CHECKLIST

Third-Party Incident Response

Security Scorecard

No matter the size, region, industry, or revenue, every organization needs a straightforward methodology for tracking supply chain risk indicators and building an incident timeline.

The SecurityScorecard MAX team created this checklist to ensure that your organization has a proactive plan in place to immediately respond to and mitigate supply chain incidents.

Step 1: Preparation

Third-Party Risk Management:

- [ ] **Create an inventory of third-party vendors:**
  - [ ] What access to data does this vendor have?
  - [ ] What system integrations do we share with this vendor?
  - [ ] If this vendor was unable to operate, how would our business be affected?
- [ ] **Conduct risk assessments of critical third parties:**
  - [ ] Business criticality risk
  - [ ] Cybersecurity assessment (are they protecting our data?)
- [ ] **Implement contractual clauses requiring incident reporting and cooperation.**

"It takes an organization 69 days on average to contain a breach. Companies that contain a breach in less than 30 days save more than $1 million."

– IBM

Internal Incident Response Plan:

- [ ] **Create clearly defined roles and responsibilities for incident response team members:**
  - [ ] Who is our communication point with the vendor?
  - [ ] What is the approval path for communication with the vendor?
- [ ] **Build communication protocols for internal and external stakeholders:**
  - [ ] Do we have a communication plan?
  - [ ] Do we have communications ready in advance for a faster response?
- [ ] **Establish procedures for incident classification, containment, eradication, recovery, and post-incident review:**
  - [ ] What steps does our organization need to take to secure our environment and our data regarding this vendor's breach?
  - [ ] Do we need legal involvement?
  - [ ] How can we help the vendor with the containment of the incident?
  - [ ] Test your organization's incident preparedness with tabletop exercises and hands-on, scenario-based training

Step 2: Detection and Analysis

Incident Identification:

- [ ] **Monitor for potential indicators of compromise (IOCs) from third-party systems.**
- [ ] **Investigate alerts or reports from the third party or internal systems.**
- [ ] **Evaluate the potential impact of the incident on your organization's data and systems.**

Incident Analysis:

- [ ] **Determine the nature and scope of the incident.**
- [ ] **Identify affected systems and data within your organization.**
- [ ] **Assess the potential risks associated with the incident.**

Step 3: Containment

- [ ] Isolate affected systems and data to prevent further compromise.
- [ ] Implement mitigation strategies based on the nature of the incident.
- [ ] Revoke access privileges for compromised third-party accounts.

Step 4: Eradication

- [ ] Identify and remove the root cause of the incident within your systems.
- [ ] Work with the third party to eradicate the threat from their environment.

Step 5: Recovery

- [ ] Restore affected systems and data from backups.
- [ ] Implement recovery procedures to resume normal operations.

SecurityScorecard MAX is the next evolution of supply chain cyber risk management and is laser-focused on delivering business and cybersecurity outcomes. MAX leverages AI, risk & threat telemetry, and elite cybersecurity experts to effectively improve the cyber-security posture of your supply chain.

> *"All of my incident response in 2024 was because of third parties."*
>
> – Healthcare VP of Enterprise Cybersecurity

Step 6: Closure and Lessons Learned

Lessons Learned:

- [ ] Conduct a post-incident review to identify areas for improvement.
- [ ] Update internal incident response plans and procedures.
- [ ] Evaluate the effectiveness of third-party risk management strategies.

Third-Party Remediation:

- [ ] Work with the third party to implement corrective actions to prevent future incidents.
- [ ] Re-evaluate the risk posture of the third party based on their response.

Documentation:

- [ ] Maintain comprehensive documentation of all incident response activities.
- [ ] Include details about the incident, containment, eradication, and recovery efforts.
- [ ] Document communication records with internal and external stakeholders.

Contact SecurityScorecard today to learn more.

securityscorecard.com/company/contact-us
info@securityscorecard.io
United States: (800) 682-1701
International: +1 (646) 809-2166