, (2019). https://jyx.jyu.fi/jyx/Record/jyx_123456789_63537

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*, *7*(1), tyab005. https://academic.oup.com/cybersecurity/article-pdf/doi/10.1093/cybsec/tyab005/36597586/tyab005.pdf

Kiarie, N. (2024). Enhancing Digital Resilience: A Cybersecurity Readiness Assessment of Kenyan TVET Institutions. *Journal of the Kenya National Commission for UNESCO*, *5*(1). https://journals.unesco.go.ke/index.php/jknatcom/article/view/191

Lillemets, P., Bashir Jawad, N., Kashi, J., Sabah, A., & Dragoni, N. (2025). A Systematic Review of Cyber Range Taxonomies: Trends, Gaps, and a Proposed Taxonomy. *Future Internet*, *17*(6), 259. https://www.mdpi.com/1999-5903/17/6/259

McGuan, C., Vijaya Raghavan, A., Mandapati, K. M., Yu, C., Ray, B. E., Jackson, D. K., & Kumar, S. (2025). Bridging Cybersecurity Practice and Law: A Hands-On, Scenario-Based Curriculum Using the NICE Framework to Foster Skill

Development. *Journal of Cybersecurity and Privacy*, *5*(4), 106. https://www.mdpi.com/2624-800X/5/4/106

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). SP 800-84. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. https://dl.acm.org/doi/abs/10.5555/2206295

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585. https://www.sciencedirect.com/science/article/pii/S0167404823004959

Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats. *Electronics*, *13*(19), 3867. https://www.mdpi.com/2079-9292/13/19/3867

Aldabjan, A., Furnell, S., Carpent, X., & Papadaki, M. (2025, June). A Prototype Tool for Incident Response Readiness Assessment. In *International Conference on Human-Computer Interaction* (pp. 163-179). Cham: Springer Nature Switzerland. https://link.springer.com/chapter/10.1007/978-3-031-92833-8_10

Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, *20*(24), 7148. https://www.mdpi.com/1424-8220/20/24/7148

Vykopal, J., Čeleda, P., Švábenský, V., Hofbauer, M., & Horák, M. (2024). Research and practice of delivering tabletop exercises. *Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1*, 220-226. https://dl.acm.org/doi/abs/10.1145/3649217.3653642

Vykopal, J., Čeleda, P., Seda, P., Švábenský, V., & Tovarňák, D. (2021, October). Scalable learning environments for teaching cybersecurity hands-on. In *2021 IEEE frontiers in education conference (FIE)* (pp. 1-9). IEEE. https://ieeexplore.ieee.org/abstract/document/9637180/

Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats. *Electronics*, *13*(19), 3867. https://www.mdpi.com/2079-9292/13/19/3867

Boghosian, H. (2025). *Cyber Citizens: Saving Democracy with Digital Literacy*. Beacon Press. https://books.google.com/books?hl=en&lr=&id=ue4jEQAAQBAJ&oi=fnd&pg=PA1&dq=Cyber+Storm+Exercise+(Wikipedia)+(2024).&ots=Amr4ZtUD7d&sig=FTgZVUULt0jZO2nMfA-Dqpyjzbg

KUMAR, C. Net-Tok: Network Security Tool-Kit for Network Administrators. https://engrxiv.org/preprint/view/3731

Netshiunda, H., & Madzvamuse, S. (2025). A Systematic Literature Review of Cybersecurity Awareness and Strategy in Rural-Based Universities. *International Journal of Applied Research in Business and Management*, *6*(5). https://www.wr-publishing.org/index.php/ijarbm/article/view/350

Gafic, M., Tjoa, S., Kieseberg, P., Hellwig, O., & Quirchmayr, G. (2022, February). Cyber Exercises in Computer Science Education. In *ICISSP* (pp. 404-411). https://www.researchgate.net/profile/Peter-Kieseberg/publication/358634544_Cyber_Exercises_in_Computer_Science_Education/links/62de4ec382bb472992a1ba88/Cyber-Exercises-in-Computer-Science-Education.pdf

Angafor, G., Yevseyeva, I., & Maglaras, L. (2024). MalAware: A tabletop exercise for malware security awareness education and incident response training. *Internet of Things and Cyber-Physical Systems*, *4*, 280-292. https://www.sciencedirect.com/science/article/pii/S2667345224000063

Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: a meta-analysis. *Computers & Security*, *150*, 104206. https://www.sciencedirect.com/science/article/pii/S016740482400511X

Too, W. K., Karume, S. M., & Masese, N. B. (2022). Defensive cybersecurity preparedness assessment model for universities. *Int. J. Comput.(IJC)*, *43*(1), 112-128. https://www.researchgate.net/profile/Simon-Karume-2/publication/363611247_Defensive_Cybersecurity_Preparedness_Assessment_Model_for_Universities/links/6324d50e071ea12e363a8c37/Defensive-Cybersecurity-Preparedness-Assessment-Model-for-Universities.pdf

Appendix

Cyberattack Simulation Exercises and Institutional Preparedness Survey

Target Respondents:

Cybersecurity managers, IT directors, incident response leads, ICT governance officers, or senior technical staff in higher education institutions.

Instructions to Respondents:

Please answer the following questions based on your institution's experience with cyberattack simulation exercises. All responses reflect institutional practices, not personal opinions. Responses are confidential and used solely for academic research purposes.

Section A: Institutional and Demographic Information

Q1. What type of higher education institution do you represent?

☐ Public university
☐ Private university
☐ Public college
☐ Private college

Q2. What is the approximate student population of your institution?

☐ Fewer than 5,000 students
☐ 5,000–20,000 students
☐ More than 20,000 students

Q3. How would you describe your institution's ICT maturity level?

ISSN 2959-6157

☐ Basic (limited centralised security controls)
☐ Developing (partial governance and controls)
☐ Mature (formalised cybersecurity governance and controls)

Section B: Cyberattack Simulation Exercise Practices

Q4. Has your institution conducted cyberattack simulation exercises in the past three years?
☐ Yes
☐ No
(If "No", please proceed to Section F)

Q5. How frequently does your institution conduct cyberattack simulation exercises?
☐ Quarterly
☐ Annually
☐ Biennially
☐ Ad-hoc / Irregular

Q6. Which types of simulation exercises does your institution use? (Select all that apply)
☐ Tabletop exercises
☐ Cyber range / technical simulations
☐ Incident response drills
☐ Hybrid (combined technical and tabletop exercises)

Section C: Types of Simulated Cyber Scenarios

Q7. Which of the following cyberattack scenarios have been simulated at your institution? (Select all that apply)
☐ Phishing attacks
☐ Ransomware attacks
☐ Data breach scenarios
☐ Insider threat incidents
☐ Distributed Denial-of-Service (DDoS) attacks
☐ Coordinated multi-vector attacks

Q8. How closely do the simulated scenarios reflect real-world cyber threats faced by your institution?
(1 = Not realistic, 5 = Highly realistic)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Section D: Institutional Response Capabilities

(Please rate the following based on your institution's current capabilities)

Q9. Rate your institution's capability in each area below:
(1 = Very Low, 5 = Very High)

Capability Indicator	1	2	3	4	5
Incident detection	☐	☐	☐	☐	☐
Response coordination	☐	☐	☐	☐	☐
Escalation procedures	☐	☐	☐	☐	☐
Communication effectiveness	☐	☐	☐	☐	☐
Recovery planning	☐	☐	☐	☐	☐

Section E: Preparedness Before and After Simulation Exercises

Q10. Please rate your institution's preparedness before participating in cyberattack simulation exercises:
(1 = Very Low, 5 = Very High)

Indicator	1	2	3	4	5
Response time readiness	☐	☐	☐	☐	☐
Staff confidence	☐	☐	☐	☐	☐
Incident coordination	☐	☐	☐	☐	☐
Policy awareness	☐	☐	☐	☐	☐

Q11. Please rate your institution's preparedness after participating in cyberattack simulation exercises:
(1 = Very Low, 5 = Very High)

Indicator	1	2	3	4	5
Response time readiness	☐	☐	☐	☐	☐
Staff confidence	☐	☐	☐	☐	☐
Incident coordination	☐	☐	☐	☐	☐
Policy awareness	☐	☐	☐	☐	☐

Section F: Organisational Learning and Policy Impact

Q12. To what extent have simulation exercises helped identify weaknesses in your institution's cybersecurity policies and procedures?

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Q13. Have simulation exercises led to updates or improvements in cybersecurity policies?
☐ Yes
☐ No
Q14. How would you describe staff awareness of cybersecurity responsibilities following simulation exercises?
☐ Significantly improved
☐ Moderately improved
☐ Slightly improved
☐ No noticeable change
Section G: Challenges and Limitations
Q15. What challenges has your institution faced in implementing cyberattack simulation exercises? (Select all that apply)
☐ Limited funding
☐ Lack of technical expertise
☐ Time constraints
☐ Limited management support
☐ Complexity of realistic scenario design
Q16. To what extent do these challenges limit the effectiveness of simulation exercises?

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Section H: Overall Assessment
Q17. Overall, to what extent do cyberattack simulation exercises enhance institutional preparedness in your institution?

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Q18. Would you recommend regular cyberattack simulation exercises as part of higher education cybersecurity strategy?
☐ Yes
☐ No