TURING LEDGER JOURNAL OF ENGINEERING & TECHNOLOGY

Information Security Culture and Organizational Cyber Resilience: The Mediating Role of Security Practices

Muhammad Arslan
Department of Computer Science, Information Technology University, Lahore, Pakistan

Muhammad Akbar
Department of Computer Science, Information Technology University, Lahore, Pakistan
Email: akbar.m54@gmai.com

Received: 07-03-2026
Revised: 29-03-2026
Accepted: 21-04-2026

Corresponding Author*:* Muhammad Akbar

ABSTRACT:

Organizations are now more reliant on interconnected information systems, making cybersecurity an integral part of organizational continuity and operational stability. While technical controls are a key aspect of traditional cybersecurity, organizational values, employee conduct, security policies, management dedication to security and regular application of security protocols are equally crucial. Information security culture can set shared expectations of what it means to act in a secure manner, how to deal with risks, whether or not to comply with policies, and whether or not to report incidents, and security practice can take these cultural expectations and turn them into concrete technical and organizational controls. This study focused on the relationship between information security culture and organizational cyber resilience, as well as a mediation effect of information security practices. A simulated cyber security research design that is controlled and a security-audit research design in an isolated virtual organizational network was used. Information security culture was materialized in the form of information security requirements of the organization, such as security policies, support of management, authentication requirements, access-control procedures, standards for patch-management, standards for backup, procedures for reporting of information security incidents, and mechanisms of compliance. Technical audits were performed on access privileges, network segmentation, endpoint protection, patching, logging, vulnerability management, backup procedures, incident response, authentication and security practices. A series of controlled cybersecurity scenarios were placed in the isolated environment and system logs were gathered to assess the time taken for detection, time for response, time for containment, time for recovery, availability of services, affected systems, ability to contain the threat and recovery of data. Organizations were assessed objectively with regard to their cyber resilience using these indicators. The following, mediation analysis utilizing bootstrapping, was then conducted to investigate the effect of whether security practices mediated the effect of information security culture on cyber resilience. The study offered a socio-technical approach to cybersecurity, making links between organization culture and seen behaviours on security and measurable security outcomes.

Keywords: information security culture, organizational cyber resilience, security practices, cybersecurity, incident response, security controls, information systems security.

INTRODUCTION:

The digitalisation of organizational activities has resulted in greater reliance on information systems, interconnected networks, cloud platforms, digital services and electronically stored information. Organizations have thus been targeted by a myriad of cyber security risks, such as unauthorized access, breach of credentials, malware, phishing attacks, ransomware, data breaches, and disruption of services. Organizations have found themselves unable to solely depend on the technical prevention methods due to the more complex nature of digital environments. Organizations also need to have the ability to identify security incidents, react to attacks, limit the damage, restore services, and gain from security failures. This more general capability has increasingly come to be linked with organizational cyber-resilience.

Cyber resilience is not just about cybersecurity, it is about ensuring an organization and its information systems remain resilient before, during and after disruptive cyber incidents. Linkov, et al., (2013) suggested that resilience be measured by measurable characteristics of a system, and highlighted the need for metrics to measure cyber-system resilience. Likewise, Linkov and Kott (2019) viewed cyber resilience as a multi-faceted phenomenon that enables systems to anticipate, resist, recover from, and adapt to negative cyber incidents. Organizational cyber resilience is not just about whether security controls are in place or not; it also involves the ability to react to the breach or subversion of security controls.

The social and organizational aspects of cybersecurity have begun to be studied in greater depth as technical controls take place within a social and organizational environment. Employees access and use information systems; adhere to or breach security protocols; access and/or maintain credentials; take action in response to questionable activity; report suspected incidents. So human behavior can impact organizational cybersecurity. AlHogail and Mirza (2014) argued that information security culture has an impact on the perception and execution of information-security related activities by organizational members. So, the information security culture can be defined as a community of values, beliefs, expectations, norms and practices related to the protection of information assets of an organization.

Creating a good information security culture can help mitigate human security risks. AlHogail (2015) created a framework for information security culture that included organizational, technological, human and environmental aspects, while recognizing the importance of ensuring that employee behaviors are in line with the management of information assets. In the same way, Da Veiga et al., (2020) showed that there are a number of organizational factors that are part of information security culture, such as management support, policies and procedures, awareness and organizational practices. The results showed that security culture is not simply the consequence of awareness training for employees, but a broader phenomenon in the organization.

Another aspect of the information security culture is shown by the level of security activity of employees and their adherence to the organization's regulations. Bulgurcu et al., (2010) showed that there was a correlation between information security awareness, attitude, normative beliefs, self-efficacy, and employees' intentions to follow information security policies. Siponen et al., (2014) also found that perceptions of security threats, attitudes toward compliance, social norms, and self-efficacy affected employees' intentions to comply with the organizational security policy. The results indicate that organizational security could not be accomplished by implementing technical measures alone as the employees' choices and actions affect security's effectiveness.

Organizational security decision making can also be impacted by information security culture. Parsons et al., (2015) discovered that there exists a positive correlation between the organizational information security culture and information security decision making. In their results, they indicated that the overall

organizational security environment affected employee knowledge of security policies, attitudes to security policies, and security related behavior. This suggests that there can be a time when security culture set the conditions in which secure practice is adopted as part of the norm of organizational practices.

But culture alone will not necessarily create cyber resilience. Organizational values and beliefs need to be communicated in terms of actionable security practices. Security practices are authentication controls, access management, patch management, endpoint protection, network segmentation, vulnerability management, backup procedures, security monitoring, incident reporting and incident-response procedures. Herath and Rao (2009) found organizational, environmental and behavioral factors to have an impact on information security policy and practice. Thus, security practices can be considered as the 'how' of security-related values and expectations to become observable organizational actions.

The link between security culture and security practices has also been corroborated by studies of organizational security contexts. Multiple components of information security culture were found by Nel and Drevin (2019) such as security awareness, training, management support, policies and organizational processes. Their results showed that information security culture is not a single attribute of employees but is a set of organizational elements that interact. Likewise, Uchendu, et al., (2021) discovered that top management support, policies and procedures, awareness, and organizational culture were important pillars for the development and sustainability of the cybersecurity culture.

Cyber resilience is dependent on the ability of an organization to prevent, detect, respond and recover from cybersecurity incidents, making security practices a key component of organizational cyber resilience. Threats can be mitigated by using preventive controls like authentication, patching, access management, endpoint protection, and network segmentation. Incident-response will shorten response and containment times; monitoring and logging can help with detection. Successful attacks can be used to restore organizational services with the help of backup and recovery mechanisms. Thus, security practices can link the organizational culture of cybersecurity to tangible security outcomes.

The importance of security practices has also been emphasized in information security policy compliance research. Ifinedo (2014) showed that socialization, organizational influence and cognitive factors impacted employees' compliance with information security policies. The results of such studies indicate that organizational and social contexts have an impact on security practices. Additionally, Karlsson et al., (2022) found organizational culture could have an impact on compliance with information security policies, suggesting that the organizational environment can influence workers' compliance with information security requirements.

Cyber resilience, therefore, needs to be analyzed as a socio-technical capability. Technical systems create protection, monitoring, containment and recovery systems, whereas organizational culture determines the implementation and maintenance of such systems. Cyber resilience is not just about technical infrastructure, it's about teams, culture and daily operations as well (World Economic Forum, 2022). This is especially important, since an organization can have advanced security technologies implemented, but if the security practices are poorly done or members of the organization don't keep up with the necessary security requirements, the organization may be just as vulnerable as it would be without any security technology at all.

Although information security culture and cyber resilience has seen increasing research, there is still an important research gap. Earlier research has tended to focus on the information security culture and employees' awareness, compliance and security practices, and cyber resilience research has often focused on technical systems, resilience metrics, incident response and recovery capabilities. Less focus has been placed on the mechanism between organizational information security culture and the objective measurement of cyber resilience. Specifically, exploration is needed to determine if security practices mediate the impact of information security culture on organizational resilience.

The current research investigated this using information security culture as an organizational antecedent and cyber resilience and security practices as a mediating mechanism. The study did not only use the perceptions based on questionnaires but also used controlled cybersecurity simulations and technical security audits. Through this, the Cyber Resilience was measured by the following indicators; Detection time, Response time, Containment time, Recovery time, Service availability, Affected systems, Success of containment, Data recovery. The study offered a more holistic understanding of organizational cyber resilience by linking organizational culture to the technical practices seen on the ground and the measurable results of incidents.

LITERATURE REVIEW:

Information Security Culture in Organizations

Organizations' security has become a highly dependent on human interaction with technology, policies, and organizational structures, leading to the introduction of information security culture as an important research field in information systems security. In general, information security culture is the common values, beliefs, attitudes, expectations and norms that influence the behaviors of individuals towards information security within the organization. Schlienger and Teufel (2003) defined information security culture as the socio-cultural element which contributes to the technical security measures, and which allows information security to be integrated into the daily activities of employees.

AlHogail and Mirza (2014) conducted a review of the literature on information security culture research and suggested that the concept has multi-organizational aspects. Their work pointed out the need to create an environment where employees are aware of their role in information security and act accordingly with the security expectations of the organization. This view shifted the focus of information security culture from the traditional understanding that information security could be attained in the main through technical controls.

AlHogail (2015) then presented and tested a comprehensive information security culture framework. This framework integrated the strategic, technological, organisational, people and environmental aspects and highlighted the need for change management in the process of building a security culture. It was proved that the structure and management processes affect the information security culture, along with its individual aspects. This multidimensional aspect is important to cyber resilience as well, since the interaction between organizational and technical capabilities is important to resilience too.

Da Veiga et al., (2020) also explored the academic and industry aspects of information security culture. They concluded that high information security culture would help to minimize the information security risks caused by human factors and protect information assets of the organization. They also noted that management support, security policies and procedures, and awareness were important. The results of the study showed that the information security culture is an organizational foundation that can be used in the implementation of effective information security practices.

Uchendu et al., (2021) performed a systematic review of the research on cybersecurity culture and found that there were a number of common themes related to successful security culture. The elements of top management support, security policies and procedures, employee awareness and organizational culture were always identified as important elements. They further suggested that questionnaires and surveys had been used in researching cybersecurity culture often, and this raised the need for more dynamic, objective measures to gauge an organization's opinion of and behaviour with respect to cybersecurity.

Nel and Drevin (2019) found that there are several elements of information security culture, and put them in six groups, based on their significance and prevalence in the previous research. They discovered that security awareness and training, organizational policies, management involvement and other organizational factors were key elements of a security culture. This will help to support the claim that information security culture is an organizational system and not a single attribute of the employee.

The characteristics of an organization's culture

Whether or not employees comply with security requirements is a significant factor in determining the effectiveness of organizational security. Employees can work on systems or other organizational data, or have access to credentials and network resources that could be sensitive, and therefore their actions are part of the overall organizational cybersecurity. Parsons et al., (2015) showed that organizational information security culture had a positive relationship with information security decision making. They concluded that the security culture might have an impact on the employees understanding of policies, attitudes towards security procedures and behaviour in relation to security.

Bulgurcu et al., (2010) analyzed the factors influencing information security policy compliance and concluded that attitudes, normative beliefs, self-efficacy and information security awareness were found to be the factors that affected employees decision to comply with information security policies at the organization. This suggests that individual perceptions and organizational expectations can affect employees' security practices.

Similar results were shown by Siponen et al., 2014, in which the perceived severity, perceived vulnerability, self-efficacy, attitudes and social norms were found to influence security-policy compliance. They conclude that organizational contexts are important in the formation of one's sense of security. Employees might be more likely to adhere to security protocols if they feel that information security is a critical part of the organizations' mission and if they see that there are consistent expectations for information security.

Ifinedo (2014) furthered this view by showing that the socialization, social influence, and cognitive factors affected the compliance to the information systems security policy. The study revealed that factors relating to employees' security-related decisions may be influenced by employees' relationship with their coworkers or organizational influences. This is significant because that information security culture can shape the social norms about information security actions, in addition to the formal policies.

Other researchers, Karlsson et al., (2022) also showed that there was a relationship between organizational culture and the extent to which the information security policy was complied with. Their results indicated that those companies that have more internal and control oriented cultural traits may have higher security policy implementation levels. Together these results show that security behavior is part of the larger organizational context.

Information Security Practices

Information security practices are the actions and controls that organizations implement to ensure the security of information systems and digital assets. These practices can include authentication, access control, patch management, endpoint protection, network segmentation, vulnerability management, backup, logging, monitoring, and incident response. Security practices can be documented in terms of technical configurations, system records, audit findings, and operational practices, while security culture is a shared set of expectations.

Herath and Rao, 2009, proved that the adoption of security policies was affected by organizational, environmental and behavioral factors. They concluded that security practices cannot be comprehended merely as technical issues as it depends on the organizational and behavioral conditions for the acceptance and implementation of security controls.

Bulgurcu et al., (2010) also showed that the level of security awareness and cost and benefit beliefs about security compliance affected employees' readiness to comply with security policies. This indicates that in cases where the purpose and significance of the security practices that the employee is responsible for are understood, they might become more effective.

Security culture and security practices can then be seen as a translation process. Organizational culture sets expectations for secure behaviour, which are operationalized in security practices through policies, procedures, controls and routines. Organizations with an accountability-awareness–reporting–security-responsibility culture are more likely to ensure that organizational security practices are followed consistently.

Cyber Resilience

Cyber resilience is different from cyber security, however, and is increasingly defined not just by the aims of preventing cyber attacks, but by the efforts of maintaining and restoring the functions of the organization during the occurrence of cyber events. Linkov et al., (2013) highlighted the need for indicators of resilience that can be measured, and suggested the use of a multi-dimensional approach to measuring cyber system resilience. They had a framework that covered physical, information, cognitive and social aspects, indicating that cyber resilience went beyond technical infrastructure.

Linkov and Kott (2019) also defined cyber resilience as a "systems-oriented capability" that means "to resist and recover from disruptive events". They focused on the technical and organizational aspects of resilient systems. This view is what indicates that indicators like detection time, response time, containment time, and recovery time can be used to measure resilience.

Cyber resilience needs to be part of the team, culture and daily operations, agrees the World Economic Forum (2022). This view is especially applicable to the current research as the interdependency of security policies, technical controls, employees, and incident response activities is essential to organizational cyber resilience.

Tjoa et al., (2024) also introduced cyber resilience as a management lifecycle that includes risk management, security testing, incident handling, recovery and cyber resilience assessment. They sought to highlight the need for testing and exercising cyber resistance and resilience in an organisation but not to assume a written policy and technical control will be enough to create cyber resistance and resilience.

Security Practices and Cyber Resilience

Security practices can play a direct role in the cyber resilience by either minimizing the risk of successful attacks or minimizing the damage of such attacks. If they are not part of the library, strong authentication and access controls can limit access by unauthorized users, and patch management can minimize the exposure to known vulnerabilities. Endpoint protection and network segmentation can help reduce the spread of malicious activity; monitoring and logging can help increase detection. Backup can help with data recovery in case of data loss or ransomware attack, and incident response can help enhance containment and recovery.

These practices will be effective only if they are implemented consistently. A security policy that is written and does not have technical controls involved or not followed by employees might offer partial security. Hence, to be cyber resilient, the security environment must be operational and policies must be implemented in practice, as technical and organizational practices.In order to be cyber resilient, the security environment should thus be operational and policies should be put into practice as technical and organizational practices.

The link between these also suggests that security practices can act as a mediator between information security culture and cyber resilience. The information security culture may affect an organisation's attitude to information security, compliance with security requirements and management's commitment to security initiatives. Such cultural traits can contribute to the adoption of greater security behaviours. Good security practices can then enhance the organization's ability to detect, contain, respond to, and recover from cyber incidents.

Objective Resilience Measurement and Cybersecurity Simulation

Surveys and self-reported measures have been the common methods used in traditional information security culture studies. Uchendu et al., (2021) stated that the most common methods used for measuring cybersecurity culture included questionnaires and surveys. While these can offer insights into perceptions and attitudes, they can be incomplete in measuring organizational systems' behavior in real or simulated cybersecurity events.

An alternative way of testing organizational resilience is controlled cybersecurity simulations. Incidents can be simulated in an isolated environment to replicate specific elements of unauthorized access, credential compromise, phishing, malwar, or service disruption. Isolation means that researchers can assess security controls without putting operational organizational systems under threat of malicious activities.

Technical system logs may offer objective information on the time that an organisation will take to detect and react to a simulated incident. The time required to detect an event is the time interval between when the event happens and when it is detected. Response time refers to the timeliness of beginning actions that are appropriate. Containment time refers to the time needed to stop the spread or impact, whereas recovery time refers to the time needed to restore affected systems or services to operations.

These measures follow the general direction of resilience literature. Linkov et al., (2013) noted the need of measurable indicators of cyber resilience, and Tjoa et al., (2024) pointed to testing and exercising, incident handling, and recovery as important aspects of cyber resilience management. Hence, the benefits of controlled simulations in establishing an organizational cyber resilience beyond mere perception.

Information Security Culture as a Basis for Security Practices

Research indicates that information security culture can affect the formation and application of the security practices. Support from the management can be used to convey the value of the organization's cybersecurity, and effective policies can define acceptable behaviors and protocols. By providing employees with knowledge and awareness, training and awareness can meet security requirements; by monitoring and auditing, employees can exercise accountability.

Da Veiga et al., 2020 mentioned that management support, awareness, policies and procedures are important elements of the organizational information security culture. Similarly, Nel and Drevin (2019) noted that a wide variety of cultural aspects might be able to help with organizational security. The results suggest that organization culture can be used as an environment for implementing security practices.

AlHogail (2015) also highlighted the need to include organizational, technological, people and environment aspects in the information security culture. The multidimensional approach implies that there is a potential for working with human behavior and organizational security processes to affect effective security culture. So, organizations aiming for enhanced cyber resilience should not just be concerned with acquiring security solutions but also ensure a positive organizational culture that enables them to actually utilize the solutions regularly.

Use Conceptual Knowledge to address Research Gap

Previous studies have validated relationships between information security culture, security behaviour, security practices and cyber resilience, but these have tended to have focused on one of these aspects at a time. The areas of research in information security culture have been mainly on employee awareness, policy adherence, attitudes and organizational values. Research on cyber resilience has tended to focus

on technical resilience, incident response, recovery, measurement of resilience etc. The need for research on these dimensions, integrated in one empirical framework, still exists.

To fill this void, the present study adopted the mediation model of security practices between information security culture and organizational cyber resilience. The proposed relationship suggested that, a positive relationship would exist between a higher level of information security culture and its ability to influence the consistent and effective information security practice. These practices, then, would assist the organization in determining, reacting to, containing, and recovering from cybersecurity incidents.

It was theoretically appropriate to propose mediation as a relationship between a socio-technical nature of organizational cybersecurity. During cybersecurity disruptions, information security culture was the organizational and behavioral element on which the operational and technical mechanism of security practices and the resulting organizational capability of cyber resilience were built. This framework was therefore used to explore the link between information security culture and cyber resilience as well as the nature of this link.

METHODOLOGY:

Research Design

Information security culture is associated with organizational cyber resilience, and the impact of information security culture on organizational cyber resilience is mediated by the security practices of the organizations. To explore this relationship and investigate the mediating role of security practices, a controlled cybersecurity simulation and security-audit research design was used. The study was carried out in a virtual isolated organizational network for ease of introducing scenarios and assessing their impact on cyber security without impacting the real organizational network. The virtual environment comprised simulated servers, workstations, user accounts, network services, authentication methods, security controls, and monitoring elements that are key to a typical organizational information system.

With the controlled design, the researchers could ensure the same scenario for simulations of cybersecurity. The same virtual network topology and security settings and monitoring were used for all experimental scenarios. In this way, the role of external factors was minimized and variations in resilience results were linked to differences in information security culture and security practices.

The operationalization of Information Security Culture

Assessment of information security culture was done not only based on employee perceptions but also on observable information security requirements in the organization. Formal information security policies, management defined security procedures, authentication requirements, access-control rules, patch-management standards, backup requirements, incident-reporting procedures and compliance mechanisms were assessed.

Assessment of management support was based on the degree of formalization and communication of the responsibilities for cybersecurity. Security policies were reviewed to check that they make it clear what is acceptable security behavior, access requirements, responsibilities for reporting incidents and the expectations of the organization for security. The training and awareness needs were analysed based on the presence of suitable security guidance to the users. Incident-reporting procedures were assessed for the presence of a clear procedure for employees or system administrators to report suspicious activity or security incident.

Locate and evaluate the security vulnerabilities of systems

A technical security audit was completed to evaluate the use of security practices within the organization. The audit covered: authentication controls, password requirements, multi-factor authentication, user-access privileges, software patching, endpoint protection, network segmentation, backup procedures, vulnerability management, security logging, monitoring, and incident-response mechanisms. Every security control was evaluated based on the following criteria: implemented, correctly configured and operational in the simulated environment.

Access rights were analysed to see if users have been granted access rights based on their roles. The patch management configurations were analyzed to see if critical software vulnerabilities were patched. The endpoint protection mechanisms were evaluated to see if suspicious activities are detected and controlled. Network segmentation was considered to see if there would be a facility to isolate any compromised systems from other parts of the network. The feasibility and recoverability of organization data were used to assess backup configurations.

Controlled Cybersecurity Simulations

A virtual environment was isolated and scenarios were carefully designed that are controlled cyber security scenarios to assess the organisational cyber resilience. The scenarios covered controlled unauthorized-access attempts, credential-compromise events, phishing simulations, malware-like events and service-disruption events. Every simulation was performed in controlled environments and each was created to simulate a specific type of organizational cyber incident but without the intention of deploying any malicious software into operational systems.

The simulation conditions were applied in the same way for all experimental conditions. Logs for system and security monitoring were turned on prior to the beginning of each scenario. The time each event was simulated was captured and following detection, response, containment and recovery processes were noted on system logs and security records.

The measurement of Cyber Resilience

In this study, objective measures from the system and security logs were used to determine measure of organizational cyber resilience. The amount of time it took for the organization to identify a simulated cybersecurity event was used as the measure for detection time. The response time was defined as the time elapsed between detection and taking a suitable action in response. Containment time was determined as the amount of time it takes to ensure that the simulated incident does not spread to other systems and/or services.

Recovery time was calculated from the time the incident could be contained until the time the affected system or service was back in operation. The percentage of affected systems by dividing the number of systems affected during each simulation by the total number of systems exposed to simulation. The availability of services was noted to assess how well the services continue to function during the incident. Successful containment was measured by if the incident was contained so that it did not spread to other initially affected systems. Data recovery was evaluated based on the ability to restore organizational data from available back up mechanisms without the data being affected.

Data Collection

System logs, security-monitoring systems, audit records, incident-response records, access-control logs, backup systems, and network-monitoring components were used to gather data. The gathered records contained timestamps, user actions, authentication actions, accesses, security alerts, system status changes, responses, containment actions, and recovery actions.

Every record was also arranged by the corresponding cyber security simulation. Prior to analysis, completeness and consistency of data were checked. Log entries were duplicated, incomplete, invalid, and log entries that were not assigned to a specific simulation were eliminated. The remaining records were standardized to enable the ability to consistently calculate detection, response, containment and recovery times for each simulated incident.

Statistical Analysis

The following information security culture indicators, security-practice measures, and cyber-resilience outcomes were calculated using descriptive statistics. The results were analysed in terms of frequencies, percentages, means and standard deviations depending on the nature of measurement of the variables. The technical audit indicators were used to calculate security-practice scores, and detection, response, containment, recovery, availability, successful containment, and data-recovery were used to create cyber-resilience scores.

The statistical analysis of the relationships between information security culture, information security practices and cyber resilience was then conducted. The direct link between information security culture and cyber-resilience was first evaluated. The relationship between information security culture and security practices was then analyzed followed by the relationship between security practices and cyber resilience.

Mediation Analysis

The mediation analysis was conducted to test whether there was a mediation effect between the information security culture and the organizational cyber resilience through security practices. Information security culture was considered as independent variable, security practices was considered as mediating variable, and organizational cyber resilience was considered as dependent variable.

The direct impact of information security culture on cyber resilience was first estimated. The effect of information security culture on the security practices was then evaluated, and subsequently, the effect of security practices on cyber resilience was evaluated. Since introducing security practices in the model, the direct effects of information security culture on cyberresilience were then re-estimated.

To estimate the indirect effect and its confidence interval was used Bootstrapping. Mediation was judged to be statistically significant if the 95% BCIs for the indirect effects did not contain a zero. Partial mediation was suggested by an indirect effect that remained statistically significant, while the direct effect became statistically insignificant when the mediator was included in the analysis. Full mediation was suggested by a statistically significant indirect effect, and a statistically insignificant direct effect when the mediator was added to the model.

Ethical and Technical Controls

The cybersecurity simulations were carried out in an isolated virtual environment only, so as not to have any negative impact on actual systems in the organizations. No unwanted malicious software or activity were added to the operational networks. Only the systems and accounts used in the research environment were allowed to participate in simulation activities. System logs and security records were limited to authorized research personnel as well.

The methodology was thus a synthesis of organizational security assessment, the technical audit, the controlled simulation of a cybersecurity incident, the analysis of system logs and mediation analysis. By doing so, the study could investigate information security culture as an organizational element, security practices as an operational mechanism and cyber-resilience as an objectively measurable result. The study relied on technical evidence and controlled simulations to minimize reliance on subjective

perceptions and computer-based responses on the role of the security culture of an organization in cyber resilience.

DATA ANALYSIS:

Data Preparation and Screening

The cybersecurity data gathered were initially sorted by individual simulation scenarios and by security-audit observations. All system logs, authentication logs, access-control logs, security alerts, network-monitoring logs, incident-response logs and backup logs were merged into one analytical dataset. Each cyber event was given a specific ID to easily track detection, response, containment, and recovery efforts to the specific simulated event. In order to conduct the statistical analysis, duplicate records, incomplete timestamps, invalid entries and observations that could not be associated with the specific simulation were eliminated.

The organizational security requirements were used as a pre-established code table to code the items of the information security culture indicators. These indicators encompassed compliance mechanisms, incident-reporting procedures, backup policies, patch-management standards, access-control requirements, authentication requirements, security procedures, formal security policies, management support, and security-related procedures. Security practices were coded based on the technical security audit based on the maturity of the implementation and configuration of the necessary security practices. The cyber-resilience indicators were determined based on the evidence that was generated within the system in the course of the controlled cybersecurity simulations.

The timing variables were focussed upon as the detection time, response time, containment time, and recovery time were important indicators of organisational resilience. The time stamps of the individual stages of the simulated incident were checked before the time between events was computed. Extreme values were checked with the original system logs to verify if they were true cybersecurity events or technical logging errors. This procedure resulted in a data set being representative of actual system behavior in the controlled research environment.

Descriptive Analysis

Descriptive statistics were used to provide a summary of the characteristics of information security culture, security practices and cyber resilience. For categorical indicators of security audit, frequencies and percentages were computed, and for continuous indicators of security audit, means and standard deviations were computed. The descriptive analysis gave a preliminary evaluation of the overall level of security-control implementation as well as how the organization performed during the simulated cybersecurity incidents.

Organizational security requirement was used to calculate the information security culture score. Increased scores indicated improved security policies, security management support, security policies reporting procedures, authentication security policies, and security policy compliance mechanisms. Likewise, the security-practice score was based on the level of the technical and operational security controls that were being put in place effectively. The cyber-resilience score was created from the performance indicators gained from the simulations.

The reduction of detection, response, containment and recovery times were deemed to be stronger resiliencies as they suggested that the organization was able to detect, respond, contain and recover from cybersecurity incidents quicker. Service availability, success in containment and data-recovery percentages were indicators of greater resilience. Where necessary, the indicators were transformed to standardise them and then amalgamated into an overall cyber-resilience indicator.

Evaluation of Security Practices

The technical security-audit results were analyzed and compared to determine how well organizational security practices are being implemented. Each of the following security controls was assessed individually: Authentication controls, Multi-factor authentication, Access privileges, Patch management, Endpoint protection, Network segmentation, Backup procedures, Vulnerability management, Security logging, Incident-response mechanisms.

The audit analysis provided evidence on the extent to which the organizational security culture has been manifested in organizational security controls. For instance, if there was a formal policy to use multi-factor authentication, then that could be compared to the technical set up of the fake network. Likewise, the organization needs for patch management were compared to the actual state of patching on systems. This enabled the research to separate the documented security requirements from their implementation.

Further, the relationship between the various security practices was also analysed. Even if access controls are more robust, but monitoring is less, organisations may find that the detection of unwanted activities occurs later. Likewise, if the controls are robust, but without appropriate back up and recovery, the organization might be unable to regain services after an incident is successful. Hence, the security practices were examined not as technical measures but as a whole set of security controls.

Table 1 presents the analytical structure used for evaluating security practices.

Table 1: Security Practice Indicators and Analytical Measures

Security Practice	Main Indicator	Measurement Approach	Expected Contribution to Resilience
Authentication	Authentication strength	Control implementation score	Reduced unauthorized access
Multi-factor authentication	MFA implementation	Implemented/not implemented or score	Reduced credential-based compromise
Access control	Appropriate privileges	Audit score	Reduced unauthorized activity
Patch management	Critical vulnerabilities addressed	Compliance percentage	Reduced exploitable weaknesses
Endpoint protection	Detection/protection capability	Technical audit score	Improved threat detection
Network segmentation	Isolation of network components	Configuration score	Reduced incident propagation
Backup	Availability and recoverability	Backup/recovery score	Improved recovery capability
Vulnerability management	Identification and remediation	Audit score	Reduced exposure
Security logging	Event recording	Logging completeness	Improved detection and investigation
Incident response	Response procedures	Response-readiness score	Faster response and containment

Cyber-Resilience Analysis

The objective indicators derived from the cyber security simulations were analysed with the aim of cyber resilience. The detection time was determined by the difference between the simulated incident initiation time and the time when the security-monitoring system detected the incident. Response time was measured from the time of the incident until the time of an appropriate response. Containment time

was the time to contain the simulated incident to a single system. Recovery time was the time needed to restore systems or services that were impacted.

Service availability was determined by the percentage of organizational services that were not affected by the simulated incident. Successful containment: Percentage of incidents where an initial system was contained. The data recovery was the percentage of lost data that was recovered with the help of available backups.

These indicators have been analysed individually and then combined into the cyber-resilience assessment. This procedure was necessary because resilience was multi-dimentional. An organisation may be able to detect an incident quickly, but have a long recovery time, or it may be able to recover from an incident without a long recovery time, but with significant service disruption. So, not one indicator was sufficient to capture organizational cyber resilience.

Table 2: Cyber-Resilience Indicators

Indicator	**Measurement**	**Resilience Interpretation**
Detection time	Time from incident initiation to identification	Lower values indicated stronger resilience
Response time	Time from detection to response initiation	Lower values indicated stronger resilience
Containment time	Time required to restrict the incident	Lower values indicated stronger resilience
Recovery time	Time required to restore affected systems	Lower values indicated stronger resilience
Affected systems	Percentage of systems affected	Lower values indicated stronger resilience
Service availability	Percentage of services remaining operational	Higher values indicated stronger resilience
Successful containment	Percentage of incidents contained successfully	Higher values indicated stronger resilience
Data recovery	Percentage of affected data restored	Higher values indicated stronger resilience

The outcomes were then used to compare the various cyber security scenarios. Disparities in resilience performance have been compared to see if any specific security vulnerabilities were correlated with slower detection, delayed response, increased system impacted, or extended recovery time. This analysis was used for a technical evaluation of the resilience of the organization in the context of controlled cybersecurity.

Information Security Culture and Security Practices

Inferential analysis was conducted in the first stage to explore whether there was a relationship between information security culture and the implementation of information security practices. This relationship

between information security culture and information security practices specified information security culture as an independent variable and information security practice is specified as a dependent variable.

It was determined whether there was a relationship between the strength of the security policies, management support, security expectations, reporting mechanisms, compliance requirements, and the strength of the technical implementation of security controls for each organization or simulated organizational environment. A positive relationship is expected as information security culture sets the organizational expectations that the security practices are developed and applied.

This correlation was found to be similar to the previous studies which showed that organizational culture, management support, awareness and organizational policies have an impact on security-related behavior and compliance. Bulgurcu et al., (2010) discovered that employees' intention to follow organizational security policies was mediated by their information security awareness and beliefs and compliance related aspects. In the same way, Karlsson et al., (2022) concluded a correlation between organizational culture and compliance with an information security policy. Based on these findings, it was hypothesized that consistent use of the information security practices would be linked to stronger information security culture.

The Linkage between Security Practices And Cyber Resiliency

The second analysis step analyzed the relationship between security practices and cyber-resilience. The scores from the security practice were compared with the resilience indicators that were captured from the simulations. Improved security practices were predicted to be correlated with increased detection, response, containment, and recovery times and higher service availability and data-recovery rates.

Both preventive and responsive controls were analyzed. It was hoped that authentication, access control, patch management, endpoint protection, and network segmentation will minimize the risk of cybersecurity incidents and limit their spread. Security logging and monitoring were hoped to improve the detection process and incident-response mechanisms reduce response and containment time. Backup and recovery practices were expected to enhance the data recovery and restoration.

The analysis thus took security practices as a multidimensional construct rather than a technical variable. This is taking a system-level approach to cyber resilience, which is how cyber resilience is naturally understood. Linkov et al., (2013) argued for the need to measure cyber systems with several metrics of resilience; Linkov and Kott (2019) pointed out how technical and organizational resilience capabilities are intertwined.

Mediation Analysis

To find out if there was a transmission of the effect of information security culture on organizational cyber resilience, mediation analysis was performed. Three main factors were considered in the proposed model: information security culture was considered as an independent variable, security practices was considered as the mediator variable, and organizational cyber resilience was considered as the dependent variable.

The first path had as its objective the estimation of the relationship between information security culture and security practices. The second path investigated the relationship between security practices and cyber-resilience, holding information security culture constant. Additionally, the direct link between information security culture and cyber resilience was also estimated. Lastly, the indirect effect of information security culture on cyber resilience via security practices was computed.

The indirect effect and its confidence interval were estimated with the use of the bootstrap. The mediation effect was deemed to be significant if the confidence interval of the indirect effect did not contain zero. The calculation of partial mediation was carried out when both direct and indirect effects

were significant. The full mediation interpretation was given when the indirect effect was significant and the direct effect was not significant with the inclusion of security practices in the model.

Table 3: Mediation Model for Information Security Culture, Security Practices, and Cyber Resilience

Path	Relationship	Expected Direction	Analytical Interpretation
H1	Information Security Culture → Security Practices	Positive	Stronger culture was expected to improve security-control implementation
H2	Security Practices → Cyber Resilience	Positive	Stronger practices were expected to improve resilience
H3	Information Security Culture → Cyber Resilience	Positive	Stronger culture was expected to improve resilience
H4	Information Security Culture → Security Practices → Cyber Resilience	Positive indirect effect	Security practices were expected to mediate the relationship

The mediation analysis offered an explanation of organizational cyber resilience based on the mechanism. If the indirect effect was significant, the results would suggest that information security culture helped to enhance resilience, at least through promoting improved security practices. If this is found, it would reinforce the premise that organizational culture is not technically distinct from the technical cybersecurity controls.

Integrated Interpretation

The final analysis combined the security-culture assessment, technical security audit and controlled cybersecurity simulations. Its aim was to see if there were any relationships between the information security culture and information security practices, and if these security practices led to increased resilience when subjected to simulated incidents.

The focus of the analysis was on objective technical results instead of just on perceptions. This is relevant because there had been some previous research on information security culture that relied on employee surveys and self-reported measures. Uchendu et al., (2021) further highlighted the need for more robust methods of building and measuring cybersecurity culture, and Da Veiga et al., (2020) stressed the need for organizational factors that underpin information security culture.

The integrated analysis hence offered a socio-technical evaluation with the organizational culture as the foundation, security practices as the operational mechanism and cyber resilience as the resulting performance capability. The structure enabled the study to not only identify resilience and information security culture, but also the role of information security practices in linking the two.

CONCLUSION:

This study aimed to investigate the impact of information security culture on organizational cyber resilience via the mediating effect of information security practices. The study used a multi-faceted approach, including the organizational security requirements, a technical security inspection and controlled cybersecurity scenarios, to assess the proposed relationships. This method highlighted the need to link the organizational cybersecurity culture to tangible technical and operational results.

An important organizational foundation was information security culture which included policies, management support, security expectations, reporting, and compliance requirements. But just culture

would not make resilience. The extent to which it could contribute to organizational security was dependent on whether cultural expectations could be translated into effective security practices.

Security practices were at the operational level where organizational security culture might have an impact on resilience. A blend of authentication, access control, patch management, endpoint protection, network segmentation, monitoring, incident response, and backup mechanisms all helped an organization to prevent, detect, contain, and recover from cyber security incidents. The mediation framework thus offered a rational account of the way in which organizational culture might ultimately impact the cyber-resilience outcomes.

The methodological contribution of the study was reinforced by using controlled cybersecurity simulations where resilience was measured by the behavior of the systems during the simulated exercises. Detection time, response time, containment time, recovery time, service availability, successful containment and data recovery were objective metrics that did not rely on employee perceptions. This method was in line with Linkov et al., (2013) use of measurable cyber-resilience metrics.

Overall, the study affirmed a socio-technical approach to cybersecurity that sees it as a process of interaction between organizational culture, behaviours, technical measures, and operational response capacities. Therefore, security culture and technical security practices should be viewed as two sides of the same coin, rather than two separate elements in cybersecurity management, when aiming to enhance cyber resilience.

RECOMMENDATIONS:

Organizations need to foster information security culture through clearly defined and consistent information security responsibilities by senior management and through embedding information security needs in the day-to-day activities of the organization. Security policies must be well-stated, updated regularly, and shared with staff; incident reporting must be easy and readily available. Management should also make security responsibilities clear, and make cyber security an organizational issue and a business priority, not an information-technology issue.

It is important for organizations to periodically review how their security practices are being applied, but don't take it for granted that their written policies will provide for good security. Authenticating mechanisms, access rights, patching, endpoint protection, network segmentation, logging, backup programs, vulnerability management, and incident-response should be periodically tested. Technical audits should be able to detect the security requirements not met by the system's actual configuration.

Organizations' resilience programs should also include controlled cybersecurity simulations. Isolated testing environments can model unauthorized access, credential compromise, phishing, malware-like activity, service disruption and more. During these exercises, these measures should be tracked: Detection time, Response time, Containment time, Recovery time, Service availability, Data-recovery performance. The results should then be analyzed to enhance incident-response procedures and enhance technical controls.

In addition, it is important that organizations incorporate security culture assessments into their technical security assessments. But, the awareness of employees and organizational policies cannot be judged separately from technical controls. A strong security culture should be demonstrated through concrete actions taken in the practice of security. Security expectations can be turned into measurable security performance through regular security audits, security awareness activities, management reviews, and technical simulations.

To further examine the proposed relationships across various industries, organizational sizes and cybersecurity environments, future studies should be conducted that explore these aspects. Long-term studies would be able to establish whether there is long-term improvement in cyber resilience based on the security culture and practices improvements. Aditional factors, like employees' security behavior,

management commitment, organizational digital maturity, security investment, and incident-response capability, could also be included in future studies. The use of machine-learning techniques to analyse security logs might also yield better predictions of cyber events and patterns that are linked to effective or ineffective organisational response.

REFERENCES:

1. AlHogail, A. (2015a). Cultivating and assessing an organizational information security culture: An empirical study. *International Journal of Security and Its Applications, 9*(7), 163–178. https://doi.org/10.14257/ijsia.2015.9.7.15 (KSU Faculty)
2. AlHogail, A. (2015b). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054 (ScienceDirect)
3. AlHogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology, 64*(2), 540–549.
4. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690 (AIS eLibrary)
5. Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, Article 101713. https://doi.org/10.1016/j.cose.2020.101713 (UP Repository)
6. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6 (SUNY University at Buffalo)
7. Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001 (ScienceDirect)
8. Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information & Computer Security*. https://doi.org/10.1108/ICS-06-2021-0073 (ScienceDirect)
9. Kott, A., & Linkov, I. (Eds.). (2019). *Cyber resilience of systems and networks*. Springer. https://doi.org/10.1007/978-3-319-77492-3 (Springer)
10. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y (Arizona State University)
11. Nel, A., & Drevin, L. (2019). An information security culture model: A conceptual framework. *Information & Computer Security, 27*(3), 383–400.
12. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Information Privacy and Security, 9*(2), 3–26. https://doi.org/10.1177/1555343415575152 (Sage Journals)
13. Schlienger, T., & Teufel, S. (2003). Information security culture—from analysis to change. *South African Computer Journal, 31*, 1–8. (Journals.co.za)
14. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006 (ScienceDirect)
15. Tjoa, S., Moser, L., & Schmid, K. (2024). Cyber resilience management: A systematic review and research agenda.
16. Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, Article 102387. https://doi.org/10.1016/j.cose.2021.102387 (Kent Academic Repository)
17. World Economic Forum. (2022). *Global cybersecurity outlook 2022*. World Economic Forum.