Planning and Preparation of Cybersecurity

Mohammed Mustafa Khan

Abstract *– In today's digital environment characterized by fast-evolving adversaries, expanded attack surfaces, and complex IT environments, having a formidable plan and being prepared could create a world of difference when faced with a potential cyber-attack. Cyber threats are growing risks to everyone and any institution. Cybercriminals target individuals and companies of all sizes. Today's attacks are agile and sophisticated. Ransom demands are elevating and advancing rapidly while attackers drill down their focus to specific victims like critical infrastructure businesses, which can spend millions of dollars in losses from cyber disasters since such companies have less tolerance for downtime. The evolution of artificial intelligence technology, which is more interesting and scarier at the same time, is impacting the field of cybersecurity. The negative side of AI is that it has enabled threat actors to blend new data theft-based extortion techniques into ransomware. Attackers can steal companies' sensitive data or even encrypt the data and demand ransom for the decryption key failure, to which they threaten the company to expose the data to the public or even trade in the dark web. The intelligent techniques and tactics utilized by threat actors are a clarion call for organizations to proactively plan and prepare adequately by developing a cybersecurity strategy as a countermeasure. A cybersecurity strategy is a comprehensive plan that stipulates an organizational approach to secure its IT infrastructure against cyber threats. The common cybersecurity strategy various organizations use to plan and prepare for inevitable attacks is the incidence response plan. Incidence response is the processes and technologies organizations use to detect and respond to cyber threats, security breaches, or cyberattacks within an organization. Developing and implementing a formal incident response plan allows organizations to minimize and prevent damage. This research paper focuses on the primary goal of the incident response of preventing cyberattacks prior to occurring and reducing the cost and business disruption emanating from cyberattacks that happen.*

Keywords – incident response, threats, Artificial intelligence, cybersecurity, threat attacks, plan, preparation.

1.0 Introduction

Cybersecurity plans and preparedness must center on resilience during cyber disasters. Incident response plan is an integral component of cybersecurity operations. Cyberattacks are whooping in scale, frequency, and the level of sophistication [2]. Incidence response plan provide windows of opportunities for an organization's digital assets security defense. It presciently helps organizations plan and prepare for cybersecurity incidents once they happen to disrupt the success and damage possible attacks and counteract threats. A study performed by Immersive Labs indicated that almost 40% of organizations lack the confidence in their teams to handle a data breach. 61% of respondents agreed the most effective way to prepare for a security incident is by developing and implementing an incident response plan. Almost 40% of respondents surveyed concluded that the last exercise resulted in no action from the business [13]. Cyberattacks can have devastating consequences like financial losses, reputational damage, and huge fines from regulatory bodies. Developing and implementing a comprehensive cyber incident response plan (CSIRP) is the ideal strategy for the planning and preparation of cybersecurity. CSIRP aims to address and mitigate the consequences of cybersecurity threats, reduce disruptions, and ensure business continuity. It is important to understand the current cyber trends to enable an organization to plan and prepare appropriately for cyber threats. The paper discusses current cyber trends, the phases of the cybersecurity incidence response lifecycle, technologies used for incident response, some of the defensive measures, and the future of the incidence response plan using the AI metric.

2.0 Understanding the State-of-the-art Cyber Trends

Looking ahead for an incident response plan and preventing and detecting security events are tremendous aspects of planning and preparing for cyber security. In today's digital transformation, many businesses are paralyzed by cyberattacks, thus emphasizing the need to have a comprehensive incident plan that will maximize cyber resilience for organizations. Organizations need to anticipate and prepare for any threat that is likely to disrupt their business operations [1]. The following aspects provide a glimpse of the modern nature of threats and demonstrate the importance of an incidence response plan in planning and preparation for cybersecurity:

- Impact of AI on Cybersecurity
- Sophisticated phishing attacks
- Mobile device threats

2.1 Impact of AI on Cybersecurity

Artificial Intelligence (AI) has made a significant impact in the field of cybersecurity. This technology has both positive and negative sides. The positive side of AI is that it has presented many opportunities for threat hunting. Organizations can detect and respond to threats in real time, thus boosting their cybersecurity posture. On the other hand, AI has widened the chances for organizational attack surfaces since it introduces complexities that can be exploited by threat actors. Organizations must ensure their security teams have the required knowledge, skills, and expertise coupled with the right tools to shield AI-driven attacks [9]. Tools that prevent threats must be superior enough in identifying, detecting, disrupting, and remediating cyberattacks.

2.2 Sophisticated Phishing Attacks

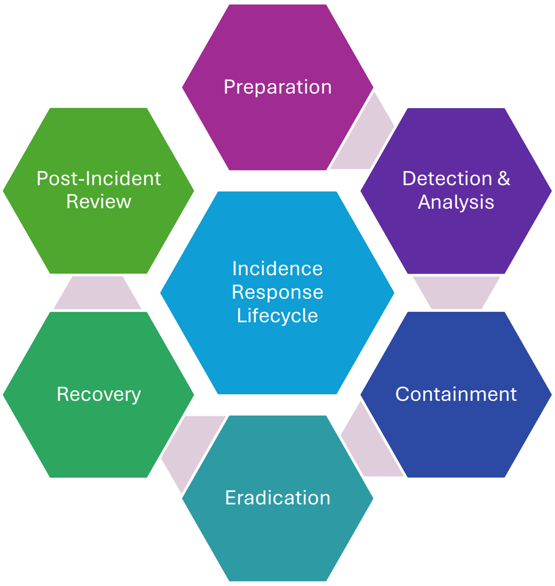
Modern phishing attacks are advanced and frequent courtesy of AI. Cybercriminals can utilize AI to quickly design a tricking backstory from organizational social media profiles, create a convincing message, and automate the attacks [9]. The effort that attacks use has decreased since AI is aiding them in properly gathering the required information that will enable attackers to make wise decisions. AI tools have become an integral component of attackers. What does this mean to an organization? An organization must adequately prepare for cyber threats by developing a comprehensive response plan to help remediate or disrupt the threat before it occurs.

2.3 Mobile Device Threats

Mobile devices have become important for personal and professional use. Mobile security must be hardened. Employees rely on their mobile devices like phones and laptops for remote work, personal communication, and financial transactions, among others. Additionally, companies are adopting the bring your own device policy to help employees perform their routine duties. Mobile devices have become a prime target for threat actors since they convey sensitive information. It is important to lobby mobile security solutions that will shield data leakage or loss. Hardening the mobile device's security will enhance its security [10].

3.0 The Incidence Response Lifecycle

There are several phases involved in responding to a cybersecurity incident. The purpose of having a step-by-step approach is to make sure that incidents, no matter their intensity, are properly dealt with [3]. An effective response helps to reduce damage and minimize the time and costs of disaster recovery. A study conducted by Ponemon Institute indicated that it takes organizations almost 280 days to detect and contain cyber threats [2]. 280 days is a lot of time that will lead to the lateral spread of threats and even cripple the operations of an organization. Organizations that do not want to take 280 days to detect and contain cyber attacks must be ready to follow the following steps of the incidence response lifecycle:



3.1 Preparation

Preparation is the premier foundation that sets the pace for effective incident response. It starts by drafting a comprehensive incidence response plan. The incident response plan defines roles, responsibilities, and procedures for handling cyber threats, training of personnel, lines of communication in case of an event, and tools and resources that must be put in place to help the team identify, detect, and disrupt cyber threats [3]. Additionally, the incident response plan addresses the system security, the type of data it handles, and the industry regulatory requirements, among others. Risk assessments help the CSIRP discover the business environments that need to be protected, the possible network vulnerabilities, and different types of security events that threaten an organization's IT infrastructure. The team prioritizes every type of incident in regard to possible consequences for the organization.

The organization assembles a cyber incident response team with prowess in crisis management. The composition of the team will include people from different environments, such as IT, public relations, legal, and human resources, to mention a few. The team is trained to ensure they are equipped with the necessary knowledge and skills to be used during an emergency. Regular simulation exercises and practices are performed to check the organization's systems and technology and to ensure the team is ready and familiar with response procedures [4]. The simulation activities will help the organization invest in setting up the right tools and technology, such as security information and event management (SIEM), needed to plan and prepare for threats.

3.2 Detection and Analysis

The second step deals with identifying and determining if an incident has happened. This stage poses a lot of challenges, especially in large enterprises, where the volume of daily events can be overwhelming. The security team ought to investigate a multitude of data points to differentiate between false positives and false negatives that are potential compromise of indicators [4]. During this stage, security team members monitor the network for anomalies and possible threats. Data, notifications, and alerts generated from different device logs and different security tools like firewalls and antivirus software are analyzed to identify incidents that are in progress. It is fundamental for the security team to utilize special tools and techniques to reconstruct the attacker's behaviors and evaluate the range of the harm.

3.3 Containment

Containment aims to limit the scope and consequences of cybersecurity incidents. The strategies for containment can be categorized into two: short-term and long-term. Depending on the nature of the incident.

Short-term strategies refer to quick and decisive actions to reduce the potential effect from further spreading to the entire network and disrupting business operations [4]. This involves isolating the affected computers by disconnecting them from the network, blocking the malicious traffic, or preventing unauthorized access by changing the access credentials. The goal of this strategy centers on reducing the impacts on company systems.

Long-term strategies aim at fixing the affected systems temporarily to ensure the systems keep in operation while rebuilding healthy systems. It involves eliminating the backdoors exploited by threats by fixing the patches, updating or replacing compromised software, and reviewing network security [4].

3.4 Eradication

This stage focuses on clearing any traces of the breach to ensure the network system is healthy and the root cause of the incident is eliminated. It involves removing the malicious content from the affected systems and cleaning the systems to block the reinfection risk. The antivirus and antimalware tools can be used to remove the malicious content [4]. The primary objective of eradication is to remediate the threat from the system.

3.5 Recovery

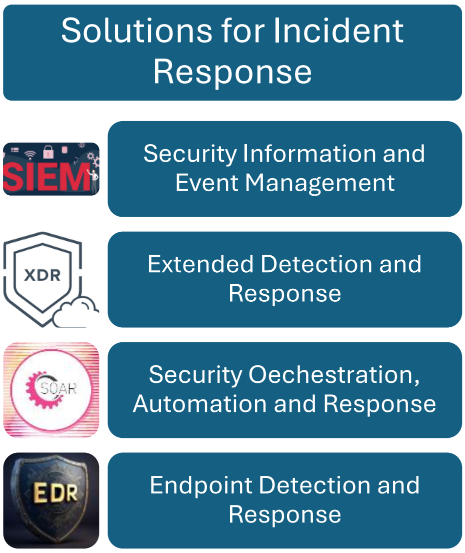
This stage involves executing disaster recovery plans to ensure business continuity. The stage ensures systems are restored to their initial state before the occurrence of the incident. During this stage, it is crucial to maintain business continuity [3]. Redundant systems that act as backups must be activated. Activating the backups helps restore critical business functions. All the disabled accounts must be re-enabled with new login credentials.

3.6 Post-incident Review

This marks the final stage of the incident response life cycle. It involves conducting a postmortem of the entire incident and documenting all the activities and security controls used [3]. Post-incident review enables the organization to comprehend how the incident happened and what can be done to prevent similar incidents from occurring in the future. The insights gained from this stage can strengthen the organization's incident response procedures and enhance the overall effectiveness of its security strategy.

4.0 Incident Response Technologies

Planning and preparing for cybersecurity involves monitoring the network traffic user behavior and counteracting suspicious activities. For an organization to achieve all these, they need to have an appropriate arsenal and technologies that will help the security team to accomplish their task. Tools and technologies are the cornerstone solutions that enable the security team to prepare and plan for cybersecurity properly. Some of the solutions used for incident response technology are:


Solutions for Incident Response
SIEM
Security Information and Event Management
XDR
Extended Detection and Response
SOAR
Security Oechestration, Automation and Response
EDR
Endpoint Detection and Response

4.1 SIEM

SIEM aggregates and correlates security events data from heterogeneous security tools like firewalls, vulnerability scanners, antivirus software, threat intelligence fields, and endpoint devices connected to a network [5]. The log files collected by SIEM can be further reviewed by the security personnel, and any suspicious logs are treated accordingly. Additionally, the frequent alarms can decentralize the security teams, leading to alarm fatigue. However, SIEM is infused with AI to differentiate indicators of compromise from the bulk of alerts generated by other security tools.

4.2 XDR

As businesses are shifting from on-premise environments to hybrid clouds, securing hybrid workloads becomes a bottleneck. XDR is a cybersecurity technology that merges all the security tools, data and telemetry sources, control points, and analytics within the hybrid IT environment [13]. XDR helps to eliminate the silos that exist among security tools and automate detection responses as the security teams sail through the cyber threat kill chain developed by Lockheed Martin.

4.3 SOAR

Security playbooks play an important role in cybersecurity. Playbooks are sets of automatically generated reports about a particular security incident. The SOAR solution has the capability of generating these playbooks, which can give insight to the security teams on how to plan and prepare for cybersecurity. Additionally, the SOAR solution streamlines workflows that entail different security operations and tools in counteracting security events [5].

4.4 EDR

An EDR is software designed to monitor, detect, and respond to threats that may evade antivirus software and other conventional security tools on endpoints such as desktops, laptops, and servers. EDR gathers data on all the endpoints connected to a network. In addition to data collection, EDR analyzes the collected data instantly to inspect any suspicious content and respond automatically to minimize the damage [13].

5.0 Defensive Measures

Defensive measures aim to protect data and information systems from potential attacks. It entails implementing security control and measures to secure organizational digital assets [6]. For instance, installing and configuring web application firewalls will help to protect web applications from cyber threats and SQL injections that bypass the network detection firewall tools [8]. The are various defensive measures that organizations need to consider when planning and preparing for cybersecurity. Here are a few sampled examples:

5.1 Password Policies

Password policy best practices must be implemented to ensure the employees can create a strong password that is difficult to crack and keep private [6]. Enforcing password policies for employees will fortify the security of workstations. It helps to minimize the malicious insiders from compromising workmate accounts. Detecting an insider threat is quite challenging since they have legitimate access to the account. Nevertheless, there are certain tools, such as SIEM, that have been infused with AI and machine learning that can analyze user behavior, leveraging the capability of user and entity behavior analytics to detect and respond to such anomalies [5].

5.2 Access Controls

It is important to create some logical barriers that ensure employees can only view and access the information they are supposed to access depending on their job roles [6]. Role-based access controls can help the IT administrator create access controls that will prevent unauthorized access to some information within an organization. Additionally, role-based access controls prevent the insider threats from navigating to their entire organization systems.

5.3 Data Encryption and Data Loss Prevention

Encryption aims to protect data during transmission, in use, or stored. Encryption technology helps to scramble data into unreadable format. To read the data, you need a key to decrypt it. Even if the intruder intercepts the data, it will be too difficult for them to view since it will demand a key. It is important to use powerful encryption algorithms such as Advanced Encryption Standard (AES). Additionally, data loss prevention security solutions must be implemented to discover and prevent inappropriate sharing, deletion, or use of sensitive data [7].

5.4 Authentication

Authentication involves the user to input login credentials for him to get access to workstations. It demands the user to provide a combination of aspects like usernames and passwords. To harden the security of endpoints, it is important to use multifactor authentication that will prompt the user to supply more credentials to validate if they are legitimate personnel. Multifactor authentication utilizes one-time password capabilities to prevent code reuse [6].

6.0 AI and the Future of Incident Response

AI can aid organizations in developing and establishing a stronger defense against cyber threats. Threat actors are utilizing AI to sophisticate their attacks, so it is paramount for the organization to invest in AI-powered intrusion and detection solutions to supersede threat actors [11]. Otherwise, organizations are likely to succumb to AI-powered threats. AI-driven security systems can enhance incidence response functionalities by detecting anomalies in real-time, predicting the potential attack channels, and using proactive response processes.

7.0 Conclusion

In conclusion, being proactive in planning and preparing for cyber threats is crucial for any organization. With the increasing sophistication of cyberattacks, especially those leveraging AI, it is essential to implement a comprehensive incident response plan. This will help to mitigate the risks of data breaches, minimize operational disruptions, and ensure business continuity. The use of advanced technologies such as SIEM, XDR, and EDR, alongside defensive measures like access controls and encryption, can enhance an organization's ability to detect, respond to, and recover from cyber incidents.

8.0 Reference:

[1] H. Kettani and P. Wainwright, "On the Top Threats to Cyber Systems," *2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT)*, Mar. 2019, doi: https://doi.org/10.1109/infoct.2019.8711324.

[2] Shekokar and Narendra M., et al, "Cyber Security Threats and Challenges Facing Human Life," *Google Books*, Sep. 01, 2022. https://books.google.com/books?hl=en&lr=&id=Dp8IEQAAQBAJ&oi=fnd&pg=PP1&dq=Ponemon+institute+indicated+that+it+takes+organizations+almost+280+days+to+detect+and+contain+cyberthreats.+&ots=HN6cgthPx-&sig=absCzQj9J3DLiI19uylFr6YZbzI

[3] Y. He, E. D. Zamani, S. Lloyd, and C. Luo, "Agile incident response (AIR): Improving the incident response process in healthcare," *International Journal of Information Management*, vol. 62, p. 102435, Feb. 2022, doi: https://doi.org/10.1016/j.ijinfomgt.2021.102435.

[4] EC-Council, "Understanding the Incident Response Life Cycle," *Cybersecurity Exchange*, Mar. 30, 2022. https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

[5] T. Ban, T. Takahashi, S. Ndichu, and D. Inoue, "Breaking Alert Fatigue: AI-Assisted SIEM Framework for Effective Incident Response," *Applied Sciences*, vol. 13, no. 11, pp. 6610–6610, May 2023, doi: https://doi.org/10.3390/app13116610.

[6] L. Irwin, "The key elements of a cyber security plan - IT Governance UK Blog," *IT Governance UK Blog*, Nov. 20, 2018.

https://www.itgovernance.co.uk/blog/the-key-elements-of-a-cyber-security-plan

[7] I. Herrera Montano, J. J. García Aranda, J. Ramos Diaz, S. Molina Cardín, I. de la Torre Díez, and J. J. P. C. Rodrigues, "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat," *Cluster Computing*, vol. 25, no. 6, pp. 4289–4302, Jul. 2022, doi: https://doi.org/10.1007/s10586-022-03668-2.

[8] Morthala, Venkatesh Reddy, "Building Firewall Application To Enhance The Cyber Security - NORMA@NCI Library," *Ncirl.ie*, Jan. 2022, doi: https://norma.ncirl.ie/6026/1/venkateshreddymorthala.pdf.

[9] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review," *papers.ssrn.com*, Sep. 01, 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317

[10] P. Weichbroth and Ł. Łysik, "Mobile Security: Threats and Best Practices," *Mobile Information Systems*, vol. 2020, pp. 1–15, Dec. 2020, doi: https://doi.org/10.1155/2020/8828078.

[11] S. Tatineni and A. Mustyala, "Advanced AI Techniques for Real-Time Anomaly Detection and Incident Response in DevOps Environments: Ensuring Robust Security and Compliance," *Journal of Computational Intelligence and Robotics*, vol. 2, no. 1, pp. 88–121, Mar. 2022, Available: https://thesciencebrigade.com/jcir/article/view/230

[12] Telelink, "Advanced Security Operations Center," Dec. 2020. Available: https://www.tbs.tech/wp-content/uploads/2022/11/telelink-monthly-security-bulletin-12.2020.pdf

[13] Olteanu and Ioana-Cristina, "Evaluating the response effectiveness of XDR technology in a scaled down environment," Dec. 2022. https://research.tue.nl/files/305661196/Olteanu_I.C..pdf