Borneo International Journal eISSN 2636-9826; Vol. 7 (2); 2024; 69-76
Published by *Majmuah Enterprise*
www.majmuah.com

Incident Response Planning and Procedures

NUR AQILAH ZAFFAN FAROK, MOHAMAD FADLI ZOLKIPLI

School of Computing, Universiti Utara Malaysia
06010 Sintok Kedah, MALAYSIA
Email: aqilahfarok@gmail.com | m.fadli.zolkipli@uum.edu.my

Received: June 07, 2024
Accepted: June 20, 2024
Online Published: June 25, 2024

Abstract

This finding examines the implementation of incident response planning and procedures in internet security, focusing on their effectiveness in tone down cyber threats. The research investigates the role of practice directions in guiding incident response processes, from threat detection to recovery. Data were collected from primary sources including industry standards, incident reports and secondary sources such as scholarly articles and books. The findings indicate that practice directions serve as essential guidelines for incident response teams, aiding in the efficient handling of security incidents. However, further analysis reveals areas where improvements are needed to address emerging challenges, particularly in legal and administrative domains. This study highlights the importance of continuously refining incident response strategies to sustain organizational resistance against evolving cyber threats.

Keywords: Incident Response; Internet Security; Practice Directions; Cyber Threats; Resistance Strategies.

1. Introduction

Computer security incident response has occurred as a essential element within information technology (IT) initiatives. With the proliferation of cybersecurity threats, attacks have not only increased in frequency and variety but also in their detrimental impact and disruptive potential. The landscape continually introduces novel forms of security incidents. While preventive measures informed by risk assessments can mitigate certain incidents, they cannot prevent all threats. (Cichonski et al., 2012). Hence, the establishment of an incident response capability becomes imperative for promptly identifying incidents, curtailing losses and damages, addressing exploited vulnerabilities, and reinstating IT services. The global nature of the internet has transformed how individuals and organizations communicate, collaborate, and conduct business. Given that almost one billion computing systems worldwide are connected to the internet, along merging of mobile telephony services and e-commerce, huge amounts of information flow from one network to another with a single command, request or click (Mitropoulos et al., 2006). However, this digital interconnectedness has also introduced exceptional vulnerabilities, making cybersecurity a vital concern. In an era showed by advanced cyber threats and persistent malicious actors, the capability to effectively counter to security incidents has develop necessary for organizational survival and continuity.

Cyber incidents, including data breaches, malware infections and denial-of-service attacks, threaten confidentiality, integrity, and availability of digital assets. These incidents lead to not only financial losses but also reputational harm, legal repercussions, and regulatory violations (Cremer et al., 2022). Moreover, the increase of communicated devices on Internet of Things (IoT) landscape, incident appear gradually to grow, amplifying the potential impact of security breaches. Given these evolving threats, organizations need to adopt a proactive stance on cybersecurity, emphasizing the significance of incident response planning and preparedness. Incident response involves one systematic approach to identifying, assessing, and mitigating security incidents to reduce their effect and quickly rebuild normal procedures. An effective incident response capability not only lowers the likelihood and severity of security breaches but also strengthens an organization's resilience against adversity. This paper aims to arrange a complete outline of incident response planning and procedures in internet security, offering practical guidance for organizations to develop and implement strong incident response frameworks. By examining the key stages of incident response, from preparation, detection to containment, eradication, and recovery, this paper reveals essential components of an effective incident response strategy. Drawing upon established principles, industry standards, and real-world case studies, we delineate actionable steps for organizations to sustain their cyber resilience and safeguard against emerging threats. Through proactive incident response planning and thorough execution of response procedures, organizations can reduce risks, minimize potential damages, and maintain trust in the digital ecosystem.

2. Literature Review

The history of incident response planning and procedures can be traced back to the early days of computing when the concept of cybersecurity began to arise. In the 1970s and 1980s, as computer networks became more established, organizations started to recognize the need for measures to protect their digital assets from unauthorized access and malicious activities (Pande,2017).One of the earliest frameworks for incident response can be seen in the development of Computer Security Incident Handling Guides by organizations like the United States Department of Defense (DoD) and the Computer Emergency Response Team (CERT). These guides offered guidelines and procedures for responding to security incidents, establishing basis contemporary incident response practices. During 1990s, with the rapid expansion of the internet and the increasing complexity of cyber threats, the need for formalized incident response processes became even more obvious Organizations began to establish dedicated teams and procedures for handling security incidents, often drawing inspiration from existing frameworks and best practices. At 1990s and early 2000s saw a particular emergence about formalized incident response frameworks such as the National Incident Management System (NIMS) and the Incident Command System (ICS), initially developed for managing emergency response efforts but later adapted for cybersecurity incident response (White & Sjelin,2022). As cyber threats continued to evolve, incident response frameworks and methodologies also evolved to keep pace. The publication of formative works such as the "Handbook for Computer Security Incident Response Teams (CSIRTs)" through Forum of Incident Response which allow CSIRT to preserve truthfulness toward the internet's network place at the local and international level (Tanczer et al., 2018). Alao Security Teams (FIRST) in 2003 provided further guidance and best practices for incident response teams (FIRST History, n.d.). In recent years, the rise of advanced persistent threats (APTs), ransomware attacks, and other advanced cyber threats has emphasized the importance of proactive and coordinated incident response efforts. Organizations have increasingly focused on developing mature incident response capabilities, including the implementation of automation and orchestration tools, threat intelligence sharing initiatives, and cross-sector collaboration efforts.

Today, incident response planning and procedures are essential components of cybersecurity programs in organizations across industries. With the growing recognition of cybersecurity as a business-critical function, incident response continues to grow, driven by ongoing advancements in technology, changes in the threat landscape, and lessons learned from past incidents

3. Security Incident Response Process

An incident response plan serves as the documented set of guidelines detailing an organization's actions in response to various security incidents, including data breaches, leaks, cyber-attacks, and similar events. These procedures are made to prepare for potential security breaches and establish protocols for recovery, the absence of such a plan can leave organizations vulnerable, potentially leading to failure in detecting attacks or responding effectively to contain, mitigate, and prevent them (Thompson, 2018). Incident response planning is crucial for understanding the impact along with interval of security incidents, distinguishing collaborator, optimizing digital forensics, enhancing time out, mitigating damaging press, including maintaining consumer trust. A robust incident response framework helps organizations address vulnerabilities, minimize losses, restore affected systems, and block further attacks. It includes preparedness for both known and emerging cyber threats, accurate identification of root causes, and effective recovery strategies. Additionally, it supports the establishment of best practices for incident handling and the creation of communication plans, including notifications to law enforcement, employees, and stakeholders.

Incident response is a critical component of modern cybersecurity practices, enabling organizations to effectively identify, mitigate, also recover from security incidents. This process is typically broken down into six distinct phases, each with its own set of actions and considerations. The first phase, preparation, lays the base for effective incident response by establishing comprehensive incident response plans, training personnel, and receiving necessary tools and resources. Regular exercises and practices are conducted to ensure readiness and familiarity with response procedures. The detection phase presents a significant challenge, particularly in large organizations where the volume of daily events can be overwhelming. Analysts must examine through a multitude of data points, distinguishing between real activities and potential indicators of malicious behavior. Advanced security controls and monitoring systems play a crucial role in identifying suspicious activities, helping to prioritize response efforts. Once an incident is detected, the analysis phase begins, involving the collection and examination of evidence starting with several resources like log files, network connections, as well as running processes. This phase can be time-consuming, depending on the complexity of the incident, as analysts attempt to comprehend the bounds, influence, and root cause of the incident. Specialized tools and techniques are used to reconstruct the attacker's behavior along with evaluate the range about the harm.

Containment is the next critical step, aimed at limiting the spread of the incident and preventing further compromise of network resources. Containment strategies vary depending on the nature of the incident but might involve separating affected systems, blocking malicious communications, either implementing temporary security measures. Quick and decisive action are vital to reduce the potential effect on business operations. Following containment, organizations focus on eradication and recovery, removing the threat actor from the network and fixing impacted systems into secure condition. This may involve running advanced malware scans, applying security patches, or restoring data from backups. Recovery efforts are closely aligned with business continuity and disaster recovery plans, ensuring minimal disruption to critical services. Post-incident activities involve a comprehensive examine regarding incident response process, including the investigation of what worked well also areas for improvement. Detailed documentation is essential to capture the sequence of events, actions taken, and lessons learned. Stakeholders from across the organization participate in questionings to obtain understandings into the incident response procedure as well as identify opportunities toward enhancement.

Ultimately, the aim of incident response upon strengthens the organization's resilience to cyber threats, enabling it acknowledge effectively to incidents and reduce their impact. Integration of lessons learned from each incident into future response processes is crucial for continual improvement and adaptation to evolving threats. By investing in tough incident response capabilities, organizations can enhance their overall security posture and safeguard against potential cyber threats.

3.1. Framework of Incident Response Process

The field of incident response has been significantly shaped by two industry standard framework which is, the NIST Incident Response Process and the SANS Incident Response Process, there are 27 SANS policy templates organise around the NIST Cybersecurity Framework (Dimitrov et al., 2021). These frameworks provide structured methodologies for managing and responding to cybersecurity incidents effectively.

1. NIST Incident Response Process:

1. Preparation: This stage engages determining and supporting an incident response capacity. Activities involve creating an incident response policy, establishing an emergency response team, also offering training and resources directed toward preparedness.

2. Detection and Analysis: Corporations emphasis on detecting plus understanding incidents as they occur. This involves monitoring systems, analysing alerts, and determining the characteristics and possibility of incidents.

3. Containment, Eradication, and Recovery: Once an incident is detected and analysed, step ahead is to control the threat to block other destruction, eradicate the root cause, also rebuild affected systems toward usual operations. This phase might include steps such as isolating involved systems, removing malware, and restoring data from backups.

4. Post-Incident Activity: The final phase includes reviewing and analysing the incident to understand what happened and how it was handled. Lessons learned are used to improve the incident response process and strengthen the organization's defences.

2.SANS Incident Response Process:

1. Preparation: Similar to the NIST framework, this stage involves preparing for incident response by developing policies, procedures, and resources, and conducting training and exercises.

2. Identification: This stage focuses on identifying potential security incidents through monitoring, alerting, and initial analysis. It is crucial to quickly and accurately recognize incidents to minimize impact.

3. Containment: Once an incident is identified, containment strategies are employed to limit the spread of the threat. This can be immediate (short-term containment) or more strategic (long-term containment).

4. Eradication: After containment, efforts shift to eradicating the underlying cause of the incident, such as removing malware and closing vulnerabilities.

5. Recovery: This stage involves restoring and validating system functionality and returning to normal operations. It includes steps to ensure systems are clean and secure before bringing them back online.

6. Lessons Learned: Post-incident analysis is aimed to gather insights and improve future incident response efforts. This involves documenting the incident, reviewing the response, and updating policies and procedures.

3.2. Incident Classification

Incident classification is a crucial aspect of any tough incident response framework, presenting the severity of an event and guiding the appropriate level of response. Recognizing that not all incidents carry equal weight in their potential impact, organizations institute classification schemes to detect between minor disruptions and critical threats to their operations and integrity (Mell et al.,2005). This stratification ensures that resources, particularly those of Computer Security Incident Response Teams (CSIRT), are allocated thoughtfully, preventing exhaustion and optimizing efficiency. A typical classification schema encompasses three tiers: high-level incidents, moderate-level incidents, and low-level incidents, each with distinct characteristics and response criteria. High-level incidents represent the gravest threats, encompassing scenarios such as network intrusions, compromises of critical information, or widespread malware infections. These events have the potential to inflict significant damage, compromise sensitive data, and ruin the organization's reputation, warranting immediate and intensive intervention. Moderate-level incidents, while less severe, still present notable risks, including anticipated or ongoing Denial of Service (DoS) attacks, instances of unauthorized access, or isolated malware infections. Though not as acute as high-level incidents, they demand immediate remediation to mitigate potential harm and safeguard operational continuity.

Conversely, low-level incidents indicate minor disruptions or inadvertent breaches that cause inconvenience without substantial impact, such as policy violations, lost or stolen devices, or isolated malware infections. While not insignificant, these incidents can typically be addressed with routine procedures and minimal disruption to business operations. Effective incident tracking is integral to the response process, ensuring comprehensive documentation of actions taken and facilitating post-incident analysis and improvement. While smaller organizations may suffice with existing IT ticketing systems for incident tracking, larger entities with frequent incidents benefit from purpose-designed tracking systems that offer specialized features personalised to incident response activities (Bramhe,2023). By implementing a well-defined classification scheme and strong tracking mechanisms, organizations can enhance their incident response capabilities, improve resilience against threats, and safeguard critical assets and operations.

4. Best Practices Incident Response

Cybersecurity incidents typically follow a defined lifecycle, and organizations with advanced incident response capabilities will have measures in place to handle incidents at each stage effectively (Killcrece et al., 2003).The process starts when the corporation first detects an sequence of occurrences indicating malicious activity. This initial detection can come from a security control alert or an external notification about a potential security issue. Upon receiving an alert, the organization moves on to analyzing the incident, implementing containment measures, and finally restoring the information system to normal operations. Creating an effective incident response plan is a critical step in establishing a healthy organizational response capability. This high-level document serves as the foundation of the Computer Security Incident Response Team (CSIRT), providing a structured framework for incident handling and coordination. Key components of the incident response plan involve various aspects crucial for efficient and coordinated response efforts. First and foremost, the incident response plan includes elements from the incident response charter, ensuring continuity between the mission statement and constituency outlined within. This alignment reinforces the key objectives of the CSIRT and its commitment to serving the organization's needs effectively. Additionally, the plan includes an expanded services catalogue, detailing specific offerings such as forensic services with comprehensive descriptions of the services rendered. This clarity enables precise differentiation between routine requests and incident-related activities, updating resource allocation and prioritization.

Central to the incident response plan are allocated roles and responsibilities of CSIRT personnel, ensuring clear understanding and accountability during incident response. By defining roles beyond ordinary titles, potential conflicts are eased, fostering collaboration and efficiency within the team. Moreover, the plan incorporates an up-to-date contact list, essential for facilitating sudden communication and coordination, particularly in 24-hour response scenarios. Rotating on-call arrangements further support responsiveness and availability. Internal communication guidance forms a critical component of the plan, addressing the flow of information between senior leadership, the CSIRT, and support personnel. By restructuring communication channels and clarifying reporting structures, chaos during incidents is minimized, enabling focused and effective response efforts. Training requirements are also outlined within the plan, requiring the frequency of exercises and tabletop simulations to enhance preparation and skill preservation. These exercises serve as invaluable opportunities for team members to refine their incident response capabilities and address any identified gaps promptly.

Finally, the plan addresses the need for ongoing maintenance and updates to adapt to evolving organizational dynamics, infrastructure changes, and emerging threats. Regular reviews ensure that the incident response plan remains current and aligned with organizational objectives, incorporating lessons learned from exercises and real-world incidents. Individual team members are encouraged to supplement their skills through training and certification programs, further enhancing the CSIRT's capabilities and resilience. In summary, the incident response plan serves as a comprehensive guide for organizational incident handling, representing a commitment to proactive preparedness, clear communication, and continual improvement. By following its structured framework and embracing a culture of preparedness, organizations can effectively less severe the effect of security incidents along with safeguard their significant resources and operations.

4.1. The Benefits of a Well-Crafted Incident Response Plan

A well-designed incident response plan offers significant advantages for successful cybersecurity management and organizational resilience. Firstly, such a plan assists faster incident response by offering a structured foundation to identifying, assessing, as well as mitigating security incidents (Kirvan, 2024). By leveraging risk assessment data and predefined response protocols, organizations can quickly recognize early indicators of potential threats and validate appropriate containment and recovery measures, thereby minimizing the impact of security breaches. Moreover, a well-organised incident response team with a comprehensive plan can accelerate forensic investigations, leading to shorter incident durations and reduced recovery times. Furthermore, a well-implemented incident response plan serves as a proactive measure to ease the potential effects of unplanned events, thereby preventing the need for invoking more complex and costly business continuity (BC) and disaster recovery (DR) plans (Nollau, 2009). By addressing incidents immediately and effectively, organizations can ease operational disruptions and financial losses, enhancing overall business continuity. Indeed, incident response planning is recognized as a fundamental component of comprehensive BC management processes by leading industry bodies such as the Business Continuity Institute and Disaster Recovery Institute International. Effective interaction is another key benefit facilitated by a well-crafted incident response plan. When an incident’s severity surpasses the incident response team’s capabilities, additional action are required, timely communication with emergency management teams and first responder organizations becomes essential. By spreading critical information promptly, incident response teams enable coordinated efforts to resolve incidents efficiently, minimizing potential damages and ensuring the safety of personnel and assets.

Moreover, regulatory compliance considerations emphasize the importance of having a effective incident response plan in order. Many regulatory frameworks and certification bodies require the implementation of incident response measures as part of broader compliance requirements. Adhering to standards such as the Payment Card Industry Data Security Standard (PCI DSS) necessitates the development of comprehensive incident response capabilities to effectively address security breaches and safeguard sensitive data. In essence, a detailed incident response plan not only improves the corporation's skill to reply swiftly and productively to security incidents but also contributes to proactive risk management, regulatory compliance, and overall business resilience. By employing effective incident response strategies, organizations can lessen the effect of security gaps, safeguard essential assets and preserve stakeholder trust in an progressively dynamic threat environment.

5. Case Studies and Real-World Examples

Incident response planning and procedures are crucial in protecting corporations from cyber threats and reducing the effect of security incidents. Via investigative report as well as real-world examples, insights can be gleaned into the practical application of incident response frameworks, highlighting the importance of proactive planning, instant action, and continuous improvement in mitigating cyber risks. One significant example is the 2017 Equifax data leakage, where confidentiality information of 147 million consumers come to term due to a shortcoming in the organization's incident response procedures. The breach occurred because of an unattended sensitivity in the Apache Struts web application framework, which Equifax failed to address despite receiving a security update two months prior to the attack (Fruhlinger, 2023). The company's response was stained by delays in detecting the intrusion, ineffective communication with affected stakeholders, and a lack of coordination among internal teams. Equifax eventually fixed up its cybersecurity practices, implementing stricter patch management protocols, enhancing network monitoring capabilities, and improving incident response training for its employees. The breach had severe consequences, including a $700 million settlement with the Federal Trade Commission, significant reputational damage, and increased regulatory scrutiny. This incident points out the criticality of timely detection, effective containment, and transparent communication in reducing the aftermath of security incidents.

Conversely, the incident response efforts of Target Corporation following a massive data breach in 2013 serve as a powerful example of effective incident response planning and execution. Target identified uncommon network activity

indicating malware that had infiltered point-of- sale systems, stolen credit and debit card information of around 40 million customers (Jones,2022). The company's response involved a coordinated effort between internal security teams, law enforcement agencies, and third-party forensic experts. By instantly containing the breach, deactivating the malware, and enhancing network security measures, Target was able to mitigate the immediate threat. The company responded clearly with involved customers, providing free credit monitoring and identity theft protection services. Despite the significant financial impact, including over $200 million in expenses and legal settlements, Target's proactive and transparent response helped restore customer trust and highlighted the importance of rapid containment and comprehensive remediation in incident response (Shu et al., 2017).

In another notable example, the WannaCry ransomware attack of 2017 wreaked havoc on organizations worldwide, exploiting a vulnerability in Microsoft Windows to encrypt data and disrupt operations. The ransomware spread rapidly, affecting over 200,000 computers across 150 countries (Lessing, 2017). Organizations with forceful incident response plans and procedures were better equipped to respond to the attack. For instance, the UK's National Health Service (NHS) faced significant disruptions, but some trusts managed to tackle the damage by quickly identifying affected systems, isolating infected endpoints, and restoring data from backups (Antony et al., 2023). The global impact included estimated damages of up to $4 billion, but the response efforts highlighted the importance of timely patch management, regular data backups, and effective incident response planning. Organizations that leveraged threat intelligence, implemented security patches, and distributed timely guidance to employees were able to minimize the impact and resume normal operations more rapidly.

Furthermore, the incident response efforts of financial institutions such as JPMorgan Chase following cyber-attacks highlight the significance based on collaboration, interact, also industry-wide align over responding to complex threats. In 2014, JPMorgan Chase faced a data leakage that exposed information from 76 million households and 7 million small businesses (Weiss & Miller, 2015). The breach was detected through abnormal network activity, prompting the bank to organize its incident response team. JPMorgan Chase worked closely with law enforcement and cybersecurity firms to contain the breach, boost its network defenses, and enhance its threat detection capabilities. The bank also invested in upgrading its cybersecurity infrastructure, including the implementation of multi-factor authentication and advanced encryption technologies. The breach's impact was mitigated by the bank's immediate response and following security enhancements, reinforcing the value of proactive incident response planning and industry collaboration in managing and mitigating cyber threats. In conclusion, examples given offer valuable lesson on the encounters as well as effective approach for incident response planning and procedures. By learning from past incidents, organizations can enhance their incident response capabilities and reduce the impact of security breaches, and safeguard critical assets and operations against evolving cyber threats. Effective incident response not only addresses the immediate threat but also sets the foundation for continuous improvement and resilience in the face of future cyber challenges.

6. Conclusion

This study highlights the critical role of incident response planning and procedures in enhancing internet security and justifying cyber threats. By examining the implementation and effectiveness of incident response frameworks, it becomes evident that well-structured practice directions are vital for guiding incident response teams through the various stages of handling security incidents. These stages include preparation, detection, analysis, containment, eradication, recovery, and post-incident review, all of which are essential for minimizing the consequences of cyber-attacks plus restoring routine as usual. The research highlights the necessity for organizations to adopt comprehensive incident response strategies that are continually filtered to address initial challenges. This includes the integration of legal and administrative measures to ensure fulfilment with guiding requirements and the alignment of incident response activities with broader organizational goals. The study’s findings also emphasize the importance of training and equipping incident response teams, fostering interdepartmental collaboration, and maintaining clear communication channels during incidents. Case studies like the Equifax data leakage, the Target data breach, also the WannaCry ransomware outbreak illustrate practical indication of incident response planning and provide valuable lessons on the importance of timely detection, effective containment, and transparent communication. These examples demonstrate that proactive and coordinated incident response efforts can significantly reduce the damage caused by cyber incidents and enhance organizational resilience.

Ultimately, this study highlights that an effective incident response capability is not static but evolves with the threat landscape. Continuous improvement through lessons learned from past incidents, regular training, and updates to incident response plans is crucial. Organizations that invest in robust incident response mechanisms, supported by practice directions and frameworks such as NIST and SANS, are better positioned to defend against and recover from cyber threats, thereby maintenance their digital assets and maintaining stakeholder trust in an increasingly interconnected and vulnerable digital ecosystem.

By fostering a culture of preparedness and resilience, organizations can not only tone down risks and minimize damages from cyber incidents but also enhance their overall security posture and ensure long-term business continuity. This study requests for action for organizations focus on and continually enhance their incident response strategies in response to the ever-evolving cyber threat landscape.

Acknowledgments

I would like to thank all members of the School of Computing who participated in this study. This study was carried out as part of the System and Network Security Project. This work was supported by Universiti Utara Malaysia

References

Antony, A., Mathew Thomas, S., Varghese, T. K., & Padman, V. (2023). *Ransomware Attacks on HealthcareSystems: Case Studies and MitigationStrategies*. https://doi.org/10.13140/RG.2.2.34192.17928

Bramhe, R. (2023, August 30). *How incident tracking can benefit your IT Organization*. https://www.onpage.com/how-incident-tracking-can-benefit-your-it-organization/

Cichonski, P., Milar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide*. National Institute of Standard and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber Risk and Cybersecurity: A Systematic Review of Data Availability. *Cyber Risk and Cybersecurity: A Systematic Review of Data Availability*. https://doi.org/10.1057/s41288-022-00266-6

Dimitrov, V., Kaloyanova, K., & Petrov, M. (2021). Adapted SANS Cybersecurity Policies for NIST Cybersecurity Framework. *Adapted SANS Cybersecurity Policies for NIST Cybersecurity Framework*. https://d1wqtxts1xzle7.cloudfront.net/84271282/paper29-libre.pdf?1650124820=&response-content-disposition=inline%3B+filename%3DAdapted_SANS_Cybersecurity_Policies_for.pdf&Expires=1717234871&Signature=WNVJmpVWge4kDovGHtPvGXIH9Ct4jFIG0IBptfjKRreBU~Pbv3LTu-N~5SZ6AEnOngSdTPd~SfThbhj7s0nm-qJGbF~0LDLZgXpLib4lHTlxqYP4g-8Kl44ErZ9Os8V~ByYamXtcEs8Mr9Bn6AFsyJzauudVBlpESc32eF-Iij8EPFphJoJluKdkmsB5gybB-v17Zgdy8T5AOeuaGoW1m91461JVTh9GGwO9~jjyfZpISc8jmktKBcEyVie2DfkmUV-ODBJmNGmF-NFY8D-TkttXzw6~C8XmWsuIUwO9KrxPpWgjHusCG4xgipAzCI4J70eNffZHMkTtmsnohmkkyQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

FIRST history. (n.d.). FIRST — Forum of Incident Response and Security Teams. https://www.first.org/about/history

Fruhlinger, J. (2023, June 28). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO Online. https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Jones, C. (2022b, May 3). *Warnings (& lessons) of the 2013 target data breach*. Red River | Technology Decisions Aren't Black and White. Think Red. https://redriver.com/security/target-data-breach

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *State of the practice of Computer Security Incident Response Teams (CSIRTs)*. https://apps.dtic.mil/sti/pdfs/ADA421664.pdf

Kirvan, P. (2024b, January 22). *How to build an incident response plan, with examples, template*. https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan

Lessing, M. (2017, June). *Case Study: WannaCry Ransomware*. https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-wannacry-ransomware/

Mell, P., Kent, K., & Nusbaum, J. (2005). *Guide to Malware Incident Prevention and Handling*. National Institute of Standards and Technology. https://profsite.um.ac.ir/kashmiri/nist/SP800-83.pdf

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. *Computers & Security*, *25*(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Nollau, B. (2009). Disaster Recovery and Business Continuity. *Disaster Recovery and Business Continuity*, *13*(3). https://www.proquest.com/docview/232833627/fulltextPDF/BC9C5A46BBDB45A7PQ/1?accountid=42599&sourcetype=Scholarly%20Journals

Pande, J. (2017). *Introduction to cyber security*. Uttarakhand Open University. https://d1wqtxts1xzle7.cloudfront.net/59862224/FCS20190625-18244-nzm6g9-libre.pdf?1561480031=&response-content-disposition=inline%3B+filename%3DIntroduction_to_Cyber_Security.pdf&Expires=1717228475&Signature=AJEHOW-oOkTMRyY5RhCCEHygxm3AYqf0aN09hSo4kjhhBEax4MtScwER-RvKxHjVhANkiDt3v9j9rXednK8aVmUTTVp9lq~8UFDTTnXQNzPz4G~FYVamRh-Tqb18q-

rXaKdTvCGOS6-fHWsgVjjoW7YWO-Ko6B9q450vpRQUqioNENlt0s7a0ik6p0KJYruEiVfbaIrkadbvS~W8Q5qUYQDiKZ56Q6QXzO7VaX6Ep1WUpMQILxlLdtT46psALDgB3E2W2sxMCawx4VBo2jrHvtbYV~5h1ZWckD2gUAEwqZkuRZz1Gv8yHyT0kWglVB~KEuqu7mzwUfxW3zfgtBnByw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017, January 18). *Breaking the Target: An analysis of target data breach and lessons learned*. arXiv.org. https://arxiv.org/abs/1701.04940

Tanczer, L. M., Brass, I., & Carr, M. (2018b). CSIRTs and Global Cybersecurity: How technical experts support science diplomacy. *Global Policy*, *9*(S3), 60–66. https://doi.org/10.1111/1758-5899.12625

Thompson, E. C. (2018). *Cybersecurity Incident Response:How to Contain, Eradicate, and Recover from Incidents*. https://books.google.com.my/books?hl=en&lr=&id=DXhvDwAAQBAJ&oi=fnd&pg=PR3&dq=incident+response+can+be+broken+down+into+six+distinct+phases&ots=-YZhfE6Kk7&sig=nW1j0d8G4n-kUQ0gLRoEDpkfcTc&redir_esc=y#v=onepage&q&f=false

Weiss, N. E., & Miller, R. S. (2015). The Target and Other Financial Data Breaches: Frequently Asked Questions. In *The Target and Other Financial Data Breaches: Frequently Asked Questions*. Congressional Research Service. https://sgp.fas.org/crs/misc/R43496.pdf

White, G. B., & Sjelin, N. (2022). The NIST Cybersecurity Framework. In *IGI Global eBooks* (pp. 39–55). https://doi.org/10.4018/978-1-6684-3698-1.ch003