CIMTK: Third-Party/Supply Chain Incident Management Plan

SANS CYBERSECURITY LEADERSHIP

Created by Steve Armstrong-Godwin, author of
LDR553: Cyber Incident Management | **sans.org/ldr553**

Supply chain breaches differ from in-house incidents in that you won't have a full picture of the breach or access to the systems under investigation. Due to this, you should prepare a plan that will help you understand your risks and their potential future impacts.

This cheat sheet's framework will kick-start your planning so you can scope your organization's incident management plan, understand your exposure as you prepare, and brief your team in the case of a supply chain attack.

CONFIRM	Confirm the claim
IDENTIFY	Identify the timeframe
RESEARCH	Research the relationship
ASSESS	Assess the immediate direct impact
INVESTIGATE	Investigate the current and historic indirect impacts
CONSIDER	Consider disabling/isolating of the third-party to reduce ongoing risk
COMMUNICATE	Plan briefings for your customers, staff, or regulators based upon known facts

CIMTK: Third-Party/Supply Chain Incident Management Plan

SANS CYBERSECURITY LEADERSHIP

Created by Steve Armstrong-Godwin, author of
LDR553: Cyber Incident Management | sans.org/ldr553

CONFIRM REPORTS (VIA)

- Their website
- General news sites
- Third-party contract sponsor
- Your legal team
- National CERT

IDENTIFY (ASK THIRD-PARTY)

- When the attack started
- When and how it was detected
- What slowed detection (evasive techniques)
- When they declared the incident
- Who is supporting/augmenting them
- When it went/will go public
- What the cadence is for updates
- What the suspected attacker's intent is
- If there were shareable indicators of compromise

RESEARCH (INTERNALLY)

- What they do for us; are they critical?
- Do they access/process customer/sensitive data?
- How integrated are they?
- Who owns the relationship?
- Is their service remote or on-prem?
- What logs/visibility do we have?
- Can we swap in another provider?
- Do we have an effective isolation plan?
- If it went badly, how bad could it get?

ASSESS THE IMPACT

- How could their access be abused?
- Did their attacker compromise us too?
- Do they access our customer's data?
- Do they support key service availability components?
- Have they covertly added more admin accounts?
- What distinguishes third-party from attacker?
- Did they access/steal or change our data?
- How long to review activity from start of their hack?

INVESTIGATE

- What access does the third-party have now?
- What access have they had since their breach?
- Could they have reconnaissanced the network?
- Could they access internal-config docs?
- Have they enumerated systems?
- What changes were made since their breach?
- What are their reporting requirements and escalation path?

CONSIDER

- What level of incident could this become?
- Ongoing risk from their continued access
- Do you block their access?
- Do you block their domain?
- Ensure impacted team are aware
- Continue technical briefings
- Are your detections sufficient?
- Do you need more support?

COMMUNICATE

- Our staff, execs, board
- Our customers
- Our investors
- The general public
- Do not overshare details
- Don't out the third-party
- Be as open as possible but brief

SANS | GIAC CERTIFICATIONS