ADGM Academy Research Centre

2024 CYBER THREAT REPORT

CYBER THREAT REPORT

The UAE Financial Sector Cyber Threat Landscape

An RA-ADGMA Research Centre Report

IN ASSOCIATION WITH

Rabdan Academy & ADGM Academy Research Centre

AUTHORED BY

Dr. Mathew Nicho
Associate Professor – Associate Researcher,
Research & Innovation Centre, Rabdan Academy

FULL PAPER

أكاديمية ربدان
Rabdan Academy

FOREWORD

Rabdan Academy (RA) is a government-owned world-class education institution established to coordinate and enhance learning outcomes for organisations and individuals in the Safety, Security, Defence, Emergency Preparedness and Crisis Management (SSDEC) Sectors. The Academy is the first higher education institution in the world specialised in the SSDEC domain that achieves top '5 star' ratings in the 2 categories of Teaching and Employability under the QS Stars University Rating System.

ADGM Academy is part of Abu Dhabi Global Market (ADGM), an International Financial Centre (IFC) located in the capital city of the United Arab Emirates. The Academy was established with the vision of becoming one of the leading academies in the region, providing world-class financial research and training services. The ADGM Academy Research Centre brings together an ecosystem of academics, financial industry practitioners, government and technology experts to unlock the shared potential to improve the financial environment in the UAE, MENA and globally.

The report is a joint undertaking by the Research and Innovation Centre of Rabdan Academy in association with ADGM Academy Research Centre and assisted by UQ Cyber at the University of Queensland. This report is the culmination of extensive research and interviews conducted with 18 IT security senior managers representing 12 institutions within the UAE financial sector including multinational financial corporations operating in UAE. Their insights, expertise, and candid perspectives have been invaluable in shaping our understanding of the cyber threats confronting the industry today.

We would like to express our appreciation to all those who have supported and contributed to the completion of this report. It is our hope that the findings presented herein will serve as a catalyst for continued dialogue, collaboration, and action towards strengthening cybersecurity resilience in the UAE and global financial sector.

ACKNOWLEDGEMENTS

This Technical Report was prepared by Dr. Mathew Nicho (RA), in collaboration with Peter Ware and Rauda Aldhaheri (ADGMA Research Centre). Peter Ware and Rauda Aldhaheri played instrumental roles in networking and assisting the author in reaching and obtaining responses from the respondents. The author wishes to acknowledge the guidance and support from Prof. Ryan Ko of UQ Cyber, University of Queensland (UQ) and Dr. Heemeng Ho of the Singapore Institute of Technology (SIT), Singapore, who have provided the direction and constructive comments towards the successful completion of this Technical Report.

The author expresses extreme appreciation and gratitude primarily to the respondents who dedicated their time away from their critical organizational responsibilities to provide valuable feedback on the project. If you would like to provide any additional information, please contact Mathew Nicho at mnicho@ra.ac.ae or Peter Ware at peter.ware@adgm.com or Ms. Rauda Aldhaheri at rauda.aldhaheri@adgm.com. Please contact mnicho@ra.ac.ae for any clarification/in depth analysis of specific topics related to threats, attacks, vulnerabilities mentioned in the report as reported by the respondents.

TECHNICAL TEAM:

1. **Dr. Mathew Nicho,** *Associate Professor – Associate Researcher, Research and Innovation, Rabdan Academy, Abu Dhabi, UAE*
2. **Peter Ware,** *Head of Research & Development, ADGMA Research Centre, ADGM Square, Al Maryah Island, PO Box 111999, Abu Dhabi, UAE*
3. **Rauda Al Dhaheri,** *Manager - Research & Development, ADGMA Research Centre, ADGM Square, Al Maryah Island, PO Box 111999, Abu Dhabi, UAE*
4. **Prof. Ryan Ko,** *Chair and Director of UQ Cyber Security, School of Electrical Engineering and Computer Science, Faculty of Engineering, Architecture and Information Technology, University of Queensland, Brisbane, Australia*
5. **Dr. Heemeng Ho,** *Adjunct Senior Lecturer, School of Electrical Engineering and Computer Science, University of Queensland, Brisbane, Australia; Senior Lecturer, ICT Custer, Singapore Institute of Technology, Singapore*

1. SUMMARY

Cyber-attacks on financial institutions present a critical threat due to the loss of financial assets, disruptions in financial markets, and global transactions, which can impact the country's economic scenario. The report presents the perspectives gleaned from senior-level IT personnel from the financial sector in the UAE, representing national, regional, and global financial institutions. While the survey conducted during Q2, Q3 and Q4 of 2023 primarily focuses on the UAE financial sector, respondents have indicated that the views presented may have global applicability and relevance. All information presented in the report represents views provided by the respondents concerning the threat landscape affecting the financial sector as a whole, without specific reference to their respective organizations.

According to respondents, seven types of cyberattacks are very common in this sector due to the nature of assets handled, the financial attractiveness of the sector, the impact of the threat to the economy, and the geopolitical stature of the region perpetrated by non-state and state sponsored actors. Significant attacks mentioned are ransomware and phishing/spear-phishing attacks leading to Advanced Persistent Threats followed by DDoS attacks, AI-facilitated manipulations, device deception attacks, operational attacks, and attacks on the information supply chain.

The report also highlights multiple vulnerabilities (classified into technical, socio-technical, and socio categories) leading to each of these attacks, which can assist IT policymakers in focusing on, prioritizing, and making decisions to counter the threats and attempted attacks. Most vulnerabilities overlap with associated threats, which can aid IT policymakers in prioritizing common vulnerabilities and thus implement measures to address and consolidate them, thereby tackling multiple threats simultaneously.

Technical vulnerabilities encompass weaknesses in infrastructure and system architecture, exemplified by spear phishing, DDoS attacks, and device deception attacks. Examples of socio-technical vulnerabilities include social engineering attempts, insufficient vendor management, and lack of security awareness underscoring the intricate interplay between technical and human factors. These vulnerabilities underscore the importance of adopting comprehensive cybersecurity strategies that leverage both technological and human vulnerabilities. Social engineering flaws, like those observed in spear phishing, voice cloning, and ransomware, typically exploit human interactions and behaviours within the financial industry.

CONTENTS

2. INTRODUCTION

Technological advancements in cybersecurity, utilizing Artificial Intelligence Artificial Intelligence (AI) and Machine Learning (ML) have emerged as playing a pivotal role in the cybersecurity landscape, facilitating accelerated anomaly detection and streamlining responses to recurring threats encountered in organisations' day-to-day operations; this dynamic duo enables swift decision-making processes and mitigating the risk associated with commonplace and repetitive bolstering their capability to prevent, detect, mitigate, and/or evade threats and attacks. Nevertheless, these very technological strides have also been extensively exploited by malicious cyber hackers to advance cyberattacks. Since, financial institutions play a crucial role in any economy through the allocation of capital, ensuring money supply, offering loans, facilitating savings and deposits, and overseeing payments and settlements, the security of assets in the financial sector assumes critical relevance.

The COVID-19 pandemic and the subsequent increased adoption of online IT initiatives in the financial services industry have heightened the sector's vulnerabilities, making it an attractive target for threat actors with financial and non-financial motivations worldwide. With 1828 cyber incidents targeted at the financial sector[1] globally in 2022, the anticipated cost of cybercrime, expected to reach $8.4 trillion in 2022[2] and transcend $11 trillion in 2023[3], underscores the urgent need for robust as well as a resilient cybersecurity to protect critical assets and ensure financial stability. While the 50 top banks in the Middle East and North Africa (MENA) region had an aggregate market value of $548.1 billion as of February 28, 2023, the Gulf Cooperation Council (GCC) banks dominated with 41 entries, with Saudi Arabia and the U.A.E. being the most represented countries, each with 10 entries[4].

Hackers target countries in the GCC region namely the UAE, Saudi Arabia, and Kuwait[5] primarily due to their high internet penetration rates and the region's high standard of living. In this respect, the UAE saw 16,667 victims of cybercrime in 2021 alone, resulting in $746 million loss[6].

1 https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/#statisticContainer
2 ahttps://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
3 bhttps://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
4 https://www.forbesmiddleeast.com/lists/50-most-valuable-banks-2023/
5 https://www.ptsecurity.com/ww-en/analytics/middle-east-cybersecurity-threatscape-2022-2023/#:~:text=According%20to%20the%20 Group%2DIB,%2C%20and%20Kuwait%20(21%25).
6 https://www.thenationalnews.com/business/technology/2021/08/13/uae-victims-of-cybercrime-lose-746m-a-year/

The continuous improvement of UAE cyber resilience is critical to strengthen its cyber infrastructure. A survey[7] conducted in the UAE found that 77% of respondents recognized the severe risk posed by thieves and hackers to their data. Furthermore, the MENA region, which includes the UAE, is expected to witness a 12.1% increase in end-user expenditure on security and risk management by 2024, reaching $3.3 billion[8], aligning with worldwide trends. This increase is attributed to the rapid development of Generative Artificial Intelligence (GenAI), which expands the scope of threats and compels businesses to fortify their security protocols[9]. Hence, the need for financial institutions to continuously scan for threats, prioritize critical cybersecurity trends, and implement organizational security culture to effectively counter emerging threats. The UAE's National Cybersecurity Strategy[10], which attempts to provide a safe digital environment supportive of achieving residents' goals and enabling businesses to prosper, reflects this necessity.

The estimated end-user spending on security and risk management in the MENA region for the years 2023–2024 is depicted in Figure 1, with statistics expressed in millions of US dollars for each segment. Among all segments, spending on data privacy is expected to grow at the fastest rate in 2024, with a projected 24% annual increase. Additionally, cloud security spending is predicted to expand at the second-highest rate in 2024, with a 17.4% increase.

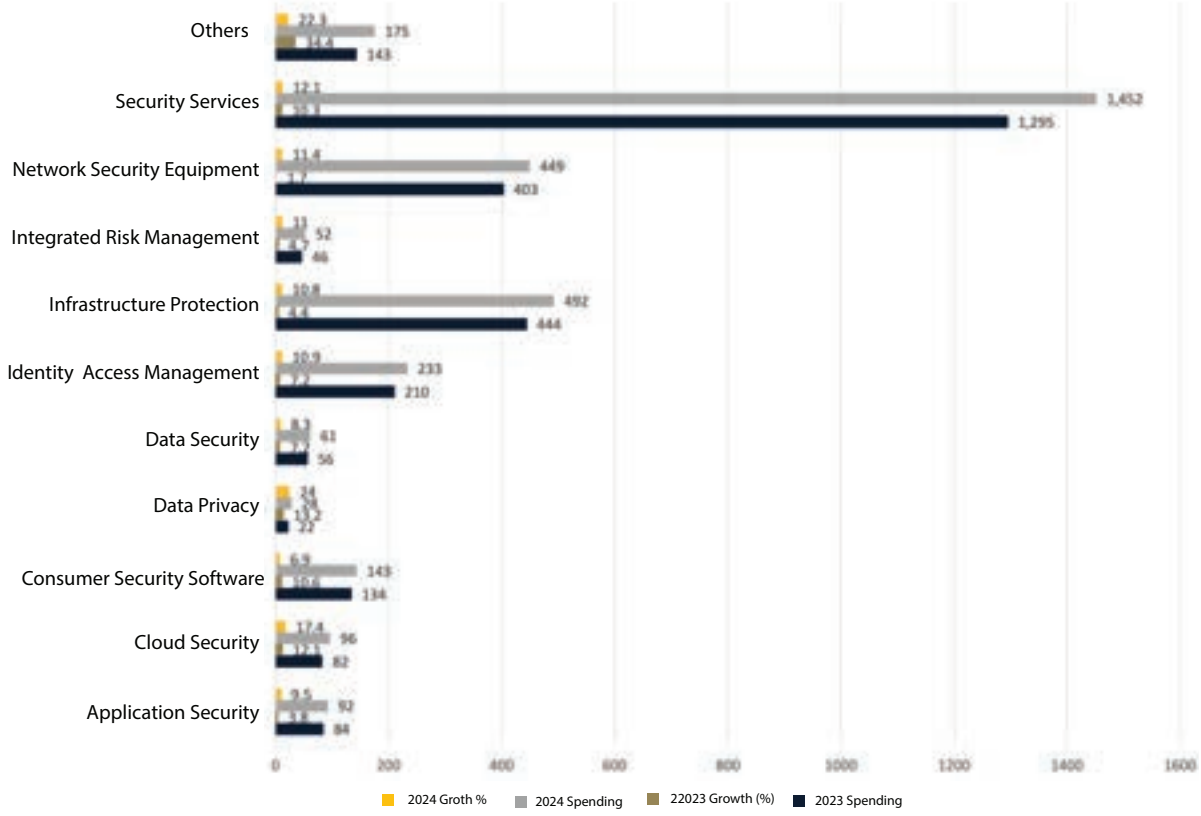


Fig 1. MENA End-User Spending on Security and Risk Management, 2023–2024 (Millions USD) Gartner in February 2024]

7 https://wam.ae/en/article/b1kt3yi-national-systems-foil-attempted-cyberattacks

8 https://www.gartner.com/en/newsroom/press-releases/2024-02-13-gartner-forecasts-security-and-risk-management-spending-in-mena-to-grow-12-percent-in-2024#:~:text=End%2Duser%20spending%20on%20security,is%20expanding%20the%20threat%20landscape.

9 https://www.zawya.com/en/press-release/research-and-studies/39-in-uae-using-ai-without-employer-or-teacher-awareness-says-oliver-wyman-eadapdc6

10 https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/national-cybersecurity-strategy-2019

The purpose of this report is to:

- Explore, analyse and illustrate current trends in cyber threats/cyberattacks affecting the financial sector in the UAE,
- Explore the primary methods, strategies, and processes employed by state and non-state actors, which are examined by analysing changes observed in cyber-attacks directed against financial institutions.
- Shed light on the effects of pertinent cyber threats viewed through a futuristic lens to explore new and emerging adversaries,
- Evaluate the vulnerabilities associated with each of the identified threats, and
- Highlight the current issues that financial institutions are facing as well as explore potential hazards that may arise in the distant future.

3. KEY TRENDS

Phishing and spear-phishing: Cybercriminals continue to operate by employing spear-phishing and phishing attacks, which take advantage of zero-day vulnerabilities that might be missed by conventional antivirus software. Among the various countermeasures suggested by respondents, one security measure is the use of sophisticated threat detection systems integrated with continuous/automated security updates and patches, to detect and mitigate zero-day vulnerabilities used in spear-phishing and phishing attacks.

Ransomware Attacks: The stealthy lateral movement of ransomware malware inside the victim's network poses a serious threat to the financial industry and often leads to delayed detection. One of the primary countermeasures proposed by respondents to address this is the deployment of comprehensive backup and recovery plans, coupled with regular data backups and offline storage options, to ensure the prompt restoration of critical systems and data in the event of a ransomware attack in the financial industry.

AI-facilitated Manipulation: A rising issue in the world of cyber threats is the use of AI to manipulate information, particularly "deep fakes" of voice clones or deep fake videos and misinformation that is facilitated by AI. In the public and professional domains, there has been a greater discussion on AI manipulation. Respondents recommended several countermeasures, including the introduction of multi-factor authentication (MFA) in all banking systems and applications, dynamic speech authentication, voice fraud education and awareness campaigns, and interactive simulation training.

Distributed Denial of Service (DDoS) attacks: Once considered less serious, DDoS attacks have now become a significant concern, possibly due to regional economic and geopolitical factors. These attacks have the potential to disrupt online banking. One of the main countermeasures recommended by respondents is the deployment of robust DDoS mitigation solutions, such as network traffic analysis tools, rate-limiting mechanisms, and Content Delivery Network (CDN).

Device deception: This is also known as deception technology or decoy technology involving using malicious decoy devices and systems that mimic legitimate assets but are designed to attract and mislead attackers who have gained unauthorized access. One area of concern that stands out is the integration of newer technologies

such as the Internet of Things (IoT). As banks move towards full digitization, some are transforming their branches into completely unmanned digitized environments. These digitized branches rely heavily on Internet-connected IoT devices. However, there is a significant risk of poor implementation of key controls such as encryption, authentication and security. As the trend of digitization in banking continues, it is critical that banks address these vulnerabilities and strengthen their defenses accordingly. The speed at which these devices can penetrate and escalate the privileges is alarming.

Operational Disruption: Since financial institutions rely heavily on IT infrastructure, any disruption to that infrastructure such as that caused by cyberattacks may impact day-to-day operations, transaction processing, and client services. Implementing robust access control measures, such as role-based access controls (RBAC) and privileged access management (PAM) systems, is one of the primary countermeasures recommended by respondents for addressing this issue.

Supply Chain Attacks: Threat groups are increasingly interested in supply chain attacks, utilizing employees as potential access points. Those having advanced privileges, including system administrators or developers, are considered high-priority targets. Implementing strict vendor risk management procedures, such as ongoing monitoring of third-party vendors, contractual obligations, and regular security assessments, is one of the primary countermeasures recommended by respondents to reduce the risk of information supply chain attacks in the banking industry.

4. ANALYSIS OF CYBER SECURITY THREAT LANDSCAPEIN FINANCIAL SECTOR

Since the project employed a qualitative approach, ratings were based on the frequency and extent of citation or mention of a topic in the discussion. A distribution of cyber threats reported in the financial industry is shown in the Figure 2. The most reported threat are spear phishing and ransomware, which are typified by focused and misleading email operations and ransomwares that encrypt data for extortion. Following this is the AI-facilitated manipulations that use AI-generated content for malicious purposes and information supply chain attacks, which are focused on the data flow within organisational supply chains.

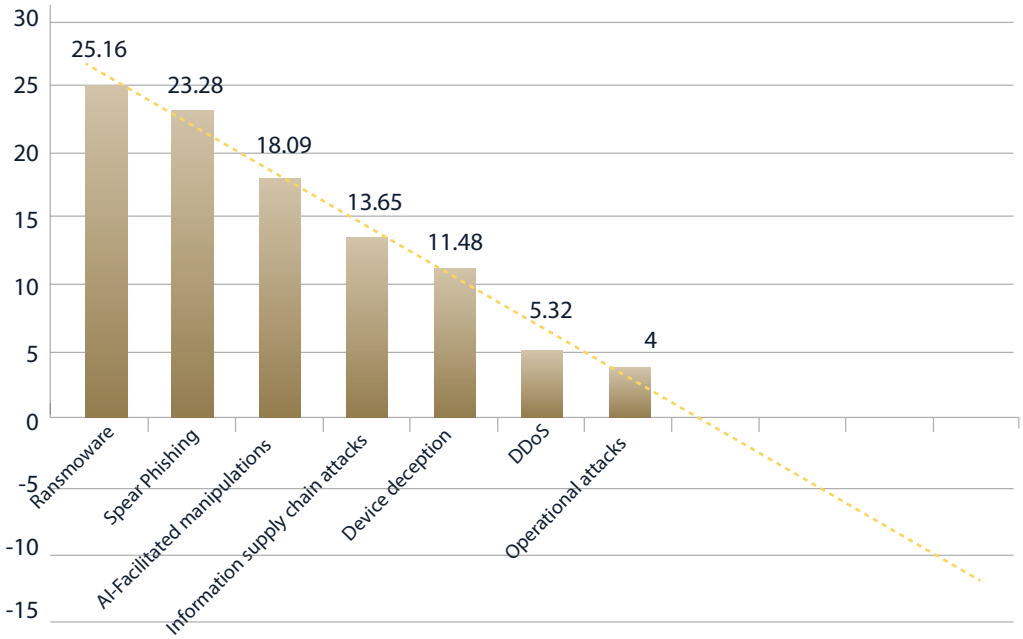
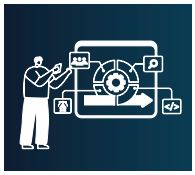


Fig 2. Threat ranking in terms of criticality in the Financial sector

Additional threats include USB attacks that compromise systems through malicious USB and IoT devices, operational attacks and DDoS attacks that cause network outages. This highlights how the financial sector faces a wide range of cyber threats that are always changing, making comprehensive security measures necessary to protect against different attack vectors. According to this analysis, the threat landscape can be categorized into three tiers based on their potential impact and to a lesser extent, frequency: Critical, moderate, and minor threats.

- Critical threats: High-priority threats that represent serious risks to the financial sector are known as critical threats. Ransomware and spear phishing are two critical threats that are highly targeted and have the potential to cause significant data breaches and financial losses. This also includes AI-facilitated manipulations, which pose major security risks because of their capacity to deceive and manipulate people or systems.
- Moderate threats: They might cause operational disruption even if they might not instantly cause large financial losses or data breaches. This category includes information supply chain attacks, which aim to disrupt and compromise sensitive information by focusing on the data flow within organisational supply chains. Even if they are serious, operational attacks don't necessarily result in permanent harm, but they can still interrupt financial services and cause network outages.
- Minor threats are considered lower-priority threats with comparatively less severe outcomes in comparison to critical and moderate attacks. Although they have the ability to cause adverse effects, device deception attacks DDoS are classified as less serious since they don't always have a significant long-term impact in comparison to other, more serious threats.

5. METHODOLOGY



This report is based on valuable insights and feedback gathered from IT security stakeholders representing 12 prominent financial institutions in the UAE. Eighteen respondents from these 12 organizations actively participated in the discussion. Although multiple respondents from one organization shared their insights, they are considered as a single respondent represented as R1, R2 ... R12. The principal aim is to initiate proactive communication with these stakeholders to gather their viewpoints on diverse facets of information technology security. The report ensures a comprehensive grasp of the prospects and challenges in the landscape of IT security by combining inputs from a variety of stakeholders. The goal is to get thorough understanding of the technical and non-technical controls necessary for the financial system.

The Nvivo14 qualitative analysis software was used for classification, coding and analysis of raw transcribed data. NVivo ensured systematic analysis and classification of the gathered responses through inductive research.

Vulnerabilities in this specific context are classified into three categories: technical, socio, and socio-technical (see Figure 3). This provides a customised viewpoint on risks that are especially pertinent and significant in the financial realm. Technical vulnerabilities encompass weaknesses in financial software and systems, socio vulnerabilities are linked to human factors within the financial industry, and socio-technical vulnerabilities provide insights into the intricate interplay between technology and human elements, offering a nuanced understanding of the multifaceted risks faced by financial institutions.

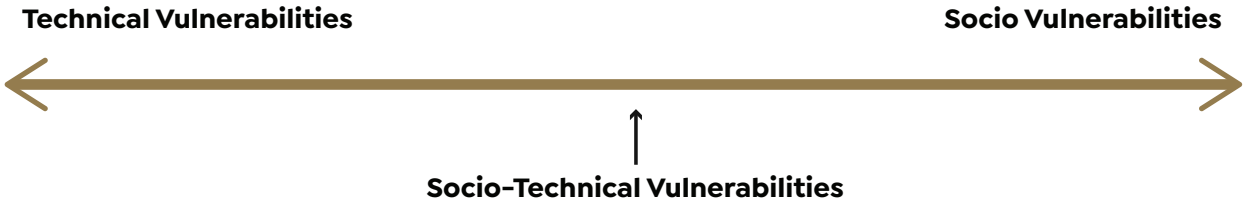


Fig 3. Vulnerability types

This report utilises the Fishbone diagram as a systematic tool to examine the various aspects linked to the threat landscape of each attack in the financial sector. These aspects include threat vectors, technical vulnerabilities, socio-vulnerabilities, socio-technical vulnerabilities, Advanced Persistent Threats (APT) influence, and AI implications.

The objective of stakeholder/respondent interaction is to provide a comprehensive viewpoint on current and emerging threats, vulnerabilities, and recommended countermeasures. The method is iterative, promoting ongoing discussion to improve recommendations and proposals. The information acquired will be an essential starting point for higher level policymakers and help improve IT security frameworks in the financial industry. This methodology's collaborative and participatory nature guarantees a thorough awareness of the opportunities and challenges associated with IT security, enabling proactive actions and advancements.

6. THREAT LANDSCAPE

Financial institutions face a variety of serious cybersecurity threats worldwide, according to information gleaned from interviews with stakeholders from twelve well-known financial institutions in the United Arab Emirates (UAE). The identified main attack types in the financial sector encompass spear phishing, ransomware device deception attacks, Distributed Denial of Service (DDoS) attacks, information supply chain attacks, AI-facilitated manipulations and operational threats as delineated in Figure 4.

These attack types will be further discussed in the subsequent sections, which delve into the factors associated with each attack's threat landscape within the financial sector and the corresponding security measures. These factors encompass threat vectors, technical vulnerabilities, socio-vulnerabilities, socio-technical vulnerabilities, APT influence, and AI implications.

Fig 4. Threat Landscape of the Financial Industry

a. Spear Phishing

Spear phishing is a sophisticated tactic used in APTs to deceive individuals into divulging personal information or committing crimes. Even with awareness campaigns in place, users' susceptibility and ignorance of phoney emails, URLs, and SMS messages continue to be exploited. R2 asserted that *"Spear phishing attacks can be planned by APT groups using strategies like zero-day attacks, which make use of vulnerabilities that have not been identified earlier".* The problem is made worse by artificial intelligence (AI), which makes people more vulnerable to phishing emails sent by AI. As stated by respondent from R1, "Executive impersonation via AI generated audio, visual or email content potentially assists in the increase of spear phishing attacks". According to R3, "Spear phishing attacks can be orchestrated by APT actors backed by state actors, strategically targeting financial institutions in their quest to gain unauthorized access to critical data, including customer records and intellectual property information". Comprehensive cybersecurity safeguards are necessary due to the compounding effects of social engineering and insider threats. Attack triggers include phishing calls, hybrid attacks compromising banking systems, and deceptive emails, both internal and external, leading to potential malware infiltration.

Spear phishing: Vulnerabilities/Triggers (Figure 5)

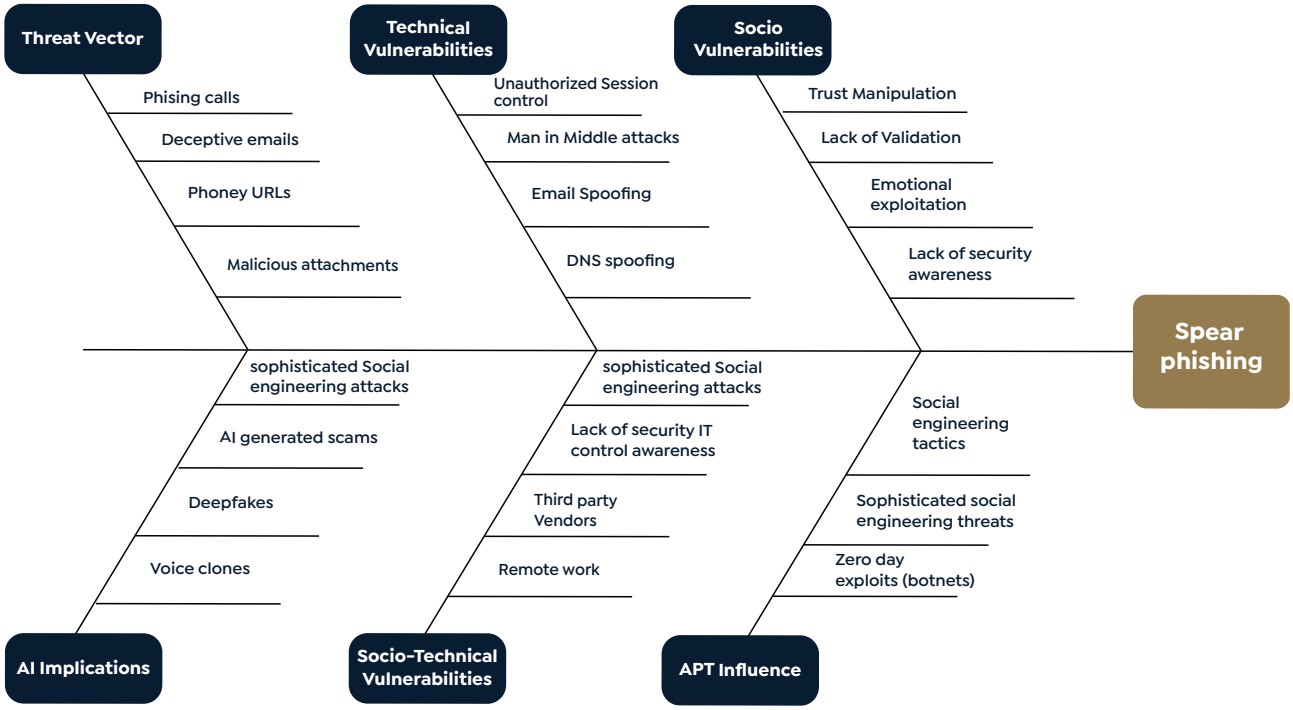


Fig 5. Factors related to Spear Phishing threat landscape in financial sector.

- The threat vectors include phishing calls, emails, phony URLs, and malicious attachment.
- The technical vulnerabilities exploited in spear phishing have been cited as email spoofing, Domain Name System (DNS) spoofing, Man in Middle attacks, and unauthorized session control. DNS spoofing refers to the manipulation of DNS records to divert consumers to phoney URLs imitating authentic banking portals.
- The socio vulnerabilities include trust manipulation, lack of validation of users, limited security awareness and emotional exploitation. Attackers use psychological cues like excitement, fear, curiosity, or urgency to persuade users to perform a desired action, like opening a malware-laden attachment or clicking on a malicious link.
- The socio-technical vulnerabilities include remote work, third party vendors, lack of security awareness, and sophisticated social engineering attacks. Employees who operate remotely may

utilize unprotected networks or personal devices that lack the robust security features typically found in office settings.

- The AI triggered threats comprise of voice clones, deepfakes, scams and sophisticated social engineering attacks. APTs utilize spear phishing in the form of zero-day exploits, sophisticated threats, and social engineering tactics.
- Zero-day exploits focus on hardware or software vulnerabilities that neither the vendor nor the cybersecurity community is currently aware of. Attackers use these exploits, which are especially deployed in spear phishing attacks, to sneak into systems and run malicious malware undetected.

Complex strategies and tactics are used by sophisticated threats to increase their impact and avoid discovery. These threats are quite successful at spear phishing attacks because they frequently involve several steps, such as reconnaissance, social engineering, and targeted exploitation using stealth and evading defences.

b. Device deception attacks

Device deception attacks (using IoT devices and USB) are a serious concern to cybersecurity because they can affect network devices as well as endpoints. The buffer overflow attack, which frequently results in privilege escalation, has been made possible by device deception that exploit IoT sensors and device storage, USB drives' auto play feature, and maliciously altered USB drivers. Data exfiltration using storage devices is a well-known malicious practice linked to device deception attacks, allowing information theft via peripherals in both directions. In one case, data from a linked USB storage device is stolen by a compromised host that has resident malware. On the other hand, a malevolent storage device could stealthily obtain confidential data from an innocent host, functioning without the host or USB device owner's knowledge and frequently evading automated forensic instruments. According to R7 *"While frontline defence against USB attacks is critical, equal attention needs to be focused on guarding against lateral, creative attacks, with all personnel receiving thorough training and awareness campaign".*

Device deception attack: Vulnerabilities/Triggers (Figure 6)

- The threat vectors include malicious IoT devices, USB drivers, buffer overflow attacks, data exfiltration and insider threats. In the financial sector, device deception attacks can result in buffer overflow incidents, wherein malevolent storage and IoT devices take advantage of software or firmware vulnerabilities to introduce large amounts of data into memory buffers. This can cause system crashes, escalate privileges, or allow arbitrary code to be executed.
- Technical vulnerabilities mainly occur due to flaws in operating systems, firmware, auto-play, and inadequate endpoint protection. Socio vulnerabilities include trust manipulation, lack of accountability, employee negligence and lack of security awareness.
- Socio-technical vulnerabilities consist of insufficient user authentication, lack of security awareness and employee mistakes.

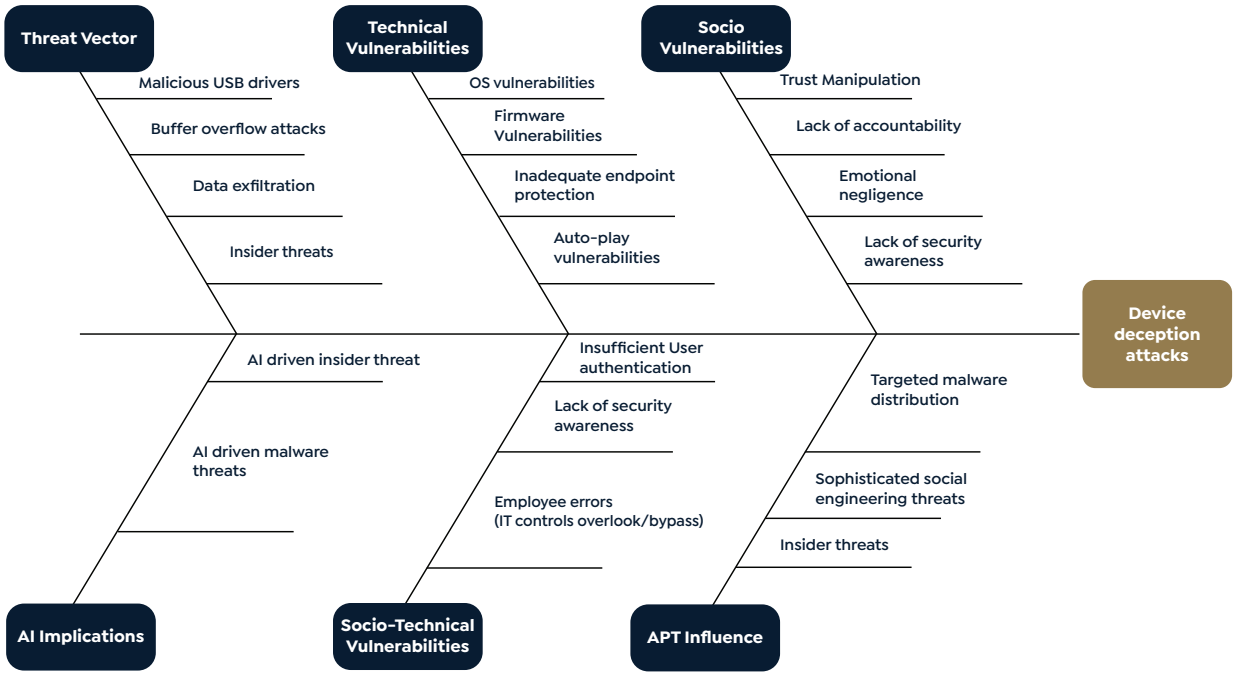


Fig 6. Factors related to device deception threat in the financial sector.

- AI implications on USB attacks comprise of AI driven insider threats and malware attacks.
- APT attacks occur in the form of targeted malware distribution, sophisticated social engineering threats and insider threats. APTs, which are frequently aided by nation-states or highly organised criminal groups, use a variety of Tactics, Techniques and Procedures (TTPs) including IoT and storage devices to penetrate and continuously target organisations or individuals for sabotage, data theft, espionage, or other malevolent objectives.

c. DDoS attacks.

Recent years have seen a significant increase in the prevalence of distributed denial of service (DDoS) attacks, which are largely due to geopolitical and economic factors. As mentioned by R4 *"The DDoS and the other Anonymous Sudan1 attacks are some of the cyber threats which are very prevalent in the region".* DDoS attacks, in contrast to more conventional security measures like firewalls and intrusion detection systems, deliberately target the availability of a system or service by flooding it with so much traffic that it becomes unusable for users. DDoS attacks have the potential to interfere with online banking systems, making it difficult for users to use digital banking services, perform transactions, or access their accounts.

DDoS Vulnerabilities/Triggers (Figure 7)

- The threat vectors include botnets, flooding, DNS manipulation and geopolitical triggers. Botnets are collections of hacked devices under the control of cybercriminals that are used to remotely command compromised machines to flood targeted systems with traffic in an attempt to coordinate and intensify DDoS attacks. Flooding attacks involve DDoS attackers flooding target systems with so much network traffic that they are unable to reply to users' valid requests. By taking advantage of holes in the DNS infrastructure, DDoS attackers can manipulate DNS servers to obstruct or reroute legitimate traffic, making it more difficult to access targeted websites or services. Geopolitical tensions or conflicts can serve as a catalyst for DDoS, in which attackers use the infrastructure or services of organisations linked with opposing governments or ideologies as a means of gaining influence or causing disruption.

1 Anonymous Sudan is a hacker group that has participated in a variety of distributed denial-of-service (DDoS) attacks since early 2023.

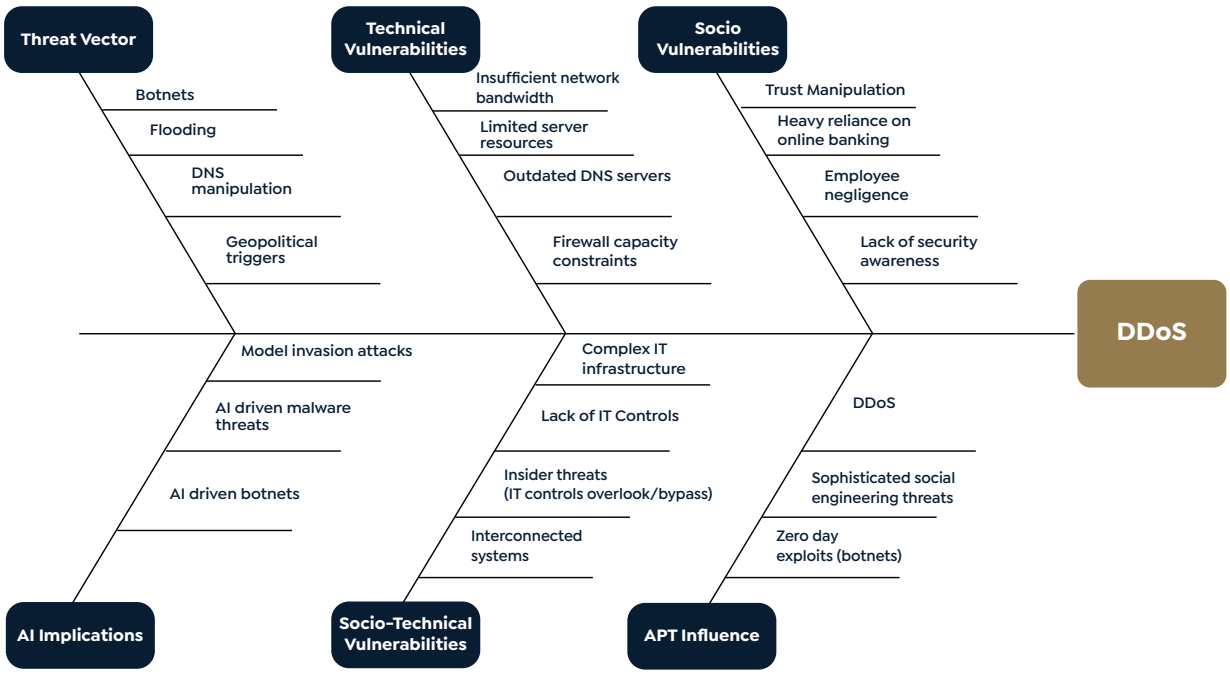


Fig 7. Factors related to DDoS threat landscape in financial sector.

- Technical vulnerabilities include insufficient network bandwidth, limited server resources, outdated DNS servers and firewall capacity constraints.
- Socio vulnerabilities include trust manipulation, heavy reliance on online banking, employee negligence.
- Socio-technical vulnerabilities include complex IT infrastructure, lack of security awareness of IT controls, insider threats and interconnected systems.
- AI implications on DDoS attacks comprises of model invasion attacks, AI driven malware threats and botnets. Attackers may use AI algorithms to dynamically modify and enhance their attack tactics, such as changing attack parameters or evasion techniques in real-time to get around detection systems and more successfully overwhelm targeted systems.
- APT influence occurs in the form of proxy DDoS attacks, insider threat and zero-day exploits. Proxy DDoS attacks are sophisticated adversarial tactics wherein targeted networks or services become the subject of coordinated and amplified DDoS attacks through hacked or compromised systems, also known as proxies.

d. AI-facilitated manipulations

Due to the development of strong AI technology, AI manipulations have become a major worry in the financial industry, especially through deepfake and voice clones. Deepfakes, which were first used by state-sponsored spy agencies, have developed into extremely powerful tools that bad actors employ. As noted by R10 “The deepfake voice and the deepfake video, which were successfully used in a few attacks, might infiltrate into banks and steal the financial assets”. These attacks use AI to produce incredibly realistic and misleading content, such as voiceovers and phoney videos. Deepfakes are a serious risk to the financial industry, especially for voice-based authentication systems that certain banks use. The trust that people invest in financial systems can be abused by fraudulent actors who can fool people into thinking they are dealing with a trustworthy organisation through these attacks. Voice cloning poses a significant threat to the finance sector, as evidenced by external incidents, urging immediate attention to processes and customer controls reliant on voice usage. Concerns have grown because of the development of AI technologies that can imitate real voices, particularly for banks using voice-based banking services. According to R8, “AI tools that are widely available can be leveraged by malicious agents to create or impersonate somebody’s voice”. Deepfake technology

has undermined the long-held belief that every person's voice is unique, casting doubt on the validity of voice-based authentication techniques. Financial institutions must decide whether to continue advancing voice authentication and re-evaluate its application considering these changing risks.

AI-facilitated manipulations: Vulnerabilities/Triggers (Figure 8).

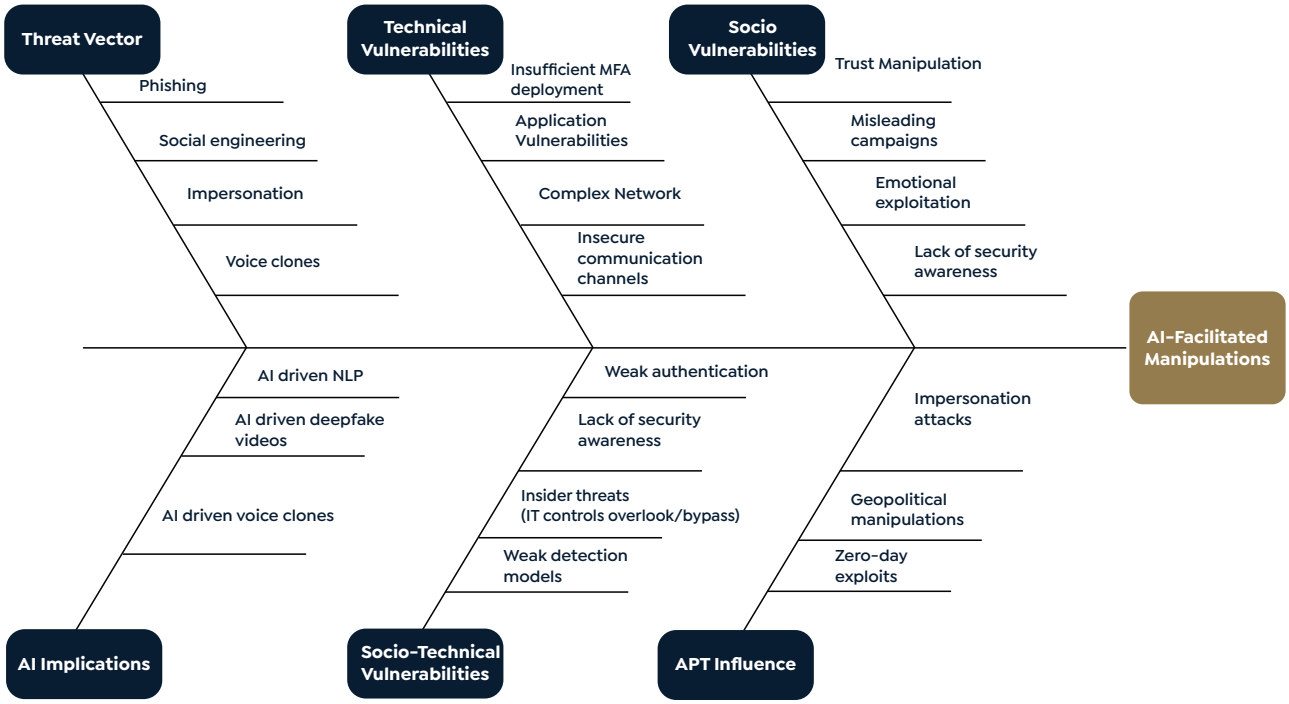


Fig 8. Factors related to AI-facilitated manipulations threat landscape in financial sector.

- The threat vectors include phishing, social engineering, impersonation, and voice clones.
- Technical vulnerabilities include insufficient MFA deployment, insecure storage of biometric data, weak AI models and insecure communication channels.
- Socio vulnerabilities include trust manipulation, misleading campaigns, emotional exploitation, and lack of security awareness. Deepfake attacks include misleading campaigns that utilize extremely realistic synthetic media, such as videos or audio files produced through deep learning techniques, to impersonate bank employees, clients, or other trustworthy individuals. The security and integrity of financial institutions and their clients are seriously jeopardized when these deepfake materials are utilized in social engineering attacks to deceive banking employees or customers into disclosing private information, transferring money to fraudulent accounts, or carrying out other fraudulent actions.
- Socio-technical vulnerabilities include weak authentication, lack of security awareness, insider threats and weak detection models.
- AI implications include AI driven natural language processing (NLP), deepfake videos, and voice clones. AI driven NLPs can be used by attackers to create persuasive messages that resemble those that banks commonly employ, such as account alerts, transaction confirmations, and customer support questions.
- AI has not only enhanced the speed at which APT threat vectors can be customised to the targeted audience but also leveraged the hackers ability to utilize and target these vectors in mass with near perfection. However, the silver lining in the cloud is the ability of the organizations to fight AI enabled attacks with AI enabled defenses.

e. Ransomware attacks

Ransomware attacks are a serious and constantly changing risk to many different industries, including finance. One problem with ransomware attacks is that they can move stealthily and laterally, which can make detection difficult and occasionally cause discovery to be delayed. According to R5, *"Ransomware attacks compromise critical data sets or system availability, posing a severe risk of rendering the bank unavailable for an extended period of time".*

Ransomware's complexity is increased by its diverse character, its assortment of extortion tactics, and its ulterior motives that go beyond monetary gain.

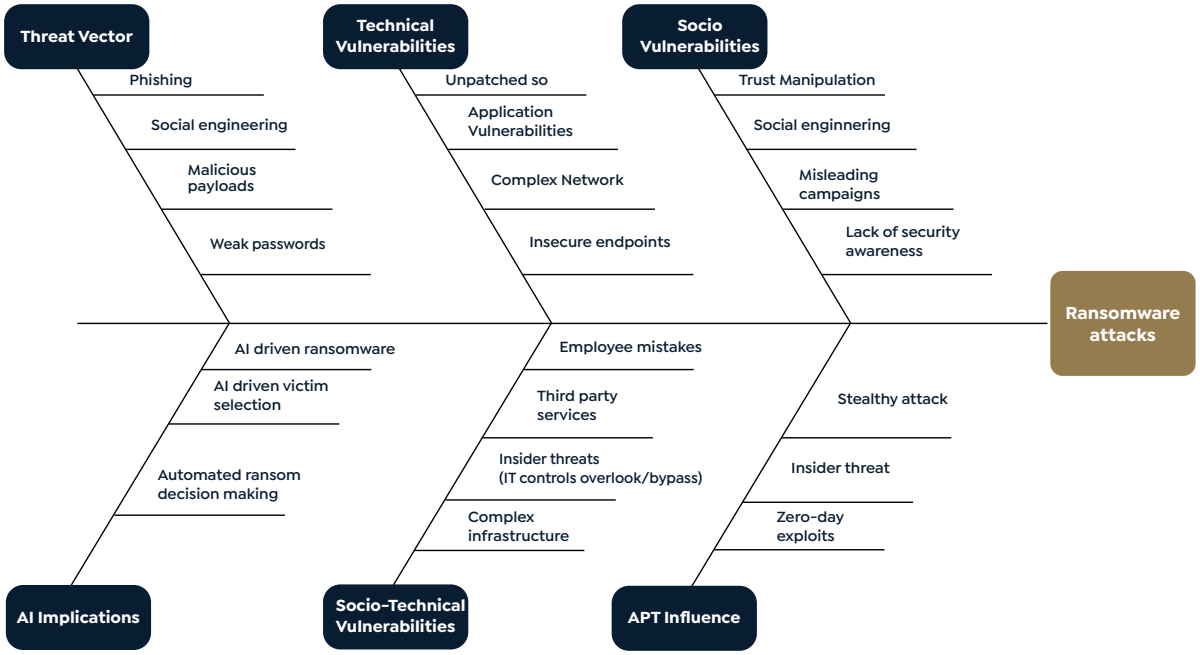


Fig 9. Factors related to Ransomware threat landscape in financial sector.

Ransomware: Vulnerabilities/Triggers (Figure 9)

- The threat vectors include phishing, social engineering, malicious payloads, and weak passwords. Ransomware attacks targeting the banking industry often contain malicious payloads such as backup deletion tools, network disruption tools, credential theft trojans, data encryption malware, and data exfiltration modules. These payloads are intended to compromise sensitive data, extort payments, and disrupt vital operations.
- Technical vulnerabilities include unpatched software, misconfigured system, weak authentication, and insecure endpoints.
- Socio vulnerabilities include trust manipulation, social engineering, misleading campaigns, and lack of security awareness.
- Socio-technical vulnerabilities include employee mistakes, third party services, insider threats and complex infrastructures.
- AI implications on ransomware attacks include AI driven ransomware, victim selection and automated ransom decision making. AI algorithms are used by malicious software to improve many parts of ransomware attacks, which is known as AI-driven ransomware. By analysing large amounts of data to identify high-value targets, such as businesses with valuable assets, shoddy security measures, or substantial financial resources, AI can be used in ransomware attacks to automate the process of victim selection. This allows attackers to focus their efforts and increase their chances of making money. Attackers can customise their extortion demands to each victim

specifically and increase their chances of successful ransom negotiations by utilising AI-driven ransomware, which can incorporate automated decision-making mechanisms to dynamically adjust ransom demands based on factors like the victim's industry, size, geographic location, or perceived ability to pay.

- APT influence on ransomware attacks includes stealthy attacks, insider threats and zero-day exploits. Stealthy ransomware attacks frequently go unnoticed for long stretches of time, using advanced evasion strategies to avoid detection while seriously damaging the targeted systems and data.

f. Operational attacks

Operational risks in the financial sector include a range of threats, such as targeted breaches and nation-state actors exfiltrating data. Data exfiltration is a common practice used by nation-state threat actors, which puts sensitive data at serious risk. The threat scenario is further amplified by the appearance of initial access brokers in the cybercriminal market. Malicious actors find these brokers to be profitable targets because they enable unauthorised access to networks. Operational staff members, including relationship managers and corporate personnel, are susceptible to phishing attacks, in which malicious emails purporting to be from reputable sources ask recipients to transfer money to unidentified organisations. As mentioned by R10 representative, *"The operational threat posed by insider actions, such as leaving endpoints vulnerable, increases the likelihood of unauthorized access to the organization's network, potentially leading to data exploitation, fraud, and other detrimental consequences".*

Operational Attacks: Vulnerabilities/Triggers (Figure 10)

- The threat vectors include phishing, geopolitical risks, state sponsored attacks, and insider threats.
- Technical vulnerabilities include unpatched software, application vulnerabilities, complex networks, and insecure endpoints.
- Socio vulnerabilities include trust manipulation, employee negligence, malicious intention, and third-party dependence.
- Socio-technical vulnerabilities include initial access brokers, data exfiltration, insider threats and complex infrastructure. Initial access brokers add another level of risk to the operational security of the banking industry by enabling threat actors to get around standard defensive measures and directly penetrate banking networks through intermediaries who are skilled at obtaining unauthorised access.
- AI implications include AI driven ransomware, victim selection, and automated ransom decision making.
- APT influence occurs in the form of social engineering tactics, sophisticated threat actors and zero-day exploits.

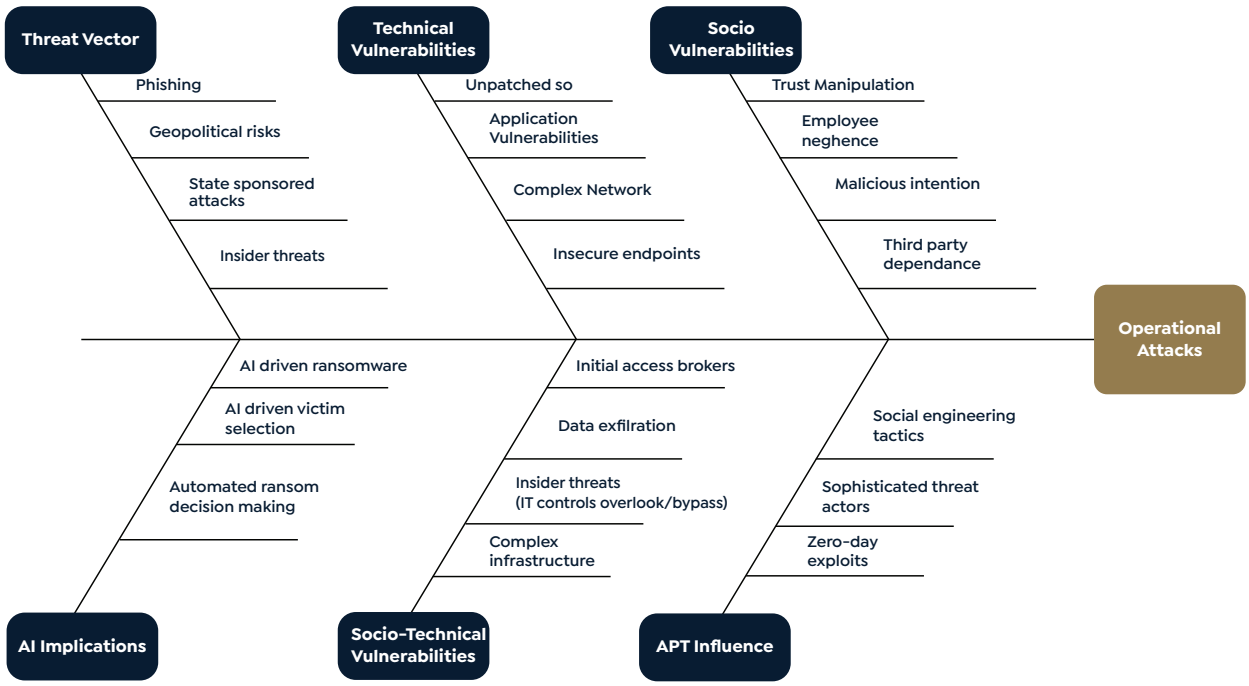


Fig 10. Factors related to Operational threat landscape in financial sector.

g. Information supply chain attacks

Information supply chain attacks, which include the compromise of the interconnected network of information flow between companies, constitute an imminent risk to the financial sector. According to R1 "With dependencies extending to various stakeholders in supply chain, including customers, suppliers, and business partners, the transmission of sensitive information introduces inherent risks". These attacks underscore the information supply chain's susceptibility and are frequently launched via conventional supply chain compromise tactics. With all the information being shared with suppliers, partners in business, and customers, the exposure is very important.

Information supply chain attacks: Vulnerabilities/Triggers (Figure 11)

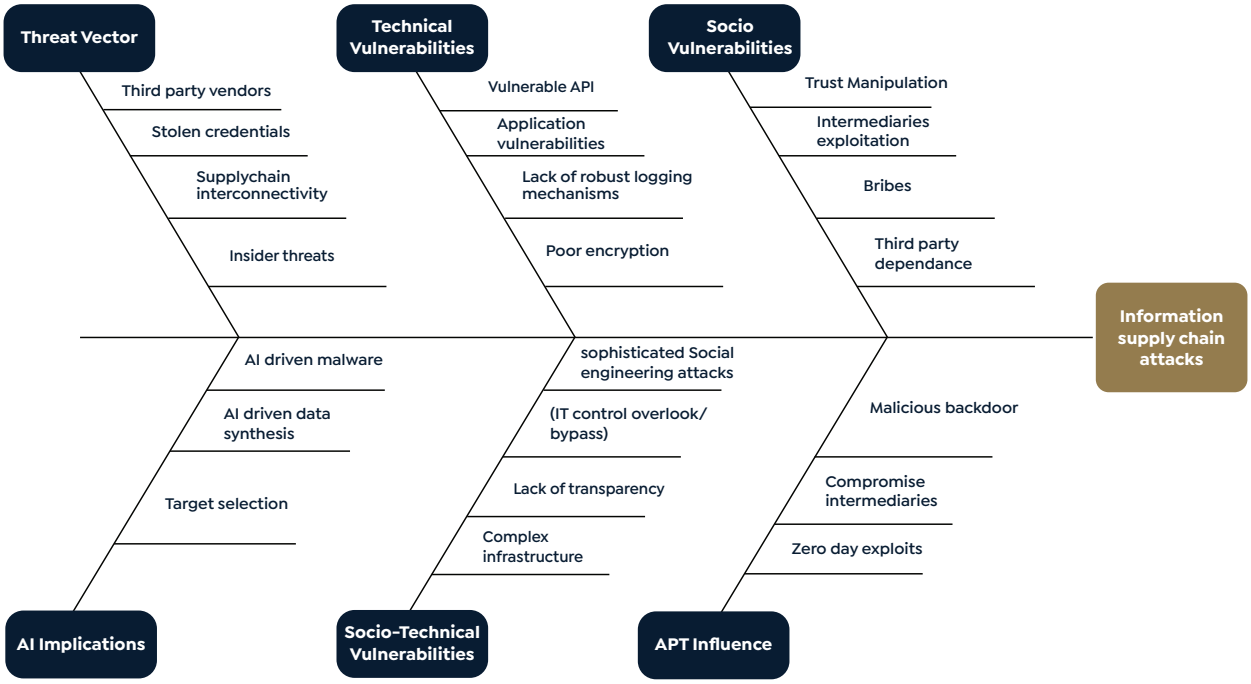


Fig 11. Factors related to Information supply chain threat landscape in financial sector.

- The threat vectors include third party vendors, stolen credentials, supply chain interconnectivity and insider threats. During an information supply chain attack, adversaries exploit vulnerabilities in the systems of third-party vendors to gain unauthorized access to the network of the financial institution. They accomplish this by taking advantage of the vendor-bank trust connection to enter the system. Adversaries penetrate the supply chain and indirectly target banking institutions by taking advantage of vulnerabilities in this interconnected ecosystem. For instance, breaching the suppliers' system could offer hackers access to the banking institution's network. Insiders may cooperate with external threat actors or act on their own in an information supply chain attack to compromise vital banking assets.
- Technical vulnerabilities include vulnerable APIs, application vulnerabilities, lack of robust logging mechanisms, and poor encryption.
- Socio vulnerabilities include trust manipulation, intermediaries' exploitation, bribes, and third-party dependence.
- Socio-technical vulnerabilities encompass insufficient vendor risk management, inconsistent security standards, lack of transparency and complex infrastructure. Insufficient vendor risk management procedures could lead to insufficient control of vendor security procedures, creating openings for malicious actors to penetrate the bank's network. Inconsistencies in security measures throughout the supply chain might result from different vendors in the banking industry adhering to different security standards and processes. Attackers can take advantage of these discrepancies by focusing on vendors who have relaxed security protocols as points of entry into the larger banking network. The term "lack of transparency" in the supply chain describes a lack of awareness or comprehension of the security procedures and controls put in place by third-party suppliers. Banking organisations might not have much knowledge about the data handling procedures, security procedures, or incident response skills of their vendors. The complex infrastructural environment in which the banking industry operates is generally made up of interconnected systems, networks, and services. The intricacies of the supply chain's linkages and exchanges create a complex network of connections that attackers can exploit, adding layers of risk.
- AI implications include AI-driven malware, data synthesis, and target selection.
- APT influence takes the form of malicious backdoors, compromised intermediaries, and zero-day exploits.

7. THREAT ACTOR TRENDS

The rationale underlying the identification of diverse threat actors within the banking industry is the comprehension of the complex cyber threat landscape. Threat actors in the banking industry are commonly referred to as adversaries that can range widely, from lone and/or unskilled hackers (such as script kiddies) to knowledgeable cyber activists to organised cybercriminal groups and syndicates to highly sophisticated nation-state actors. Hackers can be people or organisations with a variety of goals, frequently looking to take advantage of vulnerabilities for money or to cause trouble, while cybercriminals deliberately carry out illicit acts to make money. On the other hand, political or ideological goals are pursued by cyber activists using tactics like hacktivism. There are also nation-state threat actors who are sponsored by government-backed institutions involved in cyber espionage or sabotage. There is a growing trend of state-sponsored cyber espionage and sabotage directed towards financial systems, and nation-state threat actors are noted to be more active. These adversaries that threaten the financial sector in the UAE are rational decision actors seeking the most rewards with the least amount of effort and risk of detection.

Effective risk management in the rapidly changing financial sector requires an understanding of the intricacies of threat actors. Threat actors are entities that can be either technical or non-technical. They are essential in taking advantage of vulnerabilities to carry out malicious actions that are intended to inflict harm. This section offers a strategic overview of the causes, impacts, and targeting methods of these threat actors by delving into current developments related to them.

Trends of Technical Threat Actors in the Finance Sector:

Spear phishing actors: The ease with which victims can be tricked by specific tactics including fraudulent emails, false URLs, and SMS messages that contain redirection links makes spear phishing an increasingly potent threat. According to R7, *"These attacks often deceive companies into releasing payments to what appears to be legitimate payees, only to discover later that the funds have been redirected due to sophisticated intermediates".*

- **Ransomware operators:** The dynamic patterns of ransomware highlight an extreme risk to cybersecurity, as malicious actors use this type of software to encrypt important information and then demand a fee to unlock it. Ransomware attacks are more serious since they might compromise important datasets or disrupt system availability, which could cause financial institutions to go offline for a long time and thus highlight the need for effective defences. As quoted by R12, "*Some companies pay the ransom when targeted by attackers who successfully breach banks or financial institutions".*
- **Supply Chain Compromise:** Financial institutions approach supply chain exposure as a distinct threat category, recognising its importance and taking steps to reduce the risks associated with possible supply chain compromises. According to R10, *"Supply chain attacks are incredibly crucial as they create backdoors for attackers".*
- **Data Exfiltration by Nation States:** With an emphasis on prospective data exfiltration incidents and insider-facilitated breaches, data integrity concerns draw attention to the threats posed by nation-state actors engaging in targeted intrusions. As mentioned by R11, *"The financial sector is greatly threatened by data exfiltration, which puts confidential information at risk and undermines public confidence in financial institutions".*
- **Malicious Software:** A significant concern is the possibility of malicious software attacks, particularly considering current geopolitical events. The fluid geopolitical tensions and situations occurring in different regions of the world gives rise to state-sponsored actors who are increasingly innovative in their attacks. According to R6, *"The financial sector is highly vulnerable to malicious software that compromises the integrity of vital systems and data by taking advantage of security vulnerabilities".*
- **Initial Access Brokers (IABs):** It's important to keep an eye out for and remediate vulnerabilities that are taken advantage of by IAB management, since the highly profitable marketplace for IAB malware continues to be a concern. As mentioned by R9, *"Since they make it easier for unauthorised users to enter networks and may result in catastrophic breaches of confidential financial data, IAB pose a serious threat to the financial industry".*
- **Non-Technical Threat Actor Trends in the Financial Sector:**
- **Geopolitical Risks:** Geopolitical ramifications are a constant area of concern and are watched closely for potential effects on the banking industry. During the discussion, R1 representative highlighted that *"this competition, largely driven by the dynamic between global superpowers, significantly impacts operational strategies and requires careful navigation to mitigate associated risks." Since geopolitically motivated attacks can typically be attributed to the affected region, respondents have warned the sector to be cautious of traffic originating from these regions and their affiliated countries.*
- **Insider threats:** Insider threats are examined from two distinct perspectives. First, the most common kind of insider action is characterised as unintentional and careless data leaks. Secondly, concerns focus on cybercriminal organisations hiring insiders, underscoring the necessity of constant observation.
- **Strategic Fraud Manifestations:** One of the main concerns in this case is the rise in fraudulent activity involving cryptocurrencies, often associated with investment scams. Moreover, this requires careful attention to how generative AI may impact the fraud threat landscape, especially regarding the vulnerability of employees and customers.
- **AI generated scams:** This involves the risks related to executive impersonation and schemes that use executives' emulated audio to create believable and expandable scams. Deepfakes are

becoming a bigger danger to identity governance and detection systems because malicious actors are using AI to mimic real-world situations and avoid being recognised by official systems. According to R3, *"The increasing integration of AI, including systems like WormGPT and FraudGPT, into cybercriminal activities is amplifying the sophistication of their attacks, rendering them more convincing and difficult to detect such scams".*

8. EXPLORING THE VULNERABILITY LANDSCAPE

An essential tool for supporting cybersecurity plans is the thorough examination of vulnerabilities in the financial sector, which offers deep insights into changing trends, patterns, and new threats unique to this sector. This knowledge enables financial institutions to proactively address possible risks to their systems and sensitive data, prioritise patching, and allocate resources wisely. Figure 12 shows a thorough analysis of various vulnerabilities influencing the listed cyberthreats/attacks in the financial sector-technical, socio-technical, and socio. This highlights the complexity of cyber risks facing the financial sector, highlighting the need for a well-rounded strategy that considers both technical and human-centric vulnerabilities.

- It is evident that spear phishing, information supply chain attacks and AI-facilitated manipulations are predominantly rooted in socio and socio-technical vulnerabilities. These attacks exploit vulnerabilities in human and social factors within security systems, highlighting the urgent need for enhanced cybersecurity measures in the banking industry.
- Ransomware emerges as a threat that exploits both socio and socio-technical vulnerabilities. These attacks highlight the need for a diversified strategy to counter such risks in the financial sector because they not only target technical vulnerabilities but also use social engineering techniques to influence human behaviour.
- It becomes apparent that operational attacks primarily exploit socio-technical vulnerabilities. The aforementioned risks leverage the combination of technical vulnerabilities and social engineering techniques, highlighting the significance of considering human elements in addition to technology precautions in financial cybersecurity initiatives.

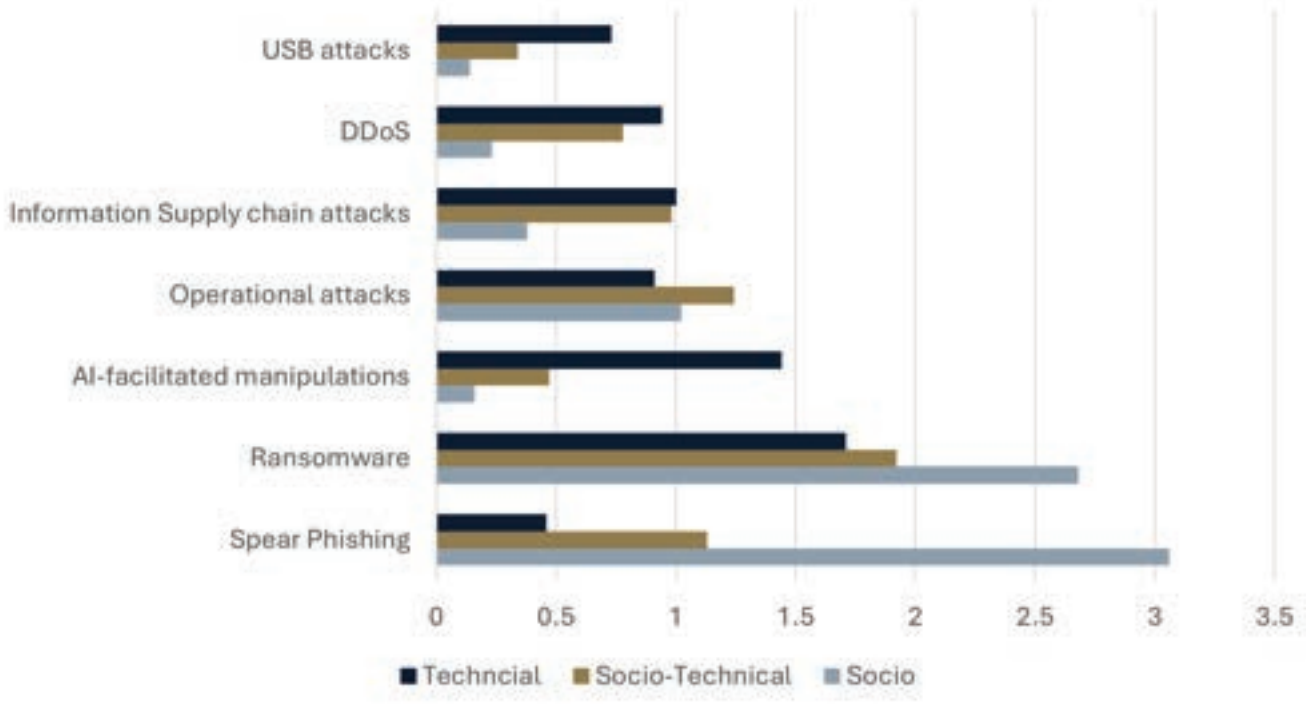


Fig 12. Exploring Vulnerabilities: Interconnected Cyberthreats in the Financial Industry

- Technical as well as socio-technical vulnerabilities are exploited by USB attacks. These attacks highlight the necessity for comprehensive cybersecurity policies that address several layers of risk within financial institutions by taking advantage of vulnerabilities in both human behaviour and infrastructure.
- DDoS attacks mostly take advantage of technical vulnerabilities. Strong defensive measures are required to lessen the impact of these attacks on financial institutions since they take advantage of vulnerabilities in network architecture and protocols.

9. EXPLORING APT LANDSCAPE

Advanced Persistent Threats are persistent, highly skilled cyberattacks that are planned and executed by knowledgeable adversaries. Financial institutions are the target of APT actors, who are frequently state-sponsored actors whose objective is to obtain unauthorised access to sensitive data, such as customer and intellectual property. Attackers with a high degree of expertise and financial resources frequently deploy APTs with a specific target in mind and are prepared to commit a substantial amount of time and money to meet their goals. The threat actors penetrate a target bank's network using a mix of malware, social engineering, and network exploitation techniques. Once inside, they stay hidden for extended periods of time while stealing confidential data. The multiple perspectives of APTs include zero-day, sophistication, dormant, stealth, and complex.

Zero-day attacks: Since zero-day attacks take advantage of undiscovered vulnerabilities, they pose substantial threat to the financial sector. Within the financial institution context, these attacks target software vulnerabilities that have not been reported to the vendor, making the organisation open to potential fraud. Financial institutions are particularly concerned about these vulnerabilities, as when left unpatched, threat actors can launch attacks that bypass traditional security measures. Due to their critical role in the global economy and the possibility of substantial financial gain, financial institutions are appealing targets for zero-day attack. As mentioned by R6, *"Zero-day attacks represent a critical cybersecurity threat, exploiting vulnerabilities in software or operating systems that are unknown to vendors and defenders. This type of attack poses significant challenges as malicious actors can capitalize on the vulnerability before it's patched, infiltrating networks and systems to carry out malicious activities".*

Sophisticated APTs: The financial sector is significantly vulnerable to sophisticated attacks, necessitating a higher degree of defence against complex and sophisticated strategies used by threat actors. APT threats are defined as cyberattacks that are more complex and involve evasion tactics, sophisticated malware, and sophisticated plans. Multiple respondents have stated that financial institutions are ideal targets for these kinds of advanced attacks where threat actors may employ a variety of strategies in these multi-stage attacks to bypass security barriers. They reiterated that attackers could, for example, deploy APTs to obtain persistent and stealthy access to systems over a long period of time, engage in social engineering to target staff, or exploit vulnerabilities in banking software. Sophisticated attacks have the potential to cause financial transactions to be disrupted, compromise client information, and grant unauthorised access to sensitive financial data in the financial industry. According to R9 *"In today's evolving cybersecurity landscape, organizations face increasingly sophisticated threats that exploit vulnerabilities across multiple vectors. The SolarWinds attack of 2020 serves as a stark reminder of the interconnected nature of cyber risk, where even trusted third parties can unwittingly become conduits for malicious activity".*

Dormant APTs: In the financial industry, dormant APTs are particularly threatening since they lie dormant for a long time, are remotely exploited, and carefully navigate the target's network in order to stay undetected. These threat actors deliberately postpone undertaking malicious acts, possibly waiting for the right opportunity to launch an attack. Since, it becomes more difficult to detect them in a timely manner, it enables them to bypass security layers. According to R7, *"Dormant APTs are a constant threat in the financial industry, quietly entering networks and ready to unleash havoc when they are activated".*

Stealth APTs: APTs skilled at stealthy tactics often target financial institutions. Multiple respondents stated that these attacks are designed to be undetectable, employing sophisticated techniques to infiltrate networks, move discreetly, and extract confidential financial information without triggering alarms. Since APTs in the banking sector are data-focused, attackers may employ email or instant chat as a means of disguising themselves as reliable organisations. As mentioned by R4, *"Stealth APTs are a silent threat to the financial industry because they operate surreptitiously inside networks and avoid detection by conventional means".*

Complex APTs: Financial institutions are especially vulnerable to complex APTs that use many strategies. Often focused on data exfiltration or espionage, these threats employ a variety of strategies, methods, and approaches to accomplish their goals. Due to the intricacy of these threats, financial institutions must implement comprehensive cybersecurity measures. As quoted by R12, *"Complex APTs are a significant threat to the financial industry because they use sophisticated techniques to enter and stay in systems without being noticed".*

The distribution of APT attacks in the financial sector is shown in Figure 13, which reveals an intricate and multidimensional threat perspective. Most of these attacks are zero-day attacks, which represent the exploitation of zero-day vulnerabilities. The frequency of complicated attacks emphasises the employment of clever and sophisticated methods by threat actors, which reflects the growing intricacy of cyberthreats. This highlights the relevance of implementing dynamic cybersecurity safeguards to successfully combat these ever-changing and complex attacks.

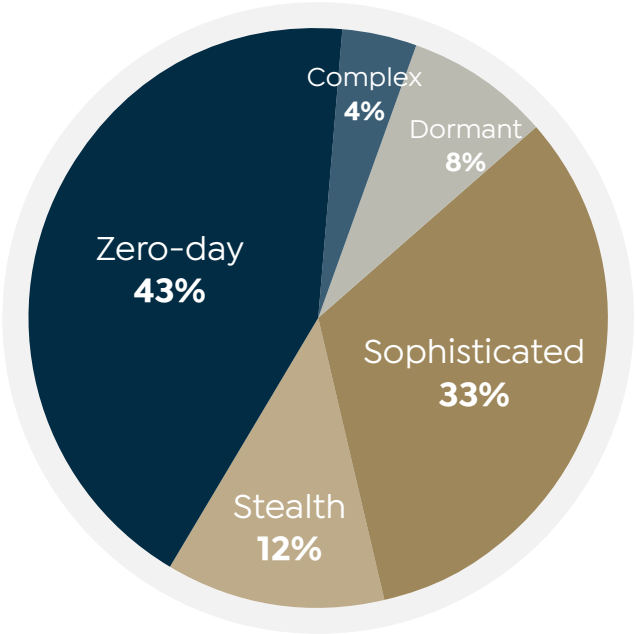


Fig 13. Distribution of APT Threats in the Financial Industry

The inherent nature of APTs (e.g., dormant, stealthy, complex, etc.) means that the financial industry is deliberately targeted by large, organised, rational and sophisticated cybercriminal syndicates and nation-states that have large amount of financial and human resources at their disposal, to achieve their illicit cybercriminal and geo-political aims. For example, these cybercriminal syndicates and nation-states devote resources to hire cybersecurity specialists and researchers to discover zero-day vulnerabilities, develop corresponding technical exploit and AI toolkits and even train personnel specialising in social engineering tactics.

Hence, to address APTs effectively, the financial industry and regulators will need to rally similar resources to address these threats, such as hiring cybersecurity researchers to develop corresponding countermeasures to break the cyber kill chain stages of a cybercriminal attack, and investing in personnel and tools for detection, prevention, recovery and resiliency. In addition, combating APTs will require not just confronting technical vulnerabilities, but also addressing the significant human and social challenges behind the socio and socio-technical vulnerabilities. By doing so it will increase the efforts and reduce the rewards of APT attackers.

To sum up, the financial industry is confronted with a constantly changing array APTs, which can range from dormant threats that wait to stealth attacks that target covert operations to sophisticated APTs that use a variety of tactics. The frequency of zero-day attacks among APTs that target financial institutions is particularly noteworthy. This highlights the necessity of a proactive and comprehensive cybersecurity measures to safeguard customer data, strengthen financial systems, and preserve overall stability in the face of continually developing advanced cyber risks.

10. CONCLUSION

The report aims to provide a comprehensive understanding of the evolving landscape so that financial institutions are equipped to navigate it and implement proactive measures to mitigate cyber risks. From a critical perspective, ransomware is considered a grave threat that leverages AI-enabled vectors, particularly spear phishing through social engineering methods. In this respect, managing the internal and external organizational human factor gain prominence. Proper interventions can ensure that human weakness can be transformed into 'human firewall'. While respondents provided mixed reactions regarding the effectiveness of SETA programs, accurate monitoring and measurement of these programs, targeted at different stakeholders through an optimal mix of delivery can mitigate these threats to a great extent. Furthermore, managing the information supply chain through continuous visibility and third-party monitoring is essential to prevent operational disruptions. While DDoS attacks were not previously a significant threat, due to geopolitical tensions, attackers have recently leveraged them for economic reasons. It remains essential to monitor the strategies, methods, and long-term patterns utilized by threat actors to enhance cybersecurity within the financial sector.

The IT operation plays a critical role in day-to-day cybersecurity within the financial sector, encompassing everything from designing and architecting secure systems to implementing solutions and managing them throughout their lifecycle, including decommissioning of Hardware or software of the digital environment. This complex operation relies heavily on the IT Service Management System (ITSMS) framework and practices to ensure effective governance and compliance with Information Security Management System (ISMS) best practices.

Misconfigurations or lapses in governance and compliance with ISMS and ITSMS standards lead to significant compromises and losses, posing serious threats to financial institutions. Therefore, it's imperative for organizations in the financial sector to prioritize these aspects to mitigate cybersecurity risks effectively. Without proper governance and compliance measures in place, security layers may remain weak and unreliable, exposing organizations to financial losses, reputational damage, and other adverse consequences.

11. EXPLORING APT LANDSCAPE: SUBSEQUENT PHASES

This is a multi-phase study with the following current ('a' and 'b', for completion by Q4 of 2024) and subsequent ('c', 'd', 'e' and f 2025/2026) studies.

a. *A Situational Crime Prevention (SCP) Model for the Financial Sector (in UAE, Singapore and Australia including both deductive and inductive reasoning). Completion by Q4 of 2024*

b. *A strategic evaluation of cyber security strategies of UAE, Singapore and Australia Completion by Q4 of 2024.*

c. *Explore existing and proposed countermeasures for the identified threats in terms of (1) threat prevention, avoidance and transference and (2) attack mitigation in a dynamic technological AI environment.*

d. *Evaluate the adequacy of technical interventions in threat prevention, avoidance and transference including attack mitigation.*

e. *Evaluate and explore the adequacy of socio-technical interventions in threat prevention, avoidance and transference including attack mitigation*

f. *Explore, Identify, Analyze, and Evaluate Critical Variables for Building and Implementing a Dynamic Cybersecurity Serious Game to Objectively Measure Employees' Threat Readiness and Detection Capability.*

ABOUT ADGM ACADEMY

ADGM Academy, the knowledge arm of Abu Dhabi Global Market (ADGM), a financial free zone in Abu Dhabi, aims to become a leading educational and human capital academy for banking, finance, digital and public services in the region.

Aligned with the UAE's vision for economic strength, we offer world-class educational experiential programs. At the forefront of financial and digital training, we partner with industry experts, professional organizations, and academic institutions to design and deliver innovative certified programs. a journey of growth, learning, and transformation where knowledge meets opportunity to shape the future of the financial industry.

ABOUT RESEARCH CENTRE

The ADGM Academy Research Centre brings together an ecosystem of academics, financial industry practitioners, government and technology experts to unlock the shared potential to improve the financial environment in MENA and beyond.

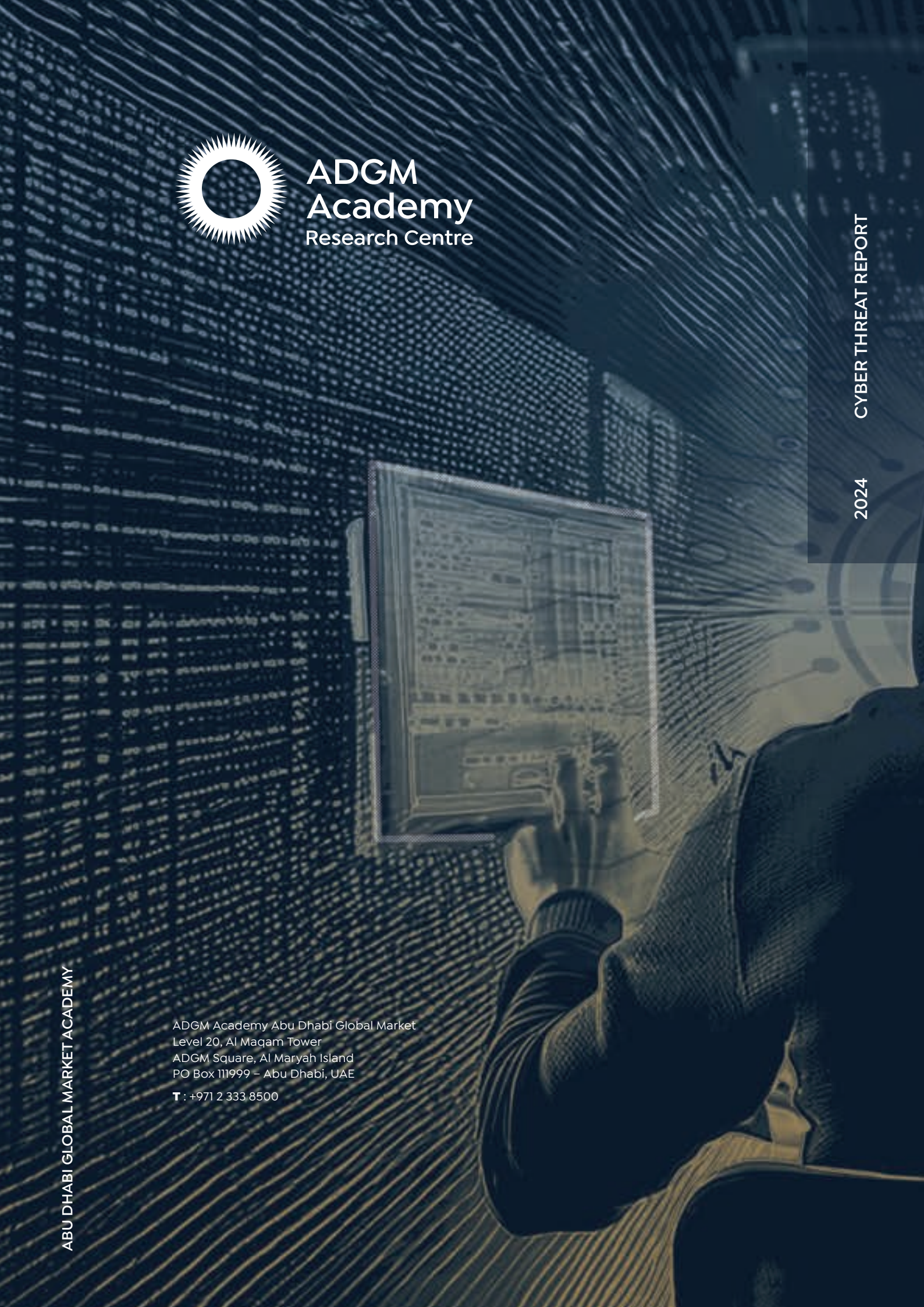
The financial industry continues to transform at a rapid pace with new technologies, disruptors, threats and opportunities appearing all the time. Independent research is crucial to be able to understand and utilise this transformation for the benefit of your business, your customers and society in general.

The Research Centre provides that understanding through insights developed in collaboration with the academic community.

Stay up to date with ADGM Academy Research Centre.

adgmacademy.com **research@adgm.com**

FOLLOW US
ON OUR SOCIAL NETWORKS



ADGM Academy
Research Centre

CYBER THREAT REPORT

2024

ADGM Academy Abu Dhabi Global Market
Level 20, Al Maqam Tower
ADGM Square, Al Maryah Island
PO Box 111999 – Abu Dhabi, UAE

T : +971 2 333 8500

ABU DHABI GLOBAL MARKET ACADEMY