

Containment of Email Security Incidents Checklist

Note: Prior to starting the containment of email security incidents, 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:			

Section 3: Checklist for Containing Email Security Incidents	
Actions	Completed
Whether the targeted system is isolated from the functional network immediately after receiving the incident reports.	<input type="checkbox"/>
Whether the users or complainants are interviewed about the email incident to determine the details of the attack and actions taken by the user.	<input type="checkbox"/>
Whether the user had downloaded the attachment, clicked the link, provided the requested information, and so on.	<input type="checkbox"/>
Whether the information is gathered about the incident, such as the type of email attack, impact, and losses.	<input type="checkbox"/>
Whether behavior analysis is performed to collect further details of the email by opening the links provided in the email in a sandboxed environment.	<input type="checkbox"/>
Whether the source of the email is identified and verified its authenticity.	<input type="checkbox"/>
Collect complete details about the email, such as its header information, including the source of the email and IP address.	<input type="checkbox"/>
Whether an investigation is performed on the email by analyzing the URL, attachments, domain names, IP addresses, and other obtained details.	<input type="checkbox"/>
Whether the malicious links and IP addresses are reported and blocked on the servers, network devices, and across all security solutions.	<input type="checkbox"/>
Check whether the attachments sent through an email contain malicious code, by opening and downloading them in a sandboxed environment.	<input type="checkbox"/>
Check whether the email contains malicious programs and perform the malware incident handling process.	<input type="checkbox"/>
Whether spam and phishing emails are reported to the service providers.	<input type="checkbox"/>
Contain the impact of the email on other employees by identifying key objectives in the mail and implementing filters to block similar signature mail.	<input type="checkbox"/>

Check the firewall logs to identify suspicious IP addresses and URLs.	<input type="checkbox"/>
Check the DNS logs as certain attackers hide their identity through frequent IP spoofing.	<input type="checkbox"/>
Ensure to analyze and verify the DHCP logs to identify the hosts associated with the suspicious IP addresses.	<input type="checkbox"/>
Ensure to analyze the organization's mail server logs to obtain additional information about the email attack, such as the number of victim systems, message IDs, and IP addresses.	<input type="checkbox"/>
Whether the passwords and other sensitive information for affected email accounts and systems are changed.	<input type="checkbox"/>
Whether all the other active sessions related to the email from the victimized system are identified and closed.	<input type="checkbox"/>
Check whether the unread phishing emails present in the queue for all employees are deleted.	<input type="checkbox"/>
Scan the affected systems using anti-virus or anti-malware software.	<input type="checkbox"/>
Check whether the email security software is updated.	<input type="checkbox"/>
Check whether automatic email forwarding to remote domains is prevented.	<input type="checkbox"/>
Check whether two-factor authentication is enabled for all employees.	<input type="checkbox"/>
Check whether the mailbox auditing feature is enabled.	<input type="checkbox"/>