Journal of Insights in Basic and Applied Sciences
مجلة رؤى في العلوم الأساسية والتطبيقية
Volume 2, Issue 2, 2026, Pages: 131-137
Journal homepage: https://jibas.com.ly/index.php/jibas/en

Assessing the Risks of Cyberattacks on Libyan Banks and Ways to Mitigate Them

Hiba Abdullah Ateeya [1]* ,Tahane mohamed Fagar [2]
[1]. Department of Information Technology College of Technical Sciences Derma, Derma, Libya
[2] Department of Information Technology, High Institute Of Science And Technology Awlad Ali, Tarhouna, Libya

تقييم مخاطر الهجمات الإلكترونية على البنوك الليبية وسبل التخفيف منها

هبه عبدالله عطيه [1]*، تهاني محمد فجر [2]
[1] قسم تقنية المعلومات، كلية العلوم التقنية درنة، مدينة درنة، ليبيا
[2] قسم تقنيات الحاسوب، المعهد العالي للعلوم والتكنولوجيا أولاد علي، مدينة ترهونة، ليبيا

*Corresponding author: Hebalibya2022@gmail.com

Received: March 14, 2026	Accepted: April 25, 2026	Published: May 11, 2026

Abstract:
Libyan banks are digitizing quickly (e-banking web sites, mobile applications, online foreign-currency reservation platform, etc.) in a threat environment shaped by global cyber crime, a regional state of war and asymmetric cyber maturity. The paper implements the risks of a cyberattack on the Libyan banks by synthesizing (i) Libya-specific evidence from reported incidents (e.g., DDoS disruption affecting the Central Bank of Libya's online foreign-currency reservation platform; bank web/mobile compromise reports; technical evidence of a vulnerability from a '2025 Nessus-based assessment' of Libyan bank websites) and (ii) global financially-sector threat baselines from recent large-scale datasets (Verizon DBIR 2025; ENISA Threat Landscape 2025; and ENISA Finance Sector Threat Landscape covering 2023–H1 2024). We use a structured qualitative risk approach which maps threats, attack surfaces and likely impacts to control objectives from NIST Cybersecurity Framework (CSF) 2.0 and SWIFT's Customer Security Controls Framework (CSCF), and to resilience expectations in the Basel Committee's principles for operational resilience. Findings suggest that three risk clusters dominate for Libyan banks: availability disruption (especially DDoS) threatening public-facing banking and central-bank platforms; credential-led intrusions that enable ransomware and account takeover; and exploitable web-application and configuration weaknesses affecting banking web assets. We present a prioritised mitigation roadmap guided by reduction of risk per unit of effort. Governance (CSF "GOVERN") should be the first priority, followed by identity hardening and phishing resistance, segmentation with secure remote access, continuous monitoring, tested incident response, and sector-wide resilience exercises, taking into account Libyan legislation on electronic transactions and cybercrime deterrence.

Keywords: Libya, Banking Cybersecurity, Ddos, Ransomware, NIST CSF 2.0, SWIFT CSCF, Operational Resilience, Risk Assessment**.**

الملخص
تشهد البنوك الليبية تحولاً رقمياً سريعاً (مواقع الخدمات المصرفية الإلكترونية، وتطبيقات الهاتف المحمول، ومنصة حجز العملات الأجنبية عبر الإنترنت، وغيرها) في ظل بيئة تهديدات تتشكل بفعل الجرائم الإلكترونية العالمية، وحالة الحرب

الإقليمية، وتفاوت مستوى النضج السيبراني. تتناول هذه الورقة البحثية مخاطر الهجمات الإلكترونية على البنوك الليبية من خلال تحليل (أ) الأدلة الخاصة بليبيا المستقاة من الحوادث المبلغ عنها (مثل هجوم DDoS الذي أثر على منصة حجز العملات الأجنبية عبر الإنترنت التابعة للبنك المركزي الليبي؛ وتقارير اختراق مواقع البنوك الإلكترونية وتطبيقاتها على الهواتف المحمولة؛ والأدلة التقنية على وجود ثغرة أمنية من خلال "تقييم قائم على برنامج Nessus لعام 2025" لمواقع البنوك الليبية الإلكترونية)، و(ب) خطوط الأساس العالمية للتهديدات في القطاع المالي المستقاة من مجموعات بيانات حديثة واسعة النطاق (تقرير Verizon DBIR لعام 2025؛ وتقرير ENISA Threat Landscape لعام 2025؛ وتقرير ENISA Finance Sector Threat Landscape الذي يغطي الفترة من 2023 إلى النصف الأول من عام 2024). نستخدم منهجية نوعية منظمة لتقييم المخاطر، ترسم خريطة للتهديدات، ونقاط الضعف المحتملة، وتأثيراتها المحتملة، وذلك وفقًا لأهداف الرقابة الواردة في إطار الأمن السيبراني (CSF 2.0 الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST)، وإطار ضوابط أمن العملاء (CSCF) التابع لسويفت، فضلًا عن توقعات المرونة في مبادئ لجنة بازل للمرونة التشغيلية. تشير النتائج إلى أن ثلاث مجموعات من المخاطر تهيمن على البنوك الليبية: انقطاع الخدمة (وخاصة هجمات DDoS) التي تهدد منصات الخدمات المصرفية العامة ومنصات البنوك المركزية؛ والاختراقات التي تعتمد على بيانات الاعتماد والتي تُمكّن من استخدام برامج الفدية والسيطرة على الحسابات؛ ونقاط الضعف في تطبيقات الويب وتكويناتها التي يمكن استغلالها والتي تؤثر على أصول الخدمات المصرفية على الإنترنت. نقدم خارطة طريق للتخفيف من المخاطر، مرتبة حسب الأولوية، وموجهة بتقليل المخاطر لكل وحدة جهد. يجب أن تكون الحوكمة (وفقًا لإطار الأمن السيبراني "GOVERN") هي الأولوية الأولى، تليها تحصين الهوية ومقاومة التصيد الاحتيالي، والتجزئة مع توفير وصول آمن عن بُعد، والمراقبة المستمرة، والاستجابة للحوادث *المختبرة*، وتمارين المرونة على مستوى القطاع، مع مراعاة التشريعات الليبية المتعلقة بالمعاملات الإلكترونية وردع الجرائم الإلكترونية.

الكلمات المفتاحية: ليبيا، الأمن السيبراني المصرفي، هجمات الحرمان من الخدمة الموزعة، برامج الفدية، إطار الأمن السيبراني NIST CSF 2.0، إطار الأمن السيبراني SWIFT CSCF، المرونة التشغيلية، تقييم المخاطر

1. Introduction

As stealing money directly from people through banks is possible, cybercriminals definitely target the financial sector. A substantial amount of empirical evidence indicates that “System Intrusion, Social Engineering and Basic Web Application Attacks – 74% of breaches” in Finance and Insurance while “Ransomware and Use of stolen credentials” are described as key drivers of breaches in the sector [11].

The banking ecosystem in Libya presents extra contextual risk factors:

- increased reliance on internet platforms for essential banking functions,
- varied maturity levels of security across institutions.
- increasing track record of disruptive attacks on national services.

The National Bank of Libya reported that a denial-of-service (DoS) attack that occurred on 14 January 2022 hampered users’ access to its online foreign-currency reservation platform and stated that it mitigated the event by stopping access from network addresses registered outside Libya. An independent threat-intelligence report from 2023 recorded continued and sustained reflective DDoS attacks targeting Libyan financial sector entities, including Yaqeen Bank (yaqeenbank.com), from early August to late August 2023 [8].

To start with governance, Libya has adopted Law no 5/2022 (Cybercrime) [12] and Law No. 6/2022 (Electronic Transaction) [13], which specifically targets enhancing trust and safety of electronic transaction along with penalties for system disturbances and cyber events in banking. Simultaneously, Central Bank Of Libya [2] released an information security policy that covers controls on password management, backups, incident response remote access precautions and network security monitoring.

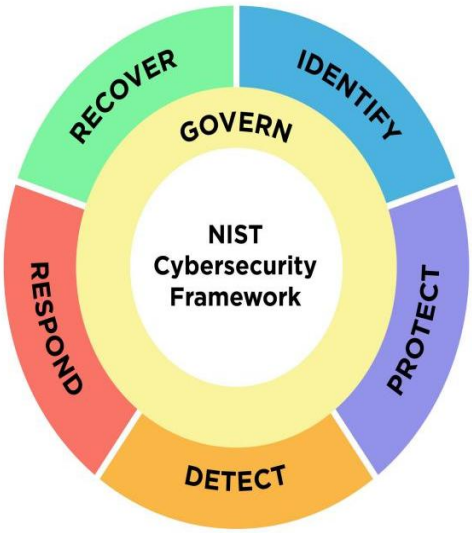

Figure 1. NIST CSF 2.0 Functions (conceptual wheel)

2. Research Methodology

2.1 Research questions

RQ1: What cyber threats and attack vectors are likely to impact operational and financial risk in banks in Libya?

RQ2:What evidence exists of exposure and realized incidents involving Libyan banking?

RQ3:Which mitigation measures will achieve the highest risk reduction in accordance with internationally accepted frameworks and the Libyan legal/regulatory context?

2.2 Study design (structured qualitative risk assessment)

We use a multi-source synthesis method designed for environments where institution-level breach datasets are not publicly available:

a) Examination of context and regulations Assessment of the nation's laws, regulations and policies on electronic banking and cybercrime. The sources of information include Libya's Law No. 5/2022 [12], Law No. 6/2022 [13] and the Central Bank of Libya information security policy [2]
b) Compiling evidence of incident. We obtain open-source reporting that highlights attacks that affect Libyan banking entities and platforms. Particularly disinformation relevant to DDoS and disruption of public-facing services which has been seen [14] [8] and the reported compromise of the web/mobile presence of a bank is occurring [15].
c) Proxy for Technical Exposure. Utilize local peer-reviewed research which did the Nessus vulnerability scanning of four Libyan banks websites (testing from September 2024), and includes counts of vulnerabilities by severity and the finding that private banks had the higher exposure than public banks in that sample [6].
d) triangulating the threat baseline Major sector-wide reports (such as Verizon DBIR 2025 [10] and ENISA threat landscapes [4] [3]) can provide a useful anchor for the likelihood assumptions and attack-pattern priors for finance.
e) Control mapping and mitigation design. Designate mitigations to efforts:
1. NIST CSF 2.0 (particularly the new GOVERN function) [7].
2. These two frameworks can be considered useful as effectual or formative proposals for establishing frameworks.
3. Principles of Basel's operational resilience that focus on capacity to withstand and recover from cyber incidents [1].
4. Good practices of financial sector cyber risk supervision in IMF

2.3 Risk scoring approach

For each of the scenarios we apply a qualitative Likelihood × Impact rating (Low/Medium/High), based on our reasoning above. This generates a priority risk register for banks and supervisors to trace later for quantitative methods (e.g., IMF work on VaR-type cyber loss scenarios) [5].

3. Analytical Results

3.1 Observed and expected threat patterns for banking (triangulated baseline)

The Verizon finance snapshot indicates that the finance sector is the top target for Denial of Service, with that pattern accounting for 35% of DoS targeting. 74% of breaches in Finance and Insurance are System Intrusion, Social Engineering, Basic Web Application Attacks [11].

- Ransomware was present in 44% of breaches reviewed in the DBIR dataset across all industries (up from 32%). It now appears that ransomware is a mainstream risk, not a fringe risk [10].
- ENISA reveals that DDoS attacks make up 76.7% of the recorded cases of DDoS, which is "overwhelmingly driven by hacktivist groups." In the EU context of the targeted incident, a hacktivist-led DDoS dominates (83.5% of incidents in its finance sectorial view); and for cybercrime incident in finance, the incident is skewed toward data breaches (64%) vs ransomware (36%) [4].
- The impact of ransomware in finance: According to ENISA's threat landscape report for the finance sector, the ransomware impact has been classified mainly as a financial loss (38%), data exposure/sale (35%), and operational disruption (20%) [3].

3.2 Libya-specific incident and exposure evidence

Interrupting services (DDoS) against crucial infrastructures. The Central Bank of Libya [2] informed of a DDoS which disrupted access to its foreign currency reservation platform, mitigated by blocking non-Libyan network addresses [14]. A threat-intelligence analysis also reported reflective DDoS attacks against Yaqeen Bank, using vulnerable services and ongoing over multiple weeks, with attacks taking place outside regular working hours [8].

- Customer-facing channels hacked. The website and mobile app of the Libyan Commerce and Development Bank reportedly hacked, forcing the bank to deactivate the app to reclaim control; the bank denied a breach of its core banking system and customer account data in that reporting [15]. Reporting of such incidents, even when partial or incomplete, reveals that reputational and customer-trust damage can occur even when the full-channel is not compromised.
- Proof of Vulnerability in Web Assets. A peer-reviewed study conducted in 2025 assessed four Libyan bank websites using Nessus (September testing in 2024) and found the number of vulnerabilities significantly higher in the two private banks than in the two public banks. Alejma'a Alarabi Bank, for instance, exhibited ten high, thirty-four medium, and one low vulnerability. Yaqeen Bank, on the other hand, demonstrated two high, eighteen medium, and three low vulnerabilities. As for the North Africa Bank, it yielded one low vulnerability, and finally, the National Commercial Bank had no vulnerabilities in that scan. This suggests heterogeneous cyber hygiene and calls for attack surface reduction for public web assets, above all.

Table 1 A cybersecurity risk assessment register tailored for the Libyan financial sector

Risk scenario	Likelihood	Impact	Evidence signals	Primary mitigations (mapped)
DDoS against central-bank or commercial-bank online platforms (availability loss)	High	High	CBL platform disruption & mitigation; reflective DDoS targeting Libyan financial entities; finance is top DoS target in DBIR snapshot	DDoS protection, upstream scrubbing, rate limiting, resilient architecture, runbooks & exercises (CSF DETECT/RESPOND/RECOVER; Basel resilience) Central Bank of Libya trendsnafrica.com NSFOCUS Global Verizon Finance Snapshot
Credential theft → account takeover / intrusion → ransomware/extortion	High	High	Finance breaches dominated by system intrusion & social engineering; ransomware widely prevalent; ENISA: phishing primary intrusion vector	Phishing-resistant MFA, privileged access management, endpoint hardening, incident containment, immutable backups (CSF PROTECT/DETECT/RESPOND) Veriz on DBIR 2025 ENISA TL 2025
Exploitation of web-application/config	Medium–High	Medium–High	Nessus findings show high/medium	Secure SDLC, patching, WAF, vulnerability management, pen testing, configuration baselines (CSF

uration weaknesses in e-banking sites			vulnerabilities in sampled Libyan banks; DBIR highlights basic web app attacks	IDENTIFY/PROTECT) Wadi Alshatti University Journal of Pure and Applied Sciences
Supply-chain compromise of critical service providers (banking IT vendors/MSPs)	Medium	High	DBIR: third-party involvement 30% of breaches; ENISA highlights cyber dependencies	Third-party risk management, contractual security outcomes, access segmentation, monitoring (CSF GOVERN + GV.SC) Verizon DBIR 2025 NIST CSF 2.0
Regulatory/legal non-compliance and evidence-handling failures	Medium	High	Libyan laws define cyber offenses, penalties, and jurisdiction; electronic transactions law sets requirements for secure processes	Governance, auditability, logging, incident reporting, forensics readiness (CSF GOVERN/RESPOND) Law Society Libya – Law 5/2022 Law Society of Libya – Law 6/2022

3.3 Consolidated risk register (Libyan bank context)

The table below summarizes the main scenarios and their qualitative risk ratings based on the evidence.

3.4 Mitigation framework synthesis (what to do, and how to prioritize)

A. Place governance with the highest priority. The CSF 2.0 adds a new GOVERN function that is responsible for establishing and monitoring the cybersecurity risk strategy, supply chain risk, roles and oversight. For banks operating in Libya, this means: board accountability, a clearly defined risk appetite for cyber outages and fraud, and enforceable policies across subsidiaries/branches and IT outsourcers.

B. The two most evidenced operational risks involve DDoS disruption and credential led intrusion. Incidents in Libya highlight disruptions to availability [8] [14]; global baselines highlight credential theft and ransomware [10] [11]. Prioritization is essential for controls.

- Availability engineering & DDoS response: upstream DDoS services, redundancy and rehearsed incident playbooks consistent with CBL own incident response, backup, continuity and network monitoring part of CBL security plan [2].
- Prevention from phishing threats and getting monitoring continuously helps the firm combat phishing attacks. These layers include using phishing-resistant multi-factor authentication and implementing strict access controls to remote systems. ENISA claim phishing is the first victim to breach [4]. Additionally, the DBIR reports focus on the finance sector and highlight stolen credentials and ransomware [11].

C. Use SWIFT CSCF wherever appropriate (payments ecosystem hardening) [7]. The CSCF, according to SWIFT, establishes a baseline for SWIFT users. The baseline includes mandatory and advisory controls and is structured around three objectives: “Secure your environment,” “Know and limit access,” and “Detect and respond.” Along with these, there are also controls that incorporate an annual attestation model.

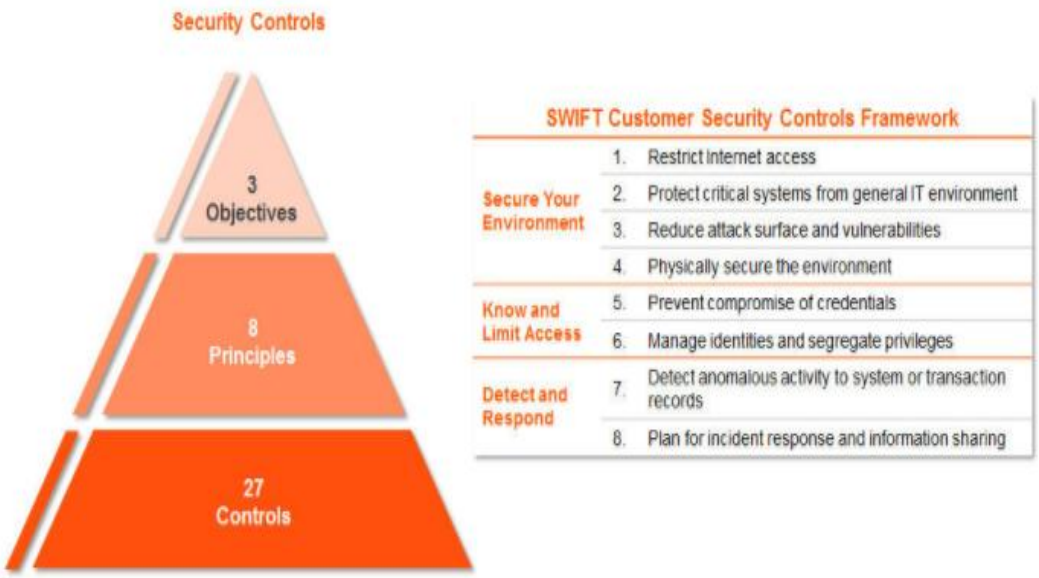

Figure 2. SWIFT CSCF overview (illustrative)

4. Conclusion

This paper assessed cyberattack risks for Libyan banks using an evidence-based synthesis grounded in (i) Libya-specific incidents and peer-reviewed vulnerability assessment of Libyan bank web assets, and (ii) global financial-sector threat intelligence and breach-pattern datasets. The findings suggest that Libyan Banks should primarily focus on strengthening the availability and DDoS resilience of their public-facing and National-level platforms, reducing the credential-driven intrusion risk which enables ransomware and fraud, and systematically remediating the web-application and configuration weaknesses demonstrated by local vulnerability research. The importance placed on governance and supply-chain risk management in NIST CSF 2.0 is also clear in the baseline approach SWIFT CSCF has taken for the payments ecosystem. Banks must be able to withstand and recover from cyber incidents and other disruptions in line with the resilience principle of Basel Committee. Some limitations are their usage of open-source incident reporting and a single published study on website scanning. Thus, these may not represent the entire Libyan Banking Sector. Future work should include (a) coordinated sector-wide measurement (phishing susceptibility, patch latency, external attack surface), (b) controlled red-team exercises, and (c) quantitative loss scenario modeling to Libyan operational realities building on the IMF's approach to financial-sector cyber risk quantification IMF Working Paper 2018.

References

[1] Basel Committee on Banking Supervision. 2021. Principles for operational resilience. Bank for International Settlements (BIS). BCBS516: 1-10.2.

[2] Central Bank of Libya. 2024. Information Security Policy. Central Bank of Libya. 1: 1-15.

[3] ENISA. 2025. ENISA Threat Landscape: Finance sector (Jan 2023–Jun 2024). European Union Agency for Cybersecurity (ENISA). 1: 1-45.

[4] ENISA. 2025. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity (ENISA). 1: 1-60.

[5] Gaidosch, T. et al. 2026. Good Practices in Cyber Risk Regulation and Supervision. International Monetary Fund (IMF). 2026(001): 1-35.

[6] Masoud, R. et al. 2025. Security Assessment of Some Libyan Banks Websites. Wadi Alshatti University Journal of Pure and Applied Sciences. 3(1): 6-10.

[7] NIST. 2024. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology (NIST). CSWP 29: 1-40.

[8] NSFOCUS Global. 2023. Turmoil in Libya: Major Industries Hit by Massive DDoS Attacks. NSFOCUS Global Threat Intelligence. 1: 1-8.

[9] SWIFT. 2024. Understand Controls (CSCF baseline, objectives, attestation). SWIFT Customer Security Programme (CSP). v2025: 1-32.

[10] Verizon. 2025. 2025 Data Breach Investigations Report. Verizon Business. 18: 1-100.

[11] Verizon. 2025. 2025 DBIR Finance Snapshot. Verizon Business. 1: 1-12.

[12] Libya House of Representatives. 2022. Law No. 5 of 2022 Regarding Combating Cybercrimes. Law Society Libya. 5: 1-25.

[13] Libya House of Representatives. 2022. Law No. 6 of 2022 Concerning Electronic Transactions. Law Society of Libya. 6: 1-30.

[14] TrendsNAfrica. 2024. Central Bank of Libya's Online Platform Hacked. TrendsNAfrica. 1: 1-2.

[15] LibyaReview. 2024. Central Bank of Libya: Cyberattack has targeted foreign currency online platform. LibyaReview. 1: 1-2.