

Containment of Network Security Incidents Checklist

Note: Prior to starting the containment of network security incidents checklist, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, if Applicable, Extension:			
<i>Additional Details (If Any):</i>			

Section 3: Checklist for containing unauthorized access incidents	
Actions	Completed
Whether the affected systems are isolated	<input type="checkbox"/>
Whether the affected services are disabled	<input type="checkbox"/>
Whether the attacker's route into the network is eliminated	<input type="checkbox"/>
Whether the user accounts used in an attack are disabled	<input type="checkbox"/>
Whether physical security measures are enhanced	<input type="checkbox"/>
Whether IDS/IPS rules configuration are reviewed and updated to stop the ongoing attack	<input type="checkbox"/>
Whether a network segmentation mechanism is deployed to separate the infected section of the network from others	<input type="checkbox"/>
Whether the identified port is blocked immediately after identifying the suspicious attempts	<input type="checkbox"/>
Whether various network security measures/tools such as firewalls, IDS/IPS, antimalware software, endpoint security solutions, and DLPs are deployed to contain unauthorized access incidents	<input type="checkbox"/>
Whether multi-factor authentication for all user accounts is implemented to thwart repeated compromise	<input type="checkbox"/>
Whether the principle of least privilege is implemented to limit user access permissions	<input type="checkbox"/>
Whether additional configuration settings for vulnerability management, patch management, and access controls are implemented	<input type="checkbox"/>
Whether unwanted permissions from users are removed	<input type="checkbox"/>
Whether the external perimeter of the network is identified and protected by analyzing the net flow traffic	<input type="checkbox"/>

Section 4: Checklist for containing inappropriate usage incidents	
Actions	Completed
Whether all malware-infected systems present in the network are turned off immediately	<input type="checkbox"/>
Whether the ports are filtered, and protocols that are affecting the network are secured	<input type="checkbox"/>
Whether the email server is filtered to block unauthorized emails	<input type="checkbox"/>
Whether URL filtering software and spam filter software are installed on the email server	<input type="checkbox"/>
Whether malicious website URLs are blocked	<input type="checkbox"/>
Whether the user privileges of employee computers and systems are restricted to prevent the installation and spreading of malicious or unwanted programs	<input type="checkbox"/>
Whether the passwords for the misused accounts are changed and activities of the users involved are tracked to determine whether the incident was intentional	<input type="checkbox"/>
Whether the compromised user's account and email access are disabled	<input type="checkbox"/>
Whether communication with the external network and suspicious IP addresses is blocked	<input type="checkbox"/>
Whether the compromised systems or network services are isolated	<input type="checkbox"/>
Whether the evidence is acquired, preserved, secured, and documented	<input type="checkbox"/>
Whether the firewall rulesets are configured to block malicious traffic and protect the network	<input type="checkbox"/>

Section 5: Checklist for containing DoS/DDoS incidents	
Actions	Completed
Whether additional bandwidth is provided to the network devices and the capacity of the servers is increased to absorb the attack	<input type="checkbox"/>
Whether the traffic is diverted by redirecting the URLs and requests to similar servers placed at other locations or using cloud scrubbing services with backup resources to divert the traffic	<input type="checkbox"/>
Whether the critical services are identified and then customized the network, systems, and application designs to cut down the noncritical services	<input type="checkbox"/>
Whether automated tools, such as advanced firewall and IDS solutions are deployed to block the attacks	<input type="checkbox"/>
Whether all services are shut down until an attack has subsided	<input type="checkbox"/>
Whether the team used the load balancing technique appropriately for mitigating the DoS/DDoS attack effect	<input type="checkbox"/>
Whether routers are set to access a server with a logic that throttles incoming traffic levels to be safe for the server	<input type="checkbox"/>
Whether the IH&R team implemented the drop requests technique to minimize the effect of DoS/DDoS attack	<input type="checkbox"/>

Section 6: Checklist for containing wireless network security incidents	
Actions	Completed
Whether the wireless access/ SSID broadcasting is disabled until the intrusion is detected	<input type="checkbox"/>
Whether wireless access is used only in case of crucial business needs	<input type="checkbox"/>
Whether credential or password security protocols such as WPA3 on wireless devices are enabled and keys are changed at regular intervals	<input type="checkbox"/>
Whether the devices connected to the victim's AP are checked properly for traces of an attack	<input type="checkbox"/>
Whether the passwords of all devices across the organization are changed	<input type="checkbox"/>
Whether the WAP devices are updated, restoring the default settings and privileges	<input type="checkbox"/>
Whether the attacker details are identified, such as IP address and MAC address, and the devices used for the attack are blocked	<input type="checkbox"/>
Whether the authorized user devices are whitelisted so that no other devices can connect to the access points	<input type="checkbox"/>
Whether the suspicious IP addresses are blacklisted to deny access	<input type="checkbox"/>
Whether additional security measures are implemented that are more difficult to compromise	<input type="checkbox"/>
Whether the evidence is documented and preserved for investigation	<input type="checkbox"/>
Whether the MAC address filtering is configured on every network	<input type="checkbox"/>
Whether the suspected privileges on the router are turned off for wireless configuration settings	<input type="checkbox"/>
Whether the URH security tool is used for wireless protocol investigation	<input type="checkbox"/>
Whether the wireless router's default configuration settings are changed	<input type="checkbox"/>
Whether the upstream ethernet switch port is disabled to break the connection immediately	<input type="checkbox"/>
Whether the WIPS is used to disconnect authorized users from rogue APs and contain rogue devices from the WLAN	<input type="checkbox"/>
Whether filters are used for all outbound routing protocol traffic, CDP, and any unused non-IP based protocols	<input type="checkbox"/>