International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 5, Sep-Oct 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cybersecurity in Banking

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

The banking sector confronts a diverse and rapidly changing threat environment. It is attractive to attackers because banks hold money, sensitive personal information, payment credentials, and commercially valuable data. A successful attack can cause several forms of damage at once, including stolen funds, operational downtime, regulatory penalties, remediation expenses, litigation, reputational harm, and declining customer confidence. Cybersecurity in banking refers to the technologies, processes, and practices used to protect financial systems, networks, and data from cyber-attacks. Cybersecurity must be treated as a continuous risk-management cycle rather than a collection of isolated tools. Banks apply this model by establishing board and executive accountability, maintaining inventories of critical systems and data, deploying preventive safeguards, monitoring for abnormal behavior, containing incidents, and restoring essential services. This paper examines the role of cybersecurity in the banking industry.

KEYWORDS: *technology, security, cybersecurity, banking, banks, banker, banking industry.*

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Cybersecurity in Banking" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-5, October 2026, pp.131-142, URL: www.ijtsrd.com/papers/ijtsrd142110.pdf

IJTSRD142110

Copyright © 2026 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

INTRODUCTION

Banking has become inseparable from digital technology. Customers expect instant payments, mobile access, automated decisions, and uninterrupted service, while banks depend on interconnected networks, cloud platforms, data analytics, and external technology providers. These innovations improve convenience and efficiency, but they also enlarge the area that criminals, hostile states, insiders, and opportunistic attackers can target. Cybersecurity in banking is therefore not merely an information-technology concern. It is a strategic requirement for protecting customers, sustaining essential services, preserving confidence, and supporting the stability of the financial system [1].

OVERVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 1, cybersecurity involves multiple issues related to people, process, and technology [2]. Figure 2 shows different components of cybersecurity [3].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cybercriminals or ethical hackers are modern-day digital warriors, possessing extraordinary skills and knowledge to breach even the most impregnable systems. A typical cybercriminal is shown on Figure 3 [5]. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [5].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [6].

These are known as the pillars of information assurance.

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Good practices for cybersecurity in construction companies should include all of these elements.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [7]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks or threats are shown in Figure 4 [8]. Sources of cyber threats are displayed in Figure 5 [9].

The social and financial importance of cybersecurity is increasingly being recognized by businesses, organizations, and governments. Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [10]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

CYBERSECURITY IN BANKING

Banking depends on trust. Customers expect deposits to remain accurate, payments to reach the intended recipient, personal information to stay confidential, and essential services to remain available at all times. As banking has moved from branch-centered operations to mobile applications, online platforms, cloud infrastructure, automated payment networks, and open application programming interfaces, that trust has become inseparable from cybersecurity. Cybersecurity in banking refers to the practices, technologies, and systems used to protect financial institutions from cyber threats. It is not merely an information-technology function. It is a strategic

system of governance, technology, processes, and human controls used to prevent fraud, protect data, preserve the integrity of transactions, and keep critical financial. Cybersecurity is crucial because banks handle highly sensitive financial and personal data [11]. Figure 6 shows the importance of cybersecurity in banking [12].

Banks confront a diverse and rapidly changing threat environment. Phishing and social engineering can bypass sophisticated controls by deceiving employees or customers. Ransomware may encrypt systems, steal information, and threaten public disclosure. Malware and account-takeover schemes can compromise online banking, while distributed denial-of-service attacks can make customer-facing services unavailable. Cyber risk is unusually serious in banking because institutions do not operate in isolation. They are connected through payment networks, clearing systems, shared software, interbank markets, and common service providers. Banking cybersecurity must therefore protect the confidentiality, integrity, and availability of systems and information [1].

Because a severe banking incident can affect the public, cybersecurity cannot be left entirely to individual firms. Banks need security operations that can detect abnormal behavior quickly, incident-response teams with clear authority, and reliable procedures for containing compromised systems. Cybersecurity succeeds only when responsibility extends beyond the security department. Figure 7 provides some reasons banks need cybersecurity [13].

APPLICATIONS OF CYBERSECURITY IN BANKING

Cybersecurity in banking has become more critical than ever as financial institutions continue to face an increasing number of cyber threats. Cybersecurity applications in banking must consequently address both the safety of a single customer account and the resilience of the financial system. The application of cybersecurity in banking is thus both broad and integrated. Figure 8 shows how to address cyberthreats [14]. Common applications of cybersecurity in banking include the following [1,15,16]:

- *Security*: The most important application of cybersecurity in the banking sector is to secure the money of customers. If the banks do not have robust cybersecurity infrastructure, then they might suffer enormous data breaches and cyber-attacks. These days, the government is giving special emphasis to ongoing digitalization. This means an increase in the proportion of the population that uses digital money, such as plastic cards and going cashless. Therefore, it has become important to deploy precautionary measures to ensure cybersecurity to protect your data and maintain privacy. When a bank suffers from a cyber-attack, not only the bank but also its customers suffer financial losses. Recovering from this loss can be costly and time-consuming. Not only does cybersecurity affect customers, but it also has a direct impact on the bank's bottom line.
- *Cybersecurity Breach*: A cybersecurity breach in banking occurs when unauthorized individuals gain access to systems, networks, or data belonging to a financial institution. These breaches can involve customer information, transaction data, credentials, or internal systems. In the context of cybersecurity breaches in banking, the consequences are often more severe due to regulatory requirements and financial exposure. Even a small breach can have industry-wide consequences. Cybersecurity breaches in banking are increasing in frequency, complexity, and impact, putting customer trust, financial stability, and regulatory compliance at risk. Figure 9 shows cybersecurity breaches in banking [17].
- *Access Management*: One of the most visible applications is identity and access management. Banks must confirm that customers are entitled to use an account, employees are authorized to perform assigned tasks, administrators receive only necessary privileges, and external providers access only approved systems. Passwords alone are often insufficient because they can be stolen through phishing, malware, credential stuffing, or social engineering. Where risk assessments show that existing measures are insufficient—especially for high-risk users or transactions—banks should use multifactor authentication or controls of equivalent strength within a layered security program.
- *Data Protection*: Another major application is data protection. Banks store information whose exposure could enable identity theft, financial fraud, and surveillance of a customer's personal or commercial activity. Strong key management is essential because encryption is only as reliable as the controls governing the creation, storage, rotation, and revocation of keys. Data classification and data-loss-prevention systems add another layer by identifying sensitive records and restricting unauthorized copying, emailing, printing, or uploading.

- *Payment Cards:* Cybersecurity also protects payment cards and transaction environments. The Payment Card Industry Data Security Standard provides baseline technical and operational requirements for organizations that store, process, or transmit cardholder or sensitive authentication data. For banks, such controls help secure card-processing networks, terminals, applications, and databases. They are complemented by anti-skimming technologies, transaction limits, chip-based authentication, tokenized mobile payments, and continuous monitoring.
- *Banking Infrastructure*: Another important application is the protection of digital banking infrastructure and software. The banking sector's infrastructure, including online banking platforms, ATMs, and payment processing systems, is a primary target for cybercriminals. A successful attack on these systems could lead to operational disruptions, making customers unable to access their funds or conduct transactions. Cyber security helps banks protect this critical infrastructure by preventing unauthorized access, detecting anomalies, and mitigating potential threats. Security requirements should be defined before an application is built; code and third-party components should be tested; secrets should not be embedded in software; and updates should be monitored after release.
- *Fraud Detection*: Banks apply cybersecurity directly to fraud detection and transaction monitoring. Traditional rules can flag conditions such as an unusually large transfer or repeated failed logins, while modern systems apply machine learning to large volumes of historical and real-time data. These models can compare a transaction with a customer's normal location, device, timing, amount, and spending behavior. When activity appears suspicious, the system may block the transaction, request additional authentication, or send the case to a human investigator.
- *Zero Trust Model*: The Zero Trust model assumes that all users, devices, and networks are inherently untrustworthy, implying that no user or system should be trusted by default, even within the organization. Every access request is verified continuously based on identity, behavior, and context. This reduces the risk of unauthorized access and limits the impact of potential breaches. Banks can prevent unauthorized access and data breaches by requiring verification at every stage. To implement such a model effectively, having a strong network security architecture is crucial, ensuring that every access point and connection within the system is secure.
- *Business Continuity*: Cyber attacks can cause significant disruptions to a bank's operations, leading to system outages, lost data, and even a halt in services. These interruptions can be costly in terms of financial losses and the negative impact on customer experience. Implementing comprehensive cybersecurity measures helps banks safeguard against such disruptions. Having a solid incident response plan, performing regular backups, and utilizing disaster recovery solutions ensure that banks can quickly recover from an attack and continue providing uninterrupted customer services.

BENEFITS

Cybersecurity provides banks with benefits that are both defensive and enabling. It protects customer data, reduces fraud, supports continuous service, preserves trust, strengthens compliance, controls costs, and makes digital innovation safer. Other benefits of cybersecurity in banking include the following [1]:

- *Costs:* Cybersecurity can also reduce long-term costs. Preventive controls require investment in skilled staff, secure infrastructure, training, testing, and monitoring. However, weak security can lead to fraud losses, system repairs, legal expenses, customer compensation, operational downtime, regulatory penalties, and reputational damage. Prevention is especially valuable because a single cyber incident may affect several parts of a bank at once. Risk assessments allow management to focus spending on the systems and services that would cause the greatest harm if compromised. In this way, cybersecurity supports more efficient use of resources and reduces the financial uncertainty associated with digital threats. Smaller institutions may struggle with cost and expertise, but their role in shared networks makes their readiness a collective concern.
- *Customer Confidence*: Strong cybersecurity also preserves customer confidence and the reputation of the bank. Financial relationships are highly sensitive because customers must believe that the institution is competent, dependable, and careful with their money. A serious data breach or prolonged service outage can weaken this confidence, even when customers are later reimbursed. Trust encourages customers to continue using digital services and supports long-term relationships between the bank, households, and businesses.

- *Protection of Confidential Information*: One of the most important benefits of cybersecurity is the protection of confidential information. Banks hold large quantities of sensitive data, including names, addresses, identification records, account details, transaction histories, passwords, and credit information. If criminals obtain such data, they may use it to steal money, commit identity fraud, or target customers with further scams. Security controls such as encryption, multifactor authentication, access restrictions, network monitoring, and secure software development reduce the likelihood that unauthorized individuals will obtain or alter this information. These safeguards support the confidentiality and integrity of customer.
- *Fraud Prevention*: Cybersecurity also helps prevent financial fraud and limit direct monetary losses. Modern banking transactions often occur instantly and remotely, which means that criminals can attempt account takeovers, payment fraud, phishing, malware attacks, and unauthorized transfers without entering a physical branch. Effective cybersecurity combines technology with strong procedures and employee awareness. Authentication systems can make stolen passwords less useful, behavioral monitoring can identify unusual activity, and rapid incident response can stop suspicious transactions before losses grow. Although no security program can eliminate every threat, layered controls make successful attacks more difficult and improve a bank's ability to detect and contain them.
- *Resilience*: Another major benefit is operational resilience, meaning the ability to continue delivering essential services during and after a disruption. Regulatory bodies have made this crystal clear by putting operational resilience at the top of their supervisory priorities. Customers depend on banks for everyday activities such as receiving salaries, paying bills, purchasing goods, accessing cash, and transferring money. Cybersecurity in banking also has a crucial operational resilience application. No institution can guarantee that every intrusion will be prevented. Cyber resilience is not simply the ability to restore servers. It is the ability to preserve confidence that balances, payments, identities, and records remain reliable. As attack speed increases and digital dependencies deepen, the decisive question will be whether a compromised component can disrupt the bank's most important services. The ultimate objective is not the unrealistic elimination of all cyber risk, but the creation of a banking system that can anticipate attacks, limit their spread, maintain critical services, recover quickly, and preserve public trust.
- *Regulatory Compliance*: A further advantage is improved regulatory compliance and governance. Banks must adhere to strict data protection and cybersecurity compliance standards in the financial industry is heavily regulated. Banks operate under rules intended to protect customer information, promote safe and sound operations, and ensure that serious incidents are reported promptly. Laws such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the US set strict guidelines for how banks must handle and protect customer data. A mature cybersecurity program helps a bank document its risks, assign responsibility, test controls, supervise third-party providers, and respond to incidents in an organized manner. Banking is heavily regulated, but compliance does not guarantee security. Regulatory compliance complexity hit new heights as regulatory bodies, including the Federal Deposit Insurance Corporation, implement stricter requirements.

Figure 10 shows some benefits of cybersecurity in banking [18].

CHALLENGES

The cybersecurity challenges facing banks arise from the interaction of technological complexity, intelligent adversaries, human fallibility, third-party dependence, regulatory pressure, and the systemic importance of financial services. Other challenges of cybersecurity in banking include the following [1,15,19]:

- *Financial Loss*: A successful cyber attack can lead to significant financial loss for banks. This may include funds being stolen directly from accounts, costs related to system downtime, or the hefty price of repairing damaged systems. Moreover, banks may be held liable for compensating customers affected by fraud or identity theft due to a cyber breach. Banks can minimize the financial risks associated with cybercrime by investing in advanced cybersecurity solutions. Proactive defense mechanisms such as real-time threat monitoring, multi-factor authentication, and AI-driven threat detection can prevent attacks before they lead to costly consequences.

- *Cooperation*: Cooperation is important because attackers reuse methods across institutions and national borders. Timely sharing of indicators, vulnerabilities, and defensive lessons can allow other banks to act before they are harmed. Joint simulations can expose gaps in communication, legal authority, liquidity arrangements, and recovery dependencies that an institution-level test might miss. Regulation should nevertheless remain risk-based rather than becoming a checklist. Compliance documents do not by themselves create resilience; institutions must continually test whether controls work under realistic conditions and revise them as technologies and threats change.
- *Trust:* Banking has always depended on public trust. Customer trust will be the ultimate measure of success. Customers deposit money, share personal information, transfer funds, and use financial products with the expectation that their assets and data will remain secure. In the digital age, that trust depends heavily on cybersecurity. Mobile applications, online banking platforms, payment networks, cloud services, automated teller machines, and links with third-party providers have made financial services faster and more convenient, but they have also created new opportunities for fraud, data theft, and operational disruption. Cybersecurity is therefore not merely a technical function within a bank; it is a foundation for customer protection, reliable service, regulatory compliance, innovation, and financial stability.
- *Speed:* One of the greatest challenges is the speed at which cyber threats evolve. Banks confront phishing, business-email compromise, credential theft, malware, ransomware, distributed denial-of-service attacks, account takeover, payment fraud, and attacks on software suppliers. Criminal groups can combine several methods: a fraudulent message may capture an employee's password, stolen credentials may provide initial access, and malware may then move through internal systems before data are encrypted or stolen.
- *Legacy Systems:* Many banks operate core systems that were developed decades ago and have been modified repeatedly. These systems may remain dependable for high-volume transaction processing, yet they can be difficult to patch, document, or integrate with modern security tools. Specialist knowledge may be scarce, and replacing a core platform can involve enormous expense and operational risk. Consequently, banks often place newer digital interfaces around older infrastructure, creating additional layers of software and complex dependencies that are difficult to map and secure.
- *Skills Gap*: Skills will also become more important as systems grow more automated. Banks will need professionals who understand cloud architecture, software supply chains, AI security, identity engineering, cryptography, resilience testing, and financial operations. At the same time, secure-by-design development must make protection an ordinary feature of products rather than a late-stage audit. This is particularly important for smaller institutions. Shared services, sector utilities, common testing resources, and supervisory support can help prevent a widening security divide between large banks and smaller institutions.
- *Human Factor Vulnerabilities*: Another cybersecurity challenge faced by banks is the constant evolution of threats and vulnerabilities. Hackers are constantly updating their techniques to get around new security measures. Social engineering attacks and phishing attacks succeed because they exploit human psychology rather than technical weaknesses. Insider threats remain a major threat to banking sector security, with employees potentially misusing access to critical data and sensitive financial data. Modern cybercriminals use deepfake technology creating convincing impersonations of executives, customers, and vendors. Identity theft schemes use synthetic identities and stolen credentials to bypass Know Your Customer screening, enabling financial fraud attempts. These attacks often target sensitive information stored in sensitive systems. Cybercriminals are turning artificial intelligence into their personal weapon, creating attacks we have never seen before.

Figure 11 shows some challenges related to cybersecurity in banking [16].

FUTURE OF CYBERSECURITY IN BANKING

Future banks will adopt a zero-trust approach in which access is limited, continuously evaluated, and tied to the sensitivity of the action. The future of cybersecurity in banking will not be defined simply by stronger firewalls or larger security budgets. It will be defined by adaptive resilience—the capacity to anticipate attacks, limit their reach, maintain critical services during disruption, and recover without allowing a technical incident to become a crisis of confidence. Artificial intelligence will be the most visible force transforming bank cybersecurity because it strengthens both attackers and defenders. Banks will answer with AI-enabled defense. Security

systems will increasingly correlate identity, device, network, transaction, and behavioral signals in real time. Yet automation will not eliminate human judgment [1].

Future banks must design controls that are both strong and usable, explain high-risk interventions clearly, provide secure recovery routes, and communicate honestly after incidents. The future of cybersecurity in banking will be an arms race, but it need not be a race that banks inevitably lose. Artificial intelligence will accelerate attacks, yet it can also give defenders machine-speed awareness. Technology alone will not determine the outcome. Banks need governance that makes cyber risk visible in strategic decisions rather than confining it to an information-security department. Boards must understand critical services, risk appetite, concentration exposures, recovery tolerances, and the trade-offs created by rapid digital innovation.

The future of cybersecurity in banking will be shaped by the evolution of advanced technologies and increasingly stringent regulatory frameworks. As cyberattacks become more sophisticated, banks will turn to innovations such as AI-driven security systems, blockchain, and quantum computing to enhance their defenses. In addition to technological advancements, regulatory pressure on banks to maintain high levels of cybersecurity will increase [13].

CONCLUSION

Cybersecurity in banking refers to technologies, practices, and processes designed to protect banks' digital systems, data, and networks from cybersecurity threats. It is fundamental to modern banking because the industry's central asset is trust. Customers must believe that their money and information are secure, transactions are accurate, and essential services will remain available during disruption. Achieving that confidence requires more than firewalls or antivirus software. Banks need layered technical defenses, accountable leadership, informed employees and customers, disciplined third-party management, rapid incident response, tested recovery capabilities, and close cooperation with regulators and peers. Cyberattacks cannot be eliminated, but their likelihood and consequences can be reduced. As banking becomes more connected and technology-dependent, cybersecurity must remain a continuing process of identifying threats, improving controls, testing recovery plans, and educating people.

Cybersecurity in banking is no longer a defensive option; it is a strategic necessity. Cybersecurity is not just a technical requirement for banks, it is a core part of their operations, reputation, and customer relationships. With the rise of digital banking and increasingly sophisticated cyber threats, financial institutions must invest in strong security frameworks to protect their systems and customers. Ultimately, maintaining robust cybersecurity not only prevents financial losses but also builds trust, ensures compliance, and supports long term growth in the digital era. More information about cybersecurity in banking can be found in the books in [20,21].

REFERENCES

[1] https://manus.im

[2] P. Singh, "A layered approach to cybersecurity: People, processes, and technology- explored & explained," July 2021, https://www.linkedin.com/pulse/layered-approach-cybersecurity-people-processes-singh-casp-cisc-ces

[3] M. Loi et al., "Cybersecurity in health – disentangling value tensions," *Journal of Information, Communication and Ethics in Society,* June 2019, https://www.emerald.com/insight/content/doi/10.1108/JICES-12-2018-0095/full/html

[4] M. Adams, "Unlocking the benefits of ethical hacking: The importance of ethical hackers in cybersecurity," April 2023, https://www.businesstechweekly.com/cybersecurity/network-security/ethical-hacking/

[5] M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[6] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.

[7] "FCC Small Biz Cyber Planning Guide," https://transition.fcc.gov/cyber/cyberplanner.pdf

[8] "The 8 most common cybersecurity attacks to be aware of," https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/

[9] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports,* vol. 7, November 2021,

https://www.sciencedirect.com/science/article/pii/S2352484721007289

[10] Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation,* University of Toledo, 2015.

[11] "Cybersecurity in banking: Importance, threats, challenges," April 2026, https://www.knowledgehut.com/blog/security/cyber-security-in-banking

[12] "Cybersecurity in banking industry: Importance, challenges, and use-cases," January 2022, https://www.europeanbusinessreview.com/cybersecurity-in-banking-industry-importance-challenges-and-use-cases/

[13] C. Sahoo, "Cybersecurity in banking sector: Importance, threats, challenges," June 2026, https://qualysec.com/cybersecurity-in-banking-sector/

[14] J. Convocar, "The role of board software in mitigating cyber threats in Kenyan banking," June 2026, https://www.azeusconvene.com/articles/board-software-role-kenyan-banking-cybersecurity

[15] C. D. Luna, "Cybersecurity in banking: Threats, solutions & best practices," September 2024, https://www.esecurityplanet.com/cloud/cyber-security-in-banking/

[16] "Cybersecurity guide for banking and financial institutions," May 2022, https://threatcop.com/blog/cybersecurity-in-banking/

[17] "Cybersecurity breaches in banking: Causes, consequences, and how to prevent them," January 2026, https://www.openedr.com/blog/cybersecurity-breaches-in-banking/

[18] https://tnnbwo.gagerbogmes.com/click.php?CAMPAIGN_ID=1472814&COST_CPC=0.180000&PLACEMENT_ID=29899096&PUBLISHER_ID=3183336&SUB_ID_SHORT=6ebc5556ec4b6d854a30002bbbff630d&ZONE_ID=5655230&_fd=cragratring.com&_pd=cragratring.com&key=d7ssokt92fb001ve6jig&landing_id=42&type=Post-Proxy

[19] S. Sharma, "Cybersecurity in banking: Challenges and how to overcome them in 2026," October 2025, https://fidelissecurity.com/threatgeek/threat-detection-response/cybersecurity-in-banking/

[20] M. N. O. Sadiku, *Cybersecurity and Its Applications*. Moldova, Europe: Lambert Academic Publishing, 2023.

[21] A. Rajput, *AI Fraud Defense Systems: Digital Banking Fraud | Machine Learning Finance | AI-Powered Fraud Systems | Cybersecurity In Banking | Predictive Analytics Finance | Fraud Detection Algorithms*. Independently published, 2026.

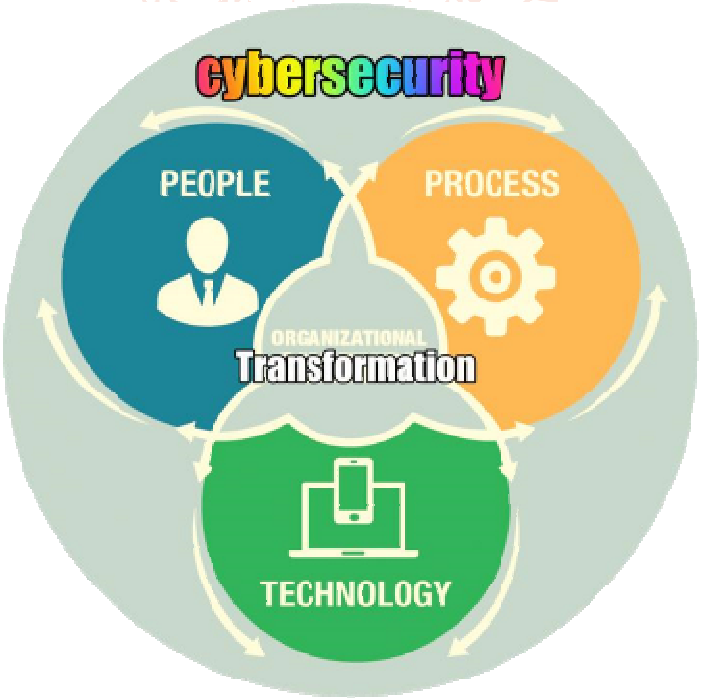


Figure 1 Cybersecurity involves multiple issues related to people, process, and technology [2].

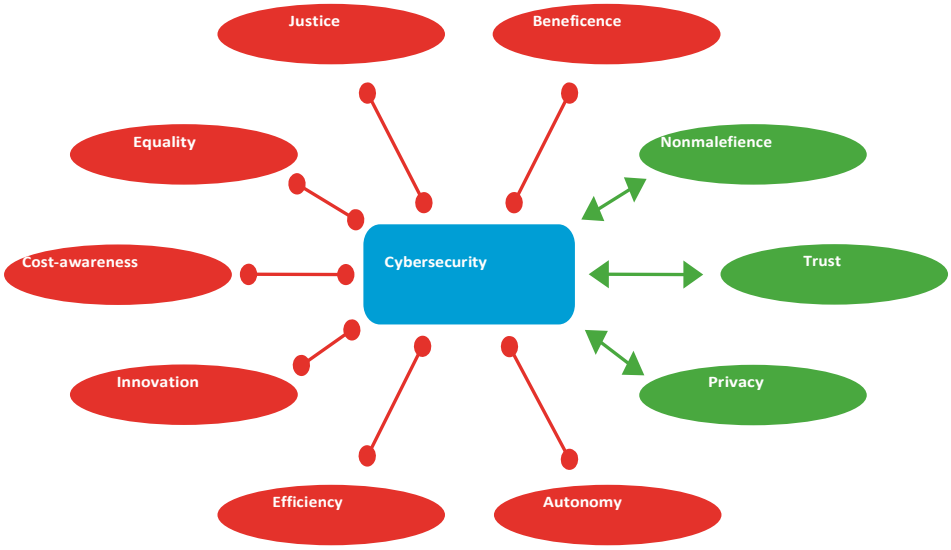


Figure 2 Different components of cybersecurity [3].(Green: supportive; red: in tension)



Figure 3 A typical cybercriminal [4].



Figure 4 Common types of cybersecurity threats [8].

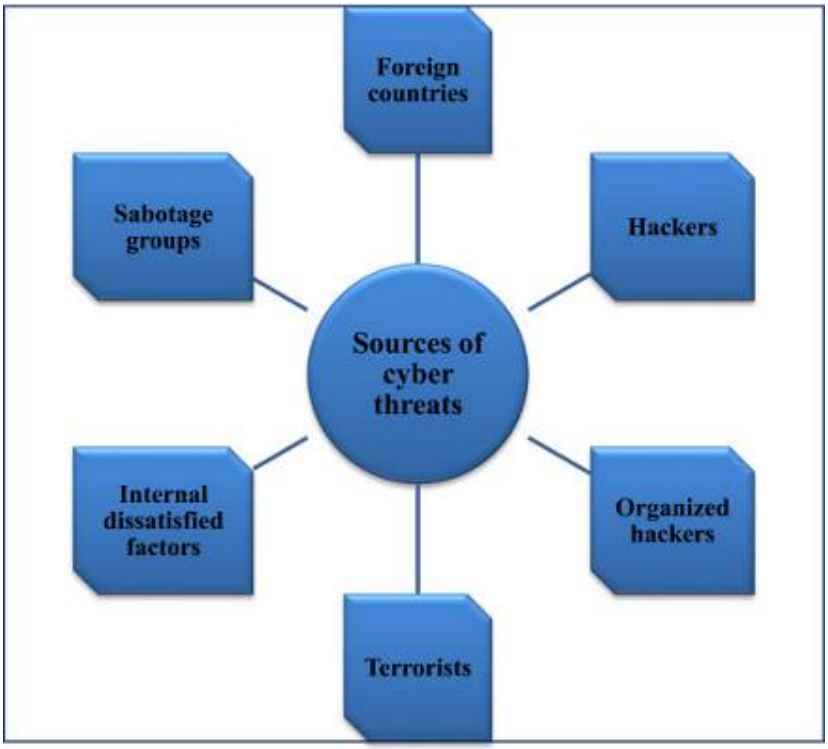


Figure 5 Sources of cyber threats [9].

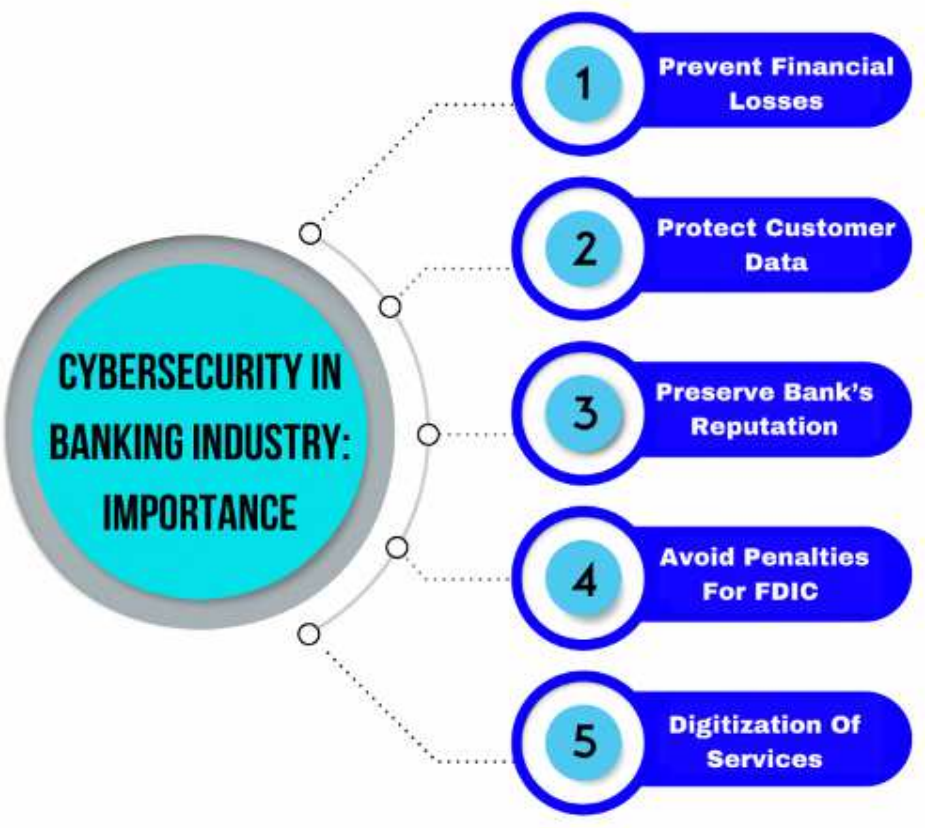


Figure 6 The importance of cybersecurity in banking [12].



Figure 7 Some reasons banks need cybersecurity [13].



Figure 8 How to address cyberthreats [14].



Figure 9 Cybersecurity breaches in banking [17].



Figure 10 Some benefits of cybersecurity in banking [18].

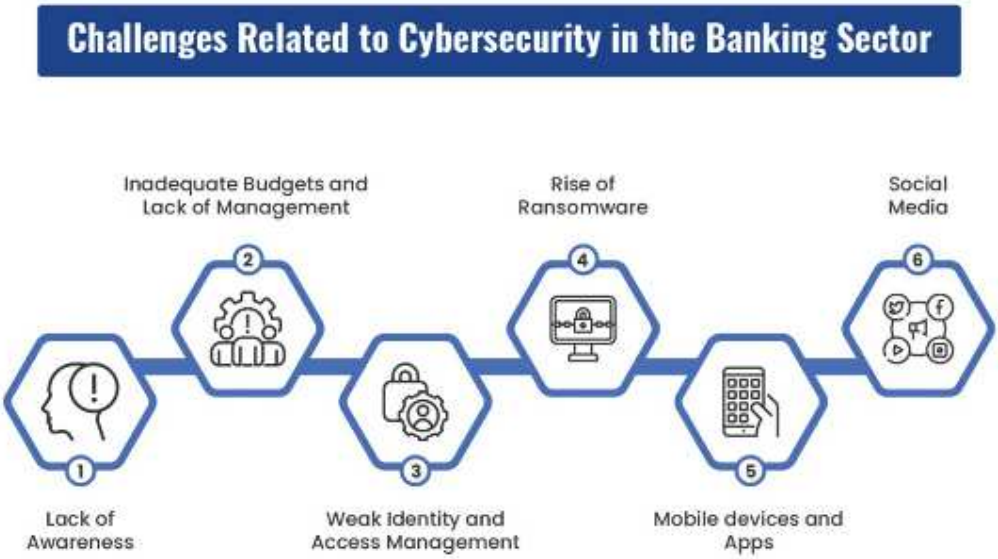


Figure 11 Some challenges related to cybersecurity in banking [16].