

# Incident Containment Checklist

The main purpose of this containment checklist is to control the effects of the attack as soon as possible and to maintain business continuity. The IH&R team must adhere to the following checklist to properly contain an incident in an organization:

Security Incident Containment	
<input type="checkbox"/>	Whether the team isolated the affected systems from the non-affected systems
<input type="checkbox"/>	Whether appropriate containment steps are taken by the team for isolation
<input type="checkbox"/>	Whether the team created backups for all the critical data
<input type="checkbox"/>	Whether the team sent the copies of the infected systems to the forensics team for further analysis
<input type="checkbox"/>	Whether the team removed all threats from the infected systems
<input type="checkbox"/>	Whether the team changed the passwords of all infected systems and accounts
<input type="checkbox"/>	Whether the team maintained proper documentation for all actions
<input type="checkbox"/>	Whether the team followed standard procedures and policies during the containment process
<input type="checkbox"/>	Whether the team ensured that containment strategies adhered to the regulatory compliance frameworks
<input type="checkbox"/>	Whether the team implemented multi-factor authentication to thwart a repeat compromise
<input type="checkbox"/>	Whether the team included threat intelligence during the containment process for effectiveness
<input type="checkbox"/>	Whether the team disabled the compromised system services
<input type="checkbox"/>	Whether the team implemented standard procedures such as using IDS, latest antivirus, etc. to trace the intruders easily and avoid further damages