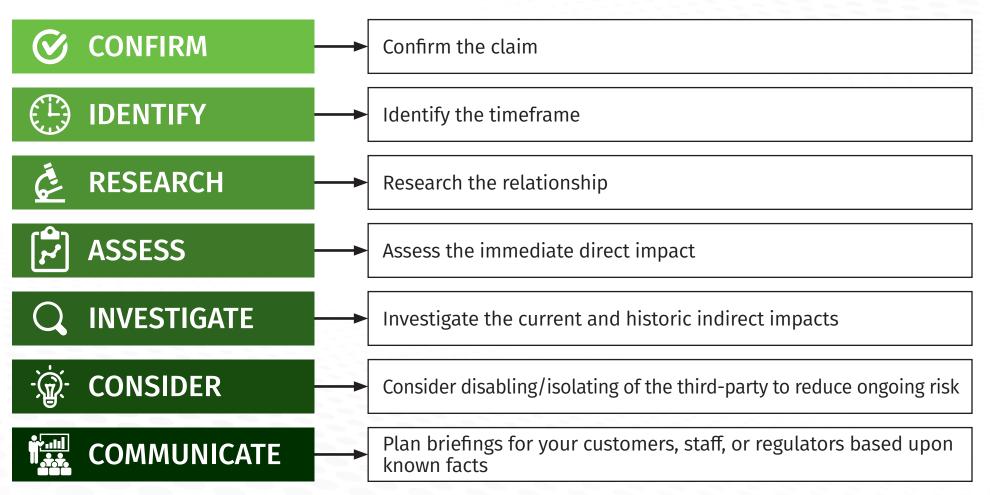
CIMTK: Third-Party/Supply Chain Incident Management Plan



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.



CIMTK: Third-Party/Supply Chain Incident Management Plan



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

<u>ج</u> 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?

		-ଲ୍ରୁ- CONSIDER	COMMUNICATE
	• What access does the third-party	• What level of incident could this become?	• Our staff, execs, board
	have now?		Our customers
	 What access have they had since their breach? 	 Ongoing risk from their continued access 	Our investors
• Could they hav			The general public
	Could they have reconnaissanced	• Do you block their access?	 Do not overshare details Don't out the third-party Be as open as possible but brief
	the network?	 Do you block their domain? 	
	 Could they access internal-config docs? 	• Ensure impacted team are aware	
	• Have they enumerated systems?	Continue technical briefings	
	· ·	 Are your detections sufficient? 	
	 What changes were made since their breach? 	Do you need more support?	
	 What are their reporting requirements and escalation path? 		
	equilibrito una cocatation patin		

