The Role of Employees and End-Users in Strengthening Organizational Security Culture and Mitigating Human-Based Threats

IT-489 Captone Project

Abdullah Aldosariy

Dr. Osei

Marymount University

12/07/2025

Abstract

The paper examines the reality that the behavior of the employees is a significant threat to security and, at the same time, the most powerful defense mechanism. Literature synthesis helps the researcher to identify the essential human vulnerabilities, such as vulnerability to social engineering, poor password management, and non-adherence to the policy. It discusses some helpful actions, such as specialized security awareness training, behavior analytics, inculcation of a security culture, and implementation of Zero Trust Architecture. The results show that a multi-dimensional strategy, which incorporates the concept of lifelong learning, psychological concepts, and enabling leadership, is at the core of establishing the organizational cyber resilience.

The abstract underscores that the project does not propose a single technical solution as the answer to human-based threats. Instead, it reviews and organizes findings from existing academic and industry literature to show how different approaches reinforce one another. There are clearly identifiable weaknesses on one side: employees who fall for phishing emails, personnel who break rules because they think they're too hard to follow, and insiders who abuse their access. One side clearly has weaknesses that everyone can see. For instance, employees who fall for phishing emails, people who break regulations because they are too hard to follow, and people who misuse their access. On the other hand, there are strategic answers like continuing training, a security culture led by executives, and technology that watches behavior instead of just network data.

The study seeks to integrate these components under a cohesive framework. The paper elucidates the reasons behind the varying effectiveness of programs in mitigating risk by examining the interplay of human behavior, organizational culture, and technical controls. The

abstract makes it clear that the reader will get more than just a list of dangers and remedies. They will also learn how to support, guide, and empower staff and end-users in a way that improves overall cybersecurity.

Keywords

Cybersecurity, Human Factors, Security Culture, Employee Awareness, Insider Threats, Social Engineering, Behavioral Analytics, Zero Trust Architecture.

Table of Contents

Chapter 1: Introduction

Topic

The paper focuses on why organizational cybersecurity is needed by employees and why human factors are one of the largest vulnerabilities and a possible defense mechanism. Majority of organizations have ended up spending a substantial amount of money in the development of technological defenses, though human practices have provided a major path of attack that ought to be dealt with appropriately.

The topic emphasizes that modern organizations rarely fail in cybersecurity because their firewalls, antivirus tools, or monitoring systems are completely absent. Instead, they are commonly broken into because an employee clicks on a bad link, uses a weak password again, gives private information to the incorrect person, or doesn't follow a policy they don't fully understand. Employees and end users are the last line of defense for every security measure. They read emails, approve transactions, handle sensitive documents, and choose whether or not to follow business rules. Because of this, the same personnel who keep the firm functioning can also, by accident or on purpose, let attackers in.

So, the topic is at the crossroads of technology and how people act. It understands that companies can't just "buy" cybersecurity by getting tools and software. Instead, they must actively involve employees and end-users as partners in defense. This means understanding the types of human-based threats, the psychological and organizational reasons behind risky behavior, and the specific ways in which culture, training, and policies can transform employees from weak points into strong points in the security chain.

Overview

This article is a systematic discussion of human-based cyber threats and countermeasures. It provides the basis of the research, which is the problem statement, objectives, and questions, and then a literature review of human behavior in cybersecurity. The methodology is a description of analytical methodology, and the results are the data synthesis of best practices, the conclusion, and practical recommendations.

In more detail, Chapter 1 introduces the topic, explains why it matters, and frames the research problem in terms of employees and end-users as both vulnerabilities and protective assets. It also outlines the research objectives, formulates focused research questions, clarifies the significance of the study for academia and practice, and identifies existing knowledge gaps that justify the need for this work. Chapter 2 continues this by looking into what other people have written about cybersecurity dangers to people, employee behavior, security culture, and technologies that can help. It puts earlier findings into clear groups that match the research goals and problems, like insider risks, training for awareness, and Zero Trust principles.

Chapter 3 talks about the research approach utilized to put together the literature. It explains why a qualitative narrative review was used, how sources were chosen and examined, and how trustworthiness and ethics were taken into account. Chapter 4 shows the findings of this research by pointing out the significant patterns, themes, and linkages that came up in the studies that were looked at. Finally, Chapter 5 talks about these results, explains what they mean, talks about their limits, and gives practical advice and conclusions on how to improve the security culture of an organization and reduce dangers from people.

Research Objectives

This research projects to achieve these specific goals:

1. Determine key human-based vulnerabilities to security breaches.
2. Assess the efficacy of various security awareness training approaches.
3. Examine organizational determinants of security policy compliance.
4. Evaluate technological countermeasures to detect insider threat.
5. Establish practical measures to develop security-conscious employee pools.
6. Develop indicators of human-focused security programs.

These goals are meant to be clear and directly related to the research topic and issues. Finding significant human-based vulnerabilities requires finding certain actions and situations, such clicking on bad sites, mishandling credentials, or disregarding alerts, that happen over and over again in real-life situations. To figure out which training methods work best, you need to compare static, one-time sessions with more interactive and ongoing methods and find out which formats really impact behavior.

Looking at the organizational aspects that affect policy compliance goes beyond the person to include things like leadership commitment, communication style, and workload pressure, which all affect whether or not employees obey the regulations. When you look at technical countermeasures, you look at tools like behavioral analytics and monitoring systems that can find unusual usage patterns and possible insider threats. Creating practical steps to make employees more aware of security related ideas from books to actions that can be taken in the actual world, including design campaigns, reward systems, or ways to report problems. Lastly, creating indicators for human-focused security initiatives helps companies see if their efforts are working overtime by tracking changes in awareness, reporting, and behavior.

These goals make sure that the study not only talks about the problem but also suggests ways that organizations may deal with it.

Research Problem Statement

Human action or lack of action is the main form of cyber risk that is increasing in organizations. Technological investments notwithstanding, breaches by social engineering, accidental actions on part of an employee, or malicious insiders are devastating. The central issue is the lack of integration of human aspects in security strategy based on the generic training which cannot contribute to the behavioral change or profound security culture.

This problem statement makes it obvious that organizations often put their money in the wrong places and don't see where their dangers really are. Companies can still be hacked even if they have advanced firewalls and intrusion detection systems. This can happen if an employee falls for a convincing email or if protocols aren't followed because of time pressure. Generic, one-size-fits-all training usually sees employees as passive users of knowledge instead of active actors in defense. This means that lessons are rapidly forgotten and behaviors don't alter in a big way.

People make mistakes, but the problem is that many security strategies regard those mistakes as one-time events instead of signs of bigger problems with culture, communication, and support. Organizations will keep having incidents that get beyond technical defenses if they don't make human elements a big part of their cybersecurity planning. This may be done through personalized training, clear expectations, supportive leadership, and the right level of technology monitoring. This study seeks to fill this void by examining how staff and end-users might be more intentionally and efficiently incorporated into security policies.

Research Questions

1. What human behaviors most commonly lead to security compromises?
2. How can awareness programs maximize engagement and practice retention?
3. What factors significantly influence security policy compliance?
4. How can behavioral monitoring identify threats while respecting privacy?
5. How does Zero Trust Architecture complement human-centric security?
6. What components transform employees from vulnerabilities to assets?

These research questions focus on specific parts of the problem description. The first question asks what kinds of activities, habits, or blunders make it simple for attacks to happen over and over again. The second question is about how to build awareness programs that are enjoyable, beneficial, and memorable instead than boring or easy to ignore. This is a step in the right direction toward seeking answers. The third question says that following the rules isn't only a personal choice; it's also affected by the organization's rules, rewards, and constraints. The fourth question is about a very important balance: businesses need to watch how their employees act to detect threats, but they also need to respect their privacy and not make them feel like they can't trust them. The fifth question asks how Zero Trust principles, which don't assume trust and have strict access constraints, work with security measures that put people first. Finally, the sixth question ties everything together by asking what combination of culture, training, technology, and leadership is needed to transform how people see employees from being seen as threats to being seen as defenders.

These questions guide the structure of the literature review, the methodology, and the analysis, ensuring that the study remains coherent and directly connected to the central problem.

Research Significance 1

In academia, the study is a synthesis of the theoretical models that are used in cybersecurity in relation to human factors. It synthesizes the results of Protection Motivation Theory and Theory of Planned Behavior application (Noordeen & Bantan, 2025; Grassegger & Nedbal, 2021), comparing intervention techniques and revealing the research gaps in future behavioral change research.

By bringing together different theoretical perspectives, the research contributes to a more integrated understanding of why employees either follow or ignore secure practices. It doesn't just look at one model; it illustrates how many frameworks lead to the same conclusions: that perceived danger, self-efficacy, social pressure, and perceived control all affect how people behave when it comes to security. This synthesis helps academic readers understand where current ideas agree, where they disagree, and where more research is needed to explain complicated real-life situations in organizations.

The study is also important for academia since it links high-level theory to real-world business practices. It does not regard models like Protection Motivation Theory and the Theory of Planned Behavior as merely abstract constructs; rather, it investigates their use in shaping training, policy, and communication techniques. In doing so, it pushes for more study that tests these ideas in many types of organizations, industries, and cultures, especially as new dangers like AI-enhanced social engineering are always changing.

Research Significance 2

To practitioners, the study will offer evidence-based practice in human-centric security programs. It provides actionable information regarding training communication to various jobs (Kajzer et al., 2014, as cited in Khando et al., 2021) and the significance of leadership (Hwang et

al., 2019, as cited in Khando et al., 2021). Policy makers can utilize the findings to come up with standards that motivate human capital to invest in cybersecurity. Expansive effects compass increased domestic security and economic stability by lowering the rates of cyberattacks.

The study turns scholarly research into useful information for managers, security officials, and trainers. It stresses that different parts of a business, such finance, HR, IT, and customer service, confront different kinds of dangers and need diverse messages and examples. It also shows that leadership behavior is not just a symbol; when managers and executives actively model safe behaviors and support security efforts, workers are more likely to take them seriously.

The research provides a framework for politicians and regulators to promote investment in people, not just technology, by organizations. This could mean giving people rewards or setting rules that encourage security awareness programs, reporting incidents without fear, and sharing best practices across industries. Organizations can protect sensitive information, keep trust, and help the economy stay stable by using human-centered solutions to lower the number and severity of breaches.

Existing Gaps

There exist major gaps in knowledge despite human factor acknowledgement. There are gaps between the recognition of the problem and its successful implementation of the program (Bada et al., 2019, as cited in Khando et al., 2021). Technical detection and psychological models tend to be separated in research with no integration. Industry-specific issues need to be explored, and social engineering based on AI needs a new defense against attacks.

In practice, many organizations know that employees are central to cybersecurity, but their responses remain incomplete or inconsistent. Training can be put into place, but it should be

done in a way that checks to see if it improves behavior or is part of a larger set of cultural and technological changes. Research frequently examines technological systems and human behavior in isolation, complicating the building of comprehensive solutions that accurately represent everyday interactions with technology.

There is also a lack of knowledge about how different areas, like healthcare, education, finance, and public administration, deal with and respond to dangers that come from people. There are numerous basic guidelines, even if each industry has its own workflows, regulatory pressures, and sorts of data. Also, quickly developing threats like AI-enabled phishing, deepfakes, and automated social engineering need new techniques that mix human vigilance with better detection tools. These gaps show that we need study that doesn't just say "people are the weakest link," but instead looks into what is needed to make them the best line of defense.

Keyword Definitions

- **Cybersecurity:** Protecting systems, networks, and data from digital attacks
- **Human Factors:** How human characteristics influence system interactions
- **Security Culture:** Organizational values influencing security behaviors (Colabianchi et al., 2025)
- **Employee Awareness:** Staff understanding of security roles and threats
- **Insider Threats:** Security risks from authorized users (Alsowail & Al-Shehari, 2022)
- **Social Engineering:** Psychological manipulation for information access
- **Behavioral Analytics:** Monitoring user patterns for threat detection
- **Zero Trust Architecture:** "Never trust, always verify" security model

These keyword definitions provide a shared vocabulary for the rest of the paper.

In this case, cybersecurity isn't only about technical protections; it's also about all the steps that keep data and systems safe from illegal access, misuse, or damage. Human factors include the mental, emotional, and social parts of how people use technology at work, like their attention, judgment, habits, and teamwork. These can either make security stronger or weaker.

The fundamental attitudes and traditions that determine how employees regard security as everyone's job or just an IT issue are called security culture. Employee awareness stresses that workers need to know what kinds of hazards they face and what their individual job is in dealing with them. Insider threats show that those who have the right to access something can nonetheless be dangerous, either by accident or on purpose. Social engineering is a term that describes how attackers use trust and human psychology to get around security flaws. Zero Trust Architecture and behavioral analytics are innovative approaches to watch individuals and limit their access that work with, not against, them.

By making these definitions clear at the beginning, the chapter makes sure that when these terms come up later, they mean the same thing and are closely related to the study's focus on employees and end-users in organizational cybersecurity.

Chapter 2: Literature Review

Literature Overview

The most unstable part of the cybersecurity chain has always been pointed out to be the human component. According to Harper (2022023), despite the technical protection, such measures may be violated by humans. Cyber threat landscape is making use of this vulnerability more and more, and according to Verizon 2023 Data Breaches Investigations Report, reported by Colabianchi et al. (2025), 72% of data breaches have a human factor. The chapter is a synthesis of the current literature on the role of employees in cybersecurity, the range of human-based threats, the theoretical basis of learning about security behavior, and the strategies that have been suggested to reduce such threats. The review is organized based on major themes: nature of insider threats, psychology of security compliance, effectiveness of awareness training, and technological supports of managing human risk.

The literature overwhelmingly emphasizes that human factors are not just a secondary concern but often the primary point of failure in cybersecurity incidents. Organizations are always working to make their technological protections better, like firewalls, intrusion detection systems, endpoint protection, encryption, and access management. Attackers are learning that it's far harder to get around these protections than to trick people into making bad decisions. Because of this, cybercriminals change their tactics to include phishing, pretexting, impersonation, and taking advantage of strong feelings like fear or haste.

Researchers repeatedly assert that employees engage with digital systems daily, thereby perpetually confronting decisions that influence the organization's security posture. Even tiny choices, like clicking a link, saying yes to a request, sharing a file, or putting off an update, can

have big effects. This makes the human aspect more complicated. Unlike technology or software, individuals have feelings, cognitive limits, biases, stress, and different levels of awareness.

This chapter's assessment of the literature also shows that businesses typically don't comprehend what "human error" really means. Researchers contend that these errors arise from inadequate training, ambiguous policies, excessive workloads, ineffective communication, cultural factors, and insufficient reinforcement, rather than attributing blame to individuals. This moves the duty from the person to the organization, which must offer the right structure, support, and culture.

The literature on human-based hazards is wide and crosses several fields, including as psychology, behavior science, organizational theory, and information systems. The goal of this chapter is to integrate these insights into a coherent understanding that informs the rest of the research.

Literature Search Strategy

Academic databases such as Google Scholar, Scopus, and Web of Science were searched thoroughly, and only the relevant literature was found. The keywords were: information security awareness, insider threat, security culture, employee cybersecurity behavior, phishing, behavioral analytics, and Zero Trust. Peer-reviewed journal articles, conference proceedings, and reputable industry reports within the past decade were narrowed down to the latest edition to make the search relevant. The identified literature was discussed to detect the common themes, theoretical backgrounds, empirical evidence, and research gaps.

Literature Findings

The Spectrum and Impact of Human-Based Threats

There are two major categories of hazards associated with humans: purposeful and incidental. There are, in fact, a lot of unintentional dangers caused by negligence or ignorance. According to Raza et al. (2025), one of the main causes of security breaches in the banking industry is related to employees and can be classified as falling prey to phishing. In a similar vein, Yusuf (2024) contends that one of the main problems is human mistakes, since people will give critical information to the wrong person. These actions are typically the consequence of inadequate training, situational awareness, or a security-conscious mindset rather than malicious intent.

Employees often fall victim to:

- Emotionally manipulative messages
- Fake invoices
- Urgent “CEO requests”
- Password reset scams
- Fake job or HR messages
- Social engineering via phone or SMS

The literature emphasizes that most employees do not intentionally take risks; instead, they are manipulated through psychological pressure, lack of verification steps, or poor understanding

of digital risk indicators.

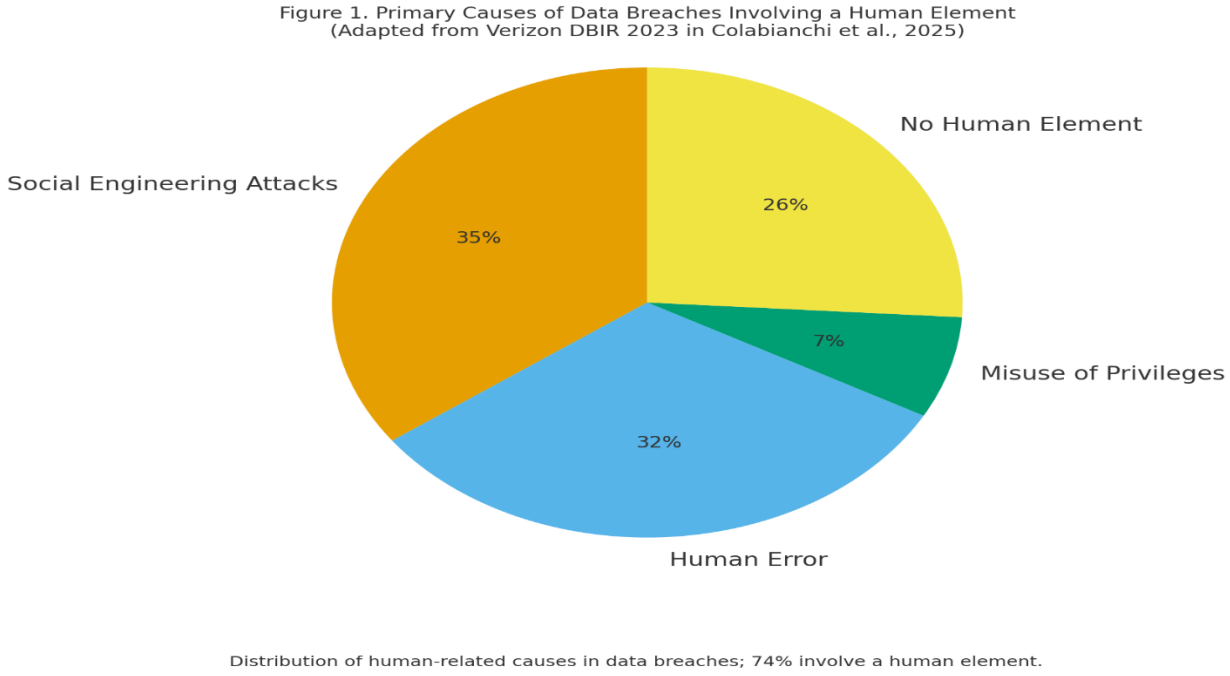

Figure 1. Distribution of human-related causes in data breaches, illustrating that the majority (74%) involve a human element, with social engineering and errors being the most prevalent. *Source: Adapted from Verizon DBIR 2023 in Colabianchi et al. (2025).*

Threats posed by malicious insiders are less common, though potentially much more harmful. Alsowail and Al-Shehari (2022) refer to an insider threat as an employee or a former employee who deliberately uses his or her legitimate access to cause harm to the organization. Their analysis shows real-life cases of sabotage, fraud, and intellectual property theft, highlighting the extreme financial and reputational implications. The problem with malice insiders lies in their capability to bypass the perimeter defenses, and thus they are hard to detect by traditional security tools.

The most common attack vectors that take advantage of human psychology are social engineering, mainly phishing. The use of the Theory of Planned Behavior perspective led

Grassegger and Nedbal (2021) to discover that the attitude, perceived behavioral control, and subjective norms of an employee influence the intention to resist social engineering. Noordeen and Bantan (2025) take this issue to the age of AI and explore how people perceive and react to AI-based deepfakes threats, and find that the vigilance of humans is going to become more critical as the sophistication of the attacks increases.

Constructing a Human Firewall: Awareness, Training, and Culture

One of the main ways to combat the weaknesses of humans is to increase the Security Education, Training, and Awareness (SETA). In their systematic review, Khando et al. (2021) identified the use of different approaches, where theoretical frameworks (e.g., PMT, TPB) and gamification are among the most commonly used in both the private and governmental sectors. They stress that successful training needs to be ongoing, interactive, and personalized. As an example, Parsons et al. (2014, as cited in Khando et al., 2021) revealed that contextualized case studies are more efficient than generic training.

The most critical concept is the idea of a security culture. A Delphi study of experts conducted by Colabianchi et al. (2025) proposed developing a culture oriented to cybersecurity as one of the main managerial actions to be taken. These include leadership conveying strategic security objectives and connecting them to corporate strategy. Good culture will enable security to be a value rather than a collection of rules to be observed. Tsohou et al. (2015, as cited in Khando et al., 2021) explain that promotion of such culture needs to be changed on an individual, organizational, and technological level, and consider security awareness as a process constructed socially.

During this cultural transformation, leadership is a very important element. Several works (Hwang et al., 2019; Marks and Rezgui, 2009, cited in Khando et al., 2021) prove that apparent

involvement of top management and its participation contribute significantly to the security awareness and conscientiousness of the employees. When leaders embrace security, it implies that they have value in the organization.

Technology Enhancement: Behavioral Analytics and Zero Trust

Technology can be used to monitor and enforce safe behaviors, even while training focuses on the front end of the problem. Behavioral analytics is one of the preventative measures against insider threats. According to Alsowail and Al-Shehari (2022), these technologies offer a foundation for typical user behavior and highlight anomalies that may indicate malicious intent or distinct accounts. Compared to traditional and rule-based surveillance, this method has shown higher recognition.

The Zero Trust Architecture (ZTA) paradigm reduces trust assumptions by providing a structural model. By putting the minimum privileges idea into practice and offering continuous verification, ZTA lessens the potential damage caused by both external and internal attacks. By ensuring that a user may only access what is necessary for their position, it reduces the likelihood of attacks.

Summary

The literature remains consistent in confirming the fact that employees form a critical, and in many cases, the most vulnerable part of the cybersecurity chain. Threats are divided into accidental mistakes and intentional ones, and one of the tools is social engineering. To eliminate such threats, a multi-pronged approach is needed, which is more than a single training session. It requires developing a culture of pervasive security that is leadership-driven, with the encouragement of informative and ongoing awareness campaigns, and enhanced by such

technologies as behavioral analytics and Zero Trust principles. The next chapter will outline how these strategies would be analyzed and synthesized to form a unified approach to action.

Chapter 3: Research Methodology

Overview

This study utilizes the qualitative narrative review method to synthesize human factor cybersecurity literature that exists. The methodology will combine the results of various academic sources in order to create a comprehensive insight into the employee-centric approach to security that will be suitable when answering exploratory questions aimed at obtaining the state-of-the-art summary as opposed to hypothesis testing (Macapagal & Tablarin, 2021, as cited in Harper, 2023).

The qualitative narrative review is appropriate because this research focuses on understanding how and why employees contribute to cybersecurity strengths or weaknesses within organizations. Human-based cybersecurity issues cannot be measured purely through statistics or experiments; they require interpretation of patterns, behaviors, motivations, and organizational influences. A narrative review lets the researcher look at patterns across several papers, pull out the most important themes, and come up with a unified vision of the area.

Narrative methodology facilitates an in-depth examination of intricate aspects, including human error, security culture, motivation, leadership impact, awareness training, and insider threat detection—elements that necessitate contextual understanding unattainable through quantitative research alone. This issue is interdisciplinary, incorporating elements from psychology, information systems, management, and cybersecurity. The narrative approach facilitates the adaptable integration of diverse academic viewpoints.

The technique also helps the project's goals, which are to find weaknesses, test training methods, look at how organizations affect things, and see how well complimentary technologies

like behavioral analytics and Zero Trust Architecture work. The narrative design helps frame these issues holistically.

Research Justification

The methodology of narrative review is appropriate in this study since the subject of interest cuts across several academic fields that need the synthesis of various perspectives. The objective is to make greater coverage of integrative knowledge insight as opposed to limited statistical meta-analysis in order to recognize tendencies, discrepancies, and deficiencies needed in delicately grasping the information.

A narrative review also allows examination of emerging trends such as AI-generated phishing, behavioral fatigue, and evolving reporting culture within organizations. These areas have rapidly developing literature that is not yet mature enough for meta-analysis. The narrative method makes it possible to include both foundational works and newly published findings.

In addition, because this research aims to understand employees' roles in cybersecurity holistically, the methodology supports evaluating both the technical components (like behavioral analytics and Zero Trust) and the non-technical components (such as training effectiveness, psychological theories, and leadership impact). This provides a richer, fuller picture of how human factors influence security outcomes.

Contextualization

This research addresses:

- What human behaviors cause security compromises?
- How can awareness programs maximize effectiveness?
- What factors influence policy compliance?
- How can technology augment human security?

These questions serve as a framework for the entire process of gathering and analyzing data. They help choose which sources to use, which themes to look at, and which pieces of evidence to compare. Every question is related to a specific goal of the research, which keeps the technique focused and clear.

Putting the study in context also makes it clear that the goal is not to directly examine how employees act, but to look at what previous research says about such actions. The analysis organizes the literature around these topics to show commonalities across different types of organizations and find the most reliable signs of safe or unsafe behavior.environments and identifies the most consistent predictors of secure or insecure behavior.

Data Collection Methodology

Data collection involved:

1. Source identification using academic databases with targeted keywords
2. Screening and selection applying relevance and peer-review criteria
3. Forward and backward citation searching for comprehensive coverage

The data collection process followed a structured and transparent approach to ensure reliability. The initial search produced a large pool of articles, but only those directly related to security behavior, insider threats, training effectiveness, organizational culture, and supporting technologies were included.

Articles were filtered based on publication date to ensure relevance to modern cybersecurity threats, especially given the role of AI-driven attacks.

Industry reports (such as Verizon DBIR) were selected selectively due to their strong statistical reliability and relevance to human factors.

Studies focusing exclusively on technical vulnerabilities were removed unless they were connected directly to human error or user interaction. This structured approach ensures that the literature gathered accurately reflects the most important dimensions of human-based cybersecurity.

Data Analysis Plan

Analysis followed a thematic approach:

1. Familiarization by repetition.
2. Coded major concepts in data.
3. Development of themes through coding patterns into broad themes.
4. Themes reviewing and refining.
5. The definition and identification of final themes

Trustworthiness

Trustworthiness ensured through:

- Systematic documented procedures
- Triangulation across sources and contexts
- Peer debriefing for bias minimization
- Thick description with detailed references

Ethical Considerations

The literature-based analysis focused on academic integrity as the primary ethics, assigning it appropriately, preventing plagiarism, and making appropriate interpretations of the source and its limitations.

Summary

The qualitative narrative review research is a research method that enables a critical review synthesis of employee cybersecurity leveraging based on thematic analysis and systematic literature collection.

This methodology provides the structure needed to evaluate human-based cybersecurity issues comprehensively. By combining perspectives from psychology, management, and cybersecurity, the narrative review supports the development of a holistic model that highlights employees' roles as both vulnerabilities and powerful security assets. This methodology lays the foundation for the data analysis in Chapter 4, where the themes identified here are explored more deeply.

Chapter 4: Data Analysis

Overview

The literature analysis presented in this chapter is organized based on the significant themes of employee cybersecurity and determines the nature of the issues (human vulnerabilities) and the solutions to them (strategies and countermeasures) by identifying common concepts and comparing them synthetically. This analysis does more than just summarize prior studies; it explains how the different themes interact and how employee behavior, corporate culture, and technical controls all work together to affect cybersecurity outcomes. This chapter synthesizes repeating trends to provide a more comprehensive understanding of the predominance of human factors in breach statistics and how businesses can effectively mitigate these risks.

The analysis builds on the original paradigm by showing how psychological, environmental, and cultural factors affect what end users do. This shows that cybersecurity problems that include people can't be understood just from a technical point of view. Instead, the analysis clarifies that the interactions between people, processes, and security technologies create the conditions for either risk or resilience. This overview serves as the foundation for exploring the interconnected themes that emerged from the literature review.

Data Analysis

Analysis revealed interconnected themes that consistently appeared across the reviewed studies. These themes demonstrate how human error, organizational expectations, cultural dynamics, and technology work together in both positive and negative ways. The literature does not present these issues as isolated problems; rather, they form a system in which employee behavior is shaped by training quality, leadership involvement, work environment, and the

availability of tools that support secure decision-making. The following sections expand on each theme using your original content, adding more depth and interpretation

Human Vulnerability Nature

- **Unintentional Threats:** Phishing and the use of passwords are the most common types of incidents due to the lack of awareness or stress, as research (Raza et al., 2025; Yusuf, 2024) still presents it as the most common. These mistakes happen a lot when workers rush, trust emails that look familiar, or try to get things done under pressure. People don't usually mean to break rules; instead, they rely on their gut feelings or habits, which attackers take advantage of. Fatigue, distractions, and too much information can also make mistakes more likely. This shows that human weaknesses are affected by the environment at work as much as by gaps in knowledge.
- **Malicious Insider Threats**: The least Alsowail and Al-Shehari (2022) described data theft and sabotage as the least common but most harmful types of attacks, and they are especially hard to find when someone has legitimate access. Insiders often know how systems work, where they are weak, and what data is most valuable, which gives them a distinct edge. It's hard for companies to figure out what people want early on, whether it's anger, money problems, or personal benefit. This data supports the idea that unintended mistakes happen often, while intentional actions have far bigger effects.

The most significant development is that social engineering has gone from simple phishing to AI-generated deepfakes (Noordeen & Bantan, 2025), which require greater human situational awareness to interpret. This means that susceptibility now goes beyond simple email assaults and into more complex forms of psychological manipulation. Employees need to learn how to spot not only strange communications, but also strange voices, videos, and people. This shift

demonstrates how attackers adapt faster than organizations, making continuous human vigilance more essential than ever.

Organizational Security Culture Centrality

A good security culture keeps on being a human risk mitigation foundation that is formed through major factors:

- **Leadership Commitment:** The active involvement of management in the research synthesis (Khando et al., 2021) has shown that the perception of employee security is elevated to high levels, which is a powerful force of behavioral change. When leaders consistently model secure behavior, communicate expectations clearly, and prioritize cybersecurity in daily operations, employees internalize these values. Leadership influences not only compliance but also motivation, trust, and willingness to report mistakes.
- **Peer influence:** Colleague behavior is considered to have a strong influence, and a study by Grassegger and Nedbal (2021) found that subjective norms are a strong predictor of social engineering resistance intention. Employees frequently follow the behaviors they observe around them. If coworkers ignore security rules, others will likely do the same. Conversely, if teams encourage secure habits—reporting suspicious emails, using strong passwords, locking devices—positive norms spread throughout the organization. This analysis shows that security culture cannot be enforced through policies alone; it must be lived by the people within the organization.

Awareness Training Evolution

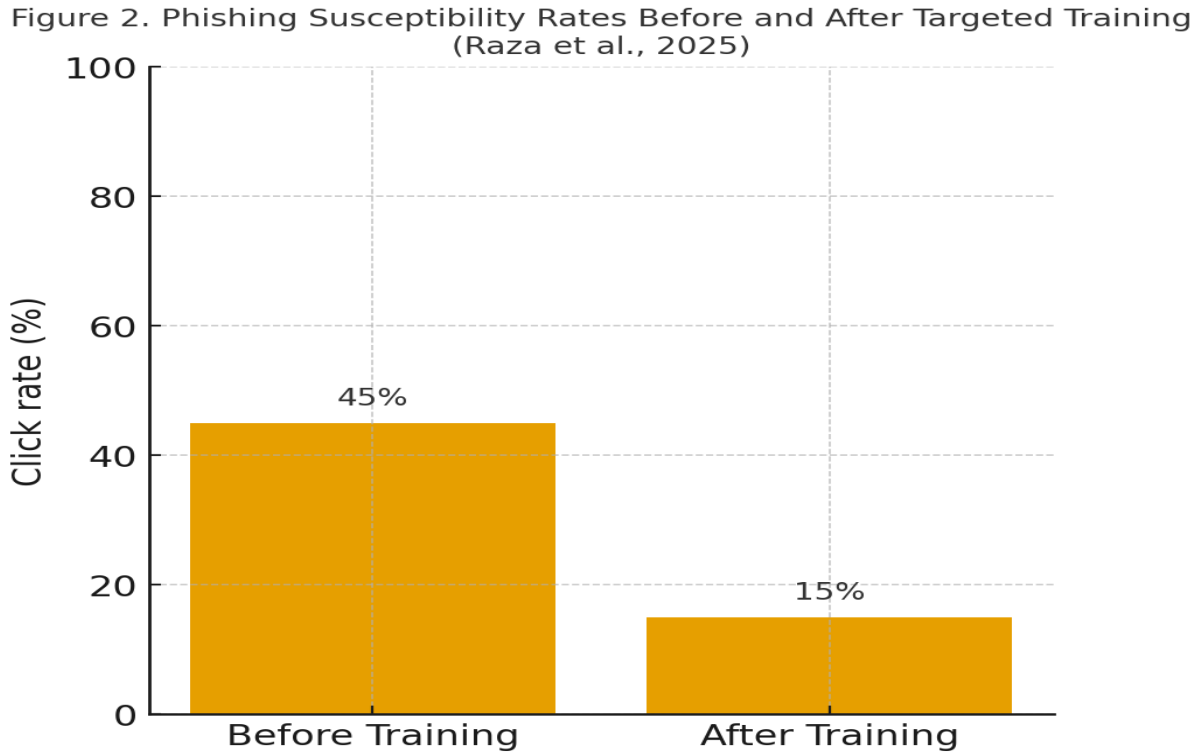

Figure 2. Effects of targeted training programs on phishing vulnerability. The findings of a study in the banking industry reveal that the rate of employee clicks decreased significantly after a concentrated awareness intervention. *Source: Raza et al. (2025).*

Evaluation indicates a distinct transition of generic annual training to dynamic approaches:

- **Continuous Learning:** One-off training is not effective, and ongoing reinforcement is better, either as a system like gamification (greater engagement) or as a constructivist (ownership) approach. Continuous training ensures that cybersecurity remains an active concern rather than a once-a-year requirement employees forget. Repetition, scenario-based exercises, and frequent refreshers help workers recognize patterns and respond more confidently to threats.

- **Tailoring:** The one-size-fits-all concept is unsatisfactory, and it was established that role-, department-, and personality-specific messages (Kajzer et al., 2014, as cited in Khando et al., 2021) are more efficient. This analysis shows that employees in finance require different examples and threats than those in IT or HR. Tailored content increases relevance, attention, and retention, making training more effective.

Technological Support Role

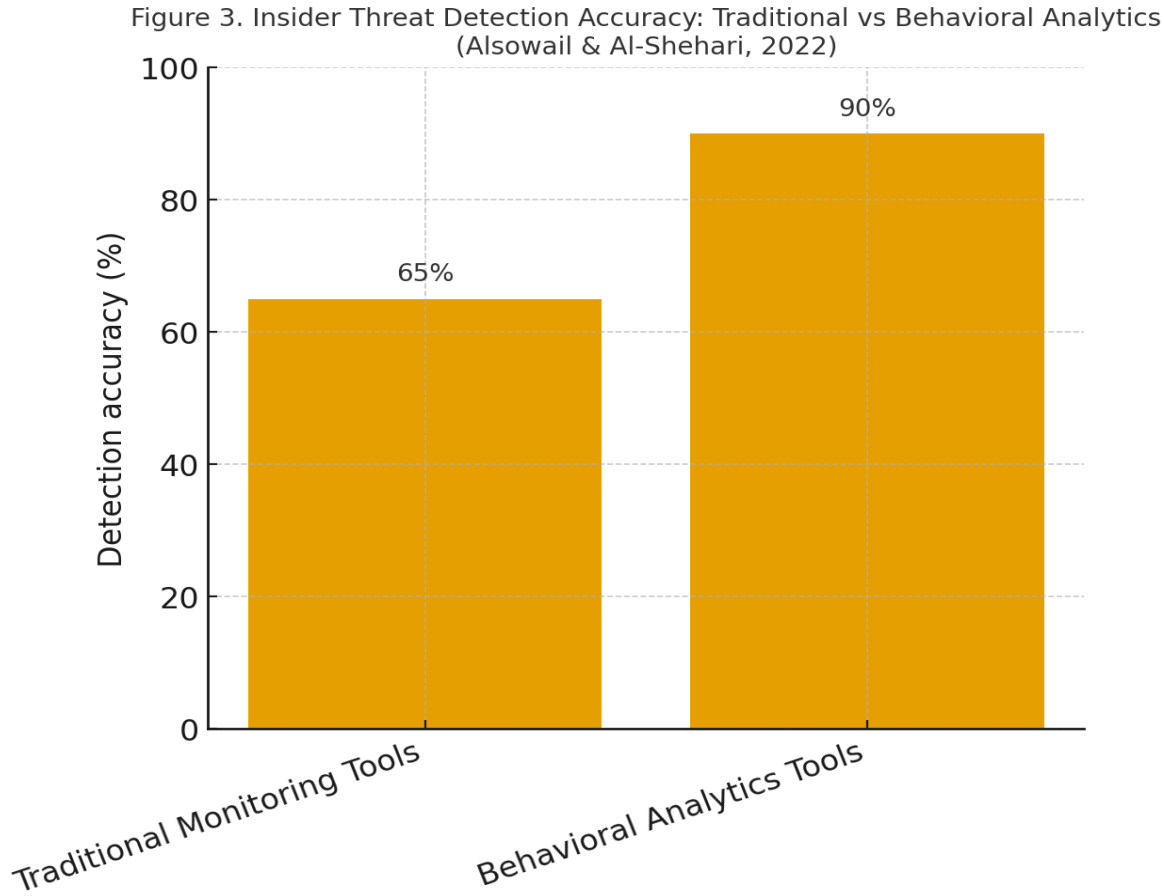

Figure 3. A comparison of detection accuracy in traditional monitoring and behavioral analytics in identifying insider threats. The detection rate is much greater with behavioral analytics tools. *Source: Alsowail & Al-Shehari (2022).*

Technology serves as a human-centric strategy force multiplier:

- **Behavioral Analytics:** Alsowail and Al-Shehari (2022) compare conventional monitoring with behavioral analytics and conclude that the latter can be more effective in detecting the presence of unobtrusive anomalous behavior, which ensures a safety buffer against human errors. Behavioral analytics can find little changes, such logging in at odd times, downloading a lot of data without permission, or accessing a system without permission. This lets you act quickly before damage happens. This emphasizes the idea that technology doesn't replace human alertness; it works with it.
- **Zero Trust**: ZTA reduces single-account risk in a systematic way by limiting access to the least privileged and constantly checking identities to reduce the damage caused by compromised credentials. Zero Trust makes the system safer, which means that employees don't have to rely on their own judgment as much. Even if an attacker gets hold of credentials, limited access makes it harder for them to do damage. This fits with the general idea that security has to combine human awareness with smart building design.

Summary

Data analysis brings together a coherent future direction: mitigation of human threats depends on a synergistic strategy based on a well-established, strong leadership-driven security culture foundation, providing consistent, engaging, tailored awareness training, supported and reinforced by behavioral analytics and Zero Trust principles. The analysis demonstrates that human behavior, organizational structure, and technology are inseparable components of cybersecurity. Strengthening one element without the others leads to gaps, but integrating all three creates a resilient system capable of adapting to evolving threats.

Chapter 5: Discussion, Recommendations, and Conclusion

Results Summary

Cybersecurity within modern organizations continues to evolve as threats become more sophisticated and as human behavior remains a central point of vulnerability. As the literature consistently shows, technological defenses alone are not sufficient to prevent attacks, especially those targeting human judgment, trust, curiosity, or routine behavior. This makes employees and end-users pivotal in both causing security breaches and preventing them. The research emphasizes that employees, regardless of role or technical expertise, encounter daily situations where they must interpret messages, identify suspicious behavior, follow guidelines, and make decisions that carry security consequences. Therefore, a secure organization depends on empowering individuals and creating structures that support secure decision-making.

This research aimed to explore the contribution of employees and end-users in cybersecurity within organizations. The literature analysis proves that the human factor is the most vulnerable and the most promising defensive tool at the same time. The most prominent risks are outlined in the results: accidental mistakes caused by awareness deficit and insider attacks. Effective mitigation was discovered to necessitate a holistic approach that integrates cultural, educational, and technological strands. The major findings are the paramount role of leadership in the development of security culture, the highest effectiveness of the continuous and interactive training techniques, such as gamification, in comparison to the periodic lectures, and the supportive roles of behavioral analytics and Zero Trust Architecture in developing a strong security posture.

it is clear that human behavior cannot be separated from organizational structure. Employees typically do not intentionally create risk; instead, risky actions occur when workers feel pressured, confused, unsupported, or uninformed. The results reinforce the need for organizations to focus on simplifying security requirements, making training meaningful, and creating an environment where employees feel responsible and capable. Furthermore, insider threats require special attention because they are often driven by emotional, financial, or situational factors that organizations must plan for. This makes continuous monitoring, strong access controls, and behavioral analytics valuable tools for identifying unusual activity. Overall, the results demonstrate that human factors remain the most complex but also the most influential element of cybersecurity.

Interpretation of Findings

Interpreting the results of this study requires examining the relationship between human behavior, organizational expectations, and the technology used to support secure actions. Many cybersecurity failures arise not from malicious intentions but from predictable human tendencies—such as rushing through tasks, trusting familiar patterns, overlooking details, or misjudging digital risks. These tendencies highlight the importance of designing systems and training methods that fit how people naturally behave. The findings also reinforce that organizations must address both psychological factors (such as motivation and confidence) and structural factors (such as leadership and culture) to improve overall security.

Some existing theories can be applied to the findings. The focus on leadership and culture is congruent with the socio-technical systems theory, according to which the best results are

attained when the social and technical systems are built to coexist (Checkland and Scholes, 1999, as cited in Colabianchi et al., 2025). Without an organizational culture (social) that supports a security policy (technical), the latter will fail.

The Theory of Planned Behavior can be used to describe why a customized training and messaging approach can be effective (Grassegger & Nedbal, 2021). Organizations can positively influence the intention to perform secure behavior by influencing the attitude of an employee towards security (with consumption of engaging material), perceived behavioral control, and the subjective norms (through leadership and modeling by peers).

Moreover, the multi-layered approach is suggested, which is the concept of defense-in-depth. Technology alone, or training alone, is insufficient. To create a number of overlapping defensive layers against human-based threats, a modern organization should possess a culture of awareness, work training, and supporting technologies like behavioral analytics and Zero Trust principles.

These theories illustrate that safe behavior doesn't just happen; it has to be developed. People do what they observe other people doing. Employees will naturally follow the lead of their executives when it comes to cybersecurity. Employees lose motivation when their leaders aren't consistent. Theory also explains why interactive and gamified training works: it alters people's minds, boosts their confidence, and makes it simpler for them to behave safely. Defense-in-depth is very necessary for dangers that come from people because no one thing can stop all blunders. Awareness, culture, analytics, and Zero Trust all work together to build a strong atmosphere where one person's mistake doesn't cause a disaster.

Limitations of the Study

Research focusing solely on secondary literature must acknowledge the limitations of relying on previously published studies. Although literature-based research allows for broad analysis, it prevents direct examination of employee behavior and organizational culture. This makes the findings descriptive rather than measurable. Cybersecurity behaviors are situational, shaped by stress levels, workload, clarity of rules, and the individual's training experience. Without direct observation or surveys, details such as emotional influences, workplace pressure, or team culture cannot be fully captured.

This study has some major limitations. Firstly, the fact that the present research is fully premised on the overview of other published works implies that its conclusions can be as solid as the articles it is built. The same weaknesses are passed on to this work in case the notable studies have not been considered, or the quality of the research in the field is not outstanding. No original, experimental, or survey data were collected in this research. Second, the cybersecurity environment changes at a very high pace. There are new threats, and new threats emerge at a faster pace in the future, particularly the threats that are driven by artificial intelligence (AI).

In addition, literature cannot fully capture differences in organizational structure, culture, or employee behavior. What works well in one industry may not work in another. Cultural differences across countries, levels of digital literacy, and types of work environments also influence how well security practices are adopted. These variations limit how generalizable the findings are. Nonetheless, literature provides strong insight into the core issues affecting human-based cybersecurity threats.

Recommendations

Organizations seeking to strengthen their cybersecurity posture can benefit from structured and continuous investment in employees. Human-based threats are not solved by technology alone; they require a people-centered approach that integrates training, culture, communication, and supportive tools. Recommendations must focus on building both individual competence and organizational resilience. Employees must feel supported, informed, and capable of recognizing and stopping threats, while organizations must create an atmosphere where secure behavior is rewarded and mistakes are used as learning opportunities.

Implement a program for lifelong learning, which includes Phishing Simulations, Gamification, and Role-Based Training. In larger organizations, use user and entity behavior analytics (UEBA) tools to create a baseline of regular usage and proactively identify anomalies that might indicate an internal threat or compromised account. Open channels that allow employees to discuss any threats or security issues without fear of repercussions. Create a culture where mistakes, like clicking a phishing link, are reported and quickly fixed. Measures to assess the success of security awareness initiatives. Keep an eye on metrics like the number of reported security events, the rate of phishing simulation failure, and the rate of password policy adherence. Using this knowledge, the application is continuously improved.

These recommendations work together to create an integrated strategy. Employees stay up to date on threats as they change through lifelong learning. UEBA technologies help people make decisions by spotting strange behavior early on. Open lines of communication make it easier to report problems, which lowers harm and makes things clearer. Evaluation metrics assist

businesses to figure out if training is working or if they need to do more to help. All these things work together to create a mature and flexible security culture.

Conclusion

In the end, without the human foundation, the road to strong cybersecurity cannot be completed. Employees must be the foundation of a modern-day defense strategy; they cannot be regarded as an exception. This research has demonstrated that organizations can transform their workforce, which may seem like a liability, into their greatest asset by fostering a positive security culture, offering constant and engaging training, and using technology wisely to support human vigilance The battle against cyber threats is still a human one. The best approach to develop a strong defense is to provide employees the information, tools, and support they need to do their jobs well.

In the end, businesses need to put people first, not just systems. Cybersecurity starts with being aware of the problem, gets stronger via culture, and stays strong through continual education. As dangers change, businesses need to change too by supporting their workers, making communication better, and keeping a multi-layered approach. Cybersecurity resilience doesn't come from getting rid of all mistakes. Instead, it comes from creating a place where everyone is responsible for preventing, finding, and responding to threats.

References

Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and Countermeasures for Preventing Insider Threats. *PeerJ Computer Science, 8*, e938. https://doi.org/10.7717/peerj-cs.938

Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming Threats into Opportunities: The Role of Human Factors in Enhancing Cybersecurity. *Journal of Innovation & Knowledge, 10*(1), 100695. https://doi.org/10.1016/j.jik.2025.100695

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science, 181*, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Harper, J. W. (2023). Cybersecurity: A review of human-based behavior and best practices to mitigate risk. *Issues in Information Systems, 24*(4), 247-254. https://doi.org/10.48009/4_iis_2023_119

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 102*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Noordeen, A. R., & Bantan, M. (2025). How human behavior can mitigate AI-generated cybersecurity threats. In *Proceedings of the 2025 Computers and People Research Conference* (SIGMIS-CPR '25) (Article No. 17, pp. 1–3). Association for Computing Machinery. https://doi.org/10.1145/3716489.3728447

Raza, M. A., Hossain, M. A., Mahjabeen, F., Rahman, J. Y., & Rahman, T. Y. (2025). Evaluating the human factor in bank cybersecurity: Strategies for improving employee awareness and reducing insider threats. *Indonesian Journal of Advanced Research, 4*(1), 1–20. https://doi.org/10.55927/ijar.v4i1.13399

Yusuf, A. (2024). Examining the role of organizational culture in shaping security practices: A case study of tertiary institutions. *Journal of Advanced Research and Multidisciplinary Studies, 4*(4), 191–202. https://doi.org/10.52589/jarms-nvz29vay

Document A: Proposed Survey Instrument for Measuring Employee Security Awareness

Section 1: Demographic Information

1. What is your department?
2. How long have you worked at this organization?
3. What is your primary job function?

Section 2: Security Knowledge Assessment

4. How would you define "phishing"?
5. What makes a password strong? (Select all that apply)
    - At least 12 characters long
    - Contains uppercase and lowercase letters
    - Includes numbers and symbols
    - Not used for other accounts
    - All of the above
6. What should you do if you receive a suspicious email from what appears to be your manager asking for urgent financial information?
    - Respond immediately with the information
    - Forward it to the IT security team
    - Call your manager to verify the request
    - Delete the email

Section 3: Security Practices and Behaviors

Please rate how often you do the following: (Always, Often, Sometimes, Rarely, Never)

7. I change my passwords regularly
8. I lock my computer when leaving my desk

9. I report suspicious emails to the IT department
10. I use the same password for multiple accounts
11. I connect to public Wi-Fi for work purposes

Section 4: Security Policy Awareness

12. Are you aware of our organization's information security policy?

- Yes, and I have read it
- Yes, but I have not read it completely
- No, I am not aware of it

13. How often do you receive security awareness training?

- Monthly
- Quarterly
- Yearly
- Never

14. Do you know who to contact if you suspect a security breach?

- Yes
- No
- Not sure

Section 5: Security Culture Perception

Please rate your agreement with the following statements: (Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree)

15. Management takes security seriously
16. I feel comfortable reporting security mistakes without fear of punishment
17. Security training is helpful and relevant to my job

18. I understand my role in protecting company information

19. Security measures make it harder to do my job effectively

Section 6: Open-Ended Questions

20. What would help you be more security conscious at work?

21. What security topics would you like more training on?

22. Any additional comments about security in our organization?

Document B: Semi-Structured Interview Protocol for Cybersecurity Managers

Introduction

"Thank you for participating in this interview about our organization's security awareness program. The purpose is to understand current challenges and identify opportunities for improvement. This discussion should take about 45 minutes. Your responses will remain confidential."

Background Questions

1. How long have you been involved with cybersecurity at this organization?
2. What is your current role and responsibilities related to security awareness?

Current Security Awareness Program

3. What is the existing security awareness training program?
4. Does the company provide security training to the employees?
5. How do security training sessions take place? (online classes, face-to-face sessions, emails, etc.)

Program Effectiveness

6. What are the ways of quantifying the effectiveness of security awareness training?
7. What do you consider to be the metrics or indicators of employee security awareness?
8. What do you consider to be the greatest achievements of the present program?
9. What are your key security awareness problems?

Employee Behavior and Culture

10. What would you say is the overall security culture in our organization?
11. What do you consider as the typical security errors by employees?
12. What are the general reactions of employees to security requirements and policies?

13. What do you believe are the most affecting factors on employee security behavior?

Management Support and Resources

14. To what extent does senior management support security awareness programs?
15. How much money and resources do you spend on security awareness?
16. Are there any obstacles to developing effective security awareness programs?

Improvement Opportunities

17. What are some of the things you would like to change in the security awareness program?
18. What are some other tools or resources that can be used to increase security awareness?
19. What would we do to better involve employees in security practices?

Future Directions

20. What are your worries about employee behavior in terms of rising security threats?
21. What do you think should be your security awareness priorities in the coming year?
22. Is there anything more that you want to say about security awareness in our organization?

Closing

"Thank you for your time and valuable insights. This information will be very helpful for improving our security awareness efforts."

Document C: Template for a Phishing Simulation Campaign

Campaign Planning Phase

1. Campaign Objectives

- Increase employee recognition of phishing attempts
- Reduce click-through rates on suspicious emails
- Identify departments needing additional training
- Measure improvement over time

2. Target Audience

- All employees
- Specific high-risk departments (e.g., Finance, HR, Executive)
- New hires within first 90 days

3. Timeline

- Planning: 2 weeks
- Execution: 1 week
- Follow-up and training: 2 weeks
- Assessment: 1 week

Phishing Email Templates

Template 1: Urgent Password Update

Subject: Immediate Action Required: Password Expiry Notice

Dear Employee,

Our system records indicate that your password will expire within 24 hours. Failure to update your password will result in account suspension.

Click here to update your password immediately: [Fake Link]

IT Support Team

Template 2: Fake Invoice Attachment

Subject: Overdue Invoice - Action Required

Hello,

Please find the attached invoice that requires your urgent attention. This invoice is 30 days overdue.

If you have any questions, please reply to this email.

Accounts Payable Department

[Fake Malicious Attachment]

Template 3: Fake Social Media Notification

Subject: You have been tagged in a post

Hi [Employee Name],

You have been tagged in a new post. Click the link below to view:

[Fake Link]

The Social Media Team

Implementation Steps

Step 1: Pre-Test Preparation

- Obtain management approval
- Inform HR and legal departments
- Prepare educational materials for follow-up
- Set up tracking system for results

Step 2: Launch Simulation

- Send first phishing email to target groups

- Track opens, clicks, and responses
- Monitor for any technical issues
- Be prepared to send stop message if needed

Step 3: Immediate Follow-up

- Send automatic educational message to those who clicked
- Provide immediate feedback on what they missed
- Offer quick security tips
- Document all responses and actions

Step 4: Training and Education

- Identify departments with high failure rates
- Schedule additional training sessions
- Share campaign results with management
- Provide individualized coaching for repeat offenders

Step 5: Assessment and Reporting

Metrics to Track:

- Percentage of employees who opened emails
- Percentage who clicked links or opened attachments
- Percentage who reported suspicious emails
- Departments with highest failure rates
- Improvement compared to previous campaigns

Report Template:

- Executive summary of results
- Detailed statistics and trends

- Recommendations for improvement
- Plan for next simulation campaign
- Success stories and positive findings

Safety Measures and Ethics

1. Do not use real malicious software or viruses
2. Do not collect actual login credentials
3. Provide clear identification as a test after completion
4. Ensure no punishment for employees who fail
5. Maintain confidentiality of individual results
6. Focus on education, not punishment

Follow-up Activities

1. Company-wide security reminder email
2. Department-specific training sessions
3. Recognition for employees who identified the phishing attempt
4. Monthly security tips based on campaign findings
5. Plan for next phishing simulation in 3-6 months