Infocyte

If they try it, we'll stop it.

INCIDENT RESPONSE PLAN CHECKLIST

A CHECKLIST OF KEY COMPONENTS FOR YOUR CYBERSECURITY INCIDENT RESPONSE PLAN.

ELEMENT	ACTION/DETAIL	STATUS	
BEFORE AN INCIDENT OCCURS			
Asset Discovery	Know what assets we must protect. Conduct an asset discovery scan and identify mission critical data and IT assets	Yes	No
Assessment	Conduct a compromise/risk assessment to identify likely risks and prioritize areas of concern. Understand the potential impact of a cybersecurity incident.	Yes	No
Response Team	Identify the key members of the response team and their backups (internal and external) and ensure that they know their roles and responsibilities.	Yes	No
Authority	Appoint an IR leader. Define when to activate the plan and establish authority to take actions, such as shutting down resources and notifying law enforcement.	Yes	No
Stakeholders	Identify stakeholders who must be notified and kept apprised throughout the incident. Stakeholders can be external as well as internal.	Yes	No
Communications	Establish clear plan: who must be notified and when. Regulatory requirements may dictate mandatory notices. Define PR plan to keep external parties informed.	Yes	No
External Contacts	Secure cyber insurance, if needed. Arrange IR contracts in advance if you lack sufficient internal resources.	Yes	No
Test Your IR Plan	Test IR plan regularly via tabletop exercises, simulations, or actual incidents. Run scenarios based on risk assessment. Update IR plan to reflect lessons learned.	Yes	No
Business Continuity	Coordinate IR plan with business continuity plan to ensure operational disruption caused by a cyber incident is addressed consistently with the continuity plan.	Yes	No
Training and Tools	Ensure your incident response team has the necessary training and tools to properly respond to security events and perform their designated roles.	Yes	No
Executive Participation	Get executive buy-in and approval of the plan.	Yes	No
Contact List	Keep an updated contact list of all IR plan participants and designated backups. ID alternate means of communication in the event that email, VoIP, etc. are down.	Yes	No

ELEMENT	ACTION/DETAIL	STATUS	
DURING A SECURITY INCIDENT			
Scope	Assess the scope and severity of the incident using alerts, sensor telemetry and by conducting active forensic triage of potentially impacted hosts. Determine if an incident should be declared and activate the incident response plan.	Yes	No
Contain	Neutralize the threat's access and any active malicious processes. This may require isolating compromised hosts, disabling stolen accounts, and/or locking down network access at the perimeter.	Yes	No
Investigate	Gather evidence from impacted hosts and network sources. Determine attack timeline, conduct root cause analysis, and identify exploited gaps. Recommend enlisting the help of a skilled (and licensed) forensic investigator.	Yes	No
AFTER INCIDENT RESOLUTION			
Post Incident Evaluation	Turn the final investigation and after-action report into action items. Address any identified gaps and implement lessons learned to reduce future response time.	Yes	No

Do you need help creating an IR plan?

Email **sales@infocyte.com** to contact our incident response experts to discuss building an IR plan for your organization.

ABOUT INFOCYTE

Founded by the leaders of the United States Air Force Cyber Incident Response Team (AFCIRT), Infocyte is the globally trusted leader in proactive threat detection and incident response. The world's leading security and incident response companies use Infocyte's platform to proactively detect and respond to vulnerabilities and threats within their customers' endpoints, data centers, and cloud environments. Infocyte's team and partner ecosystem help organizations maintain compliance, stop ransomware and account takeover, reduce risk, optimize security operations, and scale security teams. Infocyte is the faster, simpler, smarter way to detect and orchestrate response to sophisticated threats. Learn more at infocyte.com or follow us on Twitter @InfocyteInc.