CISO PLAYBOOK:

Third-Party Cyber Incident Response

- ✓ Operationalize incident response
- ✓ Document communication plans
- ✓ Implement best practices

At least **29% of breaches** have third-party attack vectors.

SecurityScorecard Global Third-Party Breach Report, 2024

SecurityScorecard

Introduction

During recent customer tabletop exercises (TTX), it became clear that many companies need a methodology for tracking supply chain risk indicators and building an incident timeline. The SecurityScorecard MAX team created this playbook to provide actionable steps on how supply chain incidents should be handled that are simple to implement and could be immediately used by cybersecurity practitioners.

As cited by the new SEC cybersecurity incident disclosure requirements, SecurityScorecard research identified:

IBM:

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.

98% of organizations have a relationship with a third party that has been breached.

SecurityScorecard & Cynetia Institue Research, 2023

A ransomware goldmine: Supply chain cyber risk

In today's interconnected digital ecosystem, supply chain cyber risk presents a growing threat that spreads like a digital forest fire. Reflecting on history, the Great Fire of London serves as a reminder of the far-reaching consequences that can arise from a single accident. Starting in a humble baker's shop, the fire engulfed the homes of an estimated 70,000 out of the city's 80,000 inhabitants. Fueled by timber construction and strong winds, the fire ravaged the medieval City of London, leaving widespread devastation.

Similarly, in today's cloud-driven business landscape, heavy reliance on a few major vendors like Microsoft, Google, and AWS is the norm. SaaS applications managing comprehensive employee HR data, such as Workday, are common. And, beneath the surface, lies a web of interconnected relationships with fourth-party tools such as JetBrains, Chef, Atlassian, GitHub, and SolarWinds.

Microsoft was using SolarWinds Orion during the SolarWinds Sunburst attack – one of history's largest supply chain attacks. The attackers had access to Microsoft's systems for an extensive amount of time. As CISOs, we always like to find the 'learning nugget' from a breach. Looking back, the security score for SolarWinds at the time was a C+. What if the industry pressed for better scores and security practices from SolarWinds at the time? Could some of the catastrophic impact have been mitigated?

Business benefits of incident response

Limit the financial impact of a cyber attack from creating further damage that results in downtime and lost customers

Respond faster with a team who has expertise in investigating high-profile events around the world, in addition to working with Federal Agencies and specialized military units

Gain board-level visibility into your organization's readiness to respond to a cyber attack

Supply chain visibility is mission-critical

The first line of defense against a supply chain cyber attack comes in the form of prevention. No defense is perfect, however, and even the best forms of protection are subject to a breach. This is where incident response comes in.

Incident response plans must be developed well before a threat because every second counts when a breach is actively occurring. Attacks can wreak more and more havoc with each passing moment, costing thousands of dollars and compromising critical data. The sooner it is stopped, the smaller the fallout.

Extending cybersecurity through the full vendor ecosystem

This is amplified when taking the supply chain and vendor ecosystem of an organization into consideration. It is imperative to have visibility into the critical vendors you are working with that have access to sensitive business and customer information. Taking this one step further, an organization should also consider the vendors of your third parties. Do they also have access to sensitive information that can lead to business interruption or financial and brand reputation loss if that data gets into the wrong hands? As you can see, these questions show the importance of understanding your full vendor ecosystem, including third-party, fourth-party, and nth party vendors, as well as what products and software they are using. This information, combined with the right threat intelligence and third party cyber risk monitoring program is an important and critical step in understanding when one of your vendors gets breached.

Top 10 questions for vendors

1. How do you protect the data you collect, process, and store, both at rest and in transit?
2. What access control measures do you have in place to ensure that only authorized individuals have access to sensitive information?
3. Can you describe your incident response plan?
4. How do you assess and manage the security of third-party vendors you may use?
5. Do you provide regular security training for your employees as well as background checks on new hires?
6. How do you ensure your systems are up to date with the latest security patches?
7. What physical security measures are in place at your offices and/or data centers?
8. Have you experienced any data breaches or security incidents in the past 12 months?
9. Do you conduct regular security testing, such as penetration testing and vulnerability assessments, to identify and remediate potential security weaknesses?
10. Are you compliant with relevant regulations and standards (e.g., GDPR, HIPAA, SOC 2)?

What happens when you do have a supply chain cyber incident? How do you put your plan in action?

Operationalizing an incident response plan is crucial for effectively responding to cybersecurity incidents when they occur. While a well-defined plan is essential, putting it into action requires careful coordination, rapid decision-making, and effective execution.

This section explores step-by-step procedures for transforming an incident response plan framework into practical measures during a real-world incident. From initiating the incident response team to preserving evidence, containing the incident, and involving external resources, the key steps in operationalizing the incident response plan to mitigate and manage cybersecurity incidents will be outlined.

When responding to a cybersecurity incident, the initial steps to take should include:

- **Activate the Incident Response team:** Activate the incident response team or designated personnel responsible for managing and coordinating the response effort.
- **Assess the situation:** Gather relevant information about the incident, including the nature and scope of the incident (was it via the organization's own attack surface, or identified through a third-party vendor), affected systems or assets, potential impact on the organization, and any suspicious activities including indicators of compromise (IOCs).
- **Containment:** Immediately contain the incident and prevent further damage or unauthorized access. This may involve isolating affected systems or deactivating compromised accounts or services.
- **Notification:** Notify key stakeholders, including senior management, IT personnel, legal counsel, and relevant business units, about the incident and the ongoing response efforts.
- **Preserve evidence:** Preserve evidence related to the incident, such as system logs, network traffic data, and any other relevant artifacts, to support forensic analysis and potential legal proceedings.
- **Invoke response plan:** Follow the organization's incident response plan or established procedures to guide the response effort.
- **Engage external resources:** If necessary, engage external resources, such as incident response consultants or forensic investigators, to assist with the investigation and containment efforts.

- **Communicate internally and externally:** Maintain clear and timely communication with internal stakeholders, including employees, customers, and partners, to inform them about the incident and any potential impacts on operations or services. Also, consider any regulatory or legal reporting requirements for external communication.
- **Mitigation and recovery:** Implement mitigation measures to address vulnerabilities or weaknesses exploited in the incident, restore affected systems or services to normal operation, and prevent similar incidents from occurring in the future.
- **Documentation and lessons learned:** Document all actions taken during the incident response process, including decisions made, actions taken, and outcomes. Conduct a post-incident review to identify lessons learned and areas for improvement.

As highlighted above, invoking the response plan is critical to the overall process. Each phase plays a crucial role in mitigating the impact of security incidents, restoring normal operations, and continuously improving the organization’s incident response capabilities for future events.

Here are the key elements for each phase in detail.

1 Preparation

The Information Security Team will continue to develop and enhance its information security policies, plans, and processes. These will be regularly tested, and assessments of emerging threats and risks will be incorporated into future iterations.

2 Identification

Monitor IT systems to detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything. Inform organizational leadership of suspected incidents.

3 Containment

Perform short-term containment, for example, by isolating the network segment under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production while rebuilding clean systems.

4 Eradication

Remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

5 Recovery

Bring affected production systems back online carefully, to prevent additional attacks. Test, verify, and monitor affected systems to ensure they are back to regular activity.

6 Closure and lessons learned

Perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it, and whether anything in the incident response process could be improved.

Supply chain cyber incident communications

For vendors, communicating promptly and effectively with customers after an incident is crucial to maintain trust.

The information a third party shares about a breach often depends on the terms outlined in the contract, including specific clauses related to breach notification. These clauses may dictate the timeframe for notification and the language used, distinguishing between an 'incident' and a 'breach'. Clear and timely communication is important to increase transparency and trust across the digital ecosystem.

Best practices and real-world examples

As we all know, despite the best planning and preventive measures, breaches are still possible. Incident response is crucial in promptly addressing breaches by implementing real-time alerts and predefined steps to minimize damage, protect data, and restore network security. Effective incident response plans must be established proactively to ensure swift action during an active breach, as every moment counts in mitigating potential damage and financial losses while safeguarding critical data.

Companies should expect their partner to send a general Q&A about the incident:

- What happened?
- How did it happen?
- Why did it happen?
- What control failures occurred?
- Who and how sophisticated were the hackers?
- What will prevent it from happening again?

Each incident and organizational relationship is distinct, yet certain principles like transparency and open communication serve as vital guidelines for exchanging incident information.

Other incident response best practices include:

Ensure you have someone on the incident response team certified to take legally defensible forensic images. This ensures that digital evidence obtained during investigations is collected in a manner that adheres to legal standards and can be presented in court if necessary. This certification demonstrates proficiency in handling and preserving digital evidence, maintaining its integrity and authenticity throughout the investigative process. Additionally, it enhances the credibility of the evidence and the overall investigation, reducing the risk of challenges to its admissibility or validity. Ultimately, having certified personnel proficient in forensic imaging strengthens the security team's ability to conduct thorough and legally sound investigations, improving the organization's overall cybersecurity posture.

Don't treat your EDR as the sole solution for preventing security incidents and breaches.

While EDR systems are valuable tools for detecting and responding to endpoint threats, they should be part of a broader cybersecurity strategy that includes multiple layers of defense, proactive threat hunting, and ongoing security assessments.

- **Limited scope.** EDR solutions can have a limited scope. They primarily focus on detecting and responding to threats at the endpoint level and may not provide comprehensive coverage across all aspects of an organization's network or infrastructure.

- **False sense of security.** Relying solely on an EDR system can create a false sense of security, leading to complacency among security teams. Threat actors continuously evolve their TTPs and seek new ways to bypass or evade EDR defenses.

- **Potential for advanced threats.** Sophisticated and targeted attacks, such as zero-day exploits or advanced persistent threats (APTs), may bypass traditional EDR defenses. These threats often require a multi-layered security approach that includes proactive threat hunting and threat intelligence beyond what EDR solutions offer.

Don't be overly reliant on tools, alerts, and automation. Security tools, alerts, and automation play a crucial role in modern cybersecurity operations. Still, they should be complemented by human expertise, contextual understanding, and a holistic security strategy that includes proactive threat hunting, continuous monitoring, and ongoing security awareness training.

Here are other best practices that should be incorporated into incident response plans:
https://securityscorecard.com/blog/6-incident-response-best-practices-you-should-follow/

Real examples from the SecurityScorecard Incident Response team

Explore a few real-world scenarios that SecurityScorecard's Incident Response team handled, illustrating their expertise and efficacy in managing cybersecurity incidents. These examples provide insights into the approach, strategies, and outcomes, offering valuable lessons for incident response preparedness.

Successful ransomware negotiation for a software company

CHALLENGE

The company faced a significant cybersecurity challenge when a third-party vendor was breached, resulting in deploying the Suncrypt RAS ransomware. The attack involved partial encryption and data exfiltration, with the client's defenses providing only limited clues. The attackers initially demanded a $4 million Bitcoin ransom, which escalated to $8 million, underscoring the severity and complexity of the incident.

RESPONSE

SecurityScorecard's solutions played a pivotal role in addressing the cybersecurity incident, offering a comprehensive suite of services, including digital forensics, incident response investigations, malware reverse engineering, and ransomware negotiation. The SecurityScorecard team efficiently aided negotiations while monitoring the dark web for reconnaissance activities.

OUTCOME

This approach resulted in over 1,000 hours of investigative work, enabling quick action to prevent full compromise and restore compromised data. Moreover, the negotiations team successfully lowered the final payment amount to just $20,000, showcasing the efficacy of SecurityScorecard's interventions. As a testament to the trust in SecurityScorecard's solutions, additional licenses were procured to augment the company's cyber posture, further strengthening its resilience against future threats.

Large Fortune 1000 company **thwarts major cyber attack**

CHALLENGE

In another recent example, SecurityScorecard's Incident Response team was contacted by a Fortune 1000 company with 3,000 employees after suspecting a limited single server compromise. Despite having a mature security defense team, the company lacked an Endpoint Detection and Response (EDR) tool.

RESPONSE

The Incident Response team swiftly deployed an EDR solution to fortify the perimeter. However, at 3 AM the following day, they received an alert indicating an active breach. After over 6 hours of intensive response efforts, the IR team successfully identified the attacker's location in Brazil and applied geofencing measures to close VPN tunnels, ultimately thwarting the attack.

OUTCOME

The company's business was saved, with the attack attributed to human error compromising access for a major Russian threat actor. This incident required over 2,000 hours of critical defense and forensic investigation. The Chief Technology Officer (CTO) expressed appreciation for SecurityScorecard's provision of an external, unbiased perspective on the company's defense posture, underscoring its immense value.

Conclusion

More than simply having an incident response plan and playbook in place is required. It is critical that these resources are regularly practiced, updated, and operationalized effectively when an incident occurs. By adhering to best practices recommended by SecurityScorecard's incident response experts, organizations can guarantee they are adequately prepared to handle future incidents swiftly and effectively, regardless of whether that incident stems from their own attack surface or in their third-party ecosystem.

Rapidly eliminate critical supply chain cyber risks

Many companies are not equipped to operationalize their supply chain risk programs on their own. 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 cybersecurity posture of your supply chain. Contact SecurityScorecard today to learn more.

> "The supplier ecosystem is a highly desirable target for ransomware groups. Third-party breach victims are often not aware of an incident until they receive a ransomware note, allowing time for attackers to infiltrate hundreds of companies without being detected."

Ryan Sherstobitoff, Senior Vice President of Threat Research and Intelligence

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com