International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1181-1193
Journal homepage: http://iieta.org/journals/ijsse

A Novel Socio-Technical Framework for Enhancing Cyber Crisis Management Capabilities

Prabaswari[1*], Yusuf Ali[1], Rudy A.G. Gultom[1], Luhut Simbolon[1], Anak Agung Ngurah Gunawan[2]

[1] Defense Technology Department, Republic of Indonesia Defense University, Jakarta 10430, Indonesia
[2] Physic Department, Udayana University, Badung 80361, Indonesia

Corresponding Author Email: prabaswari@bssn.go.id

https://doi.org/10.18280/ijsse.140415

Received: 9 June 2024
Revised: 22 July 2024
Accepted: 1 August 2024
Available online: 30 August 2024

Keywords:
capability, crisis management, cyber crisis, framework., incident response, sociotechnical

ABSTRACT

In today's digitally interconnected world, organizations face unprecedented challenges due to pervasive cyber risks. As reliance on advanced technical infrastructure grows, the potential for cyber crises to disrupt operations and compromise critical data and infrastructure has increased significantly. Poorly managed responses can have catastrophic consequences for both organizations and national security. This paper presents a Systematic Literature Review (SLR) of recent studies on cyber crisis management capabilities, spanning from 2018 to 2024, and emphasizes the need for a sociotechnical approach. By utilizing the hexagonal socio-technical systems framework by Clegg et al., which includes people, culture, goals, technology, infrastructure, and processes, and analysing them with Nvivo and Delphi, we developed a Cyber Crisis Capability Model. This model identifies eight key criteria: security regulations and policies, clarity and compliance, technological reliability, human capital competence, resources and budgets, organizations, stakeholder collaboration, and cultural integration. It integrates strategic, operational, and tactical components to provide a holistic approach to cyber crisis management. Our comprehensive framework aims to enhance organizations' capabilities to effectively manage and mitigate cyber crises.

1. INTRODUCTION

In an era characterized by digital interconnection, the omnipresence of cyber risks poses unprecedented challenges to organizations worldwide [1]. As society becomes increasingly reliant on sophisticated technical infrastructures, the potential for cyber crises to disrupt operations, compromise sensitive data, and damage critical infrastructure has never been greater [2]. Crises can arise from incidents that are not appropriately resolved, and poor responses, primarily due to inadequate management and decision-making in times of uncertainty, can be catastrophic for organizations, businesses, and even nation-states as a whole [3].

Enormous cyber-attacks pose a real threat to national security, particularly when cyber incidents spread rapidly and significantly disrupt the functioning of essential public services [4]. In recent decades, several countries have experienced significant and notable cyber attacks, including the SolarWinds supply chain attack in the U.S., cyberwar attacks in Estonia [5], the Dark Seoul incident in South Korea [6], Stuxnet in Iran [7], the NotPetya ransomware attack in Ukraine, and the DDoS attack in Russia [8]. These instances underscore the global nature of cyber threats and the urgent need for every country to enhance its cybersecurity measures, particularly its cyber crisis management capabilities.

Cyber crisis management encompasses strategic methodologies for addressing incidents or attacks that aim to destroy or paralyze information systems, disrupt economic or social activities, or endanger human lives [9]. It includes capabilities in incident response, crisis management, and cyber defense, particularly at the national level [4]. Effective cyber crisis management necessitates not only technical solutions but also an understanding of the interplay between human and organizational factors. Traditional approaches to cyber crisis management must evolve to integrate the complexities of both technological and socio-technical elements [10].

The term "socio-technical" refers to the intricate interplay between social and technical elements within a system, highlighting that effective crisis management necessitates a sophisticated coordination of human, organizational, and technological factors [11]. This study will conduct a comprehensive examination of incident response, crisis management, and cyber defense capabilities to develop effective strategies for addressing cyber crises. The delineation of capabilities derived from these three categories will be articulated through a socio-technical lens.

Previous research has explored various socio-technical aspects of cybersecurity, including socio-technical cyber resilience management frameworks [11], approaches for preventing, mitigating, and recovering from ransomware attacks [10], frameworks to mitigate supply chain risks [12], and models for designing system frameworks [13], as well as design science in data search systems [14]. This perspective has also been applied to structuring cybersecurity maturity models and metrics for small and medium-sized enterprises

(SMEs) [10], the renewable energy sector [15] and incident response management capabilities [16].

Despite numerous studies addressing the socio-technical aspects of cybersecurity, a comprehensive analysis of academic records to establish a thorough understanding of the capabilities required for national-level cyber crisis management—encompassing incident response, crisis management, and cyber defense—has yet to be conducted. This paper presents a Systematic Literature Review (SLR) of relevant and current literature on cyber crisis management capabilities within a socio-technical context. Using the hexagonal socio-technical systems framework by Clegg et al., which includes socio-components such as people, culture, and goals, as well as technical components such as technology, infrastructure, and processes [17], this review aims to assess the capabilities needed to manage cyber crises from a socio-technical perspective, drawing on theories of incident response, crisis management, and cyber defense.

By identifying and analyzing critical variables and indicators of capability within these domains, this study seeks to address the existing gap in understanding the comprehensive capabilities necessary for effective cyber crisis management. The ultimate goal is to enhance national cybersecurity strategies. The findings provide a practical framework for organizations and policymakers to assess and improve their cyber crisis management capabilities systematically. The detailed checklist and octagonal model facilitate targeted improvements, leading to better preparedness, quicker response times, and more effective mitigation of cyber incidents, also reducing the impact on national security and economic stability. Overall, the study advances cybersecurity by integrating socio-technical elements, emphasizing both technical solutions and social factors, and fostering continuous improvement and adaptation to evolving threats. This research lays a foundation for future studies to refine and validate the model's effectiveness, supporting global efforts to enhance cyber resilience.

2. THEORETICAL BACKGROUND

2.1 Cyber incidents response

An incident is defined as a disruption that causes an interruption or reduction in the quality of IT services [18]. Incident management is described as efforts to restore normal operational conditions for IT services as swiftly as possible while minimizing the impact on business processes and ensuring continuous service availability [16]. Cyber incident response is a critical component of cyber resilience, encompassing the immediate response and procedures associated with IT security events. Its objectives are to detect the occurrence of an incident, mitigate its consequences, and address the threat posed to the organization. Incident Response Management (IRMA) is a vital aspect of an Information Security Management System (ISMS), serving as a repository of information to streamline and expedite the mitigation of security incidents [19]. Generally, IRMA comprises a set of procedures for managing information security incidents with clearly defined stages. Despite variations in best practices, such as those outlined in NIST 800-6 [20] and ISO/IEC 27035 [21], the process can be categorized into the following stages: preparation, detection, and learning [19]. While Preparation and Detection focus on organizing and executing incident response, learning provides feedback to the system based on information gathered during the process.

To effectively manage incidents, a specialized team with the capacity and capability to handle cyber incidents, known as the Computer Security Incident Response Team (CSIRT), is essential [22]. CSIRTs work to mitigate and prevent the spread of computer security issues. They may consist of specialists including malware and forensics experts, as well as solicitors and public relations personnel who oversee all stages of incident response management. CSIRTs offer a variety of services based on their mission and objectives, which can be classified into three broad categories:

- Reactive services, which are triggered by an event or request and are a key component of CSIRT operations;
- Proactive services, which provide support and knowledge to help prevent and minimize future incidents;
- Security quality management services, which enhance existing services that are independent of incident handling and are typically conducted by other organizational areas such as IT, audit, or training [23].

2.2 Crisis management

Before delving into crisis management, it is crucial to establish a precise definition of a crisis. A crisis is characterized as an event, revelation, allegation, or set of circumstances that threatens an individual's or organization's integrity, reputation, or survival [24]. Although the likelihood of a crisis occurring may be low, its impact, if it does materialize, can be significantly detrimental to the organization. The causes of the crisis and the measures needed to address it may not be immediately apparent; however, resolution should be pursued as expeditiously as possible. Additionally, not all key stakeholders may immediately recognize the full impact of the crisis [25]. Effective crisis management requires preparation, including the development of a crisis management plan and readiness [26].

Crisis management involves being prepared to confront adversity and minimize its effects as effectively as possible, as well as simplifying the management process during periods of chaos [27]. It encompasses the strategic management of perceptions and coordination of efforts with stakeholders to proactively prevent, resolve, and leverage a crisis for organizational growth. This field examines the procedures involved in planning, control, analysis, and communication to limit damage and prepare for crises [26]. Generally, the literature on crisis management describes it as the process of making and implementing difficult decisions in challenging situations. It is about readiness to face adversity, minimizing impacts as effectively as possible, and streamlining the management process during chaotic circumstances [27].

2.3 Cyber defense

Cyber defense encompasses a range of operations designed to protect entities and respond swiftly to threats [28]. It refers to both strategic and operational measures aimed at safeguarding individuals from significant cyber threats, including attacks, incidents, campaigns, or operations conducted by external parties [29]. Cyber defense involves responding to threats and securing critical infrastructure and information for enterprises, government agencies, and other networks [30]. A comprehensive cyber defense strategy must recognize the roles of both public and private security actors,

as these entities are pivotal in maintaining and ensuring the essential functions of society during crises [29].

Cyber defense can be categorized into three interconnected domains: "proactive," "active," and "reactive." "proactive" measures focus on enhancing the security of the cyber environment and ensuring the optimal performance of cyber infrastructure and mission functions. "active" measures aim to effectively mitigate or contain damage caused by hostile cyber operations. "reactive" measures are designed to restore efficacy or efficiency following a successful breach [28]. In essence, cyber defense involves detecting intruders, neutralizing their activities, and preventing further hacking attempts or attacks [29]. These efforts are directed towards preventing, detecting, and responding to threats or assaults promptly to protect infrastructure and information from compromise.

A defensive posture in cyber defense incorporates two strategies: deterrence to prevent attacks and resilience and security to manage attacks if prevention fails [29]. Effective implementation of these preventive and readiness strategies requires capabilities such as detection, attribution, and incident response [29]. These factors are crucial for cyber defense, with operational and intelligence capabilities playing significant roles in both prevention and preparedness strategies [29].

2.4 Cyber crisis

The European Union defines a cyber crisis as an anomalous and chaotic situation that threatens an organization's strategic goals, credibility, or survival, thus impacting its core functions [31]. A cyber crisis represents a severe threat to the core structure, principles, and norms within cyberspace, requiring critical decisions to be made under conditions of high pressure and uncertainty [26]. According to the Netherlands, a cyber crisis involves an IT-related issue affecting critical infrastructure that cannot be managed by standard crisis management organizations. Similarly, in Czechoslovakia, a "cyber crisis" can be declared if the security of information systems jeopardizes national interests [4].

A cyber crisis refers to crises occurring within the cyberspace domain. The US Patriot Act defines critical infrastructure as systems and assets, both physical and virtual, whose damage would impact national security, the economy, public safety, health, or a combination of these [32]. Based on these definitions, a cyber crisis is an event affecting national critical infrastructure that disrupts essential business processes, threatens national interests, and generates uncertainty, necessitating immediate technical and strategic decisions. A cyber crisis typically begins with a cyber incident that escalates to an unusual scale, causing significant damage to organizations and nations [27].

2.5 Socio-technical approach

Historically, incident response has predominantly focused on the technical aspects of issues [33]. However, humans are often considered the weakest link in the cybersecurity chain [10]. As research progresses, organizational incidents are increasingly recognized as resulting from the interactive complexity and socio-technical challenges that arise from unfamiliar or unsafe conditions and risky actions by individuals within organizations [34]. Incident response contributes to a broader perspective on information security management by conceptualizing information security as a socio-technical system [33].

A socio-technical system approach involves developing a system that integrates both human and technical elements [17]. This approach analyzes work systems through two concurrent investigations: one examining potential deviations that impede the conversion process and the other gathering necessary information to design and implement jobs that promote worker engagement and commitment [13]. Socio-technical systems encompass six perspectives (Figure 1): goals/metrics/visions/values, processes/procedures, people, culture, technology, and buildings/infrastructure [17].

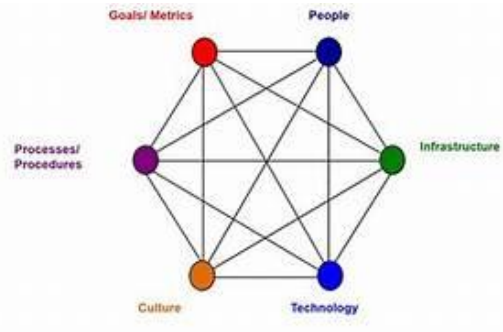

Figure 1. Socio-technical system approach by clegg et al. [17]

The hexagonal socio-technical framework presented above conceptualizes work as a complex system integrating both technical and socio elements. The technical components include technology, infrastructure, and processes, while the socio components encompass people, culture, and goals [17]. Goals refer to the objectives an organization aims to achieve or prioritize, particularly when addressing large-scale cyber incidents [35]. Processes or procedures denote the stages involved in managing cyber crises. People are the operators, staff, or stakeholders involved in responding to cyber incidents during a crisis. Infrastructure includes the physical and network facilities utilized, including those affected by cyber attacks. Culture pertains to the organizational habits or practices. Finally, technology encompasses the tools employed to manage cyber crises.

3. RESEARCH METHODOLOGY

This study employs a Systematic Literature Review (SLR) methodology, as proposed by Sepúlveda Estay [36], to examine the capabilities required for effective cyber crisis management on a national scale. The review encompasses incident response, general crisis management, and cyber defense capabilities from a socio-technical perspective, aiming to detail the capabilities necessary for managing large-scale cyber crises. Additionally, the review analyzes existing variables, frameworks, and standards for cyber crisis management to develop effective capabilities.

A Systematic Literature Review (SLR) is a formalized and repeatable process for documenting relevant knowledge within a specific research domain. It functions as a secondary study that applies a well-defined methodology to identify, analyze, and interpret all available evidence pertinent to a specific research question, ensuring that the process is unbiased and replicable [1]. The SLR process involves three stages: planning the review, conducting the review, and

reporting the review [37]. For article selection, the study employs the "Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)" protocol [38], which is widely utilized for locating literature in research related to computer security [39].

3.1 Identify research statement

The primary aim of this study is to identify effective capabilities for managing cyber crises on a national scale. To achieve this, the SLR approach will address the following questions:

1. What incident response capabilities are related to cyber crisis management capabilities?
2. What general crisis management capabilities are related to cyber crisis management capabilities?
3. What cyber defense capabilities are related to cyber crisis management capabilities?
4. What are the most recent frameworks and capabilities in cyber crisis management according to the literature?

3.2 Study identification and selection

To identify relevant studies, we utilized Scopus.com as the primary database, applying the following criteria as shown in Table 1.

The search terms included "cyber crisis," "crisis management capability," "cyber defense capability," and "incident response capability," following the criteria specified.

3.3 Study screening and extraction

The search yielded 475 articles from the Scopus database, which were then screened. After removing 96 duplicate articles, 379 articles remained. Following this, 212 articles were excluded due to lack of full texts, being conference proceedings, or not being in English, resulting in 167 articles. Of these, 43 articles could not be retrieved, leaving 124 approved articles. Further filtering based on relevance excluded 36 articles unrelated to computer science, 21 articles not aligned with the study's focus, and 23 articles not addressing incident response or crises. Consequently, 44 articles were obtained and downloaded from the Scopus database.

Additionally, references were gathered from other sources: 2 documents from organizations that publish international reports and best practices, 3 documents from journal citations, 1 dissertation thesis, and 1 book chapter, contributing 7 additional documents to the reference list. Therefore, the total number of documents analyzed was 51. The detailed selection process using the PRISMA method is depicted in Figure 2.

Table 1. The selection criteria

Criteria	Limitation
Year from	2018
Year to	2024
Tier (Q1, Q2, Q3, Q4)	Q1, Q2, Q3, Q4
Accessability	All Open Access, Gold, Hybrid Gold

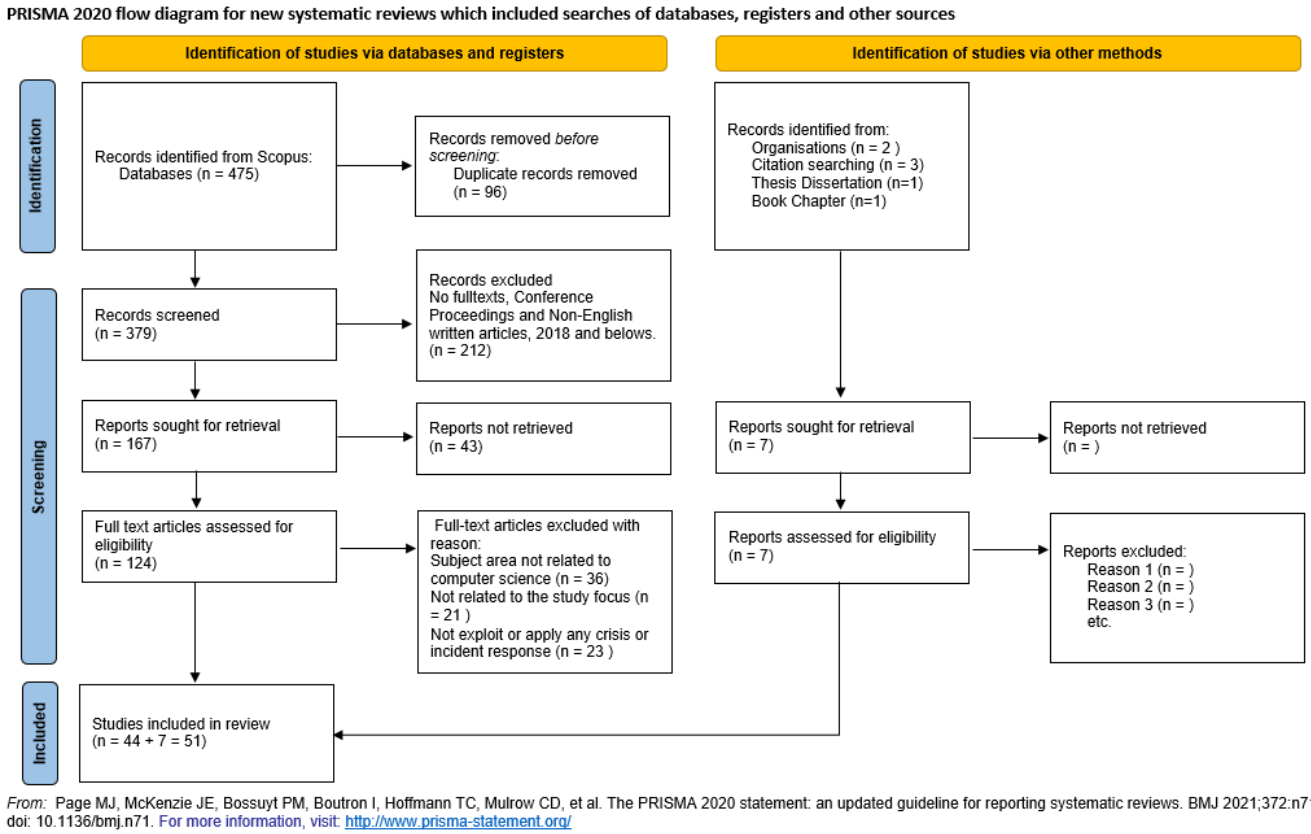

Figure 2. PRISMA 2020 flow diagram for SLR

4. RESULTS AND DISCUSSION

In developing the conceptual model of the cyber crisis capabilities framework, we conducted an identification of cyber crisis management processes in five advanced countries: Australia, the United States, Estonia, China, and the

Netherlands. The benchmarking results allowed us to identify the core processes in cyber crisis management, which were subsequently translated into nodes for coding in Nvivo. The capabilities formulated in Nvivo were then quantitatively validated using the Delphi method across two rounds, resulting in a convergent cyber crisis management framework.

4.1 Benchmarking cyber crisis management with five advanced countries

At this stage, benchmarking analysis was conducted to formulate the proposed cyber crisis management steps. The comparison was made among five advanced countries recognized for their mature management of cyber crises and proven experience in handling such crises, thus serving as a reference for cyber crisis management. Table 2 below presents the results of the comparison among China, Australia, Estonia, the United States, and the Netherlands, along with the proposed framework.

Prior to coding the capabilities using Nvivo from a socio-technical perspective, nodes were defined based on the mapping of capabilities for each core process proposed. This mapping was based on six socio-technical aspects: Goals, Technology, People, Infrastructure, Procedure, and Culture. This mapping can be seen in Table 3.

Subsequently, coding analysis will be conducted in Nvivo based on the identified nodes derived from the core processes.

4.2 Identification of capabilities through Nvivo analysis

At this stage, the results from the Systematic Literature Review (SLR) will be further analyzed using Nvivo software. Nvivo is a Computer-Assisted Qualitative Data Analysis Software (CAQDAS) tool that assists qualitative researchers in collecting, organizing, analyzing, visualizing, and reporting their data [40]. All results from the reference search were processed with the aid of Nvivo. The data processing stage involved in putting the reference collection data and coding it from a socio-technical perspective. The results of the coding process include word clouds, project maps, and mind maps. The data processing with NVivo 12 Plus is illustrated in Figure 3.

Additionally, the results of the Nvivo coding analysis are presented in the form of word clouds (Figure 4), project maps (Figure 5), and mind maps (Figure 6).

Table 2. Results of the cyber crisis management benchmark and proposed framework

Key Processes of Crisis Management	China	Australia	Estonia	United States	Netherland	Proposed Framework
Monitoring	√	√	√	√	√	
Detection	√	√	-	-	-	
Assessment	√	√	√	√	-	
Incident Identification	√	√	√	√	√	1. Cyber Incident Monitoring and Reporting
Incident Reporting	√	√	√	√	√	2. Gradual Implementation of Cyber Incident Response
Incident Response	√	√	√	√	√	3. Cyber Crisis Assessment
Incident Analysis and Classification	√	√	√	√	√	4. Early Warning
Critical Warning System	√	√	√	√	-	5. Declaration of Cyber Crisis Status
Declaration of Cyber Crisis	-	√	√	-	√	6. Formation of Cyber Crisis Task Force/Team
Establishment of Crisis Center	√	√	√	√	√	7. Establishment of Cyber Crisis Center
Crisis Mitigation and Recovery (Coordination and Technical Response)	√	√	√	√	√	8. Cyber Crisis Mitigation, including Scope Identification and Analysis, Isolation of Affected system, Evidence Pooling and Preservation, Investigation and Eradication
Crisis Communication	-	-	√	√	-	9. Attribution
Investigation and digital evidence collection	√	√	√	√	√	10. Hardening of All Systems
Attribution (if the perpetrator is identified)	√	√	√	√	√	11. Activation of Communication Protocols 12. Information Control 13. Recovery
System Security Updates (Hardening)	√	-	-	√	√	14. Mitigation Reporting
Crisis Termination	-	√	-	-	-	15. Termination of Cyber Crisis 16. Impact Calculation and Evaluation
Reporting and Evaluating	√	√	√	√	√	17. Continuous Improvement
Lesson learned and Improvement recommendations	√	√	√	√	√	

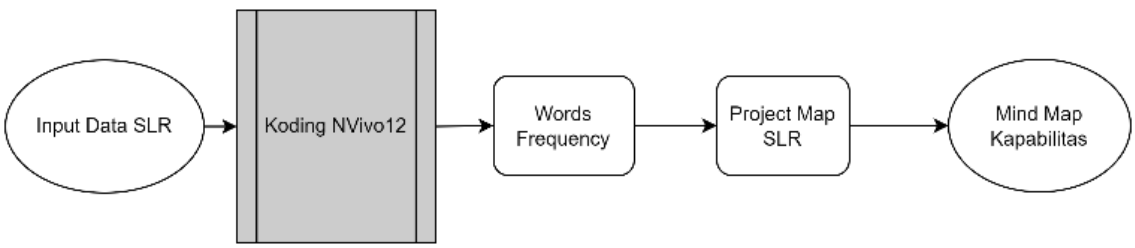

Figure 3. Nvivo 12 data processing

Table 3. Nodes identification

Socio Technical Dimensions	Key Process Mapping	Nvivo Nodes
Goals	• Formulation of contingency plan • Attribution (Attribution settings) • Activation of Communication protocols (Communication protocol settings)	1. Regulations and Security Policy
Infrastructure	• Establishment of the Cyber Crisis Task Force • Establishment of the Crisis Command Center • Cooperation between agencies, public-private and international • Budget and logistical support	2. Cyber Crisis Team 3. Organization/Crisis Command Center 4. Stakeholders Collaboration 5. Budget and Logistics
People	• Community assistance, legal experts, academics, public communication	6. Cyber security expert 7. Digital Forensic expert 8. Law Expert 9. Public communication with interpersonal skill
Procedure	• Contingency plan simulation • Monitoring, Detection, Analysis • Cyber Incident Reporting and Crisis Management • Implementation of Incident Response • Assesmen Krisis Siber • Determination of crisis status • Crisis Management • Recovery • Termination • Impact Calculation and Evaluation	10. Business Continuity Management 11. Compliance 12. Crisis dissemination and Situational Awareness 13. Incident Response Procedure 14. Risk assessment 15. Definition and threshold of crisis
Technology	• Cyber Incident Reporting (Technology, Procedure) • Early Warning • Simulation of contingency plans / mankris Monitoring, detection and analysis (culture, procedure, technology) • Implementation of Cyber Incident Response	16. Digital Forensic tools 17. Information sharing platform 18. Network Security Monitoring 19. Network Segmentation 20. Security Control 21. Security Operation Center (SOC), meliputi: 22. Service Level Agreement (SLA)
Culture	• Contingency plan simulations • Continuous Improvement	23. Awareness 24. Lesson learned 25. Training and Capacity Building

Figure 4. Word cloud

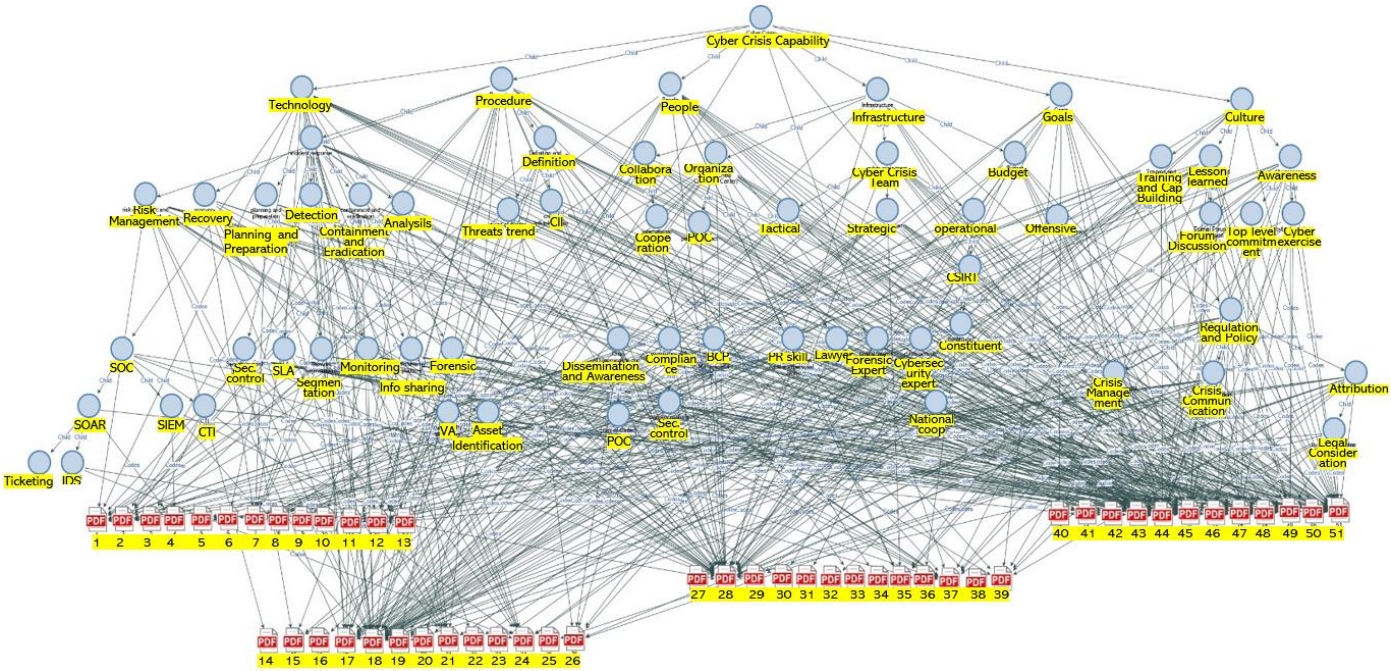

Figure 5. Project map results

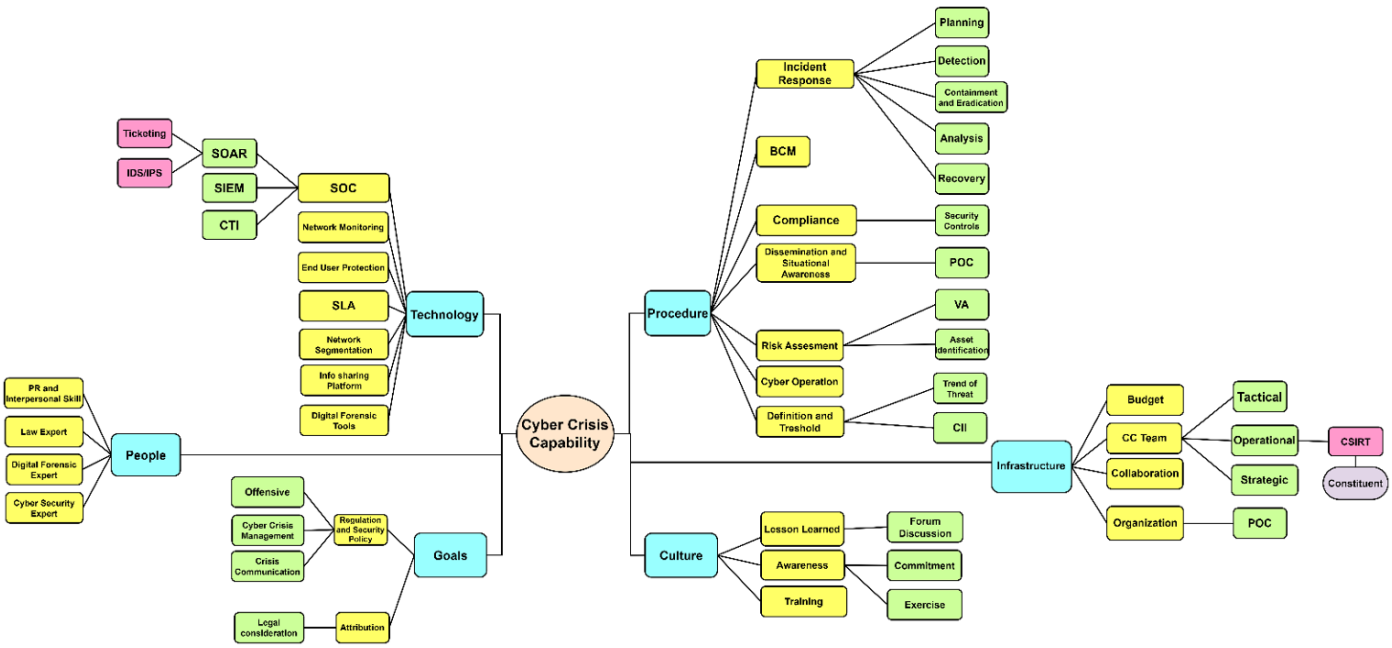

Figure 6. Mind map of cyber crisis capability

The word frequency analysis, represented as a word cloud (Figure 4), shows that several terms frequently appear in the SLR results. With a minimum word length setting of five characters, high-frequency words include "cyber," "security," "cybersecurity," "incident," "analysis," "information," "management," "crisis," "attack," "response," "organizations," and "national" and "international." These prominent terms offer preliminary insights into the capabilities that are crucial for development.

Subsequently, a project map analysis was conducted on the SLR data. The project map provides a visual representation of the results from the coding of cyber crisis management capabilities, making the findings more accessible. The capability variables are identified from a socio-technical perspective, which includes people, processes, goals, technology, culture, and infrastructure. Figure 5 displays the results of the project map analysis.

The project map results indicate that all references contribute to the six socio-technical elements identified, with each variable comprising several sub-variables. The detailed mapping of variables and sub-variables derived from the coding process is presented in Figure 6.

From the Nvivo data processing of the SLR, 27 primary capabilities along with 31 supporting capability elements for managing cyber crises were identified. Among the 27 capabilities identified through the NVivo coding results, it is evident that the majority of cyber crisis response capabilities are reflected in the incident response nodes, cybersecurity

expert nodes, and crisis communication nodes. Only two sources have indicated that ticketing is a component of cyber crisis management capability. According to most references and sources, incident response is pivotal in addressing cyber crises [16, 18, 30, 41-45]. Additionally, cybersecurity expertise plays a critical role during crises [26, 30, 41-43, 46, 47]. Conversely, socio-technical capabilities such as crisis communication are also essential for effectively managing cyber crises [39, 48-53].

4.3 Validation of identified capabilities

To validate the identified variables and capability indicators, we conducted an expert survey using the Delphi method. The Delphi technique involves soliciting expert opinions through iterative rounds to develop a consensus on multi-agency management [54]. The identified capabilities served as the basis for the expert survey, which was evaluated by 11 experts according to the following criteria in Table 4 below.

The expert survey used a Likert scale from 1 to 9, ranging from "Not Important at All" to "Extremely Important." The survey was conducted in two rounds to ensure valid results. The results from Round 1 are presented in Figure 7.

Overall, the Round 1 analysis revealed 7 capability indicators that were divergent or not yet agreed upon and 53 indicators that were convergent or agreed upon. Additionally, experts provided feedback to consolidate indicators with similar meanings and suggested modifications to variables. Consequently, in Round 2, the number of capability indicators was reduced from 60 across 8 variables to 44 indicators across the same 8 variables. Detailed results from the Delphi method in Round 2, which achieved overall convergence, are shown in Table 5.

From the final results of the Round 2 expert survey, all 44 indicators were found to be convergent (Standard deviation < 1.5) and agreed upon as essential capabilities for managing cyber crises.

4.4 Proposed model of cyber crisis capability framework

Furthermore, we developed a new cyber crisis capabilities model, as illustrated in Figure 8. This model is divided into eight variables: security regulations and policies; clarity and compliance; technological reliability; human capital competence; resources and budget; organizational structure; stakeholder collaboration; and cultural integration. This model encompasses all aspects from a socio-technical perspective and represents a novel contribution to the field of cyber crisis management.

Table 4. Experts list

Positions/Institutions	Amount
High-level Government Officials in the field of cybersecurity	2 individuals
Military CSIRT Managers	3 individuals
IT Managers in Major Private Companies	2 individuals
Lecturers and Professors in IT	3 individuals
IT Security Researchers	1 individual

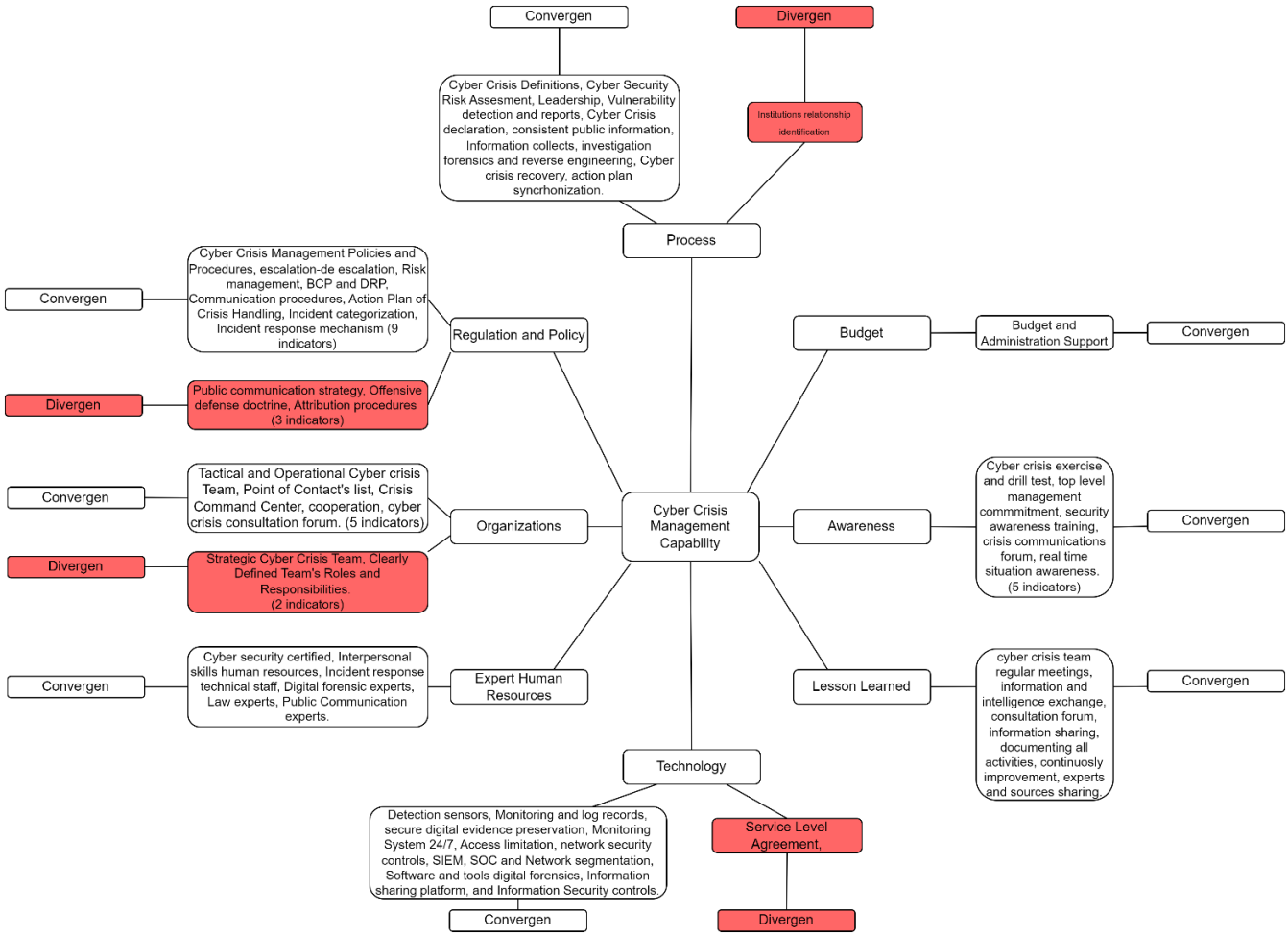

Figure 7. Round 1 results of Delphi method

Table 5. Delphi method round 2 results

No.	Instruments	Panelist											Mean	SD	Conclusion
		1	2	3	4	5	6	7	8	9	10	11			
A	**Security Regulations and Policies**														
1	Cyber crisis management	5	9	8	9	9	9	9	9	9	9	9	8.55	1.21	Convergent
2	Offensive Defense	5	9	7	9	9	9	9	9	8	9	9	7.08	1.29	Convergent
3	Crisis Communication P	8	9	7	9	9	9	8	8	8	8	8	7.00	0.65	Convergent
4	Attribution Mechanism	7	9	7	8	9	9	9	9	9	8	9	7.15	0.82	Convergent
5	Incident Response Mechanism	9	9	7	7	8	9	9	9	9	9	8	7.15	0.82	Convergent
6	Business Continuity Management	7	9	8	8	8	9	9	9	9	8	8	7.08	0.67	Convergent
7	Risk Management Guidelines	8	7	7	9	7	9	8	9	9	7	8	6.77	0.89	Convergent
8	Security Controls Procedure	8	9	7	9	9	9	9	9	8	8	9	7.23	0.69	Convergent
9	Integration of Security Policies with Organizational Objectives	7	9	7	8	9	9	9	9	7	8	9	7.00	0.90	Convergent
B	**Organizations**														
1	Cyber Crisis Command Center	6	9	6	8	8	9	9	9	9	9	8	6.92	1.17	Convergent
2	Formation Cyber Crisis Team	5	9	7	9	8	9	9	9	9	8	8	6.92	1.25	Convergent
3	Clearly Defined Roles and Responsibilities	7	9	9	8	7	9	8	9	8	9	9	7.08	0.81	Convergent
C	**Human Capital Competence**														
1	Cybersecurity Experts	8	9	8	8	8	9	8	9	8	9	8	8.36	0.50	Convergent
2	Digital Forensic Experts	8	9	8	8	8	9	9	9	7	9	8	8.36	0.67	Convergent
3	Legal Experts	8	9	8	8	8	9	9	9	8	9	8	8.45	0.52	Convergent
4	Public Communication Experts	8	7	7	7	8	9	9	9	8	9	5	7.82	1.25	Convergent
5	Adequate and Skilled Human Resources	6	7	7	9	8	9	8	9	7	9	5	7.64	1.36	Convergent
D	**Clarity and Compliance**														
1	Compliance with Security Controls	7	9	7	8	7	9	8	9	9	6	8	6.69	1.04	Convergent
2	Risk and Vulnerability Assessment	7	9	8	9	7	9	9	9	7	9	8	8.27	0.90	Convergent
3	Identification of Critical Assets	9	9	8	8	8	9	9	9	7	9	8	8.45	0.69	Convergent
4	Definition and Thresholds for Cyber Crises	9	9	8	8	7	9	9	9	7	9	8	8.36	0.81	Convergent
5	Policies Updated and Monitored	7	9	8	8	7	9	9	9	9	9	8	7.08	0.81	Convergent
E	**Technology Reliability**														
1	SOC Capabilities. including SOAR, IDS, Ticketing, CTI Tools, SIEM Systems, etc.	9	9	8	8	7	9	9	9	9	8	8	7.15	0.69	Convergent
2	Digital Forensic Tools	6	9	8	5	8	9	9	7	9	7	9	6.62	1.40	Convergent
3	Secure Information-Sharing Platform	7	9	7	8	7	9	9	9	8	7	9	6.85	0.94	Convergent
4	Network Security Monitoring Tools	8	9	8	8	8	9	8	9	9	8	8	7.08	0.50	Convergent
5	Encryption and Authentication System	8	9	8	8	8	9	9	9	7	5	8	8.00	1.18	Convergent
6	Network Segmentation	9	9	8	7	8	9	8	9	9	8	8	7.08	0.67	Convergent
7	Service Level Agreements (SLAs)	7	9	7	7	7	9	8	9	9	7	8	6.69	0.94	Convergent
8	Communication Channels and Protocols	8	9	8	8	7	9	8	9	7	7	8	6.77	0.77	Convergent
9	Knowledge Management System	6	9	7	8	7	9	9	9	8	7	5	6.46	1.36	Convergent
F	**Cultural Integration**														
1	Cybersecurity Awareness	9	9	8	8	8	9	9	9	7	9	8	8.45	0.69	Convergent
2	Cybersecurity Exercises	8	9	8	9	8	9	9	9	7	9	8	8.45	0.69	Convergent
3	Leadership Commitment	9	9	8	8	8	9	9	9	8	9	8	8.55	0.52	Convergent
4	Training and Capacity-Building	7	9	7	9	7	9	9	9	8	8	8	6.92	0.87	Convergent
5	Lessons Learned	5	9	8	8	8	9	8	9	8	8	8	6.77	1.10	Convergent
6	Information and Intelligence Sharing	7	9	8	8	7	9	8	9	8	7	8	6.77	0.77	Convergent
G	**Stakeholder Collaboration**														
1	Partnerships with Domestic Stakeholders	9	9	8	8	7	9	8	9	7	8	8	6.92	0.75	Convergent
2	Collaboration with the IT Security Community.	6	8	7	6	7	9	8	9	7	7	8	6.31	1.04	Convergent
3	International Cooperation	6	9	8	8	8	9	8	9	9	9	8	7.00	0.90	Convergent
4	Dissemination of Information and Situational Awareness	7	9	6	8	7	9	9	9	8	7	8	6.69	1.04	Convergent
5	Contact Point List	9	9	6	8	8	9	9	9	9	9	9	7.23	0.93	Convergent
H	**Resource and Budget**														
1	Sufficient Budget	9	9	9	9	9	9	9	9	8	9	8	7.46	0.40	Convergent
2	Effective Resource	9	9	9	8	8	9	9	9	9	7	9	7.31	0.67	Convergent

To enhance practicality, we propose developing a cyber crisis management model in the form of a checklist, as detailed in Table 6.

The proposed model can be visualized as an interconnected framework where each variable or criterion influences and supports the others, ensuring a comprehensive approach to cyber crisis management. The explanation of each component is as follows:

1. Security Regulations and Policies;
   Serve as the foundation, ensuring that all efforts are formalized and aligned with the strategic goals of the organization [55].
2. Clarity and Compliance;
   Control the rules and standards used as references. Ensure proper implementation of all regulatory components and best practices to support cybersecurity [47].
3. Technological Reliability;
   Ensure the availability of tools and platforms necessary for detecting, analyzing, and responding to cyber threats,

with up-to-date and active technology [56].

4. Human Capital Competence;
   Ensure the organization has personnel trained in managing and responding to cyber crises [57].
5. Resource and Budget;
   Ensure adequate resources and budgets for cyber crisis management, covering both quantity and quality [58, 59].
6. Organizations;
   A formal approach to cyber crisis management involves establishing a point of contact [54, 60], which typically includes a cyber crisis team with clearly defined roles and responsibilities.
7. Stakeholder Collaboration, and
   Efforts to manage cyber crises require collaboration not only within the country but also internationally [60]. Cooperation between Computer Security Incident Response Teams (CSIRTs) at domestic, bilateral, regional, and multilateral levels plays a crucial role, particularly in sharing information, lessons learned, and providing technical assistance [23]. Engaging with the private sector and the cybersecurity community is also vital and can facilitate the resolution of cyber crises [61].
8. Cultural Integration
   Promote a culture of security awareness and continuous improvement [62].

This model fulfils the novelty aspect by integrating all required components holistically. It combines strategic objectives with operational and tactical elements, ensuring that every level of the organization is prepared to address cyber crises. By emphasizing the importance of training, updating policies, and advancing technologies in response to emerging threats, the model supports continuous improvement. Additionally, its focus on collaboration and cooperation among stakeholders highlights the significance of unity in managing crises, supported by the ongoing development of cybersecurity awareness. Consequently, this model serves as a comprehensive framework for organizations seeking to enhance their cyber crisis management capabilities.

Figure 8. Octagon model of cyber crisis capability framework

Table 6. Cyber crisis management capabilities checklist

I.	**Security Regulations and Policies**
☐	Cyber Crisis Management Guidelines
☐	Offensive Defense Doctrine
☐	Crisis Communication Procedure
☐	Attribution Mechanism Policy
☐	Comprehensive Incident Response Mechanism
☐	Business Continuity Management and Procedures
☐	Risk Management Guidelines
☐	Security Controls Procedure
☐	Integration of Security Goals and Policies with Organizational Strategic Objectives
II.	**Clarity and Compliance**
☐	Regular Testing and Maintenance of Compliance with Security Controls and Best Practices
☐	Periodic Risk and Vulnerability Assessment
☐	Identification of Critical Assets
☐	Definition and Thresholds for Cyber Crises
☐	Policies Updated and Monitored to Align with Evolving Threats and Regulations
III.	**Technological Reliability**
☐	Comprehensive Security Operations Center (SOC) Capabilities, including SOAR, IDS, Ticketing, CTI Tools, SIEM Systems, etc.
☐	Digital Forensic Tools
☐	Secure Information-Sharing Platform
☐	Network Security Monitoring Tools
☐	Encryption and Authentication System
☐	Network Segmentation
☐	Implementation of Service Level Agreements (SLAs)
☐	Establishment of Communication Channels and Protocols for Crisis Management
☐	Knowledge Management System
IV.	**Human Capital Competence**
☐	Availability of Cybersecurity Experts
☐	Availability of Digital Forensic Experts
☐	Availability of Legal Experts
☐	Recruitment and Training of Public Communication Experts with Strong Interpersonal Skills
☐	Adequate and Skilled Human Resources
V.	**Resource and Budget**
☐	Sufficient Budget Allocation
☐	Effective Resource Management for Cyber Crisis Initiatives
VI.	**Organizations**
☐	Establishment of a Robust Cyber Crisis Command Center as the Main Contact Point
☐	Formation of a Well-Structured Cyber Crisis Team (Strategic, Operational, and Tactical Teams)
☐	Clearly Defined Roles and Responsibilities
VII.	**Stakeholder Collaboration**
☐	Development of Strong Partnerships with Domestic Stakeholders (especially CSIRT and Private Sectors)
☐	Ongoing Collaboration with the IT Security Community.
☐	Cooperation with International Stakeholders (Bilateral, Regional, and Multilateral)
☐	Dissemination of Crisis Information and Maintenance of Situational Awareness Using Available Contact Points
☐	Availability of a Contact Point List
VIII	**Cultural Integration**
☐	Promotion of Cybersecurity Awareness
☐	Regular Cybersecurity Exercises and Drills
☐	Leadership Commitment to Cybersecurity
☐	Continuous Training and Capacity-Building Programs to Foster a Proactive Cybersecurity Culture
☐	Formal Discussion Forums for Implementing Lessons Learned from Past Incidents or Crises
☐	Information and Intelligence Sharing with All Stakeholders through a Secure Platform

5. CONCLUSION

In this study, a systematic literature review (SLR) was conducted to identify the capabilities required for effective cyber crisis management at the national level. Addressing the

main research questions, we reviewed 51 credible sources using PRISMA protocols and benchmarked five advanced countries to develop an ideal workflow. Coding analysis with NVivo 12 Plus software followed with validation through two rounds of the Delphi method, resulted in 8 variables with 44 capabilities indicators. These capabilities were elaborated into a comprehensive octagon model with eight key variables: security regulations and policies; clarity and compliance; technological reliability; human capital competence; resource and budget management; organizational structure; stakeholder collaboration; and cultural integration. This model, detailed into specific indicators, forms a comprehensive checklist that enables organizations to measure their readiness and enhance their preparedness for future cyber crises effectively.

The practical implications of this research are significant. By providing a structured framework and a detailed checklist, organizations—particularly at the national level—can systematically assess and improve their cyber crisis management capabilities. The octagonal model integrates both technical and socio-technical aspects, ensuring a holistic approach to managing cyber crises. Policymakers and security practitioners can use this model to develop robust strategies and action plans, thereby enhancing national cybersecurity resilience.

However, this study has several limitations. Some variables may require deeper exploration due to the limited number of references used in the SLR. Future research should focus on validating these findings and examining each indicator in greater detail. Additionally, empirical testing of the model in various organizational contexts would provide valuable insights into its practical applicability and effectiveness. The checklist framework could also be developed into a maturity model by formulating questions based on the identified indicators.

In conclusion, this research contributes to the field of cyber crisis management by offering a comprehensive, integrated framework that organizations can use to improve their crisis response capabilities. Continuous improvement, regular training, policy updates, and fostering collaboration between stakeholders are essential for maintaining a proactive cybersecurity posture. Future research should aim to refine the model further, validate its effectiveness, and explore additional capabilities as cyber threats evolve.

ACKNOWLEDGEMENT

The authors gratefully acknowledge Indonesia Defense University (Unhan RI) for their support in the completion of this research. This research was self-funded.

REFERENCES

[1] Maček, D., Magdalenić, I., Ređep, N.B. (2020). A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. International Journal of Safety and Security Engineering, 10(2): 161-174. https://doi.org/10.18280/ijsse.100202

[2] Mott, G., Nurse, J.R.C., Baker-Beall, C. (2023). Preparing for future cyber crises: Lessons from governance of the coronavirus pandemic. Policy Design and Practice, 6(2): 160-181. https://doi.org/10.1080/25741292.2023.2205764

[3] Skopik, F., Leitner, M. (2021). Preparing for national cyber crises using non-linear cyber exercises. In 2021 18th International Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, pp. 1-5. https://doi.org/10.1109/PST52912.2021.9647795

[4] Boeke, S. (2018). National cyber crisis management: Different European approaches. Governance, 31(3): 449-464. https://doi.org/10.1111/gove.12309

[5] Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia' s eID crisis. Government Information Quarterly, 40(1): 101781. https://doi.org/10.1016/j.giq.2022.101781

[6] Hemanidhi, A., Chimmanee, S. (2017). Military-based cyber risk assessment framework for supporting cyber warfare in Thailand. Journal of Information and Communication Technology, 16(2): 192-222. https://doi.org/ 10.32890/jict2017.16.2.1

[7] Kanellopoulos, A., Vamvoudakis, K.G. (2020). A moving target defense control framework for cyber-physical systems. IEEE Transactions on Automatic Control, 65(3): 1029-1043. https://doi.org/10.1109/TAC.2019.2915746

[8] Sufi, F. (2023). Social media analytics on Russia–Ukraine cyber war with natural language processing: perspectives and challenges. Information, 14(9): 485. https://doi.org/10.3390/info14090485

[9] Spillan, J.E., Parnell, J.A., De Mayolo, C.A. (2011). Exploring crisis readiness in Peru. Journal of International Business and Economy, 12(1): 57-83. https://doi.org/10.51240/jibe.2011.1.4

[10] Van Haastrecht, M., Ozkan, B.Y., Brinkhuis, M., Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. Applied Sciences, 11(15): 6909. https://doi.org/10.3390/app11156909

[11] Christine, D.I., Thinyane, M. (2022). Socio-technical cyber resilience a systematic review of cyber resilience management frameworks. Digital Transformation for Sustainability, Springer, Cham, 573-597. https://doi.org/10.1007/978-3-031-15420-1_28

[12] Colabianchi, S., Bernabei, M., Costantino, F., Romano, E., Falegnami, A. (2023). MARLIN method: Enhancing warehouse resilience in response to disruptions. Logistics, 7(4): 95. https://doi.org/10.3390/logistics7040095

[13] Zoto, E., Kianpour, M., Kowalski, S.J., Lopez-Rojas, E.A. (2019). A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. Complex Systems Informatics and Modeling Quarterly, 4(18): 65-75. https://doi.org/10.7250/csimq.2019-18.04

[14] Gregory, K.M., Cousijn, H., Groth, P., Scharnhorst, A., Wyatt, S. (2020). Understanding data search as a socio-technical practice. Journal of Information Science, 46(4): 459-475. https://doi.org/10.1177/0165551519837182

[15] Hadi, A., Dwi, A., Onoda, H. (2022). Socio-techno-economic assessment to design an appropriate renewable energy system for remote agricultural communities in developing countries. Sustainable Production and Consumption, 31: 492-511. https://doi.org/10.1016/j.spc.2022.03.009

[16] Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., Strobel, J. (2023). Managing the inevitable – a maturity

model to establish incident response management capabilities. Computers & Security, 125: 103050. https://doi.org/10.1016/j.cose.2022.103050
[17] Clegg, C.W., Robinson, M.A., Davis, M.C., Bolton, L.E., Pieniazek, R.L., Mckay, A. (2017). Applying organizational psychology as a design science: A method for predicting malfunctions in socio-technical systems (PreMiSTS). Design Science, 3(4): 1-31. https://doi.org/10.1017/dsj.2017.4
[18] Shaked, A., Cherdantseva, Y., Burnap, P., Maynard, P. (2023). Computers & security operations-informed incident response playbooks. Computers & Security, 134: 103454. https://doi.org/10.1016/j.cose.2023.103454
[19] De Jesus, R., Luis, M., Dias, A., Germano, E., Araujo, J. (2019). Specialized CSIRT for incident response management in smart grids. Journal of Network and Systems Management, 27(1): 269-285. https://doi.org/10.1007/s10922-018-9458-z
[20] Cichonski, P., Millar, T., Grance, T., Scarfone, K. (2012). Computer security incident handling guide (draft). NIST Special Publication, 800-61. http://gocs.info/pages/fachberichte/archiv/113-draft-sp800-61rev2.pdf.
[21] Trifonov, R., Nakov, O., Manolov, S., Tsochev, G., Pavlova, G. (2021). "Cyber-security of industrial computer systems"-differentiation as a separate discipline. In 2021 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, pp. 414-419. https://doi.org/10.1109/ICAI52893.2021.9639645
[22] Prabaswari, P., Alfikri, M., Ahmad, I. (2022). The implementation of policy for the establishment of a cyber incident response team to support information security in the government sector. Matra Pembaruan, 6(1): 1-14. https://doi.org/10.21787/mp.6.1.2022.1-14
[23] Carnegie Mellon University, Create a Csirt Background, Pittsburgh, 2017. https://insights.sei.cmu.edu/documents/491/2017_019_001_485695.pdf.
[24] Oscarsson, O. (2022). Crisis-as-practice: Conceptualizing the role of everyday work practices in crisis management. International Journal of Disaster Risk Reduction, 83: 103438. https://doi.org/10.1016/j.ijdrr.2022.103438
[25] Graf, F., Lenz, A., Eckhard, S. (2023). Ready, set, crisis–transitioning to crisis mode in local public administration. Public Management Review, 26(7): 2039-2063. https://doi.org/10.1080/14719037.2023.2242851
[26] Ezioni, L., Siboni, G. (2021). Cyber crisis management and regulation. Cybersecurity and Legal-Regulatory Aspects, 1-21. https://doi.org/10.1142/9789811219160_0001
[27] Dykstra, J.A.B.S., Orr, S.R. (2017). Acting in the unknown: The cynefin framework for managing cybersecurity risk in dynamic decision making. In 2016 International Conference on Cyber Conflict (CyCon U.S.), Washington, DC, USA, pp. 1-6. https://doi.org/10.1109/CYCONUS.2016.7836616
[28] Control, J., Galinec, D., Možnik, D., Guberina, B. (2018). Cybersecurity and cyber defence: National level strategic approach. Journal for Control, Measurement, Electronics, Computing and Communications, 58(3): 273-286. https://doi.org/10.1080/00051144.2017.1407022
[29] Griffith, M.K. (2018). Strengthening the EU's Cyber Defence Capabilities, November 2. Brussels: Center for European Policy Studies (CEPS). https://euagenda.eu/upload/publications/untitled-201590-ea.pdf.
[30] Kim, D., Ahn, M.K., Lee, S., Lee, D., Park, M., Shin, D. (2023). Improved cyber defense modeling framework for modeling and simulating the lifecycle of cyber defense activities. IEEE Access, 11: 114187-114200. https://doi.org/10.1109/ACCESS.2023.3324901
[31] Boeke, S. (2016). First responder or last resort? The role of the ministry of Defence in national cyber crisis management in four European countries. Leiden University Scholarly Publications. https://hdl.handle.net/1887/46615.
[32] Gultom, R.A.G., Wadjdi, A.F., Poniman, A., Martha, S., Kristijarso. (2021). Sixware cybersecurity framework development to protect defense critical infrastructure and military information systems. International Journal of Scientific & Technology Research, 10(1): 328-332.
[33] Line, M.B., Albrechtsen, E., Jaatun, M.G., Tøndel, I.A., Johnsen, S.O., Longva, O.H., Wærø, I. (2009). A structured approach to incident response management in the oil and gas industry. Critical Information Infrastructure Security, Springer, Berlin, Heidelberg, 235-246. https://doi.org/10.1007/978-3-642-03552-4_21
[34] Ho, S.M., Gross, M. (2021). Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness. Computers & Security, 108: 102357. https://doi.org/10.1016/j.cose.2021.102357
[35] Sittig, D.F., Singh, H. (2016). A socio-technical approach to preventing, Mitigating, and recovering from Ransomware attacks. Applied Clinical Informatics, 7(2): 624-632. https://doi.org/10.4338/ACI-2016-04-SOA-0064
[36] Sepúlveda Estay, D.A., Sahay, R., Barfod, M.B., Jensen, C.D. (2020). A systematic review of cyber-resilience assessment frameworks. Computers & Security, 97: 101996. https://doi.org/10.1016/j.cose.2020.101996
[37] Pinto, D., Fernandes, A., da Silva, M.M., Pereira, R. (2022). Maturity models for business continuity–A systematic literature review. International Journal of Safety and Security Engineering, 12(1): 123-136. https://doi.org/10.18280/ijsse.120115
[38] Casal-Ribeiro, M., Boavida-Portugal, I., Peres, R., Seabra, C. (2023). Review of crisis management frameworks in tourism and hospitality: A meta-analysis approach. Sustain., 15(15): 12047. https://doi.org/10.3390/su151512047
[39] Knight, R., Nurse, J.R.C., Ct, K. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security, 99: 102036. https://doi.org/10.1016/j.cose.2020.102036
[40] Mortelmans, D. (2019). Analyzing qualitative data using NVivo. The Palgrave Handbook of Methods for Media Policy Research, 435-450. https://link.springer.com/chapter/10.1007/978-3-030-16065-4_25.
[41] Schrijvers, E., Prins, C., Passchier, R. (2021). Preparing for Digital Disruption. Springer, Zuid Holland, 33-57. https://doi.org/10.1007/978-3-030-77838-5_4
[42] Ilca, L.F., Lucian, O.P., Balan, T.C. (2023). Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response. Sensors, 23(15): 6757.

https://doi.org/10.3390/s23156757
[43] He, Y., Maglaras, L., Aliyu, A., Luo, C. (2022). Healthcare security incident response strategy - a proactive incident response (IR) procedure. Security and Communication Networks, 2022: 2775249. https://doi.org/10.1155/2022/2775249
[44] Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., Hutchison, D. (2021). A cyber incident response and recovery framework to support operators of industrial control systems. International Journal of Critical Infrastructure Protection, 37: 100505. https://doi.org/10.1016/j.ijcip.2021.100505
[45] Østby, G., Katt, B. (2020). Maturity modelling to prepare for cyber crisis escalation and management. In Proceedings of the 6th International Conference on Information Systems Security and Privacy ICISSP - Volume 1, Valletta, Malta, pp. 249-256. https://doi.org/10.5220/0008871602490256
[46] Spring, J.M., Illari, P. (2021). Review of human decision-making during computer security incident analysis. Digital Threats: Research and Practice, 2(2): 1-47. https://doi.org/10.1145/3427787
[47] Karabacak, B., Yildirim, S.O., Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. International Journal of Critical Infrastructure Protection, 15: 47-59. https://doi.org/10.1016/j.ijcip.2016.10.001
[48] Xu, M., Lu, C. (2021). China–U.S. cyber-crisis management. China International Strategy Review, 3(1): 97-114. https://doi.org/10.1007/s42533-021-00079-7
[49] Delerue, F., Kaminska, M. (2023). Governing cyber crises: Policy lessons from a comparative analysis. Policy Design and Practice, 6(2): 127-130. https://doi.org/10.1080/25741292.2023.2213061
[50] Kao, G.H., Wang, S.W., Dawes, J. (2020). Modeling airline crisis management capability: Brand attitude, brand credibility and intention. Journal of Air Transport Management, 89: 101894. https://doi.org/10.1016/j.jairtraman.2020.101894
[51] Jalali, M.S., Russell, B., Razak, S., Gordon, W.J. (2019). EARS to cyber incidents in health care Search strategy. Journal of the American Medical Informatics Association, 26(1): 81-90. https://doi.org/10.1093/jamia/ocy148
[52] Sanjeev, M.A., Pande, N., Santhosh Kumar, P.K. (2021). Role of effective crisis communication by the government in managing the first wave COVID-19 pandemic – a study of Kerala government's success. Journal of Public Affairs, 21(4): e2721. https://doi.org/10.1002/pa.2721
[53] Falowo, O.I., Popoola, S., Riep, J. (2022). Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. IEEE Access, 10: 134038-134051. https://doi.org/10.1109/ACCESS.2022.3231847
[54] Gyllencreutz, L., Rådestad, M., Saveman, B.I. (2020). Templates for handling multi-agency collaboration activities and priorities in mining injury incidents: A Delphi study. International Journal of Emergency Services, 9(3): 257-271. https://doi.org/10.1108/IJES-06-2019-0026
[55] Lehto, M., Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. Information Security Journal: A Global Perspective, 30(3): 139-148. https://doi.org/10.1080/19393555.2020.1813851
[56] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7: 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334
[57] Garcia-Perez, A., Sallos, M.P., Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: An intellectual capital perspective. Journal of Intellectual Capital, 24(2): 465-486. https://doi.org/10.1108/JIC-06-2021-0166
[58] Hutomo, A., Putro, I.N.Y., Qomariyah, L., Ningsih, S.J., Wadjdi, A.F., Lestari, A.A., Gultom, R.A.G., Purwantoro, S.A., Widodo, P., Amperiawan, G. (2021). Evaluating the interoperability of C4ISR system using cyber six-ware framework. In 2021 International Conference on Advanced Computer Science and Information Systems (ICACSIS), Depok, Indonesia, pp. 1-7. https://doi.org/10.1109/ICACSIS53237.2021.9631359
[59] Mokhtarzadeh, N., Mahdiraji, H., Beheshti, M., Zavadskas, E. (2018). A novel hybrid approach for technology selection in the information technology industry. Technologies, 6(1) 34. https://doi.org/10.3390/technologies6010034
[60] Alawida, M., Omolara, A.E., Abiodun, O.I., Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of COVID-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10): 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003
[61] da S. Avanzi, D., Foggiatto, A., dos Santos, V.A., Deschamps, F., de Freitas Rocha Loures, E. (2017). A framework for interoperability assessment in crisis management. Journal of Industrial Information Integration, 5: 26-38. http://dx.doi.org/10.1016/j.jii.2017.02.004
[62] Bagheri, S., Ridley, G., Williams, B. (2023). Organisational cyber resilience: Management perspectives. Australasian Journal of Information Systems, 27: 1-28. https://doi.org/10.3127/ajis.v27i0.4183