Business Resilience and Incident Management

Chijioke Franklin Emejuru

Project Description: This project explores real-world cybersecurity scenarios, focusing on threat identification, incident response planning, and business continuity strategies to help organisations prepare for and recover from cyberattacks.

Project Summary:
This report outlines real-world cybersecurity scenarios involving a fintech company, a hospital, and a manufacturing firm, each facing significant cyber threats such as phishing, ransomware, and operational disruptions. It highlights the need for strong **Incident Response Plans (IRPs)** and **Business Continuity Plans (BCPs)** to reduce damage and ensure continuity during and after cyber incidents.
The document covers how to identify threats, prepare tailored response strategies, assign key team roles, and use tools like **SIEM** for proactive threat detection. It also stresses the importance of effective communication and regular evaluation of response plans through audits, simulations, and performance tracking.
Overall, it demonstrates how organizations can strengthen their cyber defenses and improve resilience by planning ahead and continuously improving their response strategies.

Case scenario: Mid-sized Fintech

Organizational operations: The Fintech offers financial services to individuals and Firms. Handles large amount of customer sensitive financial information, which makes it attractive to cyber criminals.

The management team is interested in learning about how specific risks pose a potential threat to the organization and has asked for a risk assessment to be carried out to ensure the preparedness to handle emerging threats through Incident Response Plan.

Threats Identification and Impact on Business

In order to create a comprehensive and efficient Incident Response Plan for an organization, the first step is the risk assessment and identification of cyber threats the organization is prone to or evolving cyber threats (Farok and Borneo 2024).

The threats identified for the Fintech are Phishing attacks and Ransomware which have become major sources of menace for victims of such attacks (Thomas 2018).

Phishing Attacks: According to Muniandy et al. (2022), Phishing attacks can result in the stealing of sensitive information, identity theft, companies, and organizational secrets leading to huge financial losses, breach of customer information and trust, putting the business or organization's integrity at stake.

Furthermore, Phishing attacks which have been known to extend beyond the common email phishing to include various variants such as spear phishing, whaling, clone phishing, vishing, smishing, and search engine phishing have become increasingly popular (Nadeem et al. 2023).

Ransomware: Cyber attacks have learnt to leverage on interconnected systems used by organizations to infiltrate Ransomware attacks (König et al. 2018), which can lead to work

disruptions, data breaches, halt in manufacturing and supply chain delays, financial and legal liabilities (Krivokapić and Nikolic 2022).

Integration into Incident Response Plan

To prevent the Fintech from the losses associated with these cyber attacks, it is necessary to integrate them into the ok organization's incident response plan.

Phishing Attacks

Preparation:

- Implementation of software throughout the organization to detect phsising patterns
- Employee training on phishing awareness and patterns
- Implementation of the use of secure browsers with effective firewalls
- Provision of system backup

Detection and Analysis:

- Discovery and knowledge about the affected networks
- Outlining of the incident's scope, such as systems or applications, information on the cause(s) of the incident and tools and methods employed

Containment, Eradication and Recovery:

- Removing affected systems
- Disabling breached accounts
- Segregation of affected systems
- Restore the system using the provided system backups
- Replace affected software with clean versions
- Install software patches
- Tighten network perimeter security

Post-incident activity:

- Review of lessons learned from the attack
- Implementation of steps to prevent future incidents

Ransomware

Preparation:

- Implementation of multi factor authentication
- Regularly update softwares
- Facilitate employee training on Ransomware attacks and detection
- Maintain offline system backup
- Preparation of reporting

Detection and Analysis

- Identification of compromised systems
- Analysis of Ransomware incident to ascertain origin, cause, effect, damage

Containment, Eradication and Recovery:

- Isolation of unaffected systems
- Implementation of BCP
- Implementation of communication protocols

Post-incident Activity:

- Incident Response Plan audit and review

Reconmmendations for IR Tailoring

- Implementation of different playbooks for specific threats
- Regular auditing of response plan
- Update response plan based on positive or negative outcomes of incident stimulations

Through these strategies, the Fintech can achieve a strong incident Response Plan

Case Scenario: Development of a Business Continuity Plan for a Hospital

Business Continuity Plan (BCP) framework is a procedural guidance for creating incident plans that prevent, prepare, respond, manage, and recover a business from any form of disruption or incident crisis (Fani and Subriadi 2019). BCP is essential for organizations especially in these

current times where there are a lot of threats that can affect the organization flow of business operations.

Impact of Lack of BCP on Organization

Due to the hospital's lack of a BCP, it currently suffers prolonged disruptions, operational paralysis and financial losses in the wake of the recent cyber attack. In light of recent events, it would be best for the the hospital to develop a BCP that would allow for sustainability of business processes for future cyber attacks (Muflihah and Subriadi 2018).

Business Resilience and Relation to Incident Response

In the face of a cyber incident, having a BCP will provide business resilience that enables the hospital to adapt and continue operations despite disruptions (Linnenluecke 2017). Business resilience systems can include communication, hardware and IT assets with the aim of getting the hospital's technical operations to resume normalcy.

To develop the BCP, the IRP has to be focued on business resilience to achieve maintainience in availability and managing disruption. This will be done in the early stages of the IRP in order to provide a comprehensive objective plan process and identify its goals (Corrales-Estrada et al. 2021).

Application of Theoretical Concepts to Scenario

Inorder to manage cyber disruptions and achieve business resilience, the hospital's BCP will include the application of PICER (Preparation, Identification, Containment, Eradication and Recovery), with the aim of restoring systems. Using the PICERL as a framework for BCP ensures that the hospital develops a robust Incident Response Plan that prepares it for future cyber disruptions, helps it to identify suspicious actions as threats, build containment measures that will facilitate business continuity, develop an effective disaster recovery team and tools for eradication and lastly employ Disaster recovery techniques.

Case Study Scenario:

A manufacturing company has suffered a Ransomware attack. Important documents including encryption files have been encrypted by attackers leading to disruptions in supply chain, production and distribution. As the leader iof an Incident Response Team, I have been charged with leading a team, allocation of roles within the team and recommending actionable communication strategies for the team.

Identification of Key roles and Responsibilities

An incident's response team also known as Computer security incident response teams (CSIRT) typically consists of various roles that are designed to address threats posed by cyber-criminals (Bada et al. 2014). Some of these roles include skills such as Hands-on technical skills, Networking, Cybersecurity engineering, Memory analysis, Reverse-engineering, Written and oral communication skills, Leadership skills, Legal, HR and PR/Comms.

Prioritization of Roles

In this context, the Incident Response Team should be organized based on urgency aimed at containment and recovery from Ransomware attacks

Team members with outlined roles include the following:

Incident Response Manager/Coordinator

- Lead incident response team
- Carry out all effective coordination of the incident response team
- Ensure collaboration of all team members

Threat Analyst

- Estimate the Ransomware spread
- Recommend next step to facilitate Ransomware containment
- Provide information on Ransomware type, attack mode, effect and impact

IT System Administrator

- Provide steps to achieve restoration of supply chain process

Forensic Specialist

- identification of vulnerabilities that was leveraged during the Ransomware attacks
- Provide recommendations for protection against future attacks

Ciommunication Manager / PR

- Prevent Reputational damage by providing timely updates on the IR plan to the Stakeholders and the Public
- Coordinate and manage the flow of information of team members

Legal Advisor

- Provide guidance on adherence to regulatory requirements-Communications of IR policies

Communication Strategies for the Team

Based on the severity of the Ransomware attack, communication is a very important aspect that ensures each team member is up-to-date with the incident response process and allows team members to coordinate easily. According to Ioannou, Stavrou and Bada (2019), many CSIRTs face issues such as communication and cooperation, coordination.

To prevent this, as the Incident Response Manager/Coordinator, there is a need to employ practical communication protocols and channels that carry and cater to every team member during the incident response planning and execution processes. This can include:

- Forming a centralized communication channel such as the use of popular communication and project management platforms like Slack or Asana to share updates
- coordinate and assign tasks and track progress in real time
- holding regular scheduled briefings to keep track and provide progress reports
- accurate incident logging and reporting that would include decisions made, actions taken, positive or negative outcomes for future reference.

Wagner et al. (2019) define Cyber Threat Intelligence (CTI) sharing as an essential cyber defense tool to proactively mitigate increasing cyber attacks. Threat intelligence is important for

organizations to prepare themselves against rising cyber security threats, strengthen their defenses and improve their incident response plans (Bromiley 2016).

Development of Threat Hunting Strategy

After the organization receives a Threat intelligence report informing them of emerging threats, the next steps taken should include the Development of a Threat Hunting Strategy. Nursidiq and Lim (2024) defines a Threat Hunting Strategy as a strategy to improve cyber threat awareness, enabling organizations to make informed decisions and implement appropriate protective measures.

In this context of increased Phishing attacks, the need to use a Security Information and Event Management (SIEM) Threat Hunting Strategy is essential. The components of a SIEM include data sourcing, collection, parsing normalization, rule engine correlation, log storage and monitoring (Granadillo, González-Zarzosa, and Diaz 2021).

These components in this context will be used to gather the data on phishing emails provided in the threat intelligence, correlate and identify phishing patterns, monitor data for anomalies, provide visualization tools to track compiled incidents and performance metrics using Indicators of Compromise (IoCs) to identify potential phishing threats.

Integration of SIEM in Incident Response

The integration of SIEM as a Threat Hunting Strategy into the Incident Response framework enhances security operations and will provide the organization with early phishing threat detection, accurate logging of incidents, automated behavioural analysis, provision for identification of needs for continuous improvement in IR, and efficient collaboration amongst IR teams.

Through the implementation of the SIEM as a Threat Hunting Strategy, the organization moves from a reactive to a proactive posture, having the necessary tools to flag suspicious emails based on the IoC implemented by SIEM.

Case study Scenario: An organization recently recovered from cyber incident with the need to evaluate IR posture in the light of emerging threats.

According to Williams (2012), the evaluation of an incident response posture entails the effectiveness of the several countermeasures that have been implemented to protect the organisations resources against cyber disaster. The evaluation methods include measurement, reporting, auditing, and testing.

Inorder to ascertain the durability and efficiency of the IRP, it is important to assess the IR by these methods:

- **Measurement:** includes the tracking of the categories and types of cyber threats that the organization has faced overtime. Measurement can be achieved using measuring tools like Key Performance Indicator (KPIs) to measures all cyber security incidents so far.
- **Reporting**: includes the documentation of the post incident decisions and actions to evaluate the decision making process and actions taken in light of the the events.
- **Auditing**: involves the assessment of the IR team's readiness to contain the disaster.
- **Testing**: includes the performance of IR stimulation to assess the strength of the IR in addressing real word cyber threats.

After the evaluation process, the next step is to point out areas in the IR requiring improvement, such as delay in threat detection and ineffective communication throughout the IR execution. To improve these, recommendations would include integration of SIEM detection tools, outsourcing of IR to third party experts and integration of more enhanced communication protocols.

Incident Response Plans are made to be evaluated in order to ascertain their efficiency in the real-world. By assessing them through the outlined methods, measuring, reporting, auditing and testing, there is room for improvement and further security protection for future cyber disruptions.

References:

Anson, S., 2020. *Applied incident response*. USA: John Wiley & Sons.

Bada, M., Creese, S., Goldsmith, M., Mitchell, C. & Phillips, E., 2014. *Computer security incident response teams (CSIRTs): An overview*. The Global Cyber Security Capacity Centre.

Bromiley, M., 2016. Threat intelligence: What it is, and how to use it effectively. SANS Institute InfoSec Reading Room, 15, p.172.

Corrales-Estrada, A.M., Gómez-Santos, L.L., Bernal-Torres, C.A. & Rodriguez-López, J.E., 2021. Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review. *Sustainability*, 13(15), p.8196.

Fani, S.V. & Subriadi, A.P., 2019. Business continuity plan: Examining of multi-usable framework. *Procedia Computer Science*, 161, pp.275-282.

Farok, N.A.Z. & Zolkipli, M.F., 2024. Incident Response Planning and Procedures. *Borneo International Journal*, 7(2), pp.69-76.

Jimmy, FNU., 2024. Phishing attackers: prevention and response strategies. *Journal of Artificial Intelligence General Science (JAIGS*), 2(1), pp.307-318.

Granadillo, G., González-Zarzosa, S. & Diaz, R., 2021. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, 21, p.4759.

König, S., Gouglidis, A., Green, B. & Solar, A., 2018. Assessing the impact of malware attacks in utility networks. *In Game Theory for Security and Risk Management: From Theory to Practice*, pp.335-351.

Krivokapić, Đ. & Nikolic, A., 2022. Legal Obligations and Liability in a Ransomware Attack. *Zbornik radova Kopaoničke škole prirodnog prava–Slobodan Perović,* 3, pp.173-196.

Linnenluecke, M.K., 2017. Resilience in business and management research: A review of influential publications and a research agenda. International *Journal of Management Reviews*, 19(1), pp.4-30.

Muhammad, N., Zahra, S.W., Abbasi, M.N., Arshad, A., Riaz, S. & Ahmed, W., 2023. Phishing attack, its detections and prevention techniques. *International Journal of Wireless Security and Networks*, 1(2), pp.13-25.

Muniandy, M., Ismail, N.A., Yahya Al-Nahari, A.Y., & Ngo Lung Yao, D., 2022. Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience. International Journal of Little Lion Scientific Neural Computing and Applications, 34, pp.12077-12096.

Nivedita, S. & Kulkarni, P., 2021. Cyber incident response and planning: a flexible approach. *Computer Fraud & Security*, 2021(1), pp.14-19.

Nursidiq, A. & Lim, C., 2024. Fortifying the Enterprise Network: Proactive Strategies for Cyber Threat Hunting. 2024 12th International Conference on Information and Communication Technology (ICoICT), pp.419-424.

Thomas, J.E., 2018. Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International *Journal of Business Management*, 12(3), pp.1-23. doi:10.5539/ijbm.v13n6p1.

Vidiya Fani, S. & Subriadi, A.P., 2018. A basic element of IT business continuity plan: Systematic review. *Jurnal Informatika Ahmad Dahlan*, 12(1), pp.17-23.

Zainab, A., Hewage, C., Nawaf, L. & Khan, I., 2021. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, p.563060.