Cyber Security Challenges in Aden's Commercial Banks: Current Reality and Future Prospects

AL-Sanidi, K. W. S [1]
Saeed, Z. S. A. S [1]
Yahya, A. F. M [1]
Saleh, K. M. M. [1,*]
Qassem, A. H. M [1]
Abdullah, A. K [1]
Hussein, H. A. H. H [1]
Ali. B. A. S [1]

Received: 20/05/2025
Revised: 04/08/2025
Accepted: 05/08/2025

[1] Cyber security University of Science and Technology, Aden , Yemen
*Corresponding Author's Email: khalidmunassar63@gmail.com
https://doi.org/10.20428/jst.v30i12.3033

Cyber Security Challenges in Aden's Commercial Banks: Current Reality and Future Prospects

Khaled Munassar Mohammed Saleh
Cyber security
University of Science and Technology
Aden , Yemen

Abbas Fouad Musaed Yahya
Cyber security
University of Science and Technology
Aden , Yemen

Zeyad Saeed Ahmed Saeed
Cyber security
University of Science and Technology
Aden , Yemen

Khaled Waleed Salem AL-Sanidi
Cyber security
University of Science and Technology
Aden , Yemen

Bashar Ahmed Saleh Ali
Cyber security
University of Science and Technology
Aden , Yemen

Hussein Adel Hussein Hussein
Cyber security
University of Science and Technology
Aden , Yemen

Abdulrahman Kamal Abdullah
Cyber security
University of Science and Technology
Aden , Yemen

Abdul Hakim Murad Qassem
Cyber security
University of Science and Technology
Aden , Yemen

Abstract— This study examines the cybersecurity challenges facing commercial banks in the city of Aden in light of rapid digital transformation. This is because these institutions experience an increase in vulnerability to cyberattacks, even when they deploy modern technologies, such as online banking and cloud systems, due to outdated infrastructure [1], [2], [7], human error [8], [18], poor regulatory frameworks [1], [2], and low resources [1], [3]. Based on mixed-methods analysis [1], including surveys of three Aden banks [1] and a review of global trends [4], [5], the research identifies critical gaps being overreliance on reactive blue teams, inconsistent compliance with international standards (e.g., ISO 27001 [9]), and a lack of proactive red-team exercises [12] or mandatory employee training [6], [8]. Banks express confidence in threat detection, but a lack of incidents over 24 months may mean under-detection, not resilience [11]. With respect to governance, suggestions were made for individual and collective actions, e.g., imposing regular phishing tests [8], AI-based threat-detection tools [5], [16], partnerships to prototype a red team [12], [13], and regulatory reform including ISMS certification [9] and a national cybersecurity authority [14], [15]. The results highlight the need to identify and mitigate systemic vulnerabilities in order to protect financial stability and public confidence in Aden's precarious socio-political environment [2], [3]. (Abstract)

Keywords— Cybersecurity, Commercial Banks, Aden, Yemen, Human Error, Red Teams, ISO 27001, Ransomware

I. INTRODUCTION

In recent years, the financial industry has undergone a dramatic change, which has led to the widespread adoption of digital technologies. Commercial banks in Aden have adopted digital mechanisms in the form of online banking, mobile applications, and cloud portals to optimize their operational processes, improve customer service levels, and broaden their range of reach. Advancements like those have made them even more vulnerable to assaults on data or security breaches than in the past. Although great benefits have been derived from this shift in technology, it has also led to severe challenges in terms of security. Aden's commercial banks are now highly dependent on interconnected systems and digital infrastructure for network operations. This has also made them prime targets for cybercrime such as malware (in particular ransomware), phishing attacks, and insider threats, as well as more traditional forms of snooping on data. Aden's commercial banks operate in a climate where limited resources and conflicting priorities often mean that little attention is given to cybersecurity. In addition, constraints created by obsolete technological infrastructure, weak regulatory frameworks, and derisory investment in defenses against cyber warfare further aggravate the situation. Resulting in their becoming not just vulnerable to financial losses but also imperiling their public standing—which is crucial to maintaining confidence with the customers who keep their business going and ensuring long-term growth prospects.

This research seeks to present a complete picture of the cybersecurity situation at Aden's commercial banks. Through general observation of what measures are being taken today to shore up cyber defense, analysis of where these may be lacking, and some suggestions for improvements that could be made in those areas, the study attempts to help shape the larger public discourse on protecting cyberspace more effectively—particularly in fragile environments. It is anticipated that the results of this research will be of particular interest to policymakers, bank executives, IT personnel, and other stakeholders deeply involved in shaping the future course of cybersecurity within Aden's financial industry.

II. RESEARCH PROBLEM

This paper will consider the hardships facing commercial banks and financial institutions in Aden and look at how cyber threats undermine the traditional notions of security and trustworthiness that have always characterized them. As cyber threats evolve at an increasingly rapid pace and cybercriminals grow more sophisticated, providing security solutions has become an urgent necessity to ensure that sensitive data won't be compromised. Consumer confidence must remain unshaken in business dealings. Indeed, the fear of cyber threats may deter future transactions from upcoming- Even though efforts have been put forth to

reinforce it, Aden's commercial banks are vulnerable to crippling cyberattacks due to a lack of system complexity, insufficient skilled personnel, and inadequate oversight. The resolution of these matters is essential in the interests of the long-term security and safety of the banking industry. With these points in mind, we dive deeper into the heart of our analysis. And ask the question. What are the main risk management weaknesses and cybersecurity vulnerabilities that Aden's commercial banks confront, and how many of these issues could be resolved to strengthen their defenses against cyber threats?

III. Research Objectives

A. The primary objectives of this study:

To evaluate the existing cybersecurity measures introduced by the commercial banks in Aden. At the same time, identifying and then dealing with gaps that have been found in them.

To investigate what kind of cyberattacks are being launched against these institutions, how frequently they succeed, and what impact this can have on the bank's trust. This includes, of course, exploring the most common types of cyber threats that are encountered: phishing, ransomware, and "insider" threats (such as employees from your own company who turn into spies against their employers); also, realizing how such threats exploit vulnerabilities within banks' systems.

To analyze the regulatory role in strengthening cybersecurity This objective is oriented towards evaluating the absence of the current cybersecurity laws and regulations in Yemen, especially their relevance to financial institutions located in Aden. The study will examine the impacts of national laws on banking activities and financial institutions operating within its territory. Based on this, a number of measures should be investigated to counter possible cybercrime. The steps may range from investing money in advanced technology that combats virus attacks to inaugurating professional training classes for employees and promoting public-private partnerships with institutions such as banks or some other relationship between industry individuals at large. Which forms of international protection are of the greatest importance? Since cyber threats are truly global in nature, this research also emphasizes that local banks, international institutions, and cybersecurity exporters must come together to build a secure defense network. By meeting these objectives, this research can be regarded as a blueprint for Aden's commercial banks to move through the complex and ever-changing landscape of cybersecurity.

IV. Research Methodology

The analysis is mixed-methods, including secondary sources ([1], [6], [7]) and primary survey data collected from three Aden banks between March 26 and April 2, 2025.

Survey responses were collected from key personnel responsible for cybersecurity and IT operations, including IT managers, information security officers, and supervisors with operational oversight of digital systems in each bank. This ensured that the data reflected both technical implementation and managerial decision-making levels, providing a comprehensive view of current cybersecurity practices across Aden's commercial banks.

By leveraging quantitative data to evaluate tool adoption, testing frequency, and compliance levels, this analysis is complemented by qualitative insights that cover risk management approaches and challenges.

Integrating 2025 cybersecurity trends (AI adoption, ransomware threats [4]–[5]) and Yemen studies [2]–[3], findings, and recommendations critically analyzes detection confidence and red team gaps across sectors.

The three commercial banks included in this study were selected based on their market presence and operational footprint in Aden, collectively managing 18 branches—representing a significant portion of the city's banking infrastructure. While not a random sample, these institutions were chosen for their diversity in size and ownership structure (public, private, and hybrid models), willingness to participate, and varying levels of digital adoption. This purposive sampling approach enables a comparative analysis of cybersecurity practices across different institutional contexts within a constrained environment, enhancing the practical relevance of the findings for similar institutions in fragile states.

A. Ethical Validation

Peer Debriefing: Cybersecurity experts reviewed thematic interpretations to minimize bias.

Confidentiality: Participant identities and sensitive operational details are anonymized.

B. Response Bias Mitigation:

To minimize response bias, participants were assured of anonymity, and survey responses were aggregated at the institutional level. The research objectives were clearly communicated as non-evaluative and aimed at improving sector-wide resilience rather than assessing individual performance. Where possible, self-reported data were cross-checked against publicly available information and aligned with known technical standards to enhance validity.

V. Literature Review

Few issues in the history of the Internet have attracted as much attention from many different disciplines as security, especially in banking. In Aden, economic uncertainties and underdeveloped infrastructure, along with a loose regulatory environment, create special safety hazards for banks. Although an increasing number of studies on information security have been published, few systematic ones have looked into risk management practices of Yemeni banks. It is a lacuna partially bridged by Al-Ashwal and Nasser. Their research evaluates information security risk management (ISRM) practices currently being observed by Yemeni banks and organizations. Their findings show that work has gone forward in some aspects, but progress is seriously lacking, particularly in actual risk handling and risk assessment procedures [2]. These insights have relevance to the wider context of Yemen, including the banking sector in Aden. The dependence on outdated systems, human error, lack of resources, and regulatory loopholes is a common theme running through all the research reports. This is also what Al-Ashwal and Nasser say. Only the fourth level of ISRM maturity requirements is met now by Yemeni banks; the average index scores were 3.58-4.08. Even so, there is a need for them to take more aggressive and systemic approaches in managing risks, just as applicable within Aden as without.

The reliance of Aden's banking industry on outdated systems that no longer receive updates or support is one of its major

vulnerabilities. This creates large security holes for intruders to exploit in the financial data of 70 percent of banks running old systems, say Abdullah and Al-Sakkaf [1]. This conclusion finds further support from Kshetri, who studied the computer security threats facing developing countries and found that financial institutions with poor technology infrastructure are more vulnerable to cyber-attacks [7]. Therefore, similar challenges have been seen in other regions, such as Pakistan and Kenya, where presentations used old technology to make what would otherwise have been invisible problems visible [17], [18]. Even though Al-Ashwal and Nasser do not focus only on obsolete systems, their research indicates that a poor overall level of technology readiness contributes to low levels in ISRM maturity among Yemeni banks generally, including those in Aden [2]. Human error is an important cause of cybersecurity incidents. Indeed, international research shows that nearly 90 percent of such breaches result from carelessness on the part of employees [8]. In Aden, the absence of structured training programs has made banks more susceptible to phishing scams and inadvertent disclosure of sensitive information. Such problems were also found by Mwagwabi et al. in their study of Kenya, where they pointed out that poor training is a major source for enterprise risks [18].

Some key points from the research of Al-Ashwal and Nasser: Yemeni banks lack knowledge and financial resources to implement comprehensive information security training programs. Employees often disregard key security protocols, such as not clicking on suspicious emails and using long passwords. The study therefore suggests that annual training sessions be held for all employees and simulated phishing exercises be integrated into these courses [2]. Human error is responsible for many security breaches; reducing the errors that people make in their daily work will improve everyone's security posture. Talking from the same point of view as above, Abdullah and Al-Sakkaf exemplify why it is necessary to institute a culture of security consciousness that makes systematic training a prerequisite. They similarly point out problems in information security as one way how managers can help services to function efficiently [1].

Weak Legal Foundation

A secure information infrastructure in Aden's banks would require its own protective legal framework. Abdullah and Al-Sakkaf concluded that financial institutions have no common operational procedures, so they stand on thin ice [1]. Smith & Jones also found similar results in their study on regulations' impact upon national security resilience: firmer regulation less (fewer attacks and quicker recovery times) [19]. Studies from other parts of the world, such as Sub-Saharan Africa, have documented the effectiveness of regulatory systems in preventing cyber risk [20]. Although Al-Ashwal and Nasser do not go into the question of legal framework in depth in Yemen, their research implies that Aden's banks share a decentralized and inconsistent security environment. This situation can be linked with another problem for Aden's banks: there is no centralized cybersecurity government in Yemen [2].

Resource Constraints and Socio-Political Turmoil

Many problems can be caused by the fall of Aden's government, and opponents seek to exploit them, such as the political and resource limitations faced by electronic information in the city's banks. A survey by Abdullah and Al-Sakkaf reveals that less than 5% of banks' IT budgets are earmarked for protecting electronic systems, compared to an international average of more than 10% [1]. This underinvestment provides banks with powerful incentives to develop defenses that are easy targets for sophisticated attacks. For instance, the study by Al-Ashwal and Nasser concludes that ongoing conflict disrupts communication channels and damages key infrastructure, complicating yet further attempts to address security issues [2]. People lose confidence in digital banking, which causes a vicious circle to be set up for a regressive cycle upon stagnation. These obstacles pose a challenge that will need to be met with concerted efforts by policymakers, financial institutions, and the international community alike. This pattern has been found all over the world in conflict-affected regions, underscoring the importance of finding homegrown solutions contextualized by local circumstances.

International Perspectives and Comparative References

International studies can assist Aden with cybersecurity problems. AI-based monitoring tools can be used to great effect in Yemeni banks, for example, filtering out any abnormal transactions. In addition, Abdullah and Al-Sakkaf together provide us with an even more comprehensive understanding of local conditions, while reports from other areas also point out that these are global-level issues [1].

VI. Preliminary Findings

Survey responses from three banks, which together comprise 18 branches in Aden, paint a sector-wide picture of cybersecurity trends and shortcomings: Cybersecurity Measures Every bank has formal policies reviewed yearly or bi-annually and has those classical blue teams using a framework of tools (firewalls, IDS, SIEM, EDR), which shows some similarity in technical adoption. The only universal practices are regular vulnerability assessments and penetration tests (annual or quarterly), with all providing red team exercise reporting. No bank appears to have a dedicated in-house red team; rather, blue teams perform the majority of vulnerability detection, and pen testing is performed either by third parties (2 banks) or a combination of in-house and external resources (1 bank). In these exercises, only one bank includes social engineering, and only one enforces mandatory training, uncovering a sector-wide shortfall in proactive testing and employee preparedness, which can be significant vulnerabilities given trends indicating human errors [8]. International standards (ISO 27001, PCI DSS) compliance is partial: two mention them but lack full certification, and one lacks compliance, revealing weak standardization [9]. Strengths that are universal include mechanisms such as multi-factor authentication (MFA) and data encryption. Threat Detection and Response No banking cyber-incident (ransomware, phishing, etc.) occurred in 24 months; all banks expressed high confidence in 24-hour detection. Two have pressure-tested incident response plans with drills in the last 12 months, and one has not, suggesting possible complacency as worldwide ransomware rises [4]. None of these solutions share threat intelligence, a shortcoming opposite of emerging overall collaborative defense trends [10]. The problem here is two-fold: first, without red team simulation expertise, detection normally relies on blue teams,

wherein detection must be passive and threats must be reacted to, rather than proactively, instead of being "brought to the table" within Yemen's context—a fragile place to say the least. [11] Risk Management and Points of Challenge Risk management processes vary: one has no formal process (only "limit privileges"), two include risk management in enterprise strategies driven by IT and assign CVSS (two of them) scores, and one has no "prioritization method." For banks: regulatory compliance, evolution of threats, limited budgets in the organizational context, employee awareness, and expertise shortages—one bank cites budget and expertise as red team barriers (a lot of others feel they don't need red teams)—similar to Yemen's systemic constraints [2], [3]. This corresponds with fragile-state patterns where a lag exists in proactive capabilities [11]. Future Plans and Trends All plans include technological investments, and two are placing a focus on staffing, while one increases frequency of training and testing, showing intent to improve. None of them are planning for cloud-based solutions—probably because of maximum infrastructure limitations [1]—but two of them envisage some artificial intelligence in the future, agreeable to the 2025 trends [5]. The lack of red teams and high detection confidence (and no incidents) indicates potential under-detection over strong defenses [11]. The results reveal a sector with robust technical foundations and notable deficiencies in proactive red team capabilities, use of interim training, and alignment with regulatory reforms, making it susceptible to trending threats such as phishing and ransomware [4]. VII. Strengthened Recommendations Drawing from the findings and trends in 2025, the recommendations below seek to detail Aden's cybersecurity weakness in paragraph form, which confronts the objectives of the study mentioned above. As 82% of breaches are caused by human error [8], while training decreases breach costs by 17% [6], only one bank requires training; addressing the former would represent a sector-wide vulnerability. To close this gap (Objective 1), we recommend mandatory training with phishing simulations across all banks in response to the global surge in social engineering attacks [4]. Implementation is possible within the same cost-efficient online platform or local IT firms and can be scaled to 18 branches as per the recommendations in resource-poor settings [1]. This counters Yemen's personnel shortages [2], bolsters awareness and resilience to trust-impacting threats (Objective 2), and makes it especially critical in the absence of red team simulations. ISO 27001 requires proactive testing [9], and BIS notes 70% gains from red teams [12], but Aden's banks do not have red teams, relying on blue teams and third-party penetration tests, with one citing shortages of relevant expertise. For investigating and mitigating vulnerabilities to cyberattacks (Objective 2), banks should create in-house red teams or expand their outsourcing to include exercises conducted quarterly, with social engineering, funded by the World Bank [1], along with significant training programs to develop in-house expertise. This mitigates emerging ransomware threats [5], fills system complexity voids [2], and coincides with a shift to stronger safeguards (Obj. 1) in Aden's underpowered industry [3]. While ISO 27001 builds trust and compliance [9], inconsistent implementation (2 reference standards, 0 certified) is symptomatic of regulatory gaps [2]. (For the third objective of strengthening cybersecurity via regulation) ISMS (Information Security Management System) certification based on critical systems (certification may be conducted in-control starting from the critical systems with local consultancy-shift support from USAID) [13]. It fits Yemen's oversight requirements [3], matches the sporting world and others moving toward standardization [4], and offers depth of defense scalable with the nature of an advanced threat [2], promoting trust and integrity. And which none coordinate threat intelligence between one another like has become the norm [10]. In a way, from a regulatory perspective (Objective 3), banks should be pushing for the establishment of a national cyber defense center [14] analogous to Oman's Cyber Defence Centre, mandating compliance and intelligence sharing [15] in cooperation with the IMF. This approach is proactive against cybercrime (2) through partnerships, closing related gaps in Aden's fragmented defenses, and key to harnessing, for example, social networks' connectivity (3) for global sharing of security expertise and ultimately creating a trusted network to counter global threats. AI decreases response times by 30% [6]; open-source tools are compatible with fragile states [16]; however, Aden's financial institutions depend on basic infrastructures without red team assistance. In lieu of (1), to close emerging threats (2), upgrade SIEM/EDR with AI & open with a dunk from (1)—Insight & World Bank assisted by vendor pilot [1]. This is based on 2025 AI trends [5], which guarantees low-cost resilience in a context where budgets shrink [2], matching with future plans to strengthen long-term cybersecurity. Conflict reduces capacity [13], and external assistance is essential [1], with Aden lacking in personnel and experts [2]. When developing proposals in support of each of these objectives, banks stand to benefit from USAID's ERLP [13] or World Bank funding for the training, red team development, tools, and compliance needed to support them, ensuring the proposals align with broader trends in capacity-building [4]. It addresses gaps with local talent and worldwide expertise, forming a defense network (Objective 3) to protect data and trust from the troubled state of Yemen.

VII. Strengthened Recommendations

The survey responses of three banks, corresponding to 18 branches in Aden, demonstrate industry-wide cybersecurity trends and critical gaps:

Cybersecurity Measures

All banks have formal policies reviewed (annually or semiannually) and have blue teams with automated tools (firewall, IDS, SIEM, EDR); therefore, technical adoption also has been consistent. All reporting red teaming exercises, regular vulnerability assessments, and penetration tests (annual or quarterly) are universal. But none of the banks report having a focused internal red team; rather, most of the vulnerability detection is the domain of blue teams, and penetration testing is done by outside third parties (two banks) or a combination of internal and external resources (one bank). Despite this, only one bank embeds social engineering into these exercises, and just one has mandatory training, revealing a persistent gap across the sector in proactive testing and employee readiness, a crucial weakness given trends in human error [8]. Adherence to international standards (ISO 27001, PCI DSS) is inconsistent: two of them are referenced without full compliance, and one does not comply, showing weak standardization [9]. Universal

strengths include things like MFA (multi-factor authentication) and data encryption. Threat Detection and Response In 24 months, there were no cybersecurity incidents (e.g., ransomware, phishing), and all banks were highly confident of detection within 24 hours. Two have practiced incident response plans with drills in the last year, and one has not, suggesting some potential for complacency in the face of surging global ransomware [4]. None exchange threat intelligence—a gap that sets them apart from collaborative defense initiatives [10]. Blue teams' reliance on detection without red team simulation expertise raises concern about proactive threat identification focused on the development of a provider' state in Yemen's fragile context [11]. Challenges and Risk Management Risk management: no formal process in one; two consider it an extension to an enterprise; risk management is overseen by IT; different approaches to vulnerability prioritization (two use CVSS scores, one does not have any). Similar systemic factors come into play in Yemen [2], [3], but in Yemen challenges are regulatory compliance, evolving threats, limited budgets, employee awareness, and expertise shortages—one bank cites budget and expertise as red team barriers, and two see no need. Deployments are in accordance with fragile-state patterns where proactive capabilities are in the rear. [11]. Future Plans and Trends The example plans showed technological investments, two of which prioritized staffing, while another focused on training and testing frequency, which would indicate that a plan was seeking to improve. None plan to migrate to the cloud, presumably because they already have infrastructure limits [1]; however, two respondents view AI as an upcoming impact, which agrees with 2025 trends [5]. Finally, no red teams and high detection confidence (no incidents) suggest potential under-detection rather than robust defenses. [11] This data points to a sector with solid technical skills but pronounced gaps in proactive red team development and training consistency, compounded by limited regulatory alignment on security controls, making it susceptible to prevailing threats such as phishing and ransomware [4]. VII. Strengthened Recommendations In line with the objectives of the study, below is a discussion of the cybersecurity gaps present in Aden and how they can be plugged based on research findings and 2025 trends. Given that human error is a driver for 82% of breaches [8], and that training reduces costs associated with it by 17% [6], it's worrying that only one bank we examined Out of dozens we examined, magnificent workings in this area absolve them of "significant" security breaches and expose a major weakness for the industry as a whole. To bridge this gap (Objective 1), all banks should implement mandatory training with phishing simulations annually to counter the global rise in social engineering attacks [4]. Implementation can be on affordable online platforms or local IT firms, scalable across 18 branches as prescribed for resource-constrained settings [1]. This addresses Yemen's personnel shortfalls [2] and increases awareness and resilience to trust impact threats (Objective 2), a must in the absence of red team exercises. ISO 27001 requires proactive testing [9], while BIS claims 70% detection improvements from red team testing [12], but Aden's banks have no independent red team and rely on blue teams and third-party penetration tests, while one cites skill shortages. And on the other hand, to investigate and buffer against vulnerabilities to cyberattacks (Goal 2), banks should create internal red teams or add to outsourcing \begin{to add quarterly exercises with social engineering done with financing from [1]: "Protocols to Prevent Social Engineering" and subsequently expose banks to training programs to build expertise. This prevents trending ransomware threats [5] from exploiting system complexity gaps [2] and aligns with the pressing need for robust measures (Objective 1) in Aden's under-resourced sector [3]. ISO 27001 fosters trust and compliance [9], but fragmentation (two reference standards, zero certified) indicates regulatory shortcomings [2]. Objective 3: To deepen regulation as a means of enhancing cybersecurity: Banks should apply for certification with an Information Security Management System (ISMS), with a gradual approach starting from critical systems, drawing on local consultants and USAID support [13]. This addresses Yemen's oversight requirement [3], interfaces with global standardization [4], and provides scalable defenses towards advanced threats [2], with fostered trust and integrity. Weak oversight in the context of Yemen increases risks [3], and, unlike collaborative trends [10], none share threat intelligence. Finally, for the regulatory roles (Objective 3), national economic momentum suggests an effective compliance and intelligence collaboration through a national cybersecurity authority (exemplar: Oman's Cyber Defense Centre [14]), integrated through cooperation with the IMF [15]. It meets cybercrime with partnerships and meets Aden's disaggregated defenses [2], underpinning a spire of authentic network enabling to protect it against superimposed threats, making it an urgent step towards trust. AI [6] cuts down response times by 30%, and open-source [16] tools serve fragile states, but Aden's banks depend on rudimentary setups, with no red team aid. To manage emerging threats (Objective 2) and gaps (Objective 1), they must augment SIEM/EDR with AI and open-source solutions, interfacing with vendors and with World Bank support [1]. SIEM/EDR systems with AI-enhanced open-source solutions such as Wazuh (for log analysis and intrusion detection) or Snort (for real-time network threat detection), which are cost-effective, scalable, and suitable for low-resource environments [16]. This takes advantage of AI developments of 2025 [5], ensures resilience against cheaper cyber adversaries when budgets and fiscal pressures will favor business intelligence [2], supports the future [1], and is an enabling foundation for the cyber control architecture. Conflict constrains capacity [13], with external assistance paramount [1], further complicated in Aden by personnel and expertise gaps [2]. To fulfill all these aims, banks should pursue USAID's ERLP [13] or World Bank funding for training, red team creation, tooling, and overall compliance [4], tailoring bridge proposals to match capacity-building trends [4]. This connects local needs with international capabilities for a defense network (Objective 3) to secure data and trust in Yemen's context of fragility.

Phased Implementation Roadmap:
Given the resource constraints and fragile socio-political context of Aden, the following phased approach is proposed:

Table 1: Phased Cybersecurity Action Plan for the Banking Sector

Time Frame	Action
Short-term (0–6 months)	Launch mandatory cybersecurity training with phishing simulations; initiate AI-powered SIEM/EDR pilot using open-source tools (e.g., Wazuh, Snort); establish internal working group on ISMS certification.
Medium-term (6–18 months)	Form in-house red team units or partner with regional cybersecurity firms for quarterly red-team exercises; begin ISMS certification for core banking systems with USAID or World Bank technical support.
Long-term (18+ months)	Advocate for and support the creation of a national cybersecurity authority; institutionalize threat intelligence sharing among banks; achieve full ISO 27001 certification and integrate AI-driven defenses across all branches.

Key Stakeholders and Responsibilities:
To ensure effective implementation, responsibilities should be clearly assigned:
Bank Executives: Champion cybersecurity initiatives, allocate budgets, and drive cultural change.
IT Departments: Implement technical controls, conduct training, and manage red/blue team coordination.
Regulatory Bodies (proposed National Cybersecurity Authority): Enforce compliance, facilitate threat intelligence sharing, and oversee certification processes.
International Partners (e.g., World Bank, USAID, IMF): Provide funding, technical expertise, and capacity-building programs to support training, tool deployment, and policy development.

VIII. Discussion

Addressing the limiting lack of red teams, training inconsistencies, and regulatory gaps, these recommendations also capture emerging trends such as integrated AI defenses and ransomware countermeasures [4], [5]. Objective 2 is about the impact of these threats, and the dependency on blue teams and outsourced testing, coupled with a lack of in-house red team expertise, means that there are too many threat vectors that go untested; if they do not impact the security posture, their existence may still be undetected. The absence of incidents may represent under-detection, not resilience, in Yemen's context [11]. Cheap and piecemeal, they strike the best equilibrium between fragility and more systemic challenges, providing a useful way forward for Aden's commercial banks given the limited resources and socio-political instability. This complements the unique vulnerabilities of Aden's banking sector and the global cybersecurity landscape, leading to the alignment of these findings and recommendations also from a feasibility and longer-term security perspective. The absence of reported instances of cyber warfare over a period of 24 months, combined with high confidence of being able to detect Wi-Fi nodes within 24 hours, are significant anomalies when viewed within the context of Yemen's precarious political and technological ecology [11]. While this may suggest strong defenses, the absence of dedicated red teams and limited social engineering assessments indicates that under-detection rather than genuine robustness is the issue. In 2025, ransomware and phishing attacks surged globally [4], revealing reliance on reactive identification of threats through blue teams—where Aden falls short. This leads nicely to objective 2, which is to explore the frequency and impact of cyberattacks on trust. Because banks do not have internal red teams to present smart attacks, they might not see vulnerabilities that external threat actors could use to take advantage of organizations—magnifying computer losses but, more critically, reducing customer sentiment of confidence, part of data storage banks' stability. The proposal to create red teams—in-house or in addition to outsourcers—speaks directly to this, providing a proactive change that could identify flaws before they are exploited. (The bank responsible for three breaches out of the six is the only outfit in the world that requires employees to go through some sort of training, even though 82% of breaches worldwide can be attributed to human error [8]). That gap directly undermines Objective 1's mission to assess and bolster existing cybersecurity measures. Banking in Aden is especially crucial due to shortages of personnel and the nature of antiquated systems making these banks susceptible to untrained staff [2] and thus targets of phishing scams, a constant threat mentioned among the trends of 2025 [5]. The proposed annual training with phishing simulation is a resource-efficient intervention that utilizes local resources and comes with the perception that we need to balance fragility with practical interventions [1]. By minimizing human error, banks can strengthen resilience, protect confidential information, and sustain trust (Objective 2), especially in a region whereby the adoption of digital banking is predicated on the public perception of security and overall safety. 50% of its citizens also rely on digital income [2], and regulatory inadequacies, such as inconsistent ISO 27001 adoption and lack of a national cybersecurity authority [3], echo a wider governance void in Yemen. This closely connects to Objective 3's emphasis on the regulatory role in cybersecurity. Devoid of standardized frameworks or threat intelligence sharing—practices that bolster global defenses [10]—the banks of Aden are soloed and reactive, woefully unprepared to combat complex, cross-border cyber threats. Adopting the national authority and promoting the ISMS certification based on the model of operationalization of a successful initiative, i.e., the Oman's Cyber Defense Centre [14], that establishes a phased and incremental program essentially leveraging external support (even USAID [12] and IMF [15]) to fill the local expertise gap. Not only does this bolster defenses, but it also calibrates Aden's banks to international standards that will attract foreign investment and partnerships so critical to a conflicted economy. In the context of evolving threats (Objective 2) and existing gaps (Objective 1), AI-driven tools and open-source solutions

integrated into SIEM/EDR systems also avail tools capable of detecting and responding to such new threats and taking advantage of 2025 trends where AI is said to reduce response times by 30% [6]. In Aden, where limitations on its infrastructure prohibit cloud adoption [1], these improvements offer a low-cost, high-availability upgrade to barebones setups, balancing the literature-noted resource constraints [2]. But their success hinges on overcoming expertise shortages—a challenge acknowledged within its findings [3]. They also invoke external funding (e.g., World Bank, USAID [13]) for the development of training and red team capabilities, linking these technical upgrades to human capacity so as to create a holistic defense network (Objective 3). This interaction is essential in Yemen's brittle environment, where piecemeal technical fixes would likely fall flat without competent individuals and institutions to drive them forward. This is still an important consideration of feasibility. Aden's banks have limited IT budgets (less than 5% of IT budgets for security [1]) due to conflict [2], so immediate investment is limited. However, the gradual, low-cost nature of these recommendations—beginning with training, piloting AI tools, and using donor assistance—could overcome these hindrances. While a limitation, the lack of cloud adoption indicates a pragmatic approach prioritizing on-premises solutions aligned to local infrastructure [1] and avoiding dependency on unreliable connectivity. Politically, supporting a national authority needs concordance in the chaos, yet backing (e.g., IMF [15]) can spur evolution, matching international appeals for collective cybersecurity in fragile states [11]. These steps balance current necessities with the long-term conditions for resilience and can serve as a model for implementation in other conflict areas. The ramifications are far broader than Aden. The results reflect trends observed in resource-poor and oversight-weak systems in developing countries (Pakistan, Kenya [17], [18]) and are likely generalizable. By confronting human error, preventive testing, and regulation, the banks of Aden could trailblaze a scalable method for resource-constrained financial systems worldwide. But success depends on execution—banks have to put these gaps before other competing ones, and stakeholder (policymaker, IT staff) efforts have to be unified. Inaction not only risks financial losses but also a trust deficit that could freeze growth across the digital banking sector, perpetuating the stagnation cycle identified in the academic literature [2]. On the flip side, the successful adoption of these solutions would position Aden as a regional case study on resilient cybersecurity, boosting its financial stability and public relations in an increasingly digital world. In sum, this study sheds light on Aden's cybersecurity landscape—robust in technology but brittle in preemption and regulation. The recommendations provide a balanced, evidence-based way to reinforce defenses, aligning with 2025 trends [4], [5] and Yemen's unique challenges [1], [2], [3]. They underscore the interplay of technology, human factors, and governance in securing trust and data, providing actionable insights for stakeholders to navigate the complex, ever-changing terrain of cyber threats.

IX. Conclusion

Commercial banks in Aden are functioning within a high-risk environment concerning cybersecurity because of a variety of reasons, including antiquated systems [1], [7], insufficient training [8], [18], and uneven regulation practices [1], [2]. Despite having foundational measures (firewalls [3], [5] and encryption [6]) in place, the sector's reliance on reactive defenses and third-party audits [1] predisposes it to emergent threats, including ransomware [4], [5] and social engineering [8]. [9] and underinvestment in employee preparation [6] that make these threats worse with few red teams dedicated to identifying these risks are also concerning.

In response to these vulnerabilities, banks must adopt proactive measures: mandatory cybersecurity training [8], AI-enhanced monitoring tools [5], [16], and public-private partnerships [10], [15]. Regulatory reforms such as ISMS certification [9] and a centrally led cybersecurity authority [14] are crucial for standardizing defenses and aligning with global practices [4], [10]. There will also be a need for external funding from organizations such as the World Bank and USAID [13] to fill resource gaps [1], [3].

The other, however, is temperamental, and due to its character, it cannot be trained in this way, so the banks of Aden, addressing these weaknesses and systemic weaknesses, can ensure their long-term viability and resilience against cyber threats and protect the trust of customers in them. Their findings are a starting point for stakeholders who need to take action to secure fragile environments from cyber-attacks by working together through innovation and adaptive governance [2], [11], [15].

Given the exploratory nature of this study and the limited sample size, future research should include a broader survey of financial institutions across Yemen, incorporating both urban and rural banks, to generalize findings and track longitudinal improvements in cybersecurity resilience.

References

[1] N. M. Alsakkaf and M. F. Abdullah, "Leveraging Big Data in The Banking Sector: An Analysis of Challenges and Opportunities at the Central Bank of Aden," Journal of Social Studies, vol. 30, no. 5, pp. 431-448.

[2] M. Al-Ashwal and H. Nasser, "Information Security Risk Management in Yemeni Banks: An Evaluation of Current Practices," International Journal of Engineering Trends and Technology, vol. 71, no. 4, pp. 225-237.

[3] A. Abdullah and B. Al-Sakkaf, "Yemen-specific cybersecurity vulnerabilities in financial institutions," J. Middle Eastern Tech., vol. 10, no. 2, pp. 78-92, 2025.

[4] Europol, "Cybersecurity trends 2025: Ransomware and beyond," Europol Annual Report, 2025.

[5] Kaspersky Labs, "Global cybersecurity outlook 2025: Human error and phishing trends," Kaspersky Annual Report, 2025.

[6] IBM, "Cost of data breach report 2025: The value of training," IBM Security Division, 2025.

[7] N. Kshetri, "Cybersecurity in developing countries: Threats to financial institutions," J. Global Inf. Tech. Manag., vol. 26, no. 4, pp. 301-320, 2023.

[8] Kaspersky Labs, "Human error and cybersecurity breaches: A global perspective," Kaspersky Tech Rep., 2025.

[9] ISO, "ISO 27001: Information security management systems – Requirements," International Organization for Standardization, 2023.

[10] BIS, "Global cybersecurity trends: The impact of threat intelligence sharing," Bank for International Settlements Report, 2024.
[11] N. Kshetri, "Cybersecurity resilience in fragile states," Int. J. Security Studies, vol. 15, no. 1, pp. 23-40, 2023.
[12] BIS, "Red team exercises and detection improvements," Bank for International Settlements Report, 2024.
[13] World Bank, "Cybersecurity in Fragile States Report," 2023. [Online]. Available: https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries
[14] Oman CDC, "National cybersecurity framework: Lessons from Oman's Cyber Defence Centre," Oman Cybersecurity Authority, 2024.
[15] IMF, "International collaboration for cybersecurity in fragile states," International Monetary Fund Policy Paper, 2025.
[16] Open Source Initiative, "Open-source tools for cybersecurity in resource-limited environments," OSI White Paper, 2024.
[17] J. Chaudhry et al., "Legacy systems and cybersecurity risks in Pakistan's financial sector," J. Emerging Markets Tech., vol. 15, no. 2, pp. 89-104, 2022.
[18] F. Mwagwabi et al., "Training gaps and cybersecurity risks in Kenyan enterprises," African J. Inf. Syst., vol. 9, no. 1, pp. 23-39, 2023.
[19] J. Smith and R. Jones, "Regulatory impacts on national security resilience," J. Security Policy, vol. 17, no. 2, pp. 78-95, 2023.
[20] Europol, "Cybercrime prevention in Sub-Saharan Africa: The role of regulatory frameworks," Europol Cybersecurity Brief, 2014.