Infocyte

INFOCYTE / INCIDENT RESPONSE RESOURCES

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
Risk 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 response operation. 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. Establish when to enlist support if an incident occurs.	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		
Containment / Eradication	Establish effective means to isolate and contain incident to minimize damage. Eradicate residual artifacts to restore system(s) to an operable, secure state.	Yes No
Incident Event Log	Keep an incident event log to track and review pertinent information, such as how the incident was identified, assets affected, business operations impact, etc.	Yes No
Forensic Evidence	Capture and preserve forensic evidence to determine scope of impact and how incident evolved. Evidence may be needed if criminal prosecution is warranted.	Yes No
AFTER INCIDENT RESOLUTION		
Post Incident Evaluation	Following an incident, conduct a thorough review to determine what went well and what didn't. Update the incident response plan to reflect lessons learned.	Yes No

NEED HELP CREATING AN IR PLAN?

Email sales@infocyte.com to contact an incident response expert and we'll help you build an IR plan for your organization.

Infocyte

ABOUT INFOCYTE

Developed by former U.S. Air Force cybersecurity officers, Infocyte's forensics-based threat detection and incident response platform discovers the post-compromise activity of hidden cyber attackers and malware that have bypassed other defenses. The company's unique approach to security reduces attacker dwell time to help organizations and independent assessors defend networks and critical information.

CORPORATE HEADQUARTERS

Infocyte, Inc.
3801 North Capital of Texas Hwy
Suite D-120
Austin, TX 78746

(844) 463-6298
sales@infocyte.com
www.infocyte.com

REDUCE RISK, MAINTAIN COMPLIANCE, STREAMLINE SECURITY OPERATIONS AND RESPOND FASTER WITH INFOCYTE.

START YOUR FREE TRIAL

Discover why Infocyte is leader in proactive threat and vulnerability detection, on-demand incident response, and instant compromise assessments.

infocyte.com/trial