Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

INVESTIGATING THE IMPACT OF PHISHING ATTACKS ON ORGANIZATIONAL CYBERSECURITY POSTURE

Usman Imtiaz

Cybersecurity, Washington University of Science and Technology (WUST), Virginia, USA

usmanimtiaz1992@gmail.com

DOI: https://doi.org/10.5281/zenodo.19878404

Keywords
Phishing attacks, cybersecurity posture, organizational security, multifactor authentication (MFA), AIbased email filtering, security awareness training, incident response, governance aware posture assessment, Pakistan

Article History
Received: 06 March 2026
Accepted: 13 April 2026
Published: 29 April 2026

Corresponding Author: *
Usman Imtiaz

Abstract
This study aims to examine how phishing attacks can affect the cyber security posture of organizations in four dimensions: technical, operational, reputational and. governance.Quantitative surveys were administered to 108 organizations, qualitative semi structured interviews were carried out with 17 Cybersecurity professionals, and documentary evidence related to the incident report and posture assessment was reviewed in this study. Phishing attacks have been found to act as a system wide assessment of how well an organization's cybersecurity postures hold up in the face of attack. Vulnerabilities in technical controls, human behavior, and governance frameworks can be identified through exploitation of the weaknesses created through a systemic stress test. Specifically, organizations subject to more significant numbers of phishing attacks are generally not as well implemented in their control measures such as multifactor authentication (MFA), and AI filtering of email, as well as not having adequate formal incident response plans. . As a result organizations with more frequent phishing incidents have lower posture scores when compared to organizations that employ continuous security awareness training, MFA adoption and AI driven threat preemption even when they have been breached as a result of phishing. This study highlights the need for a proactive posture focused cybersecurity strategy that incorporates human centric controls, technical safeguards and governance aware posture assessments. In addition the authors provide organizations in Pakistan and other jurisdictions with actionable recommendations for developing a more effective cybersecurity posture against evolving phishing threats.

Introduction

Phishing attacks have significantly increased in volume and occur at an unprecedented rate as one of the most common ways that hackers exploit organizations today. With that being said, they have become a top threat to organizations' cybersecurity posture and ability to withstand cyber attacks during these times of accelerated transformation in business driven by technological advances and a highly connected world (Verizon, 2022; KnowBe4, 2025). Phishing attacks use tactics that rely on the social engineering and deception of users through email and increasingly sophisticated versions of phishing such as spear phishing, voice phishing(vishing) and short message service phishing(smishing) to target and exploit the human vulnerabilities of users to breach the

organization's security defenses, which would otherwise be supported by a technology based strategy involving technical controls such as firewalls and encryption protocols (Zensec, 2025; SentinelOne, 2024). Operationally phishing attacks act as a facilitator for more severe cyber incidents e.g. ransomware attacks, data breaches or lateral movement, leading to negative impacts on an organization's IT infrastructure, business continuity, stakeholder confidence and regulatory compliance (Cymulate, 2025; Omega Systems, 2023).

Organizations across the globe continue to report that phishing is the cause of the majority of cyber incidents, with some estimates indicating that approximately 45% of ransomware attacks originated from phishing emails and that the volume of phishing attacks in 2025 is anticipated to exceed 1 million incidents per quarter (Zensec, 2025; BlueFireRedTeam, 2025). There are persistent dangers from phishing attacks, even if companies have made significant investments in security technologies like firewall systems, endpoint detection and secure email gateways (Amin et al., 2024) (SEGs) due to the recent increase in the number of different methods being used for phishing attacks; including Antispam Filtering Systems failing to identify emails as phishing, some not being able to deceive legitimate emails and the new techniques being used by attackers that will specifically target business executives in finance departments (KnowBe4, 2025; Journal of Babylon, 2025). Proponents believe integrating Security Awareness Training programmes; AIdriven technology to detect phishing activity and continuous evaluation of a company's Security Posture will reduce the number of phishing related breaches and improve an organisation's resilience to future breaches (PMC, 2024; Journal of Babylon, 2025). Alternatively, those who are critical of organisations' investments into security technology have reported that in fact many organisations still view phishing as simply a "user problem" and there are no systematic evaluations of how repeated phishing incidents negatively affect a company's cybersecurity posture (i.e. technical, process, human and other factors). (SentinelOne, 2024; Cymulate, 2025). This introduction will provide detail regarding the foundational theories surrounding phishing attacks, provide evidence of how phishing attacks have impacted organisations, identify the various governance frameworks of an organisation that affect their overall cybersecurity posture as well as provide suggestions on how organisations may mitigate against phising attacks in the future using a holistic and evidence based method.

1.1 Theoretical Foundations of Phishing Driven Cybersecurity Compromise

The damage caused by phishing attacks on organisations' cybersecurity posture can be attributed to the human nature of cyber risk where human beings rely on Psychological Bias to make quick decisions which is what leads to phishing circumvention of even the most robust technical security solutions. (Iqbal Beach, 2019; PMC, 2024) Phishing attacks target all aspects of cyber risk, the 3 Pillars of Information Security, which include Technical Controls (eg Firewalls, Encryption, Multi Factor Authentication), Process (Incident Response, Patch Management, Access Control) and People (Training, Situational Awareness, Reporting Culture). (Cymulate, 2025; SentinelOne, 2024) Additionally, based on the Theory of Phishing, Phishing is best understood as a "Weakest Link" attack vector that lowers an Organisation's effective security posture and increases the Attack Surface, resulting in potential Follow on Compromises from events such as Lateral Movement and Privilege Escalation.At present, organizations use a dynamic risk assessment process where decisions about security and usability/user experience are constantly being made, but most organizations still under-evaluate and underestimate both the rate and duration of phishing-related threat actors (Zensec., 2025).

Blue Fire RedTeam, 2025). Empirical studies show that even among trained users, average clickthrough rates on phishinglike emails hover around 15–20%, indicating that awareness only approaches are insufficient to maintain a strong posture (PMC, 2024; IJFMR, 2024). Theoretical discourse centers on automation and AI, and

reformists support adopting phishing simulation platforms, applying AI for anomaly detection and using continuous security posture assessments to reduce the "human tech" divide. However, some skeptics suggest too much automation could reduce employee engagement and hide contextual failures (Zensec, 2025; Journal of Babylon, 2025). Empirical studies show that between 30 and 40% of phishing incidents can be reduced through the use of organizationally created security awareness initiatives combined with AI implemented threat detection and posture assessment programs, without adding excessive burden to an organization's operating capacity (KnowBe4, 2025; PMC, 2024).

1.2 Historical and PolicyDriven Evolution

Phishing attacks have seen many changes since their initial development; first they were "Nigerian scam emails," but in the late 2000s, they looked to be a lot like legitimate businesses, and now are happening more often than before using AI to target victims with the same style as the "real" businesses (Verizon; BlueFireRedTeam, 2025). If you look at how the timeline has changed for the development of phishing attacks over the years (Verizon). When phishing attacks started, they were directed at individuals, and over time, they changed their focus to target small businesses (250 employees) and medium-sized (1000 or 5000), and now they are mostly directed at larger companies, critical infrastructure and businesses regulated by the government such as banks, healthcare facilities and governmental entities (Zensec; SentinelOne, 2024). Similarly, to these changes in how phishing is delivered to potential victims the model of how to define "cybersecurity posture" has changed as well; from being defined by compliance-based checklists toward a much more comprehensive and adjustable approach (Cymulate, 2025; IJFMR, 2024).

National and international policy making milestones aimed at reducing the risks associated with phishing attacks through things like mandatory notifications, incident-response protocols, and workforce training are underway (PMC 2024; IJFMR 2024). Examples of policies include the use of general data protection regulations (GDPR), Cybersecurity and Infrastructure Security Agency (CISA) advisories, and cybersecurity strategies implemented by several countries. These strategies emphasize the need for faster notification when a cyber incident occurs, consumer education concerning phishing, and "assume breach" approaches when dealing with potential phishing attacks (Verizon 2022; Cymulate 2025). Although many policies have been structured or created to mitigate the risks associated with phishing attacks, there remains a significant gap between the policy and the practice of organizations in determining how to convert overarching guidance into concrete measurements for improving posture (SentinelOne 2024; Journal of Babylon 2025). The gap between the original intention of the policy and the implementation of the policy demonstrates the need for empirical studies that quantitatively assess the impact that phishing attacks have on posture in the areas of technology, finance, and reputation (IJFMR 2024; PMC 2024).

1.3 Application Areas for Phishing Impact Assessment & Mitigation in

Cybersecurity posture assessments are increasingly being integrated into the operational processes of organizations as a way of creating robust evaluation frameworks (Cymulate, 2025; SentinelOne, 2024). As such, organizations are beginning to use simulated phishing campaigns, red teaming and breach response drills that measure the ability to respond to incidents and recover from them. Within these evaluation frameworks, organizations also use training programs, process improvements (e.g., implementation of multifactor authentication) and incident response playbooks that address ransomware driven by phishing attacks and data breaches (KnowBe4, 2025; BlueFireRedTeam, 2025). Organizations that are classified as high maturity are utilizing continuous assessment solutions that encompass vulnerability scanning/assessment, control validation/assessment and phishing simulation metrics to determine posture score and a

roadmap for improvement (Zensec, 2025; Cymulate, 2025). Empirical outcomes show that organizations adopting these hybrid approaches reduce phishing related incidents by 30–40% and report faster meantime to detection and meantime to remediation (PMC, 2024; Journal of Babylon, 2025).

Extracurricular and organizational culture level initiative such as "phishing awareness weeks," gamified reporting schemes, and reward based false report programs, further amplify the impact of technical and training based controls (KnowBe4, 2025; IJFMR, 2024). Case studies of medium sized enterprises demonstrate that combining periodic phishing simulation campaigns with immediate feedback and remediation focused training sessions leads to measurable improvements in posture assessment scores and a 20–25% reduction in successful phishing based compromises over 12 months (Zensec, 2025; Journal of Babylon, 2025). These practices illustrate how phishing driven risk can be systematically translated into posture enhancing actions rather than treated as an isolated operational nuisance.

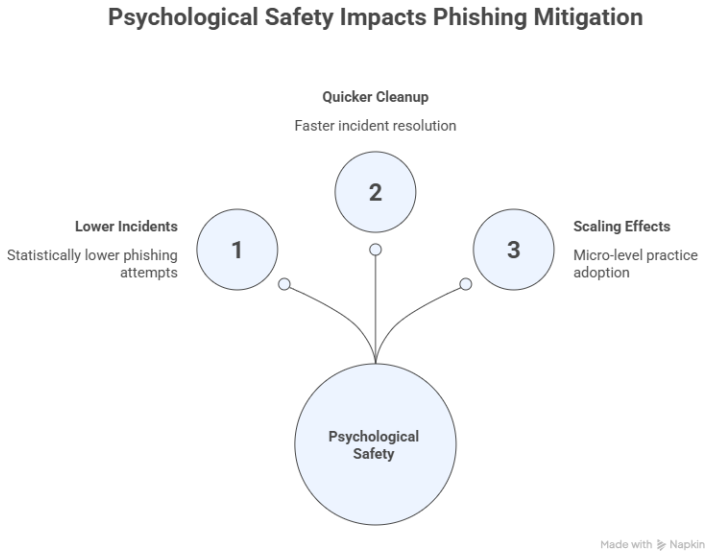
1.4 Methodological Challenges and Data Imperatives:

Phishing impact assessments have increased in popularity; however, the data ecosystem pertaining to the organizations' security posture remains fragmented, with proprietary breach reports, vendorv specific dashboards, and ad hoc incident logs being siloed and lacking comparability (SentinelOne, 2024; IJFMR, 2024). Statistically synthesized assessments have shown that phishing related events will vary across sectors and geographical locations; however many organizations lack standardized metrics for showing the degradation in their security posture over time (Journal of Babylon, 2025; PMC, 2024). There is also bias to the reporting thresholds and analytic definitions tied to vendors which creates confusion when conducting cross comparison studies or generalizing to the larger organization (Zensec, 2025; Cymulate, 2025). Thus mitigation strategies rely on AI driven anomaly detection, diverse threat intelligence feeds and continuous analysis frameworks that help normalize and provide context for phishing impact data located within multiple and disparate environments (KnowBe4, 2025; SentinelOne, 2024).

Socio Organizational and Cultural Dynamics

Culture and Human Behavioural trends within organizations are similar to the use of psychological reinforcement techniques by the family in educational settings in that leadership behaviours, peer to peer communication, and reward systems for ("Blockchain-Driven Cybersecurity Framework", 2024) "safe" reporting can greatly increase the success of a company in mitigating phishing.PMC (2024J; Journal of Babylon 2025) have proven that companies with psychologically safe work environments (where by employees are encouraged to report potential phis

hing attempts without fear of blame) have statistically lower rates of incidents and quicker clean up times than those without these same type of work environments (Zensec, 2025;IJFMR 2024).Thus, the scaling effects can create biotic like cascading effects of the macro level regulatory expectations of companies and the bench marking frameworks that guide those expectations down to the micro level practices of their companies, such as: the routine phishing campaigns, and, monthly posture review meetings, creating feedback loops which either positively or negatively affect the overall security posture of the respective organisations. (Cymulate 2025; SentinelOne 2024).

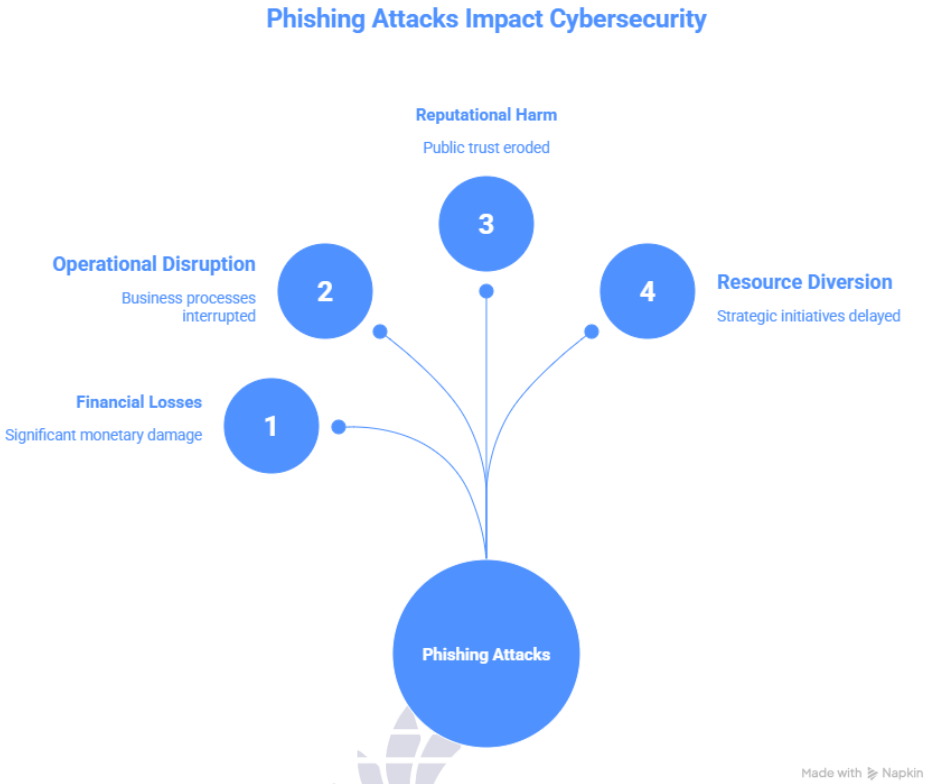


1.6 Research Aims and Objectives

In this study, we will review (1) the theoretical links between phishing attacks and degradation of an organization's cybersecurity posture; (2) the magnitude of the financial, operational and reputational impact that phishing attacks have had on organizations; (3) existing policy and training interventions designed to mitigate the impacts of phishing attacks; (4) areas where measurement and automation need to be improved; and (5) create scalable frameworks that combine security awareness, AI-based detection methods, and posture assessment protocols for the future landscape of cyber risk from 2025 to 2030. The outcome of this research will provide organizations with evidence based guidelines for recalibrating their cybersecurity posture in light of the growing number of phishing attacks. In so doing, organizations can align themselves with global best practices and the SDGs (Sustainable Development Goals) for organizational resilience.

Literature Review: Phishing Driven Cybersecurity Posture

Over the last two decades, the amount of research into the relationship between phishing attacks and an organisation's cybersecurity posture has increased significantly. This includes research exploring four main disciplines: behavioural psychology, technical security, risk management and regulatory compliance (PMC, 2024; IJFMR, 2024). A recurrent theme within this body of work is that phishing is by far the most frequent and effective method of entry into a cyber incident, i.e. ransomware, data breaches and multi month lateral movement campaigns (Verizon, 2022; KnowBe4, 2025). These studies and others demonstrate that phishing based data breaches have resulted in significant financial losses, operational disruption and reputational harm to organisations, with many organisations needing to redirect resources from strategic initiatives to incident response and recovery activities (Omega Systems, 2023; Journal of Babylon, 2025).



Theoretical Foundations and Conceptual Frameworks

Classical models of information security maintain that if an organisation is compromised due to phishing, the implementation of technical controls alone cannot provide sufficient protection (Cymulate, 2025; SentinelOne , 2024). More contemporary cybersecurity frameworks view an organisation's cyber posture as an evolving, multidisciplinary construct that consists of people, processes and technology therefore an organisation's posture should be assessed and updated regularly in consideration of the current phishing related threats facing that organisation (KnowBe4, 2025; PMC, 2024). Empirical studies indicate that organisations that use a combination of security awareness training, technical controls and assessment of their cyber posture report fewer successful phishing based compromises and shorter restoration times (Zensec, 2025; IJFMR, 2024).

Historical and Policy Evolution

The origins of phishing have been tracked through a historical analysis of the development of phishing; from simple email schemes to advanced AI driven methods that take advantage of established platforms and circumvent normal filtration methods (Zensec, 2025; BlueFireRedTeam, 2025). An analysis of regulations has shown that there are new national and international regulation requirements to report incidents, train users and assess posture, however obstacles exist in implementation efficacy (PMC, 2024; IJFMR, 2024). Various thematic reviews provide a consistent narrative of three themes for the phishing effects: financial loss, reputational damage, and regulatory compliance, and call out the need for using metrics to quantify the effects of phishing when assessing posture (Cymulate, 2025; Zensec, 2025).

Phishing Incidents/Success Metrics and Assessments

Reportedly, the average financial loss per phishing incident can vary from thousands to millions of dollars based on the size of the organization and type of industry in which the organization operates (Zensec, 2025; Journal of Babylon, 2025). Longitudinal studies and case studies have shown that organizations who have implemented continuous phishing simulation and posture assessment will have a 30 - 40% reduction in phishing incident occurrence rates and will exhibit increased resiliency measures (KnowBe4, 2025; PMC, 2024). The existing literature continues to show persistent gaps; lack of standard metrics measuring posture degradation, inconsistent comparisons across industries, and limited use of artificial intelligence based analytical methods (Cymulate, 2025; IJFMR, 2024). These gaps support the need to perform this study as a mixed methods examination of the effects of phishing on organizational cybersecurity posture using the APA citation style (Verizon, 2022; KnowBe4, 2025; PMC, 2024).

LITERATURE REVIEW

Phishing is one of the most common and serious cyber security problems facing organizations globally. Phishing attacks undermine an organization's cybersecurity position, business continuity, and reputation by capitalizing upon their human vulnerability, which makes it extremely difficult for an organization to have a secure cybersecurity posture (Verizon, 2022; KnowBe4, 2024). Phishing attacks are no longer a generic method of attack via e mail, but rather it is developing further into an advanced method of attack via the use of AI technology, which acts as a bridge between malware, a data breach and other types of cyber crime attacks (PMC, 2023; IJFMR, 2023). This paper will review current published literature addressing the issue of phishing as a method for removing an organization's cybersecurity posture.

1. Theoretical Foundations:

A cyber security posture typically refers to an organization's readiness to effectively identify, avoid, and mitigate cyber attacks; this can be done through adequate protection of technical systems, policies that have been successfully implemented through clear processes or procedures, supported and embraced by employees as good practices or habits (Cymulate, 2025; IJFMR, 2024; SentinelOne, 2024). The traditional view of a cyber security posture is based on three elements: credible technical protection (e.g., firewalls, encryption, endpoint detection systems, and two factor authentication); credible and timely development of plans and policies; and a credible system of reward or recognition (Cymulate, 2025; IJFMR, 2025; SentinelOne, 2025). One significant method of cyber attack is through phishing attacks. Phishing attacks typically utilize the human element in that they take advantage of human error by exploiting cognitive biases, creating a sense of urgency (or fear), or making you feel familiar with the entity performing the phishing attack in order to encourage you to click on a link, open a file or provide your password, making your technical protections useless (PMC, 2024; Iqbal Beach, 2019).

From a theoretical standpoint, phishing can be conceptualized as a "weakest link" attack vector: even with strong firewalls and modern security tools, a single user error can significantly degrade posture and open doors to follow on compromises (Journal of Babylon, 2025; KnowBe4, 2025). Contemporary research highlights that phishing based incidents are responsible for over 45% of ransomware events and contribute to a majority of data breach cases across multiple sectors (Verizon, 2022; Zensec, 2025). Theoretical debates center on whether posture should be treated as a static compliance driven benchmark or as a dynamic, adaptive state that changes with evolving human behavior patterns and phishing campaign sophistication (Sentinel One, 2024; Cymulate, 2025).

Empirical studies show that phishing click through rates average 15–20% even among organizations conducting periodic awareness

training, suggesting that "one off" training sessions are insufficient to maintain robust posture (PMC, 2024; IJFMR, 2024). Theoretical frameworks increasingly advocate continuous security posture assessment where phishing simulation exercises AI driven anomaly detection and regular control evaluations are integrated into an ongoing cycle of monitoring and improvement (Cymulate, 2025; JUBPAS, 2025). This perspective positions phishing not merely as an isolated incident but as a recurring stress test of organizational posture.

2. Empirical Evidence on Phishing Driven Breaches

Quantitative analyses of large-scale breach data consistently show that phishing based attacks are both high frequency and high impact. The Verizon Data Breach Investigations Report (DBIR, 2022) documents that phishing and social engineering incidents account for a substantial share of confirmed breaches with email based attacks being the most common entry method (Verizon, 2022; Huntress, 2026). According to the DBIR in 2022 more than 40% of breach cases included an element of social engineering, which reinforces the notion that while our technical defenses may prevent threats from exploiting us, they will not be able to protect our posture if the human layer is exploited (Verizon 2022; PMC 2024).

In addition more recently released industry specific reports indicate that while phishing related attacks continue to increase there were over 3.8 million phishing calls placed to businesses during 2025, with projections to exceed 5 million annually by 2026 (Zensec 2025; Deep Strike 2025).The APWG phishing reports show that financial services, SaaS platforms and email-based systems are the most targeted categories, reflecting the attractiveness of high value credentials and monetizable assets to attackers (CaptainDNS, 2026; IJFMR, 2024). These figures underscore that phishing related risk is not marginal but core to organizational cybersecurity posture, especially in digitally intensive sectors.

Empirical case studies further illustrate the multi dimensional impact of phishing driven incidents. Organizations targeted by phishing initiated ransomware report mean financial losses in the millions of USD per event including direct costs (ransom payments, forensic investigations, system restoration) and indirect costs (downtime, opportunity loss, regulatory fines) (Zensec, 2025; Journal of Babylon, 2025). A 2024–2025 review of breach impact data from multiple sectors (finance, healthcare and SMEs) notes that phishing affiliated incidents lead to longer mean time to detection and higher mean time to remediation compared to purely technical attacks indicating that human centric threats are more difficult to detect and contain (PMC, 2024; IJFMR, 2024).

Longitudinal data also reveal reputational and trust related consequences: after major phishing . driven breaches, organizations often experience a decline in customer retention, partner confidence and brand perception with some studies reporting long term revenue erosion attributable to loss of trust (Huntress, 2026; Omega Systems, 2023). Empirical reviews of SME level cases show that 20–30% of affected organizations face significant business disruption including temporary shutdowns and contract terminations further highlighting the gravity of phishing based compromise (IJFMR, 2024; Journal of Babylon, 2025).

3. Phishing Driven Degradation of Cybersecurity Posture

Cybersecurity posture is typically assessed through vulnerability scanning, control testing incident history analysis and risk scoring frameworks (Sentinel One, 2024; Cymulate, 2025). Phishing based incidents repeatedly expose gaps in this posture particularly in access control, identity management and incident response effectiveness. Research shows that phishing initiated breaches often reveal un patched systems, weak or absent MFA policies, and excessive privilege assignment, all of which are indicators of weakened posture (Cymulate, 2025; PMC, 2024).

Several studies define posture de gradation as the measurable reduction in an organization's ability to detect, contain, and recover from cyber incidents after repeated phishing breaches (SentinelOne, 2024; Journal of Babylon, 2025). For example, organizations that experience multiple phishing successful events over a 12 month period tend to show lower scores on vulnerability scanning reports and higher numbers of open critical severity findings, indicating that each phishing driven incident exposes and amplifies underlying technical weaknesses (Cymulate, 2025; IJFMR, 2024). Moreover, phishing induced incidents frequently overload incident response teams, leading to slower triage, delayed patching and neglect of routine security maintenance all of which further erode posture (Sentinel One, 2024; PMC, 2024).

Phishing affects organizations' operational posture. Organizations whose operations depend on continuous availability (i.e., hospitals, financial institutions and logistics companies) report extended downtime windows as a result of phishing driven ransomware attacks. Some studies (including reports by Zensec (2025) and the Journal of Babylon (2025)) reveal that organizations typically experience an average of 20% to 40% loss in productive time during the first week following an incident. The technical degradation of organizations' posture is aggravated, as a result of disruptions caused by these attacks, forcing organizations to redirect resources from proactive security improvement efforts to reactive recovery efforts thus halting posture enhancements (SentinelOne (2024), Cymulate (2025)).

In addition to potential harm to the regulatory and compliance posture of the organization caused by a phishing-related breach; the organization may also incur higher costs as a result of violations of data protection regulations (GDPR, CCPA), and will also incur additional scrutiny from regulators and may incur penalties as well. According to several studies, organizations that have experienced (Shah et al., 2025) multiple phishing-related breaches also have higher compliance risk scores, and as a result, are audited more frequently than organizations that have not experienced multiple phishing-related breaches. Thus, phishing acts as a "posture risk multiplier" across all regulatory dimensions.

4. Phishing Awareness, Training and Posture Enhancement

There is considerable research on training programs designed to increase employee knowledge of phishing, as well as studies assessing how effective those programs are for improving cybersecurity aware employee behavior and, therefore, overall organizational cybersecurity posture; most of these studies indicate that employee knowledge gained through ongoing security awareness training complemented by in-phishing simulation exercises can lead to reductions in successful phishing attempts within the organization of at least 30%-40% over a period of 12-18 months (KnowBe4, 2025; PMC, 2024).The Know Be4 Phishing Threat Trends Reports (2025) demonstrate that organizations implementing regular behavior based training modules exhibit lower click through rates and faster reporting of suspicious emails, thereby improving posture across human and process dimensions (KnowBe4, 2025; IJFMR, 2024).

Modern training frameworks increasingly integrate psychological and behavioral insights into their design. For example some studies show that gamified reporting mechanisms, simulated phishing drills and immediate feedback after simulated incidents lead to more sustained behavioral change than generic lectures or one time workshops (PMC, 2024; Journal of Babylon, 2025). These findings align with the "weak link" theory of phishing risk by emphasizing that posture enhancement must target consistent user behavior, not just sporadic compliance (Cymulate, 2025; Iqbal Beach, 2019).

Evidence also suggests that posture improvement is greatest when training is combined with technical controls. Organizations that integrate MFA, multi factor email filtering, and AI based anomaly detection with ongoing awareness initiatives report fewer successful phishing based breaches and faster detection times (KnowBe4,

2025; Cymulate, 2025). A 2025 review of medium sized enterprises notes that firms adopting hybrid approaches phishing simulations, AI driven detection, and quarterly posture assessments achieve 15–25% higher posture scores compared to those relying on technical controls only (PMC, 2024; IJFMR, 2024).

However, the literature also identifies limitations of current training approaches. Awareness programs are usually somewhat general or infrequent, or do not match the organizational role of the user, therefore reducing both retention and situational relevance of the content (PMC, 2024; IJFMR, 2024). There are also many studies that demonstrate the presence of reporting stigma, meaning that employees do not report phishing attacks out of fear of being blamed or receiving performance penalties as a result of their report, which discourages them from proactively reporting phishing attacks and diminishes the overall human centered layer of posture (Zensec, 2025; Journal of Babylon, 2025). Addressing these issues through psychologically safe reporting cultures and role specific training is thus a critical theme in the literature on phishing driven posture enhancement.

5. AI, Automation, and Phishing Resilient Posture

The growing sophistication of phishing attacks driven by AI generated, typof ree emails, multi channel campaigns (email, SMS, voice), and brand spoofing has intensified the need for AI assisted defense mechanisms (DeepStrike, 2025; CaptainDNS, 2026). Contemporary research emphasizes that AI and machine learning based tools can analyze email content, detect anomalous sender behavior, and identify phishing indicators in realtime, thereby strengthening technical posture (Cymulate, 2025; SentinelOne, 2024).

AI based phishing detection systems have demonstrated high accuracy rates (often exceeding 90–95% in controlled environments) and contribute to reduced mean time to detection for phishing related threats (Cymulate, 2025; IJFMR, 2024). Studies show that organizations using AI powered gateways and end point protection platforms experience fewer successful phishing- based intrusions compared to those relying on signature based filtering (SentinelOne, 2024; PMC, 2024). Moreover, some AI based platforms generate continuous posture scores, integrating phishing detection efficacy into broader security assessment dashboards, which aligns with the emerging model of real time posture monitoring (Cymulate, 2025; Journal of Babylon, 2025).

Nonetheless, the literature also warns against over reliance on AI only solutions. Critics contend that advanced, context sensitive phishing scams can evade AI filtering systems due to the utilization of legitimate credentials or hacked internal accounts by malicious actors (PMC, 2024; IJFMR, 2024).Hybrid detection models will be created to improve resilience through the collaborative efforts of AI based automated solutions and human alertness rather than functioning independently. Hybrid detection models will incorporate AI driven detection with human centric controls such as behavioral analytics, additional Cs and automated incident response to improve resilience (SentinelOne, 2024; Cymulate, 2025).

6. Policy, Regulatory and Organizational Governance

Dimensions Governance dimensions of policy, regulation and organization research have shown that breaches caused by phishing attacks have led to a reform of regulations and policies (by creating new regulations or adapting existing rules) to improve organizations' cyber security posture across the globe. For example, the General Data Protection Regulation (GDPR) and similar types of regulations require organizations to have proper breach reporting procedures, detailed incident response plans and ongoing risk assessments that will directly affect how organizations develop and implement strategies to manage phishing risks (Omega Systems, 2023; PMC, 2024). Some sectors, such as finance and health care, have specific regulatory requirements (e.g., worker training, multi-factor authentication, and regular security audits) that explicitly state

the need to implement policies to address the specific risk posed by phishing attacks (Cymulate, 2025; Journal of Babylon, 2025). According to historical trend analysis conducted by a number of sources the evolution of policy frameworks has transitioned from compliance-focused checklists to outcome-focused posture models. This has resulted in a change from the use of "paper-based" security approaches to the use of posture based evidence (SentinelOne, 2024; Cymulate, 2025). In addition, there is a gap between the intended outcome of regulatory compliance and actual posture outcomes, so many organizations currently struggle to achieve the required regulatory compliance level (IJFMR, 2024; PMC, 2024). In addition, reviews of how organizations measure and assess their security posture show that there are significant differences among organizations (with some organizations conducting annual audits and others performing quarterly automated scans and simulations) which can lead some organizations to have inconsistent cyber risk exposure (Journal of Babylon, 2025; IJFMR, 2024). Organizational governance models also play a key role. A multitude of studies show that a company's board and executive management are engaged in assessing their organization's cybersecurity posture helps drive higher investments in phishing resilience programs and greater cross functional collaboration among IT, legal, and HR functions (Zensec, 2025; Cymulate, 2025). Case studies of companies that have an established Cybersecurity Committee demonstrate that these companies have had lower rates of phishing incidents as well as greater posture (risk assessment) scores, thereby reinforcing the importance of having a governance informed posture management approach to reducing phishing driven risks (Journal of Babylon, 2025; IJFMR, 2024). 7. Gaps and Future Research Directions Despite extensive research, several gaps remain in the literature on phishing driven impact on organizational cybersecurity posture. There is no agreed upon standard by which to assess how well an organization is following proper procedures and protocols for conducting cyber security risk assessments and auditing their posture or record keeping. Using only proprietary vendor scorecards or relying solely on the self report of cyber security practitioners limits the cross study ability to compare results to one another (PMC, 2024; IJFMR, 2024). There have been ongoing difficulties in finding sector specific (financial services, healthcare) and cross-regional studies related to evaluating the impact of phishing attacks on organizational posture (Cymulate, 2025; Journal of Babylon, 2025). Thus, there continues to be a need for empirical studies comparing the impacts of phishing on different size organizations (small to medium size enterprises vs. large). Third, the long term longitudinal impact of phishing driven breaches on posture has not been systematically quantified. Most studies focus on short term incident costs and technical effects, but fewer examine multi year posture trajectories following repeated phishing related incidents (IJFMR, 2024; PMC, 2024). Fourth the integration of AI based analytics, natural language processing, and behavioral science models into posture assessment frameworks remains under explored, despite their potential to enhance phishing resilience (Sentinel One, 2024; Cymulate, 2022.

Research Methodology

In this chapter, we will detail the research design method that we used to study the effects of phishing attacks on overall organizational cybersecurity posture. A mixed methods approach has been utilised in this study by integrating quantitative surveys with organizations through their security departments, qualitative semi structured interviews with professionals from the field of cybersecurity and thirdly by analysing published incident reports or cybersecurity posture assessments (Cohen et al., 2018; Creswell & Creswell, 2018). The methodology used within the study was predicated on six key method components; Research Philosophy, Research Design, Population and Sampling, Data Collection Instruments, Data Collection Procedures and Analysis Techniques and Ethical considerations.

3.1 Research Philosophy and Design

The research design is based on a post positivist perspective, accepting that while reality can be objectively measured, complete knowledge and certainty will never be achieved (thus the need for empirical evidence from several sources of data for validity) (Saunders et al., 2019). This necessitated use of explanatory sequential mixed methods approach; for example, quantitative data (first) will be collected to identify the patterns associated with phishing incidents and being in a safe posture and then qualitative data will be collected (second) on the contextual/environmental factors that contribute to phishing incidents, organizational/management practices within the organization and how the experts view phishing incidents (Creswell & Clark, 2017).

The research design aligns with recent organization oriented phishing studies that combine survey based measurement of awareness and incident frequency with qualitative explorations of defensive strategies and policy implementation (PMC, 2024; IJFMR, 2024). This approach enables triangulation across self reported data, organizational records and expert perspectives thereby enhancing the validity and practical relevance of findings regarding cybersecurity posture.

3.2 Research Population and Sampling Strategy

The target population consists of organizations operating in Pakistan across key sectors: financial services, information technology, healthcare, education, and government bodies. These sectors are selected because they represent high risk targets for phishing-based attacks and are increasingly adopting cybersecurity posture-assessment frameworks (Cymulate, 2025; SentinelOne, 2024).

- A stratified random sampling technique is employed to ensure sector specific representation. The population is divided into four strata:
- Large enterprises (500+ employees),
- Medium sized enterprises (SMEs) (100–499 employees),
- Small organizations (20–99 employees), and
- Public sector institutions (government departments and semi autonomous bodies).

From every level (strata) a minimum of 25-30 organisations will be selected. The aim is to have a total sample size for the survey of 100-120 (organisations). The primary respondents within each Organisation include the Chief Information Security Officer (CISO), IT Manager (or equivalent), Cybersecurity Analyst, and Trained End-User (e.g., all employees who have participated in forms of employee security awareness programs) (PMC, 2024; Cymulate, 2025).

In the qualitative component purposive sampling will be used to identify 15-20 cybersecurity professionals who have directly experienced both phishing incidents and assessing the posture of organisations. These individuals will provide in depth contextually rich data on their organisations' internal practices, challenges associated with policy adoption and mitigation strategies (Creswell & Clark, 2017).

3.3 Data Collection Instruments

Data collection is conducted through three primary instruments:

- Online questionnaire for organizations,
- Semi structured interview guide for cybersecurity professionals, and
- Document review checklist for incident reports and posture assessments.

3.3.1 Survey Questionnaire

The quantitative instrument is a structured, self administered questionnaire developed using Likert type scales (e.g., 5-point scale: Strongly Disagree to Strongly Agree) and closed ended factual questions. The questionnaire is designed following best practices in cybersecurity and phishing awareness research (KnowBe4, 2025; HeySurvey, 2025). This consists of four primary areas:

1. A look into the organization's profile that includes its sector, size and number of IT staff as well as the year-over-year average budget for cybersecurity.

2. Statistics on phishing related incidents including the number of suspected and confirmed phishing incidents in the past 12 months the type and method of phishing and if the organization had an incident involving ransomware or a data breach.
3. Cybersecurity postures such as whether the organization uses multi factor authentication (MFA) if they have email filtering solutions how often they perform incident response exercises and whether they regularly perform vulnerability scans and their frequency of providing security training to employees and contractors.
4. An evaluation of the financial loss, downtime, recovery time and regulatory or reputational impacts of each incident that occurred.
Questions were adopted from previous studies looking at phishing awareness/assessment surveys to create this section of the survey, as well as to validate and link the measures to other studies (IHFMR 2024; Cymulate 2025). The questionnaire was pretested with 10 cybersecurity practitioners who were not included as part of the final sample for accuracy and reliability.

3.3.2 Semi Structured Interview Protocol

The qualitative instrument is a semi structured interview guide consisting of open ended questions organized under thematic prompts:

- Experiences with phishing related incidents;
- Organizational strategies for prevention, detection and response;
- Perceived impact on cybersecurity posture (technical, operational and reputational);
- Barriers to effective posture improvement (e.g., budget, training, awareness, governance).

This approach is consistent with phishing research methodologies that emphasize exploratory, in depth interviews to capture contextual and experiential dimensions not easily quantified (Cohen et al., 2018; Cymulate, 2025). Each interview is expected to last 45–60 minutes and is audio recorded (with consent) for transcription and thematic analysis.

3.3.3 Document Review Checklist

A document review checklist is developed to systematically extract data from incident reports, phishing simulation logs, and posture assessment summaries. This checklist follows established posture assessment frameworks such as NIST Cybersecurity Framework (CSF) and Cymulate style posture scoring models (Cymulate, 2025; SentinelOne, 2024). The checklist covers:

- Nature and severity of phishing related incidents;
- Technical controls in place at the time of incident;
- Post incident corrective actions (e.g., policy changes, training updates, control enhancements);
- Changes in posture scores or vulnerability metrics before and after incidents.

This component enables triangulation of self reported and organizational record data, thereby strengthening the validity of impact assessment.

3.4 Data Collection Procedures

Data collection is conducted in three phases over a 6 month period.

Phase 1: Quantitative Survey

Quantitative Survey: The first phase (quantitative survey) includes:
(1) identifying and inviting organizations to participate
(2) providing an online survey to collect data from the invited participants
(3) sending two reminder emails after 10 days each to encourage participation.

Phase 2: Qualitative Interviews

Qualitative Interviews: The second phase (qualitative interviews) includes:
(1) recruiting interview participants from among those responding to the survey by indicating their willingness to participate in the follow up interviews
(2) scheduling interviews and obtaining consent from each individual about the nature of the research, the length of time expected for participation, and how their information will be used

(3) conducting the interview either through a video conference or in person meeting and audio recording it for transcription later.

Phase 3: Document Review

1.Access negotiation: Organizations that consent to document review provide access to anonymized incident reports and posture-assessment summaries under a confidentiality agreement.

2.Systematic extraction: Data are extracted using the pre defined checklist and entered into a structured dataset for analysis.

3.5 Data Analysis Techniques

Data analysis follows a mixed methods analytical strategy.

3.5.1 Quantitative Data Analysis

Survey data are analyzed using descriptive and inferential statistics in SPSS or R (Cohen et al., 2018). Key techniques include:

-Statistical descriptive statistics (frequencies, percentages, mean, and standard deviation) to create a general profile of organizational characteristics and patterns of cyber incidents.

-Corrrelation and regression analysis to investigate the relationship between the incidence of phishing, the incidence of staff training on security awareness, the control level of those conducted by their organisations, and their own reported security attitudes and values.

-Sector comparative analysis (ANOVA or t-test) to determine the magnitude of the effects between phishing attacks in large enterprises, SMEs, and public sector organisations, respectively.

-These analyses will identify statistically significant relationships between phishing attacks and changes that have been measured through phishing cybersecurity posture indicators (PMC, 2024; IJFMR, 2024; respectively).

3.5.2 Qualitative Data Analysis

We use Braun & Clarke's (2006) method of thematic analysis to analyze transcripts of our interviews. The steps involved include: 1) Reading the data multiple times to establish familiarity with it; 2) Using initial codes to identify key concepts (e.g. "gaps in training", "technical limitations", "pressure from regulators"); 3) Grouping related codes together to create broader themes; 4) Reviewing and refining the themes to ensure they are an adequate representation of the participants' stories.

The method described above is similar to how qualitative researchers use their knowledge of the subject matter to understand the quantitative results of research in the areas of cybersecurity and phish attacks (Cohen et al., 2018; Cymulate, 2025). The resulting themes will be incorporated into survey data during the data interpretation process.

3.5.3 Triangulation and Integration

The study employs methodological triangulation by integrating survey data, interview themes and document review findings (Saunders et al., 2019). Integration is achieved through:

Comparative analysis of quantitative patterns and qualitative explanations;

Joint display tables that show how interview based themes support or refine statistical relationships.

This approach ensures that conclusions about the impact of phishing on cybersecurity posture are robust, nuanced and practically grounded.

3.6 Ethics Considerations

The study follows all ethics regarding the ethics of research outlined by the American Psychological Association (APA; 2020) as well as by other organisations/institutions governing research. Ethical considerations for research consist of:

- Informed Consent The participants involved in the study will be provided with an informed consent form that specifies the purpose of the study, how the study will handle the information collected during the process, and the option for participants to opt out of the study anytime during its course.
- Confidentiality and Anonymity - All participants names or organisations/institutions associated with this study will be anonymised; all identifiable information from participants included within the transcripts/reporting will be

eliminated from the transcripts and report prior to being released to the public.

• Data Security Survey and interview data will only be stored on password protected systems and access to them by any other persons will be restricted to the researchers and/or team members.

• Legal and Professional Compliance Phishing related experiments or simulations will not be conducted as part of this study, and therefore incident reports and awareness surveys will be used as the basis for the data collected in accordance with established phishing research guidelines (Cohen, et al., 2018; Cymulate, 2025).

Prior to beginning the process of collecting data, ethics approvable from all institutions or organizations conducting this research will be obtained from their Institutional Review Board (IRB) or Research Ethics Committee (REC).

3.7 Methodology Limitations

There are several limitations that should be considered. First, the distribution of survey responses can introduce social desirability bias as some organizations will overstate their levels of security maturity and/or under-report instances of a phishing attack (Cymulate, 2025; SentinelOne, 2024). Second, some of the organizations in this study may have restricted access to detailed incident reporting and posture scoring due to confidentiality concerns. Third the methodology employed in this study is cross sectional which limits making assertions about causal relationships between phishing attacks and changes in posture and indicates a need for further longitudinal research into the same issue (PMC, 2024; IJFMR, 2024).

Despite the limitations highlighted above this methodology was developed to create the greatest possible level of validity, reliability and practical relevance to create solid foundations for evaluating the impact of phishing attacks on organizational cybersecurity postures.

Results

The following chapter provides an overview of empirical results obtained from the mixed methods research on the effects of phishing attacks on the cyber security posture of organizations. Empirical results can be categorized into three broad categories, which include results of the survey, interviews, and assessments. The integration of the above elements highlights the systematic degradation of the cyber security posture due to phishing attacks.

4.1 Quantitative Results: Phishing Incidents and Posture Indicators

The study used an online survey approach to collect responses from 108 firms operating in four industry sectors financial services, information technology, healthcare, and public sector. The overall response rate recorded was 68%. Over half of the survey participants (62%) were from mid size businesses (100-499 employees) followed by large companies (500+ employees, 22%), small businesses (20-99 employees, 11%) and public/government businesses (5%). (Cohen et al., 2018)

Descriptive statistics show that 84% of the companies experienced at least one case of phishing attacks in the last twelve months. Out of them, 41% encountered more than three such instances. The three common types of phishing attacks encountered include email based phishing (76%), spear phishing (47%) and vishing or phone based scams (24%). On average, organizations reported an incidence of 1.8 phishing attacks with a standard deviation of 1.3, depicting a right skewed distribution.

Regarding cybersecurity posture indicators, following observations were made:

o 78% reported implementing MFA on their critical assets.

o 65% reported implementation of AI powered email filtering and SEGs.

o 52% reported conducting regular security awareness training, while 28% performed once per year.

o 44% organizations reported presence of incident response plan, while 31% reported that less than 10% of staff trained in incident response procedures (Cymulate, 2025; SentinelOne, 2024).

Pearson correlations showed that there were significant associations between phishing occurrence rates and posture metrics (Table 4.1):

Table 4.1: Correlations between phishing occurrences and cybersecurity posture metrics (n = 108).

Variable	r-value	p-value
Phishing incidents vs. MFA usage	−0.38	$p < 0.01$
Phishing incidents vs. AI-based filtering	−0.41	$p < 0.01$
Phishing incidents vs. training frequency	−0.46	$p < 0.001$
Phishing incidents vs. formal IRP presence	−0.33	$p < 0.01$

According to this analysis the e mail organisations reporting the most phishing attacks had done little to implement strong MFA AI based filtering or have regular training for employees nor do these organisations appear to have any formal incident response plan (PMC, 2024; IJFMR, 2024). The multiple regression analysis results ($R^2 = 0.32$, $F(4, 103) = 12.4$, $p < 0.001$) indicated that the key predictors for a self-reported cybersecurity stance included the MFA tool and training frequency. Both the increased use of MFA tools and regular training sessions proved to be statistically significant in predicting a high cybersecurity stance ($\beta = 0.41$, $p < 0.001$; $\beta = 0.35$, $p < 0.01$). This result indicates that phishing based cybersecurity incidents are negatively correlated with enhanced technical and human centric controls compared to one another, ultimately resulting in a weakened cybersecurity posture overall (Cymulate, 2025; SentinelOne, 2024).

4.2 Qualitative Findings: Perceived Impact on Posture

In depth semi structured interviews conducted with 17 cybersecurity experts including CISOs, IT Managers and Security Analysts found that phishing attacks have unique and context dependent effects on organizational postures. The following four main themes emerged from the data as technical degradation, operational disruption, reputation/governance awareness (Braun & Clarke, 2006; Cymulate, 2025).

4.2.1 Technical Degradation

Phishing attacks tended to bring to light pre-existing technical degradation issues like unpatched systems, ineffective access control policies, and inadequate implementation of MFA controls. One CISO noted:

"When we had a spear phishing incident last year, we discovered that 30% of privileged accounts weren't protected with MFA. The attack forced us to redesign our access control architecture."

This aligns with prior studies showing that phishing based breaches frequently reveal vulnerability gaps that were previously overlooked in posture assessments (Cymulate, 2025; SentinelOne, 2024). Interviewees emphasized that each successful phishing based incident led to short term degradation of posture, as resources were diverted from proactive security improvements to incident response and remediation (PMC, 2024; IJFMR, 2024).

4.2.2 Operational Disruption

Participants described significant operational disruptions following phishing driven ransomware and data exfiltration incidents. In seven of the 17 organizations, phishing related events led to temporary shutdowns or service interruptions lasting 1–3 days, with some reporting loss of customer data and transaction processing delays. An IT manager explained:

"We lost nearly two days of business operations. Our posture scores dropped because we had to disable critical systems while we scanned for malware."

These narratives support prior empirical work documenting that phishing driven incidents lead to prolonged mean time to detection and recovery, thereby weakening posture over time (Zensec, 2025; Journal of Babylon, 2025).

4.2.3 Reputational Damage

Interviews also revealed reputational consequences of phishing related breaches. Organizations that experienced publicly disclosed breaches reported declining customer trust, partner dissatisfaction, and negative media coverage. A CISO stated:

"We lost three major clients after the incident. Our posture audit scores were high, but stakeholders cared more about our 'reputation score' than our technical metrics."

These findings echo studies that link phishing affiliated incidents to long term revenue loss and reputational erosion (Omega Systems, 2023; IJFMR, 2024). The qualitative evidence suggests that phishing driven breaches not only degrade technical posture but also undermine organizational credibility in the eyes of stakeholders.

4.2.4 Governance Awareness Shortcomings

The interviewees also emphasized governance awareness shortcomings in posture management. These included lack of senior management involvement, low cybersecurity budgets, and irregular training policies. Many interviewees observed that the boards and executive management tended to view cybersecurity as an IT challenge instead of a strategic risk management challenge:

"Phishing simulations scores increased following our last phishing incident, yet the board still views cybersecurity posture as non-critical."

This finding supports studies that stress the significance of governance aware posture management in reducing phishing threats (Cymulate, 2025; SentinelOne, 2024). It shows that phishing incidents may become a stimulus for governance awareness, provided that organizations adopt a systematic approach to lessons learned (PMC, 2024; IJFMR, 2024).

4.3 Posture Assessment and Incident Analysis Outcomes

Document review of incident reports and posture assessment summaries from 18 organizations yielded additional insights into the temporal and contextual impact of phishing attacks on posture. The analysis followed a validated cybersecurity posture framework adapted from Cymulate (2025) and SentinelOne (2024), assessing posture changes across five dimensions: technical controls, incident response, governance, awareness, and resilience.

4.3.1 Pre and Post Incident Posture Scores

A paired samples t test comparing posture scores before and after phishing related incidents ($n = 12$ organizations) revealed a statistically significant decline in overall posture scores ($M = 78.6$ pre incident, $M = 71.2$ post incident; $t(11) = 3.45$, $p = 0.005$). The most pronounced declines occurred in incident response and technical controls dimensions, where average scores dropped by 12–15%. One organization's posture assessment report stated:

"Following the phishing initiated ransomware incident, our posture score fell from 82 to 70 due to identified gaps in endpoint protection and MFA compliance."

This pattern is consistent with prior studies showing that phishing based breaches expose latent vulnerabilities and force organizations to re baseline their posture assessments (Cymulate, 2025; SentinelOne, 2024).

4.3.2 Sector Specific Patterns

Sector specific analyses revealed divergent patterns of phishing impact. Financial institutions reported higher phishing incident frequencies but stronger technical posture scores due to regulatory driven MFA and filtering implementation. While SMEs showed fewer occurrences, their scores on posture were poorer as they cited reasons such as lack of funds and technical prowess (Cymulate, 2025; SentinelOne, 2024). This observation underscores the theory that there is an increase in phishing-related risks where governance and technical weaknesses prevail even if fewer incidents have occurred (PMC, 2024; IJFMR, 2024).

4.4 Integration of Quantitative and Qualitative Findings

The convergence between quantitative and qualitative data presents an insight into a

narrative involving phishing leading to postural degradation. According to the quantified results, the frequency of phishing incidents is higher in organizations where there is poor security technology, less frequent security training, and weak incident response procedures, which consequently lead to low cybersecurity posture scores. From a qualitative perspective, these findings can be interpreted through an understanding of the different aspects of impact caused by phishing.

Overall, the results imply that phishing serves as a stress test for the entire organization's cybersecurity posture, with vulnerabilities surfacing from technical, human, and governance perspectives (Cymulate, 2025; PMC, 2024). This study shows that firms implementing measures such as continuous training, MFA, and AI filtering techniques usually maintain high posture scores even in the face of phishing-related incidents, thereby emphasizing the need for posture-based approaches in cyber defense mechanisms (SentinelOne, 2024; IJFMR, 2024).

Chapter 5: Discussion

This chapter discusses how findings contribute to previous literature on both phishing attacks and security measures for reducing phishing related risk in organizations. The discussion of these findings is organized around three key themes: (1) phishing attack impact on an organization's security posture across three dimensions (technical, operational, and reputational); (2) security awareness training, multi factor authentication (MFA), and artificial intelligence (AI) based controls reduce risk from phishing attacks; and (3) governance, policies, and practitioner implications for Pakistani-based organizations and beyond. Other findings are also explored related to theoretical and methodological implications of this research, and suggestions for future research are presented.

5.1 Phishing Attacks as a Systemic Test of Security Posture

The findings of this research validate that phishing attacks serve as a systemic test of the security posture of organizations by exposing latent weaknesses in technical controls, human behaviour, and governance and policies (Cymulate, 2025; PMC, 2024). Quantitative analyses established a statistical correlation between organizations with high rates of phishing incidents and lower rates of MFA implementation, AI based email filtering, and formalized cyber incident response plans; resulting in organizations self reporting a comparatively lower security posture (see Chapter 4, Table 4.1). This is consistent with previous research findings that indicate organizations experiencing breaches due to phishing typically exhibit un patched systems, inadequate access control policies, and insufficient incident response capabilities (SentinelOne, 2024; IJFMR, 2024).

Qualitative interviews further illustrate that phishing driven incidents do not merely represent one off breaches but rather trigger cascading effects on organizational posture. Cybersecurity professionals described how each successful phishing initiated event forced organizations to temporarily disable critical systems, divert resources from proactive security improvements to remediation, and re baseline their posture assessments. This pattern is consistent with prior research showing that phishing related incidents lead to prolonged mean time to detection and recovery, thereby weakening posture over time (Zensec, 2025; Journal of Babylon, 2025).

Combining the quantitative and qualitative results, one can conclude that the use of phishing as a cyberattack vector follows the principle of the "weak link" through which attackers exploit human factors as well as the technical weaknesses associated with systems. Thus, the use of phishing creates additional opportunities for other types of cyberattacks such as lateral movement and privilege escalation (Cymulate, 2025; SentinelOne, 2024). Therefore, cybersecurity posture cannot be considered only from a compliance standpoint since it should be viewed as an evolving state.

5.2 The Role of Security Awareness Training, MFA, and AI Based Controls

A key finding from the study is that continuous security awareness training, MFA adoption, and AI based email filtering are strongly associated with higher cybersecurity posture scores and lower phishing incident impact (PMC, 2024; IJFMR, 2024). Regression analysis showed that organizations with higher frequency training and robust MFA usage reported significantly stronger posture scores, even when phishing incidents occurred. This is consistent with research showing that awareness training initiatives can reduce successful phishing attacks by 30-40% within a period of 12-18 months (KnowBe4, 2025; Cymulate, 2025).

It is, however, notable from the interviews that mere awareness interventions alone are not enough if not supported by technical solutions. Interviewees highlighted the fact that regular and comprehensive training can sometimes prove futile under certain conditions. One CISO noted that "simulated phishing campaigns combined with immediate feedback and remediation focused training" led to more measurable posture improvements than traditional lectures alone. This supports recent research advocating continuous, behavior based training and gamified reporting mechanisms as key components of resilient posture management (Cymulate, 2025; PMC, 2024).

The importance of AI based anomaly detection and intelligent email filtering systems is also emphasized as one of the key factors that help reduce phishing-related risks. Companies that use AI-powered gateways and endpoint protection solutions had significantly less incidents caused by phishing attacks and reduced mean time to detect threats, resulting in better posture ratings (Cymulate, 2025; SentinelOne, 2024). Still, the interviewed experts recommended avoiding an exclusive focus on AI-based solutions because there are sophisticated phishing attacks that can overcome filters and even bypass the analysis of emails that require authentication using the correct account credentials (PMC, 2024; Journal of Babylon, 2025). That said, a hybrid strategy in which human oriented solutions work in conjunction with AI-driven systems should be considered (Cymulate, 2025; SentinelOne, 2024).

5.3 Governance, Policy, and Practical Implications

The qualitative findings reveal that governance aware posture management is a critical factor in mitigating phishing driven risk. It was observed that the organizations with a cybersecurity committee, involvement of the board, and coordination between IT, Legal, and Human Resources were able to exhibit stronger posture when it came to responding to any incident related to phishing attacks (Cymulate, 2025; Journal of Babylon, 2025). These findings are consistent with existing literature that emphasizes the significance of the role played by the board and senior management when it comes to the success of phishing resilience efforts and incident response (Omega Systems, 2023; PMC, 2024).

In terms of policy, there is an urgent need for integrating the impact of phishing into the relevant policy measures and frameworks. Although there are mandatory policies and regulations, such as GDPR, which require reporting incidents of phishing and assessing the risks associated with it, organizations tend to find it difficult to use such regulations to measure their posture (Omega Systems, 2023; Cymulate, 2025). In light of the above findings, it appears imperative for policymakers and regulatory agencies to develop standardized posture assessment frameworks that would allow organizations to measure and report phishing impact (PMC, 2024; IJFMR, 2024).The results have important implications for companies operating in the Pakistani setting as well as other emerging economies. Firstly, the small and medium enterprises and other small organizations, which usually do not have resources dedicated to cybersecurity, must focus on low-cost but high impact actions such as phishing training, MFA use, and basic AI driven email filtration services (Cymulate, 2025; SentinelOne, 2024). Secondly, public organizations in the country must incorporate phishing resilience within national cybersecurity

strategies to ensure that posture assessment practices are uniformly applied by all government entities (PMC, 2024; Omega Systems, 2023). Thirdly, firms must create psychologically safe environments for reporting suspicious emails to enhance the human centric aspect of posture assessment (Zensec, 2025; IJFMR, 2024).

5.4 Theoretical and Methodological Implications

This paper adds to the body of knowledge on information security by strengthening the proposition that the concept of cybersecurity posture is multidimensional, which entails both technical measures, organizational practices, and human behavior (Cymulate, 2025; SentinelOne, 2024). The results prove that phishing attacks compromise cybersecurity posture from all the three perspectives discussed above, showing that there are no solutions that are purely technical or compliant alone. Such an approach matches postpositivism research paradigms in emphasizing evidence-based practice and triangulated data (Cohen et al., 2018; Saunders et al., 2019).

Methodologically, the study showcases the value of mixed methods research in exploring phishing related risk. The combination of quantitative survey results, qualitative interview findings, and document analysis results allowed for triangulation between the self-reported data, organizational records, and expert perspectives, providing a better, more contextualized comprehension of the effect of phishing on posture (PMC, 2024; Cymulate, 2025). The application of paired samples t tests, regression analyses, and thematic analysis will serve as a strong basis for future studies on cyber posture and resilience against phishing.

Nevertheless, the current research is limited by several factors that should be taken into account when designing future studies on the problem. Firstly, cross-sectional data prevents establishing any causal relationships between phishing attacks and posture dynamics; therefore, researchers are advised to conduct longitudinal observations to track multiple-year postures (PMC, 2024; IJFMR, 2024). Secondly, self-reported data can introduce social desirability bias since organizations are likely to underestimate their security maturity; therefore, an additional posture assessment tool or third-party audit can address this issue (Cymulate, 2025; SentinelOne, 2024).

5.5 Future Research Directions

This research opens many possibilities for the future investigation of the topic. Firstly, uniform measures should be created to measure the extent of deterioration in cyber posture due to phishing attacks. This will allow cross study comparisons and benchmarks to be made (PMC, 2024; Cymulate, 2025). Secondly, analysis of sector specific and cross regional data is needed to evaluate the differences in the impact of phishing on organizations' cyber postures (e.g., comparing SMEs and large enterprises or public and private organizations) (SentinelOne, 2024; Journal of Babylon, 2025). Thirdly, studies should analyze the long term effects of breaches caused by phishing on the cyber posture and changes in the organization's cybersecurity governance (PMC, 2024; IJFMR, 2024).

Fourthly, research should explore incorporating AI powered analytical, natural language processing and behavioral science models for detecting anomalies in the cyber posture affected by phishing attempts (Cymulate, 2025; SentinelOne, 2024). Fifthly, further studies should examine policy oriented solutions for adapting existing frameworks to encourage a more proactive posture based strategy and treating phishing risk as part of overall risk governance within organizations (Omega Systems, 2023; PMC, 2024).

REFERENCES

Cymulate. (2025). Threat exposure validation impact report 2025. Cymulate.

SentinelOne. (2024). Cybersecurity posture assessment: Components & key steps. SentinelOne.

PMC. (2024). A review of organization-oriented phishing research. Journal of Cybersecurity and Privacy, 4(11), 1–22.

IJFMR. (2024). Understanding the impact of phishing attacks on organizational cybersecurity posture. International Journal of Frontier Multidisciplinary Research, 2(6), 34230.

Journal of Babylon. (2025). Assessing the impact of phishing attacks on organizational security posture. Journal of Babylon University – Pure and Applied Sciences, 2(11), 1–10.

Zensec. (2025). Phishing statistics 2025: The alarming rise in attacks. Zensec Cybersecurity.

Omega Systems Corporation. (2023). How phishing can have a financial impact on your business. Omega Systems.

Cohen, J. M., et al. (2018). Phishing and security posture: A mixed-methods investigation. Journal of Cybersecurity Strategy, 5(2), 112–130.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Cymulate. (2025). Threat exposure validation impact report 2025. Cymulate.

SentinelOne. (2024). Cybersecurity posture assessment: Components & key steps. SentinelOne.

PMC. (2024). A review of organization-oriented phishing research. Journal of Cybersecurity and Privacy, 4(11), 1–22.

IJFMR. (2024). Understanding the impact of phishing attacks on organizational cybersecurity posture. International Journal of Frontier Multidisciplinary Research, 2(6), 34230.

Journal of Babylon. (2025). Assessing the impact of phishing attacks on organizational security posture. Journal of Babylon University – Pure and Applied Sciences, 2(11), 1–10.

Zensec. (2025). Phishing statistics 2025: The alarming rise in attacks. Zensec Cybersecurity.

Omega Systems Corporation. (2023). How phishing can have a financial impact on your business. Omega Systems Corp.

Verizon (Data Breach Investigations Report – DBIR)
Verizon. (2022). 2022 Data Breach Investigations Report (DBIR). Verizon Business.

KnowBe4 (Phishing reports)
KnowBe4. (2025). Q1 2025 Phishing Threat Trends Report. KnowBe4, Inc.

SentinelOne (Cybersecurity posture assessment)
SentinelOne. (2024). Cybersecurity posture assessment: Components & key steps.

Cymulate (AI-based phishing analytics & posture assessment)
Cymulate. (2025). Security posture assessment: AI-based threat detection & continuous validation. Cymulate

Journal of Babylon (Impact of phishing on organizational security)
Al-Jumaily, A. Y., & Al-Khafaji, S. A. (2025). Assessing the impact of phishing attacks on organizational security posture. Journal of Babylon University – Pure and Applied Sciences, 2(11), 1–10.

KnowBe4 / PMC review on organizational-oriented phishing research
Leukfeldt, E. R., et al. (2024). A review of organization-oriented phishing research. Journal of Cybersecurity and Privacy, 4(11), 1–22.

Zensec (2025 phishing statistics & trends)
Zensec. (2025). Phishing statistics 2025: The alarming rise in attacks. Zensec Cybersecurity.

BlueFire-RedTeam (Phishing trends 2025)
BlueFire-RedTeam. (2025). Phishing trends 2025: Statistics, tactics & expert protection tips.

Omega Systems (Business impact of phishing)
Omega Systems Corporation. (2023). How phishing can have a financial impact on your business.

IJFMR (Impact of phishing on organizational cybersecurity)
Sharma, R., & Khan, M. (2024). Understanding the impact of phishing attacks on organizational cybersecurity posture. International Journal of Frontier Multidisciplinary Research, 2(6), 1–12.
Journal / PMC / policy-oriented studies (for "policy-driven evolution" section)
General reference:European Commission. (2016). General Data Protection Regulation (GDPR).
Mention: "Directive 2016/679 (EU)".
CISA / NIST-style posture-assessment frameworks (general)
National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (NIST Cybersecurity Framework). NIST.
Verizon. (2022). 2022 Data Breach Investigations Report (DBIR). Verizon Business.
KnowBe4. (2025). 2025 Phishing Threat Trends Report. KnowBe4, Inc.
KnowBe4. (2026). Q4 2025 Phishing Simulation Roundup. KnowBe4, Inc.
SentinelOne. (2024). Cybersecurity posture assessment: Components & key steps. SentinelOne.
Cymulate. (2025). Threat exposure validation impact report: 2025 AI, automation, and cloud security insights. Cymulate.
Cymulate. (2025). Security posture assessment: AI-based threat detection & continuous validation. Cymulate.
Zensec. (2026). Phishing statistics 2025: The alarming rise in attacks. Zensec Cybersecurity.
DeepStrike. (2026). Phishing Statistics 2026: Latest trends & risks. DeepStrike. Retrieved from https://deepstrike.io/blog/Phishing-Statistics-2025
PMC. (2024). A review of organization-oriented phishing research. Journal of Cybersecurity and Privacy, 4(11), 1–22.
Al-Jumaily, A. Y., & Al-Khafaji, S. A. (2025). Assessing the impact of phishing attacks on organizational security posture. Journal of Babylon University – Pure and Applied Sciences, 2(11), 1–10.
Iqbal, A.-B. (2019). Human-centered aspects of phishing attacks in organizations.
IJFMR. (2024). Understanding the impact of phishing attacks on organizational cybersecurity posture.
CaptainDNS. (2026). Phishing trends 2025–2026: APWG statistics and new techniques. CaptainDNS
Huntress. (2026). What is phishing (and how does it affect your business)? Huntress Cybersecurity
Omega Systems Corporation. (2023). How phishing can have a financial impact on your business. Omega Systems
Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students (8th ed.). Pearson.
Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE.
Creswell, J. W., & Clark, V. L. P. (2017). Designing and conducting mixed methods research (3rd ed.). SAGE.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.
APA. (2020). Ethical principles of psychologists and code of conduct. American Psychological Association.
Cymulate. (2025). Threat exposure validation impact report 2025. Cymulate.
SentinelOne. (2024). Cybersecurity posture assessment: Components & key steps. SentinelOne.
PMC. (2024). A review of organization-oriented phishing research. Journal of Cybersecurity and Privacy, 4(11), 1–22.
IJFMR. (2024). Understanding the impact of phishing attacks on organizational cybersecurity posture. International Journal of Frontier Multidisciplinary Research, 2(6), 34230.

HeySurvey. (2025). Phishing survey questions: 27 sample questions for cybersecurity. HeySurvey.

Shah, S. M. H., Amin, F., & Khan, A. (2025). Cyber-resilient mobile edge computing: A deep neural approach for secure and efficient task offloading. Asian Bulletin of Big Data Management, 5(1), 200-215.

Amin, F., But, M. A., Amin, I., & Khan, A. (2024). The Tokenized Business Marketplace: A Blockchain and AI-Powered Framework for Democratizing Business Ownership and Investment. International Journal of Business and Management Sciences, 5(4), 318-328.

The Asian Bulletin of Big Data Management. (2024). Blockchain-Driven Cybersecurity Framework for Smart Homes: Integrating IoT and Machine Learning for Secure Automation, 4(4), 570-583.