**Incident Response Plan (IRP) for Apple Incorporation**

Student’s Name

Institutional Affiliation

Date

**Introduction**

Security incidents refer to unexpected events indicating that organizational systems or data have been compromised. Such incidents help to determine whether measures put in place to protect corporate systems have failed. In information technology, a security event involves anything that disrupts the normal functioning of the systems (Shah et al, 2021). A security event is anything that adversely affects system hardware or software. Security incidents are differentiated from security events by the degree of severity. Companies may also use potential risks associated with their systems to determine the difference between security incidents and events (Shah et al, 2021). For example, denial access for one user to system service may indicate a chance for a potential security event. It may also suggest that the system is compromised. If many users are denied access, this may be a severe problem for the organization. Denial access to service for many users may involve a denial-of-service attack classified as a security incident (Shah et al, 2021). This paper presents an Incident Response Plan (IRP) for Apple incorporation, one of the largest employers in the world. It is a company operating in the technology industry. As a result, the company is exposed to many cybersecurity incidents, especially from competitors and hackers seeking to take advantage of its technology resources.

**Security Incidents that may Occur in Apple Incorporation**

**Compromised User Accounts:** A compromised U-M account refers to the account accessed by an unauthorized person to use the account. Cybercriminals target U-M accounts to gain access to the U-M network (Shah et al, 2021). They also aim to gain processing power and storage that can help them create a security incident to the company.

**Denial of Service Attack:** This is a security incident in which the perpetrator seeks to make the company's systems or network resources unavailable to its intended users (Ahmad et al., 2015). Cyber attackers use this type of attack to disrupt the system services connected to the internet temporarily.

**System Intrusion:**Computer intrusions are security incidents that occur when someone tries to access any part of the company's computer system (Ahmad et al., 2015). The intruder uses an automated program to compromise the system's security, crash or slow it down.

**Unauthorized Access to Systems:**This is a security incident that occurs when an unauthorized person gains access to a company's server, website, or computer programs using another person's account. Typically, the attacker gains unauthorized access by guessing a password or username for a Gmail account that is not theirs (Ahmad et al., 2015). They keep guessing the passwords and usernames until they gain access to the systems, creating a security incidence.

**INCIDENT RESPONSE PLAN**

An incident response plan refers to the set of instructions and procedures that help IT staff detect, respond and recover from cybersecurity incidents. These plans help companies address several issues, including data loss, cybercrimes, and service outages that disrupt daily operations. In response to its security incidents, Apple incorporation shall follow several steps illustrated in this plan.

1. **Preparation**

Preparation involves the activities that enable the company to respond to the security incident effectively. The company may use several tools, policies, procedures, governance and communication plans to respond to the security incidents (Ahmad et al., 2015). Apple Incorporation will use some of the security response tools, including endpoint detection and response (EDR), Vulnerability management tools, and security information and management (SEIM) tools. The company may use the following mechanisms to prevent and prepare to respond to security incidents:

**Security training Awareness**: All the personnel in the company should take FBI CJIS security policy. This policy ensures that the company's personnel receive security training awareness. The company requires its personnel to update their training every two years (Shah et al, 2021). Besides, Apple shall require annual security awareness of its personnel provided through Cyber Vista security training software. The training covers the ongoing system threats such as Ransomware, phishing, malware and other threats as they emerge.

**Malware/Spyware Protection:** Apple Inc. should ensure that all information system terminals are fully protected against malware/spyware/antivirus and other malicious attacks. This is a defense mechanism that helps the company to update its systems without end-user interventions (Shah et al, 2021). The end users are denied access to the company's systems; thus, they cannot modify, disable or make any changes to the defense mechanism.

**Firewalls and Intrusion Prevention Devises:** Apple incorporation puts several firewalls and IPD within its networks to provide a necessary defense to the systems. The company's IT department also ensures that all systems are kept up to date and upgraded according to the latest security patches (Shah et al, 2021). This ensures that the company maintains an active backup of the system's latest security configurations.

**Personnel Security Measures**: All Apple Inc. personnel with access to CJI should be accessed, modified and maintained (Angafor et al., 2020). This measure ensures that the company clears its systems to the required security standards as per the FBI security policy.

**Physical security measures:** All locations within the Apple company that house CJI related information systems are secured. Any access to these locations during the response to the security incident is needed to determine the credentials for the person accessing the systems (Angafor et al., 2020). The determination of user credentials shall be achieved under the direct control of the company.

**Patching and Updating:**Organization's systems are regularly updated as new security fixes and patches are released. Any system software or hardware that reaches the end of support life for patching shall be deemed non-compliant software (Angafor et al., 2020). Therefore, the company should replace the non-compliant software as soon as possible to avoid future security threats.

1. **Staffing**

Staffing is the second step taken by the company after the occurrence of the security incident. In this step, the Apple incorporation strives to maintain adequate staff levels. It shall employ a third-party support team to thoroughly investigate each incident and communicate its severity to other company stakeholders (Ahmad et al., 2015). The selected team shall also continue to monitor the tools used to detect new events during the investigations of the current incidents.

1. **Training**

Organizations can maintain: All security incidents only with proper and ongoing training. The continuous improvement of handling security incidents implies that the organization periodically reviews its response processes. Apple Incorporation shall test and translated its response processes into recommendations to make them more effective. All members of the staff will regularly be trained in security awareness and procedures. Training is meant to help the team understand how to report post-incident findings (Ahmad et al., 2015). Proper reporting will help the company to handle the incidents consistently and more appropriately.

1. **Detection and Analysis**

**4.1. Detection**

Detection refers to the process of discovering an incident with security tools or through a notification by an internal or external party regarding the suspected incident. Detection of a security event requires an immediate activation of Interactive Response Technology (IRT) (Shah et.al, 2021). The determination of security incidents may arise from one or several circumstances. The following are some of the means through which detection can occur:

* A security event can be detected through the observations of suspicious activities within Apple incorporation computer systems.
* Apple Inc. may use Intrusion detections and protection devices that alert the company of any unusual port traffic or network.
* The company shall use its trained personnel to review the collected event data as evidence for compromised systems.

4.2. **Analysis**

Apple Company will consistently analyze all incident indicators with the type of the incident. In case of a physical incident, the company shall take appropriate steps to determine the weaknesses in its security monitoring tools, physical security facilities, and security training programs. This will help the company to assess the areas for process change or improvement. For an electronic incident, the company will utilize its IT personnel to perform dynamic and static malicious code analysis. The IT experts will also review the company's information system boundary protections to determine the source of the code. However, these analyses can be performed using automated tools depending on the situation, timeliness, and resource availability.

**Incident Categories**

Apple incorporation will categorize an incident as one of the four levels of severity. The company will determine the severity level of a security incident depending on its effects on the company's financial status and reputation. However, the severity can also be based on the impact on the company's mission and performance. The table below provides a listing of severity levels and the respective definition of each severity level.

**Table 1.0. Severity Levels**

|  |  |
| --- | --- |
| **Severity** | **Description** |
| Low | The incidents with low severity levels have a minimal impact on the company. Such incidents may include e-mail SPAM and an isolated virus infection to the computer systems. |
| Medium | These are the incidents with a significant effect on the company. For example, delayed delivery of an electronic mail or data transfer. |
| High | At this level, the impact of security incidents on the company is severe—for example, disruption of an essential service. |
| Extreme | This level involves incidents where the impact is catastrophic—for example, a complete shutdown of all company’s network services. |

1. **Containment, Eradication, and Recovery**

Containment activities involve the decision-making and application of security incident strategies. Usually, containment activities help the company control the damages caused by a cyberattack (Chen et al., 2014). They also help to cease the attack and reduce the effects of the security incident. In this case, Apple incorporation will require intelligence gathered by the detection and analysis phases of the incident. To contain the attack, the company will first identify the affected host, the malware and its capabilities and monitor the communication channels used by the attacker.

Eradication refers to the company's efforts to remove the latent threats that cause security incidents from the systems. The company shall identify and mitigate all potential vulnerabilities and misconfigurations within its systems (Chen et al., 2014). Recovery efforts for apple incorporation will involve the restoration of the affected systems. This is meant to make the systems carry out their normal operations again after the disastrous event. Recovery efforts are dependent upon the company's type of incident (Chen et al., 2014). Such measures would involve:

* Restoring the compromised systems from the security backups.
* Replacing the compromised files.
* Rebuilding systems from the company's approved baseline.
* Other recovery efforts may include changing passwords, install patches, and increasing network parameters.

1. **Post-Incident Activity**

A post-incident activity occurs after the detection, analysis, commitment, eradication and recovery from the attack. It is one of the essential phases in the company's response to the security incident. Post-incidence activities will involve the reflection, compilation and analysis of the activities that led to the security incident (Chen et al., 2014). These are general actions taken by the company's security response team. The team shall review and document the exact cause of the incident, how the staff dealt with the incident and what information was needed to stop the incident from causing more damage.

**Conclusion**

Security incident response plans are usually dynamic and ever-changing, depending on the organization and the types of security incidences. They provide business organizations with the ability to respond to security incidents for the sources of potential security events. The ability to respond to security incidents is crucial to all organizations, whether small or big. The incident plans provide the organizations with the highest priority for security and safety. However, a proper response to security incidences requires dedication and attention to great detail, which yields satisfaction.

References

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), 717-723.

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game‐based learning: A review of tabletop exercises for cybersecurity incident response training. Security and Privacy, 3(6), e126.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An organizational psychology perspective to examining computer security incident response teams. IEEE Security & Privacy, 12(5), 61-67.

Shah, A. H., Ahmad, A., Maynard, S. B., & Naseer, H. (2021). Enhancing Strategic Information Security Management in Organizations through Information Warfare Practices. arXiv preprint arXiv:2104.07144.