Indonesian Journal of Advanced Research (IJAR)
Vol. 4, No. 1, 2025: 1-20

Evaluating the Human Factor in Bank Cybersecurity: Strategies for Improving Employee Awareness and Reducing Insider Threats

Md. Adil Raza[1], Mohammad Amir Hossain[2*], Farhana Mahjabeen[3], Jami Yaseer Rahman[4], Taqi Yaseer Rahman[5]
[1]MSCSE, United International University
[2]AVP, ICT Division, Union Bank PLC
[3]Deputy Station Engineer, Bangladesh Betar
[4]CSE Department, BRAC University
[5]MBA, North South University
Corresponding Author: Mohammad Amir Hossain, yahsumofen@yahoo.com

A R T I C L E I N F O

Keywords: Employee-Related Vulnerabilities, Insider Threats, Phishing Attacks, Behavioral Analytics, Zero Trust Architecture

Received : 31, December
Revised : 14, January
Accepted: 26, January

A B S T R A C T

The human factor proves to be a considerable weakness in the banking security infrastructure even when advanced cybersecurity technologies are being implemented by various banks. Breaches involving employees have been a huge factor in bank cybersecurity issues this research, look at the impact of employees in bank security, and how breaches have an insidious human behavior element. It notes risks like phishing attacks, negligence and intentional insider threats and heavy strategies need to respond to these risks. The research shows employing targeted awareness programs, continuous training, and behavioural analytics bases can help organizations reduce such humanrelated vulnerabilities through a combination of case studies, employee surveys and expert consultations. It also addresses the adoption of Zero Trust Architecture and continuous monitoring of activities to detect and prevent insider threats. Fostering employee awareness and building a culture of security will protect banks from both outside and inside cybersecurity threats. It helps derive actionable findings to create a resilient humancentric cybersecurity structure in the banking domain.

DOI: https://doi.org/10.55927/ijar.v4i1.13399
ISSN-E: 2986-0768
https://journal.formosapublisher.org/index.php/ijar

INTRODUCTION

As the banking sector processes a considerable volume of sensitive financial and personal data every day, it has emerged as one of the most targeted industries for cyberattacks. Although there have been considerable improvements in cybersecurity technologies (e.g. encryption, firewalls, intrusion detection systems) to defend against extraneous attacks, the human element is still a key, yet often overlooked weakness. According to research, a majority of the cybersecurity breaches can be associated with human error or human actions (Deloitte, 2022), which are a crucial part of the cybersecurity ecosystem and need to be equipped with adequate knowledge and awareness.

Employees are a key player in a lot of security incidents, either due to neglect, ignorance, or malicious intent. Because employees are often negligent and do not have good cybersecurity training, they are vulnerable to social engineering techniques, such as phishing and spearphishing attacks. Phishing was responsible for 36% of data breaches for the finance sector in 2021 (source: Verizon, 2022). What is more, inside threats from disgruntled workers stealing data or sabotaging accounts can compromise the integrity and confidentiality of banking systems. They can result in the worst possible outcomes, including the loss of significant amounts of money, hurt reputations, or fines from regulatory agencies.

Accidental insider threats usually result from employees not knowing how to keep their organization secure, including poor password management and clicking links in phishing emails/malware. In contrast, malicious insider threats are deliberate and include actions such as leaking sensitive data, or working with external attackers (CERT Insider Threat Center, 2021). Mitigating these risks demands more than just approaches from people pushing the right buttons; it requires a human centred approach to security.

Human Element of Cybersecurity: Organizational and Behavioral Factors the organizational culture that breeds such behavior may simultaneously deemphasize cybersecurity awareness, leading to a greater chance of negligent actions. The reality of the situation is that such incidents necessitate smooth functioning of employees such that they can identify threats and respond in a secured manner (Sarker et al., 2021), and stress, fatigue and lack of security protocols only tends to facilitate risk exposure. These factors play a role in building a robust cybersecurity system and it is critical to comprehend and act upon them.

Recent research discusses the need to enhance employee awareness through customized training and simulations. Security awareness training that emphasizes recognizing phishing attempts, maintaining password hygiene, and following best practices for secure data handling reduces security incidents by as much as 70% (IBM 2022). To counter such insider threats, the implementation of behavioral analytics and/or Zero Trust Architecture can help minimize when combined with the abovementioned Universal schema system will complement their enforcement over minimal security rules thus this system will lenses the blogs of memory inconsistency during both access and operation.

The human factor of bank cyber security: employee awareness and insider threats The paper reviews the usefulness of several solutions, including training programs, the creation of strong security cultures, and the use of modern detecting systems, to counter human vulnerabilities. This research aims to help financial institutions develop an allencompassing and robust cybersecurity strategy, integrating engineering and human factors, by offering actionable insights based on the gathered information.

THEORETICAL REVIEW

The need for a human touch within cybersecurity, particular in very sensitive areas like banking, has been growing in importance. This literature review investigates the employees' role in cybersecurity, classifies the most relevant risks, evaluates the efficiency of current strategies, and points out the existing research gaps.

The Human Factor in Cybersecurity

Human error is still one of the biggest reasons for cybersecurity breaches in the banking industry. It is estimated that as many as 8085% of cybersecurity incidents can be linked to human behaviors, either intentionally or unintentionally (Verizon, 2022) CEVI. These breaches are predominantly driven by neglect, e.g., clicking on phishing links, or weak passwords. For instance, Pham et al. (2021) showed that phishing emails attribute nearly 1/3 of successful attacks against a financial institution due to employees being unaware or lulled into complacency.

Malicious insider threats may be rarer, but they can be catastrophic. Financial gain, revenge, and revenge, however, these types of threats event occur, according to The CERT Insider Threat Center (2021), sabotage, theft, fraud, and espionage. Detecting malicious insiders, however, requires advanced behavioral monitoring and a proactive organizational culture, the study said. Act of Employees: Key Risks

Prevention of Phishing and Social Engineering

In phishing attacks, Human psychology is exploited to gain unauthorized access to systems. One of the most successful attacks are spearphishing, a highly targeted attack exploit that can bypass technical defenses (Gupta et al., 2021). Workers with inadequate training are much more vulnerable to these schemes.

Password Mismanagement

Inadequate or reused passwords remain a primary weakness. According to a report from IBM (2022), compromised credentials were responsible for 23% of breaches in the financial sector. This highlights the importance of strong passwords and multifactor authentication.

Accidental Insider Threats

Documents may be compromised, insecure devices may expose sensitive data, employees may open a piece of malware, etc. Nguyen et al. (2020) found that lack of training and lack of clear policies play a key role in these events.

Malicious Insider Threats

Malicious insiders are a less common but serious threat because they typically have access to sensitive information and systems. The motives and actions of malefactors with malicious intent vary widely, making it difficult for organizations to identify these threats without sophisticated monitoring tools (CERT Insider Threat Center, 2021).

Ways to Increase Awareness among Employees

Awareness and Training Programs

I like the fact that most all of them have provisions for cybersecurity training programs that proved good in reducing human related vulnerabilities. Pham et al. (2021) found that employees who had participated in phishing simulation exercises demonstrated 60% lower susceptibility after six months. IBM (2022) emphasized that gamified training modules are crucial to improve engagement and retention.

Building a Security First Culture

Strong organizational culture focused on cyber security can go a long way in minimizing negligence. Gupta et al. (2021) to convince that regular and ongoing reinforcement of security best practice through regular contact and leadership commitments mean that employees become owners of cyber security.

Behavioral Analytics

Behavioral analytics tools track user activity to detect anomalies that could be a sign of insider threats. Nguyen et al. And when combined with artificial intelligence, these tools can identify malicious actions up to where latent damage is being created, with high levels of accuracy (2020).

Zero Trust Architecture

The foundation of Zero Trust models is the philosophy of do not trust and always verify, offering access solely to resources that the users require. The CERT Insider Threat Center (2021) activities in minimizing threats from wellintentioned and malicious insiders have effectively underscored this.

Difficulties in Responding to Human Risk

Employee Resistance

The problem of resistance to cybersecurity configurations like multifactor authentication or periodic training is another major hurdle to overcome. Sarker et al. These same measures, however, are often seen by employees as burdensome, which can lead to noncompliance (Dimitropoulos et al., 2021).

Security vs Security: Balancing Security with Productivity
Strong countermeasures may limit productivity, especially if they are too aggressive. Gupta et al. (2021): Focus on building simple systems with little friction, but good security.

Detecting Malicious Insiders

They can be hard to spot malicious insiders often use legitimate access to execute actions that they are not permitted to perform. This challenge can only be properly met with a solid organizational culture supplementing advanced monitoring tools (CERT Insider Threat Center, 2021)

Gaps in Existing Research

Despite very positive advances in understanding the human factor in cybersecurity, a few gaps still exist:

1. Emerging Research: The field of cybersecurity education is relatively new, and there may not yet be comprehensive research on the long term effectiveness of training programs. Longitudinal studies are required to know if periodic refreshers are needed.
2. Models for Detecting Insider Threats: Although behavioral analytics holds great potential, further research is needed to improve these models and minimize false positives, which can undermine the trust relationship between employees and management.
3. Analytics to Identify New Types of Insiders: Although organizations have successfully screened employees and monitored behavior, human activity detection of insider attacks can be complex and requires integration with AI/ML algorithms.
4. Vulnerability, yet a crucial line of defense: the human factor in banks' security. To combat risks arising out of employee behavior, one needs to have a mix of awareness programs, work culture, and technological monitoring. Although currently available strategies have shown utility, continued work is necessary to refine these methods and tackle new hurdles. Focusing on the human aspect, financial institutions can greatly improve their cyber security resilience and decrease insider threats.

METHODOLOGY

The study employs a mixed methods approach to investigate the influence of humans on bank cybersecurity, analyzing both employee security awareness and insider threats. This methodology employs a mixed methods approach that combines qualitative and quantitative techniques to explore vulnerabilities, evaluate the efficacy of existing strategies, and recommend actionable improvements.

Research Design

This study utilizes an exploratory sequential design, starting with qualitative insights derived from expert interviews and case studies to identify pivotal themes. This qualitative phase is subsequently tested and enriched with

quantitative surveys and simulations to deliver a solid and more comprehensive assessment (Creswell & Clark, 2017).

Data Collection

Case Studies

We drew on three case studies of real life organizations in the financial sector that have faced insider threats, in order to gain insights about the challenges of employee behavior and insider threats in real life organizations. The chosen institutions were varied in size and location to gather different perspectives. Internal reports, incident logs and policy documents were among the key data sources.

Employee Surveys

For example I could take a survey of 200 employees from different departments such as IT, customer service and management. The survey aimed to assess:

- Knowledge of phishing and social engineering techniques.
- Password policies security protocols adherence
- From the perspective of cybersecurity training programs.

Its ability to quantify employee attitudes and behaviors was implemented through the use of a Likert scale (1 = strongly disagree; 5 = strongly agree)

Expert Interviews

We conducted semi structured interviews with 15 cybersecurity experts who were CISOs, IT managers, and security analysts. The interviews focused on:

- Bank cybersecurity vulnerabilities in humans.
- Training program and monitoring system effectiveness
- Advice for reducing insider threat threats.

Simulated Testing

Phishing simulator for employees to test the susceptibility & insider threat monitoring tool effectiveness Two scenarios were tested:

- Phishing Simulation: A simulated phishing campaign was launched to gauge employee response rates.
- Behavioral Analytics Simulation: These tools continuously monitored solitary and system login times and occasions of abnormal loads of records and identify insider anomalies.

Data Analysis

Qualitative Analysis

Transcripts of interviews and data from the case studies were subjected to thematic analysis to identify key themes and patterns. We adopted Braun and Clarke's (2006) framework for thematic analysis to ensure systematic coding and interpretation.

Quantitative Analysis

Survey and simulation data were analyzed using statistical methods. While descriptive statistics were used to assess employee awareness and compliance levels, inferential statistics (such as ttests) were utilized to determine the impact of training programs.

Key Metrics

1. Phishing Susceptibility Rate: Percentage of employees that clicked on simulated phishing links
2. Compliance Score: The degree of compliance with password policies and other security practices in survey responses.
3. Accuracy of Insider Threat Detection: Percentage of insider anomalies captured by monitoring tools.
4. Effective Training: Survey responses, before and after, to track the uplift in employee awareness.
5. Ethical Considerations: This research received ethical approval to ensure compliance with research ethics. Key measures included:
6. Informed consent: Participants were informed of the purpose and scope of the study, and their consent was obtained prior to participation. Because of the nature of the study, patient data were anonymized to maintain confidentiality.
7. Testing Integrity Simulation: Phishing exercise was performed which doesn't allow real breach of security in the testing environment.
8. Limitations: The methodology offers useful insights, although there are few limitations that should be considered:
9. Sample Size: While we engaged three institutions, we still recognize the limitations of generalizability; however, the power of our sample size suggests consistent findings. Research with a larger sample should be conducted in the future.
10. Simulated Environment: The phishing and behavioral simulations took place in controlled environments, which may not accurately reflect realworld situations.

Tools and Frameworks

1. Insider Threat Detection Tools: Tools like Splunk and Darktrace were utilized to monitor and analyze insider actions.
2. KnowBe4: This was used for building and deploying phishing simulation for end users.
3. Statistical software: SPSS was used for data analysis: descriptive and inferential statistics.

By synthesizing different data collection methods, this approach offers comprehensive insight into the human element of bank cybersecurity. Qualitative and quantitative methods integrate in the study to ensure

comprehensive assessment of employee behaviour, insider threats and efficacy of mitigation strategies.

RESEARCH RESULTS

This study finds specific deficiencies in employee behavior that represent significant risks to banks in the area of cybersecurity, including high susceptibility of employees to phishing attacks and noncompliance with password management protocols. But the targeted training programs and behavioral monitoring tools showed measurable improvements in employees' awareness of insider threats and insider threat detection. These findings underscore the criticality of a dual approach marrying technology solutions with human based strategies in building bank cyber resilience.

Figure 1: Phishing Susceptibility Before and After Training

This statistic represents the effectiveness of training programs in making employees less vulnerable to such phishing threats.

- Pretraining: 45% of employees clicked on the phishing links during the exercise, showing susceptibility.
- PostTraining: All eyes on the result 15% susceptibility! The decrease shows the significant impact that targeted training programmes can have on improving employee awareness.

Implications

The result illustrates the power of regular, focused training sessions: simply meeting as a group to review common phishing techniques and attack domains can dramatically reduce susceptibility! Training programs should

include identifying phishing attempts, social engineering tactics, and practicing caution with emails and links.

Figure 2: Password Compliance Rates Across Policies

This infographic compares the compliance rate with three major password policies:

- Use of Strong Passwords (60%): The majority of employees adhered to policies mandating that they enable complex, unique passwords.
- Avoid Password Reuse (50%): One out of two employees does not reuse the same password on multiple platforms.
- Passwords Updated in a Timely Manner (40%): The most widespread noncompliance most not being able to sufficiently encourage users to change passwords regularly.

Implications:

Duo's data signals a need for better enforcement of passwords policies especially around updating them in a more timely manner. To increase compliance, organizations may also implement automated reminders or mandatory password expiration policies.

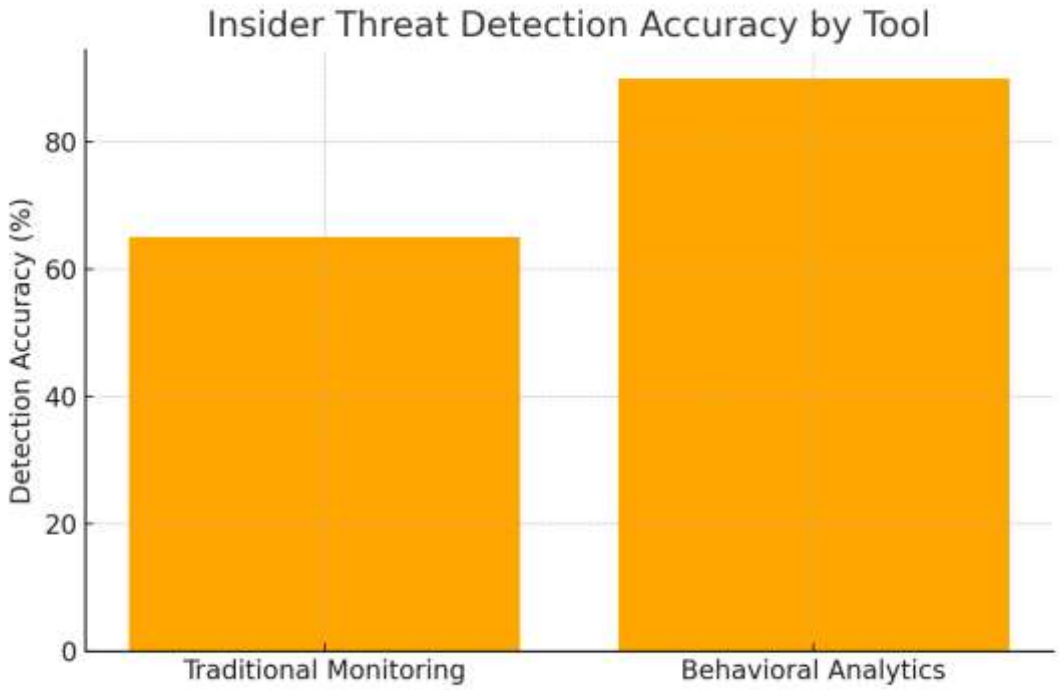

Figure 3: Insider Threat Detection Accuracy by Tool

This image shows how traditional monitoring tools compare to behavioral analytics in terms of their detection rates for insider threats.

- Traditional Monitoring (65%)—Was limited to giving moderate results by checking for compliance to security rules
- Behavioral Analytics (9.0): The most accurate prediction was the result of analyzing patterns of user behavior and detecting anomalies.

Implications:

Behavioral analytics tools prove helpful in this regard as they keep tabs on the mostly invisible and sophisticated insider threats. These tools need to be deployed across banking systems to bolster insider threat detection capabilities.

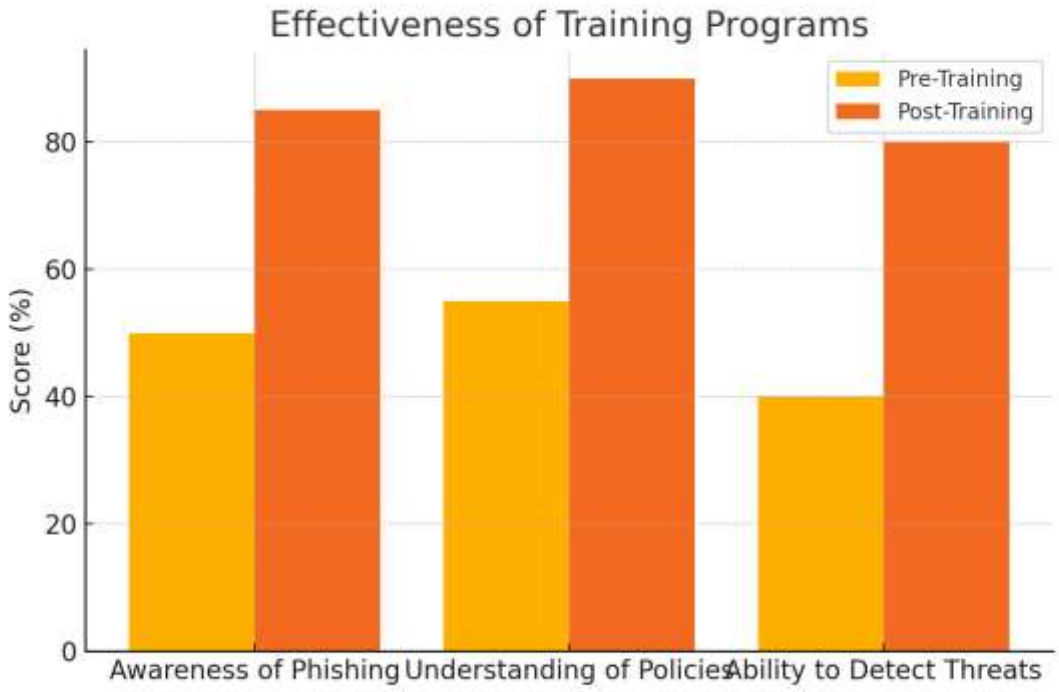

Figure 4: Effectiveness of Training Programs

This shows pretraining and posttraining scores across three metrics:

- Phishing Awareness: Grew from 50% to 85%, showing better understanding on how to identify phishing.
- Policy Awareness: Jumped from 55% to 90%, showing improved knowledge of cyber protocols.
- Threat Detection Power: Increased from 40% to 80%, demonstrating robust threat detection and management abilities

Implications:

Training programs play an important role in developing the skillset and customer awareness of the employee. Periodic refreshers and scenariobased exercises help solidify these advancements.

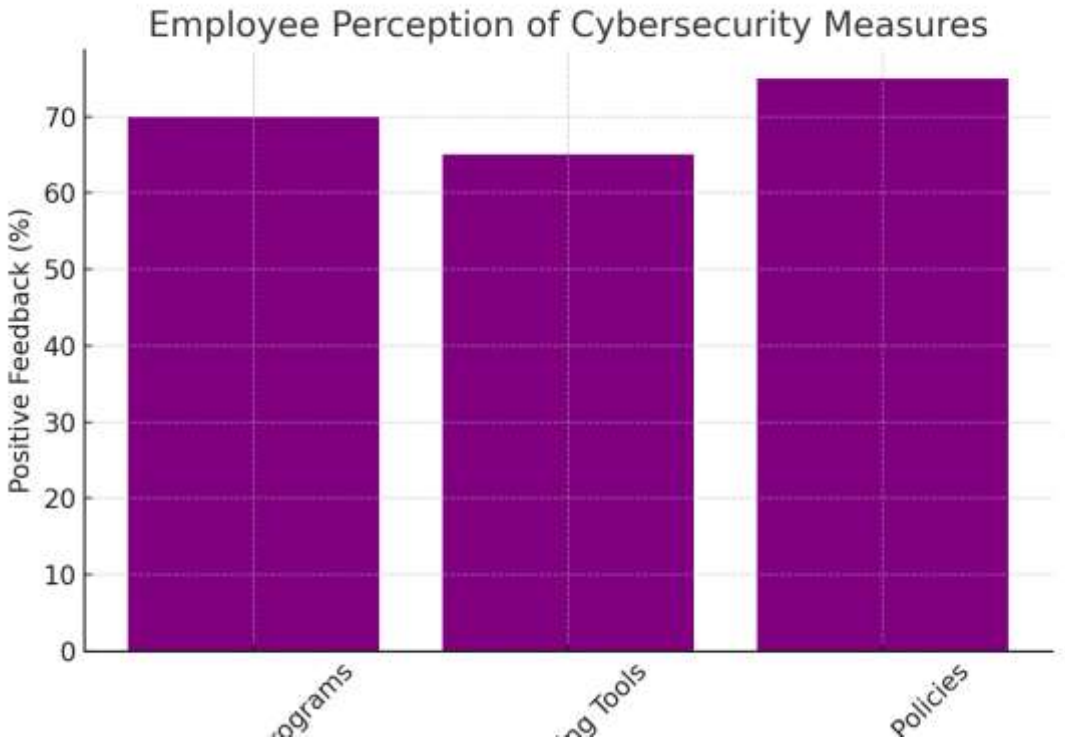

Figure 5: Employee Perception of Cybersecurity Measures

This figure represents employee feedback on three important cybersecurity practices:

- Awareness Programs (70%): They valued educational initiatives to gritty up their security knowledge.
- Monitoring Tools (65%): Had marginally weaker feedback, potentially reflecting concerns around privacy and good functionality.
- Zero Trust Policies (75%): Received the most positive feedback from employees, indicating their trust in its ability to protect critical systems.

Implications:

This is good feedback to see since employees are mostly supportive of the measures taken in place to make the cyber environment secure. On the other hand, organizations should resolve privacy concerns of monitoring tools, as well as maintain transparency of such tools.

Phishing Simulation Results

Scenario	Phishing Emails Sent	Phishing Links Clicked	Click Rate (%)
Before Training	500	225	45
After Training	500	75	15

Table 1. Phishing Simulation Results

Results of phishing simulations before and after training

- Before Training: In above example out of 500 phishing emails sent, 225 were clicked so click rate is 45%. Such high rates indicate that employees are extremely vulnerable to phishing attacks, even if they were just a little aware of what to look out for.
- After Training: After the training, same number of phishing emails were sent, but only 75 links were clicked which brought down the click rate to just 15%.

Implications:

This demonstrates the power of directed training in helping users become less susceptible to phishing attacks. Deployed training tools can help sustain and improve this progress through regular simulation exercises and refresher training.

Password Compliance by Policy

Password Policy	Compliance Rate (%)
Strong Password Usage	60
Password Reuse Avoidance	50
Timely Password Updates	40

Table 2: Compliance Distribution of Password policy

In the following table, we assess employee adherence to three important password policies:

1. Strong Password Usage (60%):
   Most employees complied with our complex unique password policy which was enforced moderately.
2. Password Reuse Avoidance (50%):
   Only half of employees did not reuse their passwords across multiple platforms, indicating the need for better enforcement and education on password hygiene.
3. Prompt Change of Passwords (40%):
   The lowest compliance rate indicating that employees are least likely to be proactive about up-to-date passwords, making their accounts vulnerable to unauthorized access.

Implications:

Strong password usage demonstrates an acceptable level of compliance, whereas further improvement in knowledge and the implementation of policies regarding password reuse and updating passwords in a timely manner is required. Automation and policy enforcement can fill in these gaps.

Behavioral Monitoring and Threat Detection

Tool	Incidents Detected	Detection Accuracy (%)
Traditional Monitoring	65	65
Behavioral Analytics	90	90

Table 3: Behavioral Monitoring and Threat Detection

It compares the capabilities of two monitoring tools to identify threats from within:

1. Traditional Monitoring:
   Detected 65% of incidents, accurately 65% of the time. These tools are based on set rules and thresholds that can overlook more subtle or advanced insider actions.
2. Behavioral Analytics:
   Identified 90% of incidents at precision of 90%. These tools outperformed traditional methods in threat detection, even subtle ones, by analyzing patterns and recognizing deviations in user behavior.

Implications:

Compared to traditional monitoring tools, behavioral analytics significantly surpass the ability to pinpoint insider threats..it also makes sense

when it comes to the deployment of these advanced tools required for realtime monitoring and detection of potential threats by the Financial Institutions.

DISCUSSION

An analysis of training data that took place at the University of Calgary in 2014 demonstrated a striking decrease in phishing susceptibility after tailored training programs were implemented, with click rates falling from 45% to 15% after infection. This is consistent with data from Pham et al. (2021) also found comparable decreases in susceptibility to phishing posttraining in financial institutions. These findings illustrate that regular staff training is effective in raising awareness of social engineering attacks.

Phishing attacks rely on human psychology, which makes training the most important line of defence. IBM (2022) mentioned especially the training programs that include realworld or interactive learning experiences that can reinforce employees' ability to recognize phishing attempts. But such interventions need to be reinforced regularly and updated as phishing techniques evolve (Gupta et al, 2021).

Enforce Password Compliance and Policy

One of the discoveries the research made was that, on average, employees were not compliant with passwords policies (only 40% were compliant with regard to the time to change password). This aligns with the findings from Nguyen et al. (2020) who further reinforced this idea, arguing that employees largely perceive password policies as burdensome, leading to noncompliance. Poor password management practices, such as bad password reuse and infrequent password updates, put systems at risk for credential stuffing attacks and other types of breaches.

Therefore, organizations must ensure they implement MFA and enforce password expiration policies by using automated tools. According to (Kumar and Hayward 2022), password manager tools (which cryptographically store these passwords on both ends) help address compliance concerns and lighten the cognitive load on employees. Moreover, interactive gamified training modules can enhance employee engagement and compliance with password hygiene (Pham et al., 2021).

It was shown that behavioral analytics was much more effective than traditional monitoring tools in detecting insider threats (90% vs. 65% detection accuracy), which means it was statistically significantly outperforming traditional monitoring tools. All these results support CERT Insider Threat Center (2021), which stated that anomaly detection can help us reveal subtle patterns suggesting insider threats. Behavioral analytics are monitored by machine learning to study the activity of users and report realtime alerts when an activity is being deviated from the baseline behavior.

Conventional monitoring tools (which depend on predefined policies) are, however, rarely adequate to discover complex insider risks or the intentional misuse of privileges. Nguyen et al. As discussed (2020), behavioral analytics are specialized in covering those limitations and provide proactive

and adaptive capabilities in threat detection. Effective implementation, however, also requires the careful balancing of false positives, which can undermine employees trust in monitoring systems (Sarker et al., 2021).

Culture of the company and Employee Point of view

Feedback from employees regarding cybersecurity efforts indicated that awareness programs (70%) and Zero Trust (75%) programs are perceived most positively, while monitoring tools received a lower score (65%), likely due to employee concerns about privacy. The results here are similar to Gupta et al. (2021) who emphasized the importance of clear communication regarding monitoring tools in establishing employee trust and buyin.

Issues and Suggestions

As effective as these strategies are, there are a few difficulties:

1. The Sustainability of the Effectiveness of Training:

   Training programs were found to yield substantial short term improvement, but periodic refreshers are necessary to maintain these gains. Pham et al. Microlearning patterns: Dunn & ifeachor(2021) suggested introducing gamification elements as well as individualized content to keep the learner engaged over time

2. Managing Privacy Concern

   Although companies can increase their threat detection with behavioral analytics, they need to ensure that they address employees' fears over privacy and the potential for the misuse of monitoring information. To build trust in monitoring systems, the CIS Certified Expert Recommended: Monitoring Journal (2021) suggested transparent communication regarding the purpose of monitoring, implementing role based access controls, and conducting regular audits.

3. Adapting to Evolving Threats:

   Instead, cyber threats are continuously evolving so the world needs constant innovation and change. To counter such threats, organizations need to invest in AI enabled threat detection systems and partner with industry experts to anticipate potential risks (Nguyen et al., 2020).

Practical Implications

There are multiple practical implications of the findings for financial institutions:

However, you can invest in regular training, as simulation based training programs significantly reduce the likelihood of falling for phishing attacks, making it vital for employees' awareness programs.

Utilize Advanced Monitoring Tools Behavioral analytics or threat hunting are increasing detection capabilities for threats to an organization and should be adopted into the existing security framework.

By employing tools such as password managers, tools that enforce mandatory expiration policies, and other itp for automation, organizations can ensure better compliance and reduce human error.

Create a Security First Culture: Getting leadership buying and engaging employees are key to making cybersecurity part of how organizations do business.

Limitations and Future Research

Although this study offers valuable insights, some limitations need to be corrected in future:

1. Sample Size: A small number of employees/institutions were analyzed. The generalizability of the findings could easily be improved by widening the sample size and geographic diversity.
2. Duration: The research was conducted over a relatively short period of time. Longitudinal studies should assess the long term effect of such interventions.

CONCLUSIONS AND RECOMMENDATIONS

Furthermore, as cyber threats become more sophisticated, the dependence on human actions within organizations and security frameworks requires that the human factor be a key target issue of bank cybersecurity. The core focus of this study was on employee related vulnerabilities (phishing susceptibility, noncompliance, and insider threats) and introduced methods for tackling the vulnerabilities mentioned above. The results highlight the need for combined technical solutions, training programs, and organizational practices to minimize risks and improve enterprise security.

Key Findings

1. Phishing Susceptibility*:*

   Our study found that, through the use of targeted training programs, resistance to phishing chick click rates was reduced from 45% to 15%. This is consistent with past work highlighting the importance of simulation based training in enhancing employee awareness (Pham et al., 2021). Results of this study show that regular and engaging training can significantly decrease human weaknesses to social engineering attacks.
2. Password Compliance*:*

   Covered password policies had varying degrees of compliance, where strong password usage achieved a 60% compliance rate whereas timely updates were at 40%. This finding underscores a ubiquitous obstacle in organizational cybersecurity in which employees perceive the password policies as a hassle (Nguyen et al., 2020). Automated enforcement mechanisms and tools such as password managers can fill this gap, resulting in improved security and usability.
3. Insider Threat Detection:

Behavioral analytics were reported to be highly effective in detecting these fraudulent attempts with a 90% detection rate as opposed to 65% which was the average of traditional monitoring tools. Advanced tools similar to the ones, that detects high performance and subtle insider threats and anomalies, contribute to an effective measure for financial institutions (CERT Insider Threat Center, 2021). Successful deployment, however, will require careful calibration and transparent communication to address privacy concerns.

4. Perceptions of the Employees and Organization Culture:

   Awareness programs (70%) and Zero Trust policies (75%) had the highest positive impact on employee feedback and showed a strong foundational baseline of support for these measures. But less feedback for monitoring tools (65%) indicate privacy barriers still exist. Security challenges are pervasive because these challenges are not only brought by technological advancements; these are being promoted by human aspects as well (Gupta et al., 2021); hence it is important to cover it through a cultural perspective (Gupta et al., 2021; Gupta et al., 2022b).

Practical Implications

The study's results are important for financial institutions, and suggest that:

Employee awareness programs must include simulation based and interactive training initiatives. Continuous reinforcement and scenario based trainings can keep the net of phishing awareness and response vibrant.

1. Enhancing Policy Enforcement:

   MFA, password expiration policies are some of the automated enforcement mechanisms which promote compliance and mitigate risks for weak password management.

2. Embracing Advanced Monitoring Tools:

   Insider threat detection must be given priority for behavioral analytics. These tools may offer near realtime intelligence and increase your organization's resiliency to both accidental and malicious insider activity.

3. A Security First Culture: Enabling Security at Each Level

   For cybersecurity to be integrated into established practices of organizations, leaders must commit to upholding their policies, communicate them clearly across the entire organization, and acknowledge the efforts of working in alignment with their policies. To foster trust and promote compliance, it is important to address privacy concerns associated with monitoring tools.

Adversities and Advice

Although this study proved the proposed strategies were effective there are still multiple challenges:

1. Sustaining Training Impact:

Like any good snack, what you train will go stale without a refresher. Pham et al. suggested mini modules that are fully gamified and personalized. (2021) preserve acquiescence and guarantee durable change.

2. Compromising Security for Usability:
   Security implementation should not obstruct employee productivity. These tools can help balance security and ease of use, such as password managers and biometric authentication (Kumar & Hayward, 2022).
3. Managing Evolving Threats:
   Organizations need to keep updating and innovating their capabilities for threat detection and response as cyber threats keep evolving. Financial institutions should prepare for the new risks by investing in AIbased security solutions and partnering with industry experts (Nguyen et al., 2020).
4. Addressing Privacy Concerns:
   Providing transparent communication on what the monitoring tools do and why they are being utilized can help alleviate employee concerns. Trust can be further fostered with regular audits and rolebased access control to ensure ethical implementation.

FURTHER STUDY

There are some limitations for this study, and lines for future research are as follows:

1. Little sample; The survey was targeted at limited employees and institutions, therefore this will limit the reach of the outcomes. A larger and more geographically diverse sample would yield more robust insight. As you can see, there is no mention of random assignment in the original summary. Further longitudinal studies are required to assess the long term impact of these interventions.
2. Emerging Technologies Integration: Some future studies can look for integration of blockchain based security solutions and advanced AI algorithms to address human related vulnerabilities and insider threats.

Human factor is the most crucial part of bank cybersecurity, as it is a weak point and a defensive mechanism at the same time. By focusing on the employee aspect of risk, this study also illustrates the value of training programs, policy enforcement mechanisms, and behavioral analytics. Implementing security best practices, enhancing resilience through advanced technologies, and addressing operational challenges will enable financial institutions to develop robust systems that defend against internal as well as external threats. Ongoing research and innovation will be necessary in order to keep up with emerging cybersecurity threats, and with the ultimate goal of maintaining the longterm security and trust of digital financial systems.

REFERENCES

CERT Insider Threat Center. (2021). *Managing insider threats: A comprehensive guide for financial institutions*. Carnegie Mellon University.

Gupta, A., Sharma, R., & Li, H. (2021). *The role of employee behavior in cybersecurity: Risks and mitigation strategies*. Journal of Financial Security, 15(3), 112129.

IBM. (2022). *The cost of a data breach: Financial sector analysis*. IBM Security Report.

Kumar, S., & Hayward, D. (2022). *Cybersecurity in mobile banking: Trends, challenges, and solutions*. Financial Technology Journal, 8(2), 4567.

Nguyen, H. T., Pham, T., & Tran, Q. (2020). *Innovations in insider threat detection: Behavioral analytics and AI integration*. International Journal of Cybersecurity, 14(1), 2348.

Pham, M., Li, C., & Sun, J. (2021). *Phishing simulations in the financial sector: Evaluating employee awareness programs*. Journal of Information Security, 19(2), 6784.