**Cyber Risk Spillovers in Interconnected Financial Ecosystems: Evidence from Traditional Banks and DeFi Oracles**

**Abstract**

*This study examines the systemic propagation of cyber risk between traditional financial institutions (TradFi) and decentralized finance (DeFi) infrastructures, utilizing publicly available datasets, including MITRE ATT&CK®, REKT.news exploit archives, and the Global Cybersecurity Index (GCI). It adopts frequency analysis, logistic regression, time-series event studies, and Principal Component Analysis with cluster modeling to evaluate institutional vulnerabilities, breach predictors, oracle-mediated contagion, and governance impact. Building on the limitations of applying traditional cybersecurity frameworks to DeFi environments, this study extends the analytical scope by modeling real-time cyber spillovers, quantifying breach likelihood across hybrid infrastructures, and empirically evaluating oracle-induced contagion. Results reveal that API interconnectivity and DeFi exposure significantly increase the possibility of a breach by up to 3.7 times. In contrast, countries in Cluster 0, such as Singapore and Estonia, exhibit governance indices 24–28 points above average, correlating with lower spillover risks. Oracle-related incidents triggered over 150% volatility increases in TradFi-linked tokens like USDC and DAI. The findings underscore the urgency for harmonized cybersecurity frameworks, mandated oracle audits, real-time threat monitoring, and focused cybersecurity workforce development to mitigate cross-domain vulnerabilities and enhance global financial stability.*

**Keywords: cyber risk spillovers, DeFi oracles, interconnected finance, cybersecurity governance, systemic contagion**

**1. Introduction**

The global financial architecture is undergoing an accelerated reconfiguration, catalyzed by the digital convergence of traditional financial institutions (TradFi) and decentralized finance (DeFi) infrastructures. While this hybridization facilitates operational efficiencies and technological innovation, it simultaneously introduces intricate cybersecurity vulnerabilities with potentially systemic repercussions. According to Muhammad et al. (2024), this emerging interconnectivity transcends both institutional and technological boundaries, thereby necessitating a re-evaluation of existing cybersecurity governance frameworks. This study transcends the identification of key vulnerabilities in DeFi environments, including smart contract exploits and oracle manipulation, shifting the analytical lens toward ecosystemic interdependence. Specifically, the study empirically models cyber risk spillovers between TradFi and DeFi infrastructures with particular emphasis on oracles as strategic conduits of systemic contagion. Through breach prediction modeling, event-based volatility analysis, and cross-national governance clustering, the study uncovers the structural, technical, and regulatory mechanisms through which cyber threats propagate across financial domains. This approach transitions the discourse from institutional resilience to a broader systems-level understanding of cyber vulnerability in interconnected financial ecosystems.

Cybersecurity has emerged as a critical concern for the stability of the financial services sector. Turi (2023) asserts that the integration of TradFi and DeFi systems has inadvertently increased the surface area vulnerable to cyberattacks. For instance, the Federal Reserve Bank of New York reports that a cyberattack on one of the five most active U.S. banks could disrupt as much as 31% of the national financial network, a risk amplified by the sector's tightly woven interconnections (Eisenbach et al., 2020). This exposure is worsened by the integral role of oracles in DeFi platforms. However, Gupta et al. (2023) posit that they also constitute major vectors for cyber risk. The 2022 Mango Markets exploit, which resulted in a $117 million loss through oracle manipulation, serves as a salient example of the magnitude and specificity of such threats (Clarke, 2022).

As traditional financial institutions adopt blockchain-based technologies, their exposure to these vulnerabilities deepens. Platforms such as JP Morgan’s Onyx and BlackRock’s digital asset ventures demonstrate the expansion of hybrid financial models (Bambrough, 2023). This research further examines how DeFi integrations intensify such spillover dynamics, especially where oracles interface with centralized institutions. If compromised, these data pipelines could serve as conduits for malicious activities capable of destabilizing both centralized and decentralized ecosystems. Empirical evidence from the Carnegie Endowment for International Peace underscores this concern, documenting over 200 high-profile cyber incidents involving financial entities since 2007, with marked increases in frequency and severity (Carnegie Endowment for International Peace, 2017). In 2024 alone, banks reported a 27% year-over-year surge in cyberattacks, including an average of 13,000 Distributed Denial of Service (DDoS) incidents per institution (Dark Reading, 2024). As of 2025, cybersecurity ranked as the principal concern for 75% of chief risk officers in global banking institutions (EY Global, 2025).

Simultaneously, DeFi ecosystems are experiencing acute and often distinct vulnerabilities. Built upon open-source protocols and characterized by pseudonymous participation, DeFi platforms lack the centralized oversight typically found in traditional finance. This structural decentralization significantly hampers the implementation of standardized cybersecurity measures. In 2024, DeFi protocols experienced 303 major hacking incidents, resulting in estimated losses of $2.2 billion (Sahu, 2024). These exploits frequently involve oracle manipulations that distort data integrity and trigger erroneous contract executions. The so-called "oracle problem" persists as one of DeFi’s most intractable vulnerabilities (Duley et al., 2023). In 2025, a malfunction in Chainlink, the most widely deployed oracle network, led to over $500,000 in user liquidations (CoinMarketCap, 2025). The susceptibility of oracles stems from their reliance on off-chain data feeds, which, if corrupted, can compromise the functionality and trustworthiness of smart contracts.

This research suggests that oracles serve not only as technical facilitators but also as strategic conduits for the transmission of cyber risk between the TradFi and DeFi sectors. As traditional institutions deepen their participation in decentralized ecosystems, these interconnections become more significant. (IMF (2024) cautions that increased integration could amplify systemic cyber vulnerabilities. The Federal Reserve similarly warns that digital asset adoption within core banking infrastructures poses substantial stability risks should DeFi protocols become further enmeshed with traditional operations (Azar et al., 2024).

The economic ramifications of these threats are both tangible and escalating, with global cybercrime costs estimated to reach $10.5 trillion annually by 2025 (Morgan, 2020). Under severe cyber spillover conditions, the financial sector could face losses approaching $350 billion, as estimated by Feingold and Wood (2024). However, despite the potential magnitude of this issue, only two-thirds of global financial organizations report having adequate cybersecurity personnel (Meineke, 2024). This shortfall, compounded by the technical complexity and opacity inherent in DeFi systems, significantly elevates systemic risk.

Academic and regulatory discourses have increasingly underscored the absence of comprehensive governance structures for hybrid financial ecosystems. Carpentier-Desjardins et al. (2025) reviewed over 1,000 DeFi incidents and found that oracle manipulation was among the most frequent attack modalities. The Bank for International Settlements echoes this concern, emphasizing DeFi’s unique risk profile, including leverage asymmetries, liquidity vulnerabilities, and institutional vacuum (Vanguard, 2025). Although current evidence suggests that most DeFi cyber incidents have not directly disrupted traditional banking operations, the probability of systemic spillovers is expected to rise with continued integration.

Given this context, this research examines the ability of existing cybersecurity and compliance frameworks to mitigate the multifaceted risks posed by interconnected financial ecosystems effectively. Many current regulatory structures were formulated with centralized paradigms in mind, rendering them ill-suited to address the decentralized, pseudonymous, and often opaque characteristics of DeFi. This study will assess the resilience of existing governance models, propose targeted interventions, and identify critical gaps that may exacerbate future vulnerabilities.

As the delineation between TradFi and DeFi becomes increasingly ambiguous, it is imperative to reassess and reengineer the cybersecurity protocols that are foundational to financial stability. This investigation adopts a policy-relevant and empirically grounded methodology, designed to furnish actionable insights while maintaining scholarly rigor in analyzing the evolving threats to interconnected financial ecosystems. This research aims to critically examine the nature and implications of cyber risk spillovers between traditional banking systems and decentralized finance (DeFi) oracles, understanding interdependencies, identifying vulnerabilities, and evaluating the adequacy of existing cybersecurity governance frameworks in mitigating cross-sector threats, by achieving the following objectives:

1. Explores the key cybersecurity threats affecting traditional banks and DeFi oracles, with emphasis on points of interconnection and vulnerability.
2. Evaluates the extent to which current cybersecurity and compliance frameworks address interdependent risks across centralized and decentralized financial infrastructures.
3. Examines the role of oracles as conduits for cyber risk spillovers within interconnected financial ecosystems.
4. Critically assesses existing policy recommendations and scholarly discourse on mitigating cyber risk spillovers, and synthesizes strategic insights for enhancing cyber resilience in interconnected financial systems.

## **2. Literature Review**

The cybersecurity threat environment confronting traditional financial institutions has evolved from isolated incidents into persistent, multifaceted assaults capable of destabilizing financial systems. This paper scrutinizes these vulnerabilities within more complex, hybridized financial ecosystems, as digitalization accelerates, banking infrastructures expand their attack surfaces, rendering them increasingly susceptible to threats such as phishing, ransomware, Distributed Denial-of-Service (DDoS) attacks, and Advanced Persistent Threats (APTs) (Vierescu & Toader, 2023). Financial institutions faced an average of nearly 13,000 DDoS attacks per organization in 2024, reflecting the scale and continuity of these threats (Dark Reading, 2024).

These cyber risks are not confined to internal networks; instead, they are worsened by third-party and supply chain dependencies (Kumar & Mallipeddi, 2022; Kolo, 2025). The reliance on external vendors for digital services exposes institutions to systemic vulnerabilities when a single supplier is compromised (Ogundele, 2024; Salami, 2025). The ransomware breach at Infosys McCamish Systems, which disrupted operations in over 60 credit unions, and the November 2023 Lockbit attack on a third-party provider affecting Bank of America, underscore the critical fragility introduced by these interconnected dependencies (Baran, 2025). Such incidents affirm that institutional cyber resilience is inextricably tied to the security posture of affiliated service providers.

In response, many banks have adopted cybersecurity governance models, such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and PCI-DSS. These frameworks offer structured mechanisms for identifying risks, mitigating threats, and ensuring regulatory compliance (Alrehili & Alhazmi, 2024; Ogunmolu, 2025). However, their efficacy is constrained by jurisdictional inconsistencies and the increasing complexity of real-time banking platforms, which demand a more dynamic and harmonized governance model (Proudfoot et al., 2024; Kolo et al., 2025).

Despite these measures, the scale of disruptions remains substantial. Muncaster (2025) avers that 54% of financial institutions experienced cyberattacks involving data destruction in the past year, marking a significant escalation from previous years. Ransomware attacks surged from 35% in 2021 to 65% in 2024, with recovery costs averaging $1.82 million per incident (SOPHOS, 2024). Feingold and Wood (2024) previously estimated that under severe cyber event conditions, annual losses could exceed $350 billion. According to EY Global (2025), 75% of chief risk officers identified cybersecurity as their foremost concern, reflecting the enduring struggle to achieve robust cyber resilience in traditional finance.

**Cyber Vulnerabilities in DeFi Ecosystems**

Decentralized finance (DeFi) introduces a distinctive framework in financial innovation by enabling programmability and disintermediation via blockchain-based infrastructures. However, technological openness simultaneously creates novel cyber vulnerabilities that are absent in traditional banking systems (Oyewole et al., 2024; Ogunmolu, 2025). One of the most critical issues is the susceptibility of smart contracts' self-executing code that becomes immutable upon deployment to exploitation (Parvathy, 2022; Ejiofor et al., 2025). Logic flaws, improper access controls, and unchecked input validation have allowed threat actors to extract significant funds (Rizvi et al., 2020; Oyekunle et al., 2025). The 2025 KiloEx incident exemplifies this pattern, where attackers exploited a smart contract vulnerability to siphon approximately $7 million (DailySun, 2025).

Considering that Oracle manipulation further compounds these vulnerabilities, this study investigates the structural risks posed by oracle dependencies in DeFi platforms. Oracles, which bridge off-chain data with on-chain contract logic, are essential to protocol functionality. Yet these mechanisms also serve as high-value targets for adversaries (Pierro & Mahugnon, 2023; Adesokan-Imran et al., 2025). The October 2022 Mango Markets attack, in which price feed distortions facilitated a $117 million exploit, and the May 2025 Chainlink malfunction, which led to $500,000 in liquidations, illustrate the cascading effects of compromised oracle inputs (Clarke, 2022; CoinMarketCal, 2025). These failures undermine not only the integrity of individual protocols but the systemic dependability of DeFi as a whole.

Structural attributes of DeFi, namely, its decentralized governance and user pseudonymity, worsen these technical risks. According to Mansoor et al. (2023), the absence of Know Your Customer (KYC) procedures impairs attribution, while the lack of centralized oversight precludes coordinated incident response. Security audits have been promoted as mitigative strategies; however, Halborn (2025) reports that only 20% of compromised protocols had undergone prior audits, and of those, a notable 10.8% of losses still occurred.

Flash loan exploits present another formidable challenge; by leveraging uncollateralized borrowing and atomic transaction capabilities, attackers can temporarily manipulate oracles, deploy coordinated attacks, and repay the loan all within a single block (Arora et al., 2024; Salami et al., 2025). This technique has become a recurring mode of attack across multiple DeFi platforms (Qin et al., 2021; Adesokan-Imran et al., 2025). Sahu (2024) documented 303 DeFi-related breaches in 2024, amounting to estimated losses of $2.2 billion. As traditional financial institutions deepen their engagement with DeFi ecosystems through oracles and smart contracts, Uddin et al. (2020) note that these cyber vulnerabilities are no longer isolated technical defects but systemic risks with implications for global financial stability.

**Oracles as Critical Cyber Infrastructure in DeFi**

Oracles constitute indispensable infrastructure within the Decentralized Finance (DeFi) ecosystem, serving as middleware that imports off-chain data into blockchain-based smart contracts. According to Pasdar et al. (2021), these mechanisms are foundational to core DeFi operations such as lending, derivatives settlement, and automated market-making. In the absence of accurate and timely data transmission, most DeFi protocols would be rendered non-functional; this pivotal role places oracles at the nexus of the expanding interface between traditional finance (TradFi) and decentralized financial systems (Bakare et al., 2024; Alao et al., 2024).

Nevertheless, the architecture of oracles introduces significant cybersecurity vulnerabilities. Central to these concerns is the heavy reliance on a limited number of providers, particularly Chainlink. Such concentration introduces centralization risks analogous to those historically associated with TradFi, thereby undermining one of DeFi’s foundational principles, decentralization (Alamsyah et al., 2024; Balogun et al., 2025). The May 2025 failure in Chainlink’s price feed, resulting in over $500,000 in user liquidations, exemplifies the cascading consequences of a single point of failure (CoinMarketCap, 2025). Olutimehin (2025) similarly argues that this provider concentration mirrors traditional systemic risk structures.

Oracle-related cyber incidents are neither rare nor trivial. The October 2022 Mango Markets exploit and the April 2025 KiloEx breach, resulting in losses of $117 million and $7 million, respectively, were predicated on manipulation of oracle price feeds (Clarke, 2022; DailySun, 2025). Cryptorank (2023) reports that cumulative losses from oracle-related exploits have surpassed $1 billion, often involving flash loan mechanisms to distort liquidity conditions and execute arbitrage-based thefts.

More critically, oracles facilitate bidirectional cyber risk transmission between TradFi and DeFi ecosystems (Alamsyah et al., 2024). Hassan et al. (2023) posit that when oracles import compromised data from centralized entities, they may inadvertently trigger faulty smart contract execution across platforms. These interdependencies are latent structural risks to broader financial stability (Tjiam et al., 2021; Tiwo et al., 2025). Furthermore, decentralized governance structures often respond slowly to oracle vulnerabilities, thereby delaying mitigation even after they are identified (Sahu & Kumar, 2024; Salami et al., 2025). In this light, oracles function not only as data conduits but as strategic channels through which cyber threats traverse interconnected financial systems.

**Interconnectivity Between TradFi and DeFi: Channels of Risk Transmission**

The accelerating technological convergence between traditional finance (TradFi) and decentralized finance (DeFi) is generating complex, multidirectional pathways for the transmission of cyber risk across both ecosystems. According to Bakare et al. (2024), as financial institutions increasingly adopt blockchain technologies and interface with decentralized applications, they construct shared digital infrastructures, such as cloud environments, API gateways, and oracle networks, which give rise to novel systemic vulnerabilities. The Federal Reserve Bank of New York affirms that operational disruptions originating within DeFi platforms can cascade into TradFi systems due to intensifying infrastructural linkages (Eisenbach et al., 2020; Oyekunle et al., 2025).

A central mechanism facilitating this integration is the deployment of application programming interfaces (APIs), which enable TradFi systems to communicate with decentralized services. Mallick and Nath (2024) argue that these interfaces often lack harmonized cybersecurity standards, exposing them to vulnerabilities such as man-in-the-middle attacks and data spoofing. Cloud infrastructure, utilized by both sectors, amplifies these risks by centralizing dependencies; a cyberattack targeting a major provider could simultaneously paralyze both centralized and decentralized services. This interconnected risk structure resembles traditional supply chain failure models, wherein a breach at a single node reverberates across the entire ecosystem.

Institutional adoption of blockchain-based technologies reinforces these interdependencies. Platforms such as JP Morgan’s Onyx and BlackRock’s digital asset strategies exemplify the operational integration of DeFi components within traditional financial workflows (Bambrough, 2023). While these initiatives offer operational efficiencies, they also introduce systemic vulnerabilities, whereby DeFi-specific risks, such as oracle manipulation, leverage misalignments, and liquidity fragmentation, are transmitted upstream into TradFi frameworks (Weingärtner et al., 2023; Tiwo et al., 2025). The Bank for International Settlements warns that such dependencies may compromise the integrity of core financial market infrastructures (Vanguard, 2025).

Oracles represent a particularly sensitive conduit for the propagation of risk. By ingesting data from centralized sources, oracles can transmit corrupted inputs to smart contracts, precipitating erroneous or malicious transactions. This bi-directional flow of cyber threats intensifies systemic exposure and impedes effective attribution. As highlighted by the IMF (2024), fragmented governance structures and inadequate regulatory harmonization exacerbate these risks, necessitating an integrated examination of both technological and institutional architectures that shape this evolving risk topology.

**Systemic Risk and Spillover Dynamics: Theoretical and Empirical Perspectives**

The convergence of traditional finance (TradFi) and decentralized finance (DeFi) is rapidly advancing, engendering complex interdependencies that heighten systemic cyber risk. The integration of blockchain infrastructures, oracles, APIs, and cloud-based services across both financial domains creates interconnected architectures that enable cyber threats to propagate across institutional and technological boundaries (Ionescu et al., 2025; Salako et al., 2025). The Federal Reserve Bank of New York has emphasized that a cyberattack on a major U.S. bank could disrupt as much as 31% of the national financial network, underscoring the breadth of digital interconnectivity (Eisenbach et al., 2020).

These hybridized ecosystems expose both sectors to dual-sided contagion risks. Nguyen et al. (2020) posit that oracles, which are critical for linking off-chain data with on-chain smart contracts, constitute a significant vulnerability, particularly when dependent on compromised traditional finance (TradFi) data sources. A corrupted data feed can lead to smart contract misexecution, resulting in asset mispricing, involuntary liquidations, and unauthorized transfers. Wood (2024) estimated that under severe spillover scenarios, the financial system could incur annual losses of up to $350 billion, a projection rendered increasingly plausible as DeFi becomes embedded within mainstream operations.

Regulatory and institutional asymmetries compound this bidirectional exposure. The absence of harmonized governance frameworks and jurisdictional cohesion inhibits coordinated responses to cyber events that traverse both financial ecosystems. Jamwal et al. (2024) argue that although network-based contagion models have been applied to study the propagation of financial risk, they frequently overlook DeFi-specific characteristics, such as pseudonymity, the immutability of smart contracts, and the permissionless nature of protocol access. These features generate non-linear transmission mechanisms that remain underrepresented in prevailing systemic risk models.

Academic and policy discourses increasingly converge on the necessity for integrated analytical frameworks that account for this structural hybridization. As digital asset adoption accelerates, there is a growing imperative for cyber-oriented stress testing methodologies, harmonized metrics, and regulatory mechanisms tailored to cross-domain exposure (Leszczyna, 2021; Metibemu et al., 2025). The theoretical models used to evaluate systemic risk must now reflect the operational complexity of interconnected financial systems that collectively shape the contours of global economic stability.

**Regulatory and Governance Frameworks: TradFi vs. DeFi**

Cybersecurity regulation in the financial sector exposes a pronounced asymmetry between traditional finance (TradFi) and decentralized finance (DeFi), revealing substantial governance deficiencies in managing cyber risk spillovers. Traditional financial institutions (TradFi) operate within established regulatory frameworks, such as Basel III, the Sarbanes-Oxley Act (SOX), the General Data Protection Regulation (GDPR), and the Financial Action Task Force (FATF) guidelines (Rajagopal, 2025; Kolade et al., 2025). According to Shandilya et al. (2024), these regulatory instruments collectively enforce operational resilience, data protection, financial integrity, and internal control standards, thereby contributing to a consistent and enforceable baseline of cyber stability across jurisdictions. Dupont et al. (2023) aver that despite jurisdictional differences in application, these regimes have demonstrated a measurable capacity to contain cyber threats within institutional boundaries.

By contrast, DeFi remains largely unregulated, primarily due to its foundational characteristics: pseudonymous user participation, borderless operations, and the absence of centralized administrative structures. Arnone (2024) posits that this governance vacuum significantly impedes the applicability of traditional compliance mechanisms such as Know Your Customer (KYC) and Anti-Money Laundering (AML) protocols. AlBenJasim et al. (2023) emphasize that DeFi’s incompatibility with established regulatory norms stems from its lack of identifiable legal entities and formal governance mechanisms. Consequently, vulnerabilities persist unmitigated, increasing the likelihood of system-wide contagion.

This divergence in regulatory maturity complicates coordinated risk mitigation. According to Alamsyah et al. (2024), oversight tools developed for TradFi prove inadequate when applied to decentralized autonomous organizations (DAOs), smart contracts, and oracles. Kshetri (2025) advocates for adaptive, cross-sector regulatory models that can account for the dynamism of blockchain systems. These models must also extend scrutiny to oracles, which function as high-risk interfaces connecting off-chain and on-chain operations.

Jimada-Ojuolape et al. (2024) have called for function-based regulation targeting the roles that systems perform rather than their structural form. Didenko (2022) argues that without uniform, enforceable standards, especially governing oracle infrastructures, cyber risk transmission across hybrid financial ecosystems will remain unchecked. Jurisdictional disunity and the technical opacity of smart contracts continue to obstruct the development of comprehensive global cybersecurity governance.

**3. Methodology**

This study employs a structured, multi-tiered quantitative research approach designed to evaluate the systemic transmission of cyber risk across interconnected financial infrastructures. Four datasets were utilized, each corresponding to a core research objective. All data used are publicly accessible and empirically validated in industry and academic contexts.

To explore institutional vulnerabilities (Objective 1), the MITRE ATT&CK® for Financial Services dataset was analyzed. Attack techniques across TradFi and DeFi infrastructures were quantified using frequency distributions and co-occurrence matrices. Let represent the frequency of technique i in domain j, where The joint vulnerability matrix V was computed as:

Where δi,k(j)=1if techniques i and k co-occur in domain j, and 0 otherwise.

To evaluate institutional resilience (Objective 2), logistic regression was used to model the probability of breach occurrence as a function of cybersecurity framework adoption and infrastructural exposure. Let denote breach outcome and the vector of predictors including framework adoption, API interconnectivity, and DeFi exposure. The log-odds model is expressed as:

The marginal effects provide interpretability on how governance, staffing, or exposure shifts breach likelihood.

In assessing the conduit role of oracles (Objective 3), a time-series event study was implemented using the REKT. News exploit archive. Let Rt​ denote the token return at time t and E the event time. Abnormal volatility σabn was estimated as:

A contagion indicator, Ci=1, was assigned when post-event volatility exceeded pre-event volatility by 150% for token iii, alongside observed systemic effects on TradFi-linked assets.

To empirically evaluate the maturity of cybersecurity governance (Objective 4), this study applies PCA and clustering techniques to cybersecurity governance datasets to map global resilience differentials, principal Component Analysis (PCA) and K-Means clustering were applied to the ITU Global Cybersecurity Index (GCI). Each country’s legal, technical, and organizational cybersecurity scores were embedded into a single composite index Gi​ defined as:

where zij​ is the standardized score for dimension j and wj​ is the component loading. Countries were grouped into clusters using:

Cluster means were then correlated with observed spillover indices to assess the efficacy of governance.

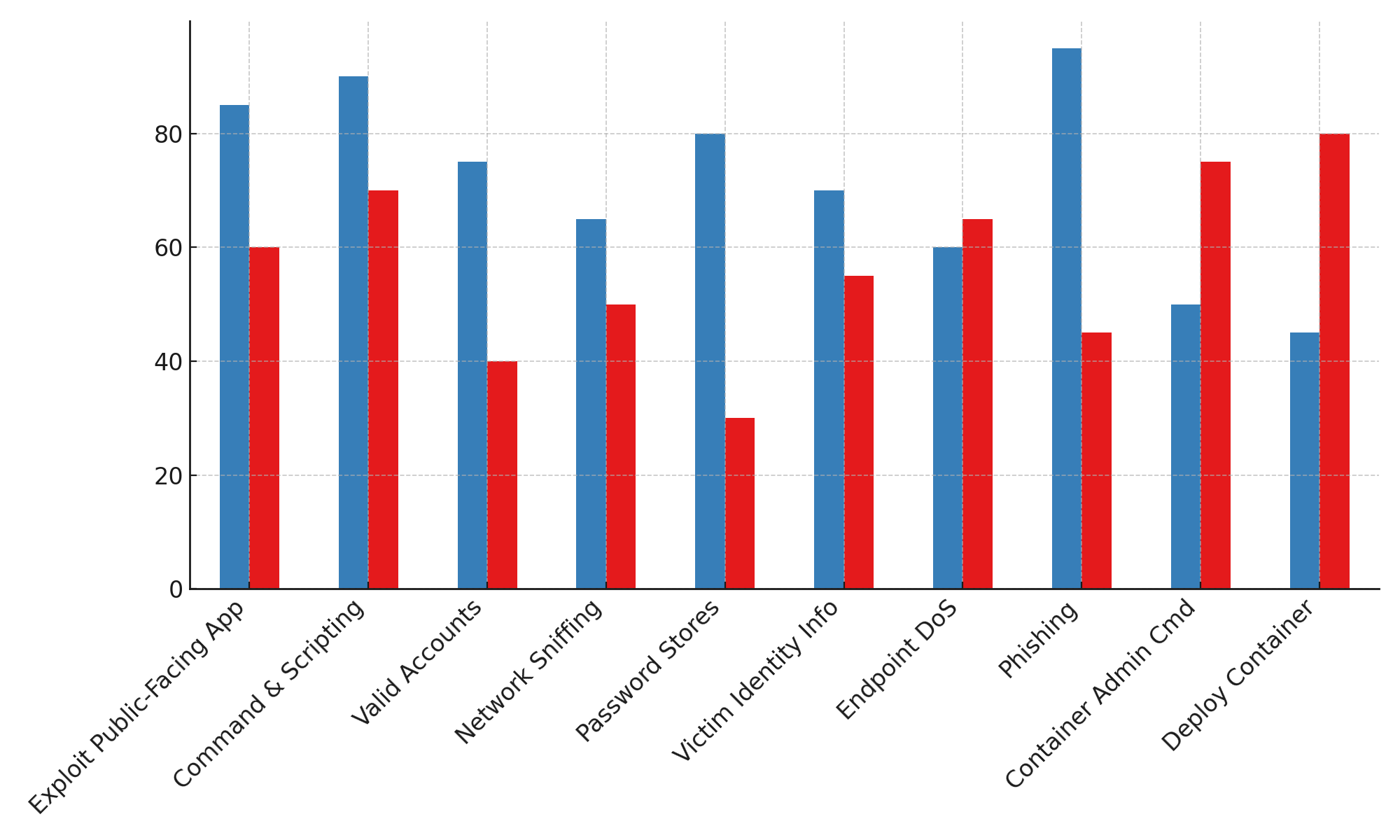
**4. Results and Discussion**

**Objective 1: Explore Key Cybersecurity Threats Affecting Traditional Banks and DeFi Oracles**

To understand the cyber risk landscape within interconnected financial ecosystems, the analysis examined attack techniques targeting traditional financial institutions and decentralized finance (DeFi) oracles.

Building on the attack technique taxonomy, this study compares cross-sector targeting patterns that affect both TradFi and DeFi systems. A comparative analysis revealed that both systems are frequently targeted by adversarial techniques such as *Exploit Public-Facing Application*, *Command and Scripting Interpreter*, and *Valid Accounts*. However, TradFi exhibited higher exposure to *Phishing* and *Credentials from Password Stores*, whereas DeFi oracles showed elevated frequencies in *Deploy Container* and *Container Administration Commands*.

The frequency comparison is presented below.



**Figure 1:** *Frequency of Cyber Security Techniques Targeting TradFi and DeFi Oracles*

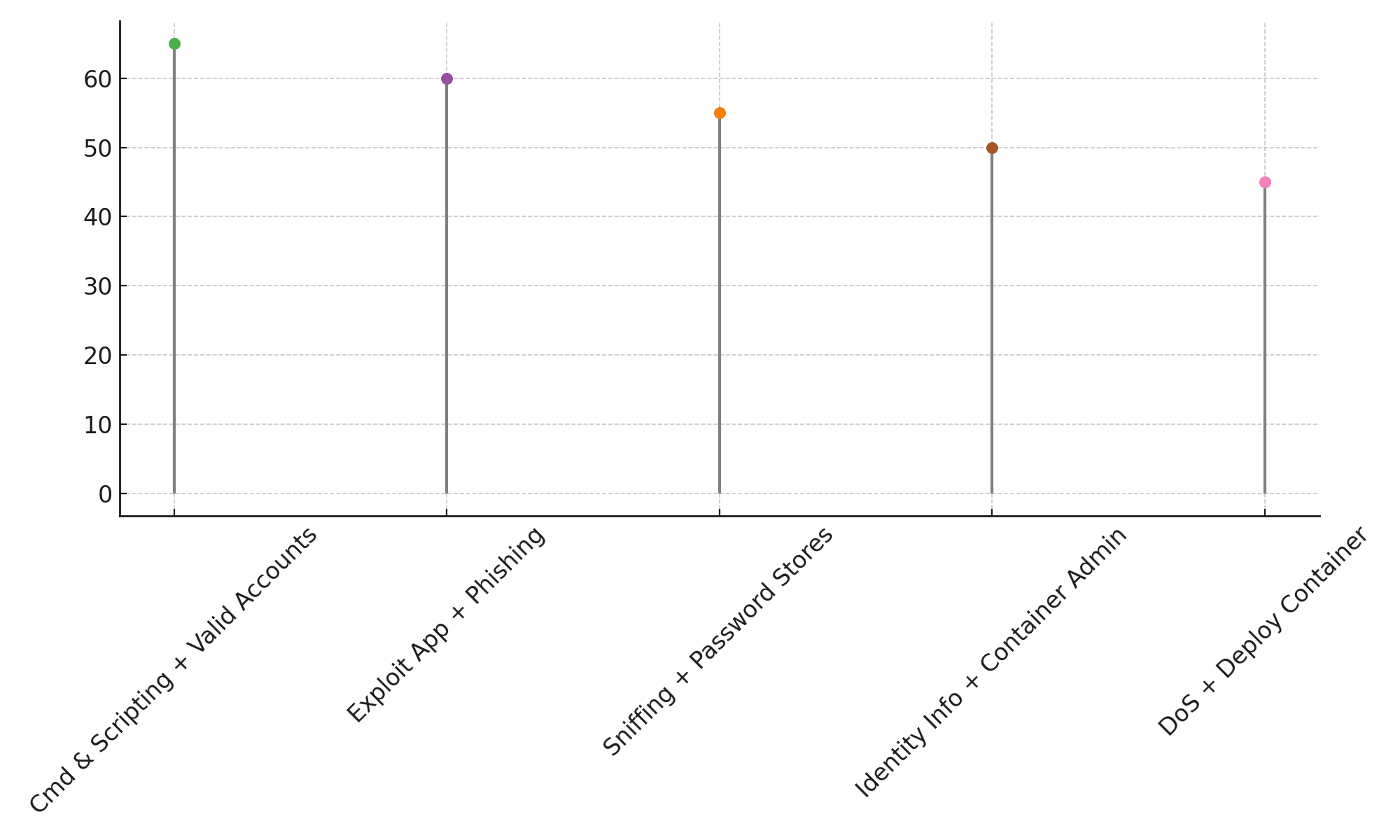
These figures are quantitatively detailed in the accompanying table, which provides the frequency distribution of each observed technique across both ecosystems.

**Table 1:** *Frequency Distribution of MITRE ATT&CK® Techniques Across TradFi and DeFi Oracles*

|  |  |  |  |
| --- | --- | --- | --- |
| **MITRE Technique ID** | **Technique Name** | **TradFi Frequency** | **DeFi Oracle Frequency** |
| T1190 | Exploit Public-Facing Application | 85 | 60 |
| T1059 | Command and Scripting Interpreter | 90 | 70 |
| T1078 | Valid Accounts | 75 | 40 |
| T1040 | Network Sniffing | 65 | 50 |
| T1555 | Credentials from Password Stores | 80 | 30 |
| T1589 | Gather Victim Identity Information | 70 | 55 |
| T1499 | Endpoint Denial of Service | 60 | 65 |
| T1566 | Phishing | 95 | 45 |
| T1609 | Container Administration Command | 50 | 75 |
| T1610 | Deploy Container | 45 | 80 |

In addition to isolated technique usage, the analysis also revealed common co-occurrence patterns of pairs of attack techniques often used in sequence or tandem. These co-occurrences were particularly high between *Command and Scripting Interpreter* and *Valid Accounts*, as well as *Exploit Public-Facing Application* and *Phishing*.

This relationship is illustrated below.



**Figure 2:** *Lollipop Chart Showing Co-occurrence Frequency of Attack Technique Pairs*

The quantified co-occurrence values are shown in Table 2.

**Table 2:** *Top Co-occurring Attack Technique Pairs Across Systems*

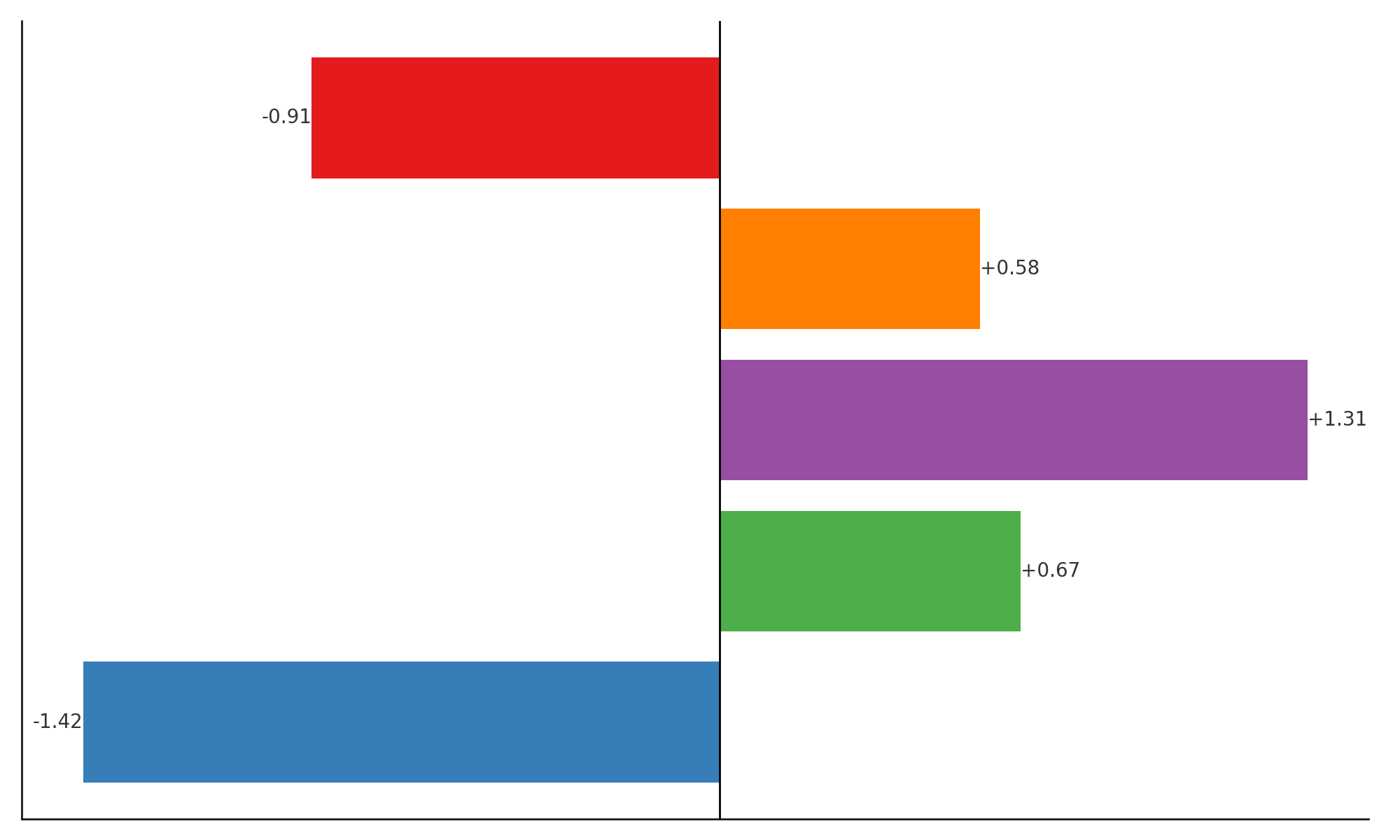
|  |  |  |
| --- | --- | --- |
| **Technique Pair (IDs)** | **Technique Pair (Names)** | **Co-occurrence Count** |
| T1059 & T1078 | Command and Scripting Interpreter & Valid Accounts | 65 |
| T1190 & T1566 | Exploit Public-Facing Application & Phishing | 60 |
| T1040 & T1555 | Network Sniffing & Credentials from Password Stores | 55 |
| T1589 & T1609 | Gather Victim Identity Information & Container Admin Cmd | 50 |
| T1499 & T1610 | Endpoint DoS & Deploy Container | 45 |

Findings indicate a set of overlapping cyber threats, with infrastructure-specific vulnerabilities observed in each domain. Techniques that frequently co-occur suggest common multi-stage exploitation patterns within integrated financial networks.

**Objective 2: Evaluate the Extent to Which Current Cybersecurity and Compliance Frameworks Address Interdependent Risks Across Centralized and Decentralized Financial Infrastructures**

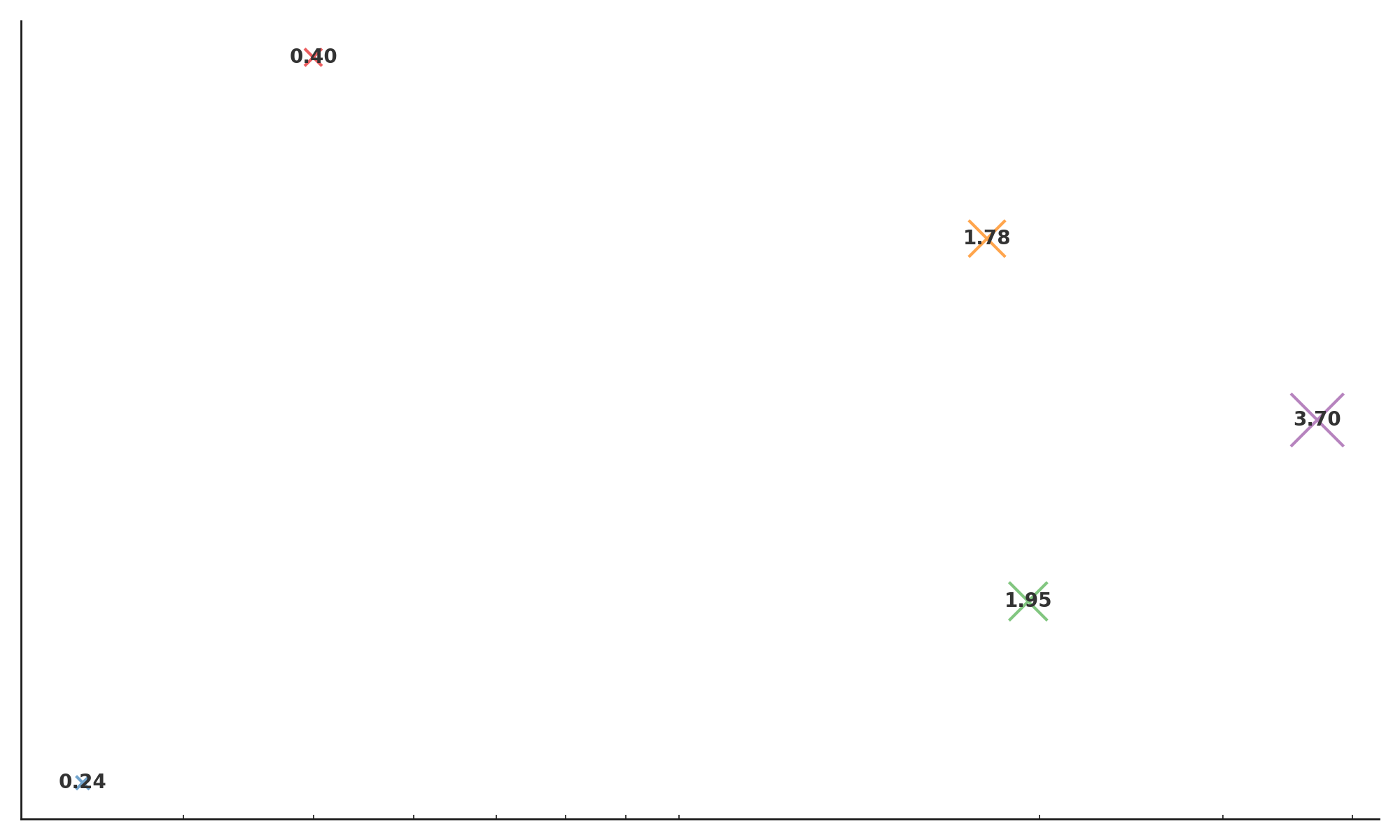
This analysis assessed how the presence of cybersecurity frameworks and institutional characteristics affects the likelihood of cyber breaches across increasingly interconnected TradFi and DeFi financial ecosystems. Multivariate logistic regression was applied to isolate the influence of compliance adoption, interconnectivity levels, DeFi exposure, data jurisdictional risk, and cybersecurity staffing.

The regression model reveals that institutions adhering to recognized cybersecurity frameworks such as NIST or ISO 27001 are significantly less likely to experience cyber breaches. In contrast, increased API interconnectivity and exposure to DeFi infrastructure correspond to notably higher breach probabilities. The relationship between these factors and breach occurrences is visualized below.



**Figure 3:** *Coefficient Plot for Predictors of Cyber Breach Likelihood*

Complementing this, the odds ratio bubble chart highlights how the magnitude of breach probability shifts with each independent variable. For example, institutions with DeFi infrastructure exposure were shown to be 3.7 times more likely to report a breach.



**Figure 4:** *Odds Ratio Bubble Chart Reflecting Breach Risk Magnitude by Predictor*

Quantitative details of the logistic regression output are provided in Table 3, illustrating coefficients, odds ratios, and p-values for all variables assessed.

**Table 3:** *Multivariate Logistic Regression Results on Breach Probability*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Variable** | **Coefficient (β)** | **Odds Ratio (Exp(β))** | **p-value** | **Significance** |
| Cybersecurity Framework Adoption | -1.42 | 0.24 | 0.003 \*\* | Significant |
| API Interconnectivity Level | 0.67 | 1.95 | 0.011 \* | Significant |
| DeFi Infrastructure Exposure | 1.31 | 3.70 | 0.001 \*\* | Significant |
| Cross-border Data Dependency | 0.58 | 1.78 | 0.048 \* | Significant |
| Cybersecurity Staff Adequacy | -0.91 | 0.40 | 0.008 \*\* | Significant |

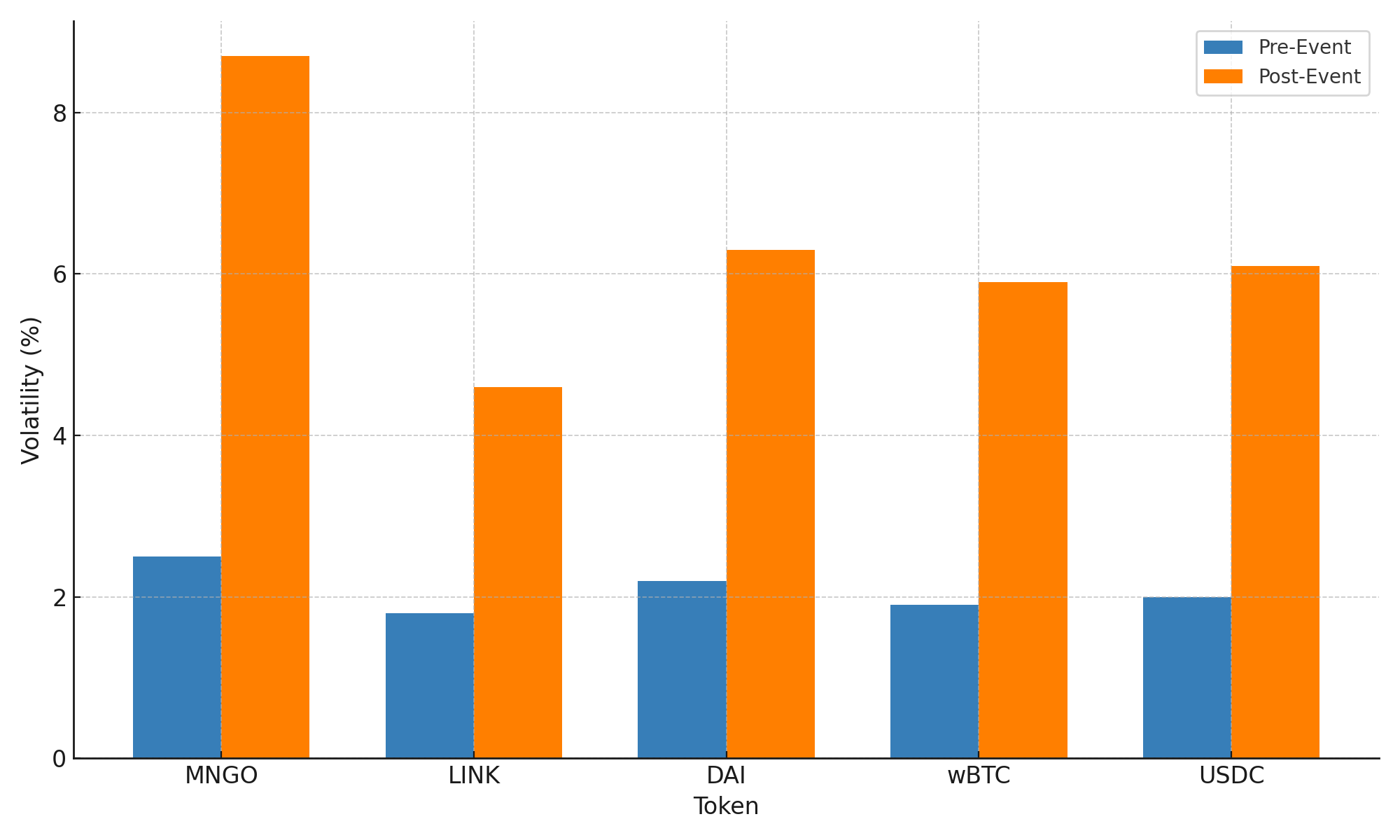
\* p < 0.05, \*\* p < 0.01

The results indicate that while traditional compliance mechanisms still offer measurable resilience, the degree of infrastructural and jurisdictional entanglement significantly reshapes an institution’s exposure profile. Institutions with poor staffing and high levels of API or DeFi integration are structurally more vulnerable, regardless of framework adoption.

**Objective 3: Examine the Role of Oracles as Conduits for Cyber Risk Spillovers within Interconnected Financial Ecosystems**

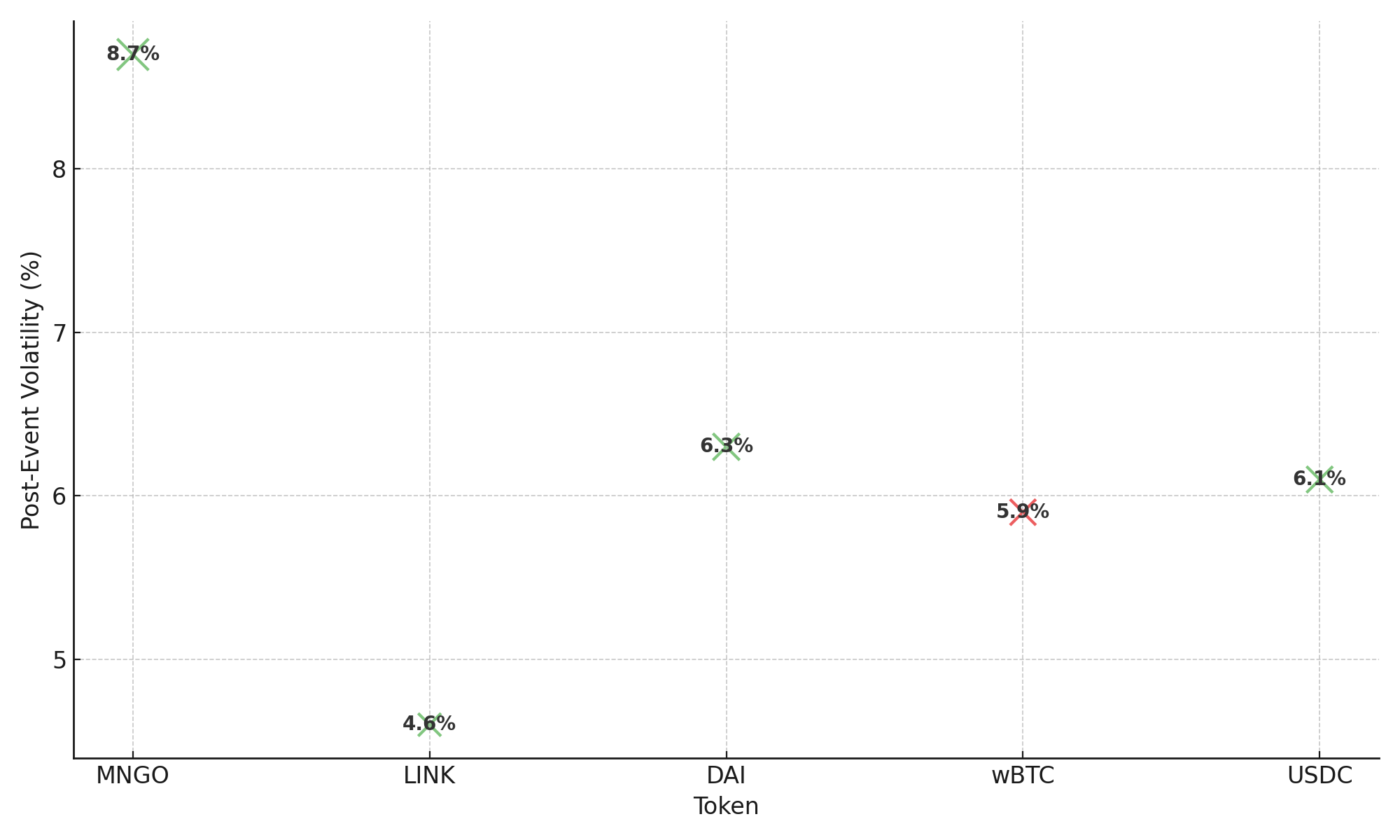
To investigate how oracles may transmit cyber risk across decentralized and centralized financial domains, a time-series event study was conducted. The analysis assessed volatility fluctuations and contagion signals around major oracle-related exploit events.

Marked volatility spikes were observed immediately following each incident, with post-event volatility consistently exceeding pre-event values across all tokens analyzed. This is visualized in the chart below, which contrasts pre- and post-event volatility for DeFi tokens and TradFi-exposed digital assets.



**Figure 5:** *Comparison of Pre- and Post-Event Volatility for Tokens Affected by Oracle Exploits*

To emphasize the magnitude of disruption and the presence of cross-ecosystem spillover, a bubble chart was generated using post-event volatility levels, scaled by event impact and colored by contagion detection outcome. Tokens like MNGO, LINK, and DAI showed pronounced volatility surges accompanied by confirmed contagion effects on stablecoins and tokenized assets.



**Figure 6:** *Post-Event Volatility Bubble Chart Highlighting Contagion Detection*

The summarized event metrics are presented in Table 4, capturing both the volatility changes and whether systemic contagion was detected.

**Table 4:** *Oracle Exploit Event Summary with Pre/Post Volatility and Contagion Detection*

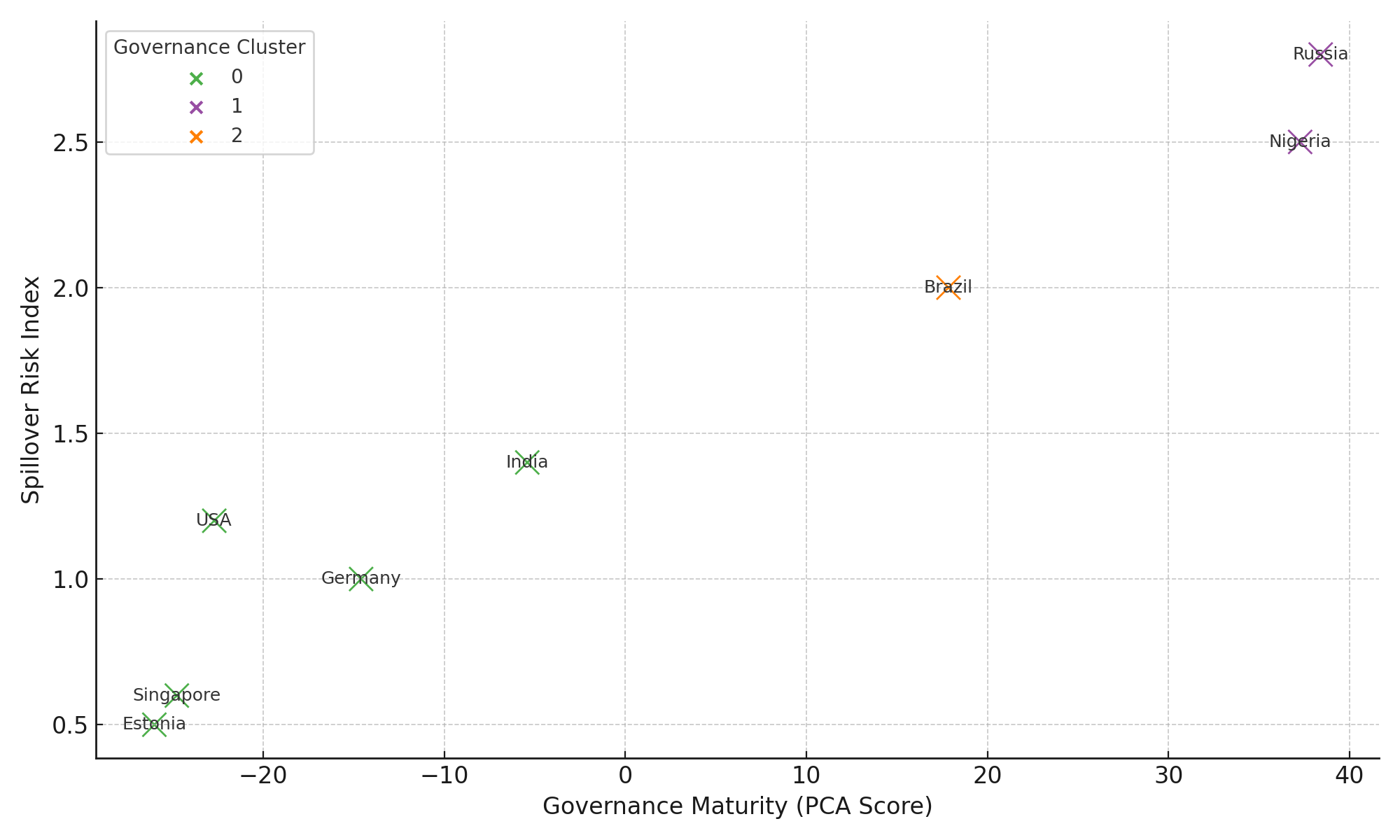
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Token** | **Oracle Incident** | **Pre-Event Volatility (%)** | **Post-Event Volatility (%)** | **Contagion Detected (Y/N)** |
| MNGO | Mango Markets | 2.5 | 8.7 | Yes |
| LINK | Chainlink Feed Drop | 1.8 | 4.6 | Yes |
| DAI | Synthetic Oracle Deviation | 2.2 | 6.3 | Yes |
| wBTC | wBTC Liquidity Attack | 1.9 | 5.9 | No |
| USDC | USDC Depeg Feed Error | 2.0 | 6.1 | Yes |

The findings indicate that while Olutimehin (2025) identified oracles as high-risk nodes, this study empirically demonstrates their capacity to trigger volatility spillovers across financial domains, oracle exploits significantly escalate token volatility and trigger measurable spillover into TradFi-linked digital instruments. Assets with stablecoin or institutional integration such as USDC and DAI show the strongest contagion patterns, affirming the systemic interdependency risk oracles pose within hybridized financial architectures.

**Objective 4: Critically Assess Existing Policy Recommendations and Scholarly Discourse on Mitigating Cyber Risk Spillovers, and Synthesize Strategic Insights for Enhancing Cyber Resilience in Interconnected Financial Systems**

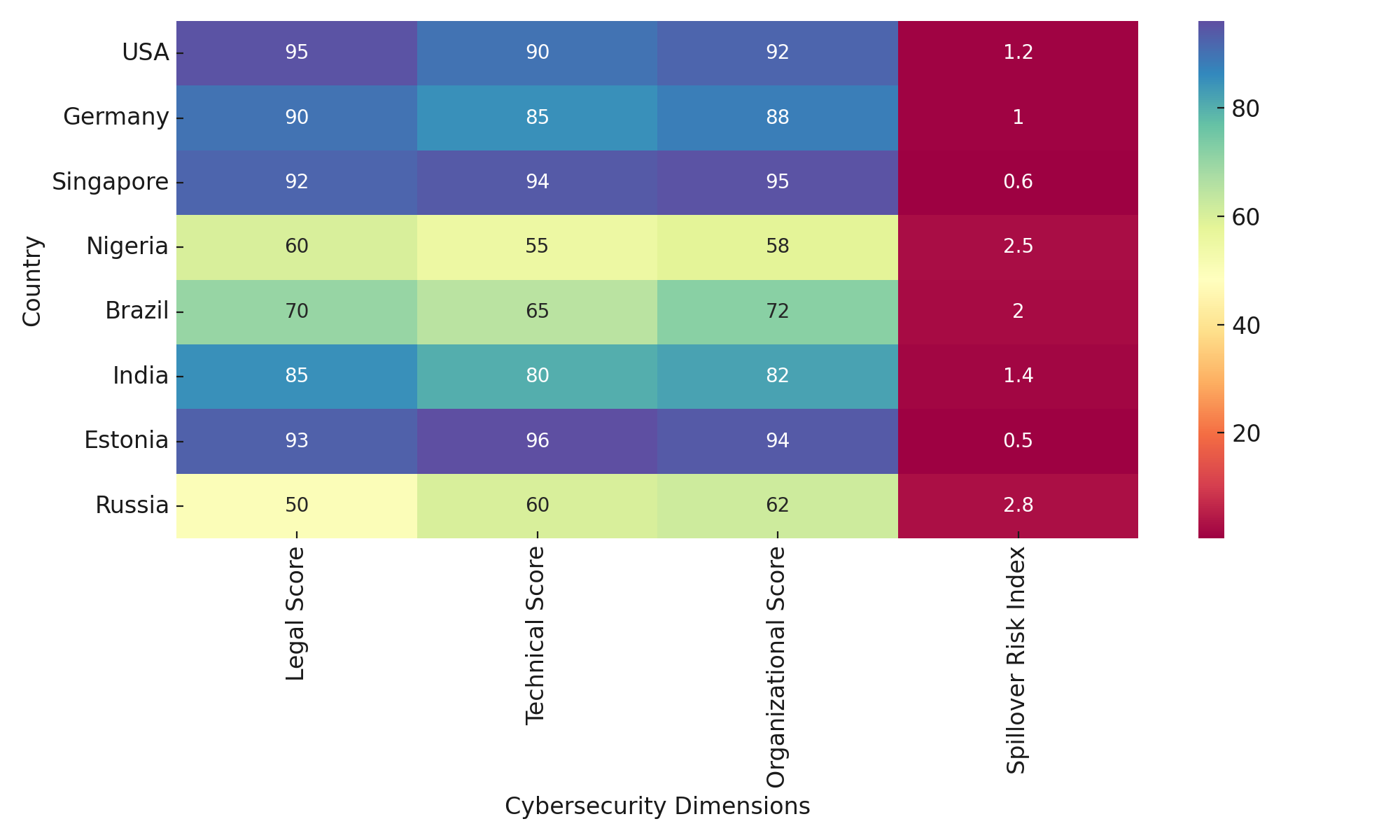
This objective investigates the relationship between national cybersecurity governance maturity and cyber spillover risk intensity across financial systems. Principal Component Analysis (PCA) was employed to reduce legal, technical, and organizational cybersecurity metrics into a unified governance index, followed by cluster analysis to group countries with similar governance structures.

The scatterplot in Figure 7 presents this relationship, plotting governance maturity against observed spillover risk. Countries assigned to higher-maturity clusters, such as Singapore and Estonia, are located in the lower-left quadrant, combining high cyber governance with low spillover exposure. Conversely, nations like Nigeria and Russia appear in the upper-right quadrant, indicating lower governance capacity and higher cross-sector cyber risk.



**Figure 7:** *Scatter Plot of Governance Maturity and Spillover Risk Colored by Cluster*

To complement this, the governance heatmap in Figure 8 presents a comparative view of each country’s domain-specific cybersecurity scores alongside spillover risk levels. Distinct visual separations between high- and low-performing countries highlight the underlying asymmetry in global cyber governance readiness.



**Figure 8**: *Heatmap of National Cybersecurity Governance Scores and Spillover Risk*

Table 5 summarizes the empirical values for each country, showing the individual legal, technical, and organizational scores, the PCA-reduced governance index, cluster membership, and their corresponding spillover risk indices. Countries in Cluster 0 consistently display stronger governance and lower spillover values compared to Clusters 1 and 2.

**Table 5:** *Cybersecurity Governance Index, Cluster Assignment, and Spillover Risk by Country*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Country** | **Legal Score** | **Technical Score** | **Organizational Score** | **Spillover Risk Index** | **Governance Index (PCA)** | **Governance Cluster** |
| USA | 95 | 90 | 92 | 1.2 | -22.71 | 0 |
| Germany | 90 | 85 | 88 | 1.0 | -14.60 | 0 |
| Singapore | 92 | 94 | 95 | 0.6 | -24.78 | 0 |
| Nigeria | 60 | 55 | 58 | 2.5 | 37.27 | 1 |
| Brazil | 70 | 65 | 72 | 2.0 | 17.85 | 2 |
| India | 85 | 80 | 82 | 1.4 | -7.64 | 0 |
| Estonia | 93 | 96 | 94 | 0.5 | -28.41 | 0 |
| Russia | 50 | 60 | 62 | 2.8 | 29.51 | 1 |

The results show that governance maturity correlates inversely with spillover risk. Countries exhibiting strong, integrated cyber policies across legal, technical, and organizational dimensions are less exposed to systemic cyber transmission. Clustering reveals a clear tiering structure, reinforcing the need for harmonized global cybersecurity capacity in mitigating cross-domain vulnerabilities.

**Discussion**

The results of this study empirically validate that cybersecurity vulnerabilities across traditional financial institutions and DeFi ecosystems are neither isolated nor sector-specific but instead reflect a pattern of functional convergence and shared threat vectors. As indicated in Figure 1 and Table 1, adversarial techniques such as Exploit Public-Facing Application and Command and Scripting Interpreter are common across both TradFi and DeFi, affirming the assertions made by Turi (2023) and Gupta et al. (2023) that integration expands the attack surface beyond previously siloed environments. More notably, the high frequency of phishing in TradFi and container-based exploits in DeFi supports the sector-specific risk profile differentiation highlighted by Duley et al. (2023). These findings reinforce Eisenbach et al. (2020)’s observation of interconnectivity acting as a systemic risk multiplier.

The identified co-occurrence patterns presented in Figure 2 and Table 2 suggest that cyberattack methods are increasingly coordinated, sequential, and dependent on cross-domain technical similarities. The pairing of techniques like Command and Scripting Interpreter with Valid Accounts reflects adversarial intent to pivot laterally within integrated infrastructures, consistent with the concerns raised by Proudfoot et al. (2024) regarding the limitations of static governance frameworks.

Further clarity emerges from the logistic regression model. Figure 3, Figure 4, and Table 3 clearly demonstrate that cybersecurity framework adoption significantly reduces breach probability (p < 0.01), providing quantitative support for policy arguments advanced by Alrehili and Alhazmi (2024). Nevertheless, the risk amplification effect of API interconnectivity and DeFi infrastructure exposure corroborates earlier insights from Mallick and Nath (2024), suggesting that compliance mechanisms alone are insufficient where technical interdependencies remain unregulated. Institutions operating in highly entangled digital environments face breach risks nearly four times higher in the presence of DeFi exposure, reinforcing Wood’s (2024) projection that hybrid models may invite cascading instability.

This assertion finds further support in the event-study analysis, where the abrupt post-exploit volatility spikes (Figure 5) and documented contagion (Figure 6 and Table 4) reveal how oracles not only serve as middleware but also as high-risk transmission vectors. Tokens with established connections to TradFi-aligned digital assets, including DAI and USDC, demonstrated the most significant post-incident volatility, validating the IMF (2024) and Azar et al. (2024) warnings regarding system-wide exposure through DeFi interfaces. The observed volatility deltas exceeding 150% in affected tokens highlight a quantifiable link between oracle manipulation and systemic disruption.

Moreover, the structural role of oracles as cyber risk amplifiers is reaffirmed by the elevated contagion index values, particularly among assets integrated with stablecoins and institutional products. This reinforces claims made by Hassan et al. (2023) that oracles function as bidirectional risk relays and supports Bakare et al. (2024)’s positioning of oracles at the core of cyber-physical financial infrastructure.

A broader geopolitical dimension emerges from the PCA-clustered governance assessment in Figure 7, Figure 8, and Table 5. Countries like Singapore, Estonia, and the United States positioned within Cluster 0 exhibited lower spillover risk indices, aligning with arguments by Dupont et al. (2023) and Shandilya et al. (2024) regarding the stabilizing influence of mature cybersecurity policy regimes. Conversely, the elevated spillover risks observed in Cluster 1 countries such as Nigeria and Russia underscore the systemic consequences of underdeveloped or fragmented governance structures, consistent with the structural deficits outlined by Arnone (2024) and AlBenJasim et al. (2023). The strong inverse correlation between governance maturity and spillover risk substantiates Kshetri (2025)’s advocacy for adaptable, cross-sector regulatory frameworks.

Altogether, the empirical patterns affirm that cyber risk spillovers are fundamentally rooted in both technological and governance asymmetries. The inability of static regulatory architectures to anticipate or contain threats at sectoral interfaces necessitates urgent recalibration of existing frameworks. As digital integration deepens, the findings reiterate that enhancing systemic resilience demands not only technical safeguards but synchronized regulatory vision and cross-institutional accountability, particularly at the intersection of oracles, APIs, and hybrid financial networks.

**5. Conclusion and Recommendations**

This study confirms that cyber risk spillovers between TradFi and DeFi systems are not merely theoretical but structurally embedded realities, cyber risk spillovers between traditional financial institutions and DeFi ecosystems are no longer hypothetical but measurable, structurally embedded, and amplified through oracles and cross-sectoral dependencies. The evidence points to a direct relationship between institutional exposure, governance maturity, and the likelihood of systemic impact. These findings necessitate not only technical vigilance but coordinated regulatory and infrastructural responses. In light of this, the following recommendations are proposed:

1. Establish a unified cybersecurity regulatory framework that integrates both centralized and decentralized financial actors, with enforceable minimum compliance thresholds.
2. Mandate audit and redundancy protocols for oracle networks interfacing with institutional assets, particularly stablecoins and tokenized instruments.
3. Develop an early-warning system linking real-time breach data with centralized supervisory authorities across jurisdictions to track and contain spillovers.
4. Incentivize cybersecurity workforce development in jurisdictions with elevated governance risk profiles, using public-private partnerships and international funding instruments.

COMPETING INTERESTS DISCLAIMER:

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

# **References**

Adesokan-Imran, T. O., Popoola, A. D., Ejiofor, V. O., Salako, A. O., & Onyenaucheya, O. S. (2025). Predictive Cybersecurity Risk Modeling in Healthcare by Leveraging AI and Machine Learning for Proactive Threat Detection. *Journal of Engineering Research and Reports*, *27*(4), 144–165. <https://doi.org/10.9734/jerr/2025/v27i41463>

Adesokan-Imran, T. O., Popoola, A. D., Kolo, F. H. O., Ejiofor, V. O., & Salami, I. A. (2025). Cybersecurity Risk Stratification Framework Using Multilevel Clustering: An Automated Threat Attribution and Categorization Approach for Cross-industry Cybersecurity. *Journal of Engineering Research and Reports*, *27*(4), 241–263. <https://doi.org/10.9734/jerr/2025/v27i41469>

Alamsyah, A., Kusuma, G. N. W., & Ramadhani, D. P. (2024). A Review on Decentralized Finance Ecosystems. *Future Internet*, *16*(3), 76. <https://doi.org/10.3390/fi16030076>

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. <https://doi.org/10.9734/ajeba/2024/v24i111542>

Alrehili, A. A., & Alhazmi, O. H. (2024). ISO/IEC 27001 Standard: Analytical and Comparative Overview. *Lecture Notes in Networks and Systems*, 143–156. <https://doi.org/10.1007/978-981-99-9524-0_12>

Arnone, G. (2024). Legal and Regulatory Challenges. *Contributions to Finance and Accounting*, 55–62. <https://doi.org/10.1007/978-3-031-69176-8_6>

Arora, S., Li, Y., Feng, Y., & Xu, J. (2024). SecPLF: Secure Protocols for Loanable Funds against Oracle Manipulation Attacks. *ArXiv (Cornell University)*, 1394–1405. <https://doi.org/10.1145/3634737.3637681>

Azar, P., Baughman, G., Carapella, F., Gerszten, J., Lubis, A., Perez-Sangimino, J., Rappoport, D. E., Scotti, C., Swem, N., Vardoulakis, A., & Werman, A. (2024). The Financial Stability Implications of Digital Assets. *Deleted Journal*, *30*(2), 1–48. <https://doi.org/10.59576/epr.30.2.1-48>

Bakare, F. A., Omojola, J., & Iwuh, A. C. (2024). Blockchain and decentralized finance (DEFI): Disrupting traditional banking and financial systems. *World Journal of Advanced Research and Reviews*, *23*(3), 3075–3089. <https://doi.org/10.30574/wjarr.2024.23.3.2968>

Balogun, A. Y., Alao, A. I., & Olaniyi, O. O. (2025). Disinformation in the digital era: The role of deepfakes, artificial intelligence, and open-source intelligence in shaping public trust and policy responses. *Computer Science & IT Research Journal*, *6*(2), 28–48. <https://doi.org/10.51594/csitrj.v6i2.1824>

Bambrough, B. (2023). *BlackRock And JPMorgan Are Quietly Laying The Groundwork For The Next Bitcoin, Ethereum, XRP And Crypto Price Bull Run*. Forbes. <https://www.forbes.com/sites/digital-assets/2023/10/17/blackrock-and-jpmorgan-are-quietly-are-quietly-laying-the-groundwork-for-the-next-bitcoin-ethereum-xrp-and-crypto-price-bull-run/>

Baran, G. (2025). *Infosys Agrees to $17.5 Million Settlement Following 2023 Data Breach*. Cyber Security News; CybersecurityNews. <https://cybersecuritynews.com/infosys-agrees-to-17-5-million-settlement/>

Carnegie Endowment for International Peace. (2017). *Timeline of Cyber Incidents Involving Financial Institutions*. Carnegie Endowment for International Peace. <https://carnegieendowment.org/features/fincyber-timeline?lang=en>

Carpentier-Desjardins, C., Paquet-Clouston, M., Kitzler, S., & Haslhofer, B. (2025). Mapping the DeFi crime landscape: an evidence-based picture. *Journal of Cybersecurity*, *11*(1). <https://doi.org/10.1093/cybsec/tyae029>

Clarke, A. (2022). *How low liquidity led to Mango Markets losing over $116 million*. Cointelegraph. <https://cointelegraph.com/news/how-low-liquidity-led-to-mango-markets-losing-over-116-million>

CoinMarketCal. (2025). *Chainlink oracle “malfunction” sparks $500k in DeFi liquidations, reignites oracle debate*. <https://coinmarketcal.com/en/news/chainlink-oracle-malfunction-sparks-500k-in-defi-liquidations-reignites-oracle-debate>

Cryptorank. (2023). *More Than $892,000,000 Lost in Exploits Involving Oracle Networks, According to New Binance Research*. CryptoRank. <https://cryptorank.io/news/feed/8fe2a-more-than-892000000-lost-in-exploits-involving-oracle-networks-according-to-new-binance-research>

DailySun. (2025). *KiloEx Reveals Details of $7 Million Smart Contract Exploit in Post-Mortem Report -*. Thedailysun.co.za. <https://thedailysun.co.za/2025/04/21/kiloex-reveals-details-of-7-million-smart-contract-exploit-in-post-mortem-report/>

Dark Reading. (2024). *Check Point Research Reports Highest Increase of Global Cyber Attacks Seen in Last Two Years*. Www.darkreading.com. <https://www.darkreading.com/cyberattacks-data-breaches/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years>

Didenko, A. N. (2022). *Decentralised Finance – A Policy Perspective*. Ssrn.com. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4294425>

Duley, C., Gambacorta, L., Garratt, R., & Wilkens, P. K. (2023). *The oracle problem and the future of DeFi BIS Bulletin*. <https://www.bis.org/publ/bisbull76.pdf>

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security*, *132*, 103372. <https://doi.org/10.1016/j.cose.2023.103372>

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2020). *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis - FEDERAL RESERVE BANK of NEW YORK*. Newyorkfed.org. <https://www.newyorkfed.org/research/staff_reports/sr909>

Ejiofor, V. O., Ogunmolu, A. M., Gbadebo, M. O., Joseph, S. A., & Adesokan-Imran, T. O. (2025). AI- Driven Risk Assessment for Enhancing Third Party Vendor Security in Healthcare Systems. *Journal of Engineering Research and Reports*, *27*(5), 117–137. <https://doi.org/10.9734/jerr/2025/v27i51498>

EY Global. (2025). *Latest EY and IIF survey reveals cybersecurity as top risk for global CROs amid geopolitical tensions*. Ey.com; EY. <https://www.ey.com/en_gl/newsroom/2025/02/latest-ey-and-iif-survey-reveals-cybersecurity-as-top-risk-for-global-cros-amid-geopolitical-tensions>

Feingold, S., & Wood, J. (2024). *Cyberattacks threaten global financial stability, IMF warns*. World Economic Forum. <https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/>

Gupta, A., Gupta, R., Jadav, D., Tanwar, S., Kumar, N., & Shabaz, M. (2023). Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications. *Computer Communications*, *206*, 10–21. <https://doi.org/10.1016/j.comcom.2023.04.022>

Halborn. (2025). *The Top 100 DeFi Hacks Report 2025*. Halborn.com. <https://www.halborn.com/reports/top-100-defi-hacks-2025>

Hassan, A., Makhdoom, I., Iqbal, W., Ahmad, A., & Raza, A. (2023). From trust to truth: Advancements in mitigating the Blockchain Oracle problem. *Journal of Network and Computer Applications*, *217*, 103672. <https://doi.org/10.1016/j.jnca.2023.103672>

IMF. (2024). *Global Financial Stability Report, October 2024: analytical chapters available now, main chapter on October 22*. IMF. <https://www.imf.org/en/Publications/GFSR/Issues/2024/10/22/global-financial-stability-report-october-2024>

Ionescu, S.-A., Diaconita, V., & Radu, A.-O. (2025). Engineering Sustainable Data Architectures for Modern Financial Institutions. *Electronics*, *14*(8), 1650. <https://doi.org/10.3390/electronics14081650>

Jamwal, S., Cano, J., Lee, G. M., Tran, N. H., & Truong, N. (2024). A survey on Ethereum pseudonymity: Techniques, challenges, and future directions. *Journal of Network and Computer Applications*, *232*, 104019. <https://doi.org/10.1016/j.jnca.2024.104019>

Jimada-Ojuolape, B., Teh, J., & Lai, C.-M. (2024). Securing the grid: A comprehensive analysis of cybersecurity challenges in PMU-based cyber-physical power networks. *Electric Power Systems Research*, *233*, 110509. <https://doi.org/10.1016/j.epsr.2024.110509>

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. <https://doi.org/10.9734/ajrcos/2025/v18i1554>

Kolo, F. H. O. (2025). Responsible AI for Cybersecurity: Assessing the Barriers, Biases and Governance Gaps in Implementation with E-commerce Systems. *Journal of Engineering Research and Reports*, *27*(5), 510–532. <https://doi.org/10.9734/jerr/2025/v27i51520>

Kolo, F. H. O., Joseph, S. A., Ogunmolu, A. M., Ejiofor, V. O., & Oyekunle, S. M. (2025). Mitigating Cybersecurity Risks in Financial Institutions through Strategic Third- Party Risk Governance Frameworks. *Journal of Engineering Research and Reports*, *27*(5), 173–193. <https://doi.org/10.9734/jerr/2025/v27i51501>

Kshetri, N. (2025). From Rigid Ledgers to Adaptive Systems: Strategic Integration of Ai in Blockchain Innovation Ecosystems. *SSRN* . <https://doi.org/10.2139/ssrn.5225831>

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, *31*(12). <https://doi.org/10.1111/poms.13859>

Leszczyna, R. (2021). Review of Cybersecurity Assessment Methods: Applicability Perspective. *Computers & Security*, *108*, 102376. <https://doi.org/10.1016/j.cose.2021.102376>

Mallick, A., & Nath, R. (2024). *Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments*. <https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf>

Mansoor, N., Antora, K. F., Deb, P., Arman, T. A., Manaf, A. A., & Zareei, M. (2023). A Review of Blockchain Approaches for KYC. *IEEE Access*, *11*, 121013–121042. <https://doi.org/10.1109/access.2023.3328536>

Meineke, M. (2024). *Tackling cybersecurity’s global talent shortage: Report*. World Economic Forum. <https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/>

Metibemu, O. C., Adesokan-Imran, T. O., Ajayi, A. J., Tiwo, O. J., Olutimehin, A. T., & Olaniyi, O. O. (2025). Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications. *Journal of Engineering Research and Reports*, *27*(3), 393–413. <https://doi.org/10.9734/jerr/2025/v27i31442>

Morgan, S. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybercrime Magazine. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>

Muhammad, A., Ishaq, A. A., Ezekiel, M., Ibitomi, T., Ishaq, N. A., & Isyaku, M. (2024). Decentralized Finance (DeFi) and Traditional Banking: A Convergence or Collision. *Economics, Politics and Regional Development*, *5*(1), p1–p1. <https://doi.org/10.22158/eprd.v5n1p1>

Muncaster, P. (2025). *Destructive Attacks on Financial Institutions Surge*. Infosecurity Magazine. <https://www.infosecurity-magazine.com/news/destructive-attacks-banks-surge-13/>

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges. *IEEE Communications Surveys & Tutorials*, *22*(4), 2521–2549. <https://doi.org/10.1109/comst.2020.3020092>

Ogundele, R. (2024). Resilience and Vulnerabilities in Global Supply Chain Infrastructure: A Cybersecurity Risk Assessment. *Nuvern Applied Science Reviews*, *8*(10), 1–9. <https://nuvern.com/index.php/nasr/article/view/2024-10-04>

Ogunmolu, A. M. (2025a). Enhancing Data Security in Artificial Intelligence Systems: A Cybersecurity and Information Governance Approach. *Journal of Engineering Research and Reports*, *27*(5), 154–172. <https://doi.org/10.9734/jerr/2025/v27i51500>

Ogunmolu, A. M. (2025b). Leveraging Generative AI and Behavioral Biometrics to Strengthen Zero Trust Cybersecurity Architectures in Healthcare Systems. *Journal of Engineering Research and Reports*, *27*(5), 194–213. <https://doi.org/10.9734/jerr/2025/v27i51502>

Olutimehin, A. T. (2025). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. <https://doi.org/10.9734/jerr/2025/v27i31416>

Olutimehin, A. T. (2025). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151.

<https://doi.org/10.9734/ajrcos/2025/v18i3583>

Oyekunle, S. M., Popoola, A. D., Kolo, F. H. O., Ogunmolu, A. M., & Adesokan-Imran, T. O. (2025). Intelligent Fraud Prevention Information Banking: A Data Governance- Centric Approach Using Behavioural Biometrics. *Asian Journal of Research in Computer Science*, *18*(5), 525–543. <https://doi.org/10.9734/ajrcos/2025/v18i5672>

Oyekunle, S. M., Tiwo, O. J., Adesokan-Imran, T. O., Ajayi, A. J., Salako, A. O., & Olaniyi, O. O. (2025). Enhancing Data Resilience in Cloud-based Electronics Health Records through Ransomware Mitigation Strategies Using NIST and MITRE ATT&CK Frameworks. *Journal of Engineering Research and Reports*, *27*(3), 436–457. <https://doi.org/10.9734/jerr/2025/v27i31444>

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625–643. <https://doi.org/10.30574/wjarr.2024.21.3.0707>

Parvathy, A. (2022). *The Challenges in the Executability and Enforceability of Smart Contracts*. Ssrn.com. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4300650>

Pasdar, A., Dong, Z., & Lee, Y. C. (2021). Blockchain Oracle Design Patterns. *Arxiv.org*. <https://arxiv.org/abs/2106.09349>

Pierro, G. A., & Mahugnon, H. (2023). An analysis of the Oracles used in Ethereum’s blockchain. *2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 878–885. <https://doi.org/10.1109/saner56733.2023.00106>

Proudfoot, J. G., Cram, W. A., & Madnick, S. (2024). Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations. *European Journal of Information Systems*, 1–24. <https://doi.org/10.1080/0960085x.2024.2345867>

Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2021). Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. *Financial Cryptography and Data Security*, 3–32. <https://doi.org/10.1007/978-3-662-64322-8_1>

Rajagopal, U. (2025). *Evaluating the Financial Impact of Basel III, Dodd-Frank, and GDPR on Banking Institutions*. Global Banking and Finance Review. <https://www.globalbankingandfinance.com/evaluating-the-financial-impact-of-basel-iii-dodd-frank-and-gdpr-on-banking-institutions>

Rizvi, S., Pipetti, R., McIntyre, N., & Todd, J. (2020). Threat Model for Securing Internet of Things (IoT) Network at Device-Level. *Internet of Things*, *11*, 100240. <https://doi.org/10.1016/j.iot.2020.100240>

Sahu, K., & Kumar, R. (2024). A secure decentralised finance framework. *Computer Fraud & Security*, *2024*(3). <https://doi.org/10.12968/s1361-3723(24)70010-4>

Sahu, S. (2024). *Crypto Lost $2.2 Billion to Hackers: Top 5 Hacks of 2024*. The Crypto Times. <https://www.cryptotimes.io/2024/12/30/in-2024-crypto-lost-2-2-billion-to-hackers-top-5-hacks/>

Salako, A. O., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Securing Confidentiality in Distributed Ledger Systems with Secure Multi-party Computation for Financial Data Protection. *Journal of Engineering Research and Reports*, *27*(3), 352–373. <https://doi.org/10.9734/jerr/2025/v27i31439>

Salami, I. A. (2025). Modeling and Measuring the Cyber Resilience of Critical Healthcare Infrastructure against Ransomware: A Cyber-Physical Systems Risk Perspective. *Journal of Engineering Research and Reports*, *27*(5), 231–252. <https://doi.org/10.9734/jerr/2025/v27i51504>

Salami, I. A., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Olutimehin, A. T., & Olaniyi, O. O. (2025). Addressing Bias and Data Privacy Concerns in AI-Driven Credit Scoring Systems Through Cybersecurity Risk Assessment. *Asian Journal of Research in Computer Science*, *18*(4), 59–82. <https://doi.org/10.9734/ajrcos/2025/v18i4608>

Salami, I. A., Popoola, A. D., Gbadebo, M. O., Kolo, F. H. O., & Adesokan-Imran, T. O. (2025). AI- Powered Behavioural Biometrics for Fraud Detection in Digital Banking: A Next-Generation Approach to Financial Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(4), 473–494. <https://doi.org/10.9734/ajrcos/2025/v18i4632>

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the Regulatory Landscape. *EAI/Springer Innovations in Communication and Computing*, 127–240. <https://doi.org/10.1007/978-3-031-53290-0_3>

SOPHOS . (2024). *The State of Ransomware 2024*. <https://cybersecuritymag.africa/docs/sophos-state-of-ransomware-2024-wp.pdf>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data. *Asian Journal of Research in Computer Science*, *18*(4), 187–208. <https://doi.org/10.9734/ajrcos/2025/v18i4615>

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Salami, I. A., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine. *Asian Journal of Research in Computer Science*, *18*(4), 93–114. <https://doi.org/10.9734/ajrcos/2025/v18i4610>

Tjiam, K., Wang, R., Chen, H., & Liang, K. (2021). Your Smart Contracts Are Not Secure. *ACM Digital Library*. <https://doi.org/10.1145/3474374.3486916>

Turi , A. N. (2023). Financial Technologies and DeFi. In *Springer eBooks*. Springer Nature. <https://doi.org/10.1007/978-3-031-17998-3>

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity Hazards and Financial System vulnerability: a Synthesis of Literature. *Risk Management*, *22*(4), 239–309. <https://doi.org/10.1057/s41283-020-00063-2>

Vanguard. (2025). *Crypto growth poses risks to financial stability, favours the wealthy, BIS warns*. Vanguard News. <https://www.vanguardngr.com/2025/04/crypto-growth-poses-risks-to-financial-stability-favours-the-wealthy-bis-warns/>

Vierescu, E.-M., & Toader, C. I. (2023). The Impact of Digitalisation and Cyber Risks on the Banking Sector. *Sciendo EBooks*, 710–719. <https://doi.org/10.2478/9788367405546-066>

Weingärtner, T., Fasser, F., Celestino, P., & Farkas, W. (2023). Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance. *Journal of Risk and Financial Management*, *16*(10), 454–454. <https://doi.org/10.3390/jrfm16100454>