2023 International Conference on Data Security and Privacy Protection (DSPP) | 979-8-3503-0315-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/DSPP58763.2023.10404318

An Assessment of Capabilities Required for Effective Cybersecurity Incident Management - A Systematic Literature Review

1st Olufunsho I. Falowo
School of Information Technology
University of Cincinnati
Cincinnati, United States of America
ORCid: 0000-0002-4460-0986

2nd Kehinde Koshoedo
School of the Built Environment
Oxford Brookes University
United Kingdom
19072984@brookes.ac.uk

3rd Murat Ozer, Ph.D.
School of Information Technology
University of Cincinnati
Cincinnati, United States of America
ozermm@ucmail.uc.edu

***Abstract*—Reports from multiple independent sources reveal that a lack of preparation/readiness for cybersecurity incidents detrimentally affects business continuity and delays the recovery of operations. The current cybersecurity paradigm suggests that any organization can have cyberattacks anytime, regardless of the security principles applied. Therefore, the preparation/readiness phase is vitally essential to respond to these attacks adequately. We first identified a report on major cybersecurity incidents that is compiled by the Center for Strategic & International Studies, from which we examined major cybersecurity incidents, and we then established its credibility, non-partisan, global outreach, and attack coverage by cross-referencing it with Data Breach Investigation Report (DBIR). Given this context, this study conducts a systematic literature review to understand the body of knowledge that highlights administrative and technical capabilities of organizations to respond to a likely cybersecurity attack. Study findings show that about 72 percent of surveyed papers suggest that more organizations embrace administrative capabilities, especially compared to technical skills. More organizations also recognize the importance of having Cybersecurity Incident Response Team (CSIRT) abilities to enhance readiness to combat potential cybersecurity incidents - this is validated by the 88.89 percent score identified in this study. We emphasize the significance of organizations' readiness to conduct cybersecurity incident triage and or thorough investigation based on the fact that major incidents will always occur as we validated in this study. As a result, using the National Institute of Standards and Technology (NIST) framework as an example, we suggest that organizations should determine which stages of the NIST framework are applicable.**

***Index Terms*—Cybersecurity incident handling, Cyber threat management, Incident management, Incident response, Security administrative control, Security technical control**

I. Introduction

Building on the claims that administrative and technical mitigation controls are critical towards ensuring effective incident response to cybersecurity threats as documented in the conclusion aspect of the article published by IEEE titled "Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents" [1], this study is an attempt to validate that claim and to confirm how relevant are the claims vis-a-vis the modern day enterprises. Statistics suggest that over 200 organizations worldwide, including multiple US government agencies, announced compromised cases due to the data breach incident of SolarWinds in 2020 [2]. Between 2013 and 2017, more than 170 universities worldwide lost $3.4 billion worth of intellectual property as a result of data theft incidents [2]. The general overview of cybersecurity incidents from 2005 to 2022 shows that many incidents have impacted various organizations in different regions of the world [2], [3], [4].

The likelihood of a cybersecurity incident occurring in any organization is a fact. Therefore, any small, medium, or large organization must have the proper cybersecurity incident detection and response capabilities to deal with it if or when it happens [5]. Cybersecurity incident detection and response capabilities often require the combination of human resources, security systems, information technology infrastructure, and processes to be in place for a practical readiness to respond to an incident when it occurs [6]. The processes of building cybersecurity incident detection and response capabilities are often very complex and might usually require specific customization to the need of an organization [7]. Therefore, this study conducted a secondary study exploring how organizations handle cybersecurity incidents.

Organizational strategies to handle cybersecurity incidents matter because a lack of effective detection or response capabilities to an incident can have a devastating impact on the way the organization is perceived by not just its customers but shareholders as well [8]. One example of an organization that experienced a catastrophic cybersecurity incident that we can learn from is Target Incorporation [9], [10]. Following the facts of the data breach incident at Target Incorporation and exploring how its management handled and addressed the cybersecurity incidents that impacted them in 2013, one of the lessons learned is that there is often an indicator that ineffective cybersecurity detection and response capabilities have very high chances of leading to an unfavorable outcome that often times may be significant loss of customers' confidence, reputational damage and financial loss [11]. Another

example of a major incident to learn from is the Equifax data breach announced in 2017, which impacted over 100 million customers and subsequently exposed Equifax to legal liability, and reputational damage [12]. These examples of Equifax and Target Inc. are to further highlight the importance of having effective cybersecurity incident management capabilities in place as part of organizational efforts to be prepared and ready for a cybersecurity attack when it happens.

This paper presents an exploratory systematic literature review on cybersecurity incident management capabilities, aiming to identify what is currently popular in the industry. This study used multiple models of systematic literature review including AbuHassan [13] as a framework and guidelines. One of the objectives of this study is to identify the commonalities and differences in how organizations manage incidents to determine what lessons business entities can learn by looking for information on how to handle cybersecurity incidents effectively. During our exploratory investigation of the eighteen papers that were selected for this systematic literature review, we identified that all the capabilities leveraged to respond to cybersecurity incidents are grouped into (1) Administrative capabilities, (2) Technical capabilities, and (3) Hybrid of both technical and administrative capabilities. While physical capabilities are often also relevant, it is out-of-scope for this study. In order to ensure a convergence of how organizations are handling cybersecurity incidents, our systematic literature review incorporated coverage of a wide array of publishing databases.

After exploring online electronic scholarly search engine databases, targeting an array of diverse publishing organizations and ensuring coverage of relevant studies is maximized, we initially identified over a hundred papers but eventually cut down to a final list of eighteen pieces of literature that serve as the primary sources of information that helped answer the question posed by this literature review. In this study, it is crucial to highlight the fact each of the eighteen literature reviewed echoes bits and pieces of cybersecurity incident management capabilities. Still, none of them adequately described a capability that captures the approach toward the management of cybersecurity incidents. Therefore, after exploring these studies, another important question arose: is there an ideal approach toward the management of cybersecurity incidents? While part of this question is addressed in this study, it may be important to deep-dive into answering it in future research.

A. Research Question (RQ)

As the tenacity of threat actors continues to disrupt organizations [14], some will lead to data breach incidents and people's data privacy violation [15], [16], [17], [18] that will result in financial loss or even national security concerns [2], [8] as well. Therefore, the primary objective of this study is to conduct a secondary research to explore what other papers have identified as the necessary administrative or technical capabilities that are essential towards effective management of cybersecurity incidents. Given this introduction, the core research question that influenced this study is highlighted below:

- RQ1: What capabilities are being leveraged by organizations to respond to cybersecurity incidents?

II. Background Literature

No organization, including small, medium, and big businesses and government institutions, is safe from today's sophisticated cyberattacks, even those with the highest or most robust security controls in place [14]. When these cyberattacks are successfully launched to cause adverse consequences to a targeted entity, it becomes a cybersecurity incident [19]. Given that cybersecurity incidents can be compared to emergencies that may have catastrophic repercussions, the longer they are ignored or improperly controlled, the more severe the results will be [20]. These aforementioned premises echo the importance of having a prepared incident management capability in place. While having an incident management protocol is very important, it is even more significant to ensure that it is well tested [21].

A. Administrative Capabilities

In this section, we highlight some of the administrative controls that organizations employ or at least think about when preparing for or handling a cybersecurity incident. The list here is not exhaustive but at least summarizes some of our findings from the literature that we surveyed in this study:

1) Communication: Projecting a positive outlook and ensuring effective but transparent public communication during incident handling tends to calm not just the stakeholders but may also stabilize the market forces as well [22]. This suggests the importance of a communication policy that does not only provide coverage for external but internal audiences as well. Having a policy drafted and approved may not be enough. Policy enforcement is also crucial for effective communication during handling of an incident [23]. Given how in "today's cyber threat landscape, a wide variety of skills and coordination are needed to combat increasingly complex challenge" [24], leveraging an effective internal and external communication during the handling of a cybersecurity incident may be valuable towards addressing the identified cyber threats.

2) Information Sharing: Having the necessary information sharing strategy in place and effectively executing such strategy, whether it is prior the occurrence of a major security event or during an active cybersecurity incident management, is very crucial towards ensuring that all parties are kept informed in the prior, during and post stages of any given cybersecurity incident [20], [25], [26], [24], [27], [28]. The goal of the collaboration during cybersecurity incident management is very critical, especially with respect to information sharing, hence this goal is to provide or establish a defined framework for sharing relevant and important information that enhances consistency in handling cybersecurity incidents among relevant stakeholders [20]. To echo another importance of information sharing, "multiple analysts might collaborate to determine the

extent to which an attack has penetrated a system, while others might coordinate announcements and alerts to additional teams in the organization or even outside agencies" [26].

"Information about threats can improve an organization's situational awareness, expand its understanding of the current threat horizon and increase its defensive agility by improving decision making" [24]. Beyond an organization's internal communication, it is also very important to highlight how information sharing can enhance cybersecurity incident response on a global scale by ensuring the reduction of disparity of cybersecurity information that is available among countries and organizations [27]. Therefore, national governments, industries, businesses, and organizations, as well as individual end users of digital devices, share responsibility for cybersecurity information sharing [25]. It suffices to say that nation states often coordinate shared cyber defense obligations in order to build capacities to achieve cyber resilience, lower cybercrime, and secure crucial national infrastructure [25].

3) Training: An organization's "information assets leak out due to employees' careless behavior, for instance, downloading emails sent by an unidentified sender, checking linked-pages incautiously or setting passwords by their own birthdays" [29], hence it is very important that the necessary investments are made, with the right programs designed to ensure the implementation of information security training and education for employees [29]. Also, given that the global information technology skills shortages have surpassed four million, one of the identified remedies is for organizations to take a look inward and strengthen the cross-training of existing information technology professionals where possible [30]. Incorporating information security into some of these cross-training programs may also alleviate some of the challenges posed by a lack of cybersecurity education. A routine tabletop exercise is one of the best ways to get ready for handling a significant cybersecurity event since it raises the knowledge, comprehension, and readiness of cybersecurity incident response teams [21].

4) Policies, Processes, Procedure and Standard Frameworks (PPP & SF): Having an enterprise incident response policy, well documented processes, clear procedure, defined standards and other relevant artifacts in place as part of the effort to ensure readiness for a potential cybersecurity incident is fundamentally a necessary foundation for an effective incident management and if well enforced, could not only ensure adequate response during incident handling but may also prevent a disastrous fiasco [31], [32], [33]. Since it is impossible or economically unrealistic to prevent all cybersecurity incidents, it makes sense to have the necessary plans and procedures to handle them when they occur [33]. Leveraging standard frameworks such as the National Institute of Standards and Technology (NIST) special publication 800-61, computer security and incident handling guide, revision 2 or the SANS Institute's Computer security incident handling, is very critical towards building a robust cybersecurity incident response capability [34], [35], [36], [37].

B. Technical Capabilities

Monitoring security events, gathering and storing security logs, and correlating and analyzing all data connected to the incident that has occurred or is occurring are some of the primary operations required to deal with cybersecurity problems [14]. In this section, we highlight some of the technical capabilities organizations leverage to manage cybersecurity incidents. Capabilities referred to in this section often require some sophisticated technology and technical expertise.

1) Monitoring and Detection: In order to successfully execute a timely and appropriate response to a cybersecurity incident, it is essential to gain visibility into the constantly evolving security threats, identify indicators of compromise early on, and correlate security logs in order to confirm if a cybersecurity incident has occurred [38], [14], [30]. This may help an organization achieve a reasonable mean-time-to-detect a cybersecurity incident. The available logs gathered during security monitoring are very helpful in understanding (a) the nature of what happened, (b) the scope and impact of a cybersecurity incident, (c) if the incident is false-positive or true-positive, (d) how to contain it if it is a true-positive cybersecurity incident [19], [14], [38].

2) Analysis and Correlation of Security Logs: The frequency, scale, sophistication, and severity of cybersecurity incidents, which constantly threaten organizations, governments, and businesses, are rising [38]. As a result, it is equally important to be able to ensure real-time analytics of the incident as it is to conduct data-driven analysis [38], [14]. Organizations incur significant costs due to time delays in detecting, analyzing, and responding to cyber threats [14]. As a result, more and more businesses are adopting security information and event management (SIEM) solutions to analyze security logs and ensure proper correlations of events across multiple sources in order to fully assess the scope or impact of the threat and then implement the necessary containment measures [14], [30], [38], [19].

3) Containment, Remediation and Recovery (CRR): Right after the detection and analysis of an incident, the next phase is usually to contain, remediate and ensure recovery where applicable [34]. Containment capabilities include employing intrusion prevention systems, patching the vulnerable application, operating system hardening, password resetting, blocking hash values of malicious files, and leveraging endpoint protection systems [34], [39], [40], [41]. Identifying other associated indicators of compromise to eradicate them are all vital steps in mitigating a cybersecurity incident, thereby aiding the prevention of further propagation of an attack [42], [43]. After the initial containment of an incident, it is often necessary to assess the scope, impact and severity of what happened and then determine what level of enterprise level remediation or recovery may be required to further enhance a stable environment [44], [45], [46], [47], [48].

4) Automation: By automating incident handling procedures, incident response capabilities may be quickly and effectively changed to detect and respond to complex and emerging cybersecurity threats. This can help assure business

continuity during and after a cybersecurity security incident [14]. Given the level of complexity and thorough analysis that are required to gather indicators of compromise, establish nature of an incident, determine scope and impact of what happened, the use of automated processes to correlate security logs from multiple sources will not only enhance effectiveness and efficiency but may cut down the rate of false-positive or benign detection (or incomplete analysis), thereby allowing the incident response team to triage or investigate more higher severity incidents [49], [50], [51], [52].

C. Hybrid of Administrative and Technical Capabilities

This section highlights how organizations combine both administrative and technical capabilities together to address cybersecurity incidents. Some organizations build Cyber Security Incident Response Teams (CSIRT) and then leverage them to carry out security operations [53], [28], [24], [26]. It is very important to ensure and establish an effective communication, collaboration and coordination during the handling of a cybersecurity incident, therefore by leveraging a CSIRT makes it easier to do so [53]. Some "organizations usually build a Security Operation Center (SOC) which is a centralized location where CSIRT monitor, detect, analyze and respond to cybersecurity incidents, typically on a 24/7/365 basis" [54].

1) CSIRT: A cybersecurity incident can have serious consequences for businesses, including liability and loss of reputation, customer confidence, and productivity [24]. The evolving nature of the current cyber threat landscape has created the need for not only specialized skills in the prevention of and response to cyber attacks, but also for global cooperation, which can be achieved by CSIRT [24]. The CSIRT is able to effectively and efficiently plan for and respond to cybersecurity issues by working with the infrastructure team, other information technology professionals, end users, management, and other external entities [26]. A CSIRT is capable of enabling the capabilities to detect, analyze, eradicate, and recover from potential cybersecurity incidents in a timely and cost-effective manner, taking into account how organizations need efficiency to deal with uncertainty and to improve their decision-making process during cybersecurity incident response [54]. The creation of a CSIRT in running cybersecurity incident management operation enhance the ability to differentiation benign alerts from true-positive incidents and also make information sharing exercises better coordinated [28].

2) SOC: "When a security incident, data breach, policy violation, or compromise occurs, the first people that are contacted are the security operation center (SOC) of the organization who provide the audacious task of safeguarding, protecting, monitoring, and managing security incidents for the organization" [20]. This suffices that a SOC is where all the administrative and technical capabilities are skillfully leveraged with all the necessary playbooks to manage cybersecurity incidents. Some of the activities that take place in a SOC include the gathering or aggregating of security events from various log sources, correlation of those logs, analysis to determine whether an incident has occurred, and investigation of threats to understand the root cause [20], [55], [56]. Storage and archiving of security logs for potential digital forensic analysis are some of the other key component of a SOC [55].

Based on the review outlined above, our systematic literature review differ from the related studies that we investigated in the following ways:

1) We investigated how organizations are managing cybersecurity incidents from an end-to-end viewpoint.
2) We looked into how organizations are leveraging administrative and technical capabilities to address cybersecurity incident.
3) With respect to incident triage, investigation and resolution, we also investigated how organizations are leveraging CSIRT to enhance efficiency in cybersecurity incident management.
4) Unlike most of the studies we investigated, our systematic literature review ensure inclusion of guidelines from the SANS and NIST frameworks.

III. Methodology

This systematic literature review provides an exploratory investigation and discussion of the current state-of-the-art research on how cybersecurity incidents are being managed by organizations. To accomplish this review, we leveraged the models of the studies conducted by AbuHassan [13] and Kitchenham [62] as guide. The subsequent subsections indicates details of how we carry out this study.

A. Study Strategy

The literature review we conducted is a secondary study because our paper is based on prior primary studies. In order to find the answers we needed to meet our research goal, we found relevant literature and studied it. We conducted an initial review after the Google Scholar search engine turned up over a hundred pieces of literature. The initial review's goal was to comprehend and determine which of them, based on their titles and abstracts, were most pertinent to our study. Given the restricted focus of this study and the Google Scholar search result, we found and chose the eighteen pieces of literature that were reviewed.

B. Research Question

In order to provide answers to our research question, our proposed literature review first identifies pertinent current literature on cybersecurity incident management. The results of the investigations of these primary studies were crucial in helping us to discover answers to our study topic.

C. Study Selection

In order to select the appropriate or relevant studies and to filter out the unrelated or out-of-scope ones, we define the following inclusion and exclusion criteria based on the guidelines found in Kitchenham [62] and AbuHassan [13].

No.	Authors	No. of Author(s)	Research Period	Pages	Main Focus Area (Summarized)	References
1.	Hassanzadeh et al.	5	2020	12	Cybersecurity incidents in the water sector	[19]
2.	Takahashi et al.	3	2010	4	Cybersecurity operational information	[27]
3.	Bradshaw	1	2015	24	Combating cyber threats	[24]
4.	Skiljic	1	2020	11	Cybersecurity and remote working	[57]
5.	Kim et al.	2	2020	22	Cybersecurity breach and crisis response	[58]

TABLE I
OVERVIEW OF LITERATURE CONSULTED IN THIS STUDY (1 - 5)

No.	Authors	No. of Author(s)	Research Period	Pages	Main Focus Area (Summarized)	References
6.	Ioannou et al.	3	2019	4	Cybersecurity Culture in CSIRT	[53]
7.	Catota et al.	3	2018	20	Cybersecurity incident response capabilities	[28]
8.	Sun et al.	6	2018	29	Data-driven cybersecurity incident prediction	[38]
9.	Naseer et al.	3	2021	11	Analytical information processing capability	[54]
10.	Jalali et al.	4	2019	15	Cyber incidents in health care	[59]

TABLE II
OVERVIEW OF LITERATURE CONSULTED IN THIS STUDY (6 - 10)

No.	Authors	No. of Author(s)	Research Period	Pages	Main Focus Area (Summarized)	References
11.	Bajramovic et al.	2	2016	6	Forensic readiness of smart buildings	[60]
12.	Angafor et al.	3	2020	19	Tabletop exercises for cybersecurity incidents	[21]
13.	Takano	1	2014	6	Cybersecurity incident response	[61]
14.	Steinke et al.	9	2015	10	Improving cybersecurity incident response	[26]
15.	Uramova et al.	4	2020	6	Management of Cybersecurity Incidents	[30]

TABLE III
OVERVIEW OF LITERATURE CONSULTED IN THIS STUDY (11 - 15)

No.	Authors	No. of Author(s)	Research Period	Pages	Main Focus Area (Summarized)	References
16.	Naseer et al.	5	2021	10	Incident response process	[14]
17.	Onwubiko et al.	2	2020	21	Cybersecurity incident management	[20]
18.	Kweon et al.	4	2021	13	Security training and education	[29]

TABLE IV
OVERVIEW OF LITERATURE CONSULTED IN THIS STUDY (16 - 18)

1) Inclusion Criteria: Given the enormous population of literature that the Google scholar search result produced, our inclusion criteria are:

- Literature title may contain "Cyber" OR "Cybersecurity".
- Element of the title may contain "Incident" OR "Response".
- Element of the title may combine both "Incident" AND "Response".
- Element of the title may combine both "Cyber" AND "Incident".
- Element of the title may combine both "Cybersecurity" AND "Incident".
- Its theme may be about different components of Cybersecurity Incident Management.
- Must be published article.
- Must be published in English language.
- Published between 2010 and 2022.

2) Exclusion Criteria: The research articles filtered out from the final literature reviewed were excluded based on the following criteria:

- Articles with title that did not include "Incident" OR "Cyber" OR "Cybersecurity" OR "Response".
- Its theme are external to components of Cybersecurity Incident Handling.
- Non-English articles, books and monographs.
- Articles with missing full texts.

3) Search Process: Following the identification of the selected literature from our Google Scholar search results, the final papers were all downloaded from electronic databases. The first author of this paper conducted the searches and identified all the primary studies used in this paper. With reference to Figure 1, the phases of the search is described below:

- Phase 1: While the title of each of the selected primary studies checked using our defined inclusion and exclusion criteria, all the research articles unrelated to our study subject were omitted. All the retrieved references of all the primary articles were documented using the OverLeaf [63] tool.
- Phase 2: In this phase, the first author of this study read the abstract of all the papers identified in phase 1 against the inclusion and exclusion criteria. At this stage, almost 110 articles have been identified.
- Phase 3: All the retrieved articles were carefully read using their full text in alignment with the inclusion and exclusion criteria. At this stage, the number of articles had decreased to 18. This final selection were studied based on their full text before including them into our systematic literature review.

4) Search Scope: Given the capability of Google Scholar as a tool to conduct an online web search for either full texts or metadata of scholarly literature across an array of publishing formats and disciplines [64], [65], we conducted our final search against it, on November 8th 2022 and given the scope of this study, a total population of about 110 literature were identified and reviewed. Below is highlight of how we scoped our search

- Cybersecurity incidents response.

Several combinations of search queries were tried but based on the research question that we attempted to answer, the search query "Cybersecurity incidents response" returned the result that produced the most relevant studies.

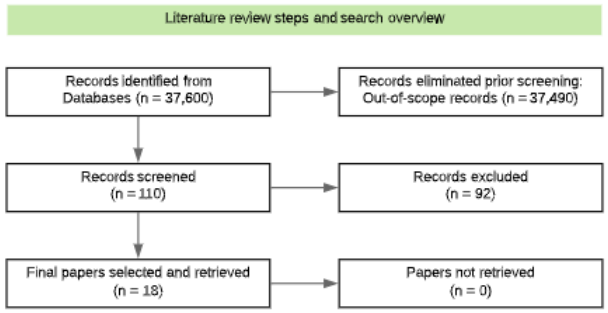

Fig. 1. Review procedure

5) Data Extraction: In order to ensure the validity of the final selection of literature and to be able to obtain answers to our research question (RQ1), data extraction criteria were developed, and field A1 to A10 in table 5 highlight all the questions that we posed to all the eighteen papers covered in our literature review. Extracting data from the themes in the 18 literature we investigated was significantly aided by the questions in Table 5. Field A1, for example, is designed to obtain information where any of the 18 articles briefly or significantly highlight the importance of communication in cybersecurity incident response. Field A2 aims to investigate if articles echo the relevance and importance of information sharing in handling cybersecurity incidents. A3 on the other hand is designed to establish where articles emphasize how training or security educational awareness can be very instrumental to proactively or reactively responding to cybersecurity incidents. Field A4 helps to obtain insights from articles that highlight in any way, shape or form the significance of monitoring and detection in gaining visibility into cybersecurity threats.

A5 on one hand looks at where articles suggests the relevance of analysis of security events or correlation of security logs in the handling of cybersecurity incidents while field A6 on the other hand investigates what article highlights the importance of one of policies or processes or procedures or standards or combination of more than one of them, in cybersecurity incident management. Field A7 looks for themes that echo either the importance of containment or remediation or recovery or combination of more than one of them in the handling of cybersecurity incidents. A8 is designed to obtain information from articles that suggest the importance of any form of automation in the cybersecurity incident handling process. Field A9 helps to look for themes that suggest the importance of CSIRT in how organization combine administrative and technical capabilities in responding to cybersecurity incidents. A10 aims to look for themes or information in articles that emphasize either the importance of security operations or administration of security operation centers, in the management of cybersecurity incidents.

6) Quality Assessment: Subsequent to leveraging the inclusion and exclusion criteria to assess the quality of the initial 110 papers identified and leading to the final 18 literature, the first author thoroughly studied all the final selections to determine relevance to this study. Another method of assessing the quality of the final 18 literature is using our defined data extraction criteria to determine the validity of these papers. Given the limited number of literature in scope for this study, the first author, who was at the time of this study a Ph.D. student in information technology and a practicing Certified Information Systems Security Professional (CISSP), conducted the quality assessment of all the 18 papers selected for the literature review to determine relevance to this study.

IV. Results

Using the data extraction criteria detailed in table 5 and based on the quality assessment, this systematic literature obtained answers that provide quantitative insights into the 18 literature consulted. Answers to questions A1 to A10 are summarized in table 6.

A. Publishing Affiliation of Literature

Subsequent to using the inclusion and exclusion criteria to select the final 18 literature that we conducted our literature review on, figure 3 indicates the distribution of various publishing electronic databases affiliated with the literature.

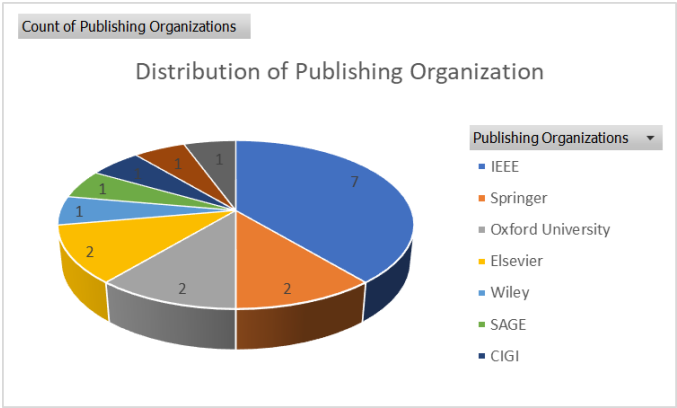

Fig. 2. Literature's Publishers' Distribution

B. Attributes

In this section, we highlight key summary, observation and findings from the quantitative data extracted from all the 18 literature that we investigated for this systematic literature review.

1) Looking at field A1 as indicated in table 6, just 55.56 percent of the literature consulted suggests or highlights the importance of effective communication in the coordination of cybersecurity incident response.
2) From what we observe in field A2, slightly above 60 percent of the 18 articles we investigated, more or less echo the relevance and importance of information sharing (either with internal functional units, external stakeholders, or as applicable) in handling cybersecurity incidents.

Field	Attributes	Description	Associated RQ
A1	Communication	Does the article highlight the importance of communication?	RQ1
A2	Information Sharing	Does the article echo the usefulness of information sharing?	RQ1
A3	Training	Does the article confirm the usefulness of training or security awareness?	RQ1
A4	PPP & SF	Does the article reference the importance of PPP?	RQ1
A5	Monitoring & Detection	Does the article suggest monitoring or detection capabilities as relevant?	RQ1
A6	Analysis & Log Correlation	Does the article highlight importance of analysis or correlation of logs?	RQ1
A7	CRR	Does the article highlight the significance of either containment or remediation, or recovery?	RQ1
A8	Automation	Does the article suggest that leveraging of automation may enhance efficiency?	RQ1
A9	CSIRT	Does the article highlight the relevance of CSIRT in handling of cybersecurity incidents?	RQ1
A10	SOC	Does the article confirm or suggest the relevance of a SOC?	RQ1

TABLE V
EXTRACTION FORM FOR RETRIEVED ARTICLES

Field	Attributes	% of Yes	% of No
	Administrative Capabilities		
A1	Communication	55.56	44.44
A2	Information Sharing	61.11	38.89
A3	Training	77.78	22.22
A4	PPP & SF	94.44	5.56
	Average Score	72.22	27.78
	Technical Capabilities		
A5	Monitoring & Detection	88.89	11.11
A6	Analysis & Log Correlation	72.22	27.78
A7	CRR	44.44	55.56
A8	Automation	38.89	61.11
	Average Score	61.11	38.89
	Hybrid Capabilitiess		
A9	CSIRT	88.89	11.11
A10	SOC	44.44	55.56
	Average Score	66.67	33.34

TABLE VI
QUANTITATIVE SUMMARY OF LITERATURE

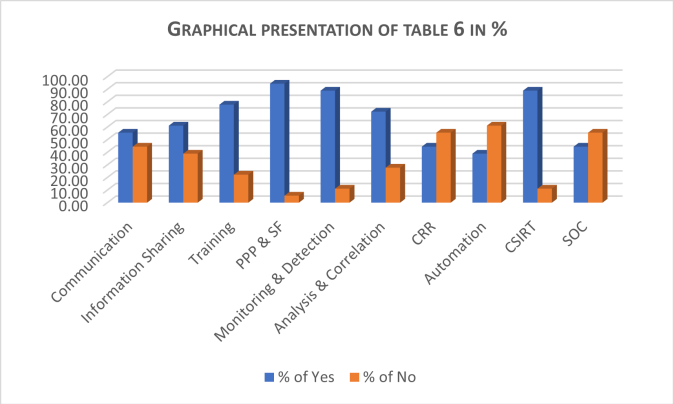

Fig. 3. Chart of Quantitative Analysis of Literature

3) Field A3, on the other hand, indicate that 77.78 percent of the literature looked into, directly or indirectly emphasizing how training or security educational awareness can be very instrumental to proactively or reactively responding to cybersecurity incidents.
4) Almost 95 percent of the 18 literature investigated for the literature review highlights the importance of at least one of the policies, processes, or standards, or a combination of more than one in cybersecurity incident management.
5) In field A5, almost 90 percent of the 18 literature we investigated seems to indicate insights that highlight in some way, shape or form the significance of monitoring and detection in gaining visibility into cybersecurity threats.
6) Over 70 percent of articles looked into (in A6) suggests the relevance of analysis of security events or correlation of security logs in the handling of cybersecurity incidents.
7) Roughly 45 percent of the articles looked into echo themes that suggest either the importance of containment or remediation or recovery or combination of more than one of them in the handling of cybersecurity incidents.
8) In A8, less than 50 percent of these 18 literature either suggests or highlights the importance of any form of automation in enhancing efficiency in cybersecurity incident handling process.
9) From A9, almost 90 percent of all the literature investigated in table 1 to table 4 suggests or echoes the relevance or importance of CSIRT in how organizations combine administrative and technical capabilities to respond to (or manage) cybersecurity incidents.
10) In A10, almost 45 percent of the 18 literature we investigated suggests or emphasize either the importance of security operations or administration of security operation centers (SOC) in the management of cybersecurity incidents.

V. DISCUSSION

In this section and within the context of capabilities that help organizations combat cybersecurity incidents, we looked at results from our systematic literature review to adequately interpret, analyze, and provide explanations for the identified findings. As much as possible, we reviewed our findings in the context of our research questions defined in the early part of the research paper while also observing unexpected results and possible limitations of such results. Most importantly, we leveraged writers' corporate experience when interpreting results to make our output more meaningful and result-oriented with respect to how organizations can develop an adequate defense against cyberattacks.

The analyzed data revealed that certain parameters stand within the three classifications of capabilities (defined as administrative, technical, and hybrid) necessary for a formidable cyber incident management system. Policies, Processes and Procedures and Standard Frameworks (PPP, SF), Monitoring and Detection, and CSIRT are factors that scored the highest points within the three categories of capabilities. But more importantly, in our result, we detected that in terms of average score, the administrative capabilities achieved an outstanding result leading to over 11.11 percentage points above the technical capabilities.

On average, about 70 percent of reviewed literature mentioned that administrative capabilities are appropriate mechanisms for responding to cybersecurity incidents compared to the average performance of 66 percent and 61 percent for hybrid and technical capabilities, respectively. Based on our overall assessment, the PPP SF scored 94 percent, while monitoring and CSIRT scored 88 percent each. At the bottom of the ranking of capabilities for building effective cyber response is the technical capabilities. The lowest factor within the category is automation, which was mentioned by only 39 percent of papers reviewed as a viable capability.

A. Contribution

Although our methodology inculcates an empirical approach to analyze the data derived after investigating the selected literature within the context of different types of contributions as defined by Wobbrock [66], this paper is a survey contribution. This study has been able to derive empirical evidence on the various organizational capabilities and identified those considered necessary for other similar organizations to build a resilient cybersecurity incident response program. With a combined industry experience of over 40 years in risk management, cybersecurity incident response, and governance, the authors of these papers are not surprised with the outcome of this research, which clearly emphasized the need for building adequate administrative capability as a prerequisite for a good cybersecurity incident management system.

VI. Conclusion

Apart from looking at the Significant Incident Report published by the Center for Strategic & International Studies [2], we also extensively cross-reference the Data Breach Incident Reports [15], [16], [17], [18] in order to validate some of the notable security events, from which we drew the introduction of this paper. As we write this conclusion, one surprise in our reviewed literature was the emphasis placed on automation as one of the technical capabilities considered in this study. This factor scored the lowest mark, accepting a 'Yes' of 39 percent among the literature reviewed. This result is ironic considering the huge budget most organizations allocate for automation (as well as other technical capabilities) of security infrastructures on yearly basis [67], [68], [69], [70]. It might be necessary at this stage to ask why organizations allocate significant budgets for technical capabilities that have been proved in this paper to be less potent than administrative factors when building effective cybersecurity defense systems.

Human factors play crucial role in formation of an adequate risk management [71], [72]. Most of the concerns associated with human factors are usually addressed through adequate governance that relies heavily on effective policies, processes, and procedures [73], [74], [75]. This result further emphasizes various works that have proved human factor as a major flaw or weak link that must be continuously emphasized to build a resilient system. Hence the supporting results of 77 percent result for training as one of the key capabilities.

Also looking at the data analyzed in this paper, combining this with our decades of experience in information security, risk management, and governance, we also opined that the results are complementary. One of the major game changers in the security space in the last two decades is the emergence of security automation systems that enable security professionals to simultaneously scan logs of security incidents across infrastructures [76], [77]. These measures are humanly impossible to achieve, and they underpin the importance of security architecture.

We expect technical tools of this nature to continue to play significant roles amid the advent of more sophisticated technology such as Augmented Reality, Virtual Reality, Internet of Things, Blockchain, etc. However, this paper emphasizes the need for emerging technical capabilities to be adequately supported with sufficient administrative tools. Policies, processes, and frameworks must support increased investments in technical security tools. For technology tools to achieve optimal results, risk must be reduced to the bare minimum in organizations. In governance systems, the board of directors, senior management, and staff members of organizations must be equipped with adequate security knowledge through continuous training and development programs.

A. Recommendation

Given the score of 88.89 percent for CSIRT which according to our study suggests the importance of organizations' readiness for combating cybersecurity incidents with key components of CSIRT capabilities, we have identified two of the most popular guidelines i.e. SANS and NIST incident response frameworks [78] that could be leveraged. As indicated in figure 4, both incident response frameworks agree on similar steps required for effective incident response:

No.	NIST Framework	SANS Framework
1	Preparation	Preparation
2	Detection & Analysis	Identification
3	Containment, Eradication & Recovery	Containment
4		Eradication
5		Recovery
6	Post-Incident Activity	Lesson Learned

Fig. 4. Incident Response Steps

The National Institute of Standards and Technology, better known by its abbreviation NIST, is a U.S. government

organization that focuses on all things technological [78], [79], [80]. The Cybersecurity Framework it offers is one of the most well-known approaches to better understanding and managing cybersecurity risk [78], [79], [80]. The NIST Incident Framework, one of the most widely-used incident response standards globally, is a part of the NIST overall framework [78], [79], [80]. SANS, a private organization that conducts research and imparts knowledge to industry in the four primary cyber disciplines, stands for Sysadmin, Audit, Network, and Security but unlike the NIST framework, which has a wider operational scope, the SANS framework primarily focuses on security [78], [79], [80].

Based on the validation that incidents will always occur as we have indicated in the earlier paragraph, the readiness of organizations to conduct triage and or thorough investigation is very important, therefore using the example of a NIST framework, we suggest that organizations should based on the severity of every incident, determine what stages of the NIST framework for incident response is applicable. Figures 5 & 6 are highlights how we believe that this NIST framework should be applied based on the severity of a cybersecurity incident.

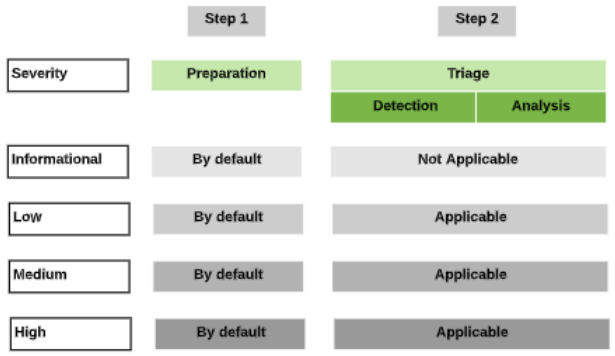

Fig. 5. Application of NIST Steps 1 & 2

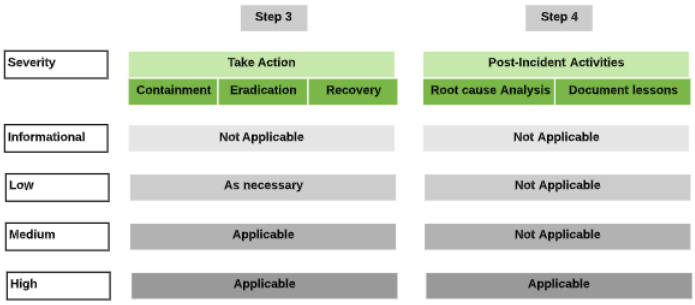

Fig. 6. Application of NIST Steps 3 & 4

VII. Limitation

A. Limited scope of work

We acknowledged the limitation of this study that was reduced to about 18 literature from over 100 initially identified through queries from the Google scholar system. However, the logical steps in filtering the literature have enabled us to come to a reasonable conclusion regarding key capabilities organizations must possess to respond to and treat cybersecurity incidents effectively.

B. Potential Size bias

It is pertinent to state that while primary publications reviewed for purpose of this study provided empirical content on security incidents management, there is no consistent evidence that suggested or provided hints on specific sizes of organizations considered under their research works. While on one hand among OECD countries, Small and medium-sized entities account for 95 percent of businesses - controlling a significant portion of economic activities [81], [82] and they also constitute vast majority of businesses in the United States of America as well [83]; on the other hand, mostly it is big-size organizations that adopt significant technical capabilities such as automation or CSIRT or SOC as part of their security management system due to the huge budget required, besides small-size firms that leverage security-as-a-service to achieve similar fit. Considering the huge population of small and medium-sized firms, it is possible then that empirical inputs from most papers we surveyed could be size-biased and invariably our output could have favored less costly capabilities such as administrative measures (such as policies, frameworks, training etc). Therefore, we assert the possibility that the low score achieved by capabilities such as automation and SOC could result from this size bias.

VIII. Further Study

In response to the size bias mentioned under the limitations section, we also recommend further research to investigate possible roles sizes of organizations could play in determining the appropriate capabilities necessary for building resilient cybersecurity incident response systems. While it appears to be common knowledge that budget plays a crucial role in an organization's choice of capability, cybersecurity systems can be optimized within a given context of the organization's size. The work for further research would therefore need to focus on optimizing appropriate capabilities for a given financial capacity of the firm to eliminate size bias from such a study.

Organisations and their Senior Management team must place emphasis on administrative capacity to strengthen human factors when building an effective cybersecurity system. Also, we are posing additional research questions as an outcome of this paper. We are challenging other researchers further to investigate the justification for huge budgets for technical capabilities when building a cybersecurity response system compared to related budgets for administrative capabilities. Are automated and technical tools such as end-point detection infrastructure addressing human gaps in cybersecurity systems as intended?

Acknowledgment

Appreciation to the School of Information Technology, University of Cincinnati Ohio, for providing us with the tools,

environment and guidance to conduct this study. Thanks for the co-authors of "Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents" [1] for providing the foundation from which this study is conducted.

REFERENCES

[1] O. I. Falowo, S. Popoola, J. Riep, V. Adewopo, and J. Koch, "Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents (december 2022)," *IEEE Access*, pp. 1–1, 2022.

[2] C. for Strategic and I. Studies, "Significant cyber incidents," in *Center for Strategic and International Studies, Significant Cyber Incidents Since 2006*, 2022. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[3] L. Lazarovitz, "Deconstructing the solarwinds breach," *Computer Fraud & Security*, vol. 2021, no. 6, pp. 17–19, 2021.

[4] S. Peisert, B. Schneier, H. Okhravi, F. Massacci, T. Benzel, C. Landwehr, M. Mannan, J. Mirkovic, A. Prakash, and J. B. Michael, "Perspectives on the solarwinds incident," *IEEE Security & Privacy*, vol. 19, no. 2, pp. 7–13, 2021.

[5] G. B. White, G. Dietrich, and T. Goles, "Cyber security exercises: testing an organization's ability to prevent, detect, and respond to cyber security events," in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. IEEE, 2004, pp. 10–pp.

[6] R. Van der Kleij, G. Kleinhuis, and H. Young, "Computer security incident response team effectiveness: A needs assessment," *Frontiers in psychology*, vol. 8, p. 2179, 2017.

[7] T. R. Chen, D. B. Shore, S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, and A. K. Gorab, "An organizational psychology perspective to examining computer security incident response teams," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 61–67, 2014.

[8] R. R. Perols and U. S. Murthy, "The impact of cybersecurity risk management examinations and cybersecurity incidents on investor perceptions and decisions," *Auditing: A Journal of Practice & Theory*, vol. 40, no. 1, pp. 73–89, 2021.

[9] M. Plachkinova and C. Maurer, "Security breach at target," *Journal of Information Systems Education*, vol. 29, no. 1, pp. 11–20, 2018.

[10] J. Pescatore, "Cyber security trends: Aiming ahead of the target to increase security in 2017," *SANS Institute InfoSec Reading Room*, 2017.

[11] N. Manworren, J. Letwat, and O. Daily, "Why you should care about the target data breach," *Business Horizons*, vol. 59, no. 3, pp. 257–266, 2016.

[12] C. Kenny, "The equifax data breach and the resulting legal recourse," *Brook. J. Corp. Fin. & Com. L.*, vol. 13, p. 215, 2018.

[13] A. AbuHassan, M. Alshayeb, and L. Ghouti, "Software smell detection techniques: A systematic literature review," *Journal of Software: Evolution and Process*, vol. 33, no. 3, p. e2320, 2021.

[14] A. Naseer, H. Naseer, A. Ahmad, S. B. Maynard, and A. M. Siddiqui, "Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis," *International Journal of Information Management*, vol. 59, p. 102334, 2021.

[15] W. Baker, M. Goudie, A. Hutton, C. D. Hylender, J. Niemantsverdriet, C. Novak, D. Ostertag, C. Porter, M. Rosen, B. Sartin *et al.*, "2011 data breach investigations report," *Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigationsreport-2011_en_xg. pdf*, pp. 1–72, 2011.

[16] V. R. Team, "2015 data breach investigations report," 2015.

[17] M. Jartelius, "The 2020 data breach investigations report–a cso's perspective," *Network Security*, vol. 2020, no. 7, pp. 9–12, 2020.

[18] P. Langlois, "2020 data breach investigations report," 2020.

[19] A. Hassanzadeh, A. Rasekh, S. Galelli, M. Aghashahi, R. Taormina, A. Ostfeld, and K. Banks, "A review of cybersecurity incidents in the water sector," *arXiv preprint arXiv:2001.11144*, 2020.

[20] C. Onwubiko and K. Ouazzane, "Soter: A playbook for cybersecurity incident management," *IEEE Transactions on Engineering Management*, 2020.

[21] G. N. Angafor, I. Yevseyeva, and Y. He, "Game-based learning: A review of tabletop exercises for cybersecurity incident response training," *Security and privacy*, vol. 3, no. 6, p. e126, 2020.

[22] P. Wang and C. Johnson, "Cybersecurity incident handling: a case study of the equifax data breach." *Issues in Information Systems*, vol. 19, no. 3, 2018.

[23] S. Barman, *Writing information security policies*. New Riders Indianapolis, IN;, 2002.

[24] S. Bradshaw, "Combating cyber threats: Csirts and fostering international cooperation on cybersecurity," *Global Commission on Internet Governance Paper Series, Paper*, no. 23, 2015.

[25] M. Malatji, A. L. Marnewick, and S. von Solms, "Cybersecurity policy and the legislative context of the water and wastewater sector in south africa," *Sustainability*, vol. 13, no. 1, p. 291, 2020.

[26] J. Steinke, B. Bolunmez, L. Fletcher, V. Wang, A. J. Tomassetti, K. M. Repchick, S. J. Zaccaro, R. S. Dalal, and L. E. Tetrick, "Improving cybersecurity incident response team effectiveness using teams-based research," *IEEE Security & Privacy*, vol. 13, no. 4, pp. 20–29, 2015.

[27] T. Takahashi, H. Fujiwara, and Y. Kadobayashi, "Building ontology of cybersecurity operational information," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 2010, pp. 1–4.

[28] F. E. Catota, M. G. Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the ecuadorian financial sector," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy002, 2018.

[29] E. Kweon, H. Lee, S. Chai, and K. Yoo, "The utility of information security training and education on cybersecurity incidents: an empirical evidence," *Information Systems Frontiers*, vol. 23, no. 2, pp. 361–373, 2021.

[30] J. Uramová, P. Segeč, J. Papán, and I. Brídová, "Management of cybersecurity incidents in virtual lab," in *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*. IEEE, 2020, pp. 724–729.

[31] A. Ahmad, S. B. Maynard, and G. Shanks, "A case analysis of information systems and security incident responses," *International Journal of Information Management*, vol. 35, no. 6, pp. 717–723, 2015.

[32] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams–challenges in supporting the organisational security function," *Computers & Security*, vol. 31, no. 5, pp. 643–652, 2012.

[33] C. Hove, M. Tårnes, M. B. Line, and K. Bernsmed, "Information security incident management: identified practice in large organizations," in *2014 Eighth international conference on IT security incident management & IT forensics*. IEEE, 2014, pp. 27–46.

[34] P. Cichonski, T. Millar, T. Grance, K. Scarfone *et al.*, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, no. 61, pp. 1–147, 2012.

[35] P. Kral, "The incident handlers handbook," *SANS Institute*, 2011.

[36] R. F. Rights, "Sans institute infosec reading room," *GIAC*, 2003.

[37] A. Torres, "Incident response: How to fight back," *SANS Institute, August*, 2014.

[38] N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang, and Y. Xiang, "Data-driven cybersecurity incident prediction: A survey," *IEEE communications surveys & tutorials*, vol. 21, no. 2, pp. 1744–1772, 2018.

[39] N. Miloslavskaya, "Security operations centers for information security incident management," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, 2016, pp. 131–136.

[40] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl, "Computer security incident response team development and evolution," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 16–26, 2014.

[41] P. H. Meland, I. A. Tondel, and B. Solhaug, "Mitigating risk with cyberinsurance," *IEEE Security & Privacy*, vol. 13, no. 6, pp. 38–43, 2015.

[42] S. G. Batsell, N. S. Rao, and M. Shankar, "Distributed intrusion detection and attack containment for organizational cyber security," *Cyber and Information Security Research*, 2005.

[43] J. Babcock, J. Kramár, and R. V. Yampolskiy, "Guidelines for artificial intelligence containment," *Next-Generation Ethics: Engineering a Better Society (Ed.) Ali. E. Abbas*, pp. 90–112, 2019.

[44] M. T. Khorshed, A. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," *Future Generation computer systems*, vol. 28, no. 6, pp. 833–851, 2012.

[45] J. Wynn, J. Whitmore, G. Upton, L. Spriggs, D. McKinnon, R. McInnes, R. Graubart, and L. Clausen, "Threat assessment & remediation analysis (tara): methodology description version 1.0," MITRE CORP BEDFORD MA, Tech. Rep., 2011.

[46] S. Chandel, S. Yu, T. Yitian, Z. Zhili, and H. Yusheng, "Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat," in *2019 international conference on*

cyber-enabled distributed computing and knowledge discovery (cyberc). IEEE, 2019, pp. 81–89.
[47] E. C. Thompson, *Cybersecurity incident response: How to contain, eradicate, and recover from incidents*. Apress, 2018.
[48] M. A. Lopez, J. M. Lombardo, M. López, C. M. Alba, S. Velasco, M. A. Braojos, and M. Fuentes-García, "Intelligent detection and recovery from cyberattacks for small and medium-sized enterprises," 2020.
[49] P. Kampanakis, "Security automation and threat information-sharing options," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 42–51, 2014.
[50] A. Moser and M. I. Cohen, "Hunting in the enterprise: Forensic triage and incident response," *Digital Investigation*, vol. 10, no. 2, pp. 89–98, 2013.
[51] K. G. Zografos, K. N. Androutsopoulos, and G. M. Vasilakis, "A real-time decision support system for roadway network incident response logistics," *Transportation Research Part C: Emerging Technologies*, vol. 10, no. 1, pp. 1–18, 2002.
[52] R. Trifonov, R. Yoshinov, S. Manolov, G. Tsochev, and G. Pavlova, "Artificial intelligence methods suitable for incident handling automation," in *MATEC Web of Conferences*, vol. 292. EDP Sciences, 2019, p. 01044.
[53] M. Ioannou, E. Stavrou, and M. Bada, "Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination," in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 2019, pp. 1–4.
[54] H. Naseer, S. B. Maynard, and K. C. Desouza, "Demystifying analytical information processing capability: The case of cybersecurity incident response," *Decision Support Systems*, vol. 143, p. 113476, 2021.
[55] A. Madani, S. Rezayi, and H. Gharaee, "Log management comprehensive architecture in security operation center (soc)," in *2011 International Conference on Computational Aspects of Social Networks (CASoN)*. IEEE, 2011, pp. 284–289.
[56] R. Bidou, "Security operation center concepts & implementation," *avalable at http://www. iv2-technologies. com*, 2005.
[57] A. Škiljić, "Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats," *International Cybersecurity Law Review*, vol. 1, no. 1, pp. 51–61, 2020.
[58] N. Kim and S. Lee, "Cybersecurity breach and crisis response: An analysis of organizations' official statements in the united states and south korea," *International Journal of Business Communication*, vol. 58, no. 4, pp. 560–581, 2021.
[59] M. S. Jalali, B. Russell, S. Razak, and W. J. Gordon, "Ears to cyber incidents in health care," *Journal of the American Medical Informatics Association*, vol. 26, no. 1, pp. 81–90, 2019.
[60] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests," in *2016 IEEE International Smart Cities Conference (ISC2)*. IEEE, 2016, pp. 1–6.
[61] M. Takano, "Ics cybersecurity incident response and the troubleshooting process," in *2014 Proceedings of the SICE Annual Conference (SICE)*. IEEE, 2014, pp. 827–832.
[62] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and software technology*, vol. 51, no. 1, pp. 7–15, 2009.
[63] A. B. Pacheco, "Creating documents with latex and overleaf."
[64] P. Jacsó, "Google scholar: the pros and the cons," *Online information review*, 2005.
[65] P. Mayr and A.-K. Walter, "An exploratory study of google scholar," *Online information review*, 2007.
[66] J. O. Wobbrock, "Seven research contributions in hci," *studies*, vol. 1, no. 1, pp. 52–80, 2012.
[67] T. Moore, S. Dynes, and F. R. Chang, "Identifying how firms manage cybersecurity investment," *Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14)*, vol. 32, 2015.
[68] I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," *Business Horizons*, vol. 64, no. 5, pp. 659–671, 2021.
[69] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision support systems*, vol. 86, pp. 13–23, 2016.
[70] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, "Increasing cybersecurity investments in private sector firms," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 3–17, 2015.
[71] B. E. Biringer, R. V. Matalucci, and S. L. O'Connor, *Security Risk Assessment and Management: A professional practice guide for protecting buildings and infrastructures*. John Wiley & Sons, 2007.
[72] D. Landoll, *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press, 2021.
[73] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of information systems*, vol. 18, no. 2, pp. 106–125, 2009.
[74] Q. Hu, Z. Xu, T. Dinev, and H. Ling, "Does deterrence work in reducing information security policy abuse by employees?" *Communications of the ACM*, vol. 54, no. 6, pp. 54–60, 2011.
[75] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of is security policy in organizations: An integrated model based on social control and deterrence theory," *Computers & Security*, vol. 39, pp. 447–459, 2013.
[76] M. Lehto and P. Neittaanmäki, *Cyber security: Analytics, technology and automation*. Springer, 2015, vol. 78.
[77] S. M. Mohammad and L. Surya, "Security automation in information technology," *INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)–Volume*, vol. 6, 2018.
[78] P. Shedden, A. Ahmad, and A. Ruighaver, "Organisational learning and incident response: promoting effective learning through the incident response process," 2010.
[79] R. Andrade, J. Torres, and S. Cadena, "Cognitive security for incident management process," in *International Conference on Information Technology & Systems*. Springer, 2019, pp. 612–621.
[80] N. Shinde and P. Kulkarni, "Cyber incident response and planning: a flexible approach," *Computer Fraud & Security*, vol. 2021, no. 1, pp. 14–19, 2021.
[81] E. Bartelsman, S. Scarpetta, and F. Schivardi, "Comparative analysis of firm demographics and survival: evidence from micro-level sources in oecd countries," *Industrial and corporate change*, vol. 14, no. 3, pp. 365–391, 2005.
[82] M. A. Carree and A. R. Thurik, "The lag structure of the impact of business ownership on economic performance in oecd countries," *Small business economics*, vol. 30, no. 1, pp. 101–110, 2008.
[83] B. Headd and B. Kirchhoff, "The growth, decline and survival of small businesses: An exploratory study of life cycles," *Journal of Small Business Management*, vol. 47, no. 4, pp. 531–550, 2009.