Information Security

Incident Response Guide

Document review and log

Document Owner: (Lead)

Version	Date Modified	Date Approved	Author	Comments
1.0	6/21/2021	6/21/2021	Cowbell	Doc created

Overview

The **(Organization Name)** Incident Response Plan has been created to provide strategy around and effectively manage information security incidents that adversely affect **(Organization Name)** information assets. The **(Organization Name)** Incident Response Plan applies to all stakeholders involved in the Incident Response Plan team, appointed by the lead/owner of the Incident Response Plan.

Roles and Responsibilities

Stakeholder	Responsibility	Contact information
INFORMATION SECURITY		
CISO - Chief Information Security Officer	Strategic/Management lead, oversees technical decisions, and potential financial risk and impact of the incident. Reports to the executive team and board of directors.	Name Email Phone
Incident Response Team Leader	Organizes immediate stakeholders for the IR team, authorizes incidents and escalates the event to CISO/C-Suite level, involved in all stages of a cyber incident. Develops IR plan and guidance, periodically revises IR plan and team. Responsible for identifying, confirming, and evaluating the extent of the	Name Email Phone

	event/incident.	
IT/Security Team Member (create more rows for this category to add all team members)	Responsible for identifying, confirming, and reporting incidents to team and team lead. Take actions to reduce the impact of the incident with approval of the team lead.	Name Email Phone
IT Operations	Controls access to systems and applications. Understands where critical assets are within the organization network. Manages patches, software updates, and any updates to stop a cyber attack from exploiting a vulnerability.	Name Email Phone
External Vendor		
COMPLIANCE		
Legal Counsel		Name Email Phone
Human Resources		Name Email Phone
External Breach and Incident Response Counsel		Name Email Phone
Audit Vendors		Name Email Phone
COMMUNICATIONS		
		Name Email Phone

Incident Response Process and Guidelines

Preparation
Prepare and establish an organizational security policy, initiate a risk assessment, identify sensitive assets, define critical security incidents the response team should focus on, and build the Incident Response Team (IRT).

Identification and assessment
The **(Organization Name)** should monitor IT systems and detect abnormalities and unusual traffic from normal operations and determine whether it indicates a security incident. When the incident is confirmed, collect evidence, establish incident type and severity (the extent of the compromise organization-wide), and document this process.

Containment
Once the intruder or threat is identified, containing the threat is the top priority. Steps should be implemented to guarantee that evidence is not tampered with, this may include restricting access to hardware and software. Depending on the type of incident, devices and systems may need to be shut down, segregated to a local VLAN, or left running in order to perform an investigation. The primary reason for gathering evidence during an incident is to determine the extent of the incident. The collection and preservation of evidence may be used for legal proceedings. Clearly document how all evidence has been collected.

Eradication
Once **(Organization Name)** has contained the threat and collected evidence, the next step should be to remove malware from the affected systems, identify the root cause of the cyber attack, and implement controls to prevent similar attacks from occurring.

Recovery
Start bringing affected systems back online in a safe environment, to prevent further attacks. Start testing, verifying, and monitoring affected systems to ensure they are functioning properly without any unusual activity. Apply any necessary patches and updates to systems found to be vulnerable. Be proactive with the recovery process, including the preparation of backups of critical systems, databases, and data as well as images which preserve settings of operating systems and applications.

Lessons Learned
Perform a retrospective overview of the incident. Have the complete incident documented, continue to investigate the occurrence, try to understand what was done to mitigate the attack, and how can **(Organization Name)** improve the incident response process in the future.

Incident Response Checklist

INCIDENT RESPONSE STEPS	PROCESS	TEAM MEMBER	TIME LOG
Incident Discovery and Confirmation	How did the team first learn of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.).		
	Examine audit logs and security applications for unusual or suspicious account behavior or activities that indicate a potential attack, and confirm attack has transpired.		
	Describe potential attackers, including capabilities, behaviors, and motivations that are known or expected.		
	Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party.		
	Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response.		
	Check for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites in your applications.		

	Assess the scope of the damage and the risk to systems and privileged accounts upon discovery. Check to see if any privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed.		
	Examine your list of information assets to identify which assets may have been compromised. Take note of the assets' integrity as well as the evidence gathered.		
	Diagram the path of the incident/attack to provide an "at-a-glance" view from the initial breach to escalation and movement tracked across the network.		
	Collect meeting notes in a central repository to use in preparing communications with stakeholders.		
	Inform employees regarding discovery.		
	Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools.		
	Potentially share information externally about breach discovery. To improve your chances of catching the attacker, you may choose to hold communications during this phase until the breach has been contained. If so, make sure that it complies with your legal requirements.		
Containment and Continuity	Allow the technical and security team to utilize temporary privileged accounts to quickly access and monitor systems.		
	Evidence must be safeguarded. Before performing any actions that may affect data integrity on the original media,		

	make a backup of any compromised systems as soon as possible.		
	Force multi-factor authentication or peer review to ensure privileges are being used appropriately.		
	Change passwords for all users, service, application, and network accounts.		
	To prevent malicious malware from being distributed by the attacker, increase the sensitivity of application security controls (allowing, denying, and restricting).		
	Remove systems from production or take systems offline if needed.		
	Inform employees regarding breach containment.		
	Analyze, record, and confirm any instances of potential data exfiltration occurrences across the network.		
	Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.).		
Eradication	Close firewall ports and network connections.		
	Test devices and applications to be sure any malicious code is removed.		
	Compare data before and after the incident to ensure systems are reset properly.		
	Inform employees regarding eradication.		

	Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.).		
Recovery	Download and apply security patches.		
	Close network access and reset passwords.		
	Conduct vulnerability analysis.		
	Return any systems that were taken offline to production.		
	Inform employees regarding recovery.		
	Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.).		
Lessons Learned	Review forensic evidence collected.		
	Assess incident cost.		
	Write an Executive Summary of the incident.		
	Report to the executive team and auditors if required..		
	Implement additional training for everyone involved in incident response and all employees.		
	Update incident response plan.		
	Inform employees regarding lessons learned, additional training, etc.		
	Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.).		