MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

Cyber Threats and Workplace Vulnerabilities: A Strategic Approach to Cyber Protection Management

Shonan Kanuga[1], Dr. G. Sathish Kumar[2]
[1]Research Scholar, [2]Guide
[1,2] Department of Management and Commerce, Nims University Rajasthan, Jaipur
[1]advshonan@gmail.com, [2]sathish.kumar@nimsuniversity.org

Abstract

The modern work environment, embodying a digital environment of interconnection and working remotely, is confronted with the unstopping range of cyber threats that capitalize on the technological and human weaknesses. The strategic framework of Cyber Protection Management (CPM) described in this paper is aimed at striking the balance between the tactical implementation of cybersecurity and organizational strategic goals. Based on the recent reports in the industry (IBM, 2023; Verizon, 2024) and academic studies published after 2021, we review the dynamic nature of cyber losses, the importance of Situation Awareness (SA), and the incorporation of Cyber Threat Intelligence (CTI) in the risk management procedures. Our hypothesized risk assessment methodology is a new dynamic framework that can be used to promote proactive defense by tapping into the frameworks such as MITRE ATT&CK and combining CTI platforms. The paper concludes with the strategic CPM model, which is justified by a design science research approach, which aligns security investments with business priorities and optimizes incident response and promotes a resilient organizational culture. The results show that an integrated, intelligence-based, and strategic response is the most important to reduce the effects of breaches (financial and operational) in the contemporary digital workplaces.

Keywords: Cyber Protection Management (CPM), Dynamic Risk Assessment, Strategic Cybersecurity Governance, Intelligence-Led Security, Hybrid Work Security

1. Introduction

The cyber revolution of the workplace has permanently increased the size of the attack surface of organizations across the globe. The convergence of cloud services, Internet of Things (IoT) devices, and hybrid work models has created a complex environment in which technological vulnerabilities intersect with human factors, particularly susceptibility to social engineering attacks (Verizon, 2024). The economic implications are substantial, with the average global cost of a data breach reaching USD 4.45 million in 2023—an increase of nearly 15 percent over the past three years (IBM, 2023). Beyond direct financial losses, cyber incidents increasingly result in reputational damage, operational disruption, regulatory penalties, and long-term erosion of stakeholder trust (Bederna and Szádeczky, 2023).

Conventional cybersecurity practices—largely compliance-driven, control-centric, and operationally siloed—are increasingly inadequate in addressing the agility, adaptability, and intelligence-driven nature of contemporary cyber adversaries. This limitation has prompted a growing recognition of the need to transition from tactical, tool-oriented security postures toward a strategic and holistic **Cyber Protection Management (CPM)** paradigm. Prior research emphasizes that effective CPM must extend beyond technical safeguards to incorporate intelligence-led risk awareness and deep integration within organizational strategy and governance structures (Mizrak, 2023; Kotsias et al., 2023).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

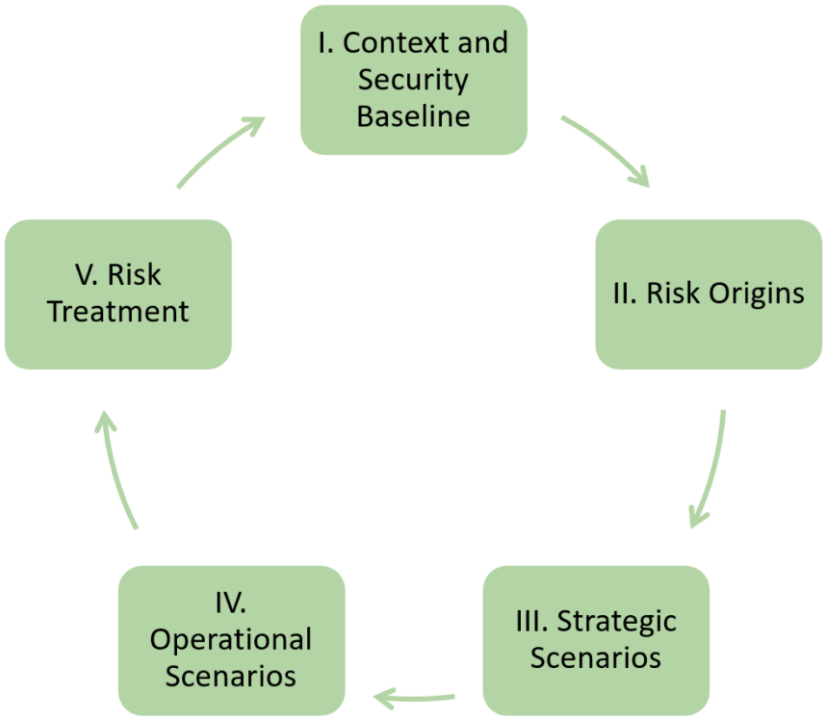

Figure 1. EBIOS Risk Manager workshops

This figure illustrates the structured, workshop-driven nature of contemporary risk management approaches, emphasizing stakeholder involvement and iterative threat evaluation. Its relevance lies in demonstrating how risk assessment is no longer a purely technical exercise but an organizational process requiring cross-functional coordination. Within the proposed CPM framework, such participatory risk identification mechanisms support strategic alignment by ensuring that cyber risks are contextualized in relation to business objectives and decision-making structures.

Recent scholarship has further reinforced the shift from reactive cybersecurity controls toward resilience-oriented and measurement-driven approaches. Abdelkader et al. (2024) demonstrate that securing complex digital infrastructures—particularly cyber-physical and power systems—requires integrated strategies that combine technical controls with organizational preparedness and adaptive governance. Extending this perspective, Alhidaifi et al. (2025) propose a probabilistic cyber resilience quantification model (PEQCRM) that enables systematic estimation of infrastructure resilience under uncertainty, highlighting the growing emphasis on quantifiable, decision-support-oriented cybersecurity metrics. Similarly, Lezzi et al. (2025), through a systematic review of industrial IoT environments, emphasize the need for structured frameworks capable of measuring cyber resilience across technological and organizational dimensions. Collectively, these studies underscore a critical gap in existing research: while resilience measurement and quantification models are advancing, their integration into a unified, strategic Cyber Protection Management framework aligned with organizational governance remains limited, thereby motivating the approach proposed in this study.

What is new in this study is the explicit positioning of Cyber Protection Management as a strategic, intelligence-led organizational capability rather than a purely technical or operational function. While existing studies have examined cyber threat intelligence (CTI), risk assessment methodologies, and adversary frameworks such as MITRE ATT&CK largely in isolation, this paper advances the literature

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

by integrating these elements into a unified strategic CPM framework aligned with business governance and decision-making processes. Specifically, the study introduces a dynamic, intelligence-driven CPM model that (i) embeds CTI directly into continuous risk assessment mechanisms, (ii) contextualizes organizational risk using adversary behavior mapped through the MITRE ATT&CK framework, and (iii) aligns cybersecurity investments and response strategies with enterprise-level objectives and resilience goals. By doing so, the paper addresses a critical gap in current research, which often lacks a coherent linkage between cyber risk intelligence and strategic management at the organizational level.

Figure 2: Cyber threat intelligence process

This figure highlights the cyclical and intelligence-driven nature of cyber threat intelligence, encompassing data collection, analysis, dissemination, and feedback. It underscores the importance of transforming raw threat data into actionable insights rather than isolated technical indicators. In the context of CPM, this process forms the backbone of intelligence-led risk assessment, enabling proactive defense and continuous recalibration of security priorities in response to evolving threats.

Using leading academic and industry references published from 2021 onward, the present study seeks to: (1) examine the evolving landscape of cyber threats and workplace vulnerabilities; (2) critically synthesize contemporary approaches to cyber risk assessment and threat intelligence integration; and (3) propose a holistic, strategic CPM framework capable of supporting proactive defense and organizational resilience. The study adopts a design science research approach (Hevner et al., 2004) to develop and present the proposed CPM framework as a conceptual artifact grounded in recent empirical insights and theoretical advancements in cybersecurity and strategic management.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

2. The Changing Landscape: Threats, Vulnerabilities and Costs

2.1. Cyber Losses and Business Impact Nature

Losses resulting out of cyber activities are no longer single entities but are grouped in various vectors. Shevchenko et al. (2023) classify the types of losses as direct financial (e.g., ransom, fraud), operational (e.g., business interruption, data loss), and strategic (e.g., reputational harm, loss of intellectual property). The industry has a great impact on loss profile; one example is that the financial sector experiences greater direct financial fraud whereas healthcare is more affected by operational disruptions.

IBM Cost of a Data Breach Report 2023 contains essential quantitative data, according to which the average lifecycle of breach is 277 days (212 to discover, 65 to contain), and the organizations with high utilization of security AI and automation had a 108-day shorter lifecycle that saved organizations around 1.76 million on average (IBM, 2023). This highlights the financial necessity of high-level, computerized security measures.

2.2. Workplace Vulnerabilities and Primary Attack Vectors.

The Verizon 2024 Data Breach Investigations Report (DBIR) is still the most renowned source of information on attack vectors. Some of the main trends applicable in the workplace are:

Human Element: More than 68 percent of breaches include a non-malicious human component (e.g. error, misuse) or social engineering (e.g. phishing). Phishing is a leading initial access method.

System Intrusions: It is the most popular type of breach that is frequently based on compromised credentials or on vulnerabilities.

Ransomware: With more than 24 percent of the attacks, ransomware remains a leading threat ever, and it is rampant across all industries (Verizon, 2024).

These results indicate that the vulnerabilities at the workplace are more about people and processes than they are about technology. These risks are compounded by the hybrid working model, which extends the corporate security boundaries to home networks and personal devices that are not managed.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

Table 1: Top Cyber Threat Vectors and Associated Workplace Vulnerabilities (Synthesized from IBM, 2023; Verizon, 2024)

Threat Vector	Description	Key Workplace Vulnerability Exploited	Typical Business Impact
Phishing & Social Engineering	Deceptive communications to trick users into revealing credentials or executing malware.	Lack of security awareness; pressure of remote work; trust in apparent authority.	Credential compromise; initial network access; data exfiltration.
Exploitation of Public-Facing Apps	Attackers scan for and exploit vulnerabilities in web applications, VPNs, and servers.	Slow patch management cycles; misconfigured cloud services; legacy systems.	System intrusion; data breach; ransomware deployment.
Compromised Credentials	Use of stolen or weak usernames/passwords to gain unauthorized access.	Poor password hygiene; lack of multi-factor authentication (MFA); credential reuse.	Unauthorized data access; lateral movement; privilege escalation.
Ransomware	Malware that encrypts data, demanding payment for decryption.	Often follows initial access via phishing or credential compromise; inadequate backups.	Operational halt; financial loss (ransom/extortion); reputational damage.
Insider Threats (Negligent/Malicious)	Actions by employees or contractors that harm security, either unintentionally or deliberately.	Inadequate access controls; lack of monitoring; employee dissatisfaction.	Data theft (IP, PII); sabotage; compliance violations.

This table synthesizes key cyber threat vectors with corresponding workplace vulnerabilities and business impacts, providing a consolidated view of how human, technological, and process-related weaknesses are exploited. Its significance lies in linking threat mechanisms directly to organizational consequences rather than isolated technical failures. For CPM, this mapping supports risk-informed prioritization of controls and awareness initiatives, particularly in hybrid work environments where human-centric vulnerabilities are amplified.

3. Research Methodology

This study adopts a Design Science Research (DSR) approach (Hevner et al., 2004) to develop a strategic Cyber Protection Management (CPM) framework addressing the limitations of compliance-driven and operationally fragmented cybersecurity practices in contemporary hybrid workplaces.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

The research problem is defined as the absence of a strategically integrated, intelligence-led cybersecurity management model aligned with organizational governance and decision-making. Accordingly, the objective is to design a CPM framework that systematically integrates cyber threat intelligence, dynamic risk assessment, and adversary behavior modeling within a business-oriented strategic structure.

The framework is designed and developed through structured synthesis of post-2021 academic literature, industry reports, and established cybersecurity standards. Its applicability is demonstrated conceptually by mapping framework components to recognized mechanisms such as the MITRE ATT&CK framework, CTI processes, and advanced risk assessment models.

Evaluation of the artifact is theoretical and analytical rather than empirical, relying on internal coherence, logical consistency, and alignment with validated findings reported in prior studies. This approach is consistent with early-stage DSR and provides a foundation for subsequent empirical validation.

4. Pillars of Strategic Management of Cyber Protection.

4.1. The aspects of Cybersecurity as part of Strategic Management.

To be effective, cybersecurity should no longer have an IT-centric role. In a well-formed literature review, Mizrak (2023) persuades that cybersecurity risk management should be completely incorporated into strategic management processes. This is done by aligning the security-focused objectives with the business goals, having board-level supervision, and seeing cybersecurity as a primary facilitator of business continuity and digital confidence instead of just a cost centre. Strategic integration will help give security investment top priority considering its contribution to the mitigation of risks that can derail strategic objectives.

4.2. Constructing Organizational Situation Awareness (SA).

The situation of responding effectively to the incident depends on the capacity of an organization to gain and sustain Situation Awareness (SA). In a case study, Ahmad et al. (2021) outline the key practices needed to develop SA: (1) Intense sharing and communication of information among technical and management teams; (2) The use of visualization tools to understand the threat environment; and (3) The establishment of a culture of collaboration which disintegrates silos between IT, security, and business divisions. Their work shows that SA is not a passive state but an active organizational capacity, which has to be developed in order to be able to make timely and informed decisions under crisis situations.

4.3. The Integration of Cyber Threat Intelligence (CTI) Imperative.

Cyber Threat Intelligence (CTI) delivers the evidence-based information regarding the existing or new threats required to inform security-related decisions. Kotsias et al. (2023) address the topic of adoption and integration of CTI in a commercial organization and outline the main success factors: organizational buy-in, process alignment (making CTI a part of established security processes, such as vulnerability management and incident response), and technical integration (by using standard formats such as STIX and platforms such as OpenCTI or MISP). They assume that CTI changes the reactive security stance to the proactive posture by revealing the tactics, techniques and procedures (TTPs) of the adversary.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

5. Integrating the Next Generation Strategies: Risk Assessment to Intelligence-led Response.

5.1. Evolution Towards Dynamic Risk Assessment.

The dynamic cyber threat environment cannot be covered by static and periodic risk assessments. In the system of the literature review, Cheimonidis and Rantos (2023) define Dynamic Risk Assessment (DRA) as an ongoing process that adjusts the level of risk in real-time depending on the alterations in the threat environment, the value of assets, and the vulnerability of systems. Ferreira et al. (2023) present a version of the predictive approach called Predictive Cyber Security Risk Assessment (PCSRA) based on machine learning usage to predict attack directions and their effects. These strategies are the needed transition of the point-in-time analysis into continuous monitoring and prediction.

5.2. Using Adversary Frameworks The MITRE ATT&CK Benefit.

The MITRE ATT&CK framework offers a publicly available body of knowledge of adversary TTPs, which is organized according to the cyber attack lifecycle (Strom et al., 2018). It is a major innovation in its incorporation in the risk assessment. Ahmed et al. (2022) suggest an approach to the assessment of cyber risks based on the MITRE ATT&CK, wherein assets and vulnerabilities of an organization are mapped to particular techniques used by adversaries to determine the probability of occurrence and the severity of such a multi-step attack. This enables organizations to place their risks in context of actual adversary behavior making the prioritization of risks more applicable and practical.

Table 2: Comparison of Advanced Risk Assessment Methodologies Incorporating CTI (Post-2021)

Methodology / Study	Core Approach	Integration of CTI	Key Strength	Primary Use Case
PCSRA (Ferreira et al., 2023)	Predictive analytics & ML to forecast attack paths and risk.	Implicit; uses threat data to train predictive models.	Proactive risk forecasting; quantitative output.	Organizations with mature data analytics capabilities.
MITRE ATT&CK-Driven (Ahmed et al., 2022)	Maps assets/vulnerabilities to adversary TTPs from ATT&CK matrix.	Direct and explicit; ATT&CK is a structured CTI source.	Contextualizes risk within real-world adversary behavior.	Prioritizing defenses against most likely attack chains.
Hybrid Model (Lyvas et al., 2022)	Combines traditional RA models with runtime behavioral monitoring.	CTI informs threat likelihood and TTPs for monitoring.	Balances proactive assessment with real-time detection.	Cyber-Physical Systems (CPS) and critical infrastructure.
Threat-Intelligence Driven with Uncertainty (Dekker & Alevizos, 2023)	Incorporates probabilistic models to handle uncertainty in CTI data.	Central; CTI feeds are modeled with confidence levels.	Enhances decision-making under uncertainty.	Strategic planning and resource allocation.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

This comparison demonstrates the evolution of cyber risk assessment from static, compliance-based models toward dynamic and intelligence-integrated approaches. It reveals how methodologies incorporating CTI and adversary behavior provide greater contextual accuracy and decision relevance. Within the CPM framework, these insights justify the adoption of dynamic, intelligence-led risk assessment as a strategic capability rather than a periodic reporting activity.

Table 3: Cyber Protection Management

Category	Publication Year	Key Contribution & Relevance to Strategic CPM	Limitations / Notes
1. Threat Landscape & Impact Analysis			
	2023	Provides critical quantitative benchmarks: global average breach cost (₹36.94 crore), impact of security AI/automation (108-day shorter lifecycle, ₹14.61 crore savings), and key cost factors (e.g., cloud security, remote work). Essential for financial justification of CPM investments.	Proprietary report; methodology behind data collection is not peer-reviewed.
	2023	Categorizes cyber losses into direct financial, operational, and strategic. Highlights how loss profiles vary by business sector. Provides a nuanced framework for understanding the full business impact beyond immediate costs.	Conceptual model; requires organizational data for specific application.
	2024	The authoritative source on attack vectors. Key findings: 68% of breaches involve the human element, credential theft is a top action, ransomware remains prevalent. Critical for identifying and prioritizing workplace vulnerabilities (people, processes, technology).	Descriptive statistics; focuses on patterns rather than prescriptive solutions.
	2023	Discusses strategies for financial risk transfer and retention post-incident. Connects technical incidents to financial management, supporting the strategic integration pillar of CPM.	Focuses on post-incident financial management rather than proactive prevention.
2. Strategic & Organizational Integration			

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

	2023	Makes a compelling case for elevating cybersecurity from an IT issue to a core strategic management concern. Argues for board-level oversight and alignment with business objectives. Foundational for the Governance & Strategy pillar.	A review paper; synthesizes existing arguments rather than presenting new empirical data.
	2021	Identifies key practices for building Organizational Situation Awareness (SA): effective communication, visualization tools, and a collaborative culture. Vital for effective incident response and the Resilience & Response pillar.	Single case study; findings may not be universally generalizable.
	2023	Provides data on market trends and spending, indicating where the industry is investing (e.g., cloud security, AI). Useful for contextualizing strategic decisions and budget planning within CPM.	Gated/paywalled report; only summary insights are typically available.
3. Threat Intelligence & Integration			
	2023	Explores the organizational process of CTI integration. Identifies success factors: organizational buy-in, process alignment, and technical integration (e.g., with STIX/TAXII, OpenCTI). Core to the Risk Intelligence & Assessment pillar.	Focuses on commercial organizations; may not fully address public sector or critical infrastructure nuances.
	2020	Explains the CTI capability needed by practitioners. Provides a theoretical foundation for developing human analytical skills, complementing the technical integration focus of Kotsias et al.	Published in 2020; pre-dates some of the latest platform developments but theory remains sound.
	2023	Proposes a novel methodology to incorporate uncertainty from CTI feeds into risk analysis using probabilistic models. Addresses a key challenge in making CTI actionable for strategic decision-making.	Preprint; not yet peer-reviewed.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

4. Advanced Risk Assessment Methodologies			
	2023	Defines and reviews Dynamic Risk Assessment (DRA), establishing the need for continuous, real-time risk updating over static assessments. Provides the conceptual basis for a key component in the CPM framework.	A review; does not propose a specific new methodology.
	2023	Proposes a predictive, ML-driven risk assessment model. Represents the evolution towards proactive, data-driven risk forecasting, aligning with the DRA concept.	Proposed methodology; requires empirical validation in diverse environments.
	2022	Presents a practical method for mapping organizational assets to MITRE ATT&CK techniques. Crucial for contextualizing risk within real-world adversary behavior, making risk assessments more relevant and actionable.	Technical focus; requires expertise to implement the ATT&CK mapping.
	2022	Demonstrates a hybrid model combining traditional RA with runtime monitoring for Cyber-Physical Systems (CPS). Shows the application of DRA principles in a critical context (e.g., industrial workplaces).	Specific to CPS; adaptation needed for general IT/OT environments.
5. Foundational Frameworks & Standards			
	2022	A comprehensive survey of major risk management frameworks (e.g., ISO 27005, NIST SP 800-30, OCTAVE, EBIOS). Provides the landscape of tools from which organizations can select and adapt components for their CPM strategy.	Descriptive compendium; does not prescribe a specific integration path.
	2020	Proposes a lightweight, pragmatic RA method suitable for fast-paced decision-making. Useful for organizations needing a practical, less	"Lightweight" approach may not suffice for highly regulated or critical sectors.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

		resource-intensive starting point for risk assessment.	
	2023	Proposes an innovative framework using blockchain for secure, transparent risk information sharing in collaborative environments (e.g., supply chains). Points to future directions for enhancing trust in shared risk intelligence.	Conceptual/early-stage framework; significant technical and adoption hurdles remain.
6. References Excluded from Core Analysis (Pre-2021 or Limited Relevance)			
	2021	Foundational works in cyber warfare, intrusion analysis (Diamond Model, Kill Chain, Pyramid of Pain). Important historically but superseded by more integrated frameworks like MITRE ATT&CK for contemporary CPM.	Excluded from detailed review per the 2021+ requirement, though their concepts underpin modern CTI.
	2021	Focus on specific domains (healthcare, IoT) or techniques (ML for IDS). Relevant for specialized applications but not central to the overarching strategic management thesis.	Provide context but not directly aligned with the core strategic, organizational focus.
	2021	Discuss the EBIOS Risk Manager methodology. While a robust framework (cited in ENISA compendium), the specific references are not recent enough for the core analysis, though the framework itself remains relevant.	The framework is valid, but these specific citations are supplemental.
	Various	Established risk assessment methodologies/tools. Included in the ENISA (2022) compendium. They represent available options within the ecosystem but are not the focus of recent innovation discussed in the paper.	Important for practitioner awareness but not the subject of recent scholarly advancement post-2021.

6. A Strategic Framework of Proposed Cyber Protection Management (CPM)

Based on the literature examined, we put forward the Strategic Cyber Protection Management (CPM) Framework, which is holistic. This model, as depicted in Figure 1, should be an iterative, intelligence-led and business strategy-oriented model.

The framework will have four strategic pillars, which are interdependent and each is composed of core operational elements.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

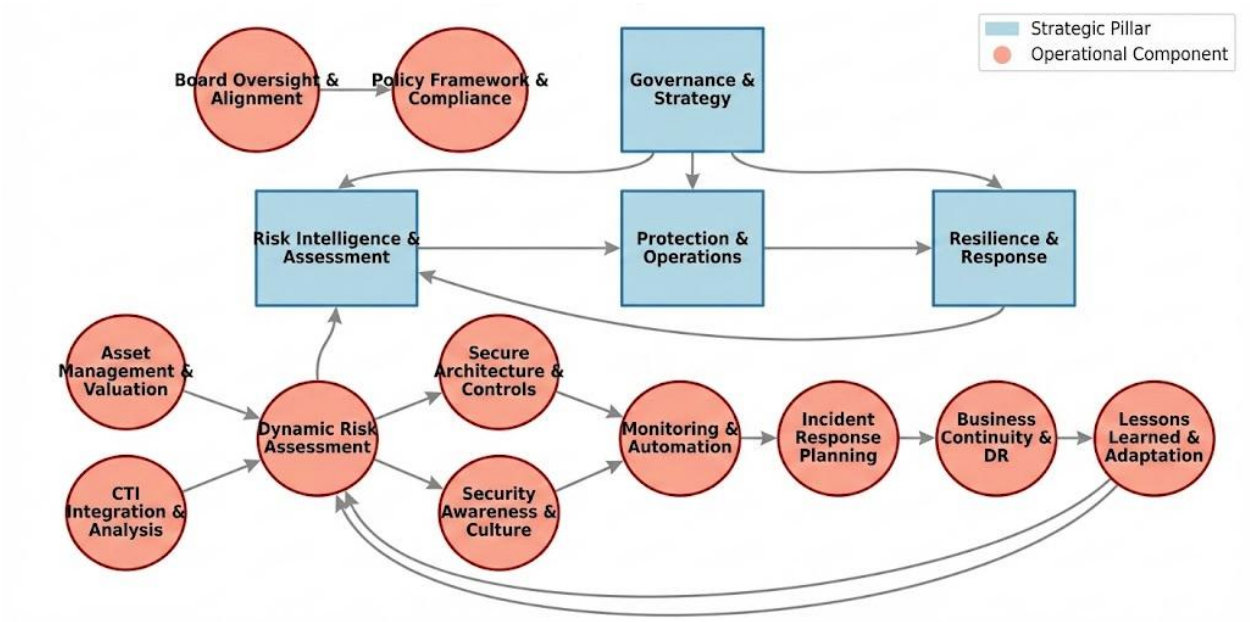

Figure 3: The Strategic Cyber Protection Management (CPM) Framework

This figure presents the integrated CPM framework, illustrating the interdependence between governance, risk intelligence, protection operations, and organizational resilience. Its importance lies in visually demonstrating cybersecurity as a continuous, strategic management cycle rather than a linear technical process. By aligning intelligence, risk assessment, and operational response with business governance, the framework operationalizes CPM as a strategic enabler of organizational resilience.

6.1. Pillar 1: Governance and Strategy.

This pillar makes cybersecurity a board-level issue, which is working hand in hand with business purposes.

Value Chain: Board Oversight and Alignment. Create a cyber risk board committee, which should ensure that security strategy contributes to business growth, digital transformation, and compliance requirements (Mizrak, 2023).

Part: Policy Framework and Compliance. Write and implement policies (e.g. acceptable use, data handling, remote work) that are dynamically agile and responsive to the changing threat and regulatory environment.

6.2. Pillar 2: Risk Intelligence and Assessment.

This pillar is aimed at ensuring that the threat landscape and organizational risk posture is kept informed and continuously.

Others: Asset Management and Valuation. Have a dynamic list of digital assets (data, systems, applications) that has a business criticality value assigned to it.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

Part: CTI Integration and Analysis. Institute measures to ingest, process and share tactical, operational and strategic CTI both internal and external (Kotsias et al., 2023). Manage with systems such as OpenCTI or MISP.

Component: Dynamic Risk Assessment. Utilize a DRA approach (e.g., incorporating MITRE ATT&CK according to Ahmed et al., 2022) that keeps recalculating the risk scores due to CTI feeds, vulnerability scans, and business context.

6.3. Pillar 3: Protection and Operations.

This pillar is a translation of risk intelligence into implemented security measures and operations.

Component: secure Architecture and Controls. Defend in depth based on outputs of risk assessment. Prioritize controls (e.g., Zero trust, encryption, MFA) which address high-likelihood/high-impact ATT&CK techniques.

Personality: Security Awareness and Culture. Take phishing simulation and scenario-based training instead of annual training and move to a continuous engagement model, based on current threats (Verizon, 2024).

Aspect: Monitoring and Automation. Implement Security Orchestration, Automation and Response (SOAR) systems and SIEM systems driven by CT to identify TTPs identified by Pillar 2. Use AI to find anomalies and minimize response time (IBM, 2023).

6.4. Pillar 4: Response and Resilience.

This pillar makes sure that the organization can withstand, respond and recover about incidents.

Overview: Incident Response Planning. Create and test IR playbooks, which are based on CTI and ATT&CK scenarios, and have well-defined roles and communication channels (Ahmad et al., 2021).

Element: Business Continuity and Disaster Recovery (BC/DR). Correlate BC/DR plans with cyber incidences, to be able to restore critical activities within acceptable time periods.

Lesson learned and adaptation are considered a component. Carry out formal post-incident reviews to refresh CTI understanding, enhance risk evaluation, and improve controls and procedures and complete the circle of feedback to Pillar 2 and 1.

7. Discussion: Strategic Benefits and Implementation Problems.

The CPM framework presented has a number of strategic benefits. It also bridges the intelligence gap, by officially connecting post incident lessons to CTI and risk models. It maximizes allocation of resources by focusing more on investments as opposed to adversary behaviors that are most pertinent

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

to the organization. Lastly, it develops systemic resilience by bringing together technical, human, and process components into an aligned strategy that is business-centric.

Nevertheless, there are problems with implementation. The integration needed to implement SA can be blocked by the cultural resistance to the de-silosification of business and security departments (Ahmad et al., 2021). The amount and quality of CTI can be overwhelming; companies have to acquire the analytical capacity to filter and place information into context (Kotsias et al., 2023). Additionally, the ROI of proactive, intelligence-led security is hard to quantify, but frameworks that relate controls and mitigated ATT&CK methods can contribute to its articulation.

8. Conclusion

The contemporary work environment is a good target in a highly advanced cyber threat environment. Protecting it needs a radical change in the currently fragmented and reactive security practices to coherent strategic management field. The current paper has summarized the current research to present the argument that the successful Cyber Protection Management needs to be embedded within strategic integration, ongoing risk intelligence, and situational awareness of the organization.

The Strategic CPM Framework that is proposed allows following the blueprint of this change. With governance, risk assessment over time with energy provided by CTI and adversary models such as MITRE ATT&CK, proactive defenses and resiliency response mechanisms, organizations can build a more predictive and adaptive security posture. The future research ought to be based on the idea of empirical validation of this framework in various organizational settings, standardized measures of CPM maturity, and investigation of the role of AI in the model of automating the intelligence-to-action cycle. At a time of incessant cyber attacks, strategic, integrated and smart approach to Cyber Protection Management is not only and only an IT issue but a fundamental determinant of organizational survival and success.

Managerial and Policy Implications

From a managerial and policy perspective, the proposed Cyber Protection Management (CPM) framework offers actionable guidance for multiple organizational stakeholders. For Chief Information Security Officers (CISOs), the framework provides a structured mechanism to translate cyber threat intelligence and dynamic risk signals into prioritized control investments and response strategies. For board members and senior executives, CPM enables informed oversight by linking cybersecurity initiatives to business objectives, risk appetite, and organizational resilience, thereby supporting strategic decision-making and governance accountability. Risk managers can leverage the intelligence-led and continuous risk assessment approach to move beyond static compliance reporting toward forward-looking risk prioritization. In the context of hybrid workforce policies, the framework highlights the need to embed human-centric risk awareness, adaptive controls, and situational awareness into remote work governance, ensuring that security policies evolve alongside changing work practices. Collectively, these implications underscore the practical relevance of CPM as a strategic enabler rather than a purely technical function.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

9. Limitations and Future Research Directions

This study proposes a conceptual Cyber Protection Management (CPM) framework validated through a systematic synthesis of recent academic literature and industry reports. As the framework has not yet been empirically tested, its effectiveness across different organizational sizes, industries, and cybersecurity maturity levels cannot be quantitatively assessed.

Future research should focus on empirical validation and practical application of the proposed model. In particular, organizational case studies can examine implementation feasibility and contextual challenges, while survey-based quantitative studies may assess the relationship between CPM maturity, cyber resilience, and organizational performance. Further work may also establish industry-specific benchmarks and maturity indicators to support comparative evaluation and strategic decision-making. Additionally, future studies could explore the role of artificial intelligence and automation in strengthening intelligence-led risk assessment and response within CPM.

References

1. Abbass, W.; Baina, A.; Bellafkih, M. Using EBIOS for risk management in critical information infrastructure. In *Proceedings of the 2015 5th World Congress on Information and Communication Technologies (WICT)*, Marrakech, Morocco, 14–16 December 2015; pp. 107–112.
2. Abdelkader, S.; Amissah, J.; Kinga, S.; et al. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *2024*.
3. Ahmad, A.; Maynard, S.B.; Desouza, K.C.; Kotsias, J.; Whitty, M.T.; Baskerville, R.L. How can organizations develop situation awareness for incident response: A case study of management practice. *Comput. Secur.* 2021, *101*, 102122.
4. Ahmed, M.; Panda, S.; Xenakis, C.; Panaousis, E. MITRE ATT&CK-driven cyber risk assessment. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, Vienna, Austria, 23–26 August 2022; pp. 1–10.
5. Akyeşilmen, N. Cybersecurity and cyberwar: What everyone needs to know. *Cyberpolitik J.* 2016, *1*, 368–372.
6. Alhidaifi, S.; Asghar, M.R.; Ansari, I.S. Cyber resilience quantification: A probabilistic estimation model for IT infrastructure (PEQCRM). *Reliability Engineering & System Safety* 2025.
7. Alnajim, O.A.; Kautzman, D.M. Towards a conceptual cyber risk assessment framework for healthcare systems. *Procedia Comput. Sci.* 2017, *121*, 785–792.
8. ANSSI. *EBIOS Risk Manager: Going Further*; Technical Report; ANSSI: Paris, France, 2019; Version 1.0.
9. Bederna, Z.; Szádeczky, T. Managing the financial impact of cybersecurity incidents. *Secur. Def. Q.* 2023, *41*, 15–35.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

10. Belfadel, A.; Boyer, M.; Letailleur, J.; Petiot, Y.; Yaich, R. Towards a security impact analysis framework: A risk-based and MITRE ATT&CK approach. In *Proceedings of the European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 212–227.
11. Bianco, D. The pyramid of pain. 2013. Available online: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (accessed on 31 May 2024).
12. BSI. *BSI-Standard 200-2: IT-Grundschutz-Methodology*. Available online: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html (accessed on 4 February 2023).
13. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* 2016, *18*, 1153–1176.
14. Caltagirone, S.; Pendergast, A.; Betz, C. The diamond model of intrusion analysis. *Threat Connect* 2013, 1–61.
15. Cheimonidis, P.; Rantos, K. Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet* 2023, *15*, 324.
16. Dekker, M.; Alevizos, L. A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision making. *arXiv* 2023, arXiv:2302.13082.
17. El Amin, H.; Oueidat, L.; Chamoun, M.; Samhat, A.E.; Feghali, A. Blockchain-based multi-organizational cyber risk management framework for collaborative environments. *Int. J. Inf. Secur.* 2023, *23*, 1231–1249.
18. Ferreira, D.J.; Mateus-Coelho, N.; Mamede, H.S. Methodology for predictive cyber security risk assessment (PCSRA). *Procedia Comput. Sci.* 2023, *219*, 1555–1563.
19. Filigran. OpenCTI—Open platform for cyber threat intelligence. Available online: https://www.filigran.io/en/products/opencti/ (accessed on 4 February 2023).
20. Gartner. *Forecast: Information Security and Risk Management, Worldwide, 2021–2027, 2Q23 Update*. Available online: https://www.gartner.com/en/documents/4488199 (accessed on 31 May 2024).
21. IBM. *Cost of a Data Breach Report 2023*. Available online: https://www.ibm.com/security/digital-assets/cost-data-breach-report/ (accessed on 31 May 2024).
22. Information Security Forum. *Information Risk Assessment Methodology 2 (IRAM2)*. Available online: https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-2-iram2/ (accessed on 31 May 2024).
23. Kotsias, J.; Ahmad, A.; Scheepers, R. Adopting and integrating cyber-threat intelligence in a commercial organisation. *Eur. J. Inf. Syst.* 2023, *32*, 35–51.
24. Kure, H.; Islam, S. Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *J. Univers. Comput. Sci.* 2019, *25*, 1478–1502.
25. Lambrinoudakis, C.; Gritzalis, S.; Xenakis, C.; Katsikas, S.; Karyda, M.; Tsochou, A.; Papadatos, K.; Rantos, K.; Pavlosoglou, Y.; Gasparinatos, S.; et al. *Compendium of Risk Management Frameworks with Potential Interoperability*; ENISA: Athens, Greece, 2022.
26. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* 2020, *12*, 157.
27. Lezzi, M.; Corallo, A.; Lazoi, M.; Nimis, A. Measuring cyber resilience in industrial IoT: A systematic literature review. *Management Review Quarterly* 2025.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 1500-1516

28. Lyvas, C.; Maliatsos, K.; Menegatos, A.; Giannakopoulos, T.; Lambrinoudakis, C.; Kalloniatis, C.; Kanatas, A. A hybrid dynamic risk analysis methodology for cyber-physical systems. In *Proceedings of the European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 134–152.
29. Mathey, F.; Bonhomme, C.; Rocha, J.; Lombardi, J.; Joly, B. *Risk Assessment Optimisation with MONARC*. Available online: https://www.monarc.lu/assets/files/publications/2018-HACK.LU-CASES.pdf (accessed on 31 May 2024).
30. Mizrak, F. Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Res. J. Bus. Manag.* 2023, *10*, 98–108.
31. Schmitz, C.; Pape, S. LiSRA: Lightweight security risk assessment for decision support in information security. *Comput. Secur.* 2020, *90*, 101656.
32. Shevchenko, P.V.; Jang, J.; Malavasi, M.; Peters, G.W.; Sofronov, G.; Trück, S. The nature of losses from cyber-related events: Risk categories and business sectors. *J. Cybersecur.* 2023, *9*, tyac016.
33. Shin, B.; Lowry, P.B. A review and theoretical explanation of the cyberthreat-intelligence capability needed by information security practitioners. *Comput. Secur.* 2020, *92*, 101761.
34. Verizon. *2024 Data Breach Investigations Report*. Available online: https://enterprise.verizon.com/resources/reports/dbir/ (accessed on 31 May 2024).
35. Zahra, B.F.; Abdelhamid, B. Risk analysis in Internet of Things using EBIOS. In *Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 9–11 January 2017; pp. 1–7.