Exploring Personalized Personnel Protection within Cybersecurity

Oludolamu Onimole[1][1], Austin James[2], Denzel A. Pryor[3], Angel-Khalil Jones[3], Xavier Palmer[4], Lucas Potter[4] and Jude Osamor[5]
[1]Independent Researcher, UK
[2]University of East London, UK
[3]Independent Researcher, USA
[4]BiosView Labs, USA
[5]Glasgow Caledonian University

oludolamuonimole@gmail.com (Corresponding author)
pryordlsa@gmail.com (Corresponding author)

Abstract: Due to their substantial cross-platform exposure, high-profile persons are disproportionately at danger as cyber threats grow across linked digital ecosystems. Most prior research has focused on discrete platform vulnerabilities; however, the ways in which interconnections across services create compound socio-technical hazards have received less attention. By taking a socio-technical systems approach, this study highlights a major flaw in current methods that treat users as a homogeneous population, despite notable differences in exposure and behaviour. The study identifies recurring vulnerability patterns and illustrates how coordinated adversarial activity leverages digital interdependencies to cause financial, reputational, and physical harm through a cross-sector analysis of five high-demand service categories, ranging from remote healthcare to on-demand gig services. It identifies recurring structural vulnerability configurations across sectors, demonstrating that risk stems from shared choices rather than platform specifics. This paper contributes a cross-platform vulnerability map, a socio-technical risk model for high-visibility individuals, and a unified framework linking adversarial behavior to privacy erosion across interconnected services, offering practical insights for developing targeted cybersecurity strategies. Findings show how attackers exploit digital interdependence to achieve blended online compromise, financial loss, reputational harm, and physical danger. The study concludes by proposing a paradigm shift to personalized, privacy-centric, multi-layered cybersecurity capable of safeguarding both high-profile and everyday users emphasizing the importance of adapting security measures to individual user needs while prioritizing the protection of sensitive information. This study employs a socio-technical systems framework, acknowledging that cybersecurity risk arises from the interplay of human behaviour, platform structures, and data flows, rather than from isolated technical vulnerabilities.

Keywords: Account takeover, Coordinated cyber-attacks, Cross-platform risk, High-profile individuals, Socio-technical vulnerabilities

1. Introduction

High-profile individuals represent a critical and differentiated target set within the contemporary digital service economy, increasingly subjected to complex, multi-stage cyberattacks orchestrated by organized criminal networks seeking financial exploitation, reputational compromise, and direct extortion. The defining vulnerability of this demographic stems not merely from reliance on single platforms, but from the necessity of engaging with a vast, interconnected ecosystem of digital services spanning social media, cloud infrastructure, financial technology, and on-demand services which dramatically expands their aggregate, compound attack surface. For targets with high visibility, a breach in one service often serves as the precursor to financial loss, severe reputational damage, or a physical safety risk across another. This systemic exposure is conceptually explored through the lens of Socio-Technical Systems (STS) theory, which asserts that systemic deficiencies originate from the dynamic misalignment between an organization's human and technical components (Walker et al., 2008). Traditional applications of STS in security often treat the human element as a homogeneous unit, thereby failing to account for the dramatic variations in exposure, risk tolerance, and digital conduct among individuals of high public profile. The present study refines the STS perspective by conceptualizing these individuals as differentiated, high-exposure risk nodes, whose unique digital footprint creates distinct vulnerabilities at the intersection of human behavior and platform interdependency (Malatji et al., 2019). The core objective of this study is to qualitatively synthesize existing literature to identify and structurally map the specific vulnerability pathways that emerge across five high-demand service categories. The paper contributes a cross-platform conceptual risk map, articulates a refined STS risk model emphasizing individualized exposure, and presents a framework linking cross-service adversarial exploitation to privacy erosion. Ultimately, this analysis underscores the urgent need for a paradigm shift toward personalized, privacy-centric cybersecurity

[1]Oludolamu Onimole and Austin James - Shared First Authorship

strategies capable of safeguarding differentiated users within an intrinsically interconnected threat environment.

1.1 Methodology and Study Design

This work is an exploratory, qualitative synthesis of the contemporary cyber threat landscape, focusing on high-exposure targets. It is fundamentally a structural exploration, not a systematic review, designed to map converging threat vectors that emerge from digital interdependencies. The overall procedure was structured around five key elements:

(a) Conceptual Framework: We adopted an adapted Socio-Technical Systems (STS) approach, conceptualizing high-profile individuals as differentiated, high-exposure "risk nodes" within a complex ecosystem. The framework's primary function was to guide the structural exploration by identifying vulnerabilities arising from the interplay between user behaviors, platform data flows, and heightened digital exposure.

(b) Sector Selection Criteria: Five service categories - Gig Services, Digital Content, Fintech, E-Learning, and Remote Healthcare were purposefully selected based on their high demand, the volume of sensitive Personally Identifiable Information (PII) and financial data they process, and their critical role in the daily lives of high-visibility users.

(c) Data Collection and Scope: Data was gathered via an unstructured collection and interpretative review of secondary sources published primarily between 2014 and 2024. Sources included academic papers, industry threat reports, and analyses of documented cyber incidents, utilized to construct a foundational map of the contemporary threat landscape.

(d) Analytical Synthesis: The collected sources were subjected to a qualitative, interpretative synthesis focused on identifying and aggregating recurrent vulnerability patterns described in the literature. This process informed the construction of a cross-platform conceptual risk visualization and the development of a socio-technical risk model. No formal coding or systematic protocol was applied to the unstructured data collection.

(e) Case Studies (Constructed Scenarios): Four case studies were developed as constructed, hypothetical scenarios (referred to as "plausible routes"). These scenarios are designed to illustrate the potential financial, reputational, and physical consequences of converging threat vectors, serving as conceptual models rather than real-world empirical demonstrations.

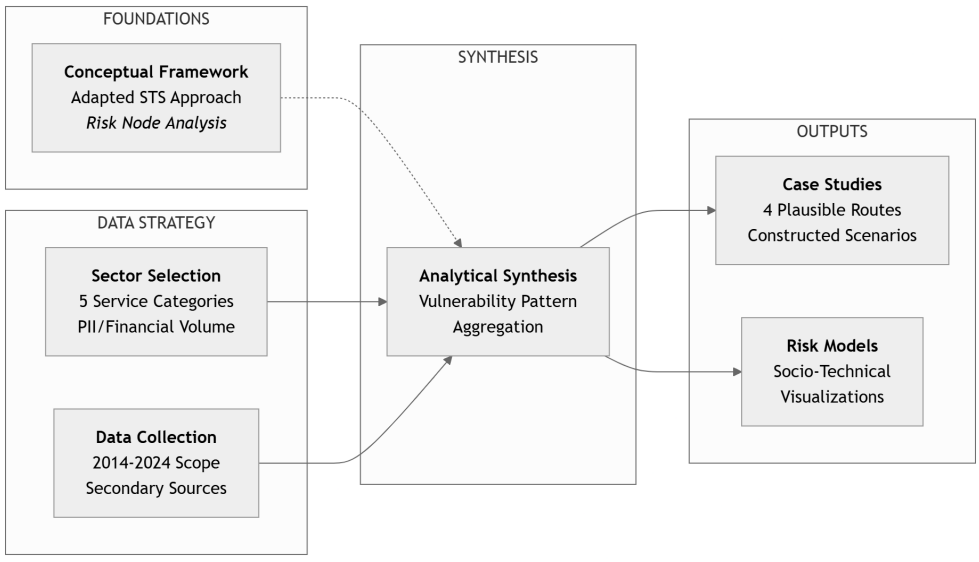

Figure 1: Overview of the study's methodological workflow from conceptual foundations to outputs

2. Analysis of Vulnerabilities Across Service Categories

Table 1: Cross-Sector Cyber Vulnerabilities and Criminal Utility. This matrix maps technical attack vectors to their socio-economic consequences across five domains. It highlights the transition from data-centric losses to cyber-physical threats, illustrating that modern breaches now directly jeopardize financial stability, personal privacy, and human life

Service Category	Primary Attack Vectors	Primary Criminal Utility	Security & Real-World Impact
Digital Content & Subscriptions	Credential Stuffing, Zero Day exploits in legacy servers (FTP)	IP Theft & Account Resale: Authorized publication of media / code, Double extortion ransomware	High financial loss; competitive erosion; reputational damage via leakage
Fintech & Payments	Sim-swapping, Deepfake, Phishing, API exploitation, credential stuffing	Asset Exfiltration: Rapid transfer of funds / crypto; Market manipulation (pump and dump)	Immediate financial devastation for individuals; systemic risk to financial trust
On-Demand Gig Services	Insider threats (Admin access), Database compromise	Physical surveillance: mapping location history, home/work address for stalking	High physical/psychological danger; direct threat to life and personal safety
E-Learning & Skill Acquisition	Poor API security, SQL Injection, Malware via course files	Psychographic profiling: Building identities for "Synthetic fraud" and lateral movement into corporate networks	Long-term identity theft; lateral movement into more sensitive sectors (Gov/Fin)
Remote Healthcare (Telemedicine / OT)	RAAS (Ransomware-as-a-Service), OT malware (Surgical Robots)	Extortion & sabotage: "Shame-based" blackmail of private records; physical interference with surgery	Life-and-death risk; severe psychological trauma; massive HIPAA/legal penalties

2.1 Category 1: On-Demand Gig Services (e.g., Rideshare, Food Delivery, Tasking)

The most widespread attack here is Credential Stuffing, which exploits users' habit of reusing passwords across services by leveraging lists of compromised credentials to perform automated login attempts (Nathan, 2020). Successful stuffing leads to an Account Take Over (ATO) with critical consequences (Wang and Reiter, 2020; El-Taj, Hamedah and Saeed, 2025). ATO grants access to sensitive data, including user behavior, viewing history, and, for B2B software, confidential business plans, representing a direct compromise of corporate or individual privacy (Nathan, 2020). It also enables billing fraud, in which criminals may change subscription tiers, purchase in-app content, or use a legitimate account to test stolen credit cards, resulting in financial loss for the subscriber and reputational damage to the service provider. Furthermore, ATO facilitates intellectual property theft by premium providers, allowing criminals to download source code, proprietary algorithms, unreleased media, or client lists, thereby fuelling sophisticated criminal activities such as corporate espionage and competitive sabotage (Walton, 2023; Meurs et al., 2024).

2.2 Category 2: Criminal Network Utility

The ultimate goal of a cyberattack is the monetization of compromised data or system access, which, for digital content and subscription services, takes several high-impact forms. One method is Ransomware on Intellectual Property (IP), utilizing a "double extortion" tactic where criminals first exfiltrate IP (e.g., source code, unreleased films) and then threaten its publication or sale unless a ransom is paid, leveraging the company's fear of competitive disadvantage and reputational harm (Meurs et al., 2024). A second utility involves blackmail using private content obtained through ATO attacks, where access to deeply personal data in communication channels or cloud storage is weaponized to blackmail high-profile victims, forcing substantial payments to prevent the exposure of embarrassing or confidential information (Al Habsi, Butler and Percy, 2023). Finally, unauthorized publication for financial gain is a straightforward monetization route, including the resale of stolen premium accounts on dark web marketplaces and the theft and unauthorized sale of unreleased IP, directly undercutting the legitimate business model and causing significant lost revenue (Shu et al., 2020; Kramer, Streicher and Niemietz, 2025). The diversity and severity of these criminal utilities underscore the critical need for robust security measures, such as multi-factor authentication (MFA) and continuous monitoring, in the digital content industry.

2.3 Category 3: Fintech (Financial Technology – e.g., Digital Banking, Trading Apps, Payments)

The primary vectors for cyberattacks in the Fintech space blend technical exploits and social engineering, targeting end users or their account credentials. Phishing remains highly effective, evolving into sophisticated spear-phishing that uses deepfake technology to target privileged accounts for login credentials, MFA codes, or cryptocurrency seed phrases (Li et al., 2020; Berrios et al., 2023). Research highlights that psychological manipulation in phishing exploits user trust, a trust that is disproportionately high in mobile-first Fintech environments (Ali, Dida and Sam, 2020). Furthermore, while two-factor authentication (2FA) via SMS is a security boon, the underlying mobile infrastructure is systematically exploited through SIM swapping (or SIM jacking), in which criminals socially engineer a mobile carrier into porting the victim's number (Kim et al., 2022). This provides an effective bypass of SMS-based 2FA and enables rapid account takeover, leveraging the weak link in the telecommunications provider rather than the fintech application itself (Mokhtar et al., 2023). Beyond direct theft, criminals exploit high-frequency trading and consumer investment applications to engage in subtle manipulation, including coordinated "pump-and-dump" schemes. This aligns with broader findings on how organised crime leverages market vulnerabilities to distort financial systems (Mesioye, 2025). and exploiting API security to manipulate trades, unauthorized liquidations, or target opaque instruments like derivatives. The difficulty of detection is compounded by the volume of legitimate algorithmic trades.

2.4 Category 4: E-Learning and Skill Acquisition (e.g., Online Courses, Tutoring)

Since 2020, the E-Learning sector (MOOCs, virtual tutoring, and corporate training) has grown, simultaneously increasing digital security and privacy risks, making these platforms prime targets for criminal networks due to the extensive personal, financial, and behavioral data they hold (Al-Mekhlafi et al., 2020; Waelchli & Walter 2025). Vulnerabilities include user-level compromise, often via credential stuffing exploiting password reuse, platform-level breaches, and pedagogical manipulation with compromised enrollment credentials grant access to academic progress and personal data (Wang and Reiter, 2020; Sahin & Li, 2021). Platform breaches via poor API security or SQL injection expose data, allowing criminals to construct detailed psychographic profiles for successful, personalized social engineering (Oliveira and Fiser, 2024). Internal trust is exploited to distribute malware via seemingly innocuous files (Al-Mekhlafi et al., 2020; Kumar, Sai and Radhika, 2026). The gained data serves multiple high-value objectives: psychographic profiles enable contextualized spear-phishing, and behavioral data is critical for synthetic identity fraud, enabling credible mimicry for schemes like business email compromise (Suthar, 2026). Ultimately, a compromised e-learning account serves as a stepping stone for lateral movement into more critical domains (corporate, government, financial) by exploiting linked primary email addresses to reset passwords (Al-Mekhlafi et al., 2020). The E-Learning sector is a lucrative frontier for criminal networks, transforming educational portals into high-yield targets for multi-stage cyberattacks, underscoring the urgent need for enhanced security and user education (Jawaid, 2023; Waelchli & Walter, 2025).

2.5 Category 5: Remote Healthcare (Telemedicine – e.g., Virtual Visits, Online Therapy, and Robotic Surgery)

Criminal networks highly value remote healthcare vulnerabilities due to data sensitivity and service criticality. Telemedicine data, especially regarding stigmatized conditions, is potent for "shame-based" extortion, targeting high-net-worth individuals for substantial cryptocurrency ransoms (Prasad et al., 2025; Meurs et al., 2024). The RaaS model favors healthcare facilities, where encrypting EHRs and clinical systems compel rapid ransom payment to restore patient care (Anderson et al., 2019). The unique threat posed by robotic surgery enables sophisticated actors to cause physical harm through sabotage or to demand an ultimatum by threatening to interfere with a procedure (e.g., locking the robotic arm) in exchange for an immediate ransom (Amos, 2024; Ludvigsen and Nagaraja, 2022). This transforms utility from mere financial gain to the achievement of significant physical and political objectives.

Table 2: Synthesis of categories showing attack vectors, Assets targeted and Criminal utility plus impact

Service Category	Attack Vectors & Vulnerabilities	Assets Targeted	Criminal Utility & Impact
On-Demand Gig Services	Credential stuffing exploiting password re-use leading to Account Takeover (ATO)	User accounts, payment data, confidential business plans	Billing fraud, card testing, account resale, IP theft; scalable attacks causing financial loss and reputational damage
Criminal Network Utility	Ransomware, data exfiltration, reuse of compromised accounts	Intellectual property, private content, premium accounts	Double extortion (ransom + leak), blackmail, dark web resale; high financial and reputational damage
Fintech	Phishing (incl. deepfake), SIM-swapping, social engineering + telecom weaknesses	Bank accounts, crypto wallets, trading systems	Financial theft, unauthorized trades, market manipulation
E-Learning & Skill Acquisition	Credential stuffing, SQL injection, API flaws, malware via trusted channels; rich behavioural data exposure	Academic data, psychometric profiles, emails	Identity fraud, spear-phishing, lateral movement into other sectors; enables multi-stage attacks
Remote Healthcare (Telemedicine / OT)	Ransomware, system/device exploitation; high sensitivity & critical infrastructure	EHRs, clinical systems, sensitive patient data	Ransomware (RaaS), shame-based extortion, potential physical harm; highest severity including life-threatening consequences

3. The Converging Vectors of Digital Threat: An Analysis of Sophisticated Cyberattack Methodologies Targeting High-Value Individuals

The digital lives of high-value individuals (HVIs) comprise a mosaic of vulnerabilities scattered across multiple platforms. This distributed footprint facilitates brand management but provides sophisticated actors with a broad surface for exploitation. Rather than isolated events, the four vectors analyzed below: cross-platform credential exploitation, advanced social engineering, supply chain attacks, and insider threats, function as interlocking components of modern cyber espionage. These methodologies are underpinned by advancements in data aggregation and artificial intelligence (Prasad et al., 2025).

The following synthesis reveals a dangerous convergence: technical exploits (IT) increasingly impact physical systems (OT) and human safety. While credential stuffing remains the primary "low-effort" entry point, sectors like Gig Services and Healthcare show a "physical pivot", where data breaches serve as precursors to stalking or surgical interference. Ultimately, while some attacks seek data for its own sake, most aim for rapid monetization through ransom, blackmail, or asset theft.

3.1 Cross-Platform Credential Exploitation: The Weakness of Password Reuse

Credential stuffing exploits the systemic habit of password reuse; a breach on an obscure site can unlock a principal's core accounts as botnets automate the testing of stolen login pairs across thousands of unrelated services (Pal et al., 2022; Ali, Dida & Sam, 2020). While Multi-Factor Authentication (MFA) provides a defense, actors increasingly bypass these controls via SIM-swapping or session hijacking, maintaining exploitation as a persistent threat (Kim et al., 2022).

3.2 Advanced Social Engineering: Psychological Manipulation in the AI Era

Modern social engineering has evolved from generic phishing into highly personalized attacks. By aggregating data to build a psychological profile, actors use "whaling" techniques to create urgent, fear-based narratives that bypass judgment (Kumar, M., Sai, D. and Radhika, M., 2026; Gonzaga et al., 2026). Generative AI and deepfake audio, trained on publicly available recordings, allow attackers to impersonate trusted contacts to intercept MFA codes or authorise fund transfers (Malik et al., 2022).

3.3 Supply Chain Attacks: Targeting the Digital Periphery

Supply chain attacks bypass the hardened security of major platforms by targeting the "weakest link": third-party vendors. For HVIs, this includes PR firms, financial advisors, and gig workers who hold legitimate, high-level access to core accounts. Because smaller firms often lack robust cybersecurity budgets, they offer a simpler entry point. This "inherited risk" means that an HVI's security is only as strong as that of their least secure partner (Ilori, Nwosu and Naiho, 2024). The gig economy exacerbates this, as temporary contractors often use personal, unmonitored devices for professional tasks.

3.4 Insider Threats: The Human Element of Breach

Insider threats from employees or associates are uniquely difficult to mitigate because they bypass perimeter defenses using authorized credentials (Whitelaw, Riley and Elmrabit, 2024). In the context of HVIs, this includes platform moderators or customer service agents who may be bribed by organized crime to execute account takeovers or provide real-time location data (Almukheiran and Li, 2020). Mitigation relies on behavioral analytics to detect anomalous access patterns such as a billing clerk accessing private messages - alongside rigorous vetting and psychological screening.

The preceding synthesis of these four primary attack vectors demonstrates a dangerous convergence of technical and human vulnerabilities, confirming that the risk is systemic rather than platform-specific. To illustrate the severe, compounding nature of these threats, the following section presents a series of constructed, hypothetical case studies that translate these systemic weaknesses into tangible financial, reputational, and physical harms. Figure 2 presents the cross-platform vulnerability map derived from the converging attack vectors outlined in this section, illustrating how sector-specific weaknesses accumulate into systemic socio-technical risk.

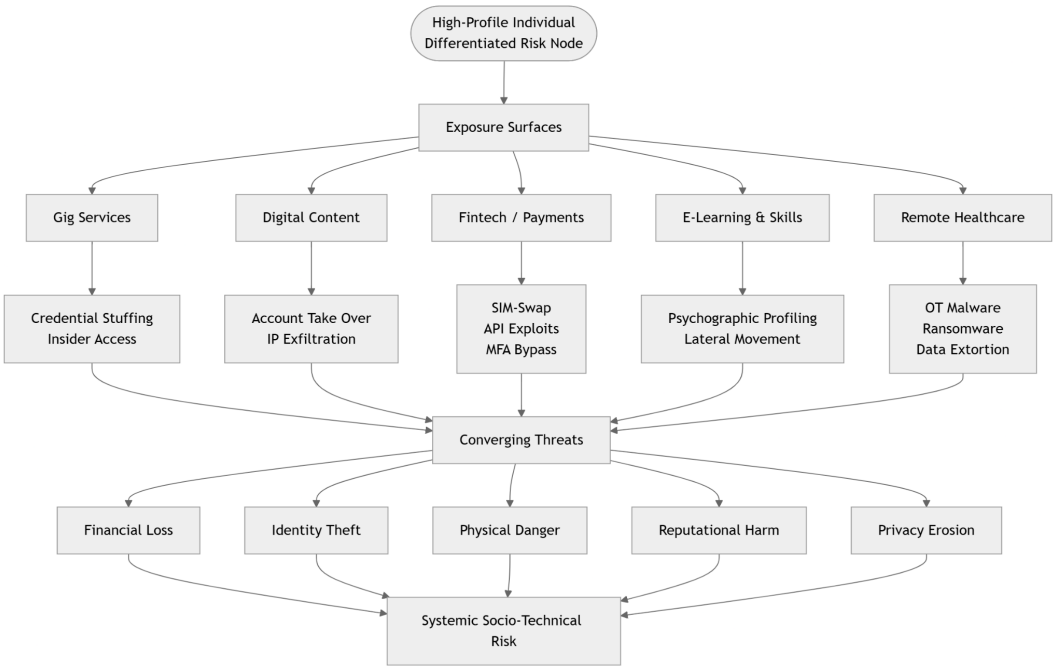

Figure 2: CrossPlatform Vulnerability Map

The cross-platform vulnerability map in Figure 2 shows how distinct weaknesses across gig services, digital content, fintech, elearning, and healthcare converge into shared adversarial pathways. It illustrates that modern cyber risk emerges not from isolated platform failures but from the compounding effects of crossservice interdependencies.

4. Hypothetical Case Studies

All four case studies presented in this section are explicitly constructed, hypothetical scenarios. They are not drawn from specific real-world incidents, nor do they represent anonymised reports of actual events. As disclosed in the methodology (Section 1.1e), these scenarios were developed as "plausible routes" as conceptual models grounded in empirically documented attack patterns and supported by the peer-reviewed

literature cited throughout Sections 2 and 3. Each scenario illustrates the potential financial, reputational, legal, and physical consequences of converging threat vectors, serving as illustrative demonstrations rather than reports of verified incidents. The use of constructed scenarios is a recognised methodological approach in qualitative and exploratory cybersecurity research, where real incident data is frequently unavailable due to non-disclosure agreements, ongoing legal proceedings, or victim anonymity requirements. Their validity as analytical tools rests on the fidelity of the underlying threat intelligence rather than the empirical occurrence of any specific event. Accordingly, the scenarios should be interpreted as conceptual demonstrations that translate the structural vulnerabilities identified in the preceding analysis into tangible, plausible harm pathways. Readers seeking empirical incident data are directed to the primary sources cited within each sub-section.

4.1 Example 1: Ransomware Attack Linked to Digital Content Service Compromise

In a hypothetical scenario, a major Digital Content Service (DCS) falls victim to a sophisticated ransomware attack triggered by a zero-day vulnerability in a third-party vendor's legacy FTP server. In this case, attackers successfully exfiltrate petabytes of sensitive data, including unreleased original content, proprietary algorithms, and extensive subscriber PII such as geographic data and payment details. The subsequent deployment of ransomware paralyzes content delivery, leading to catastrophic financial losses from system rebuilding and subscriber churn. Beyond the technical breach, the company faces global class-action lawsuits for GDPR violations, while the exposure of personal viewing histories creates a long-term risk of personalized spear-phishing against its high-profile users. This scenario illustrates how a single weak link in a complex supply chain can evolve from a simple data leak into a crisis of operational paralysis and competitive erosion.

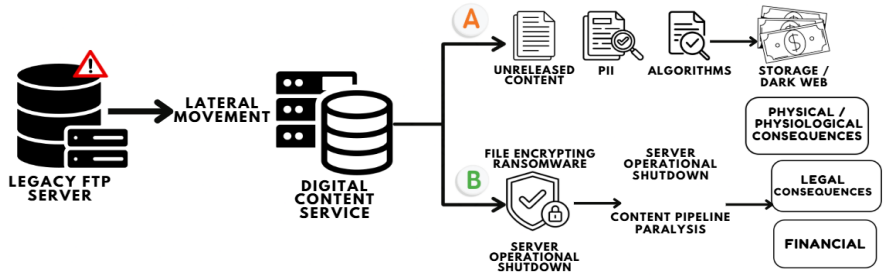

Figure 3: Multi-Vector Impact Model of a Supply Chain Ransomware Attack

4.2 Example 2: Financial Fraud via Fintech Account Takeover and SIM-Swapping

In this hypothetical scenario, attackers socially engineer a carrier representative into porting a victim's phone number, thereby intercepting all SMS-based two-factor authentication (2FA) codes. By pairing these with credentials harvested from a prior third-party breach, the criminals bypass the Fintech app's defenses to execute substantial transfers to untraceable cryptocurrency wallets. This rapid capital flight - depleting the victim's liquid assets in under three hours - demonstrates the "Achilles' heel" of SMS-based 2FA. The resulting financial devastation underscores a systemic vulnerability at the intersection of telecommunications and financial technology, necessitating a shift away from SMS-dependent verification channels.

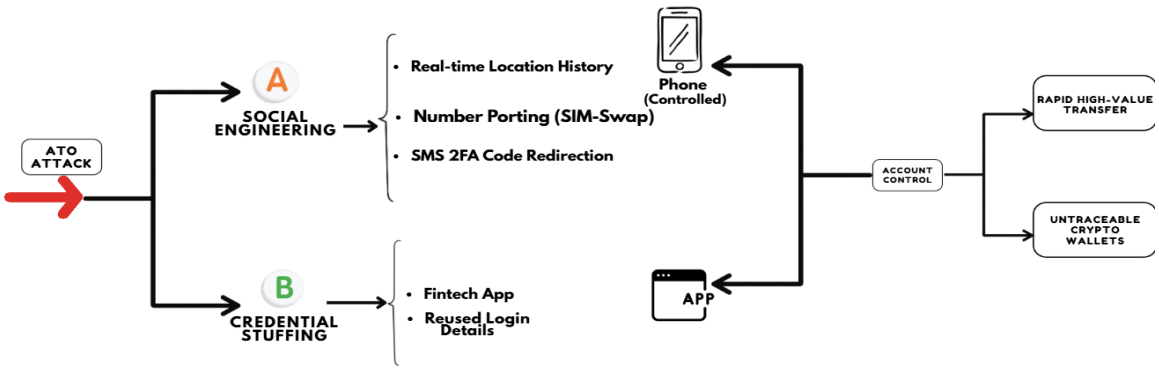

Figure 4: Systemic Vulnerability Matrix in Fintech Account Takeover (ATO)

4.3 Example 3: Stalking/Physical Threat Derived from On-Demand Gig Service Data

In a hypothetical scenario, a high-profile user of a popular on-demand gig service falls victim to a targeted stalking incident facilitated by a significant internal security failure. In this case, a disgruntled former employee leverages retained high-level administrative access to compromise the service's customer and driver database. The perpetrator gains access to highly granular data, including the victim's real-time location history, home and work addresses, and private contact numbers. This intimate data allows the stalker to anticipate the victim's movements, escalating the threat from electronic harassment to direct physical confrontation and creating a sustained environment of fear. This scenario illustrates how a digital breach can transition from abstract data loss directly into the domain of physical safety, necessitating immediate life changes for the victim. For the Gig service provider, the incident results in profound reputational damage and legal challenges arising from a failure of their duty of care, underscoring that location data is often the most dangerous form of compromised information.

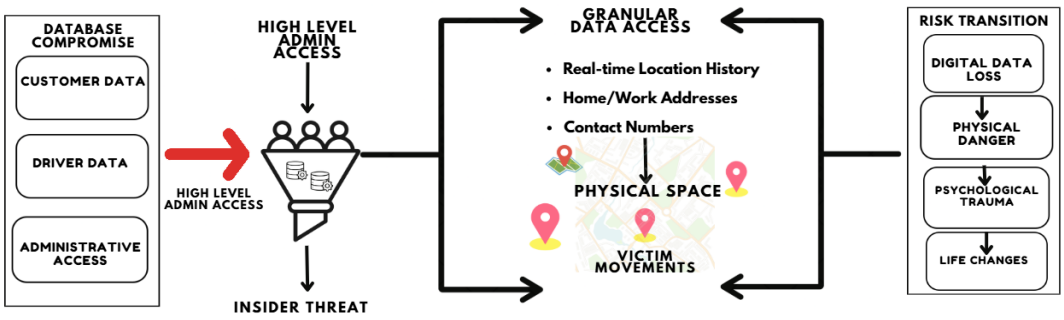

Figure 5: Cyber-Physical Risk Transition Map: Insider Threat and Stalking

4.4 Example 4: Disruption of Robot-Assisted Surgery and Data Leak

In a hypothetical scenario, a politically motivated cyber-attack targets a hospital network during a robot-assisted surgery. In this case, malware is injected into the surgical robot's control system, causing momentary latency and precision failures. Simultaneously, attackers breach the EHR system, stealing the celebrity patient's medical history and genetic data. The incident places the patient in immediate physical danger, highlighting the life-and-death stakes in healthcare OT security. Furthermore, the hospital faces severe legal consequences, including massive HIPAA fines and criminal investigations, following the public data leak. This case illustrates that in connected medical environments, a digital breach is also a physical safety incident, necessitating a paradigm shift toward active risk management of patient safety.

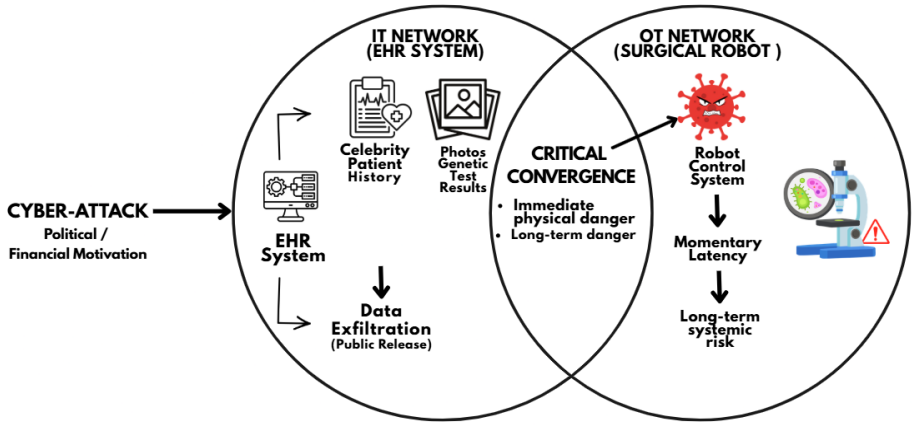

Figure 6: Convergence of IT and OT in Healthcare Cyber-Attacks.

These four examples (Figs. 1-4) collectively illustrate the potential breadth of cyber risk, ranging from financial and corporate liabilities to plausible physical and psychological harm to individuals, further establishing cybersecurity as a core societal and public safety concern.

Together, these four scenarios illustrate how the sector-specific vulnerabilities identified in Section 2 and the converging attack vectors synthesised in Section 3 manifest as real-world financial, reputational, and physical harms. This progression from sector analysis to methodological convergence to applied scenarios sets the foundation for the following discussion of systemic implications and mitigation strategies.

5. Discussion, Mitigation Strategies, and Future Research

This study's qualitative synthesis of the contemporary cyber threat landscape confirms that the risks facing high-profile individuals are fundamentally systemic, stemming from the convergence of cross-platform vulnerabilities and the complex interplay of digital service dependencies. The constructed case studies illustrate that a digital security failure in one domain (e.g., Gig Services or Fintech) acts as a vector that can translate abstract data loss into severe, tangible consequences, including financial ruin, reputational damage, and physical safety threats. This necessitates a strategic shift from generic, perimeter-focused security to a personalized, multi-layered defense posture that addresses the socio-technical vulnerabilities unique to high-exposure risk nodes.

Mitigation strategies must be simultaneously applied across three interdependent domains:

Individual Defense: For high-exposure individuals, fundamental proactive security (von Solms & van Niekerk, 2013) must transition from simple password strength (Berrios et al., 2023; Suthar, 2026) to mandatory, hardware-based two-factor authentication (2FA) (FIDO2/WebAuthn). This measure is paramount for defeating advanced social engineering and mitigating SIM-swapping attacks that bypass weaker SMS-based 2FA (Mokhtar et al., 2023). Furthermore, targeted security training must explicitly focus on the human factors that remain the weakest link, including social engineering and supply chain risk awareness (Indira, 2025; Waelchli and Walter, 2025).

Digital Service Provider (DSP) Measures: DSPs must counter supply chain and insider threats, the principal vectors for high-profile compromise, by implementing stringent organizational controls. Technical measures such as micro-segmentation and strict role-based access controls (RBAC) are essential for limiting the blast radius of any breach and preventing lateral movement into sensitive user data (Kuo et al., 2020). Continuous anomaly monitoring of internal access patterns is also critical for detecting malicious insider activity that exploits legitimate credentials (Jongh et al., 2025; Sharma, 2021).

Regulatory and Legal Frameworks: The transnational nature of organised cybercrime requires a robust legal framework. This includes stricter enforcement of data protection laws like GDPR and HIPAA, coupled with heightened penalties to deter actors in critical sectors (Coupland, 2025). Enhanced international cooperation is required to streamline information sharing, close jurisdictional loopholes, and harmonize standards for evidence collection in transnational cybercrime cases (Cerezo, Lopez and Patel, 2007; Coupland, 2025). In conclusion, this

analysis underscores the critical vulnerabilities inherent in the widespread use of internet-connected services, particularly for high-profile individuals. The findings advocate for a tailored cybersecurity posture that is responsive to individual digital conduct and the cross-platform dependencies that create compound risk.

Future research should operationalize the socio-technical risk model by developing measurable indicators of cross-platform exposure, behavioral vulnerability, and inherited supply-chain risk, and empirically validate the pathways identified in this qualitative synthesis. Studies are also warranted to explore the impact of artificial intelligence and machine learning for both adversarial tools and defense-in-depth solutions. Furthermore, research should examine personalized security interventions for high-visibility users, such as hardware-based authentication and identity compartmentalization, and inform policy frameworks through interdisciplinary research combining cybersecurity, behavioral science, and digital governance.

6. Limitations

This work is subject to several methodological and conceptual limitations that should be acknowledged. First, the data collection process was structured as an unstructured, qualitative synthesis rather than a systematic review; as such, no formal coding protocol or systematic search criteria were applied to the secondary sources. This exploratory approach may lead to the omission of relevant literature outside the selected databases or timeframe. Second, while the Socio-Technical Systems (STS) framework was employed to guide the analysis, it was used conceptually to map vulnerabilities rather than as a tool for empirical operationalization. Consequently, the study's focus on high-profile individuals limits the generalizability of the findings to broader, low-visibility populations. Furthermore, the case studies presented in Section 4 are constructed scenarios intended for conceptual illustration rather than real-world empirical demonstrations and thus represent plausible routes rather than verified incident reports. Finally, the analysis primarily treats service sectors in isolation, with restricted engagement in cross-platform interaction analysis.

7. Conclusion

This study demonstrates that the risks facing high-profile individuals arise from the systemic interaction of human behaviour, platform architectures, and cross-service data flows. By analysing five high-demand service categories and synthesising their shared vulnerabilities into converging adversarial pathways, the paper shows that contemporary cyber threats are inherently cross-platform and socio-technical. The constructed scenarios further illustrate how discrete weaknesses escalate into financial, reputational, and physical harm. These findings highlight the limitations of platform-centric security models and underscore the need for personalised, multi-layered protection strategies tailored to differentiated user profiles. Future research should operationalise the socio-technical risk model introduced here, develop metrics for cross-platform exposure, and evaluate targeted interventions for individuals with elevated visibility. As digital interdependence deepens, cybersecurity must evolve toward proactive, systemic approaches capable of safeguarding both high-profile and everyday users.

Ethics Statement: No experiments were conducted on people or property. An additional ethics statement is not needed.

AI Ethics Statement: This document was organized and spell/grammar checked using AI tools within Google Docs and Grammarly.

References

Al Habsi, A., Butler, M. and Percy, A. (2023) 'Blackmail and the self-disclosure of sensitive information on social media: prevalence, victim characteristics and reporting behaviours amongst Omani WhatsApp users', Security Journal, 22 April, pp. 1–19. Available at: https://doi.org/10.1057/s41284-023-00376-3

Almukheiran, M., & Li, T. (2020). Identifying Insider Threats in Enterprise Networks: A Survey and Taxonomy. Journal of Network and Computer Applications, 161, 102640. doi:10.1016/j.jnca.2020.102640

Al-Mekhlafi, K. K., Qasim, Z., Thabit, F. A. & Abdullah, Z. (2020). Security vulnerabilities in e-learning platforms: A comprehensive review and a proposal for a secure framework. International Journal of Advanced Computer Science and Applications, 11(11). DOI: 10.14569/IJACSA.2020.0111164.

Amos, Z. (2024). 4 cybersecurity risks of robot-assisted surgery. The Journal of mHealth. Available at: https://thejournalofmhealth.com/4-cybersecurity-risks-of-robot-assisted-surgery/ (Accessed: 30 April 2026).

Anderson, J. G., Goodman, K. W., & Prumi, S. (2019). Ransomware and Electronic Health Records: An Epidemic of Cyberattacks. Journal of Medical Systems, 43(8), 244.[https://doi.org/10.1007/s10916-019-1385-z]

Cerezo, A. I., Lopez, J. and Patel, A. (2007) 'International Cooperation to Fight Transnational Cybercrime', in Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007). Karlovassi, Greece, 27–28 August. IEEE, pp. 13–27. Available at: https://doi.org/10.1109/WDFIA.2007.4299369.

Berrios, J., Mosher, E., Benzo, S., Grajeda, C., Baggili, I., Hobbelink, E. and Roelofsma, P. (2023) 'Factorizing 2FA: Forensic analysis of two-factor authentication applications', Forensic Science International: Digital Investigation, 45(Supplement), 301569. doi: 10.1016/j.fsidi.2023.301569.

Coupland, H. (2025) 'Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them', York Law Review, 6. Available at: https://doi.org/10.15124/yao-23h6-cf66.

Jongh, D., de Ridder, Y., Hobbelink, E., Zięcik, N., Bouma, D., Treur, J. and Roelofsma, P. (2025) Supply chain risk management of insider threats: A network-oriented computational analysis. Unpublished manuscript.

Kramer, J., Streicher, A. and Niemietz, M. (2025) 'From Sign-Up to Multi-million Revenues: A Deep Dive Into Vendors on Darknet Marketplaces', in Availability, Reliability and Security: ARES 2025 International Workshops, Ghent, Belgium, August 11–14, 2025, Proceedings, Part III. Berlin: Springer-Verlag, pp. 221–238. https://doi.org/10.1007/978-3-032-00635-6_13

Gonzaga, K., Serra, S., Gomes, M. and Malta, S. (2026) 'AI-powered social engineering: Emerging attack vectors, vulnerabilities, and multi-layered defense strategies', Computers, 15, 128. doi: 10.3390/computers15020128.

Ilori, O., Nwosu, N. T. and Naiho, H. N. N. (2024) 'Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies', World Journal of Advanced Research and Reviews, 22(03), pp. 213–224. Available at: https://doi.org/10.30574/wjarr.2024.22.3.1727.

Jawaid, S.A. (2023) 'Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity', International Journal of Data Science and Big Data Analytics, 2(2), pp. 11–17. doi: 10.51483/IJDSBDA.2.2.2022.11-17

Kuo, A.J., Glick, T. and Cova, M. (2020) 'Micro-segmentation: A Survey and Taxonomy', IEEE Communications Surveys & Tutorials, 22(3), pp. 1957-1985. DOI: 10.1109/COMST.2020.3005886.

Li, J., Shi, W., & Zhang, Y. (2020). Advanced phishing attacks and detection techniques in the age of AI. Security and Communication Networks, 2020, 1-15. DOI: 10.1155/2020/8896593

Ludvigsen, K.R. and Nagaraja, S. (2022) 'Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective', Computer Law & Security Review, 44, 105656. doi: 10.1016/j.clsr.2022.105656.

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. Information & Computer Security, 27(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031

Meurs, T., Cartwright, E., Cartwright, A., Junger, M., Abhishta, A. and Abhishta, A. (2024) 'Deception in double extortion ransomware attacks: An analysis of profitability and credibility', Computers & Security, 138, p. 103670. https://doi.org/10.1016/j.cose.2023.103670.

Mokhtar, R., Zulkifli, S., & Roslan, M. (2023). A review of SIM-swapping attacks: Taxonomy, techniques, and countermeasures. International Journal of Computer Science and Network Security, 23(10), 101-110. DOI: 10.22937/CSNS.2023.23.10.10

Nathan, M. (2020) 'Credential stuffing: new tools and stolen data drive continued attacks', Computer Fraud & Security, 2020(12), pp. 18–19. Available at: https://doi.org/10.1016/S1361-3723(20)30130-5

Pal, B., Islam, M., Bohuk, M. S., Sullivan, N., Valenta, L., Whalen, T., Wood, C., Ristenpart, T. and Chatterjee, R. (2022) 'Might I Get Pwned: A Second Generation Compromised Credential Checking Service', in Proceedings of the 31st USENIX Security Symposium. Boston, MA: USENIX Association, pp. 2639–2656. Available at: https://www.usenix.org/conference/usenixsecurity22/presentation/pal.

Prasad, N., Diro, A., Warren, M. and Fernando, M. (2025) 'A survey of cyber threat attribution: Challenges, techniques, and future directions', Computers & Security, 157, 104606. doi: 10.1016/j.cose.2025.104606.

Sharma, H. (2021) Impact of DSPM on insider threat detection: Exploring how DSPM can enhance the detection and prevention of insider threats by monitoring data access patterns and flagging anomalous behaviour.

Shu, Z., Hu, Z., Ma, D., & Chen, G. (2020). Analyzing the underground market for stolen digital credentials. IEEE Transactions on Dependable and Secure Computing, 17(5), 1060-1073. DOI: 10.1109/TDSC.2018.2863920

Suthar, H. (2026) Social engineering attacks and human behaviors: The science behind human vulnerability in cybersecurity. Unpublished manuscript.

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', Computers & Security, 38, pp. 97-102. DOI: 10.1016/j.cose.2013.04.004.

Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A review of sociotechnical systems theory: A classic concept for new command and control paradigms. Theoretical Issues in Ergonomics Science, 9(6), 479–499. https://doi.org/10.1080/14639220701635470

Waelchli, S. & Walter, Y. (2025), Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study, Computers & Security, 148, 104137. https://doi.org/10.1016/j.cose.2024.104137

Walton, M. (2023) 'Beware corporate espionage, sabotage and spying', [Publication title unavailable], 12, pp. 43–46.

Wang, K. C. and Reiter, M. K. (2020) 'Detecting Stuffing of a User's Credentials at Her Own Accounts', in Proceedings of the 29th USENIX Security Symposium. Austin, TX: USENIX Association, pp. 2025–2042. Available at: https://www.usenix.org/conference/usenixsecurity20/presentation/wang-ke.

Whitelaw, F., Riley, J., & Elmrabit, N. (2024). A review of the insider threat, a practitioner perspective within the UK financial services. IEEE Access, 12, 34752-34768. https://doi.org/10.1109/ACCESS.2024.3373265