**Course: Incident Handling & Response**

**Final Project Report**

**Topic: Unauthorized Access (Software)**

**Name of the Students:**

**Bhudev Nevaniya (100848467)**

**Maisha Khatoon (100899259)**

**Shreeraj Shah (100848468)**

Contents

[Project Report- Unauthorized Access (software) 3](#_Toc132580213)

[Incident Description 3](#_Toc132580214)

[Indicators 4](#_Toc132580215)

[Possible indicators 4](#_Toc132580216)

[Probable indicators 4](#_Toc132580217)

[Definite indicators 4](#_Toc132580218)

[IRP-During an attack 4](#_Toc132580219)

[IRP-after the attack 5](#_Toc132580220)

[IRP-Before an attack 6](#_Toc132580221)

[References 7](#_Toc132580222)

# Project Report- Unauthorized Access (software)

## Incident Description

A recent cyber attack was launched against the well-known financial institution known as XYZ Bank, and it was carried out with the support of a phishing campaign that was professionally constructed. The goal of this attack was to steal sensitive information from the organization that was targeted, and it was successful. The purpose of this attack, which was to steal sensitive information from the target, was completed. It is believed that the perpetrators are members of a skilled hacker gang and that they began the attack by sending phishing emails to employees of XYZ Bank, which appeared to be a legitimate financial institution. This is how the attack was initiated. They were able to collect the employees' personal information by using this method. This theory receives additional support from the fact that the attackers themselves were the ones who sent out the emails. These emails contained harmful attachments that were disguised as important financial records, which encouraged employees who were ignorant of the danger to open the emails. The attachments may have been used to steal sensitive information from the target. The attachments were masked as vital financial records to conceal their true nature. To conceal the true nature of the papers, they were disguised as important financial documents and masked.

After the attachments were accessed, the virus that had been hiding in them began to spread throughout XYZ Bank's internal network. The virus had been hidden within the attachments. As a direct consequence of this vulnerability, the criminals had unrestricted access to both essential information and key systems, which enabled them to continue with their illegal actions. After that point, the criminals continued their spree by stealing information from customers, seizing control of financial transactions, and wreaking havoc on the business's daily operations.

As a result of this attack, there is a considerable likelihood that the ordinary business activities of XYZ Bank will be significantly affected in some important way. This is a possibility that shouldn't be discounted. Theft of customer information may result in significant damage to the company's reputation, which may reduce customers' faith in the company as well as their loyalty to the brand. If there is a breach in the security surrounding financial transactions, cash may be lost, in addition to fines from regulatory organizations and legal responsibilities. If there is a breach in the security surrounding financial transactions, there will be a loss of cash. A slowdown in business activity may result in a decline in productivity in addition to having a negative influence on the organization's current financial situation. In addition, the event may have legal and regulatory repercussions, which would influence XYZ Bank's capacity to comply with the rules and regulations that control the business. These repercussions would have an impact on the ability of XYZ Bank to comply with the rules and regulations that govern the business. The ability of XYZ Bank to stay in compliance with the law would be negatively impacted because of these legal and regulatory ramifications. Because of the legal and regulatory problems, XYZ Bank's capability of adhering to the laws and regulations that govern the company's operations would be negatively harmed.

## Indicators

### Possible indicators

* Phishing scams put employees in jeopardy when they unexpectedly get emails from unknown or questionable sources pretending to be financial companies and sending the emails in the employee's name. These emails are sent in the employee's name. These emails are sent out using the employee's name as the sender. When employees get emails like this one, they put themselves in danger of falling prey to phishing scams that attempt to steal their personal information.
* Emails that contain files or links that demand sensitive information such as login passwords or financial data are a common sort of cyber assault. Other common forms of cyber attack include phishing and spear phishing. Phishing and spear phishing are two further types of cyber attacks that can be carried out. Phishing and the distribution of malicious software are two of the most common types of cyberattacks. The level of sophistication that can be attained in assaults of this kind continues to rise over time.
* Details of any attempt to access the internal network of XYZ Bank that is either unusual or not authorized will have the details of that attempt noted. These details will be logged regardless of whether the attempt was successful or not.

### Probable indicators

* Employees who, after having been tricked by phishing emails, download potentially malicious attachments, or click on dangerous websites without being aware of the risk they are putting themselves in. One common tactic used by hackers is sending emails to potential victims that contain links to phishing websites.
* Claims of shady actions, such as data access patterns that are out of the norm or money deals that were not approved to take place; are some examples of the accusations that have been made.

### Definite indicators

* It has been proven beyond a shadow of a doubt that unauthorized users were able to establish connections to the internal network of XYZ Bank.
* Confirmation that either the data of the customers or the financial transactions of the customers have been tampered with and may have been harmed because of the tampering. Additionally, the customers' experiences may have been negatively impacted because of the tampering. Because of the tampering, the consumers may have encountered disruptions in their service.

## IRP-During an attack

The Incident Response Plan (IRP) developed by XYZ Bank should be implemented without delay. It's imperative to carry out the following steps:

* When an attack is discovered, the compromised machines must be removed from the network promptly to stop it from spreading.
* To facilitate forensic analysis and investigation, all relevant logs, data, and evidence relating to the assault must be kept.
* To organize the reaction, you should call in the incident response team, which includes IT security experts, lawyers and regulators, and top executives.
* The incident response team must first undertake a complete evaluation of the attack to ascertain its breadth, nature, and impact, as well as to locate any affected systems or data.
* Notify the proper parties as soon as possible under legal obligations and company policy, including law enforcement, regulatory bodies, and affected customers.
* To stop the attack from spreading, you must immediately disconnect the compromised machines from the rest of the network.
* Determine the nature and origin of the attack, and collect any relevant data on the attack vector, malware, and potential damage.
* Alert the appropriate parties, such as IT security staff, legal/regulatory representatives, and upper management.
* Put into action the channels and protocols for reporting and coordinating incidents that have already been established.
* Determine the extent, type, and seriousness of the attack by doing a preliminary evaluation.
* Stopping malicious IP addresses from doing additional damage and suspending hacked user accounts are two examples of such mitigations.
* For forensic purposes, call logs, documents, and evidence must be kept.
* Add more layers of security like intrusion detection systems (IDS), firewall rules, and endpoint protection to keep the threat at bay.
* Keep an eye on how the attack is going, recording and archiving each step for later use.
* Report back to upper management and other affected parties on the current incident state, including any foreseeable consequences and expected resolution time.
* Communicate and collaborate with outside crisis response teams, such as local police or private security firms, if needed.
* Check the security of other systems and networks frequently so that flaws can be fixed.
* If a data breach has occurred, you must comply with all applicable laws and regulations regarding the notification, reporting, and handling of sensitive information.
* Be on the lookout for any shifts in the attack and adjust your defenses as needed.
* To better prepare for future incidents, it is important to assess what was learned from this one and revise the IRP accordingly.
* An organization's policy, available resources, and the specifics of the cyber attack will determine the best course of action. To respond to incidents and reduce possible harm, it is essential to have a clearly defined IRP in place that is routinely updated.

## IRP-after the attack

The following steps need to be taken once the attack has ended:

* Vulnerabilities exploited by attackers must be mitigated as soon as possible to prevent further attacks.
* All security precautions should be taken before normal activities may resume, and then the affected systems and operations should be brought back online.
* After an event has occurred, it is important to perform an in-depth analysis of the situation to determine what happened, how effective the reaction was, and how it may be made better in the future.
* Maintain open and regular communication with customers, employees, regulators, and other stakeholders to keep them apprised of the incident's status, its effects, and any preventative measures being done.
* Conduct a thorough post-incident investigation to determine the attack's motivations, the full degree of the damage, and the efficiency of the response.
* The best way to learn about the attackers' TTPs is to review and analyze the forensic evidence gathered at the scene of the incident.
* Examine the compromised infrastructure carefully to find and close any security holes you may have missed.
* Following established recovery methods and backups, bring back online all affected systems and networks.
* Make sure there are no traces of malware or other threats left behind by verifying the restored systems and data.
* Learn from this occurrence by reviewing and updating your security policies, processes, and configurations.
* Employees should be given security awareness training to stress the significance of cybersecurity and each person's part in preventing future attacks.
* Work with your legal and regulatory teams to report the occurrence to the proper authorities and notify affected customers as required by law.
* Keep upper management and interested parties updated on the recovery process and the outcome of the incident response.
* Review the incident response plan (IRP) after it has been implemented, with the incident response team, to see how well it has worked and where it may be improved.
* A complete analysis of the incident's aftermath is necessary to eliminate any lingering dangers and implement preventative measures against future occurrences. It is critical for the organization's cybersecurity posture that the IRP is continuously improved based on post-incident analysis.

## IRP-Before an attack

For XYZ Bank to be fully prepared for any prospective cyber assaults, the following tasks need to be completed by the financial institution:

* Backups of the data should be produced consistently and safely to ensure that the data can be recovered if it is lost as a result of an attack. This will ensure that the data will be able to be recovered. The safety of the backups will be ensured because of this action.
* Making contingency plans for the aftermath of a disaster It is vital to develop comprehensive disaster recovery plans and put them through periodic drills to ensure that normal company operations will continue even in the event of a cyber attack or any other kind of crisis. These plans and drills are essential for ensuring that normal business operations will continue.
* Employee education and training opportunities It is essential to give employees continual education and training courses to educate staff members about the dangers posed by phishing attempts, the significance of examining emails and attachments, and other best practices that are pertinent to information security.
* Establishment of stringent regulations and processes for security It is necessary to implement stringent security standards to provide adequate protection against the risk posed by cyber-attacks. Attacks on a company's computer network have the potential to cause significant harm to both its reputation and its bottom line. These protocols include things like firewalls, intrusion detection systems, antivirus software, and multi-factor authentication, just to name a few examples of what can be found in this area.
* Regular and comprehensive examinations of the security system It is essential to carry out inspections of the security system regularly to locate any flaws or vulnerabilities that may exist.

## References

Lee, J., Lee, Y., Lee, D., Kwon, H., & Shin, D. (2021). Classification of attack types and analysis of attack methods for profiling phishing mail attack groups. *IEEE Access*, *9*, 80866-80872.

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing email detection using natural language processing techniques: a literature survey. *Procedia Computer Science*, *189*, 19-28.

Shankar, A., Shetty, R., & Nath, B. (2019). A review on phishing attacks. *International Journal of Applied Engineering Research*, *14*(9), 2171-2175.

Sahu, K. R., & Dubey, J. (2014). A survey on phishing attacks. *International Journal of Computer Applications*, *88*(10).

Süzen, A. A. (2020). A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem. *International Journal of Computer Network & Information Security*, *12*(1).

Okpa, J. T., Ajah, B. O., & Igbe, J. E. (2020). Rising trend of phishing attacks on corporate organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology*, *14*(2), 460-478.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626.

Nish, A., Naumann, S., & Muir, J. (2020). *Enduring Cyber Threats and Emerging Challenges to the Financial Sector*. Carnegie Endowment for International Peace..