HOW CIOS CAN PREPARE FOR SUPPLY CHAIN SECURITY ISSUES HEADING INTO 2022

November 17, 2021 • Forbes • Kevin Beasley

CIOs have a lot on their plates as they manage the nuanced security infrastructure requirements for remote and hybrid work. But with a 42% increase in attacks on the supply chain in Q1 2021 — and an expectation that number will grow — leaders must remain vigilant.

As hard as organizations have worked to shore up security for hybrid operations, cybercriminals have worked just as diligently to find new ways of infiltrating and holding ransom major players in the supply chain. If the number of data breaches keeps pace with the first half of the year, 2021 will end with a record-high number of data compromises.

With the candle burning at both ends, organizations cannot afford to turn a blind eye to these threats. CIOs need to take steps now to prepare for the growing frequency of cyberthreats against the supply chain.

A Vulnerable Supply Chain

Imagine a large fuel company is hacked via security flaws in its third-party software. While the breach is not directly their fault, the fuel company now must answer to the bread truck driver who is unable to make deliveries. This leaves delivery drivers trying to make amends with their grocery partners for the late delivery. And the grocery stores then must explain the bread shortage to their customers. This scenario recently played out when the Colonial Pipeline was hacked, causing fuel shortages on the east coast of the U.S.

Unfortunately, that is the kind of havoc cybercriminals can wreak on the supply chain. Once they work their way in, cybercriminals can cause disruption after disruption — it is a domino effect that affects suppliers, buyers and even consumers.

In addition to the logistical nightmare, an attack on the supply chain can incur millions of dollars in recovery costs. From 2020 to 2021, there was a 10% increase in the average cost of a data breach, bringing the average total cost to $4.24 million. Using tactics like ransomware and phishing, cyberattacks have also increased both in severity and frequency this year — so much that the U.S. Congress passed a bill to incentivize cybersecurity planning for state and local governments.

In 2021, we have also seen a shift in who is being targeted by cybercriminals. Large enterprises have historically been the primary target of supply chain attacks, and these attacks tend to garner the most media coverage. Small businesses have been targeted just as frequently, even if we are not seeing coverage of these attacks as often in the news.

The most concerning trend we are seeing, however, is the unpreparedness of enterprises in response to cybercrime. According to research from IBM,

77% of companies do not have a cybersecurity incident response plan applied consistently across their organization. A lack of preparation results in slower response times to cyberthreats and other issues. During the remainder of 2021 and looking ahead to 2022, cybersecurity needs to be the top priority for CIOs and their teams.

Cybersecurity Considerations For CIOs

With the cost, frequency and severity of attacks on the rise, a robust end-to-end security posture is critical. From perfecting your incident response plan to regularly monitoring your networks, there are several initiatives you can take to bolster your cybersecurity.

1. Create a thorough and effective incident response plan.

The rise in cyberattacks in the first half of the year highlighted the importance of a thorough incident response plan. President Biden even signed an executive order in hopes of improving the country's cybersecurity protections, communications plans included.

Crafting and implementing an incident response plan can significantly increase your organization's response time to a cybersecurity threat. It is worth the effort to form a cross-functional task force in your organization or outsource the development of an incident response plan to a third-party expert.

Additionally, consider using a cloud-based disaster recovery plan that provides the necessary tools for impervious data protection and backup. Your response plan should include a business continuity plan, critical recovery processes for your network and devices and a communications plan for internal and external communications. Prepare to communicate with full transparency about what has happened and what you are doing to fix it. In many jurisdictions, you are required by law to report a data breach.

For your incident response plan to be fully effective, it needs to be formalized, documented and communicated across the enterprise so every employee understands their role. You may also want to create incident response scenarios as a training tool for your team.

2. Regularly test for vulnerabilities.

The majority data breaches involve known network and system vulnerabilities, so continuously assessing and monitoring for vulnerabilities is critical in closing security gaps.

The European Union Agency for Cybersecurity (ENISA) studied attacks on the supply chain discovered from January 2020 to July 2021. They found that malware was the tactic used in 62% of cases. Knowing that ransomware is a fast-growing malware technique, you should focus on preventive measures such as hardening edge equipment, patching operating systems and enabling multiple layers of malware protection. Regularly testing these measures, along with other endpoint security defenses and authentication requirements such as multifactor authentication (MFA), can help mitigate the risk of ransomware attacks.

When working with third-party suppliers or vendors, you also need to ensure their technologies are protected — communication is critical. Identify all access points to sensitive information to keep track of which employees and vendors have access to your network and data, and keep access roles to a minimum. Additionally, you should regularly assess your third-party partners' cybersecurity measures

and networks for vulnerabilities.

Do not wait to improve your security strategy.
Unfortunately, cyberattacks are inevitable. But with adequate preparation and education, you can improve your overall security posture and response time when faced with a cyberthreat. If 2021 taught us anything about security, it is that proactivity is key, and time spent improving your cybersecurity strategy is never wasted time.