**Name:** Siman Bitrus Boaz  
**Course:** Cybersecurity

**Fellow ID:** FE/23/64112618A  
 **Date:** 3rd September, 2024.

**ASSIGNMENT**

From the group work on potential risk assessment, pick one potential risk identified by the group and apply the Six Core Cybersecurity Functions on how to protect the asset.

**ATTEMPT**

Customer’s information is an important asset identify by group 3 batch II that could be affect by potential threat. Protecting Customer’s Information by applying the Six Core Cybersecurity Functions of Identify, Protect, Detect, Respond, Recover, and Govern. As a cybersecurity practitioner, safeguarding customer information is very important. Customer's information as an asset is highly sensitive and crucial to maintaining the trust and integrity of the organization. I will attempt an outline on how I would apply the six core cybersecurity functions effectively to secure customer’s information.

1. Identify

The first step in protecting customer information is to identify where this data is stored, processed, and transmitted within the organization's IT infrastructure. I would start by mapping out all systems, databases, and applications that handle customer data. This includes cloud storage, internal servers, and third-party integrations. By conducting a thorough risk assessment, I would identify potential vulnerabilities and threats to this data, such as unauthorized access points, weak encryption methods, or inadequate access controls. Understanding the flow and storage of customer information is essential to prioritize and tailor security measures effectively.

2. Protect

Once the customer information assets are identified, the next step is to implement protective measures. I would ensure that all systems handling customer data are secured through encryption, both in transit and at rest. Access controls would be tightened, with strict role-based access to ensure that only authorized personnel can access sensitive information. Additionally, I would enforce multi-factor authentication (MFA) across all platforms that interact with customer data. Regularly updating and patching systems would be a priority to protect against known vulnerabilities. Implementing data loss prevention (DLP) tools to further safeguard against accidental or malicious data breaches.

3. Detect

Detecting potential threats to customer information is critical in preventing data breaches. I would deploy Security Information and Event Management (SIEM) systems to monitor all network traffic and system logs for any signs of suspicious activity. By setting up specific alerts for unauthorized access attempts, unusual data transfers, or any anomalies in user behaviour, to ensure that potential breaches are detected early. Regular audits of system logs and continuous monitoring of network activity would be key components of this function, allowing for the timely identification of threats.

4. Respond

In the event of a detected threat or breach involving customer information, a swift and effective response is crucial. I would develop and regularly update an incident response plan specifically tailored to data breaches. This plan would include steps to contain the breach, such as isolating affected systems, notifying relevant stakeholders, and beginning investigations to understand the breach's scope and impact. The response would also involve working closely with legal and public relations teams to manage the situation and mitigate reputational damage.

5. Recover

After the breach has been contained, I will focus on recovery. I would ensure that secure backups of customer information are maintained and regularly tested for integrity. So that in the case of a breach, these backups would be used to restore data to a secure state. Recovery efforts would involve analysing the breach to identify and address any security gaps that allowed it to occur. This could include implementing stronger encryption methods, revising access controls, or enhancing network security protocols. The goal of recovery is to restore normal operations quickly while ensuring that similar incidents do not happen in the future.

6. Govern

Governance involves establishing and maintaining security policies and procedures to ensure ongoing protection of customer information. I would work to align the organization’s data protection practices with relevant cybersecurity frameworks and compliance regulations, such as GDPR or CCPA. Regular security audits, training for staff on data protection best practices, and continuous improvement initiatives would be part of this governance process. By fostering a culture of security awareness and adherence to best practices, I would help ensure that customer information remains protected over the long term.

By systematically applying these six core cybersecurity functions of Identify, Protect, Detect, Respond, Recover, and Govern, I would effectively safeguard customer information from potential threats. Each function plays a crucial role in building a comprehensive security strategy that not only protects sensitive data but also ensures the organization's resilience in the face of evolving cybersecurity challenges. This approach would help maintain customer trust, ensure compliance with regulations, and protect the organization from financial and reputational harm.