RIZAL TECHNOLOGICAL UNIVERSITY
COLLEGE OF ENGINEERING AND INDUSTRIAL TECHNOLOGY
COMPUTER DEPARTMENT

Information Assurance Security
2nd sem. S.Y. 2022 – 2023

Enhancing Cybersecurity Measures and Protecting Customer Data: A Case Study of Bank of the Philippine Islands (BPI)

CASE STUDY

Introduction:

Effective procedures for handling reports of unauthorized emails aimed at deceiving employees into giving away valuable information are necessary for organizations to maintain their security. Phishing is a common method of gaining access to accounts and other information that is then used in more destructive attacks. One of the most important parts of most large organizations' security plans is to protect employees from such attacks. This often involves teaching employees how to recognize and report phishing attacks and setting up internal procedures to respond quickly to phishing reports. In our case study, we will discuss the important part of cyber security to give awareness to users from being fooled by unauthorized or scammers and how the employees will protect valuable data.

Background:

The Bank of the Philippine Islands, or BPI is off to a rocky start for 2023, as users have flocked to its social media page with complaints of unauthorized transactions on their accounts. While the scale of the problem is still unknown, the amount seems to vary per account, with the common denominator being that the transactions are categorized with the code 0431 Debit Memo. In response to one of the comments, the bank defined it as a general term for all debits made on one's account prior to a system update, and that transaction details will be posted once a system update has been made.

At the time of writing, I was able to access the BPI mobile app, but it's sluggish. There were also no such transactions made on my personal account.BPI acknowledged the issue and stated that some debit transactions from December 30 to 31, 2022, were posted twice and that they are already working to resolve the issue.

Threats and Risks:

These are the possible threats and risks to the information assets involved and how it can impact the organization.

Glitches and System Errors:

Threat: Attackers can take advantage of Internal system glitches or errors in the bank's IT infrastructure that can result in incorrect balances, duplicate transactions, and other transaction-related issues.

Risk: Technical glitches might lead to incorrect transactions, account discrepancies, and financial loss for its customers. Additionally, it can also greatly affect the bank's ability to operate efficiently, lower customer satisfaction, and can also pose doubts in the reliability of the bank's systems. They may also indicate vulnerabilities of the bank's IT infrastructure which can be exploited by malicious actors.

Unauthorized Transactions:

Threat: Attackers conducting unauthorized transactions on customer accounts.

Risk: Unauthorized transactions can result in financial losses for customers and damage to the bank's image as it showed just how weak the bank's authentication mechanisms and security controls are causing to have issues with their customer's trust and money.

Cybersecurity Attacks:

Threat: Attackers will try to trick the bank’s clients and staff into revealing sensitive information or data breaches using various cyberattacks to deceive them and target the bank’s IT infrastructure.

Risk: Cybersecurity attacks might lead to compromised private information as well as login credentials, giving attackers unrestricted access to the customer’s accounts or internal systems. The result of these incidents is financial loss, unauthorized transactions, and potential data breaches.

Lack of Security Awareness:

Threat: Customer and staff’s insufficient information regarding security risks and awareness.

Risk: Without proper awareness, staff as well as customers can fall into victim of phishing attempts or fail to recognize suspicious activities. Customers might also become more easier to be a target of fraudsters because they are more vulnerable to social engineering tactics and so, this increases the overall chances of security breaches to the firm and their own personal accounts as well.

Operational Disruptions:

Threat: Disruptions in the bank's online and mobile app-based facilities, causing inconvenience for customers.

Risk: Operational disruptions can result in customer dissatisfaction, loss of business, and damage to the bank's reputation. Operational disruptions or downtime can indicate flaws in the bank's IT infrastructure or insufficient disaster recovery and business continuity measures which can cause customer dissatisfaction, loss of business and also harm the bank’s reputation as customers will lose their faith in the bank's ability to protect their information and money, leading to customer loss and negative publicity.

Regulatory Compliance:

Threat: Failure to adhere to regulations' standards and requirements for information security and technology risk management.

Risk: Failure to comply can result in fines from the government, harm to one's reputation, and legal ramifications. It could also be a sign of governance and risk management flaws within the bank.

In summary, these threats and risks can have a negative impact on the business in the form of financial losses, legal liabilities, fines from the government, and a decline in customer trust. To have more chances of reducing these risks and further protecting related information assets, the bank must implement robust security measures such as strong authentication methods, regular system updates, personnel training programs, incident response places, and proactive monitoring.

Overview:

The information assets and general security of the Bank of the Philippine Islands (BPI) are subject to a number of threats and vulnerabilities. Incorrect balances, duplicate transactions, and other transaction-related problems can result from glitches and system faults in the bank's IT infrastructure. Customers run the danger of suffering financial losses as a result of unauthorized transactions, which can harm the bank's image. Cybersecurity attackers can also compromise sensitive data can lead to financial loss and unlawful activities. Customers and employees are more susceptible to social engineering tricks and security breaches due to a lack of security knowledge. Furthermore, customer discontent and reputational damage can result from operational disruptions in online and mobile app-based services.

BPI should establish strong security measures to reduce these dangers. Strong authentication procedures, frequent system upgrades, security awareness training programs for employees, incident response plans, and proactive monitoring are all part of this. BPI can improve its security posture, protect customer data, and lessen the likelihood and impact of security incidents by adopting a proactive approach to security, continuously improving security protocols, maintaining open communication with customers during incidents, encouraging employee vigilance, and having a well-defined incident response plan. To avoid negative legal and reputational repercussions, compliance with laws and standards for information security and technological risk management is also essential.

Challenge:

June 2017, when Bank of the Philippine Islands first experienced a glitch in their systems. At that time, some clients complained about internal system errors or unauthorized withdrawals.

January 2023 when another issue was complained against the Bank of the Philippine Islands. The clients of the said bank stated that their ATM transactions done between December 30 and 31, 2022 were posted twice. Some clients complained about money deduction even without transactions in the bank, and some complained about being unable to access the bank's online banking channels to check their banking account.

The specific security challenge faced by BPI was the occurrence of unauthorized transactions on customer accounts, categorized as 0431 Debit Memo. This challenge threatened the security and integrity of customer accounts and raised concerns about the bank's ability to protect customer data.

This issue needs to be addressed since the money of the bank's clients is at risk. The system flaw is concerning because it undermines customers' trust and confidence in the nation's banking system generally and affects the government's goal of increasing financial inclusion in light of a persistent trend toward using digital space for conducting financial transactions. In addition, It was essential to investigate and resolve the issue promptly to mitigate financial losses, maintain the bank's reputation, and ensure the security of customer accounts. If the bank maintains the bank reputation it can continue to encourage more individuals to join and engage in the formal financial sector, which is a crucial factor in supporting sustainable economic growth, banking institutions must assure the safety and security of their clients' hard-earned money.

Solution:

Threat actors are people or organizations that engage in cyberattacks or other criminal acts with the intention of causing harm or stealing confidential data from an institution. They could be driven by personal benefit, political or ideological convictions, or financial gain.

The bank released recommendations on IT risk management and information security management to give BSFIs a thorough framework, a set of guiding principles, and fundamental hygiene practices that they must adhere to in order to safeguard themselves from threat actors.

The bank built a set of methods for identifying system flaws, and it has a framework in place for escalating such incidents based on their seriousness or impact. The bank also formed an incident response team, which is critical in reducing and managing the harm and impact that could result from a potential incident involving information and communication technology. They enhanced their monitoring systems to detect suspicious activities, unauthorized access attempts, and abnormal transaction patterns. This included implementing intrusion detection systems (IDS), security information and event management (SIEM) tools, and log monitoring mechanisms. Aside from that they also implemented two-factor authentication for customer accounts to provide an additional layer of security. This required customers to provide a second verification factor, such as a unique code sent to their mobile devices and their login credentials. Then as for their employees, they conducted regular training sessions and awareness programs for employees to educate them about common cybersecurity threats, phishing techniques, and best practices for data protection. This helped employees recognize and report suspicious activities promptly.

Implementation:

BPI experienced major glitch incidents in June 2017 and January 2023. These incidents resulted in the double-posting of transactions and incorrect balances on customer accounts. BPI took immediate action to address the glitches by shutting down ATMs, online and mobile app-based facilities, and working to reverse the duplicate transactions. The bank resolved the issues promptly. BPI is required by the Bangko Sentral ng Pilipinas (BSP) to implement sound technology and cybersecurity risk management. BPI continuously reviews and improves its banking systems, processes, and controls to prevent recurrence and address any gaps. In 2014, BPI, like other Philippine banks, was mandated by the BSP to shift to Europay Mastercard Visa (EMV) technology. The EMV card system uses microchips instead of magnetic stripes, providing enhanced security and protection against skimming. Communication and Customer Relations: BPI acknowledges the impact of glitches on its customers and maintains open communication channels with them. The bank strives to minimize losses and inconvenience by responding quickly and providing timely updates during incident resolution.

During the process, several challenges occurred including the following. *Inherent Vulnerabilities*, the BSP acknowledges that cybersecurity and technology-related incidents are not completely avoidable due to inherent vulnerabilities in systems, technologies, processes, and people. BPI, like other banks, faces these challenges in ensuring the security of its systems. *Human Errors*, BPI attributed some glitches to human errors. While the bank has implemented layers of control to contain errors and maintain system integrity, the potential for human mistakes remains a challenge.

Overall, BPI has implemented measures such as technology risk management, EMV card system adoption, incident response protocols, and customer communication to enhance security and address challenges associated with glitches and cybersecurity risks.

Results:

The glitches in BPI's systems were attributed to internal data processing errors rather than external threats. BPI ensures that access to its systems and information is strictly limited to internal personnel with a business need to know, minimizing the occurrence of events attributed to outsiders.

The Bangko Sentral ng Pilipinas (BSP), the central bank of the Philippines, monitors incidents in the banking sector and states that incidents related to banking glitches are minimal and within the capability of financial institutions to contain and manage. The BSP emphasizes the importance of implementing sound technology and cybersecurity risk management, as laid down in BSP regulations and guidelines.

BSP issued guidelines on information technology (IT) risk management and enhanced guidelines on information security management to provide a comprehensive framework for banks to protect themselves from cyber threats. The BSP conducts examinations for banks encountering major cyber or disruptive events and applies supervisory enforcement actions to address the root cause and prevent a recurrence.

In line with global best practices, Philippine banks, including BPI, completed the shift to Europay Mastercard Visa (EMV) technology by June 2018. This technology, utilizing microchips instead of magnetic stripes, enhances the security of card transactions and reduces the risk of skimming.

In general, while BPI encountered glitches in its banking systems, the bank took prompt action to resolve the issues and improve its security posture. The incidents have led to ongoing efforts to enhance technology risk and cybersecurity management in the banking sector.

Lessons Learned:

During the process, BPI learned valuable lessons about information security assurance that emphasized the importance of human involvement:

1. **Proactive Approach**: BPI realized the significance of taking a proactive stance towards security. They understood that regular training and awareness programs are crucial to equip employees with the knowledge and skills to mitigate risks and prevent security incidents.
2. **Continuous Improvement**: BPI recognized that security measures must constantly evolve to keep up with the ever-changing landscape of threats and vulnerabilities. By regularly evaluating and improving their security protocols, BPI ensures they stay ahead of potential risks.
3. **Customer Communication**: BPI understood the importance of transparent and timely communication with customers during security incidents. By keeping customers informed about the situation and the steps to address it, BPI can maintain its trust and minimize any potential damage to its reputation.
4. **Employee Vigilance**: BPI acknowledged that employees play a crucial role in maintaining the organization's overall security. They realized the necessity of regular training and awareness programs to keep employees vigilant and capable of effectively identifying and reporting potential threats.
5. **Incident Response Readiness**: BPI realized the value of having a well-defined incident response plan. This plan allows them to respond swiftly and effectively to security incidents, minimizing the impact and potential losses. BPI can maintain a robust security posture by ensuring they are prepared to handle such situations.

By implementing these lessons, BPI can continue strengthening its security measures. They can safeguard customer data and enhance the organization's overall security posture, reducing the likelihood of security incidents and their associated consequences.

References:

https://www.onenews.ph/articles/glitch-hits-bpi-computer-system?fbclid=IwAR3WHd243sSDt5XHBR5uVF5VIDJhJSZ2MiNDxJNEAXWtHb8PsWIXlZC9-JI