IT Protection and Security: MIT 264
Alden A. Quiñones
Activity 7: Data Breach Incident Response

Scenario: A data breach exposed customers' credit card details at your company.

Tasks:

a. List 5 key steps in your incident response plan.

1. Preparation - Before a breach occurs, it is essential to have robust policies, effective tools, and established breach response protocols in place. Regular training should be conducted for security and IT staff to ensure they are well-equipped to handle potential threats and understand their roles during an incident.

2. Identification - Once a breach is suspected, the first step is to confirm the unauthorized access to customer credit card data through system logs, security alerts, or user reports. It is also important to determine the full scope of the incident by identifying which systems, types of data, and users have been affected.

3. Containment - To prevent the breach from escalating, compromised systems should be immediately isolated from the network. This includes disabling any access points or services that may be connected to the breach, limiting further damage or data loss.

4. Eradication - After containment, the focus shifts to removing any malware from the systems, closing known vulnerabilities, and applying necessary patches. A thorough audit of all systems should be conducted to detect and eliminate persistence mechanisms, such as backdoors, that attackers may have installed.

5. Recovery - Once the systems are clean, they should be restored from verified backups to ensure integrity. Continuous monitoring should follow the recovery process to detect any abnormal activity and confirm that the threat has been completely neutralized.

b. Identify teams and individuals who should be involved.

1. Incident Response Team (IRT) - Leads the technical response by investigating the breach, containing the threat, and restoring affected systems.
2. IT and Security Team - Handles the isolation of compromised systems, eradicates threats such as malware, and implements system hardening measures to prevent further attacks.
3. Legal and Compliance Officers - Ensure that AGC complies with applicable data protection laws, particularly the Philippine Data Privacy Act of 2012 (DPA), and international standards like the GDPR if necessary. They are also responsible for breach notification filings with the National Privacy Commission (NPC) and guiding the company’s legal exposure.

4. Executive Management - Makes high-level decisions, approves public statements, allocates resources, and ensures the organization's strategic interests are protected throughout the breach response process.
5. Customer Support Team - Manages communication with affected customers by addressing inquiries, providing guidance on protective measures, and offering reassurance to maintain customer trust.
6. Public Relations - Crafts official public statements and press releases, coordinates with media outlets, and ensures that messaging is transparent, consistent, and aligned with legal and regulatory requirements.

c. How would you communicate this breach to customers?

In the event of a confirmed data breach involving personal information that is likely to pose a real risk of serious harm to affected individuals, AGC must notify customers as soon as possible, ideally within 72 hours from discovery of the breach, in compliance with the Data Privacy Act of 2012. The primary mode of communication should be through email, supplemented by announcements on the official website and, if appropriate, through social media platforms. The notification must acknowledge the breach, express sincere regret, and clearly explain what specific personal information was compromised, such as credit card details. It should describe the measures AGC has taken or will take to contain and mitigate the breach, provide recommended steps for customers to protect themselves such as monitoring their bank statements and changing passwords and offer available support options like free credit monitoring. Finally, the message should reassure customers by highlighting the security enhancements being implemented to prevent future incidents, while ensuring that all communications comply with the guidelines set by the National Privacy Commission.

Like for instance:

Dear Mr. Juan Dela Cruz,

We're writing to inform you that we've recently discovered a data breach at Alden's Group of Companies (AGC) that may have affected your credit card details. We deeply regret this incident and understand the concern it may cause. We've acted quickly to contain the issue and are working with cybersecurity experts to fully investigate. While we work to resolve this, we recommend the following steps to protect yourself:

1. Monitor your credit card statements for any unusual charges.
2. Change your online banking passwords.
3. Contact your bank or credit card provider to report any suspicious activity.

If you have any questions or need assistance, please don't hesitate to reach out to our Customer Support Team at customer.support@agc..com

We apologize for the inconvenience and are working to improve our security to prevent this from happening again.

Thank you for your understanding.

Sincerely,

Alden A. Quiñones
Incident Response Team – Leader
Alden's Group of Companies (AGC)