RJEST Research Journal of Education Science & Technology

Volume 4, Number 1 (2024)
ISSN: 2783-0225

www.rjest.org

Research Article

A Conceptual Framework for Building a Knowledge Base in Cybersecurity Incident Responses

Matthew Henry P. Bibangco[a]

[a]University of the Philippines Diliman, Roxas Ave., Diliman, Quezon City, Metro Manila, 1101, Philippines

ARTICLE INFO

Corresponding Author:
Matthew Henry P. Bibangco
Email:
mhbibangco@gmail.com

Article History
Received: Dec. 10, 2023
Revised: Aug. 25, 2024
Accepted: Dec. 20, 2024

Keywords
Cybersecurity
Framework Development
Incident Response
Knowledge Base
Knowledge Management

DOI
10.63179/rjest.v4i1.54

ABSTRACT

The long-term survival of organizations operating in a highly competitive environment, such as cybersecurity, requires an effective strategy for knowledge management. This paper brings a conceptual framework for building a knowledge base (KB) that will enhance the efficiency and efficacy of Cybersecurity Incident Response (CSIR) teams through integrated KM processes: the acquisition, codification, storage, retrieval, dissemination, and utilization of knowledge. The framework provides a structured system for tackling the challenges of managing tacit and explicit knowledge in CSIR environments. Developed through a comprehensive review of literature and theoretical models, it aligns well with established principles, like the SECI model, and industry standards, such as ITIL and ISO/IEC 27001. It focuses on the triad of people, processes, and technologies to facilitate access and application of organizational knowledge. This framework will shorten incident resolution time, support decision-making, and enhance organizational learning by providing a central knowledge repository.

1. INTRODUCTION

Knowledge capital plays a deciding role in maintaining the long-term success of organizations (Hosseini, 2014). In OECD countries, investments in knowledge capital were on par with, or exceeded, traditional investments in physical assets such as machinery and infrastructure (Andrews & de Serres, 2012). This trend puts knowledge management (KM) on the corporate radar, as strong KM practices have become strategically critical and operationally indispensable to organizations.

KM is a systematic approach that involves creating, capturing, storing, sharing, and using knowledge to improve decision-making and organizational performance (Cho & Korte, 2014). Its adoption helps organizations focus on leveraging tacit and explicit knowledge to create an insight-driven organization and make mission-critical decisions. Tacit knowledge includes personal, experience-based knowledge that is not easily articulated or documented. It better reflects the kind of knowledge gained through experience, observations, and interactions. In contrast, explicit knowledge is understood as more structured and codified information that can be stored, documented, and easily shared in a specific format, such as manuals, white papers, or databases (Haradhan, 2017).

In the knowledge-based economy era, with the industrial revolution giving way to a massive transition to the data-driven economy (Xue, 2017), it is considered a necessity for modern organizations to treat KM as an important technology to convert knowledge into the strategic insights optimal for continuous process improvement and innovation (Edvinsson, 1997). In post-pandemic times, this importance was further solidified as the digital market and society started to merge organically. In

Recommended Citation: Bibangco, M.P. (2024). A Conceptual Framework for Building a Knowledge Base in Cybersecurity Incident Response. *Research Journal of Education, Science and Technology*, *4*(1), pp. 13-24. https://doi.org/10.63179/rjest.v4i1.54

fact, many organizations that were resistant to adopting technologies had to migrate their processes to cyberspace during the pandemic, while the few organizations that were planning to digitalize processes had to rush their implementation plans. Furthermore, the pandemic expanded horizons in the digital economy and increased the use of digital platforms, pushing digital transformation initiatives forward by an average of 4 years (McKinsey & Company, 2020). Consequently, several entities moved their operations online, while others prioritized the digitalization of their workflows and services. This was when decision-makers and executives began to realize the criticality of KM, especially to remain competitive in the digital landscape. Regardless, there remains an evident gap as most organizations are yet to evolve their KM processes, particularly within Cybersecurity Incident Response (CSIR) teams.

CSIR teams mostly use traditional methodologies to detect and mitigate security threats. But even these teams suffer from ineffective incident resolution due to fragmented knowledge storage, knowledge silos that inhibit collaboration, and uncoordinated information sharing among team members. As a result, many organizations experience slow response time, redundancy, and a lack of use of historical incident data to enhance cybersecurity efforts. The worst part is that some organizations lack processes for knowledge creation and management.

To alleviate the above-mentioned concerns, the researcher proposed a centralized repository, the Knowledge Base (KB), to store high-quality CSIR knowledge. Analogous to organization-wide knowledge transfer at the mission level, this repository is bolstered by a strong network infrastructure that facilitates access to and sharing of relevant knowledge across the organization (Brown, 2019). Hence, implementing KB in CSIR will strengthen the CSIR team's response, ultimately helping the organization to achieve success and resilience in the digital age (Gonashvili, 2019).

This research presents a new conceptual framework for incorporating KB in CSIR processes. Unlike traditional KM frameworks, the proposed framework is specifically designed to address the constantly changing landscape of cyber threats. The framework incorporates an AI-facilitated knowledge retrieval feature, a context-based decision-support component, and a self-learning mechanism that helps CSIR teams efficiently adapt to evolving cyberattack landscapes.

2. KNOWLEDGE MANAGEMENT

According to the Information Technology Infrastructure Library (ITIL), KM is one of the most essential elements in modern organizations. It is designed to collect, analyze, store, and share knowledge to prevent the unnecessary rediscovery of information and lessons learned. By documenting knowledge and making it accessible across the organization, KM enhances efficiency and collaboration (ITIL Foundation, 2019). KM is structured around four main processes: Knowledge Creation, Knowledge Storage, Knowledge Dissemination, and Knowledge Application.

- Knowledge Creation, or Knowledge Acquisition, involves generating new knowledge or updating existing organizational content. This process encompasses both explicit knowledge and tacit knowledge.
- Knowledge Storage focuses on the collection and maintenance of both explicit and tacit knowledge within the organization. Effective knowledge storage ensures that critical information is preserved and remains accessible for future reference and decision-making.
- Knowledge Dissemination, or Knowledge Transfer, refers to the process of sharing and exchanging knowledge. It occurs between individuals, teams, or departments within an organization, as well as between individuals and explicit knowledge sources. This process facilitates the widespread distribution of valuable information, ensuring that knowledge is accessible to those who need it (Alavi et al., 2005).
- Knowledge Application involves utilizing acquired knowledge to solve problems, make informed decisions, improve efficiency, and reduce cost. It is pivotal in shaping an organization’s strategic direction, enabling continuous improvement and innovation (Markus et al., 2002).

3. KNOWLEDGE MANAGEMENT IN CSIR

The cybersecurity market has experienced exponential growth, increasing from $3.5 billion in 2004 to $138 billion in 2017—a 39-fold growth in just 13 years (Prime Index, 2019). Tulane University (2020) attributes this rapid expansion to several factors: First, hackers are becoming more sophisticated. Second, cybercrime imposes high financial costs on organizations. Third, automation has expanded attack surfaces, creating new vulnerabilities. Lastly, security weaknesses are widespread across systems and networks, making them attractive targets for cybercriminals.

The increasing frequency, sophistication, and severity of cyberattacks have been well documented. According to the National Institute of Standards and Technology (NIST, 2006), not all security incidents can be prevented, necessitating a shift in the cybersecurity industry from a detect-and-prevent model to one that includes CSIR. A well-defined CSIR capability enables organizations to rapidly detect security incidents, minimize damage, identify vulnerabilities, and swiftly restore IT operations (Bowen et al., 2006). Adobe Inc. (2016) emphasized that a cohesive, organization-wide incident response program is as critical to its success as its core product strategy.

Implementing CSIR capabilities into an organization aims to achieve three objectives (Albluwi, 2017). It seeks to ensure the rapid identification and classification of security incidents, facilitate effective containment and impact minimization through structured procedures, and implement efficient processes that eliminate threats and restore operations.

KM plays a critical role in achieving CSIR teams' objectives. However, many teams face significant challenges, including the lack of centralized knowledge repositories, difficulties retrieving relevant incident data, and inadequate mechanisms for knowledge sharing among team members and departments. These inefficiencies often lead to duplicated efforts, delayed decision-making, and an inability to respond effectively to emerging threats. Implementing efficient KM practices helps streamline processes, improve response times, and enhance the overall effectiveness of CSIR teams (Veryat, 2016).

Successful CSIR operations rely on balancing the three pillars of KM: people, process, and technology (Bose, 2002). Each pillar plays a distinct role in cybersecurity: protection systems are primarily technology-driven, with support from processes and personnel; detection systems require equal contributions from people, processes, and technology to identify threats accurately; and response systems are primarily driven by human expertise, supported by structured processes and technological tools, for a couple of seconds. Striking the right balance among these elements is essential to achieving robust protection, detection, and response capabilities.

Large organizations that successfully integrate people, processes, and technology often develop strong KM systems. This is achieved through a continuous learning cycle, system refinement, and a culture of knowledge sharing and improvement (Veryat, 2016). Research indicates a significant positive correlation between effective KM practices and the seamless integration of these three pillars, ultimately leading to enhanced cybersecurity performance (Hosseini, 2014).

4. KB AND ITS ROLE IN KM

KB is a centralized repository for storing, organizing, and sharing information, making it a core component of effective KM (Brown, 2019). The explicit formal description of concepts within a domain, their properties, relationships, and axioms, forms the foundation of a KB (Martinez & Taboada, 2003). According to Atlassian ITSM (2020), a KB may include resources such as frequently asked questions (FAQs), manuals, troubleshooting guides, and runbooks. These resources are essential for facilitating KM practices and supporting the four key KM processes.

Shrestha et al. (2016) emphasized that storing knowledge for future use is one of KM's fundamental goals, particularly for organizations establishing Centers of Excellence (CoEs) for CSIR. CoEs serve as focal points for KM, enhancing CSIR's organizational expertise and capabilities (Belyh, 2016). For CSIR teams, a robust KB is critical. The CERT Coordination Center (2004) highlighted the importance of efficient tracking systems that allow organizations to receive, store, and retrieve information. Several factors enhance KB usage, including standardized replies and technical tips, data sharing (Minina, 2013), and incident resolution documentation (Jia et al., 2018). Stored incident data and past resolution procedures are particularly valuable during cybersecurity emergencies, as they enable incident responders to promptly and effectively explain and justify their actions (Ahmad & Rughaver, 2012; Colome et al., 2019).

Knowledge Articles (KAs) within a knowledge base provide several advantages (ServiceNow, 2020). For example, employees can access a single, easily searchable source of up-to-date information, and relevant KAs are automatically suggested when security requests or incident response tasks are manually created, thereby improving efficiency. However, as identified by Minina (2013), organizations face challenges in implementing knowledge management systems, including users not recognizing the value of knowledge creation, a lack of the skills necessary for effective KM system use, overlapping knowledge locations, limited functionality of KM tools, and irregular updates to knowledge.

Diniz et al. (2005) emphasized that while training is essential, it alone cannot guarantee that critical information reaches decision-makers during emergencies. They argued that effective KM systems must capture, store, and selectively disseminate data to ensure accessibility when needed. Furthermore, they noted that recommendations are only impactful when supported by a well-structured KM system, as contextual KM is essential for guiding decisions and complementing emergency plans. Martinez and Taboada (2003) further asserted that to fully realize the potential benefits of a KB, organizations must ensure continuous access to the necessary knowledge sources and resources. A well-maintained KB preserves critical cybersecurity knowledge and enhances decision-making and response effectiveness within CSIR teams.

5. METHODOLOGY

This study is based on a systematic literature review to develop a conceptual framework for knowledge acquisition and transfer mechanisms, using the SECI Model and the Knowledge Acquisition Matrix (KAM) as guiding frameworks. This study synthesized existing knowledge to provide insights into effective KM practices. To ensure the applicability of these frameworks, this study explicitly highlights their relevance within the context of CSIR.

5.1 Research Design

This study adopts a qualitative research design focused on literature review and conceptual analysis. The objective is to explore existing theories and frameworks related to knowledge transfer, critically examining scholarly articles, books, and industry reports. The selection of sources was guided by relevance, credibility, and impact on the field of knowledge management.

5.2 Application of the SECI Model

The SECI Model (Nonaka & Takeuchi, 1995) describes the dynamic knowledge conversion process, structured into four phases: Socialization, Externalization, Combination, and Internalization. Figure 1 illustrates the SECI Model.

Socialization involves exchanging tacit knowledge through interactions, observations, and discussions. In CSIR, organizations facilitate socialization by conducting training programs, cross-team collaborations, and post-incident debriefs. For example, analysts and responders participate in simulated cyberattacks, fostering experiential knowledge transfer that improves real-time decision-making during security incidents.

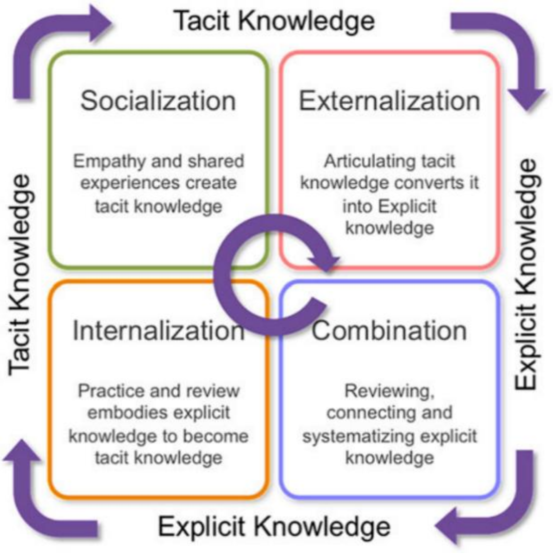
Tacit Knowledge
Socialization
Empathy and shared experiences create tacit knowledge
Externalization
Articulating tacit knowledge converts it into Explicit knowledge
Internalization
Practice and review embodies explicit knowledge to become tacit knowledge
Combination
Reviewing, connecting and systematizing explicit knowledge
Tacit Knowledge
Explicit Knowledge
Explicit Knowledge

Figure 1. Knowledgebase Framework for CSIR.

Externalization refers to the process of articulating tacit knowledge into explicit forms, such as documentation, reports, or formal procedures. In CSIR, companies convert cybersecurity incident experiences into structured knowledge assets, including threat intelligence reports, attack pattern databases, and incident response playbooks. A multinational organization, for instance, may document lessons learned from previous cybersecurity breaches to refine its intrusion detection and response protocols.

Combination involves integrating and systemizing explicit knowledge from multiple sources. CSIR-oriented organizations aggregate diverse knowledge into comprehensive threat intelligence frameworks, including security logs, forensic reports, and government advisories. A case study highlights how a financial institution synthesized security alerts from global threat feeds, regulatory compliance requirements, and past breach analyses to enhance its cyber defense strategies.

Internalization occurs when individuals absorb explicit knowledge through learning and practice, turning it into tacit knowledge. CSIR applications of internalization include hands-on cybersecurity exercises, red-team/blue-team drills, and continuous learning through security certifications. For example, security professionals who undergo advanced malware analysis training develop an intuitive ability to detect and mitigate sophisticated cyber threats. Research suggests that organizations integrating continuous cybersecurity education into their workflows experience faster incident response times and improved breach mitigation strategies.

5.3 Knowledge Acquisition Matrix

The Knowledge Acquisition Matrix (KAM) provides a structured approach to understanding how knowledge is captured, stored, and transferred within an organization. This study synthesizes existing research on KAM to highlight its relevance in KM, particularly in the CSIR domain.

The matrix considers multiple dimensions, including the source of knowledge, the type of knowledge, the acquisition mechanism, and the retention method. In the context of CSIR, organizations acquire knowledge from internal sources (e.g., security operations teams and penetration testers) and external sources (e.g., government cybersecurity agencies, industry consortia, and threat intelligence providers).

Tacit knowledge in CSIR is often gained through hands-on investigations, real-world incident handling, and collaborative threat-sharing platforms. In contrast, explicit knowledge is systematically documented in cybersecurity frameworks, attack pattern repositories, and digital forensics manuals.

Existing studies demonstrate how organizations map knowledge flows and assess retention strategies to ensure long-term accessibility to critical cybersecurity knowledge. For instance, multinational enterprises engaged in threat-hunting programs apply KAM principles to collect best practices from previous attack scenarios, benchmark them against evolving cyber threats, and disseminate them across their security operations teams. This structured KM approach ensures continuous learning and improvement in CSIR programs.

5.4 Data Collection and Analysis

Since this study is based on a literature review, data collection involved identifying and analyzing relevant academic and industry sources. A structured approach was used to search for peer-reviewed journal articles, conference proceedings, white papers, and best practice reports. Databases such as Scopus, Web of Science, and Google Scholar were utilized to ensure the inclusion of high-quality sources. Particular attention was given to sources discussing CSIR applications of KM frameworks.

The data analysis process involved thematic synthesis and conceptual mapping. Thematic analysis identified recurring themes related to knowledge acquisition and transfer in CSIR. Key insights from multiple sources were compared and integrated into a cohesive conceptual framework. The comparative analysis evaluated best practices across industries to ensure a broad perspective on KM methodologies applicable to CSIR.

6. THE PROPOSED FRAMEWORK

The proposed framework builds on existing KM models while introducing three key innovations that make it uniquely suited for CSIR: AI-assisted knowledge retrieval, enabling real-time access to threat intelligence and past incident records; context-aware knowledge evaluation, ensuring that stored information remains relevant and actionable through dynamic validation mechanisms; and adaptive threat intelligence integration, allowing the KB to refine its stored knowledge based on emerging attack patterns continuously.

Unlike conventional KM models that primarily focus on static documentation, this framework actively evolves in response to new cybersecurity challenges, making it a powerful tool for CSIR teams (Mostert & Synman, 2003). This framework is grounded in the organizational knowledge model (Mostert & Synman, 2007). It incorporates the four key KM processes as outlined by Kayworth and Leidner (2003), Zaim (2006), Fong and Choi (2009), and Turner et al. (2012). As illustrated in Figure 2, this framework contextualizes the processes of knowledge acquisition, codification, evaluation, and utilization within the CSIR domain.

The model delineates the composition and processes of the KB. Knowledge inputs are derived from internal and external environments. External knowledge is further categorized into tacit and explicit knowledge (Haradhan, 2017). These inputs undergo three critical processes: acquisition, codification, and evaluation. Once processed, the knowledge is organized and stored in the KB, making it available for utilization and implementation.

6.1 Knowledge Acquisition

Knowledge acquisition is the process of learning through experience and experimentation, drawing on internal and external sources (Ramaiah, 2019). It focuses on building a competitive advantage by capturing, integrating, and adapting information to solve problems or foster innovation (Matthew, 1985). Common mechanisms for acquiring external knowledge include formal methods (e.g., education, training, recruitment, and partnerships) and tacit knowledge elicitation techniques (Hoffman et al., 1995; Jafari et al., 2011).

Gonzales and Martins (2017) outlined key organizational actions for knowledge acquisition, including training individuals, encouraging a trial-and-error approach, fostering a learning culture, hiring employees to introduce new knowledge, forming partnerships with other firms, and acquiring

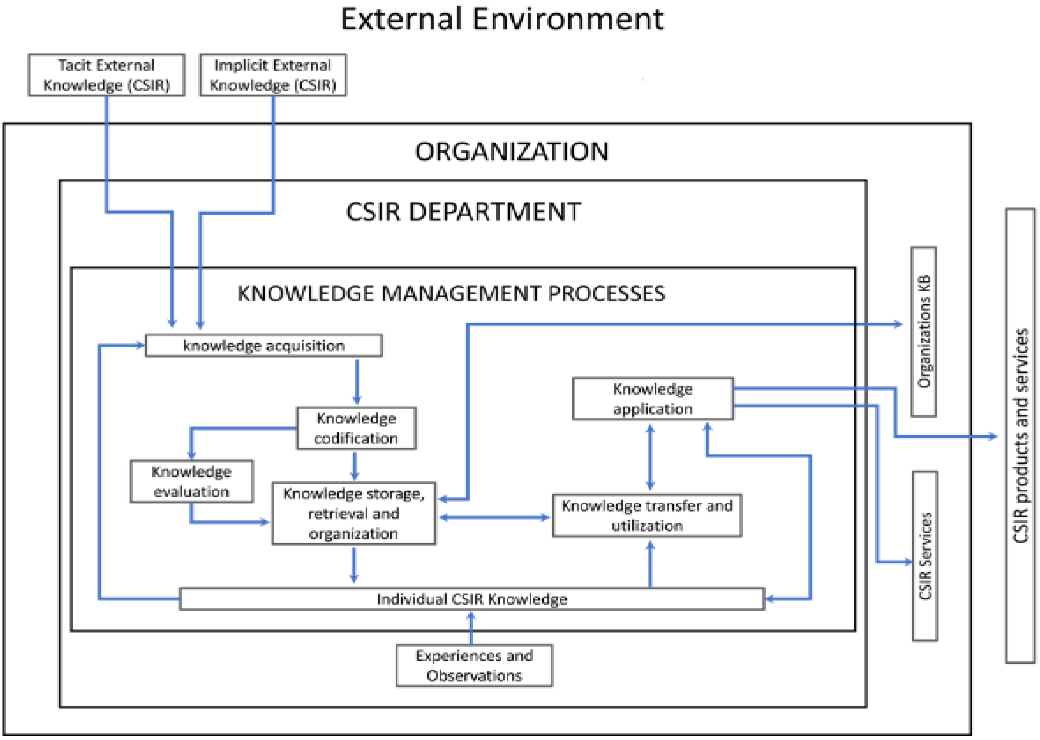
External Environment
Tacit External Knowledge (CSIR)
Implicit External Knowledge (CSIR)
ORGANIZATION
CSIR DEPARTMENT
KNOWLEDGE MANAGEMENT PROCESSES
knowledge acquisition
Knowledge codification
Knowledge evaluation
Knowledge storage, retrieval and organization
Knowledge application
Knowledge transfer and utilization
Individual CSIR Knowledge
Experiences and Observations
Organizations KB
CSIR Services
CSIR products and services

Figure 2. Knowledgebase Framework for CSIR

patents. Emberey et al. (2007) also proposed a knowledge acquisition matrix featuring eleven techniques to elicit specific types of knowledge. Meanwhile, existing models, such as SECI, can be used to understand how knowledge is created and shared within organizations (Nonaka & Takeuchi, 1995).

6.2 Knowledge Codification

Knowledge codification in CSIR involves structuring incident response procedures, attack pattern repositories, and forensic analysis reports into a systematic and accessible KB (Jassimuddin, 2005). Organizations implement automated documentation systems, such as Security Orchestration, Automation, and Response (SOAR) platforms, to facilitate real-time knowledge capture and retrieval.

Organizations employ standardized templates and structured ontologies to ensure consistency and interoperability across cybersecurity teams. Additionally, AI-driven documentation assistants help convert tacit knowledge into structured reports, thereby reducing response time and enhancing decision-making capabilities.

From an IT perspective, knowledge codification must meet technological requirements, including data capture, storage, and processing. On the other hand, from a KM perspective, codification must align with human cognition and decision-making processes using IT systems.

Common codification methods include text-oriented approaches, formula-oriented methods, data-oriented structuring, rule-based models, multimedia-oriented integration, and process-oriented frameworks (Natek & Zwilling, 2017). Templates can further simplify and expedite codification (Gonashvili, 2019). These techniques can be leveraged to develop a CSIR KB that incorporates both tacit and explicit knowledge.

Diniz et al. (2005) argued that knowledge systems should provide contextualized information rather than a uniform view for all users. Similarly, Kabir (2013) emphasized that codifying knowledge for future use requires minimal technology input. Organizations should adopt advanced technologies to enhance KM activities and overall organizational performance, thereby maximizing the utility of tacit knowledge.

6.3 Knowledge Evaluation

Knowledge evaluation ensures that KB contains accurate, relevant, and actionable information. This process involves verifying cybersecurity procedures, validating incident response strategies, and ensuring that documented protocols remain effective against evolving cyber threats (Mach & Owoc, 2001). Acquired knowledge from experts must undergo quality assessment. Organizations must ensure that their KBs are valid, reliable, and appropriately structured (Turban et al., 2001).

In CSIR, knowledge evaluation involves continuously validating threat intelligence reports, security advisories, and incident playbooks. To assess the reliability of stored knowledge, it is necessary for organizations to impellent peer review mechanisms and machine learning-driven anomaly detection. One widely used approach is Red Team-Blue Team exercises, where simulated cyberattacks test and refine incident response procedures. Additionally, metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) are employed to measure the practical utility of stored knowledge.

Despite its benefits, knowledge evaluation faces several challenges, including outdated threat intelligence, inconsistent documentation, and poorly designed information silos. Organizations implement periodic knowledge audits, automated knowledge verification systems, and collaborative knowledge-sharing platforms to address these issues. As knowledge flows from internal and external sources, its applicability must be critically assessed (Mostert & Snyman, 2007). Retaining irrelevant or outdated knowledge can clutter storage, rendering the KB inefficient (Jassimuddin, 2005).

Mostert and Snyman (2007) suggested that tacit knowledge from external sources can be evaluated through psychometric testing and interviews. Meanwhile, explicit knowledge can be assessed through the selection of technical articles for corporate databases. Explicit knowledge must be well-structured to aid incident responders. This process involves identifying and analyzing essential documentation and knowledge resources (Gonashvili, 2019); evaluating internally created tacit knowledge through practical tests; and validating explicit knowledge through expert panels or peer reviews within the CSIR department.

6.4 Knowledge Storage, Retrieval, and Organization

Organizations must establish effective knowledge storage and retrieval processes to ensure that previously acquired knowledge remains accessible for current and future use (Mostert & Snyman, 2007). This section presents the key aspects of knowledge storage, organization, and protection, along with strategies for retrieval and retention to optimize KM.

Knowledge storage is the systematic process of recording and organizing explicit knowledge in structured repositories, such as databases and document management systems (Mostert & Synman, 2007). This process involves both soft and hard methods of recording knowledge in a retrievable manner. Transferred knowledge must be stored in a centralized repository to allow organizational access without requiring direct interaction with the original knowledge holder (Jassimuddin, 2005). A KB serves as this central repository, reducing the need for redundant knowledge transfer and saving time and resources while improving organizational performance (Caroline et al., 2015). The KB relies on modern information infrastructure, including hardware and software solutions, to systematically identify, code, and index knowledge for future retrieval (Nonaka & Takeuchi, 1995).

To enhance knowledge storage, Gonzalez and Martins (2017) identified several key organizational actions, including identifying and documenting best practices, retaining tacit knowledge within individuals, and incorporating acquired knowledge into organizational procedures and rules. Additionally, organizations should foster a knowledge-sharing culture and utilize IT for organizational memory training. Three guiding principles for knowledge storage include: (1) recognizing the importance of individuals in tacit knowledge retention, (2) leveraging publications and structured documentation for knowledge organization, and (3) utilizing IT systems such as databases for effective KM (Gonzales & Martins, 2017).

Within a KB, knowledge is stored in Knowledge Articles (KAs)—structured information units that capture issues, describe solutions, answer questions, provide reference information, and outline processes (Minina, 2013). KAs serve as structured sources of information, offering answers to common questions, step-by-step procedures, tutorials, diagnostic guides, and general topic explanations (Clayton, 2015). Key KA attributes include problem descriptions, environmental context, solution outlines, categorization, visibility groups, and feedback mechanisms (Minina, 2013). ServiceNow (2020) outlines additional KB elements, such as article numbers, categories, publication status, validity periods, attachments, workflow processes, and textual content.

Knowledge retention focuses on preventing the loss of critical knowledge, particularly tacit knowledge, by implementing strategies such as mentorship programs, training, and knowledge-sharing initiatives (Mostert & Synman, 2007). Retention strategies include education and training programs, communities of practice, professional networks, and documentation of organizational processes (Wamundila & Ngulube, 2011). Organizations risk losing tacit knowledge when employees retire or leave (Chigada, 2014). Barriers to knowledge retention include downsizing, restrictive knowledge exchange policies, and ineffective knowledge-sharing practices (Kumar, 2017). Meanwhile, explicit knowledge is vulnerable to media decay, theft, vandalism, and sabotage. Strategies to protect explicit knowledge include high-quality storage media and secure storage environments (Mostert & Snyman, 2007).

Knowledge retrieval involves locating and accessing relevant tacit and explicit knowledge for organizational use. An effective retrieval system should provide advanced searching, indexing, and knowledge organization capabilities (Mostert & Snyman, 2007). Jabar et al. (2010) defined the retrieval stage in knowledge management as involving profiling and personalizing knowledge, leveraging past experiences to enhance decision-making, and retaining lessons from previous projects to minimize redundancy. Martinez and Taboada (2003) further emphasized the importance of tools that facilitate knowledge reuse, allowing organizations to import, combine, and reorganize content for improved efficiency.

Knowledge protection requires a multi-layered approach integrating technical and organizational measures to safeguard sensitive information. Technical measures include encryption, access controls, and secure storage systems. In contrast, organizational measures include non-disclosure agreements (NDAs), intellectual property policies, and awareness training to mitigate the risk of knowledge leaks (Thalmann & Sarigianni, 2016). The key focus areas for knowledge protection include preventing knowledge spillovers, reducing knowledge visibility, and ensuring knowledge security (Ahmad et al., 2014; Lee et al., 2007; Jennex et al., 2013). However, relying solely on technical information security measures (e.g., firewalls and antivirus software) is insufficient. Instead, organizations should adopt a comprehensive protection strategy, combining: (1) Technical measures, such as encrypted communication channels, secure data storage devices, and access control mechanisms, and (2) Organizational measures, including NDAs, contractual agreements, and security awareness programs (Thalmann & Sarigianni, 2016).

Knowledge organization involves the classification, indexing, and structuring of information to facilitate efficient access and retrieval, a process typically undertaken by librarians, archivists, information specialists, and computer algorithms (Hjorland, 2008). Knowledge organization systems aim to meet users' information needs by categorizing information systematically. For instance, Jabar et al. (2010) suggested grouping information into structured categories, while Takahashi and Kadobayashi (2014) proposed a reference ontology for cybersecurity information management to enhance efficient cybersecurity operations. This paper adopts their ontology-based structure, organizing knowledge into categories encompassing user, provider, incident information, products and services, cyber risk, countermeasures, and client resources.

6.5 Knowledge Transfer and Utilization

Knowledge transfer enhances an organization’s ability to leverage institutional knowledge by ensuring that valuable expertise and insights are shared among employees rather than being confined to a single individual. This process includes both formal methods, such as structured training, documentation, and mentorship, as well as informal knowledge-sharing activities that foster collaboration (Levine & Prietula, 2012). It can be accomplished through various approaches, including self-learning by accessing firm reports and documentation, engaging in social interactions where knowledge is exchanged through interpersonal contact, participating in structured group-based exchanges, and collaborating with external entities through inter-organizational exchanges (Levine & Prietula, 2012).

Knowledge transfer effectiveness is influenced by organizational and technological factors (Nguyen & Burgess, 2014). While Knowledge Bases (KBs) rely heavily on technology, their success is ultimately shaped by social and cultural values, trust, language, and interpersonal relationships (Hassan et al., 2017). From an incident learning perspective, effective knowledge-sharing enhances response times, procedural improvements, and cybersecurity training programs (Ahmad & Rughaver, 2012).

Utilizing KB knowledge allows organizations to make sense of problems, threats, and opportunities, ultimately enabling strategic decision-making and effective problem-solving (Mostert & Snyman, 2007). By fostering systematic knowledge transfer, organizations can reduce redundancies, improve incident response efficiency, and strengthen cybersecurity defense mechanisms.

6.6 Knowledge Application

Knowledge application ensures that stored knowledge is actively used for innovation and problem-solving. This process begins with leveraging existing and newly acquired knowledge to stimulate creativity and drive innovation (Datta, 2010). Organizations that effectively apply knowledge and experience benefit from reduced response times, enhanced decision-making, and an improved security posture. For example, a case study by Ahmad and Ruighaver (2012) highlights how a multinational corporation improved its incident response efficiency by systematically applying knowledge from past cybersecurity incidents, resulting in a 40% reduction in incident resolution time, minimized impact of data breaches, and enhanced team coordination and collaboration.

Similarly, a government agency implementing a structured knowledge management approach within its cybersecurity unit experienced significant improvements by integrating threat intelligence reports and historical attack data into its knowledge repository, enhancing its ability to predict and mitigate cyber threats (Jia et al., 2018). Applying knowledge strategically provides organizations with a competitive advantage by enhancing economic returns, maintaining knowledge as a key organizational asset, and facilitating continuous knowledge creation. Organizations incur acquisition and storage costs without proactively applying knowledge, thereby yielding tangible benefits. The application of knowledge is embedded within organizational processes, spanning formal procedures that represent explicit knowledge to informal work habits that embody tacit knowledge (Mostert & Snyman, 2007).

Organizations must actively integrate knowledge into workflows and operational strategies to fully realize the benefits of stored knowledge. The case studies illustrate how systematic application of knowledge improves cybersecurity readiness, speeds response times, and enhances overall operational efficiency.

7. CONCLUSION

This study highlights the critical role of an adaptive KM framework in enhancing the efficiency of CSIR team collaboration. The proposed framework advances traditional KM methodologies by integrating AI-driven knowledge retrieval, contextual knowledge validation, and real-time threat intelligence processing. These characteristics set the framework apart from existing KM models, which are often dependent on static, manually updated documents, particularly in the context of CSIR. This study fills this gap and presents a novel approach that weaves these components together to enhance knowledge flow in security operations, thereby minimizing incident response time and improving decision-making accuracy. As mentioned, the growing importance of knowledge capital for organizational success requires strengthening KM practices. CSIR teams encounter critical challenges, such as managing a wide array of knowledge assets and ensuring that knowledge is quickly available during decision-making and incident response; the proposed framework is designed to directly address those challenges.

To ensure alignment with best practices, the framework integrates insights from established KM theories, such as the SECI Model, and adheres to industry standards, including ITIL and ISO/IEC 27001. This adaptability allows organizations to tailor KM strategies to their specific operational needs while ensuring compliance with recognized guidelines. Furthermore, this study emphasizes the interdependent roles of people, processes, and technology in establishing a balanced and effective KM system, noting that organizations can improve communication, accelerate incident resolution, and enhance organizational learning by centralizing knowledge into a knowledge base. However, a key limitation of this study is the lack of empirical validation; while the proposed framework is grounded in extensive literature and theoretical models, further research is required to assess its feasibility and effectiveness in real-world settings. To address this limitation, future studies will focus on expert validation of the framework's practical applicability, benchmarking against international standards to evaluate its competitiveness, and pilot implementations within organizations to assess their real-world impact.

Even with this limitation, the study is an important step in the right direction, providing a fundamental model for entities to better govern their knowledge resources. KM practices will enable CSIR teams to respond promptly to incidents when they occur, know what to utilize, and improve the overall efficiency of their operation.

ACKNOWLEDGMENT

The author extends heartfelt gratitude to Prof. El Jireh Bibangco for his valuable insights and guidance throughout the development of this study. Deep appreciation is also expressed to the author's wife, Lanie M. Bibangco, for her unwavering support, encouragement, and assistance, especially during challenging times.

DECLARATIONS

Conflict of Interest

The authors declare they have no conflict of interest.

Informed Consent

Not applicable. This study did not involve human participants; thus, informed consent was not required.

Funding Agency

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

Adobe Inc. (2016). *Incident Response Overview White Paper.* https://tinyurl.com/tjd8kf7d

Ahmad, A., Bosua, R. & Scheepers, R. (2014). Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective. *Computers & Security, 42*, 27—39. doi: 10.1016/j.cose.2014.01.001

Ahmad, A., & Ruighaver, A. B. (2012). Organisational learning and incident response: Promoting effective learning through the incident response process. *Proceedings of the 10th Australian Information Security Management Conference*. https://tinyurl.com/2mmum9xk

Alavi, M., Kayworth, T. & Leidner, D. (2005). An Empirical Examination of the Influence of Organizational Culture on Knowledge Management Practices. *Journal of Management Information Systems, 22*(3), 191—224. doi: 10.2753/MIS0742-1222220307

Albluwi, Q. A. H. (2017). *Framework for performance evaluation of computer security incident response capabilities* (Doctoral dissertation, University of Rhode Island). doi: 10.23860/diss-al-harfi-albluwi-qutaiba-2017

Andrews, D., & A. de Serres (2012). "Intangible Assets, Resource Allocation and Growth: A Framework for Analysis," *OECD Economics Department Working Papers*, No. 989, OECD Publishing, Paris. doi: 10.1787/5k92s63w14wb-en.

Atlassian ITSM. (2020). *What is a knowledge base?* Atlassian. https://www.atlassian.com/itsm/knowledge-management/what-is-a-knowledge-base

Belyh, A. (2016). *How to Set Up a Center of Excellence*. Cleverism. https://www.cleverism.com/how-set-up-center-excellence/

Bose, R. (2002). Customer relationship management: Key components for IT success. *Industrial Management & Data Systems*, *102*(2), 89—97. doi: 10.1108/02635570210419636

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers* (NIST Special Publication 800-100). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf

Brown, J. (2019). *Why a knowledge base is critical for your business*. HelpJuice. https://helpjuice.com/blog/knowledge-base

Caroline, K. S., Mugun, B. T., & Loice, M. (2015). Knowledge Storage, Retrieval and Employee Performance: The Moderating Role of Employee Engagement. *International Journal of Small Business and Entrepreneurship Research*, *3*(6), 1—13. https://tinyurl.com/4ch8adp8

CERT Coordination Center (2004). Creating and Managing Computer Security Incident Response Teams (CSIRTs). Retrieved from https://www.first.org/conference/2004/papers/t1_01.pdf

Chigada, J. (2014). *The role of knowledge management in enhancing organisational performance in selected banks of South Africa* (Master's thesis, University of South Africa). University of South Africa, Pretoria. https://uir.unisa.ac.za/handle/10500/14332

Cho, T., & Korte, R. (2014). Managing knowledge performance: Testing the components of a knowledge management system on organizational performance. *Asia Pacific Education.* doi: 10.1007/s12564-014-9333-x

Clayton, I. (2015). The Guide to the Universal Service Management Body of Knowledge. https://www.itgovernanceusa.com/files/USMBOK-Guide-Contents-Sample.pdf

Colome, M., Nunes, R. C., & de Lima Silva, L. A. (2019). Case-Based Cybersecurity Incident Resolution. *Federal University of Santa Maria, 204*. doi: 10.18293/SEKE2019-204

Datta, P. (2010). From knowledge codification to application: An agent perspective. Kent State University. https://www.tlainc.com/articl241.htm

Diniz, V. B., Borges, M. R. S., Gomes, J. O., & Canos, J. (2005). Knowledge management support for collaborative emergency response. *Proceedings of the Ninth International Conference on Computer Supported Cooperative Work in Design, 2*, 1188—1193. doi: 10.1109/CSCWD.2005.194358

Edvinsson, L. (1997). Developing intellectual capital at Skandia. *Long Range Planning*, *30*(3), 366—373. doi: 10.1016/S0024-6301(97)90248-X

Emberey, C. L., Milton, N. R., Berends, J. P. T. J., van Tooren, M. J. L., van der Elst, S. W. G., & Vermeulen, B. (2007). Application of knowledge engineering methodologies to support engineering design application development in aerospace. *Seventh AIAA Aviation Technology, Integration, and Operations Conference (ATIO).* doi: 10.2514/6.2007-7708

Fong, P. S. W., & Choi, S. K. Y. (2009). The process of knowledge management in professional service firms in the construction industry: A critical assessment of both theory and practice. *Journal of Knowledge Management*, *13*(2), 110—126. doi: 10.1108/13673270910942736

Gonashvili, M. (2019). Knowledge Management for Incident Response Teams. *Master's Thesis, Masaryk University.* https://is.muni.cz/th/pupg1/Knowledge_Management_For_Incident_Response_Teams.pdf

Gonzalez, R. V. D., & Martins, M. F. (2017). Knowledge management process: A theoretical-conceptual research. *Gestão & Produção*, *24*(2), 248—265. doi: 10.1590/0104-530X0893-15

Haradhan, M. (2017). Tacit knowledge for the development of organizations. *ABC Journal of Advanced Research*, *6*(1), 17—24. https://mpra.ub.uni-muenchen.de/id/eprint/83040

Hassan, N. A. H., Hussin, N., & Noor, M. N. M. (2017). Knowledge transfer practice in organization. *International Journal of Academic Research in Business and Social Sciences*, *7*(8), 750—760. doi: 10.6007/IJARBSS/v7-i8/3291

Hjørland, B. (2008). What is knowledge organization (KO)? *Knowledge Organization*, *35*(2/3), 86–101. doi: 10.5771/0943-7444-2008-2-3-86

Hoffman, R. R., Shadbolt, N. R. Burton, A. M., & Klein, G. (1995). Eliciting knowledge from experts. A methodological analysis. *Organizational Behavior and Human Decision Processes*, *62*(2), 129—158.

Hosseini, M.R. (2014). The Impact of People, Process, and Technology on Knowledge Management. *European Journal of Business and Management*, *6*(28), 230—241. https://www.iiste.org/Journals/index.php/EJBM/article/view/16022

ITIL Foundation. (2019). *ITIL 4 Foundation edition*. Axelos. https://www.axelos.com

Jabar, M., Sidi, F., & Selamat, M. H. (2010). Tacit Knowledge Codification. *Journal of Computer Science*, *6*(10), 1170—1176. doi: 10.3844/jcssp.2010.1170.1176

Jafari, M., Akhavan, P., Nik, M. G., & Akhtari, M. (2011). Knowledge acquisition techniques: a comprehensive review. *Elixir International Journal, 34*(84), 11—21.

Jassimuddin, S. (2005). An Integration of Knowledge Transfer and Knowledge Storage: An Holistic Approach. *Semantic Scholar.* https://api.semanticscholar.org/CorpusID:3201106

Jennex, M. & Durcikova, A. (2013). Assessing Knowledge Loss Risk. *46TH Hawaii International Conference On System Sciences,* 3478—3487. doi: 10.1109/HICSS.2013.103

Jia, Y., Qi, Y., Shang, H., Jiang, R., & Li, A. (2018). A practical approach to constructing a knowledge graph for cybersecurity. *Engineering, 4*(1), 53–60. doi: 10.1016/j.eng.2018.01.004

Lee, S. C., Chang, S. N., Liu, C. Y., & Yang, J. (2007). The effect of knowledge protection, knowledge ambiguity, and relational capital on alliance performance. *Knowledge and Process Management*, *14*(1). doi: 10.1002/kpm.270

Levine, S.S. & Prietula, M. (2012). How knowledge transfer impacts performance: a multilevel model of benefits and liabilities. *Organization Science*, *23*(6), 1748—1766. doi: 10.1287/orsc.1110.0697

Kabir, N. (2013). Tacit knowledge, its Codification, and Technological Advancement. *International Journal of Knowledge Management*, *11*(3), 235—243. https://academic-publishing.org/index.php/ejkm/article/view/993

Kayworth, T., & Leidner, D. (2003). Organizational culture as a knowledge resource. *Handbook on knowledge management 1*(1), 235–252. doi: 10.1007/978-3-540-24746-3_12

Kumar, A. A. (2017). Knowledge Retention: A Key Attribute in Organizational Growth. *Pelagia Research Library*, *8*(1), 1—9. https://www.primescholars.com/articles/knowledge-retention-a-key-attribute-in-organizational-growth.pdf

Mach, M. & Owoc, M. (2001). Validation as the Integral Part of a Knowledge Management Process. *Informing Science*. doi: 10.28945/2399

Markus, L., Majchrzak, A. & Gasser, L (2002). A Design Theory for Systems that Support Emergent Knowledge Processes. *MIS Quarterly*, *26*(3), 179–212. https://mari.usc.edu/wesrac/wired/bldg-7_file/Markus.pdf

Martínez, D. & Taboada, M. (2003). Knowledge Base Development. *Lecture Notes in Computer Science*, 2774, 1373-1380. doi: 10.1007/978-3-540-45226-3_186

Matthew, R. M. (1985). Social analysis of information production and consumption: The new challenges and tasks of Third World Countries, in: A.I. Mikhalov (Ed.), *Theoretical problems of informatics: Social aspects of modern informatics*, All Union Institute for Scientific and Technical Information, 1985, pp. 37–47.

McKinsey & Company. (2020). *How COVID-19 has pushed companies over the technology tipping point—and transformed business forever*. Retrieved from https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

Minina, N. (2013). *Development of Knowledge Management Process to Enable Incident Management*. Helsinki Metropolia University of Applied Sciences. https://core.ac.uk/reader/38093380

Mostert, J. C., & Synman, M. M. M. (2007). Knowledge management framework for the development of an effective knowledge management strategy. *South African Journal of Information Management*, *9*(2). doi: 10.4102/sajim.v9i2.25

Natek, S., & Zwilling, M. (2017). Knowledge codification – The knowledge management systems perspective. In *Management challenges in a network economy: Proceedings of the MAKELEARN and TIIM International Conference 2017.* https://toknowpress.net/ISBN/978-961-6914-21-5/papers/ML17-084.pdf

Nguyen, T., & Burgess, S. (2014). A case analysis for ICT for knowledge transfer in small businesses in Vietnam. *International Journal of Information Management*, *34*(3), 416—421. doi: 10.1016/j.ijinfomgt.2014.02.009

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.

Prime Index (2019). Cybersecurity Industry Overview. https://www.primeindexes.com

Ramaiah, C. K. (2020). Measuring Knowledge Acquisition and Knowledge Creation: A Review of the Literature. *Library Philosophy and Practice (e-journal)*. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=8616&context=libphilprac

ServiceNow (January 23, 2020). *Create a security incident knowledge article*. https://docs.servicenow.com/bundle/orlando-security-management/page/product/security-incident-response/task/t_CrtScrIncdtKnwArt.html

Shrestha, S., Regm, B., Dotel, S., Bhattarai, D. & Adhikari, M. (2016). Creating a Knowledge Base to Enhance Knowledge Sharing: A Case Study of Computer Department at Kathmandu University. *Journal of Information Technology and Software Engineering, 6, 1—5.* doi: 10.4172/2165-7866.1000175

Takahashi, T. & Kadobayashi, Y. (2014). Reference Ontology for Cybersecurity Operational Information. *The Computer Journal*, *58*(10), 2297—2312. doi: 10.1093/comjnl/bxu101

Thalmann, S. & Sarigianni, C. (2016). Knowledge Protection the Unexplored Knowledge Management Strategy. *Edition Donau-Universität Krems,* 141—151. https://tinyurl.com/h9dbspv2

Tulane University (2020). *School of Professional Advancement, Emergency and Security Studies*. https://sopa.tulane.edu/blog/four-reasons-cybersecurity-field-rapidly-growing

Turban, E., Aronson, J., Liang, T., & Sharda, R. (2007). *Decision Support and Business Intelligence Systems. Eight Edition. Chapter 18: Knowledge Acquisition, Representation, and Reasoning.*

Turner, J. R., Zimmerman, T., & Allen, J. (2012). Teams as a sub-process for knowledge management. *Journal of Knowledge Management*, *16*(6), 963—977. doi: 10.1108/13673271211276227

Veryat, P. (2016). *Technology, People, and Processes in Knowledge Management*. https://www.heflo.com/blog/bpm/technology-people-and-processes/

Wamundila, S. & Ngulube, P. (2011). Enhancing Knowledge Retention in Higher Education: A case of the University of Zambia. *South African Journal of Information Management*, *13*(1), 1—9. doi: 10.4102/sajim.v13i1.439

Xue, C. T. S. (2017). A Literature Review on Knowledge Management in Organizations. *Research in Business and Management*, *4*(1). doi: 10.5296/rbm.v4i1.10786

Zaim, H. (2006). Knowledge Management Implementation in IZAGAZ. *Journal of Economic and Social Research*, *8*(2), 1—25. https://tinyurl.com/2meun5a8

AUTHOR'S BIOGRAPHY

Matthew Henry P. Bibangco is a licensed Electronics and Communication Engineer (Technological University of the Philippines Visayas, 2012) with a master's in Technology Management (University of the Philippines Diliman, 2020). He also completed 12 academic units in Information Technology, specializing in CISCO Networking, at the University of Negros Occidental-Recoletos (2015). With over nine years of experience in cybersecurity, he has expertise in incident response and knowledge management. He began his career as a SOC Analyst at Masergy Philippines (now COMCAST) and is currently a Senior Cybersecurity Incident Response Consultant at Verizon Philippines. Mr. Bibangco holds certifications as a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).