IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

Enhancing Cybersecurity in Conventional Security Organizations

John Owoyemi

Department of Information Security, University of the Cumberlands, Kentucky, USA

Abstract: Emergence of advanced cyber threats has radically redrawn the operating environment of traditional security establishments like police, military, and private security companies. This paper critiques vulnerabilities, threats, and new strategies needed for bolstering cybersecurity across these domains based on empirical evidence, industry reports, and case studies such as the 2021 Washington D.C. Police ransomware attack and attacks on U.S. defense contractors. The paper identifies prominent groups of cyber threats: phishing and social engineering, ransomware and malware, insider threats, and hybrid cyber–physical attacks based on such analyses. Insights indicate that the majority of traditional security establishments remain technologically under-capacitated and structurally disjointed when planning for a cyber defense approach, giving more priority to physical over virtual protection. As a solution, the study outlines a multidimensional approach consisting of a five-step key strategic action: risk-based critical asset priority, integrated incident planning, cross-sector information sharing and collaborative approach, capacity enhancement with recurring training, and policy alignment with standardized governance. This holistic framework stresses the view that cybersecurity is both a technological issue and organizational, a culture-driven imperative. Finally, bolstering cybersecurity across traditional security establishments necessitates a unified effort blending advanced technologies, active risk management, and inter-agency cooperation towards bolstering national resilience and retaining public confidence at a time when the world is increasingly online.

Keywords: Cybersecurity Resilience, Conventional Security Organizations, Risk-Based Cyber Management, Incident Response Planning, Hybrid Threats, and Inter-Agency Collaboration

I. INTRODUCTION

In the contemporary discourse of cybersecurity and defense against perpetrators, Awodiji and Owoyemi (2025) suggested that it is pertinent to understand the practical events concerning cybersecurity infiltration of security organizations which have unfolded contemporarily. In 2015, investigation reports from several national news outlets including AbcNews reported that hackers infiltrated the U.S. Office of Personnel Management and compromised the personal records of over 21 million employees, including military officers and law enforcement staff. Also, in 2021, the Washington, D.C. police department was hit by a ransomware attack that exposed sensitive case files, officer disciplinary records, and informant data.

Hence, on one hand, military institutions across the globe now contend with espionage campaigns targeting classified communication systems and defense contractors. Private security companies, on the other hand, entrusted with safeguarding corporate and individual assets, have also been exploited through breaches of surveillance networks and poorly secured client databases (Nemeth, 2022).

According to Duraklar (2025), these incidents make one thing clear: “the frontline of conventional security has shifted. What was once defined by patrols, checkpoints, and physical deterrence is now equally contested in the digital arena”. In the context of the police force, cybersecurity is no longer a peripheral concern but a core operational issue. Breaches of digital evidence repositories or criminal databases not only disrupt investigations but can also compromise witness safety and undermine judicial processes (Turner, 2019).

However, military institutions face even graver risks as cyber intrusions can paralyze command-and-control systems, corrupt logistical supply chains, or reveal national defense strategies to adversaries (Stoddart, 2022). In a different light, private security organizations are operating in an increasingly data-driven environment, thus, Nemeth (2022) posits that these organizations carry the dual responsibility of protecting clients’ physical assets while securing digital surveillance tools, encrypted communications, and sensitive corporate information. In each case, a successful cyberattack proves it is not just about technical disruption, but it directly erodes public trust, jeopardizes human lives, and weakens national resilience.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

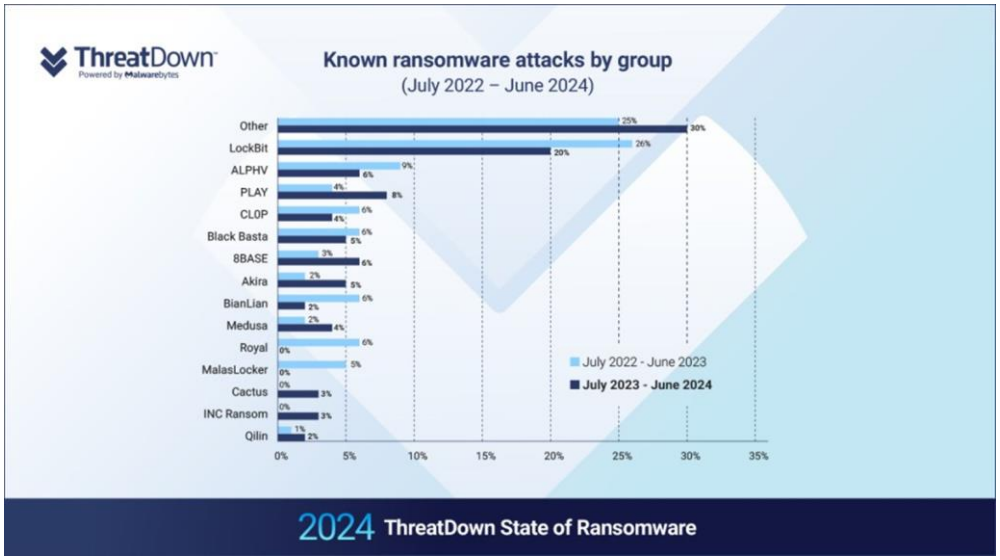
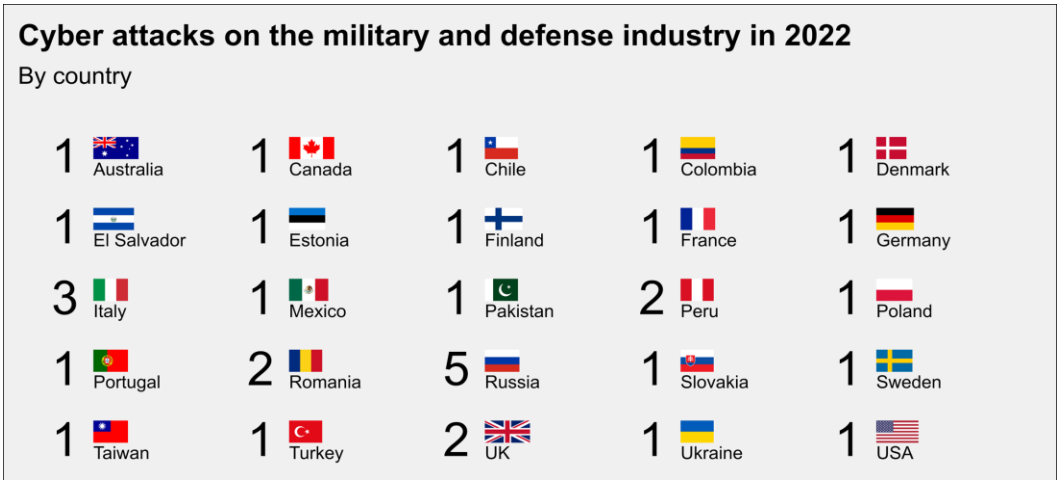


Figure 1. Known Ransomware Attacks by Group in 2022 and 2024.
Source: Malwarebytes Report 2024

However, Okolie (2022) critiqued that conventional security organizations remain relatively underprepared in comparison with perpetrators advancement. For instance, police forces in many jurisdictions operate with legacy IT infrastructure that cannot withstand modern attacks, while funding tends to prioritize physical resources such as vehicles and weaponry over digital safeguards (Stoddart, 2022). For militaries, despite their vast resources, often struggle with the complexity of defending vast supply chains and integrating cybersecurity seamlessly into modus operandi (Sobb et al. 2020). Private security firms, many of which lack standardized regulations or oversight, frequently underinvest in cybersecurity due to cost pressures or limited expertise (Clinton, 2023). These vulnerabilities are exacerbated by evolving threats, from ransomware and phishing schemes to state-sponsored cyber warfare, alongside insider risks that exploit human error and organizational blind spots.



IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

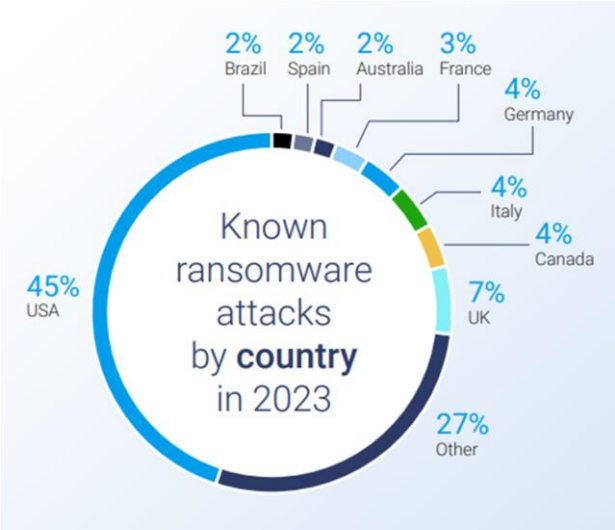


Figure 2. Cyber Attacks on the Military and Defense Industry per Country and Prevalence of Ransomware Attacks by Country in 2023. Source: Malwarebytes Report 2024

Against this backdrop, a pressing question arises: What strategies can conventional security organizations adopt to strengthen their cybersecurity posture and effectively respond to emerging digital threats? Answering this requires moving beyond abstract recommendations to practical, sector-specific strategies as opined by Awodiji et al. (2022): how police can fortify databases and evidence systems; how militaries can institutionalize cyber defense within national strategies; and how private security companies can professionalize digital protection through global standards and specialized expertise. This article therefore seeks to critically examine the vulnerabilities of conventional security organizations and propose actionable pathways for enhancing their cybersecurity resilience in an era where the line between physical and digital security is increasingly blurred.

II. LITERATURE REVIEW

Empirical and industry literature increasingly emphasizes that cybersecurity is no longer peripheral but fundamental to the functioning of conventional security organizations. In law enforcement, researchers such as Florella et al. (2021) argue that digital resilience is essential for maintaining the integrity of criminal justice systems, particularly as evidence and records move online. Industry reports from Europol (2022) similarly highlight that police forces face heightened risks from ransomware and data theft, which can obstruct investigations and compromise witnesses.

Military-focused literature adopts a more strategic tone. Moore (2022) stress that cyber capabilities are now integral to national defense, serving both defensive and offensive functions. NATO's policy briefs in 2023 underscore that modern warfare increasingly blends kinetic and digital domains, requiring militaries to secure command-and-control systems, satellite communications, and defense supply chains against intrusion (Macci, 2023).

For private security, the discourse is less developed. Industry analyses including PwC (2021) Vaid (2023) warn that private firms often underinvest in cybersecurity, even as they manage vast troves of client data and deploy digital surveillance systems vulnerable to interception. Academic studies by Kalmenovitz et al. (2025), observe that fragmented regulation leaves private firms exposed, with standards varying widely across jurisdictions.

Hence, deductively, cybersecurity has become central to the functioning of conventional security organizations, though its integration varies across sectors. In law enforcement, digital resilience is vital to preserving the integrity of justice systems as evidence and records move online, while in the military, cyber defense is now embedded in national strategies that blend kinetic and digital warfare (Stephens et al. 2025).

Practically, this underscores the need for tailored strategies to protect critical operations, while academically, it reveals comparative gaps in research, particularly in the private security sector, and calls for more holistic, cross-sectoral inquiry.

Cybersecurity Threats and Infiltrations in Conventional Security Organizations

Cybersecurity threats in conventional security organizations refer to malicious digital activities that target the technological infrastructure, data, and communication systems of police, military, and private security institutions (Prasad

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

et al. 2020). These organizations, traditionally focused on physical safety, now depend heavily on digital tools such as databases, surveillance networks, communication platforms, and intelligence systems (Vermesan et al. 2022).

Therefore, cyber threats exploit vulnerabilities in these systems to disrupt operations, steal sensitive information, or compromise trust (Awodiji and Williamsburg, 2022). Common threats include ransomware, which encrypts critical data until a ransom is paid; phishing, where deceptive communications lure personnel into revealing credentials; and malware, designed to damage or infiltrate systems (Ryan, 2021). More advanced threats involve distributed denial-of-service (DDoS) attacks that paralyze networks, and state-sponsored cyber operations aimed at espionage or sabotage. Insider threats, which can occur either through human error or intentional misconduct, can also pose a significant risk by bypassing external security barriers (Asasfeh et al. 2024).

Infiltrations, on the other hand, are described by Nadji (2024) as the successful breaches where adversaries gain unauthorized access to secure systems within conventional security organizations. For law enforcement, Fiorella et al. (2021) asserted that this could mean the compromise of digital evidence repositories or criminal databases, undermining ongoing investigations and exposing witnesses. In military contexts, infiltrations often target command-and-control systems, defense logistics, or satellite communications, with the potential to cripple strategic operations or leak classified intelligence to adversaries (Moore, 2022). Private security firms, which manage client surveillance data and corporate information, are particularly vulnerable due to underinvestment in cybersecurity and poorly enacted regulatory frameworks (Alwan, 2018). In a deeper context, infiltrations in this sector not only endanger client confidentiality but can also create weak links that attackers exploit to reach more prominent targets.

Overall, it can be deduced that cybersecurity threats and infiltrations in conventional security organizations represent more than technical risks; they directly jeopardize national security, operational integrity, and public trust. Therefore, addressing them requires a proactive and multi-layered approach, combining technological safeguards with organizational culture, staff training, and cross-sector collaboration. However, before the development of a multidimensional approach to safeguard security organizations from cyber attacks, it is necessary to understand the varying incidents of attacks that contribute to the causes and effects of the contention.

Case Studies of Cyber Incidents

Recent incidents highlight how theoretical vulnerabilities manifest in practice. In 2021, the Washington, D.C. Metropolitan Police Department suffered a ransomware attack by the Babuk group, which leaked sensitive internal data, including officer disciplinary records. According to Brayne (2018), this case illustrates the risks of inadequate database security in law enforcement.

In the military sector, a popular incident was the 2015 cyberattack on Ukraine's power grid, widely attributed to Russian state actors, demonstrated how cyber operations can paralyze critical infrastructure and support broader kinetic conflict. More recently, reports of breaches in U.S. defense contractors' networks (GAO, 2022) underscore the persistent vulnerabilities of military supply chains.

Private security companies have also been targeted. In 2020, G4S, a global security provider, faced scrutiny after contractors reported cyber weaknesses in its surveillance systems, raising concerns about the protection of client data. Similarly, smaller private firms whose incidents have not been widely reported would have been exploited as weak links in larger corporate networks, often serving as entry points for attackers seeking high-value targets.

Despite growing attention, significant gaps remain in the literature and theoretical framework to deal with this. First, Fischerkeller et al. (2022) critiqued that most research treats cybersecurity in sectoral isolation; comparative analyses across police, military, and private security organizations are not dominant in academic and theoretical discourse. Second, while national defense receives substantial scholarly and policy focus, law enforcement and private security are often overlooked, particularly in low- and middle-income contexts where digital infrastructure is weak (Owuondo, 2025). Additionally, following a meta-analysis literature review by Willie (2023), results show that existing research emphasizes technological solutions (encryption and firewalls predominantly) but pays less attention to organizational culture, training, and governance structures that are equally critical to cybersecurity resilience. Finally, empirical studies tend to concentrate on large-scale breaches in developed nations, leaving a gap in understanding how smaller jurisdictions and private firms manage or fail to manage cyber threats.

III. CYBERSECURITY THREATS IN CONVENTIONAL SECURITY ORGANIZATIONS

Conventional security organizations including the police, military, and private security firms are increasingly exposed to complex cybersecurity threats that compromise operational integrity, endanger human lives, and erode public trust (Shaheen, 2023). Traditionally structured around physical deterrence and enforcement, these organizations rely heavily on digital technologies such as surveillance systems, evidence repositories, communication platforms, and intelligence

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

databases. While these technologies enhance efficiency, Jony et al. (2023) contended that they also widen the attack surface for malicious actors. This is largely possible as cyber adversaries exploit the convergence of outdated infrastructures, human error, and advanced attack methods, making conventional security organizations both lucrative and vulnerable targets (Bardin, 2025). Empirical finding by LADO (2024) shows that among the most pressing threats are phishing, malware and ransomware campaigns leading to data breaches. Each of these categories has demonstrated significant consequences, offering critical lessons for resilience and reform.

Phishing and Social Engineering Attacks

Phishing and social engineering attacks exploit the human factor, which remains the weakest link in cybersecurity (Nonum et al. 2025). Practically, by crafting deceptive emails or fraudulent messages, attackers lure security personnel into revealing login credentials or downloading malicious attachments. These tactics are particularly concerning because they bypass even the most advanced technical safeguards by targeting psychological trust (Hartzog, 2024). In 2021, the FBI reported an increase in phishing scams aimed at U.S. police departments, many of which were disguised as pandemic-related health advisories. Once infiltrated, attackers gained access to sensitive case files and internal communications.

The consequences of such attacks extend beyond temporary disruption. Compromised police databases can expose confidential information about witnesses and ongoing investigations, potentially jeopardizing trials and even endangering lives (Nemeth, 2019).

In the military, successful phishing schemes could provide adversaries with entry points into secure communication systems, creating risks of espionage or sabotage. The lesson here is clear: while technical defenses are essential, cultivating cyber-awareness among personnel is equally vital (Aslaner, 2024). Thus, it is important that trainings are structured beyond routine awareness sessions to scenario-based simulations that mirror real-world attacks, thereby strengthening human resilience against manipulation, Odo (2024) suggested. Failure to invest in such training could risk leaving conventional security institutions technologically armored, but socially fragile.

Malware and Ransomware Attacks

Ransomware attack trends in 2025 indicate a continued surge in incidents and increasingly sophisticated tactics, with the first quarter of 2025 witnessing a 213% increase in reported victims compared to Q1 2024. Incidents are not only increasing but also diversifying, with attacks on industrial organizations down slightly in Q2 2025 but still significantly impacting manufacturing, and a rise in attacks targeting cloud systems of security organizations. As a result, ransomware represents one of the most destructive cyber threats facing conventional security organizations. In these attacks, malicious software encrypts critical files, rendering them inaccessible until a ransom is paid. The 2021 ransomware attack on the Washington, D.C. Metropolitan Police Department illustrates the severity of such threats. The Babuk group classified under ‘Other’ in Figure 1 exfiltrated more than 250 GB of sensitive data, including disciplinary files and informant records, before releasing part of them publicly. This incident endangered informants’ lives, damaged officer morale, and undermined public confidence in law enforcement’s ability to protect sensitive information.

On the other hand, military organizations face parallel risks, with malware infiltrations into defense contractors’ systems posing significant threats to national security (Lewis, 2019). Reports by the U.S. Government Accountability Office (2022) revealed that hackers compromised systems linked to weapons development projects; however, no major infiltration was recorded but this could have potentially exposed classified designs and weaponry information. Beyond operational disruption, Lele et al. (2019) argued that these breaches have strategic implications, eroding the technological advantage that militaries seek to maintain.

The critical lesson deduced herein is that resilience against ransomware and malware cannot rely solely on reactive strategies. Robust backup protocols, network segmentation, and rapid incident response are non-negotiable. Moreover, organizations must critically evaluate the ethics and practicality of ransom payments, as yielding to demands risks incentivizing further attacks (Morgan, 2021). A critical position, therefore, is that any futuristic approach requires not only investment in advanced intrusion detection systems but also cultivating inter-agency cooperation to share intelligence about evolving ransomware tactics.

Insider Threats and Data Breaches

Insider threats remain an entirely threatening category as they are initiated from within security organizations, bypassing outer defenses (Catrantzos, 2022). Insiders, by accident, coercion, or design, can inflict catastrophic compromises. The Edward Snowden disclosures in 2013 remain the highest-profile example of how one individual with legitimate access can release huge amounts of sensitive material. While this incident involved intelligence, the implications for conventional security are profound: a trusted insider or contractor can beat systems designed to be secure from external penetrations.

In this context, private security firms are particularly vulnerable, as they frequently employ contracted staff (Nemeth, 2022). Lack of proper screening has led to situations where employees have obtained unauthorized access to client watch information, damaging security and corporate reputation (Landoll, 2021). Similarly, Oettinger (2022) added that police forces run the risk of compromise when officers mishandle electronic evidence or when disgruntled employees disclose sensitive documents.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

In a real sense, insider threats illustrate that culture and governance are just as much a part of cybersecurity as technology (Catrantzos, 2022). Thus, Reddick et al. (2025) suggested that intraorganizational vetting processes must be rigorous, access rights must be graded, and user behavior must be constantly monitored for patterns of concern. Additionally, institutions must grapple with the ethics of balancing trust with aggressively monitoring harm morale, while inadequate levels invite exploitation.

Hybrid Threats: The Emergence of Cyber–Physical Threats

An emerging frontier in cybersecurity is the rise of hybrid threats that fuse cyber operations with physical tactics, creating compounded risks for conventional security organizations (Aslaner, 2024). These threats are designed not merely to steal data but to disrupt critical infrastructure, disable operational capacity, or initiate chaos during physical confrontations (Lewis, 2019). For instance, the Russia–Ukraine conflict has provided a stark demonstration of hybrid warfare, where cyberattacks against energy grids, communications, and command systems were synchronized with ground assaults, magnifying their impact. For militaries, this convergence means that vulnerabilities in digital systems can directly translate into battlefield disadvantages (Fawkes and Burden, 2025).

For law enforcement, hybrid threats manifest through coordinated cyber intrusions during civil unrest or terrorism events. For example, attackers may launch denial-of-service (DoS) attacks against police communication networks during large-scale protests, limiting officers' ability to coordinate and respond effectively. Private security firms also face hybrid risks, particularly those protecting critical infrastructure such as airports, energy facilities, or financial institutions. A cyberattack that disables surveillance or access control systems could facilitate physical break-ins, theft, or even terrorism (Naha, 2022).

However, Swejis et al. (2021) noted that the critical challenge with hybrid threats is their unpredictability and multi-domain nature. Traditional cybersecurity frameworks that compartmentalize digital and physical risks are inadequate (Howard, 2023). Thus, addressing this requires adopting integrated security doctrines that bridge cyber defense, crisis management, and physical response. Academically, Arkan (2025) suggested that hybrid threats underscore the necessity of revisiting security theory itself, expanding it to capture the blurred boundaries between cyber and kinetic warfare. Practically, they demand cross-training: military units must be equipped with cyber-defense awareness, while police and private firms must integrate digital resilience into their physical security protocols (Sehgal et al. 2023).

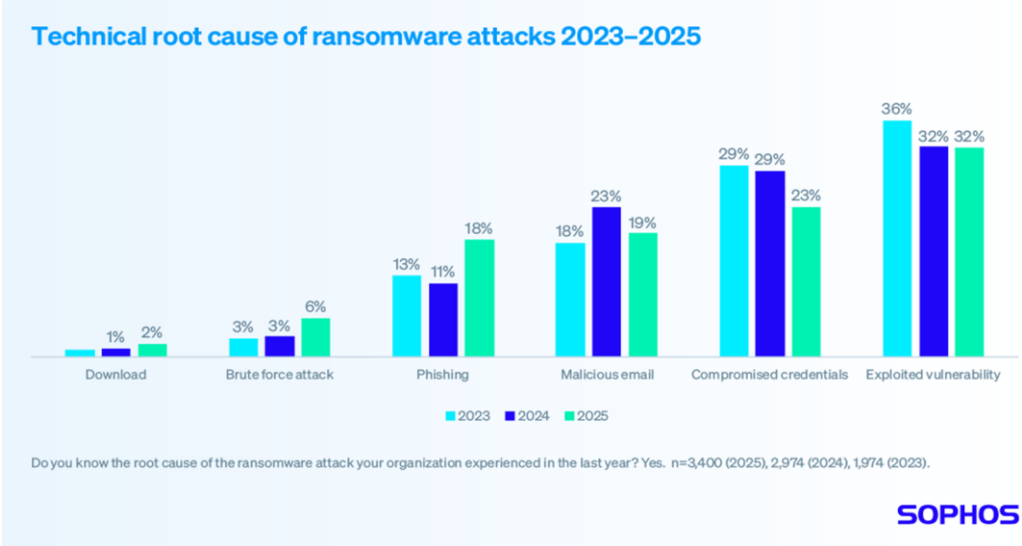


Figure 3. Technical Root Causes of Ransomware Attacks from 2023-2025.
Source: Adam (2025)

Overall, these threats reveal a persistent pattern of social, personal and organizational exploitation, for which technological solutions alone are insufficient. Phishing, ransomware, and insider breaches expose vulnerabilities not just in systems but in training, organizational culture, and governance frameworks (Bishop, 2025). The critical inference is that cybersecurity resilience requires a holistic approach that integrates advanced technology with human awareness, policy reform, and cross-sector collaboration, as also identified by Kure (2021). Without this, McCarthy et al. (2022) developed a conclusion that conventional security organizations remain dangerously exposed in a domain that adversaries increasingly exploit.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

Sector	Best Practices	Technologies and Solutions	Unique Challenges
Police	• Role-based access control (RBAC) to protect evidence databases. • Regular audits of legacy systems (Police National Computer vulnerabilities). • Intensive, scenario-based phishing and awareness training.	• AI-powered anomaly detection in evidence systems. • Blockchain for chain-of-custody in digital evidence. • Advanced encryption for witness protection and case communications.	• Balancing cybersecurity with transparency and accountability to the public. • Budgetary constraints in local forces limit adoption of cutting-edge tech. • High exposure to phishing/social engineering due to daily public interaction.
Military	• Tiered access to classified data post-Snowden. • NATO-mandated cyber audits of defense systems. • Embedding cyber drills into combat exercises.	• AI/ML for satellite communication and intrusion detection. • Blockchain to secure defense supply chains. • Quantum-resistant encryption for command-and-control systems.	• Adversaries use cyber as a weapon of war (Russia–Ukraine). • Hybrid threats combining cyber and kinetic tactics. • Balancing operational speed with cyber precautions in combat.
Private Security	• Rigorous staff vetting and tiered data access. • Regular penetration testing of client surveillance systems. • Training guards/operators on cyber hygiene.	• AI for real-time surveillance monitoring. • Blockchain for client data and contracts. • Encryption of client footage, logs, and access systems.	• Chronic underinvestment in cybersecurity compared to public counterparts. • Fragmented regulatory frameworks across jurisdictions. • Vulnerability of surveillance systems to interception.

Table 1. Comparative Framework to Enhance Cybersecurity in Conventional Security Organizations

This comparative framework (Table 1) highlights that while core principles such as access control, audits, training, AI, blockchain, and encryption cut across all sectors, their application and challenges diverge. Police forces must emphasize public trust and affordability, militaries face geopolitical hybrid threats, and private firms struggle with underinvestment and inconsistent regulation. The implication is that cybersecurity strategies must be sector-specific yet interconnected, fostering cooperation across domains since vulnerabilities in one (private contractors) often cascade into others (such as military supply chains).

IV. CYBERSECURITY STRATEGIES FOR CONVENTIONAL SECURITY ORGANIZATIONS

Developing effective cybersecurity in conventional security organizations is not dependent on simply adopting technological tools; it requires coherent strategies that align risk management, preparedness, and collaboration. While best practices and emerging technologies are vital, without a strategic framework their impact is fragmented (Bilgihan et al. 2024). This section critically explores three interlinked strategies: adopting a risk-based approach, establishing robust incident response planning, and fostering collaboration and information sharing across agencies and sectors.

1. Risk-Based Approach to Cybersecurity

Risk-based management guarantees cyber defense is deployed according to the likelihood of threat and likely effect, and not in a uniform fashion or after an incident occurs (Brooks, 2023). Conventional security organizations possess a variety of digital assets, ranging from routine administrative data to highly classified intelligence. So, priority to the data is required since all systems do not have to be secured equally, and resource availability renders global protection not feasible.

In policing, high-risk assets include evidence storage facilities, witness protection registries, and live surveillance networks. The 2020 Manchester Police accidental data loss scandal, in which sensitive victim data was leaked through carelessness in cyber practices, demonstrates the consequences of risk overestimation. Therefore, as claimed by Gellert (2020), risk-based assessment would guarantee more sensitive case-sensitive data protection on less critical systems, ensuring continuity of justice and protecting vulnerable victims.

For the military, the stakes are even higher. Command-and-control networks, satellite communications, and weapons development programs are at greatest risk as their compromise can most directly affect the outcome of battles (Acton, 2025). For instance, the 2015 cyberattack against the U.S. Office of Personnel Management (OPM), blamed on state-backed actors, exposed data on numerous federal employees, including military members. By implementing a risk-based system, the exposed data would be categorized as high-priority, subjecting them to apex encryption, multifactor authentication, and compartmentalization.

In private security, risk is client-type dependent. Firms with infrastructure of high interest such as airports or nuclear power plants, will have systems integrity and access controls as top priorities (Shapiro et al., 2021). Small firms, however, invest limited resources in excessively protecting trivial administrative data while leaving surveillance feeds open to interception. Such disconnect is a demonstration of organizational failure to adopt a disciplined risk-based plan (Weiner, 2022).

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

Critically, risk-based cybersecurity is not a uni-enabled task but a continuous process (Brooks, 2023) because, as threat landscapes evolve, such as the rise of ransomware-as-a-service or quantum computing attacks, risk analysis must be constantly refreshed. Failing this agility, organisations risk defending yesterday's threats while exposed to tomorrow's.

2. Incident Response Planning

The hubris of all preparation, proactiveness and risk-based factors against cyber threats is that no cybersecurity defense is infallible. According to Dupont (2019), breaches will occur, and what differentiates resilient organizations from vulnerable ones is not just the ability to prevent attacks, but the capacity to respond effectively when they happen (that is, incident response). Incident response (IR) planning provides a structured framework for detecting, containing, mitigating, and recovering from cyber incidents (Thompson, 2018).

Within law enforcement, a lack of IR planning can shut out entire departments. The 2021 Babuk ransomware attack against the Washington, D.C. Metropolitan Police is an example: sensitive disciplinary information and informant identities were stolen and released, endangering lives and eroding public trust. A robust IR plan would have included encrypted backups, segregated networks, and rapid notification procedures for those affected (Murthy et al. 2024). Therefore, Davidoff and Sprenger (2022) suggested that regular practice exercises that mimic ransomware attacks would have allowed the police force to reduce disruption and safeguard compromised informants more effectively.

For the military, IR planning needs to include cyber defense within operational principle. Gupta et al. (2025) recommended. Cyberattacks during conflict are not stand-alone operations but typically integrated with kinetic actions, as in the Russia–Ukraine conflict where cyberattacks against Ukrainian command and control infrastructure precipitated missile strikes (Libicki, 2025). The military IR plans need to therefore function practically with redundant communications, rapid system isolation, and cross-domain coordination between cyber divisions and traditional armed forces (Carlson, 2019). Regular war games involving cyberattack scenarios are a key component of preparing military staff for hybrid warfare theatres.

Overall, a quality IR plan should anticipate contingencies, such as manual overrides of surveillance systems, pre-approved crisis communication lines with clients, and contractual provisions for state and breach disclosure (Fowler, 2023).

3. Collaboration and Information Sharing

Cybersecurity threats rarely respect organizational boundaries. A vulnerability in one institution can quickly cascade into others through interconnected systems and shared infrastructure. Therefore, collaboration and information sharing are essential to building collective resilience across law enforcement, military, and private security sectors (Radanliev, 2025).

For law enforcement agencies, collaboration often implies liaison with intelligence agencies or national cybersecurity centers. The Europol European Cybercrime Centre (EC3) provides a useful example, focusing expertise and intelligence from many states to counter cybercrime. However, issues remain at local levels, where smaller police forces lack the resources or institutional culture for cross-agency information sharing. Unless they collaborate, they risk being blind-sided by threats already flagged elsewhere.

In the military context, collaboration must occur both nationally and internationally. NATO's CCDCOE in Estonia provides a mechanism for the member nations to share strategies, conduct joint exercises, and develop interoperable doctrine. This framework for collaboration acknowledges that in modern warfare, a weakness in one ally can compromise everyone's security. Yet cooperation is not without its challenges: states may withhold sensitive intelligence for fear of espionage or political mistrust. Overcoming these barriers requires building foundations of trust, underpinned by legal agreements and confidence-building measures.

For private security firms, collaboration with public authorities is critical, not least because private firms often control access to critical infrastructure. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has made strides in promoting public–private collaboration, offering information-sharing programs that help prepare private firms for emerging threats. Yet many smaller firms remain excluded due to a lack of awareness or capacity. Also, private organizations are often fearful of reputational damage from disclosure of breaches, which discourages openness. Regulatory incentives must be provided to overcome these barriers, such as safe-harbor protection for disclosure of breaches and mechanisms that anonymize shared threat intelligence.

Most importantly, the partnership must extend from information-sharing to joint operational responses. Two examples demonstrate this. First, in the aftermath of the WannaCry ransomware attack (2017), collaboration between the UK's National Health Service, law enforcement, and private cybersecurity experts was instrumental in restoring services. This indicates that effective collaboration can be especially helpful even in ameliorating large-scale crises once it extends beyond data-sharing to coordinated action.

A critical examination of these strategies reveals both their potential and their limitations. A risk-based approach offers a rational model for prioritization but is vulnerable to politicization: what is deemed “high risk” may reflect organizational biases rather than objective analysis (Paul, 2021). Incident response planning is indispensable, yet without resources and

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

leadership support, plans remain symbolic rather than practically effective (Canton, 2019). Collaboration and information sharing enable collective resilience but are hindered by mistrust, reputational concerns, and institutional inefficiency.

As a result, the way forward lies in integrating these strategies (that is, risk-based approach, incident response planning and collaborative framework) into a holistic framework as presented in Figure 4. Risk-based approaches must feed directly into incident response planning by identifying the systems and assets most in need of protection (Staves, 2023). Incident response drills must incorporate inter-agency collaboration to simulate real-world interdependencies. Above all, conventional security organizations must cultivate a culture of continuous adaptation, recognizing that cybersecurity is not a fixed goal but a moving frontier shaped by adversaries who are constantly innovating (Bishop, 2025).

Figure 4. Integrative Framework of Cybersecurity Lifecycle

Sector-Specific Recommendations and Application of Cybersecurity Strategies

Cybersecurity has become central to the functioning of national and private security globally. From protecting digital evidence and surveillance feeds to safeguarding the integrity of criminal records, military bodies and law enforcement agencies now operate in environments where digital breaches can cripple national security operations and justice delivery (Dev, 2024).

However, by establishing a collaborative system for these entities, these security organizations can all leverage advanced capabilities, share intelligence, and establish resilient frameworks for cyber defense. This action plan outlines practical steps for enhancing cybersecurity across five domains: risk-based prioritization, incident response planning, collaboration and information sharing, capacity building and training, and policy alignment.

Action Step 1: Joint Risk-Based Prioritization of Critical Assets

1. **Cross-Sector Asset Mapping**

Police, military, and private security firms in required cases can jointly identify high-value systems across domains, such as criminal databases, surveillance networks, military command systems, and private client records. For such asset mapping, a tiered classification system (which classifies assets into critical, high, medium, and low) should be utilised to determine resource allocation and access for each security organisation in order to ensure independence and autonomy despite combined efforts (Stanisci and Moffatt, 2024).

2. **Military Adaptation of Defensive Models**

Military expertise in protecting command-and-control and satellite systems is highly sophisticated and effective, and this can be repurposed to secure police digital evidence labs and private client data protection. For example, adapting NATO's cyber risk assessment frameworks to justice systems would strengthen its digital efficiency and resilience to cyber threats.

3. **Private Sector Audits and Red Teaming**

Police departments, military organisations and private security firms should engage vetted cybersecurity firms to conduct penetration tests and simulate insider threats. One effective approach is the red-teaming exercises, which are already common in critical infrastructure sectors; this should stress-test all security organizations networks.

Practically, this risk-based framework prevents critical justice systems from being deprioritized, thereby reducing the likelihood of paralysis in investigations and ensuring that essential law enforcement functions remain operational even during cyber incidents, while academically, it demonstrates the value of structured prioritization models in operational

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

security by illustrating how military doctrines and risk assessment strategies can be effectively adapted to strengthen civilian policing and enhance resilience in justice systems.

Action Step 2: Integrated Incident Response Planning

1. **Unified Response Protocols**

Developing a standardized integrative incident response (IIR) templates across police, military, and private security organizations would ensure interoperability during crises, enabling seamless coordination and reducing confusion. This is particularly critical in scenarios where ransomware attacks on private security contractors could spill over into police systems; by adopting joint protocols, these organizations can prevent fragmented responses, maintain operational continuity, and safeguard sensitive information across interconnected security networks (Kalinaki, 2024).

2. **Cross-Sector Cyber Drills**

Conduct annual joint cyber exercises, modeled on NATO's Locked Shields, with scenarios targeting evidence databases, 911 call centers, and surveillance systems. Include simulations of cascading attacks across public and private security ecosystems.

3. **Military Cyber Assistance**

Establish legal provisions enabling police to request support from national cyber defense units in severe cases (e.g., state-sponsored attacks). Safeguards should ensure civilian oversight and limit military involvement to technical support roles. The importance of this approach lies in its dual value: practically, it ensures that police responses to cyber incidents are rapid, lawful, and supported by advanced expertise, while academically, it contributes to incident response planning theory by demonstrating how civilian–military cooperation enhances resilience in safeguarding critical security systems.

Action Step 3: Structured Collaboration and Information Sharing

Local police agencies often lack visibility into advanced cyber threat intelligence. Meanwhile, military bodies guard classified information, and private firms worry about reputational damage (Cameron and Chetail, 2013). Bridging these lacunae requires structured, trusted mechanisms, including cyber fusion centers and cross-sector channelling.

1. **Cyber Fusion Centers**

This implies the establishment of regional or national hubs where police, military cyber commands, and private firms share real-time intelligence. These centers mirror counterterrorism "fusion centers", adapted for digital threats. It is important to note that these organizations get linked on join operation when need arises such as seen in the United States crackdown against illegal immigrants and transnational criminal organization like the MS-13. However, there is a lack of a cyber-fusion center designated for preparation and proactive response to cyber threats.

2. **Secure Cross-Sector Channels**

Build encrypted communication platforms for sharing time-sensitive cyber alerts across agencies will be critical, as it will remove the constraints of bureaucracy in information sharing and collaborative efforts. For example, adapting the UK's Cyber Security Information Sharing Partnership (CiSP) model for police–military–private collaboration.

Action Step 4: Capacity Building and Training

Advanced technical systems are vulnerable without trained personnel. Human error remains a leading cause of breaches, particularly phishing and social engineering. Police officers, particularly, unlike dedicated cyber units, often underestimate cyber risks.

1. **Cross-Sector Training Programs**

Police officers should attend joint cyber courses with military cyber units and private security experts. Police colleges and training modules should include digital forensics, ethical hacking, and incident triage, not just as abstract courses but as practical courses like other physical training.

2. **Civil Rights-Focused Training**

Cyber training for these security organizations must emphasize civil liberties, ensuring that digital investigations comply with privacy and legal standards. This prevents "mission creep" when either the police department or other private firms are working with military bodies.

3. **Embedded Cyber Specialists**

Military cyber mentors could provide tactical advice on securing high-priority assets for police departments.

Action Step 5: Policy and Governance Alignment

Collaboration fails without clear organizational governance. Police, military, and private firms often operate under different legal regimes, creating confusion in crisis response.

1. **Standardized Cybersecurity Regulations, Legal Framework and Funding**

Governments should mandate uniform cybersecurity standards across all conventional security actors, covering essential areas such as encryption protocols, breach reporting timelines, and access control policies. Complementing this, legal

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

frameworks must clearly define the conditions under which military cyber units can support police operations, ensuring proper oversight and accountability. Furthermore, funding partnerships should be established through joint mechanisms that draw on both national security budgets and private sector contributions, for instance, subsidies could enable local police departments to access advanced cyber defense tools, co-financed by critical infrastructure firms.

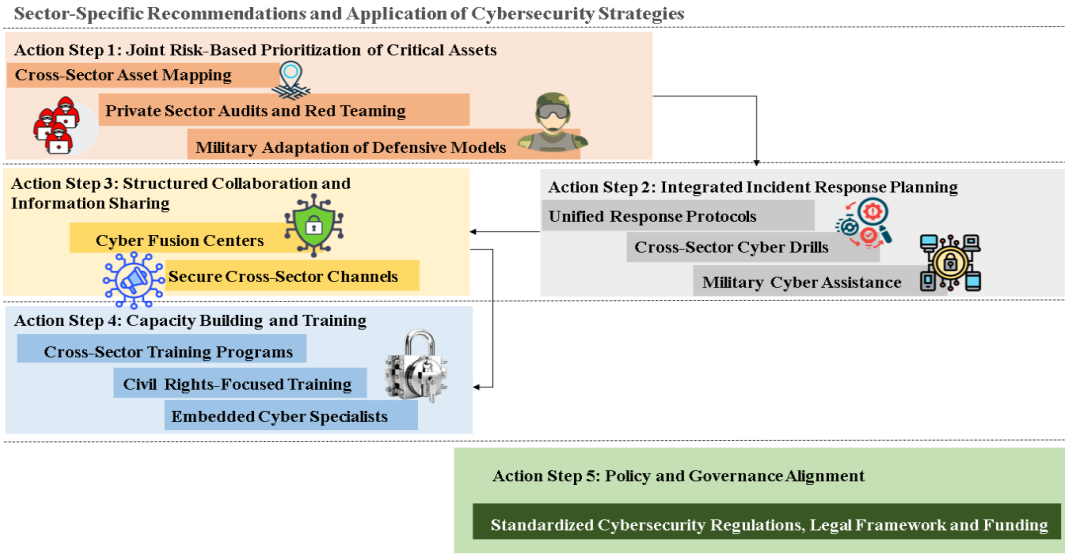


Figure 5. Developed Cybersecurity Strategic Framework

Summary

The vulnerabilities of security organizations (public or private) to cyber threats are neither isolated nor manageable within law enforcement alone. Therefore, by adopting a risk-based prioritization framework, integrating cross-sector incident response planning, fostering collaboration through fusion centers and intelligence sharing, investing in capacity building, and aligning policy and governance, these organizations can dramatically strengthen their cybersecurity posture through the collaborative framework presented herein. The military contributes advanced defense expertise, private firms bring agility and specialized tools, and police ensure accountability to civil rights and justice. Together, these bodies can create a resilient, multi-layered defense ecosystem that protects not only sensitive digital assets but also public trust in security institutions.

V. CONCLUSION

Digital security in security organizations has shifted from being a background concern to becoming a core pillar of how law enforcement, armed forces, and private protection services operate (Nemeth, 2022). The dangers they encounter keep changing, whether it is fraudulent email schemes, malicious software that locks systems, or trusted insiders leaking information. Each type of threat creates different problems: police could see criminal investigations collapse, the military might lose control of critical defense systems, and private firms must fight to defend their clients with fewer financial and technical resources. The damage is not hypothetical. The Babuk ransomware incident against the Washington, D.C. police department and Russia's cyber campaigns in Ukraine reveal how intrusions expose secret records, weaken public trust, and in extreme cases put lives directly at risk. While the basic defensive ideas remain similar across these sectors, their focus areas diverge. Law enforcement protects judicial processes, armed forces guard national defense structures, and private companies strive to keep clients safe with limited capacity.

To meet these challenges, the five-step action plan outlined above stands out as important. Beyond these core measures, advanced tools like artificial intelligence, blockchain-based records, and sophisticated encryption can raise defenses even higher. When combined with staff training and a culture that treats online responsibility as part of everyday practice, organizations would gain more resilience. Overall, improving cybersecurity is not just a technical requirement, it is a responsibility owed to the public's confidence and safety.

REFERENCES

[1]. AbcNews. (2015). '22 Million Affected by OPM Hack, Officials Say'. ABC News. Available from: https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731 (Accessed on 12 August 2025).

DOI: 10.17148/IARJSET.2025.12758

[2]. Acton, J. M. (2025). The survivability of nuclear command-and-control capabilities. Journal of Strategic Studies, 48(2), 407-464.
[3]. Adam, S. (2025). The State of Ransomware 2025 [online]. Available from: https://news.sophos.com/en-us/2025/06/24/the-state-of-ransomware-2025/ (Accessed on 18 August, 2025)
[4]. Al Jazeera. (2021). 'DC police suffer 'massive' info leak after ransomware attack'. Al Jazeera. Available from: https://www.aljazeera.com/news/2021/5/13/dc-police-suffer-massive-info-leak-after-ransomware-attack (Accessed on 12 August 2025).
[5]. Alwan, H. B. (2018). Policy Development and Frameworks for Cyber Security in Corporates and Law Firms. International journal of legal information, 46(3), 137-162.
[6]. Arkan, Z. (2025). European Security and Hybrid Threats: A Narrative in the Making. Springer Nature.
[7]. Asasfeh, A., Alnawayseh, S. E., AbdElkareem, R., & Salahat, M. (2024, February). Human Factors In Security Management: Understanding And Mitigating Insider Threats. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-10). IEEE.
[8]. Aslaner, M. (2024). Cybersecurity Strategies and Best Practices: A comprehensive guide to mastering enterprise cyber defense tactics and techniques. Packt Publishing Ltd.
[9]. Bardin, J. S. (2025). Cyber warfare. In Computer and Information Security Handbook (pp. 1345-1380). Morgan Kaufmann.
[10]. Bilgihan, A., & Ricci, P. (2024). The new era of hotel marketing: integrating cutting-edge technologies with core marketing principles. Journal of Hospitality and Tourism Technology, 15(1), 123-137.
[11]. Bishop, G. (2025). Cybersecurity Culture. CRC Press.
[12]. Brayne, S. (2018). The criminal law and law enforcement implications of big data. Annual Review of Law and Social Science, 14(1), 293-308.
[13]. Brooks, T. T. (Ed.). (2023). Adaptive Security and Cyber Assurance for Risk-based Decision Making. IGI Global.
[14]. Cameron, L., & Chetail, V. (2013). Privatizing war: private military and security companies under public international law. Cambridge University Press.
[15]. Canton, L. G. (2019). Emergency management: Concepts and strategies for effective programs. John Wiley & Sons.
[16]. Carlson, T. F. (2019). Using Modular Open Systems Approach (MOSA) to Address System Survivability in Army Weapon Systems.
[17]. Catrantzos, N. (2022). Managing the insider threat: no dark corners and the rising tide menace. CRC Press.
[18]. Clinton, L. (2023). Fixing American cybersecurity: Creating a strategic public-private partnership. Georgetown University Press.
[19]. Davidoff, S., Durrin, M., & Sprenger, K. (2022). Ransomware and cyber extortion: response and prevention. Addison-Wesley Professional.
[20]. Dev, D. K. V. (2024). Securing Justice: Enhancing Cybersecurity in the Criminal Justice System. International Journal of Science and Research (IJSR), 13(8), e65-e79
[21]. Duraklar, K. (2025). Security Technologies for Law Enforcement Agencies. CRC Press.
[22]. Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of cybersecurity, 5(1), tyz013.
[23]. Fiorella, G., Godart, C., & Waters, N. (2021). Digital integrity: Exploring digital evidence vulnerabilities and mitigation strategies for open source researchers. Journal of International Criminal Justice, 19(1), 147-161.
[24]. Fawkes, A., & Burden, D. (2025). The Military Metaverse. CRC Press.
[25]. Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). Cyber persistence theory: Redefining national security in cyberspace. Oxford University Press.
[26]. Fowler, B. (2023). Information Assurance and Risk Management Strategies.
[27]. Gellert, R. (2020). The risk-based approach to data protection. Oxford University Press.
[28]. Gupta, B. B., & Ip, A. W. (Eds.). (2025). Advanced Cyber Defense for Space Missions and Operations: Concepts and Applications: Concepts and Applications.
[29]. Hartzog, W. (2018). PrivacyOs Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press.
[30]. Howard, R. (2023). Cybersecurity first principles: a reboot of strategy and tactics. John Wiley & Sons.
[31]. Jony, A. I., & Hamim, S. A. (2023). Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. Journal of Information Technology and Cyber Security, 1(2), 53-67.
[32]. Kalinaki, K. (2024). Ransomware threat mitigation strategies for protecting critical infrastructure assets. In Ransomware Evolution (pp. 120-143). CRC Press.
[33]. Kalmenovitz, J., Lowry, M., & Volkova, E. (2025). Regulatory fragmentation. The Journal of Finance, 80(2), 1081-1126.

DOI: 10.17148/IARJSET.2025.12758

[34]. Kure, H. (2021). An Integrated Cybersecurity Risk Management (I-CSRM) framework for critical infrastructure protection (Doctoral dissertation, University of East London).
[35]. LADO, M. J. (2024). Cybersecurity Essentials Protecting Your Digital Life, Data, and Privacy in a Threat-Driven World: Comprehensive Guide to Preventing Hacks, Phishing, Malware, and Identity Theft. Amazon Digital Services LLC-Kdp.
[36]. Landoll, D. (2021). The security risk assessment handbook: A complete guide for performing security risk assessments. CRC press.
[37]. Lawson, S. T. (2019). Cybersecurity discourse in the United States: Cyber-doom rhetoric and beyond. Routledge.
[38]. Lele, A., Lele, B., & Bose, B. (2019). Disruptive technologies for the militaries and security (Vol. 132, pp. 205-215). Singapore: Springer.
[39]. Lewis, T. G. (2019). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.
[40]. Libicki, M. C. (2025). The New Calculus of Escalation: Avoiding Armageddon in Great Power Conflict. Georgetown University Press.
[41]. Macci, F. (2023). The Use of Quantum-Based Technologies for Secure Satellite Communications in Support of European Union Space Security and Defence.
[42]. Malwarebytes (2024). ThreatDown 2024 State of Malware: From Malware to Threats a Comprehensive Defense Guide [online]. Available from: https://www.tdsynnex.com/na/us/cybersolv/wp-content/uploads/sites/10/2024/05/Partner-State-of-Malware-2024-Partner_03252024-2.pdf. (Accessed on September 8 2025)
[43]. McCarthy, A., Ghadafi, E., Andriotis, P., & Legg, P. (2022). Functionality-preserving adversarial machine learning for robust classification in cybersecurity and intrusion detection domains: A survey. Journal of Cybersecurity and Privacy, 2(1), 154-190.
[44]. Moore, D. (2022). Offensive cyber operations: Understanding intangible warfare. Oxford University Press.
[45]. Morgan, G. (2021). Ethical Issues in cybersecurity: employing red teams, responding to ransomware attacks and attempting botnet takedowns (Doctoral dissertation, Dublin City University).
[46]. Murthy, J. S., Siddesh, G. M., & Srinivasa, K. G. (Eds.). (2024). Cloud Security: Concepts, Applications and Practices. CRC Press.
[47]. Nadji, B. (2024). Data security, integrity, and protection. In Data, Security, and Trust in Smart Cities (pp. 59-83). Cham: Springer Nature Switzerland.
[48]. Naha, A. (2022). Emerging cyber security threats: India's concerns and options. International Journal of Politics and Security, 4(1), 170-200.
[49]. Nemeth, C. P. (2019). Private security and the investigative process. CRC Press.
[50]. Nemeth, C. P. (2022). Private security: An introduction to principles and practice. CRC Press.
[51]. Nonum, E. O., Avwokuruaye, O., & Umar, A. M. (2025). Social engineering: understanding human factors in cyber security. International Journal of Convergent and Informatics Science Research, 3(2), 16-37.
[52]. Odo, C. (2024). Strengthening cybersecurity resilience: The importance of education, training, and risk management. Training, and Risk Management (March 31, 2024).
[53]. Oettinger, W. (2022). Learn Computer Forensics–2nd edition: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence. Packt Publishing Ltd.
[54]. Okolie, U. C. (2022). Distinction between Traditional security and modern security: A conceptual discourse. Journal of Administrative Science, 19(2), 247-266.
[55]. Owuondo, J. O. (2025). Kenya's Hybrid Warfare Threats and National Security Infrastructure. National Security: A Journal of the National Defence University-Kenya, 3(1), 84-96.
[56]. Paul, R. (2021). Varieties of risk analysis in public administrations: problem-solving and polity policies in Europe. Routledge.
[57]. Prasad, R., & Rohokale, V. (2020). Cyber security: the lifeline of information and communication technology. Cham, Switzerland: Springer International Publishing.
[58]. Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 9(1), 28-78.
[59]. Reddick, C., Demir, T., & Perlman, B. J. (Eds.). (2025). Public Sector Ethics: Compliance, Integrity, and Comparison. Taylor & Francis.
[60]. Ryan, M. (2021). Ransomware Revolution: the rise of a prodigious cyber threat (Vol. 85). Berlin/Heidelberg, Germany: Springer.
[61]. Sehgal, K., & Thymianis, N. (2023). Cybersecurity Blue Team Strategies: Uncover the secrets of blue teams to combat cyber threats in your organization. Packt Publishing Ltd.
[62]. Shaheen, A. (2023). Cybersecurity in the Modern Era: An Overview of Recent Trends. Journal of Engineering and Computational Intelligence Review, 1(1), 39-50.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12758

[63]. Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics, 9(11), 1864.
[64]. Shapiro, L. R., & Maras, M. H. (Eds.). (2021). Encyclopedia of security and emergency management. Springer.
[65]. Stanisci, G. & Moffatt, F. (2024). Developing a Mature Public Safety and Security Analytics Capability. Information Management Capabilities in Public Safety and Security: Challenges, Strategies and Frameworks (pp. 123-154). Cham: Springer Nature Switzerland.
[66]. Staves, A. J. (2023). Operational Technology Preparedness: A Risk-Based Safety Approach to Scoping Security Tests for Cyber Incident Response and Recovery. Lancaster University (United Kingdom).
[67]. Stephens, D., Stubbs, M., & White, S. (Eds.). (2025). Digital Resilience: International and Domestic Legal Responses to Cyber Security and Artificial Intelligence. Springer Nature.
[68]. Stoddart, K. (2022). Cyberwarfare: threats to critical infrastructure. Springer Nature.
[69]. Thompson, E. C. (2018). Cybersecurity incident response: How to contain, eradicate, and recover from incidents. Apress.
[70]. Turner, J. I. (2019). Managing digital discovery in criminal cases. The Journal of Criminal Law and Criminology (1973-), 109(2), 237-312.
[71]. Vaid, M. S. (2023). Cyber Security Awareness, Challenges And Issues.
[72]. Vermesan, O., & Friess, P. (Eds.). (2022). Digitising the industry internet of things connecting the physical, digital and VirtualWorlds. CRC Press.
[73]. Wiener, H. M. (2022). Agile Enterprise Risk Management: Risk-based Thinking, Multi-disciplinary Management and Digital Transformation. CRC Press.
[74]. Willie, M. M. (2023). The role of organizational culture in cybersecurity: building a security-first culture. Journal of Research, Innovation and Technologies, 2(2 (4)), 179-198.

