Journal of
Cyber Security

Tech Science Press

https://doi.org/10.32604/jcs.2026.080111

ARTICLE

Organizational Determinants of Cybersecurity Readiness: Evidence from a Quantitative Analysis

Darlington Okeke*

Department of Computing and Engineering, University of Gloucestershire, Cheltenham, UK

*Corresponding Author: Darlington Okeke. Email: okekechigozied2023@gmail.com

Received: 03 February 2026; Accepted: 15 June 2026; Published: 21 August 2026

ABSTRACT: Background: Novel cyber threats to organizations have greatly escalated due to the high digitalization rates of organizations, and cybersecurity readiness is a critical capability of organizations and not a technical issue. Although there is increased awareness, most organizations are ill-equipped due to weaknesses in human behavior, governance, leadership commitment, technology infrastructure, and incident response mechanisms. This paper discusses organizational factors that play a major role in cybersecurity readiness. **Methods:** Primary data from 230 participants were collected using a questionnaire approach and analyzed using IBM SPSS software. The quantitative methods adopted include descriptive statistics, Cronbach's reliability test and Pearson's Correlation analysis. **Results:** The findings indicate significant positive relationships between employee training, technological assistance, incident response planning and cybersecurity readiness, underscoring the importance of cybersecurity readiness. **Conclusions:** There are significant relationships between employee cybersecurity training, security policy enforcement, management support for cybersecurity, availability of cybersecurity tools, incident response planning, and organizational cybersecurity readiness.

KEYWORDS: Cybersecurity readiness; employee training; security policy enforcement; management support; incident response; cybersecurity tools

1 Introduction

This chapter sets the stage for the study by providing background on the growing significance of cybersecurity readiness in organisations. It describes the problem statement, the research gap, the objectives and the hypotheses that underpin the research. It sets the stage for exploring the impact of organisational factors on cybersecurity readiness.

1.1 Motivation and Problem Statement

The rapid digitalization of organizations has fundamentally changed how they operate, communicate, and store information [1]. The level of interconnection among digital infrastructures increases, making an organization more susceptible to a host of cyber threats [2]. There has been an upsurge in the frequency and complexity of cyber-attacks, such as ransomware, phishing, and advanced persistent threats, which puts organizational defenses under pressure like never before [3]. These attacks are no longer considered independent technical incidents but risks to the system that have the capacity to end the entire ecosystem of operations. It has been found that many organizations are being exposed due to fragmented security designs and inadequate preparedness systems [4]. The consequences of lapses in cybersecurity go well beyond

monetary losses, which are further compounded by reputational losses, fines, and stakeholder trust [5]. Cybersecurity has become a high strategic value and not just a technical issue, and must be responded to by the organization in this dynamic atmosphere.

Structural and human vulnerabilities are adding to the organizational cybersecurity problems that advanced technical defense mechanisms cannot overcome. Cyber threats are frequent, and in most cases, employees do not have knowledge of cyber risks, which may lead to unsafe work practices such as weak passwords and social engineering attack vulnerability [6]. The literature shows that insider-related vulnerabilities account for a substantial share of successful cyberattacks in contemporary organizations [7]. Besides the human factor, several institutions have a problem of poor infrastructure and a lack of constant implementation of security measures [8]. Technological innovation usually occurs rapidly, reducing the rate at which organizations adapt, leaving constant gaps between new threats and defense preparedness. These facts underscore the importance of cybersecurity resiliency being an organization-wide strategy based on culture, governance, and capability building.

Cybersecurity readiness has thus proven to be a significant framework for assessing organizations' readiness against online attacks. Ready implies coordination of policies, technologies, employee skills, and leadership determination to maintain long-term protection of information assets [3]. Scholars note that readiness is an organization's capability to predict, identify, and respond to cyber incidents effectively [6]. An increase in readiness has been linked with a faster response to an incident and a decreased disruption of operations. Digitalization of organizations has occurred in a very fast manner, and this has fundamentally changed how organizations are run, communicate, and store information. The degree of interconnection of digital infrastructures rises, and it means that an organization is more prone to the impact of a hostage of cyber threats [9]. The rate and sophistication of cyber-attacks, including ransomware, phishing, advanced persistent threats, and so on, have increased, and this puts organizational defenses to the test like never before [1]. Such attacks are no longer seen as isolated technical incidents but as a danger to the system that can bring the whole ecosystem of operations to an end. As it has been discovered, numerous organizations are being exposed because of poor security design and poor preparedness systems [4]. The after-effects of cybersecurity failures extend far beyond a loss of money, which is, in turn, accompanied by a loss of reputation, financial penalties, and lost confidence of the stakeholders. Cybersecurity has been a top strategic value and not just a technical concern and should be addressed by the organization in this dynamic environment.

The organizational cybersecurity issues that sophisticated technical defenses cannot overcome are being compounded with the structural and human vulnerabilities [9]. Cyber threats are common, and most of the time, employees lack awareness of cyber risks, which can result in wrong practices at work, like the use of weak passwords and vulnerability to attacks through social engineering [5]. Compliance with regulatory and industry requirements that are growing more and more demanding in terms of proving security capabilities is also strengthened by preparedness. Moreover, robust cybersecurity preparedness helps build confidence among stakeholders and gain a competitive edge in digitally oriented markets [8]. The above advantages make readiness one of the elements of the modern organizational strategy.

1.2 Research Gap

Despite increased awareness of cybersecurity readiness, empirical studies examining the organizational factors of preparedness [8] still reveal notable gaps. A large portion of the literature that exists is focused on technical protection measures and ignores behavioral and managerial factors. Some researchers claim that the effectiveness of cybersecurity is not comprehensible without analyzing the organizational culture and dynamics of leadership [9]. Most past studies tend to view readiness as an ideal concept and not an

operational construct that can be measured using operational variables [8]. The limitation deprives the organizations of the right to come up with evidence-based improvement plans. A more analytical framework embedded in the paper is needed to capture the general effects of organizational factors on preparedness.

The paper addresses the identified gap in the literature by systematically examining the advocates of organizational readiness for cybersecurity. It takes into consideration training, governance, management support, technological infrastructure, and incident response planning perspectives. This is one of the features of the complicated nature of cybersecurity readiness in contemporary institutions. The empirical measurement of the said relations by the study will yield practical findings on improving organizational resilience. The outcome will be desired to support strategic decision-making and will result in the design of holistic cybersecurity measures.

1.3 Specific Objectives

Given the research gap and need to study organizational cybersecurity readiness, the following research objectives are put forward:

RO1: To examine the relationship between employee cybersecurity training and organizational cybersecurity readiness.

RO2: To determine the relationship between security policy enforcement and organizational cybersecurity readiness.

RO3: To assess the relationship between management support for cybersecurity and organizational cybersecurity readiness.

RO4: To evaluate the relationship between availability of cybersecurity tools and organizational cybersecurity readiness.

RO5: To analyze the relationship between incident response planning and organizational cybersecurity readiness.

1.4 Research Hypotheses

In line with the research objectives and existing theoretical and empirical evidence, the following hypotheses are proposed to test the relationships between the study variables:

H1: *There is a significant relationship between employee cybersecurity training and organizational cybersecurity readiness*.

H2: *There is a significant relationship between security policy enforcement and organizational cybersecurity readiness*.

H3: *There is a significant relationship between Management support for cybersecurity and organizational cybersecurity readiness*.

H4: *There is a significant relationship between availability of cybersecurity tools and organizational cybersecurity readiness*.

H5: *There is a significant relationship between incident response planning and organizational cybersecurity readiness*.

2 Literature Review

This section examines existing research on cybersecurity readiness and its antecedents. It draws on theoretical and empirical research to offer a holistic view of the role of human, technology, and managerial factors in preparedness. It also sets the conceptual and theoretical groundwork for this study.

The section presents a literature review of current knowledge on organizational cybersecurity readiness and its critical determinants. The review has been organized in a way that gives a logical flow starting with conceptual premises up to empirical evidence. To start with, the notion of organizational cybersecurity readiness is considered to define its multidimensional character. This is then followed by the discussion of the main independent variables, which are employee cybersecurity training, enforcement of security policies, management support, accessibility of cybersecurity tools, and incident response planning, which are discussed as separate subsections to explain their theoretical and practical roles. This section moves on to discuss the theoretical frameworks beneath the study, before concluding with an empirical review which summarizes previous research on the study topic and identifies gaps in the existing research body. This organized methodology helps improve clarity, provide coherence, and facilitate the creation of the study's conceptual framework.

2.1 Concept of Organizational Cybersecurity Readiness

Organizational cybersecurity readiness is a concept that defines how an institution is ready to foresee, avert, identify, and react to cyber threats in a coordinated and sustainable way. According to scholars, readiness is a state in which organizational structures, processes, and technologies are aligned in a manner that enables effective handling of cyber risks [10]. This viewpoint states that readiness cannot be restricted to technical controls, but it encompasses governance and behavioral aspects [11]. Researchers also note that cybersecurity readiness is a dynamic state that enables organizations to counter the evolving threat environment [12]. Readiness as a practical capability is an inherent capacity that must be strengthened during organizational learning and strategic planning.

The concept of cybersecurity readiness is inherently multidimensional, as the modern digital world is inherently complex. Several frameworks define readiness as being a set of awareness, prevention, detection, and recovery capabilities [13]. Such schemes indicate that readiness implies coordination of human and technological systems [14]. The readiness in the systems perspective can also take the form of an organizational maturity process, built over time through the provision of improvements [15]. Such a way of thinking reinforces the idea of cybersecurity resilience, which is founded on lifelong review and improvement. Companies that fail to recognize this dynamic nature are subjected to stagnation and vulnerability to cyber threats.

The behaviour of employees and human capital development is also an aspect of the organizational readiness area that is most critical. The most important aspect of cybersecurity readiness is employees' level of awareness and competence, as they are the first line of defense. It is empirically shown that organized cybersecurity training programs can be applied effectively in enhancing the levels of readiness [16]. Human-oriented models clarify that the organizational culture must be supportive of secure behaviors and shared responsibility [17]. Security controls tend to be successful or unsuccessful depending on the behavioral compliance with the set policies. Even technical investments cannot guarantee effective protection of resources when personnel are not involved regularly.

Governance and policy implementation are other sub-factors underlying cybersecurity readiness. Good governance plays a vital role in ensuring that the role of cybersecurity has been spelled out and embedded in the leadership systems. The research demonstrates that executive commitment becomes one of the major predictors of organizational readiness [18]. The existence of well-developed governance systems will allocate resources and generate accountability for cybersecurity activities [10]. Adoption of a policy creates a certain level of predictability by which employees can be governed and identifies limited areas of vulnerability within the working processes. Cybersecurity becomes a strategy in the governance of organizations and is more stable and resilient.

Another significant basis of cybersecurity readiness in organizations is technological infrastructure. The modern world requires technologies capable of detecting threats and destroying them immediately. There are also findings that technological readiness is positive in ensuring continuity in operations in the event of a cyber-incident [19]. Security platforms contain automation and analytics, which provide situational awareness and response time [20]. However, technological infrastructure alone is insufficient; it must be supported by effective governance and knowledgeable personnel to achieve organizational cybersecurity readiness. Technology complements governance and human knowledge by enabling policy implementation, strengthening monitoring capabilities, and supporting security awareness and informed decision-making. The combination of tools, processes, and human resources leads to sustainable readiness.

The critical role of cybersecurity readiness is related to operational resilience and service continuity. Best-prepared companies will be able to react better to any event of a cyber-attack. It is disclosed that a prepared institution can recover more quickly than those that have not been prepared [13]. Virtualization readiness also assists in compliance with regulatory norms and industry standards [11]. These security controls assist in securing the organization's plants as well as making sure the interested parties remain assured. Readiness then becomes a stabilizing mechanism in digitally reliant environments.

Besides the effectiveness of the operations, there is a high strategic value of cybersecurity readiness. The well-prepared institutions enjoy competitive advantages in the markets where trust is a critical element. Stakeholder confidence has been established to be directly related to the perceptions of cybersecurity capability [12]. A well-prepared readiness plan builds a good reputation and reduces the risk of disastrous failures [14,21]. The reputational risks facing those organizations that are unprepared extend well beyond the direct financial losses. Strategic readiness positions institutions to succeed in unpredictable digital environments.

On balance, organizational cybersecurity readiness is a complicated phenomenon, and it has human, governance, and technological dimensions. Its definitions can be grounded in capability development, emphasizing proactivity and the continuous process of adaptation. The concept underlines the need to make cybersecurity a component of organizational strategy and culture. Companies that have an institutionalized readiness are in a better position to overcome the shifting threats. A holistic readiness strategy also determines the sustainability of digital activities within the present organizations.

2.2 Cybersecurity Training of Employees

It is typically acknowledged that the training of employees on cybersecurity can be regarded as one of the foundations of cybersecurity readiness in the organization. Modern cyber threats tend to exploit human vulnerabilities and not technology vulnerabilities. Research has continuously shown that employee behavior is one of the factors that will either succeed or fail in an attack [22]. The training programs will be geared towards solidifying awareness of phishing, malware, social engineering, and unsafe digital behavior [13]. Researchers believe that lifelong learning inculcates a proactive security attitude, resulting in low-risk exposure for organizations [23]. The staff will not be mere users in their cybersecurity defense training.

Cybersecurity education is not only informational but is rather behavioral. It focuses on developing behaviors that make employees act in accordance with organizational security policies. Research has shown that sustained exposure to security education is a major contributor to observing safe computing behaviors [12]. Behavioral reinforcement theories help focus on the fact that learning should be continuous, but not episodic [24]. Simulations and real-life scenarios are especially useful in the training process of resilience to social engineering attacks [25]. Routine training is institutionalized within organizations and results in the detection of threats and the reporting of incidents.

Another significant issue with employee training is that it helps develop an organizational security culture. With a good security culture, shared responsibility and collective vigilance are promoted. Studies have established that training has a direct effect on the inculcation of security-conscious norms among the employees [18]. Training programs facilitated by leaders are an indication of the strategic significance of cybersecurity [21]. Motivation and retention levels go up when the employees feel that training is a serious process and not a show [26]. Cultural alignment will ensure the integration of cybersecurity into daily decision-making.

Instructions and delivery of cybersecurity training rely on the design of the instruction. Conventional lecture-based lessons are being supplanted by interactive, technology-based learning models. Experience indicates that learning through experience enhances knowledge retention and behavioral change [10]. Training tools that are ramified encourage employees to engage in security training proactively [27]. Adaptive learning systems enable organizations to individualize the training content based on the risk profile [28]. These inventions demonstrate that training must be modified to reflect the threat environment.

Cybersecurity training also contributes to making organizations prepared by improving their ability to respond to an incident. The employees who have been trained and know how to detect the abnormalities will report the suspected behavior at earlier stages. Research indicates that timely reporting is very influential in derailing the severity of cyber-attacks [16]. Coordination is improved through training programs that include incident response exercises [29]. Simulated drills train employees to respond calmly when they are under pressure [30]. Trained staff acts as a pre-attack warning system to boost technical defenses.

Although cybersecurity training is beneficial, there are several challenges in implementing it. Organizations usually do not estimate the resources needed to maintain working programs. On research ineffectively designed training could result in disengagement, as well as compliance fatigue [15]. Training initiatives without executive involvement can be seen as having low priority [31]. Testing and evaluation systems are required to assess the training success and implement changes based on the results [32]. Management commitment and participation of employees must be unified in sustainable programs.

Employee cybersecurity is vital to the company's strategy, beyond just reducing risks. Skilled workers will help in the resilience and continuity of the organization in operation. As evidence shows, the level of training investment is associated with a reduced number of successful cyber intrusions [20]. Companies with established education programs rebound sooner after security attacks [33]. Continued learning enables institutions to remain flexible in evolving threat environments [34]. Training as a long-term strategic resource is exposed by such results.

In summary, staff cybersecurity training is a significant factor in defining organizational readiness. It aids in the creation of awareness and behavior, as well as enhances the capacity for response to incidents. The culture of security is influenced by training programs and enhances governance. Firms that invest in lifelong learning gain resilience in cybersecurity, and this is sustainable. The gap between human vulnerability and computer security is eventually bridged with proper training.

2.3 Security Policy Enforcement

Security policy is one component of organizational cybersecurity readiness. Policies constitute a formal rule on how the subjects ought to behave, access control, and the protection of information assets. As it has been discovered, clear cybersecurity policies reduce uncertainty and influence employee decision-making [17]. Enforcement also ensures that the policies are not mere documents but operational standards that constitute part of day-to-day practice [35]. Researchers repeatedly report that fewer security violations

are observed in organizations with a strong enforcement culture [19]. Effective enforcement transforms policy regimes into working governance instruments.

Cybersecurity performance concerns the connection between policy implementation and employee adherence. Compliance is dependent on frequent monitoring and accountability procedures as well as awareness. Studies have shown that strong enforcement goes hand in hand with adherence to cybersecurity implementation, with the penalty program being conspicuous [36]. Behavioral models assume that the consistency of enforcement underlies the organizational norms [11]. Whenever employees believe that security policies are just and applied uniformly, there is a high likelihood of abiding by them [37]. The next behavioral control is enforcement, which reinforces the institutional demands.

Leadership involvement is closely related to policy implementation. An indicator of the importance of governance of cyberspace is the executive commitment. This has been demonstrated in the literature, which indicates that organizations where leadership is actively supervised implement policies more consistently [13]. Confirmative behavioral models of managers have a positive influence on the organizational culture [24]. Obviously, active leadership will be justified by imposition of enforcement and reduced resistance among employees [31]. Organizational commitment to cybersecurity purposes is improved through policy-based enforcement.

The implementation of cybersecurity policies is enhanced using technological support systems. Automated monitors can detect violations of policies whenever they take place and reduce the role of manual management. It has been hinted that the built-in security management systems increase the compliance tracking capacity [10]. The auditing and logging technologies may provide a measurable record of digital activities [23]. Such systems enable organizations to adopt policies systematically rather than reactively [26]. Technological reinforcement ensures that the enforcement mechanism can be scaled to complicated environments.

Policy enforcement is also vital for standardizing security procedures and minimizing risks. Implementing regulations brings consistency, which minimises procedural variation and limits opportunities for intruders to exploit security weaknesses. It has been found that the implementation of a consistent policy impedes the possibility of insider threats [18]. The enforcement structures offer a predictable environment where the cybersecurity expectations are clearly spelt out [25]. Standardization increases the capacity of an organization to withstand pressure through the minimization of loopholes in a process.

Over-enforcement or incorrect enforcement, however, would have undesired consequences. Excessive discipline can create resentment among employees and lead to the cover-up of incidents. Studies have cautioned against enforcement based on fear, as this would discourage prompt reporting of security breaches [15]. Combined enforcement measures that incorporate both accountability and education are more effective [29]. Companies have to develop ways of dealing with enforcement mechanisms that are cooperative and not intimidating [28]. The implementation to be sustainable will need trust between the management and the employees. Compliance and external accountability are also supported by the security policy enforcement. Numerous sectors have strict cybersecurity guidelines that mandate documentation with enforcement practices. It has been demonstrated that companies with formal enforcement systems in place have higher compliance ratings [20].

2.4 Management Support for Cybersecurity

Management support is also a critical determinant of an organization's readiness for cybersecurity. Leadership sets priorities, resources and creates the tone of the culture of security of the institutions. The studies indicate that executive engagement is one of the critical determinants of the success of cybersecurity

measures [13]. The management should openly embrace cybersecurity programs to make employees perceive them as necessities and not luxuries [33]. The researchers believe that leadership commitment helps fill the gap between strategic intent and operational implementation [23]. Well-designed cybersecurity frameworks cannot be sustainable without managerial support.

Top management is key to incorporating cybersecurity into the organizational strategy. Risk management and corporate governance are also increasingly involved in cybersecurity decisions. Research shows that companies that integrate cybersecurity management at the board level are better prepared [18]. Strategic leadership also makes certain that the investments in cybersecurity are focused on the long-term goals of the organization [36]. Security policies and enforcement mechanisms are supported by executive sponsorship [26]. A strategy driven by leadership incorporates cybersecurity into institutional planning processes.

Another important aspect of management support is resource allocation. Implementing cybersecurity programs requires funding, talented staff, and technological infrastructure. There is evidence that low-budget cybersecurity initiatives are associated with increased exposure to cyberattacks [10]. Commitment to budgeting by the management is an indication of the level of seriousness of the readiness of an organization [27]. Sufficient financing facilitates the constant upgrading of security devices and the training courses [25]. Sustainable readiness relies on a regular supply of resources as opposed to occasional investment.

The culture of an organization and employee engagement are also influenced by management support. Leaders make the difference in how cybersecurity is regarded as a collective responsibility or a technical task. The studies further indicate that supportive leadership promotes a positive security culture [16]. When employees feel that the managers are involved in cybersecurity programs, they react better [24]. Cultural enforcement encourages self-reporting of threats and compliance with security practices. Organizational alignment is thus triggered by leadership behavior.

The cybersecurity responsiveness is influenced by the management structures. Quick response to emerging threats should be decentralized with strategic control. Studies have shown that agile leadership increases the efficiency of incident management [11]. Companies that have lax decision-making tiers respond faster to cyber crises [31]. Communication with the executives makes the incident response process less confusing [34]. Good governance ensures coordinated activity across departments.

Cybersecurity readiness is also enhanced by management accountability processes. Compliance is higher in institutions that assess leaders based on their cybersecurity performance. It has been shown that security-related performance measures and their outcomes motivate executive involvement [20]. Good reporting lines support managerial accountability [21]. Accountability systems converge the leadership incentives and organizational security objectives [32]. Such mechanisms will make cybersecurity a management priority rather than a marginal concern.

Management also supports cybersecurity due to the expectation of external stakeholders. The regulatory bodies, clients, and even partners are continually insisting on demonstrating readiness. There is an indication that leadership commitment enhances an organization's reputation in virtual markets [14]. Positive pressure by stakeholders may promote active investment in cybersecurity [35]. The competitive world recognizes institutions that possess excellent executive management of security [28]. Management's responsiveness to external expectations increases institutional credibility.

To conclude, management support is a strategic tool of cybersecurity readiness. Leadership commitment has an impact on culture, distribution of resources as well as effectiveness of governance. The presence of the executive incorporates cybersecurity into organizational strategy and performance. Those institutions

that put more emphasis on managerial involvement are more prepared sustainably. Effective leadership will eventually make cybersecurity a technical issue into an organizational competency.

2.5 Availability of Cybersecurity Tools

One of the main technical aspects of organizational readiness is the availability of cybersecurity tools. Contemporary organizations are based on a layered defense structure that incorporates hardware, software and monitoring systems. It has been shown that the existence of sophisticated cybersecurity systems increases threat detection levels to a considerable extent [22]. Security tools such as firewalls, intrusion detection systems, endpoint protection and others form a defensive line to unauthorized access [34]. According to researchers, institutional cyber defense relies on the technological infrastructure [20]. Organizational preparation, per se, is constrained by the absence of adequate instruments, regardless of any policy or training programs.

The cybersecurity tools support a real-time view of the organization's networks and digital assets. Under constant monitoring systems, anomalies are noted even before they can evolve into massive incidents. It suggests that organizations that have automated threat analytics experience fewer successful breaches [24]. High-tech detection systems refer to those that use artificial intelligence to find out patterns associated with malicious activity [15]. Automated monitoring systems can help reduce reliance on manual tasks and minimize the risk of human error while allowing organizations to monitor their network continuously [26]. The presence therefore helps strengthen the defensive action against reactive action.

The cybersecurity tools are based on integration within the organization. Separated technologies merely provide partial security when they have not been incorporated into governance processes. It has been shown that interoperability improves cross-platform security coordination of response [18]. The centralized security management systems enable the similarity in the implementation of policies across departments. Integrated architectures reduce the gaps that may be exploited by attackers [38]. The tools, procedures and people can only be successfully implemented through coordination.

The maintenance and regular upgrading of cybersecurity devices is also a significant aspect of cybersecurity. Hackers continue to advance their tactics and render the previous security systems ineffective. Research indicates that there is a high reduction in vulnerability exposure in patch management and system upgrades [10]. When they are not upheld by such organizations, they risk exploitation [29]. The automated update systems enhance system resiliency and stability [30]. Maintenance is also used to ensure that defensive technologies are not worn out in dynamic environments.

Forensic evidence used in understanding the attack vectors is provided by the logging systems. It has been proven that those organizations that possess powerful logging skills are more effective in solving incidents [16]. Technologies for backup and recovery reduce downtime in the event of breaches [36]. Incident management platforms facilitate communication between the response teams [32]. Technical readiness thus goes further to include recovery capability in addition to prevention.

Nevertheless, excessive dependence on technology without strategic planning may introduce new risks. Complicated security systems can create operational blind spots if not well managed. The research cautions that over-fragmentation of the tools decreases situational awareness [17]. Companies are known to implement duplicate systems that add maintenance expenses yet do not add security [31]. The main tool selection will be strategic so as to guarantee efficiency and effectiveness [25]. Technology should serve organizational goals, not be their master.

Decisions regarding cybersecurity tools are a higher organizational priority. The institutions that are more prepared exist because they allocate sufficient funds to finance infrastructure. Cybersecurity has

been identified to support fewer incidents when invested in [14]. Financial commitment refers to social commitment in the long term to digital resilience [27]. The strategic procurement believes in the truth that tools are in congruence with the dynamic threat scenarios [28]. Technical readiness is thus a significant component that involves budget planning.

In conclusion, operational defense and resiliency is dependent on the existence of cybersecurity tools. Relevant tools enhance detection and management of incidents as well as visibility. They can be useful only when combined with, and kept up to date and strategic alignment with governance structures. The readiness is enhanced by companies that make sound investments in information technology infrastructures. Cybersecurity readiness eventually is complemented by technical capability on human and managerial aspects.

2.6 Incident Response Planning

Another pillar of organizational readiness to cybersecurity is incident response planning. Even advanced defense mechanisms fail to offer maximum protection against cyber-attacks. Research indicates that readiness must also include mechanisms for responding to such eventualities to minimise the risk of damage in the event of an occurrence [11]. Incident response plan is an official guideline of procedures that delineate detection, containment, eradication, and recovery routines [24]. Researchers argue that organizations that have put on record response frameworks experience fewer interruptions to their activities when breaches occur [37]. The unexpected crisis is addressed through planning.

A plan, including the incident response plan, will assist in clarifying the roles and responsibilities of the different units of the organization. Clear delegation will not cause confusion and wastage of time due to emergencies. It has been established that the pre-established roles increase the coordination of activities and the speed of decision making [15]. Incident command systems assist teams in acting when there is a need to act [36]. The communication protocols ensure that the stakeholders receive the appropriate information to the appropriate time [23]. Planned organization in cyber crises therefore boosts organizational control.

Training and simulation exercises are used to achieve good response planning. Practices have to be made on how to stay operational in real conditions. It is demonstrated that simulation exercises increase team readiness and confidence [13]. The repetition of exercises reveals weak points in the processes prior to real accidents taking place [31]. Companies that practice incident response have shorter recovery times [26]. Experience converts theory into practice.

Learning and continuous improvement are also supported by incident response planning. Every computer hack is an informative experience in the organizational weaknesses. The literature indicates that institutional resilience improves following post-incident reviews [14]. Breach lessons are incorporated in future defense mechanisms [35]. Feedback loops allow companies to streamline their policies and technical controls [24]. Response frameworks that are based on learning transform failures into learning opportunities.

Jurisdiction between incident response and greater cybersecurity governance is crucial. The response planning should be consistent with the policies and risk management strategies of the organization. Studies have shown that integrated governance will help promote cross-departmental collaboration during incidents [10]. Transparency will guarantee that the technical units and the top management team pull together [29]. Combined structures prevent the absence of coordination and miscommunication [25]. The integrity of the cybersecurity strategy is enhanced by integration.

Timely reporting and escalation mechanisms are the other significant aspect of incident planning. Early detection can significantly reduce the extent of cyber damage. It is demonstrated that fast reporting systems limit attackers' lateral movement [16]. The staff must be familiar with the way and time in which they report

suspicious activity [33]. Warning mechanisms help to improve the speed of decision-making [32]. Good reporting systems build strong organizational perceptions.

The incident response plan also influences compliance with regulations and stakeholder trust. Many sectors require documented response skills, as a section of the law. Research has revealed that prepared organizations are more plausible in the eyes of the public when breaches occur, and that open response mechanisms reduce the reputational harm [22]. Conformance with regulations helps institutions avoid fines [34]. Readiness indicates the accountability of institutions during the crisis.

As a conclusion, incident response planning turns a haphazard battle against cybersecurity into a set of rules. It defines the roles, enhances teamwork and promotes ongoing education. Good planning incorporates systems for planning, training and communication. Companies that make response structures institutional are more resilient during pressure. Being ready means that cyberattacks become manageable rather than devastating.

2.7 Conceptual Framework

The conceptual framework visualizes the determinants important to organizational cybersecurity readiness by showing the direct effects of five independent variables on a single dependent variable. The human-capacity dimension is employee cybersecurity training, which focuses on human knowledge and awareness of cyber risk reduction. One of the most widely used governance and compliance measures, where organizations regulate acceptable behavior and standardize security practices, is security policy enforcement. Cybersecurity management support takes the strategic and leadership position in giving a priority to cybersecurity in terms of commitment, funding, and decision-making. The technological infrastructure needed to combat, detect, and respond to cyber threats is the availability of cybersecurity tools. Incident response planning reflects an organization's readiness and resiliency to address and recover from a cybersecurity incident.

The framework is holistic because it treats all five variables as direct predictors of organizational cybersecurity readiness, incorporating the human, managerial, technical, and procedural aspects. According to this structure, the issue of cybersecurity readiness cannot be attributed to the influence of a single element but is the result of interactive and collective efforts involving organizational policies, leadership support, staff competence, technological capabilities, and response.

2.8 Underpinning Theory

The theoretical background of organizational cybersecurity readiness can be explained in terms of the dynamic capability theory. This is the view of how organizations grow, combine and reorganize both internal and external capabilities in order to respond to the rapidly changing environments. Cyber threats are ever-changing, and institutions need to keep up with them more rapidly than adversaries. The researchers explain that digital security readiness is one of the reflections of organizational dynamic ability [13]. Dynamic capability is focused on the ability to perceive new threats, seize protective opportunities, and modify structures to maintain resilience [31]. This theoretical prism makes cybersecurity an organizational strategic operational capability and not an immutable technical necessity.

The dynamic capability theory emphasizes that learning and adaptation are important for cybersecurity readiness. Organizations are forced to continue to obtain new information relating to vulnerabilities and threat patterns. The research reports show that adaptive learning helps to increase the resilience of the institute against cyber risks [35]. Cybersecurity readiness depends on the organization's ability to translate the learning from incidents into structural changes [18]. The feedback system is persistent, which enables

modification of the policies and technical defenses [26]. Learning-oriented organizations thus are better placed to be better equipped in the uncertain digital environments.

The other theoretical approach to cybersecurity readiness is the socio-technical systems theory. This model puts emphasis on the interdependence between the human actors and the technological infrastructure. It has been found that, in most cases, cybersecurity failures are largely attributed to the lack of congruence between systems and individuals [10]. The socio-technical theory assumes that effective readiness should entail a coordination of technical protection and human activities [33]. Organizations should also come up with systems that facilitate safe decision-making as opposed to merely using enforcement [25]. Balanced integration is also used to ensure that technology complements human capacity.

The central contribution of the organizational culture to the outcomes of cybersecurity is also explained by the socio-technical theory. Culture determines employees' interpretation and adherence to security policies. It has been shown that security-sensitive cultures minimize insider-related vulnerabilities [16]. Protective practices [28] are upheld through shared values. Trust and cooperation are enhanced by cultural alignment when dealing with incident response [38]. Those institutions that integrate cybersecurity into their organizational identity achieve better readiness outcomes.

Another theory relevant to explaining cybersecurity readiness is the resource-based theory. This theory considers organizational capabilities as a strategic resource that creates competitive advantage. The conceptualization of cybersecurity readiness may be in the form of value, uncommon, and not easily reproducible [19]. Cybersecurity infrastructure investments within institutions build up protective resources that cannot easily be duplicated by competitors [29]. Resource allocation is strategic and improves resilience to changes in threats [15]. Cybersecurity is thus an investment in organizations that is long-term.

The institutional theory also explains why cybersecurity readiness frameworks are adopted in organizations. Security behavior is affected by external forces of regulators, partners, and industry standards. According to research, the incentives that regulate expectations lead to readiness investment [22]. Ethics within the organization influence the perception of cybersecurity responsibility [27]. Conformity demands promote the use of a formal readiness framework [32]. External legitimacy is intended to serve as a driving force for security investment.

Another point emphasized by institutional theory is the role of legitimacy in terms of stakeholder trust. Companies should show a willingness to be credible in online markets. There is an indication that the observable cybersecurity resources strengthen reputation [11]. Stakeholders also attach meaning to readiness, viewing it as an indication of organizational reliability [24]. Cybersecurity governance entails long-term investment, which is strengthened by public accountability [34]. Institutional survival is thus related to cybersecurity performance through legitimacy.

In short, organizational cybersecurity readiness is grounded in dynamic capability, socio-technical, resource-based, and institutional theoretical perspectives. All of these frameworks describe how organizations develop, maintain, and legitimize cybersecurity capabilities. The theories focus on adaptation, integration, strategic resources and external pressures. They all constitute a broad prism through which readiness in complex environments can be comprehended. Theoretical justification guarantees that cybersecurity readiness is approached as a dynamic organizational system and not a technical problem.

2.9 Empirical Review

There is empirical research on the readiness of organizational cybersecurity that has more often been aimed at determining the drivers of successful readiness. Most of the literature has highlighted the fact that organizational behavior and governance systems play a significant role in determining readiness to

cybersecurity. Quantitative studies indicate that universities that have established security systems face less serious cyber-attacks [14]. Experimental data show that organized cybersecurity programs correlate with enhanced operational resilience [33]. Researchers have noted that readiness has a positive relationship with coordinated management practices [34]. These findings indicate the applicability of organizational systems in influencing the security outcomes.

Cybersecurity training of the staff has been subject to a lot of examination as a measure of readiness. Empirical research data would support the fact that awareness and susceptibility to social engineering attacks decline with the use of training. Survey-based research has indicated that organizations that engage in training periodically have higher readiness scores [10]. It is also confirmed through experimental work that phishing exercises run in simulation make employees more alert [36]. Long-term behavioral change has been observed in studies that have implemented long-term training [37]. These results advocate the relevance of education as one of the central defense mechanisms.

Another area that has had much empirical analysis is security policy enforcement. It has been proposed that organizations that are strict in their policy implementation have reduced incidences of internal security breaches. Studies that apply compliance principles have shown that consistent behavior is reinforced by predictable enforcement [18]. The cross-industrial analyses reveal that stronger enforcement structures are associated with enhanced incident reporting [35]. Companies that have effective disciplinary systems attain greater compliance amongst employees [13]. The implementation of policy thus acts as a stabilizer in its operation.

Empirical support for management support as the key determinant of cybersecurity success has been demonstrated. Leadership engagement affects funding, culture and strategic alignment. Research indicates that the higher the level of cybersecurity maturity, the higher the executive sponsorship [22]. Companies that have dynamic leadership management invest more money in protection procedures [23]. Empirical models indicate that managerial engagement predicts greater employee engagement in security programs [12]. The institutional readiness patterns are influenced by leadership commitment.

The empirical literature has also examined the availability of cybersecurity tools. Technical infrastructure directly affects the process of identifying and responding to threats within an organization. It has been shown that institutions with sophisticated monitoring systems have fewer long-term breaches [20]. Evidence-based research associates measures of technological investment and recovery performance [24]. Companies that have implemented combined security systems report better situational awareness [26]. Technology thus serves as a facilitator of operational defense.

Another dimension of readiness that is empirically validated is incident response planning. Studies indicate that companies that have a written code of responding to cyber-attacks recover quicker. Case analysis indicates structured response frameworks minimize the downtime of operations [31]. Experiments with simulation show that coordination in prepared teams is improved [25]. The results of the empirical assessments prove the strengthening of the crisis management abilities in the result of rehearsal exercises [11]. Planning will bring theoretical readiness to actual performance.

Empirical models have proposed that cybersecurity readiness arises from the interplay of various organizational factors. Multivariate results indicate that training, governance, technology and leadership are all predictors of readiness levels. Structural equation modelling research demonstrates that these variables are mutually supportive [28]. Cross-sectional surveys have proved that readiness is best achieved through balanced investment across dimensions [27]. The disproportionate vulnerability experienced is in institutions that do not pay attention to any element [32]. Systemic integration is therefore necessary in readiness.

To conclude, the empirical literature provides strong evidence that organizational cybersecurity readiness is multidimensional and measurable. The significance of training, policy enforcement, management support, technological infrastructure, and incident response planning is always proven in studies. By applying evidence-based methods, organizations can create more effective cybersecurity frameworks.

The summary of previous empirical studies is presented in Table 1.

Table 1: Summary of empirical studies on cybersecurity readiness.

Author(s)	Methodology	Key Variables	Sample/Context	Key Findings
[10]	Survey (Quantitative)	Employee training, awareness	Organizational employees	Regular cybersecurity training significantly improves awareness and reduces vulnerability to social engineering attacks.
[18]	Cross-sectional survey	Policy enforcement, governance	Multi-sector organizations	Strong policy enforcement is positively associated with compliance and reduced internal security breaches.
[22]	Empirical regression analysis	Management support, leadership	Corporate organizations	Executive involvement significantly predicts cybersecurity maturity and resource allocation.
[20]	Quantitative study	Technological infrastructure	IT-dependent firms	Availability of cybersecurity tools enhances threat detection and operational continuity.
[24]	Survey + statistical modeling	Incident response planning	Organizations with security frameworks	Organizations with structured response plans recover faster from cyber incidents.
[23]	Survey research	Training, management support	Mixed workforce	Combined human and managerial factors significantly improve cybersecurity readiness.
[34]	Cross-sectional analysis	Integrated cybersecurity factors	Industry-wide	Cybersecurity readiness is best explained through a combination of governance, training, and technology.
[37]	Experimental/ Simulation study	Training, response capability	Organizational teams	Simulation-based training improves incident detection and response effectiveness.
[32]	Multivariate analysis	Organizational systems	Multi-sector sample	Cybersecurity readiness is a multidimensional construct influenced by interdependent factors.

3 Methods

This chapter discusses the research design used to study the factors affecting organisational cybersecurity readiness. It explains the research design, sampling method, data collection, and analysis techniques used to test the hypotheses. The purpose is to provide an overview of the research process to ensure transparency, validity, and replicability.

3.1 Research Design

This research was based on the quantitative cross-sectional survey research design to focus on examining the organizational factors that affect cybersecurity readiness. The quantitative method was correct as the purpose of the study was to quantify the relationships between variables and test hypotheses with the help of statistical methods. The quantitative designs make it possible to objectively measure perceptions and behaviors, that is, to convert them into numerical values that can be represented in a statistical form. Cross-sectional survey designs have been widely applied in cybersecurity and organizational research to examine relationships among variables and provide empirical evidence on organizational phenomena. The study used structured measurement to reduce subjectivity, thereby increasing reproducibility.

The survey design was cross-sectional, which entailed collecting data at a single point in time and on a specific population. Cross-sectional studies are also useful where the researcher wants to measure the current conditions of an organization instead of making long-term measurements. This design would enable the researcher to obtain a picture of the cybersecurity readiness and its contributing variables among the participating organizations. Past research has demonstrated that cross-sectional techniques can be effective for assessing institutional readiness and governance practices [27,31]. The technique is also affordable and allows the simultaneous analysis of multiple variables.

The questionnaire was well-designed to facilitate the same data-gathering process for all respondents. The participants were all asked the same questions in the questionnaire, making the comparison standardized. Measurement bias is minimized through consistency in data collection, thereby enhancing validity in the quantitative research [25]. The design facilitated hypothesis testing by coming up with structured numerical datasets. This approach to the study offered a secure foundation for statistical inference and interpretation.

3.2 Study Population and Sampling

The target population was employees of organizations that depend heavily on digital information systems and network infrastructure. These workers engage with the cybersecurity tools, policies and operational procedures directly in their day-to-day activities. Their experiences can help in giving a good insight into organizational readiness. Having both technical and non-technical staff represented meant that there was a representation of different organizational roles. It has been found that behavior influences cybersecurity readiness at all levels of employees, not just in technical departments [33].

Participants were chosen using a simple random sampling method on the available population. Simple random sampling ensures equal selection probabilities and minimizes sampling bias. The method enhances the representativeness of the sample and external validity. It is commonly recommended in organizational survey research that random selection helps avoid systematic exclusion of subgroups [16,23]. The sampling frame consisted of the list of employees, and respondents were selected randomly.

The sample size of 230 respondents was determined to be adequate to conduct multivariate statistical analysis. The adequate sample size is essential to the statistical power. Empirical studies suggest that sample sizes must exceed 200 to conduct trustworthy research on organizations [15,28]. The selected sample fit these criteria and enabled the test of hypotheses in a strong manner. The determination of the sample was based on the formula with which Yamane (1967) advises to determine the sample in survey research:

Yamane's (1967) formula is used to determine the sample size:

$$n = N/(1 + N(e)^{\wedge}2)$$

where:

n = sample size

N = population size

e = margin of error (0.05)

Assuming a population (N) of 541 employees:

$n = 541/(1 + 541(0.05)^{\wedge} 2)$

$n = 541/(1 + 541 \times 0.0025)$

$n = 541/(1 + 1.3525)$

$n = 541/2.3525$

$n \approx 230$

Therefore, the calculated sample size is approximately 230 participants.

3.3 Data Collection Instrument and Procedure

The data to be used in this study were gathered with the help of a structured questionnaire, which is specifically created to assess the level of organizational cybersecurity readiness and factors that determine it. Quantitative research. Structured questionnaires are popular in quantitative studies as a useful instrument for creating standardized, comparable data from large groups of respondents. The tool was created based on existing cybersecurity models and previous empirical research on security behavior in organizations. The structured items provided a measure of consistency in measuring and reduced bias during the data collection by the researcher. In survey research, standardization is important because it enables the researcher to interpret questions consistently across participants and to apply reliable statistical analysis [10,18].

The questionnaire was divided into several blocks related to the study variables: employee training in cybersecurity, enactment of security policies, management support, access to cybersecurity tools, incident response planning, and general organizational readiness. The different dimensions of the concept were measured using multiple statements per construct. The use of multi-item measurement in social science research is suggested to increase both reliability and minimize measurement error [23]. The questionnaire was sent electronically so that many people can participate in it and the data can be captured easily. This is because electronic surveys eliminate the possibility of transcription error, enable automatic summation of responses, and enhance the accuracy of data [27].

The five-point Likert scale, commonly used to measure perceptions and attitudes in organizational studies, was used to collect responses. The answers were on a scale of:

1—Strongly Disagree

2—Disagree

3—Neutral

4—Agree

5—Strongly Agree

The Likert scale provides respondents with an opportunity to respond to a question with differing levels of agreement, thus yielding ordinal data that can be summed into continuous indices for use in statistical modelling. This has been applied best in cybersecurity research in which perceptions and behavioral inclinations have to be measured [33]. The scale offered enough sensitivity to identify the differences between respondents and at the same time was easy to use and interpret.

The questionnaire was pilot tested with a small group of participants before its full implementation to determine its clarity and structure. Johnson (2013) indicates that pilot testing is an essential step in instrument validation, as it helps uncover unclear wording and enhance internal consistency [25]. The feedback of pilot respondents was used to make amendments to the final questionnaire. The refinement process improved face validity and congruence with the research objectives.

3.4 Variable Measurement

The study used five independent variables and one dependent variable, measuring them with composite scales based on Likert items. The recommendation to use composite measurement is common since it represents a range of possible aspects of a construct and enhances reliability as opposed to single-item measurements [20]. All the variables had been operationalized with a number of statements reflecting theoretical dimensions that were recognized in previous literature on cybersecurity.

The independent variables were employee cybersecurity training, enforcement of the security policy, management support for cybersecurity, provision of cybersecurity tools and a cybersecurity incident response plan. All the independent variables were assessed using multi-item indices that indicated behavioral practices, organizational policies, leadership commitment, technical infrastructure and preparedness processes. The responses were summed to obtain an average score for each construct. Aggregation minimizes random measurement error and improves the stability of the variables [24].

The dependent variable was cybersecurity readiness at the organizational level. This construct is used to assess readiness, threat detection, response, and recovery after cyber-attack incidents. A multi-dimensional measure guaranteed that there was a broad representation of readiness as opposed to a technical definition. The previous studies highlight that readiness is not a specific characteristic but a compound ability of the organization [23]. The index scores were higher, denoting greater institutional readiness. All operational definitions were done to guarantee the correspondence between conceptual constructs and empirical measurement. The items were all directly related to theoretical underpinnings as covered in the literature review.

The information in this study was gathered by having a structured electronic questionnaire filled under an online survey platform (Google Forms). The online platform enabled highly effective distribution, the captured data was standardized, and transcription errors were minimal. The complete survey instrument used for data collection is provided in Appendix A.

A diversity of responses was achieved by spreading the questionnaire through several channels to ensure sufficient coverage. These platforms were email invitations, organizational communication networks, and professional social (e.g., LinkedIn and WhatsApp groups). The study was described to participants briefly, and a consent statement was presented before they could access the questionnaire.

The data were collected over four weeks (e.g., January–February 2026), which gave participants enough time to reply. To increase response rates, reminder messages were sent every now and then.

The questionnaire consisted mainly of closed-ended questions, with responses on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). This method was used to guarantee uniformity in answers and allow quantitative analysis. The tool targeted six constructs, which included employee training on cybersecurity, implementation of security policies, management support, provision of cybersecurity tools, incident response plan, and organizational cybersecurity readiness.

Inclusion and Exclusion Criteria:

Study participants were recruited when they:

Were workers of companies that use digital systems and network infrastructure.

Had fundamental exposure to organizational cybersecurity practices.

The subjects were not eligible when they:

✓ Had responses (participation) that had not been completed.
✓ Gave Inconsistent or invalid responses (e.g., straight-lining all items)
✓ Preprocessing and Cleaning of Data.

The dataset was pre-processed to attain quality and reliability before analysis. The following steps have been used:

✓ Deletion of blank answers.
✓ Duplicate entry screening.
✓ Determination and removal of patterns of response which signify low levels of engagement (e.g., same answer to all questions).
✓ Consistency of the Likert-scale responses in terms of coding and validation.

These processes ensured that the end dataset used in the analysis was accurate, complete, and had the statistical capacity to be tested.

3.5 Data Analysis Techniques

The data analysis was performed with the assistance of statistical software to ensure accuracy and reliability. The analysis involved descriptive statistics, reliability test, and Pearson's correlation. The selection of these methods followed the purpose of the research and the hypothesis-testing model. The first one was the descriptive statistics of frequencies, percentages, means and standard deviations. Descriptive analysis will give a summary of the characteristics of the participants and distributions of their responses. It helps researchers to discover trends, central tendencies, and variability in the data set [10]. The inferential results can be interpreted using descriptive statistics as well to put the results in context.

The second step involved a reliability test using Cronbach's alpha. Reliability testing determines the internal consistency of the items in a questionnaire within a construct. Cronbach's alpha is a popular measure of scale reliability that is applicable in organizational research. When the value is above 0.70, this is normally acceptable given that the items are intended to measure the same underlying concept [20]. The reliability tests helped to ascertain that the questionnaire yielded consistent measurements of the constructs.

3.6 Ethical Considerations

All the stages of the research were based on ethical principles. The questionnaire was completed by participants who provided informed consent. The consent statement described the study's purpose, voluntary participation, and the right to withdraw at any time without penalty. Open consent protocols help protect participants' autonomy and support ethical research practice [11].

The study was conducted with strict confidentiality. No personally identifiable information was collected, and responses were anonymized before analysis. The data were stored securely and were accessible only to the researcher. Protecting participants' privacy promotes honest responses and upholds ethical standards in organizational research.

This study involved an anonymous, voluntary questionnaire survey that posed minimal risk to participants and was conducted in accordance with the ethical guidelines of the authors' institution and the relevant ethical standards for research involving human participants.

3.7 Data Availability

Data created and examined in this research can be found in publicly available data to enhance transparency and reproducibility. Before sharing the data, all personally identifiable information was removed to preserve participants' confidentiality. The data consist of survey responses, variable codes and records that allow the analysis to be recreated.

3.8 Limitations of the Study

It is important to note that this study has some shortcomings despite its contributions. To begin with, the research design that was used was a cross-sectional study, which involves the collection of data at a single time. This leads to the inability to determine causal relationships between variables conclusively, and the results are indicative of relationships and not causation.

Second, the research was based on self-report, and it is prone to response bias, such as social desirability bias and subjectivity of survey questions. Even though the necessary steps were taken to provide anonymity and ensure honesty, one cannot be sure that those kinds of biases can be fully removed.

Moreover, the study's context is organization-specific, i.e., cybersecurity practices, governance structures, and resource availability would vary across organizations. That is why it must be taken into consideration when applying the findings to other settings. It is recommended that future studies use a longitudinal design, examine other organizational settings and employ more sophisticated modeling methods (e.g., structural equation modeling) to further support and apply them.

4 Results

The results of the statistical analysis carried out on the collected data are presented in this section. The results are presented in subsections according to the study objectives and hypotheses, which include demographic characteristics, descriptive statistics, reliability and inferential statistics. This section aims to present and interpret the data about organizational factors that affect cybersecurity readiness straightforwardly.

4.1 Demographic Characteristics

The demography of the respondents gives a valuable background on which the study results can be understood. There were 230 respondents, and most of them were females (62.6%) as opposed to males (37.4%). Such gender distribution indicates that female involvement in the surveyed organizations is strong and can be attributed to changing workforce trends in technologically oriented environments. A more gender-balanced sample reinforces the representativeness of perceptions of cybersecurity readiness, since the organizational security culture is shaped by employees' diverse experiences and opinions.

The Demographic characteristics of participants (N = 230) is presented in Table 2.

Regarding age, the greatest percentage of respondents were in the age group of 25–29 years (49.6%), then came those between the ages of 18–24 years (21.3%). The age group of 30–34 years was the most represented, with 19.1%, and 10.0 years was the least represented with 35 years and above. This means the workforce is mostly youth, implying high exposure to current digital applications and up-to-date cybersecurity measures. Organizational readiness, as demonstrated in Fig. 1, can be positively affected, as younger employees are usually more flexible in the face of technological change. Nevertheless, a younger population can also

mean insufficient professional experience in the long term, which can affect strategic decision-making on cybersecurity matters.

Table 2: Demographic characteristics of participants (N = 230).

Variable	Category	n	%
Gender	Male	86	37.4
	Female	144	62.6
Age	18–24 years	49	21.3
	25–29 years	114	49.6
	30–34 years	44	19.1
	35 years and above	23	10.0
Level of Education	High school	52	22.6
	Diploma/Certificate	116	50.4
	Bachelor's degree	39	17.0
	Others	23	10.0
Years of Experience in Cybersecurity	Less than 1 year	49	21.3
	1–3 years	110	47.8
	4–6 years	48	20.9
	More than 6 years	23	10.0

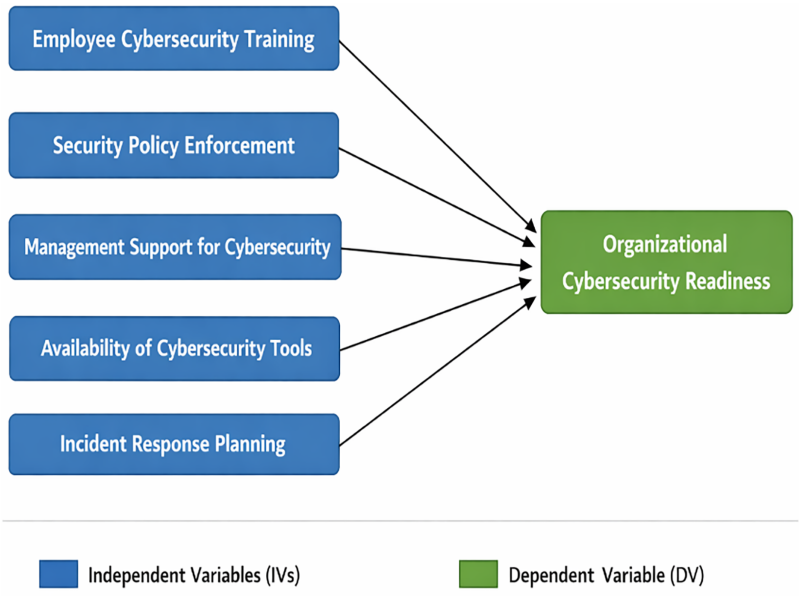

Figure 1: Determinants of organizational cybersecurity readiness.

The level of educational attainment indicated that the majority of the respondents had Diploma or Certificate education (50.4%), with 22.6% having high school education, 17.0% having bachelor's degree qualifications, and 10.0% having other qualifications. Such distribution means that the population is moderately

educated and highly vocationally oriented. Practical use of training may not depict high-level theoretical knowledge, yet it may depict more tangible cybersecurity.

Experience in cybersecurity also puts the sample in perspective. The respondents were identified to have experience of 1–3 years almost half (47.8%) and less than one year (21.3%). Respondents who had 4–6 years' experience made up 20.9 and only 10.0 years had over six years' experience. This means that most respondents are young professionals. Although the lack of experience can be an issue when it comes to dealing with advanced threats, it also implies a constantly growing workforce with cybersecurity competencies. In general, the demographic profile is characterized by a young and moderately educated and developing professional population, which should be taken into consideration when decoding organizational readiness outcomes. The distribution of gender among the participants is also supported by the pie chart in Fig. 2 below:

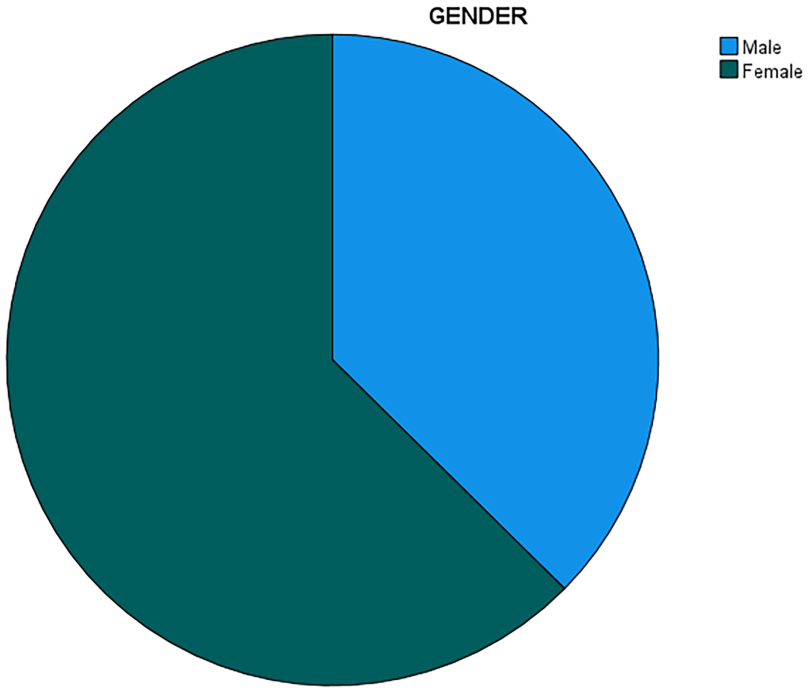

Figure 2: Participants' gender distribution.

4.2 Descriptive Statistics

The descriptive statistics reveal that the perceptions of cybersecurity readiness are mostly positive in all dimensions that were measured. The mean scores of all items were between 3.59 and 3.86 on a five-point Likert scale, which implies that the respondents were inclined to agree with the statements that the cybersecurity structures and practices exist in their organizations. The standard deviations were not too high (around 0.60–0.82), which means that responses were rather consistent, and there was no significant spread of the data around the mean.

The descriptive statistics are presented in Table 3.

The items concerned with cybersecurity training of employees showed statistically significant high means, and the best score (M = 3.86, SD = 0.81) was obtained regarding the statement that the company provides adequate training on the use of information systems safely. The respondents also accepted that cybersecurity training made them more skilled in detecting threats and more employee readiness in case of a cyber-attack. These results indicate that companies have realized the significance of lifelong learning as one

of the fundamental defensive measures. The fairly constant standard deviations suggest that the perceptions of respondents are shared, which means that the training practices are institutionalized and not individual.

Table 3: Descriptive statistics.

	N	Mean	Std. Deviation
Cybersecurity training of employees in my organization is a regular practice.	230	3.7348	0.72636
The offered training on cybersecurity enhances the skills of employees to detect cyber threats.	230	3.7087	0.74024
The company offers sufficient training in safe usage of information systems.	230	3.8565	0.81005
Training regarding cybersecurity is provided to both non-technical and technical personnel.	230	3.7652	0.81825
Training processes can increase the readiness of employees during cyber-attacks.	230	3.7348	0.72636
The organization has well-documented cybersecurity policies.	230	3.7174	0.81640
Staff management is conversant with cybersecurity policies.	230	3.7174	0.81640
The organization has a firm policy of cybersecurity.	230	3.5957	0.75748
Failure to adhere to the policies of cybersecurity is punishable.	230	3.6261	0.80891
Security policies help to determine day-to-day business that deals with information systems.	230	3.7449	0.60858
The top management puts emphasis on cybersecurity programs.	230	3.7217	0.62370
The management offers sufficient resources to cybersecurity activities.	230	3.7087	0.74024
There is a proactive role of leadership in cybersecurity awareness programs.	230	3.7870	0.74927
The management checks the cybersecurity posture of the organization on a regular basis.	230	3.7652	0.81825
The strategic planning of the organization incorporates cybersecurity.	230	3.7348	0.72636
The organization possesses sufficient cybersecurity platforms to secure its systems.	230	3.7174	0.81640
There is regular updating of firewalls and antivirus software.	230	3.7174	0.81640
There exist intrusion prevention or intrusion detection systems.	230	3.5957	0.75748
The cybersecurity tools are capable of identifying possible threats.	230	3.7174	0.81640
Employees are provided with the required cybersecurity technologies.	230	3.5957	0.75748
The company possesses a documented plan of cybersecurity incident response.	230	3.6261	0.80891

(Continued)

Table 3 (continued)

	N	Mean	Std. Deviation
There are procedures that employees know when there is an incident related to cyber.	230	3.7449	0.60858
There is a clear role and responsibility for incident response.	230	3.7217	0.62370
The incident response plan is drilled or exercised on a regular basis.	230	3.7087	0.74024
The organization is capable of reacting fast to cybersecurity attacks.	230	3.7870	0.74927
The company has been fully prepared to curb cyber-attacks.	230	3.7652	0.81825
The problem of cybersecurity is controlled in the organization.	230	3.7348	0.72636
The company is able to identify cyber threats in time.	230	3.7174	0.81640
Whenever such incidents as cyber are reported, they are handled efficiently.	230	3.7174	0.81640
On the whole, the organization has a great extent of cybersecurity readiness.	230	3.7130	0.81755
Valid N (listwise)	230		

It was also the same with responses on policy enforcement as far as security is concerned. The majority of the participants concurred that their organizations had written down their cybersecurity policies and they were aware that their policies were used in the information system's day-to-day activities. Nevertheless, there are some slight differences in the means of the statements about policy firmness and punishment for not obeying the requirements, which indicate that the enforcement intensity is not uniform. This can be interpreted to mean that there are policies, but there may be variation in terms of implementing the policies at different departments or at different levels within an organization.

Management support measures had a high level of agreement, especially on the involvement of leadership in awareness programs and frequent review of the cybersecurity posture. Such findings suggest that executive engagement is positively perceived by the respondents as being active and visible. Similarly, the results under items related to the availability of cybersecurity tools indicate that organizations already have the necessary defensive infrastructure, but the scores of intrusion detection systems are slightly lower, which implies the possibility of enhancing advanced technical features.

Lastly, items that assessed incident response planning and general readiness indicated that there were positive perceptions towards readiness, ability to respond quickly, and effective management of incidents. The mean score of preparation of organization (M = 3.71) shows moderate-high organizational readiness. Taken together, the descriptive statistics have made the picture of active organizations developing cybersecurity capacity, though some spheres of operation could use more effective enforcement and investment in technology.

4.3 Reliability and Validity Results

The reliability test generated Cronbach's alpha of 0.964 on the 30 questionnaire items, meaning that the internal consistency was extremely high. The alpha value of more than 0.70 is typical of a research study in

the social sciences, whereas the alpha value of more than 0.90 is associated with high reliability. Thus, the coefficient received indicates that the measuring tool is quite stable and the items always measure the same underlying constructs concerning organizational.

The reliability results are presented in Table 4.

Table 4: Cronbach's reliability test.

Reliability Statistics	
Cronbach's Alpha	**N of Items**
0.964	30

4.4 Pearson's Correlation

The results of the correlation show that positive correlations between all the variables of the study are strong and statistically significant ($p < 0.01$) and prove that organizational cybersecurity readiness is directly connected to its main determinants. The training of employees on cybersecurity is significantly correlated with readiness (r = 0.742), which suggests that readiness is likely to be higher in organizations that invest in employee capacity building. Training increases awareness and compliance in the behavior of employees and decreases vulnerabilities of human nature. Previous research also highlights workforce education as one of the key foundations of cybersecurity resilience and a direct contributor to threat detection capacity [23,27].

The Pearson correlation results are presented in Table 5.

Table 5: Pearson's correlation on the relationship between different variables.

		Employee Cybersecurity Training	Security Policy Enforcement	Management Support for Cybersecurity	Availability of Cybersecurity Tools	Incident Response Planning	Organizational Cybersecurity Readiness
Employee Cybersecurity Training	Pearson Correlation	1	0.535**	0.918**	0.379**	0.794**	0.742**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000
	N	230	230	230	230	230	230
Security Policy Enforcement	Pearson Correlation	0.535**	1	0.678**	0.937**	0.805**	0.887**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000
	N	230	230	230	230	230	230
Management Support For Cybersecurity	Pearson Correlation	0.918**	0.678**	1	0.521**	0.929**	0.859**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000
	N	230	230	230	230	230	230
Availability Of Cybersecurity Tools	Pearson Correlation	0.379**	0.937**	0.521**	1	0.604**	0.835**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000
	N	230	230	230	230	230	230

(Continued)

Table 5 (continued)

		Employee Cybersecurity Training	Security Policy Enforcement	Management Support for Cybersecurity	Availability of Cybersecurity Tools	Incident Response Planning	Organizational Cybersecurity Readiness
Incident Response Planning	Pearson Correlation	0.794**	0.805**	0.929**	0.604**	1	0.829**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000
	N	230	230	230	230	230	230
Organizational Cybersecurity Readiness	Pearson Correlation	0.742**	0.887**	0.859**	0.835**	0.829**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	
	N	230	230	230	230	230	230

Note: **Correlation is significant at the 0.01 level (2-tailed).

Security policy enforcement shows an even stronger association with readiness (r = 0.887), underscoring the importance of formal governance structures. Well-defined policies establish standardized security behavior and minimize operational uncertainty. The studies show that the more stringent the cybersecurity policies are in organizations, the greater the institutional maturity and the defensive posture [35,37]. Policies are a continuation of strategy to practice and therefore play an important role in the protection of an organization.

Ready is also strongly associated with management support (r = 0.859), which also demonstrates the strategic value of leadership in the cybersecurity culture. Executive commitment affects how funding is made, accountability mechanisms, and priorities in security initiatives. It is always shown in the literature that engagement of leadership in the implementation of cybersecurity is a deciding factor in success [34,39].

Likewise, the relationships of readiness with the availability of cybersecurity tools (r = 0.835) and incident response planning (r = 0.829) are high. Readiness planning and technological infrastructure facilitate quick reaction and restoration of cyber-incidents. Researchers state that the best cybersecurity solution arises out of the combination of human, procedural, and technical protection and not a single-level intervention [25,32]. All these findings are consistent with the multidimensionality of organizational cybersecurity readiness.

4.5 Hypotheses Testing

The hypothesis testing results indicate that all five proposed hypotheses were supported, as each independent variable exhibited a positive and statistically significant relationship with organizational cybersecurity readiness ($p < 0.001$). As presented in Table 6, these findings confirm that strengthening organizational, technical, and human-related cybersecurity practices significantly enhances overall organizational cybersecurity readiness.

Table 6: Conclusions on hypotheses.

Hypothesis	Relationship Tested	r-Value	*p*-Value	Decision
H1	Employee Cybersecurity Training → Organizational Cybersecurity Readiness	0.742	0.000	Supported
H2	Security Policy Enforcement → Organizational Cybersecurity Readiness	0.887	0.000	Supported

(Continued)

Table 6 (continued)

Hypothesis	Relationship Tested	r-Value	*p*-Value	Decision
H3	Management Support → Organizational Cybersecurity Readiness	0.859	0.000	Supported
H4	Availability of Cybersecurity Tools → Organizational Cybersecurity Readiness	0.835	0.000	Supported
H5	Incident Response Planning → Organizational Cybersecurity Readiness	0.829	0.000	Supported

5 Findings, Limitations, and Future Work

This chapter discusses the findings of this research and their implications with regard to the relevant literature and theory. It describes the findings' contribution to the understanding of organisational cybersecurity readiness and their value to organisations.

5.1 Key Findings

A quantitative analysis of the factors shaping cybersecurity readiness was conducted. It shows that cybersecurity training, security policy enforcement, management support, cybersecurity tool availability and incident response planning are positively associated with cybersecurity readiness. Particularly, security policy enforcement and management support are the most important predictors, suggesting that governance and leadership play a critical role in enhancing cybersecurity readiness. This research supports the notion that cybersecurity readiness is a multifaceted construct shaped by the interplay of human, technical, and organisational factors.

5.2 Interpretation of Findings and Comparison with Previous Studies

The results of this research show that organizational cybersecurity readiness is strongly and positively connected with internal structural and behavioral aspects. The outcomes of the Pearson correlation reveal that the correlation of each of the investigated variables with cybersecurity readiness is statistically significant, which means that readiness is not a chance occurrence but a systematic relationship between the variables and the major dimensions of the organization. This implies that cybersecurity readiness must be regarded as an organizational potential integrated into governance frameworks, people, and technologies instead of being a technical process [32].

One of the most positive relationships between security policy enforcement and organizational readiness for cybersecurity was observed. This observation means that organizations that have developed policies that are clear and have implemented them religiously are more likely to show increased levels of readiness. Efficient execution of the policies can make cybersecurity more than an abstract notion and make it an orderly and functioning practice. This is consistent with previous research that has found institutionalized policy frameworks to be key to attaining cybersecurity maturity [40]. Policies thus play a vital role as a critical link between strategic intent and operational security practices in day-to-day operations.

Cybersecurity management support similarly reported a positive and high direction relationship with organizational readiness. This shows that the level of commitment of a leader relates closely to the level of preparation. By ensuring the top management takes an active lead in emphasizing cybersecurity, it impacts the organization by making it a priority within the organization, shaping the allocation of resources,

and holding people accountable. The observation aligns with the current body of knowledge that has demonstrated a positive link between leadership participation and the resilience of an organization alongside the culture of security [37,41]. The involvement of executives will ensure that cybersecurity is incorporated into their strategic decision-making and not restricted to technical areas.

The training on employee cybersecurity was also revealed to have a high positive correlation with cybersecurity readiness, which, again, stresses the necessity to develop human capital. The employees are dual actors and can be both weak spots and active lines of defense in organizational systems. The correlation is rather high, suggesting that the higher the readiness rates in organizations that invest in continuous training, the more likely it is to reach the highest levels. This improves earlier studies that highlight the need to establish sustainable cybersecurity defense as one that greatly depends on human-based interventions and behavioral awareness [42]. Training helps improve employees' ability to detect and respond to threats such as phishing and social engineering attacks.

Organizational readiness also demonstrated a strong, positive relationship with cybersecurity tools. It means that technological infrastructure is an important facilitator of cybersecurity readiness. Firewalls, intrusion detection systems, and monitoring platforms can help to increase threat detection and response. Nevertheless, in line with the earlier research, technology does not suffice to be effective unless it is properly incorporated into its organizational procedures and human competence [37,43]. This further justifies the necessity of harmonization between technical investments and governance structures.

The cybersecurity readiness was also strongly correlated with incident response planning, which emphasizes the role of readiness over prevention. Companies that have clear response systems are likely to have an increased degree of readiness, since they are in a better position to handle and recover after a cyber-attack. This is in line with already known facts that structured response planning can help organizations become more resilient and less vulnerable in case of a cyber crisis [43]. Readiness, however, does not entail only defense measures but also the ability to recover.

On the whole, these results align with previous research that conceptualizes cybersecurity readiness as a multidimensional variable dependent on interrelated organizational factors [37]. The strong, robust correlations among the variables confirm that cybersecurity readiness is the outcome of the interaction among leadership, governance, human behavior, and technological infrastructure. Other interdependence patterns have been noted to be similar across comparative industry studies, further attesting to the strength of these findings [44].

In addition, the high interrelationships between the independent variables indicate that cybersecurity functions are not independent parts but a unitary system. Enhancing a single aspect, such as training or enforcing a policy, is likely to strengthen other aspects of readiness, creating a chain reaction of increased readiness. This observation supports the systems-oriented approaches that contend that organizational resilience is gained by integrative and comprehensive initiatives as opposed to independent ones [45]. As a result, cybersecurity maturity can be described as the coordinated advancement across various areas of organizations.

5.3 Theoretical and Practical Implications for Organizations

Theoretically, the results support the socio-technical systems theory in cybersecurity. The findings have shown that readiness is not exclusively technological but a result of relations among human, structural, and technical subsystems. This substantiates the theoretical models that consider organizations as complex adaptive systems [46]. The topic of cybersecurity should thus be viewed from an interdisciplinary perspective.

The research also contributes to organizational readiness theory by extending it to digital risk management. Conventional readiness models are change management-based or crisis response-based. Current data

indicate that cybersecurity readiness has the same structural principles. Leadership convergence, procedural precision, and workforce capability create organizational readiness [47]. Cybersecurity may, therefore, be presented as a readiness field.

The other theoretical implication is institutional theory. The high power of policy enforcement indicates that cybersecurity behavior is determined by formal rules and norms. There are institutional pressures that facilitate standardization and compliance. Security practices become internalized in the organization when policies are made part and parcel of the way of life. Institutional research highlights the strength of organized governance in controlling behavior [48]. Security culture develops through institutional reinforcement.

In practice, the findings provide practical advice to organizations. Firstly, cybersecurity policies must be a priority in their development and ongoing updating. The policies should be made easy to understand and backed up by enforcement. Frequent compliance reviews and audits are effective. Organizations that fail to maintain policies are likely to experience inconsistency and vulnerability.

Second, the executive leadership should be able to demonstrate visible support for cybersecurity efforts. Examples of activities that should be performed by leaders include budget allocation, involvement in awareness initiatives, and the incorporation of cybersecurity indicators into performance management activities. An apparent dedication creates a sense of responsibility. Employees perceive leadership behavior as an indicator of organizational priorities.

Third, employee training should not be a one-time event. Training should be updated to keep up with new threats. Exercises and simulations are better at enhancing retention through scenarios. The awareness programs must involve all organizational positions, not just IT staff. A trained workforce can be viewed as a proactive defensive barrier.

Fourth, cybersecurity equipment needs to be strategic and coordinated. The tools must align with an organization's risk profile. Periodic reviews and evaluations are necessary. The policy should be enhanced by technology in terms of enforcing and training. Maximal protection is achieved through integration.

Lastly, institutionalization of incident response planning is required. The companies are expected to have documented procedures and perform regular drills. Strict role allocation enhances response speed. Resilience is enhanced through learning experiences of simulated incidents. Well-equipped organizations will heal soon and have fewer long-term effects.

To recap, cybersecurity readiness is enabled by long-term organizational consistency, not quick fixes. The results indicate the relevance of coordinated governance, commitment of leaders, development of the workforce, and technical capability. Companies that fear dynamic digital threats are better positioned to embrace cybersecurity as a strategic discipline.

5.4 Broader Organizational Meaning and Strategic Implications

In addition to the statistical ties found in the research, the results indicate that the concept of cybersecurity readiness should be regarded as a strategic management function rather than a technical issue. Companies that elevate cybersecurity to the executive level are also more likely to embed protective practices across operational levels, ensuring continuity and alignment. Cybersecurity is becoming a component of institutional sustainability and a risk management pillar in strategic governance frameworks [32]. This perspective reverses the concept of the preparatory phase as long-term organizational investments.

The interrelationship between the predictors signals the fact that cybersecurity readiness is a reinforcement process in the organizational systems. Leadership commitment increases the implementation of policies and thus the degree of employee conformity and the effectiveness of the training programs. The

systems-based research proves that resilience is a result of the agreement between the work of governance, behavior, and infrastructure [40]. Dividend investments do not always lead to long-term defense effects.

The other significant implication concerns the contribution of organizational culture to the development of secure behavior. By constantly reinforcing expectations regarding cybersecurity, the employees will develop the habits of protection as an integral part of their work processes. Cultural normalization reduces the need for surveillance and enhances voluntary adherence to security measures. Research on organizational behavior demonstrates how cultural embedding is the key to the sustainable performance of cybersecurity [43]. Culture makes cybersecurity not a requirement, but rather a sense of identity.

The results also indicate the importance of learning-oriented organizations. There is adaptive capacity within the institution, which regularly assesses its posture, conducts drills, and revises policies in response to changing threats. Adaptive learning can enable organizations to foresee vulnerabilities to the occurrence of incidents. Studies have highlighted that lifelong learning is a key difference between the resilient and the reactive digital institutions [42]. Static approaches cannot match dynamically evolving threats.

As a risk management approach, readiness acts as a shock absorber of operational impact. Incident response planning minimizes uncertainty by providing systematic channels in crisis situations. Companies that have a disaster response procedure rehearsed recover more quickly and cause less damage in the long run. In the literature on risk governance, readiness is always one of the key factors of institutional resilience [43]. The response capacity is organized to turn the disruption into an organizational risk.

The findings also indicate that resource constraints do not prevent organizations from achieving preparedness. Numerous factors identified in this study, such as leadership involvement and policy transparency, rely more on organizational discipline than on financial size. Smaller institutions can reinforce preparedness through governing and behavioral congruency. The availability of cybersecurity in research has proved that efficient measures can be applied to protect a system through well-organized management methods [45]. Technology is not always sophisticated.

The paper also stresses collective responsibility. The culture of cybersecurity is also promoted when it is not concentrated on the IT departments but through the departments that share it. Sharing of ownership fosters faster discovery and immediate response. According to organizational security studies, distributed accountability is a resilience multiplier [46]. Multi-layered defense is achieved through shared responsibility.

The other strategic implications are compliance with regulations and stakeholder trust. A firm that is well prepared in cybersecurity will be more likely to meet evolving regulatory demands. Ready is a predictor of institutional reliability and risk perception. Governance scholarship is linked to cybersecurity maturity, stakeholder trust, and competitive legitimacy [47]. Reliance on apparent security capability is becoming more reliable.

It must also incorporate cybersecurity in the overall organizational plan. Security planning should overlap with business continuity, human resource development, and operational management. Communication among functions reduces the blind spots and increases readiness. It is proven that efficiency and resilience improve with integrated governance structures [48]. Cybersecurity must become a priority within the organization.

Finally, the findings highlight how the online space is transforming leadership. To mobilize strategic action, modern executives must transform technical risk into strategic action. Leadership effectiveness is now part of online literacy and digital cybersecurity governance. The literature on leadership focuses on the influence of executives who can help organizations emerge from technological uncertainty [49]. Adaptive capacity is determined by strategic leadership. When combined, these implications support the idea that cybersecurity readiness is a dynamic capacity of an organization. Long-term resilience is characterized by

the interaction of governance, culture, learning, and leadership. Organizations that make cybersecurity a strategic discipline develop structures capable of absorbing disruption. The modern resilience theory considers readiness as an ongoing process of adaptation [50]. The willingness to read thus makes it a characteristic of contemporary institutions.

6 Findings, Limitations, and Future Work

6.1 Summary of Key Findings

The Pearson correlation analysis provided valuable insights into the association between the independent variables and organizational cybersecurity readiness. The results suggest that the five organizational variables comprising employee cybersecurity training, security policy enforcement, management support, cybersecurity tools availability, and incident response planning are all positively related to cybersecurity readiness with significant and statistically significant correlations.

In particular, the relationship between employee cybersecurity training and organizational readiness was found to be strongly positive, indicating that ongoing training improves employees' ability to identify and respond to cyber threats. On the same note, when security policies were implemented, a strong correlation with readiness was observed, indicating that the more policies are well implemented, the greater the organization's cybersecurity readiness.

One of the strongest influences, with an extremely high positivity coefficient with cybersecurity readiness, was management support. This underscores the importance of leadership commitment in driving security initiatives, allocating resources, and fostering a culture of cybersecurity in organizations. Also, access to cybersecurity tools was closely linked to readiness regarding the significance of technological infrastructure for identifying and averting, as well as responding to, cyberattacks.

Cybersecurity readiness also had a strong positive relationship with incident response planning, meaning that organizations with established response procedures are better able to deal with and recover from cyberattacks.

On the whole, the outcomes of the correlation analysis indicate that cybersecurity readiness is a complex, multidimensional construct formed by related organizational, human, and technological factors. The robustness of the connections also indicates that improvements in any of the areas can greatly enhance the organization's overall cybersecurity readiness.

6.2 Cybersecurity Research Contributions

This research paper is relevant to the field of cybersecurity research because it empirically confirms a multidimensional organizational readiness model. Although there is significant literature on cybersecurity that focuses on the technical aspects of the issue, this study shows that organizational and managerial issues also play an important role. The results are associated with socio-technical approaches that perceive cybersecurity as a complex system of governance, culture, and technology.

The study also applies organizational readiness theory to cybersecurity. It shows that readiness for cyber threats is in line with crisis management and institutional resilience principles. The quantitative study of correlating leadership backing, policy implementation, training, and response preparation with measurable readiness outcomes provides a systematic foundation for prospective empirical research.

The other contribution is the possibility to demonstrate the interdependence among factors in organizational cybersecurity. The predictors do not act alone; they form a self-affirming network. This knowledge at the systems level extends to the development of a theoretical discussion of cybersecurity maturity and the role of integrated security governance.

6.3 Practical Recommendations

Based on the findings, several feasible recommendations can be provided on how organizations can better prepare for cybersecurity. First, businesses should aim to provide and establish cybersecurity policies. The policies are to be appropriately documented, made known to all employees, and updated periodically to reflect changes in emerging threats. This should be enforced through mechanisms that ensure they remain in charge and always remain in compliance.

Secondly, top management must be an advocate of cybersecurity measures. The presence of top management indicates that the organization is dedicated and encourages employee contributions. It is suggested that leaders allocate sufficient resources, incorporate cybersecurity into strategic planning, and inculcate a culture of shared accountability.

Third, companies ought to have constant employee training programs. They should be trained both technically and non-technically, and updated frequently to address emerging threats. There can be simulated drills and practical workshops to raise awareness and response power.

Fourth, technological investments must be presented in line with the organization's needs. Cybersecurity instruments will need ongoing maintenance, proper setup, and the ability to be incorporated into broader governance frameworks. Human and procedural controls should not be substituted by technology. Lastly, incident response planning should be institutionalized. Organizations should document procedures, limit roles, and conduct regular drills. Being prepared reduces the recovery period and the operational loss after the cyber-attack.

6.4 Methodological Limitations and Contextual Limitations

This research has several limitations, even though it makes some contributions. First, the study was cross-sectional, meaning it measured perceptions at a single point in time. Cybersecurity readiness is not static, and longitudinal research would provide a clearer picture of how preparedness evolves.

Second, the research was based on self-reported survey data. In structured questionnaires, standardized measurement is obtained; however, responses may be influenced by social desirability bias or subjective perceptions. Future analyses might be enhanced by using observational or mixed-method approaches.

Third, the sample was also confined to a given organizational setting and might not be representative of all industries and geographic regions. Cybersecurity settings across sectors vary, and situational factors may affect readiness variables. The findings should therefore be generalized carefully.

6.5 Future Study Recommendations

The work should be pursued in several important directions that future research should follow up on. Longitudinal studies can also examine changes in cybersecurity readiness in response to new threats, regulatory requirements, or restructuring. To understand the concepts of sustainability and adaptation, it is appropriate to observe readiness over time.

A mixed-method study, using surveys, interviews, or case studies, could help shed more light on organizational culture and decision-making practices. The qualitative data would be included alongside the quantitative data and would provide contextual information.

It would also be useful to conduct comparative research across industries and nations. Cybersecurity governance differs significantly across sectors and regulatory settings. Cross-context studies would be useful in determining universal principles and context-specific practices.

Another research area that must be presented in future studies is the impact of emerging technologies, including artificial intelligence, automation, and cloud infrastructure, on readiness development. With the

development of digital ecosystems, the model of organizational cybersecurity must also change. Lastly, researchers should examine the psychological and cultural aspects of cybersecurity behavior. Understanding employees' perceptions of risk, responsibility, and accountability may improve training and governance practices.

Acknowledgement: Not applicable.

Funding Statement: The author received no specific funding for this study.

Availability of Data and Materials: The dataset and SPSS analysis output supporting the findings of this study are provided as a research data file (see Supplementary Material) submitted with this manuscript. Additional information is available from the corresponding author on reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The author declares no conflicts of interest.

Supplementary Materials: The supplementary material is available online at https://www.techscience.com/doi/10.32604/jcs.2026.080111/s1.

Appendix A

Structured Questionnaire

Section A: Demographic Information

Tick (✓) or select the most appropriate option.

1. **Gender**

   □ Male □ Female □ Prefer not to say

2. **Age Group**

   □ Below 25 years
   □ 25–34 years
   □ 35–44 years
   □ 45–54 years
   □ 55 years and above

3. **Highest Level of Education**

   □ Diploma
   □ Bachelor's Degree
   □ Master's Degree
   □ Doctorate
   □ Other (Specify): _____

4. **Years of Work Experience**

   □ Less than 2 years
   □ 2–5 years
   □ 6–10 years
   □ Over 10 years

Section B: Enforcement of Security Policy

No.	Statement	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
1	The organization has well documented cybersecurity policies.	□	□	□	□	□
2	Staff management is conversant with cybersecurity policies.	□	□	□	□	□
3	The organization has a firm policy of cybersecurity.	□	□	□	□	□
4	Failure to adhere to the policies of cybersecurity is punishable.	□	□	□	□	□
5	Security policies help to determine day to day business that deals with information systems.	□	□	□	□	□

Section C: Management Supporting Cybersecurity

No.	Statement	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
1	The top management puts emphasis on cybersecurity programs.	□	□	□	□	□
2	The management offers sufficient resources to cybersecurity activities.	□	□	□	□	□
3	There is a proactive role of leadership in cybersecurity awareness programs.	□	□	□	□	□
4	The management checks the cybersecurity posture of organization on a regular basis.	□	□	□	□	□
5	The strategic planning of the organization incorporates cybersecurity.	□	□	□	□	□

Section D: Availability of Cybersecurity Tools

No.	Statement	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
1	The organization possesses sufficient cybersecurity platforms to secure its systems.	□	□	□	□	□
2	There is regular updating of firewalls and antivirus software.	□	□	□	□	□
3	There exist intrusion prevention or intrusion detection systems.	□	□	□	□	□
4	The cybersecurity tools are capable of identifying possible threats.	□	□	□	□	□
5	Employees are provided with the required cybersecurity technologies.	□	□	□	□	□

Section E: Incident Response Planning

No.	Statement	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
1	The company possesses a documented plan of cybersecurity incident response.	□	□	□	□	□
2	There are procedures that employees know when there is an incident related to cyber.	□	□	□	□	□
3	There is a clear role and responsibility of incident response.	□	□	□	□	□
4	The incident response plan is drilled or exercised on a regular basis.	□	□	□	□	□
5	The organization is capable of reacting fast to cybersecurity attacks.	□	□	□	□	□

Section F: Organizational Cybersecurity Readiness

No.	Statement	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
1	The company has been fully prepared to curb cyber attacks.	□	□	□	□	□
2	The problem of cybersecurity is controlled in the organization.	□	□	□	□	□
3	The company is able to identify cyber threats in time.	□	□	□	□	□
4	Whenever such incidences as cyber are reported, they are handled efficiently.	□	□	□	□	□
5	On the whole, the organization has a high extent of cybersecurity preparedness.	□	□	□	□	□

References

1. Stevens T. Knowledge in the grey zone: AI and cybersecurity. Digit War. 2020;1(1):164–70. doi:10.1057/s42984-020-00007-w.
2. Awan M, Alam A. Cybersecurity threats and defensive strategies for small and medium firms: a systematic mapping study. Adm Sci. 2025;15(12):481. doi:10.3390/admsci15120481.
3. Donepudi PK. Crossing point of artificial intelligence in cybersecurity. Am J Trade Policy. 2015;2(3):121–8. doi:10.18034/ajtp.v2i3.493.
4. Musser M, Garriott A. Machine learning and cybersecurity: hype and reality. Washington, DC, USA: Center for Security and Emerging Technology; 2021. doi:10.51593/2020CA004.
5. Abushark YB, Irshad Khan A, Alsolami F, Almalawi A, Mottahir Alam M, Agrawal A, et al. Cyber security analysis and evaluation for intrusion detection systems. Comput Mater Contin. 2022;72(1):1765–83. doi:10.32604/cmc.2022.025604.
6. Ijiga OM, Idoko IP, Ebiega GI, Olajide FI, Olatunde TI, Ukaegbu C. Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. Open Access Res J Sci Technol. 2024;11(1):1–4. doi:10.53022/oarjst.2024.11.1.0060.
7. Zhang S, Xie X, Xu Y. A brute-force black-box method to attack machine learning-based systems in cybersecurity. IEEE Access. 2020;8:128250–63. doi:10.1109/ACCESS.2020.3008433.
8. Sarker IH. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Ann Data Sci. 2023;10(6):1473–98. doi:10.1007/s40745-022-00444-2.
9. Zaman S, Alhazmi K, Aseeri MA, Ahmed MR, Khan RT, Kaiser MS, et al. Security threats and artificial intelligence based countermeasures for Internet of Things networks: a comprehensive survey. IEEE Access. 2021;9:94668–90. doi:10.1109/ACCESS.2021.3089681.
10. Shaukat K, Luo S, Varadharajan V, Hameed I, Chen S, Liu D, et al. Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies. 2020;13(10):2509. doi:10.3390/en13102509.
11. Kheruddin MS, Zuber MA, Radzai MM. Phishing attacks: unraveling tactics, threats, and defenses in the cybersecurity landscape. Preprint. 2024. doi:10.22541/au.170534654.48067877/v1.
12. Shojarazavi T, Barati H, Barati A. A wrapper method based on a modified two-step league championship algorithm for detecting botnets in IoT environments. Computing. 2022;104(8):1753–74. doi:10.1007/s00607-022-01070-9.

13. Ansari MF, Sharma PK, Dash B. Prevention of phishing attacks using AI-based cybersecurity awareness training. Int J Smart Sens Adhoc Netw. 2022:61–72. doi:10.47893/ijssan.2022.1221.
14. Ayoola VB, James UU, Idoko IP, Ijiga OM, Olola TM. Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. Global J Eng Technol Adv. 2024;20(3):94–117. doi:10.30574/gjeta.2024.20.3.0164.
15. Shojarazavi T, Hamid B, Barati A. A survey on botnet detection methods in the Internet of Things. Int J Smart Electr Eng. 2023;12(2):99–111.
16. Putra FPE, Ubaidi U, Zulfikri A, Arifin G, Ilhamsyah RM. Analysis of phishing attack trends, impacts and prevention methods: literature study. Brilliance. 2024;4(1):413–21. doi:10.47709/brilliance.v4i1.4357.
17. Iqbal F, Yusof ZB. Efficacy of cybersecurity awareness training in reducing phishing vulnerabilities in organizations. J Adv Cybersecur Sci Threat Intell Countermeas. 2024;8:10–21.
18. Okokpujie K, Kennedy CG, Nnodu K, Noma-Osaghae E. Cybersecurity awareness: investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (a case study of a Nigerian leading university). Int J Sustain Dev Plan. 2023;18(1):255–63. doi:10.18280/ijsdp.180127.
19. Waqas M, Hania A, Yahya F, Malik I. Enhancing cybersecurity: the crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks. Sage Open. 2023;13(4):21582440231217720. doi:10.1177/21582440231217720.
20. Pinto L. Assessing the relevance of cybersecurity training and policies to prevent and mitigate the impact of phishing attacks. J Internet Serv Inf Secur. 2022;12(4):23–38. doi:10.58346/jisis.2022.i4.002.
21. Savaş S, Karataş S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. Int Cybersecur Law Rev. 2022;3(1):7–34. doi:10.1365/s43439-021-00045-4.
22. Abrahams TO, Farayola OA, Kaggwa S, Uwaoma PU, Hassan AO, Dawodu SO. Cybersecurity awareness and education programs: a review of employee engagement and accountability. Comput Sci IT Res J. 2024;5(1):100–19. doi:10.51594/csitrj.v5i1.708.
23. Xu H, Wang S, Li N, Wang K, Zhao Y, Chen K, et al. Large language models for cyber security: a systematic literature review. ACM Trans Softw Eng Methodol. 2025:3769676. doi:10.1145/3769676.
24. Zhang J, Bu H, Wen H, Liu Y, Fei H, Xi R, et al. When LLMs meet cybersecurity: a systematic literature review. Cybersecurity. 2025;8(1):55. doi:10.1186/s42400-025-00361-w.
25. Fernandez De Arroyabe I, Arranz CFA, Arroyabe MF, Fernandez de Arroyabe JC. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: a UK survey for 2018 and 2019. Comput Secur. 2023;124(2):102954. doi:10.1016/j.cose.2022.102954.
26. Gernhardt D, Groš S, Gledec G. Innovating cyber defense with tactical simulators for management-level incident response. Information. 2025;16(5):398. doi:10.3390/info16050398.
27. Jada I, Mayayise TO. The impact of artificial intelligence on organisational cyber security: an outcome of a systematic literature review. Data Inf Manag. 2024;8(2):100063. doi:10.1016/j.dim.2023.100063.
28. Ghelani D. Cyber security, cyber threats, implications and future perspectives: a review. Am J Sci Eng Technol. 2022;3:12–9. doi:10.22541/au.166385207.73483369/v1.
29. Scherb C, Heitz LB, Grimberg F, Grieder H, Maurer M. A cyber attack simulation for teaching cybersecurity. EPiC Ser Comput. 2023;93:129–40. doi:10.29007/dkdw.
30. Abdullayeva F. Cyber resilience and cyber security issues of intelligent cloud computing systems. Results Control Optim. 2023;12(1):100268. doi:10.1016/j.rico.2023.100268.
31. Alqahtani MA. Factors affecting cybersecurity awareness among university students. Appl Sci. 2022;12(5):2589. doi:10.3390/app12052589.
32. Petcu I, Barbu DC. The new challenges of Romania's cyber security policy. Rom Cyber Secur J. 2022;4(1):57–67. doi:10.54851/v4i1y202207.
33. Safitra MF, Lubis M, Fakhrurroja H. Counterattacking cyber threats: a framework for the future of cybersecurity. Sustainability. 2023;15(18):13369. doi:10.3390/su151813369.

34. Sai S, Yashvardhan U, Chamola V, Sikdar B. Generative AI for cyber security: analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space. IEEE Access. 2024;12(4):53497–516. doi:10.1109/ACCESS.2024.3385107.
35. Admass WS, Munaye YY, Diro AA. Cyber security: state of the art, challenges and future directions. Cyber Secur Appl. 2024;2(1):100031. doi:10.1016/j.csa.2023.100031.
36. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023;12(6):1333. doi:10.3390/electronics12061333.
37. Safaei Pour M, Nader C, Friday K, Bou-Harb E. A comprehensive survey of recent Internet measurement techniques for cyber security. Comput Secur. 2023;128(5):103123. doi:10.1016/j.cose.2023.103123.
38. de Azambuja AJG, Plesker C, Schützer K, Anderl R, Schleich B, Almeida VR. Artificial intelligence-based cyber security in the context of industry 4.0—a survey. Electronics. 2023;12(8):1920. doi:10.3390/electronics12081920.
39. Yamin MM, Katt B. Modeling and executing cyber security exercise scenarios in cyber ranges. Comput Secur. 2022;116(1):102635. doi:10.1016/j.cose.2022.102635.
40. Lokare A, Bankar S, Mhaske P. Integrating cybersecurity frameworks into IT security: a comprehensive analysis of threat mitigation strategies and adaptive technologies. arXiv:2502.00651. 2025.
41. Cyber-security. Netw Secur. 2014;2014(1):4. doi:10.1016/s1353-4858(14)70003-0.
42. Horowitz BM, Lucero DS. System-aware cyber security: a systems engineering approach for enhancing cyber security. Insight. 2017;20(3):66–8. doi:10.1002/inst.12165.
43. Covarrubias JZL. Effective communication as a pillar of cybersecurity: managing incidents and crises in the digital era. J Risk Anal Crisis Response. 2025;15(2):34. doi:10.54560/jracr.v15i2.564.
44. Wazid M, Das AK, Chamola V, Park Y. Uniting cyber security and machine learning: advantages, challenges and future research. ICT Express. 2022;8(3):313–21. doi:10.1016/j.icte.2022.04.007.
45. Mohammed A. Protecting space assets: cybersecurity challenges and solutions for the final frontier. Balt J Eng Technol. 2023;2:55–61.
46. Chirra DR. AI-enabled cybersecurity solutions for protecting smart cities against emerging threats. Int J Adv Eng Technol Innov. 2021;1(2):237–54.
47. Department for Digital, Culture, Media and Sport. DCMS: cyber security breaches survey 2019. Netw Secur. 2019;2019(4):4. doi:10.1016/s1353-4858(19)30044-3.
48. Alsharif M, Mishra S, AlShehri M. Impact of human vulnerabilities on cybersecurity. Comput Syst Sci Eng. 2022;40(3):1153–66. doi:10.32604/csse.2022.019938.
49. Rademaker M. Assessing cyber security 2015. Inf Secur Int J. 2016;34:93–104. doi:10.11610/isij.3407.
50. Mersinas K, Bada M, Furnell S. Cybersecurity behavior change: a conceptualization of ethical principles for behavioral interventions. Comput Secur. 2025;148(12):104025. doi:10.1016/j.cose.2024.104025.