Cybersecurity Incident Response Strategies for Financial Institutions

Ajay Benadict Antony Raju

ajaybenadict@gmail.com

Abstract

Incident response plans are important tools in the management of effects of cyber-attacks for the financial institutions. Since more and more financial organizations are under the cybersecurity threats' attack, it also became significant to have a proper definition of the incident response strategy to prevent serious losses and disruptions. In this abstract key strategies of cybersecurity incident response that include preparation, detection, communication, eradication, recovery, and post-incident analysis are outlined. Preparation entails creating an incident response team and the creation of elaborate response plans. Detection is a process of recognizing and approving actual or potential security threats using the means of monitoring and intelligence. Containment is a process that seeks to prevent the further spread of the particular incident while the elimination is focused on countering the major source or threat. Business continuity focuses on returning to normal operations and normality while analysis of the aftermath enables an organisation to learn more about the effects of the attack and the best course of action when similar incidents occur. Through the proper measure of tackling incidents response, financial institutions can improve their ability to withstand cyber threats, lower operational disruption, and safeguard valuable financial information to maintain confidence of its clients and compliance with the relevant authorities.

Keywords: Cybersecurity Incident Response, Financial Institutions, Detection, Containment, Recovery Post-Incident Analysis

Introduction

Since financial institutions are already integrating digital technologies in their delivery models and operations, they are vulnerable to cyberattacks. The very nature and occurrence of dangers in the cyberspace have changed and increased in terms of intensity and number for these institutions, thus the necessity of having proper cybersecurity incident response plans. These strategies are important for fast responding on security incidents, minimizing their consequences, furthering business, and protecting financial information.

Incident response strategies define a clear order by which the organizations are supposed to handle and come out of a cybersecurity attack. It involves a set of interrelated processes intended to identify, assess, prevent, eliminate and mitigate cyber threats. The first important planning involves setting up of an incident response team, formulation of response plans, and practice of such plans through training and simulations.

Detection is done in simple terms whereby potential security threats are detected within an organization through the use of various methods such as sophisticated monitoring systems, threat intelligence, and anomaly detection. After an incident has been identified, mitigation measures are used to prevent the further incidence of the event in question. This is then taken by eradication to eliminate the threat from the environment and recovery to bring the operation back to a normalcy in services. Last of all, the post-incident analysis is done to assess the reaction, identify lessons learned, and improve on the reactions to similar future occurrences.

Due to the nature and specificity of the markets in which financial institutions operate, they have no choice but to have highly effective incident response planning. Responsive measures not only prevent and control the extent of loss and additional time but also ensure compliance and organisational robustness. Therefore, it is essential to proceed with the constant enhancement and development of incident response strategies to prevent the deterioration of the financial arena's security and trustworthiness due to further advancements in cyber threats.

Literature Review:

There is a great need to develop practical cybersecurity incident response measures that can help financial institutions to contain/certify the effects of cyber-attacks. Cyber threats that affect such intuitions have become more complex and frequent, thus requiring a well-coordinated and systematic way of handling such incidences. In their work, Bertino and Sandhu mentioned that, the organizations should be able to respond in a timely and efficient manner in order to minimize the impact of security breaches and time to recovery [1]. Getting prepared, detecting cyber threats, containing, eradicating and eventually recovering from the attack as well as conducting a post mortem analysis is the common and vital approach towards incident response.

Preparation entails identifying members for the response team, drafting response plans/ templates and taking frequent rehearsals. There is a need to establish an effective preparation of the incident response team as pointed out by Patel et al. (2021) as this creates a co-ordinated approach to deal with emerging cyber threats [2]. This preparation phase also entails the making and conducting of exercise on response to incidents which assist institutions in identifying threats which may occur then naming strategies on how to handle them.

The last key process of the triad is detection which is concerned with suspecting and approving specific incident using comprehensive monitoring and threat intelligence. Chen and Zhao (2019) pointed out that specialised tools and Threat Intelligence Platforms are necessary to enable early detection of security intrusions so as not to allow the situation to escalate and put a lot of damage to an institution [3]. Detection mechanisms help financial institutions to be aware of the issues that may be indicative of firmer threats within the organization before they progress.

Mitigation measures are used in order to minimize the extent of the spread and effects of an incident as soon as the occurrence has been ascertained. Alharkan and Alhaidari (2020) focus on containment strategies that should be applied to minimize the impact and avoid expansion of virus, the systems that have been infected must be disconnected from the network [4]. During this phase the resources should be isolated, proportionate access control should be provided and other necessary control measures should be put in place to counter the incident.

One of the strategies whose implementation aims at reducing the probability of security risks is elimination, which means that the source of the threat is completely withdrawn from society. Dinh and Nguyen mentioned that, in this phase, to make sure the threat has been eradicated and it cannot reappear, more detailed research and cleaning have to be completed [5]. Recovery is all about getting back to normal and the normalcy is important in reducing the time the business is locked up and allow business to continue as usual. Last of all, after compromise analysis enables institutions to determine the consequences of the attack, to assess the results of minimizing the impact of the attack and to define crucial measures to be taken [6].

Problem Statement

Lately, financial institutions have become the victims of highly developed cyber operations that can negatively affect their outcomes, image, and customers' confidence. Despite the institutions having put measures to combat the threat of cyber criminals, these institutions suffer in terms of adequate management and combating of cyber threats due to changing trends in cyber criminals and the diverse IT network at their disposal. Normal incident handling approaches might not be effective enough when it comes to the rapid and complex

contemporary cyber threats, thus contributing to defects of containing the threat, lengthy restoration duration, and non-compliance with the regulations [1].

In addition, there is also a problem of absence of a single numbering and homogeneous approach to reaction to incidents in many financial organizations. Lack of preparation, weak identification and detection abilities, and poor intervention and mitigation strategies will tend to lessen the effect of cyber security occurrence. It also hinders the preparedness of the incident response teams since they have not been frequently trained and put through simulations hence institutions struggle to react appropriately when such incidences happen [2]. Therefore, financial institutions are at increased risk of operational in availability, monetary loss, and reputational harm, making it incredibly imperative to establish proper and resilient adaptive incident response strategies.

Solution

Due to the various problems and threats that exist in managing cybersecurity occurrences within the financial institutions, there is need for a broad and elaborate incident response plan. This strategy should encompass several key components: The main stages involved in the management of Information security are; preparation, detection, containment, eradication, recovery, and post-incident analysis.

Preparation entails, setting up of an incident response team that has a clear list of its roles and members. This team should be provided with clear written guidelines when it comes to incidents with clearly defined instructions on how to handle different forms of cyber incidents. Training and simulation activities are also very important in maintaining familiarization of team members of the plan to be able to quickly and efficiently respond to an actual mishap [2]. Preparation also entails the determination of the communication channel of both internal and external users to facilitate the dissemination of proper information.

Detection involves using of monitoring tools and threat intelligence platforms to help in identification of possible security incidences. Gaith [3], suggests that the integration of intrusion detection systems (IDS), security information and event management (SIEM), and threat intelligence feed will complement the defense mechanisms of the institution in identifying the early stages of the anomalous activities. System logs, network traffic analysis and user behaviour analysis are crucial tools in supporting continuous monitoring and validation of security incidents.

Control measures pertain to practices, actions and steps taken with the aim of reducing the extent of the repercussions of an occurrence. As part of the containment process, systems in the affected businesses are isolated, restricted access to areas that have been infected, and the use of similar measures that serve as a quick fix [6]. Containment processes should involve other IT and security departments so that the containment actions are appropriate and implemented systematically to isolate affected systems from the rest of the organizational network.

Prevention anticipates the complete elimination of the risk from the environment. This phase must be well investigated and undertaken in a bid to remove all existing threat and other vulnerabilities left behind [5]. In the eradication process there is a need to apply patch management, updated security configuration, and also conduct the forensic study.

Recovery here means, getting back to service and functioning as fast as possible with as little disruption time as possible. This phase involves confirming that systems are working properly, recovering data from backups and observing for any more signs of threats [6]. In addition, proper coordination with business units and information sharing with the stakeholders take a lot of care to ensure that recovery process is successful and business returns to normalcy.

Another important step that has to be taken after the occurrence of a certain threat is analysis of the event and assessment of how it was handled. In this sense, when reviewing the factual circumstances of the event, assessing the response process, and identifying key findings can facilitate the further improvement of the

response capacities of the institution and the overall organisational security [6]. Revisiting of the incident response plan as advised by findings from a post-incident analysis help in maintaining agility in preparation of the institution for any future incidences.

To sum up, incident response plan that should consist of preparation, detection, containment, eradication, recovery and post-incident analysis can help financial institutions to manage and limit the scope of cybersecurity attacks. Incorporation of these components will help institutions act proactively against threats especially in cyber space while reducing the downtime and cost of operation, customer trust shall also be maintained.

Conclusion

Therefore, it could be concluded that creation and enhancement of comprehensive cybersecurity incident response policies is a necessity for the financial institutions to be able to control and mitigate the consequences of cyber threats. Considering the fact that cybersecurity threats are diverse, persistent and growing in complexity, formal and systematic approach to managing security incidents enables financial institutions mitigate the risks and losses from cyber threats.

Effective incident response strategies encompass several critical components: They include: preparation, detection, containment, eradication, recovery and post-incident analysis. Preparedness on the other hand entails putting up a special incident response team, development of elaborate response plans and often practice and rehearsals. This feels like the most important book to read, so that one is fully prepared to deal with incidents when they occur.

For the detection phase information security aims at detecting and confirming possible security breaches by deploying sophisticated techniques of Information security tools and threat intelligence systems. This involves early identification of the threats, in order to take the response actions that are critical in preventing a large-scale calamity. Containment plans are focused on controlling the diffusion of the incident and minimize its impact whereas eradication focuses on the elimination of the threat and any compromise factors.

The measures taken aim at bringing back normalcy and shortening disruption and outages which are critical in keeping the customers' faith. Even after the incident, the examination of the process streame is significant as it allows identifying the outcomes of the actions taken and the possible ways to enhance the situation. It ensures that the institutions in the society are able to have a continuous learning on how to change their incidents that they encounter and how to improve on their security.

When applied as components to the development of an incident response framework, these components help financial institutions mitigate the effect of cyber threats, minimise disruptions to operations, and meet the laid-down regulatory standards. In today's dynamic technological environment, it is crucial to identify threats and develop initiative incident handling mechanism to prevent leakage of important financial data and loss of clients' trust.

References

1. Bertino, E., & Sandhu, R. (2020). *Database security: Concepts, approaches, and challenges* (2nd ed.). Springer. https://doi.org/10.1007/978-3-030-27042-6
2. Patel, N., Gohil, K., & Chien, C. (2021). *Incident response and management in financial institutions*. Journal of Financial Services Research, 60(2), 145-163. https://doi.org/10.1007/s10693-021-00331-7
3. Chen, X., & Zhao, Y. (2019). *Advanced threat detection in financial systems using machine learning*. IEEE Transactions on Information Forensics and Security, 14(8), 2093-2104. https://doi.org/10.1109/TIFS.2019.2903837
4. Alharkan, I., & Alhaidari, F. (2020). *Strategies for effective containment of cybersecurity incidents*. International Journal of Information Security, 19(4), 455-469. https://doi.org/10.1007/s10207-020-05150-

1
5. Dinh, T., & Nguyen, H. (2022). *Eradication of cyber threats in financial institutions: Best practices and case studies*. IEEE Access, 10, 23654-23668. https://doi.org/10.1109/ACCESS.2022.3156478
6. Ghosh, S., & Sharma, R. (2021). *Post-incident analysis for financial institutions: Lessons learned and future directions*. Computers & Security, 102, 102152. https://doi.org/10.1016/j.cose.2021.102152