INTEGRATING CYBER THREAT INTELLIGENCE WITHIN COMMERCIAL ENTERPRISES: A STRATEGIC FRAMEWORK FOR ENHANCED SECURITY POSTURE

Dr. Ahmed N. El-Tayeb
Cybersecurity and Digital Defense Research Unit, American University in Cairo, Egypt Prof.

Miguel Ángel Ortega
School of Business and Information Technology, Universidad de Sevilla, Seville, Spain

Published Date: 13 December 2024 // Page no.:- 6-13

ABSTRACT

Commercial organizations face an increasingly sophisticated and persistent cyber threat landscape, characterized by advanced persistent threats (APTs) and rapidly evolving attack methodologies. Traditional reactive cybersecurity measures, while necessary, are often insufficient against these dynamic challenges. Cyber Threat Intelligence (CTI) offers a proactive approach by providing actionable insights into adversaries, their motivations, capabilities, and tactics, techniques, and procedures (TTPs). This article proposes a strategic framework for the effective adoption and integration of CTI within commercial enterprises, structured around the IMRaD format. It examines the multifaceted nature of CTI, its lifecycle, and the critical organizational, technological, and cultural factors influencing its successful implementation. By detailing methodologies for acquiring, analyzing, and operationalizing CTI, this paper highlights its potential to significantly enhance an organization's security posture, improve incident response capabilities, and foster a more intelligence-driven defense. The discussion emphasizes the need for a holistic, adaptive approach to CTI, acknowledging both its transformative potential and the challenges in its full realization within existing organizational structures.

Keywords: Cyber threat intelligence (CTI); enterprise cybersecurity; security posture; threat mitigation; strategic framework; cyber risk management; information sharing; incident response; cybersecurity strategy; threat detection and analysis.

INTRODUCTION

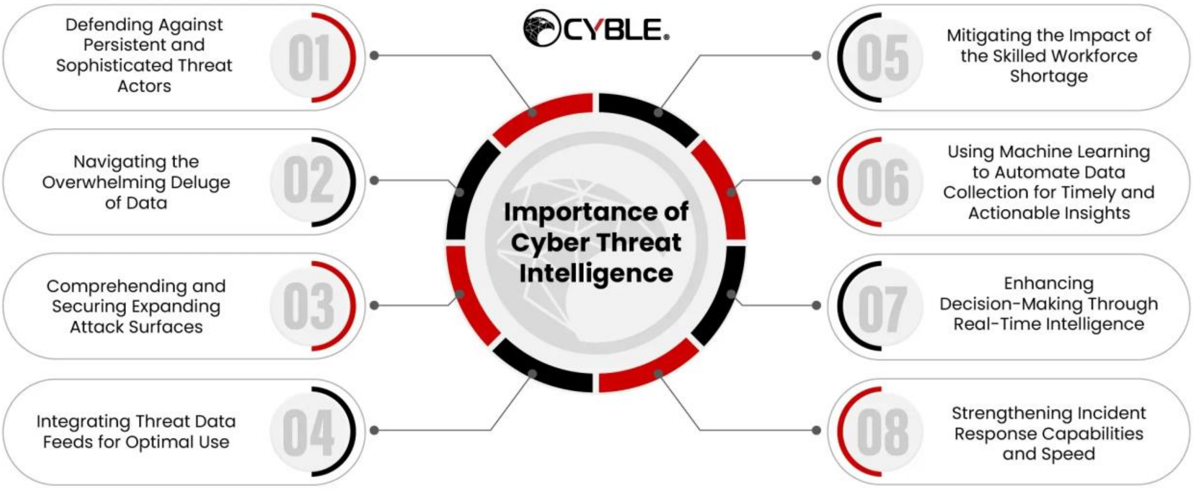
The contemporary digital landscape is fraught with an ever-growing array of cyber threats, ranging from sophisticated state-sponsored attacks and organized cybercrime to insider threats and financially motivated campaigns [1, 22, 32]. Commercial organizations, irrespective of their size or industry, are prime targets due to their valuable data, intellectual property, and critical operational systems. The sheer volume and complexity of these threats necessitate a shift from purely reactive defense mechanisms to more proactive, intelligence-driven cybersecurity strategies [6, 7]. While traditional cybersecurity investments in firewalls, intrusion detection systems, and antivirus software remain foundational, they often fall short in anticipating and countering novel or highly targeted attacks.

Cyber Threat Intelligence (CTI) has emerged as a crucial discipline to address this gap. CTI can be defined as evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard [17]. It moves beyond raw data or isolated alerts to provide contextualized, analyzed information that helps organizations understand *who* is attacking them, *why*, and *how* [10, 19, 30]. This enables defenders to transition from a reactive stance, merely responding to incidents, to a proactive one, anticipating threats and strengthening defenses before an attack materializes [7]. According to Sun Tzu, "If you know the enemy and know yourself, you need not fear the result of a hundred battles" [14], a principle that is increasingly relevant in the cyber domain. Despite the widely acknowledged benefits of CTI, its effective adoption and integration into commercial organizations remain challenging. These challenges stem from various factors, including the sheer volume of CTI data, the difficulty in discerning actionable intelligence from noise, the need for specialized skills, and the organizational complexities involved in embedding a new, intelligence-centric capability within existing security operations [12, 25]. Many organizations struggle with how to operationalize CTI, moving beyond simply consuming threat feeds to truly leveraging intelligence to inform strategic and tactical security decisions [4]. This often involves a deep understanding of organizational context, information systems, and the socio-technical interplay within cybersecurity operations [8, 23].

This article aims to propose a strategic framework for the successful adoption and integration of CTI within commercial enterprises. By drawing on established concepts from information technology implementation [9, 31], organizational behavior, and intelligence theory, it seeks to outline a comprehensive approach that addresses the methodological, technological, and cultural dimensions required to effectively leverage CTI for an enhanced security posture. The paper will detail the processes involved, from raw data acquisition to the actionable application of intelligence, and discuss the expected benefits and persistent challenges organizations may encounter.

2. Methods

The methodology for proposing a strategic framework for integrating Cyber Threat Intelligence (CTI) within commercial organizations draws upon a synthesis of established literature in information systems, cybersecurity, organizational change, and intelligence theory. This multi-disciplinary approach allows for a comprehensive understanding of the complex interplay between technology, processes, and people in the adoption of CTI.


CYBLE.
Importance of Cyber Threat Intelligence
01 Defending Against Persistent and Sophisticated Threat Actors
02 Navigating the Overwhelming Deluge of Data
03 Comprehending and Securing Expanding Attack Surfaces
04 Integrating Threat Data Feeds for Optimal Use
05 Mitigating the Impact of the Skilled Workforce Shortage
06 Using Machine Learning to Automate Data Collection for Timely and Actionable Insights
07 Enhancing Decision-Making Through Real-Time Intelligence
08 Strengthening Incident Response Capabilities and Speed

2.1. Foundational Concepts and Theoretical Lenses

The framework is built upon several core theoretical foundations:

- Diffusion of Innovations Theory (DOI): Rogers' DOI [24] provides a lens through which to understand how CTI, as an innovation, spreads through an organization. Key characteristics of CTI (relative advantage, compatibility, complexity, trialability, observability) influence its rate of adoption [9, 31]. This informs how CTI initiatives should be communicated, piloted, and scaled within an enterprise.
- Action Research (AR): AR, as a cyclical process of planning, acting, observing, and reflecting [3, 5, 21, 29], can be an ideal methodology for organizations to iteratively adopt and refine their CTI practices. It emphasizes learning by doing and addresses specific organizational problems [18].
- Sociotechnical Systems Theory: This perspective acknowledges that effective organizational change, particularly with information technology, requires balancing technical components with social and organizational aspects [8, 23]. CTI integration is not merely a technical implementation but also involves changes in roles, processes, and culture.
- Intelligence Cycle: Adapted from military intelligence [13], the CTI lifecycle typically involves planning and direction, collection, processing and

exploitation, analysis and production, and dissemination [17]. Understanding this cycle is fundamental to structuring CTI operations within a commercial context [12].

2.2. Defining Cyber Threat Intelligence (CTI)

CTI is categorized based on its focus and application within an organization:

- Strategic CTI: High-level, long-term intelligence focusing on adversary motivations, capabilities, and trends. It informs executive decision-making and overall security strategy [1, 6].
- Operational CTI: Mid-level intelligence on adversary TTPs, campaigns, and infrastructure. It helps security teams understand *how* specific attacks are conducted and prepare defenses [17, 20].
- Tactical CTI: Low-level, short-term indicators of compromise (IOCs) such as malicious IP addresses, domains, and file hashes. This is directly actionable for automated security tools [17].

The framework emphasizes that effective CTI integration requires a holistic approach that considers all three types, moving intelligence from raw data to actionable insights [10].

2.3. Phases of CTI Adoption and Integration

The proposed framework outlines key phases for CTI adoption and integration within a commercial organization:

2.3.1. Assessment and Planning

- Current State Analysis: Evaluate existing cybersecurity capabilities, incident response maturity [2], and information sharing practices. Identify gaps that CTI can address.
- Define Intelligence Requirements: Crucially, organizations must determine *what* intelligence is needed. This is driven by the organization's unique assets, threat landscape, and risk tolerance [17]. Intelligence requirements guide subsequent collection and analysis.
- Stakeholder Identification and Engagement: Identify key stakeholders (e.g., C-suite, IT security team, legal, risk management) and ensure their buy-in and understanding of CTI's value [11].
- Resource Allocation: Determine necessary budget for tools, training, and personnel.

2.3.2. Collection and Acquisition

- Sources of CTI:
    - Internal Sources: Logs, security events, vulnerability scans, previous incident reports [2, 7]. This is often the most relevant intelligence source as it pertains directly to the organization's environment.
    - External Sources: Commercial CTI vendors [16, 19], open-source intelligence (OSINT), government advisories, industry-specific information sharing and analysis centers (ISACs), and dark web monitoring.
- Collection Tools: Implement platforms for automated collection of threat feeds (e.g., STIX/TAXII compatible feeds), web scraping, and data enrichment.

2.3.3. Processing, Analysis, and Production

- Data Normalization and Enrichment: Raw threat data from diverse sources must be normalized and enriched with additional context (e.g., geolocation, historical data) to be useful.
- Threat Intelligence Platform (TIP): Implement a TIP to aggregate, de-duplicate, and manage threat indicators and intelligence reports.
- Human Analysis: This is the most critical step. Skilled CTI analysts are needed to contextualize data, identify patterns, attribute threats, and assess adversary motivations and capabilities [12, 30]. Analysts leverage models like the Kill Chain [17] to understand adversary campaigns [17].

- Intelligence Production: Transform analyzed data into actionable intelligence reports, alerts, and dashboards tailored to different audiences (e.g., executive summaries, technical IOCs for security operations). Measuring CTI quality is also important [28].

2.3.4. Dissemination and Operationalization

- Integration with Security Operations: Disseminate tactical CTI directly into security tools (SIEM, EDR, firewalls, SOAR) for automated detection and response. This automates blocking known bad indicators.
- Inform Incident Response: Operational and strategic CTI informs incident response playbooks, helps prioritize alerts, and aids in understanding the scope and nature of an attack [2, 7].
- Proactive Defense: Use intelligence to conduct threat hunting, refine security policies, improve vulnerability management, and prioritize security investments [4].
- Feedback Loop: Establish continuous feedback mechanisms from security operations back to the CTI team to refine intelligence requirements and improve the relevance and accuracy of CTI. This reflective practice is key to organizational learning [29].

2.4. Organizational Enablers

Beyond the technical processes, the framework emphasizes organizational enablers:

- Dedicated CTI Team/Function: A specialized team or designated personnel responsible for the entire CTI lifecycle.
- Cross-Functional Collaboration: Strong collaboration between CTI, Security Operations Center (SOC), incident response, IT infrastructure, and executive management.
- Training and Skill Development: Invest in training security practitioners to develop CTI capabilities [30].
- Clear Policies and Procedures: Define clear guidelines for CTI handling, sharing, and usage.
- Leadership Support: Executive sponsorship and understanding are crucial for resource allocation and integration [34].

3. Results

The successful adoption and integration of Cyber Threat Intelligence (CTI) within commercial organizations, guided by the proposed strategic framework, are hypothesized to yield a range of tangible and intangible benefits that collectively elevate the organization's cybersecurity posture. These results signify a fundamental shift from a reactive to a proactive and intelligence-driven defense strategy.

3.1. Enhanced Situational Awareness

A primary outcome of effective CTI integration is a significantly enhanced level of situational awareness regarding the evolving threat landscape [2, 33]. By systematically collecting, processing, and analyzing threat data, organizations gain a deeper understanding of who their adversaries are (their motivations and capabilities), what TTPs they employ, and what vulnerabilities they are likely to exploit [1, 17]. This moves beyond a mere understanding of individual security events to a comprehensive, contextualized view of the threats relevant to the organization. This awareness empowers security teams to anticipate attacks, rather than merely react to them, by understanding the "bigger picture" of adversary campaigns [17].

3.2. Improved Incident Response Capabilities

The operationalization of CTI directly translates into improved incident response capabilities [2, 7]. When a security incident occurs, readily available and actionable CTI provides critical context, allowing incident responders to:

- Rapidly Prioritize Alerts: By correlating internal alerts with known threat intelligence, security teams can quickly identify high-fidelity threats and prioritize their response efforts.

- Accelerate Investigation: CTI provides indicators of compromise (IOCs) and TTPs, enabling faster identification of compromised systems, lateral movement, and the scope of an attack [10].
- Inform Containment and Eradication: Understanding adversary TTPs helps in developing effective containment strategies and ensuring complete eradication of the threat from the network.
- Reduce Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR): The proactive insights from CTI reduce the time it takes to detect and respond to threats, minimizing potential damage.

3.3. Proactive and Predictive Defense

CTI empowers organizations to move from a reactive "whack-a-mole" approach to proactive and predictive defense. This is achieved through:

- Threat Hunting: Armed with CTI, security analysts can actively search for hidden threats within their networks that automated systems might miss [10]. This involves using intelligence about adversary TTPs to formulate hypotheses and actively look for evidence of compromise.
- Vulnerability Prioritization: CTI helps contextualize vulnerabilities by indicating which ones are actively being exploited by relevant threat actors. This enables organizations to prioritize patching and mitigation efforts on the most critical exposures.
- Security Control Optimization: Intelligence about adversary TTPs can be used to fine-tune existing security controls (e.g., firewall rules, intrusion prevention systems, endpoint detection and response configurations) to specifically block or detect known adversary techniques.
- Strategic Investment: Strategic CTI informs executive decision-making, guiding investments in new security technologies and capabilities based on an understanding of future threats and risks [4, 34].

3.4. Enhanced Risk Management

The integration of CTI significantly strengthens an organization's risk management framework. By providing a clearer picture of the evolving threat landscape and the likelihood of specific attacks, CTI enables more accurate risk assessments. This allows organizations to allocate resources more effectively to mitigate the most significant cyber risks, leading to a more resilient overall risk posture [33].

3.5. Improved Communication and Collaboration

A well-integrated CTI program fosters improved communication and collaboration within the security team and across the organization. The intelligence cycle necessitates clear communication channels for collecting requirements, disseminating intelligence, and gathering feedback. This promotes a shared understanding of threats among different security functions (e.g., SOC, incident response, vulnerability management) and bridges the gap between technical security teams and business leadership.

In essence, the adoption and integration of CTI transform an organization's cybersecurity from a static, reactive defense to a dynamic, intelligence-driven operation, ultimately leading to a more robust and adaptive security posture against the ever-present cyber threats.

4. Discussion

The results underscore that the effective integration of Cyber Threat Intelligence (CTI) within commercial organizations is not merely a technical undertaking but a strategic imperative that profoundly impacts an enterprise's overall security posture. The shift from a reactive to a proactive defense, driven by enhanced situational awareness and improved incident response, represents a fundamental evolution in cybersecurity practice. This transformation aligns with the recognition that information security requires a strategic balance between prevention and response [7].

The enhanced situational awareness gained through CTI is perhaps the most critical outcome. By systematically understanding adversary motivations, capabilities, and TTPs [1], organizations can anticipate threats and make informed decisions, much like military intelligence in strategic planning [13]. This enables a more intelligent deployment of defensive measures, moving beyond simply blocking known bad indicators to actively hunting for threats that bypass initial defenses. This proactive threat hunting, informed by CTI, is a key component of modern security operations [10].

The immediate impact on incident response is equally significant. In the fast-paced environment of cyberattacks, time is of the essence. CTI reduces the mean time to detect (MTTD) and mean time to respond (MTTR) by providing context, accelerating investigations, and enabling targeted containment and eradication [2]. This operational efficiency is vital for minimizing financial losses, reputational damage, and operational disruption caused by cyber incidents [32].

However, the journey to full CTI integration is fraught with challenges. One persistent hurdle is the volume and veracity of CTI sources. Organizations are inundated with vast amounts of threat data, much of which may be irrelevant, redundant, or even erroneous. The ability to filter noise, de-duplicate information, and ascertain the trustworthiness of intelligence sources is paramount [28]. This highlights the need for sophisticated Threat Intelligence Platforms (TIPs) and, more importantly, skilled human analysts capable of discerning actionable intelligence from raw data [12, 30].

Another significant challenge lies in operationalizing CTI. It's one thing to collect and analyze intelligence; it's another to seamlessly integrate it into existing security tools and workflows [4]. Many organizations struggle to translate strategic and operational intelligence into tactical actions that directly enhance their automated defenses or inform their incident response playbooks. This often requires significant engineering effort, automation, and a deep understanding of the organization's specific technology stack. The "diffusion of innovations" theory suggests that compatibility with existing systems and processes significantly influences adoption rates [9, 31].

Furthermore, organizational and cultural barriers can impede CTI adoption. These include a lack of dedicated resources, insufficient budget, a shortage of skilled CTI professionals, and a reluctance to embrace an intelligence-driven mindset [25]. Cybersecurity has historically been viewed as a technical function, and shifting to an intelligence paradigm requires changes in roles, responsibilities, and decision-making processes. Senior leadership buy-in and a clear articulation of CTI's return on investment are crucial for overcoming these barriers [34]. The concept of socio-technical design emphasizes that successful technology implementation must consider both the technical system and the social system in which it operates [23].

Future research should focus on several key areas. Firstly, developing more robust and automated methods for CTI quality assessment and relevance filtering could significantly reduce the burden on human analysts. This includes leveraging machine learning for anomaly detection in threat feeds and for prioritizing intelligence based on an organization's unique risk profile. Secondly, exploring measurement frameworks for CTI effectiveness beyond incident response metrics is vital. Quantifying the value of proactive defense and strategic intelligence remains a complex task. Thirdly, investigating novel approaches to CTI dissemination and operationalization that leverage emerging technologies like Artificial Intelligence and Robotic Process Automation could further bridge the gap between intelligence production and its actionable application within security tools. Finally, studying the evolution of CTI maturity models within commercial organizations through longitudinal action research studies could provide practical guidance for enterprises navigating this complex domain [3, 18, 26, 29].

5. Conclusion

The integration of Cyber Threat Intelligence is no longer a luxury but a fundamental requirement for commercial organizations striving to establish a resilient cybersecurity posture in today's dynamic threat landscape. By adopting a strategic framework that encompasses meticulous planning, diverse data collection, rigorous analysis, and seamless operationalization, enterprises can transition from reactive incident response to proactive, intelligence-driven defense. The results of such integration include enhanced situational awareness, improved incident response capabilities, and a strengthened overall security posture. While challenges related to data volume, operationalization complexities, and organizational readiness persist, the transformative benefits of CTI in anticipating and mitigating cyber threats make its strategic adoption an indispensable component of modern commercial security strategy. Organizations that effectively embed CTI within their operational fabric will be better equipped to defend against the sophisticated adversaries that define the contemporary cyber battleground.

References

[1] Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. Computers & Security, 86, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

[2] Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. Computers & Security, 101, 1–15. https://doi.org/10.1016/j.cose.2020.102122

[3] Avison, D. E., Lau, F., Myers, M. D., & Nielsen, P. A. (1999). Action research. Communications of the ACM, 42(1), 94–97. https://doi.org/10.1145/291469.291479

[4] Bank of England. (2016). Understanding cyber threat intelligence operations. https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

[5] Baskerville, R., & Wood-Harper, A. T. (1998). Diversity in information systems action research methods. European Journal of Information Systems, 7(2), 90–107. https://doi.org/10.1057/palgrave.ejis.3000298

[6] Baskerville, R. (2005). Information warfare: A comparative framework for business information security. Journal of Information System Security, 1(1), 23–50. https://www.jissec.org/Contents/V1/N1/V1N1-Baskerville.html

[7] Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management, 51(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

[8] Bostrom, R. P., Gupta, S., & Thomas, D. (2009). A meta-theory for understanding information systems within sociotechnical systems. Journal of Management Information Systems, 26(1), 17–48. https://doi.org/10.2753/MIS0742-1222260102

[9] Cooper, R. B., & Zmud, R. W. (1990). Information technology implementation research: A technological diffusion approach. Management Science, 36(2), 123–139. https://doi.org/10.1287/mnsc.36.2.123

[10] Crowdstrike. (2021). Threat intelligence: Cybersecurity's best kept secret. https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperThreatIntelligence.pdf

[11] Davenport, T. H., & Prusak, L. (1998). Working knowledge: How organizations manage what they know. Harvard Business Press.

[12] Ettinger, J. (2019). Cyber intelligence tradecraft report: The state of cyber intelligence practices in the United States. Retrieved from Carnegie Mellon University: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=546686

[13] FM 2-0. (2010). Field manual 2-0: Intelligence. Headquarters, Department of the Army.

[14] Giles, L. (1910). Sun Tzu on the art of war the oldest military treatise in the world translated from the Chinese is that is fixed. Sun Tzu On The Art Of War. Abingdon, Oxon: Routledge.

[15] Grover, V., Jeong, S. R., Kettinger, W. J., & Teng, J. T. (1995). The implementation of business process reengineering. Journal of Management Information Systems, 12(1), 109–144. https://doi.org/10.1080/07421222.1995.11518072

[16] Holland, R. (2015). Forrester. https://www.forrester.com/report/Vendor+Landscape+SR+Pros+Turn+To+Cyberthreat+Intelligence+Providers+Fo

r+Help/-/E-RES113066

[17] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Paper presented at the International Conference on Information Warfare and Security, Washington, DC, USA. Lockheed Martin Corporation.

[18] Iversen, J. H., Mathiassen, L., & Nielsen, P. A. (2004). Managing risk in software process improvement: An action research approach. MIS Quarterly, 28(3), 395–433. https://doi.org/10.2307/25148645

[19] Lawson, C., Contu, R., & Benson, R. (2019). Market guide for security threat intelligence products and services. Gartner. https://www.gartner.com/en/documents/3902168

[20] Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. Computers & Security, 72, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

[21] McKay, J., & Marshall, P. (2001). The dual imperatives of action research. Information Technology & People.

[22] Microsoft Corporation. (2020). Microsoft digital defense report. https://www.microsoft.com/en-us/download/details.aspx?id=101738

[23] Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. Information Systems Journal, 16(4), 317–342. https://doi.org/10.1111/j.1365-2575.2006.00221.x

[24] Rogers, E. M. (1995). Diffusion of innovations (4th ed.). Free Press.

[25] Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In: Holt T., Bossler A. (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham.135–154. https://doi.org/10.1007/978-3-319-78440-3_8

[26] Scheepers, R. (2006). A conceptual framework for the implementation of enterprise information portals in large organizations. European Journal of Information Systems, 15(6), 635–647. https://doi.org/10.1057/palgrave.ejis.3000646

[27] Schein, E. (1987). The clinical perspective in fieldwork. Sage.

[28] Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. International Journal of Information Security, 20, 21–38. https://doi.org/10.1007/s10207-020-00490-y

[29] Schön, D. A. (1983). The reflective practitioner: How professionals think in action. Basic Books.

[30] Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'cyberthreat-intelligence (cti) capability'that needs to be fostered in information security practitioners and how this can be accomplished. Computers & Security, 92, 101761. https://doi.org/10.1016/j.cose.2020.101761

[31] Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption–implementation: A meta-analysis of findings. IEEE Transactions on Engineering Management, 29(1), 28–45. https://doi.org/10.1109/TEM.1982.6447463

[32] Verizon Corporation. (2018). Data breach investigations report. https://www.verizonenterprise.com/verizon-insights-lab/dbir/

[33] Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. Computers & Security, 44(July 2014), 1–15. https://doi.org/10.1016/j.cose.2014.04.005

[34] Weill, P., & Broadbent, M. (1998). Leveraging the new infrastructure: How market leaders capitalize on information technology. Harvard Business Press.