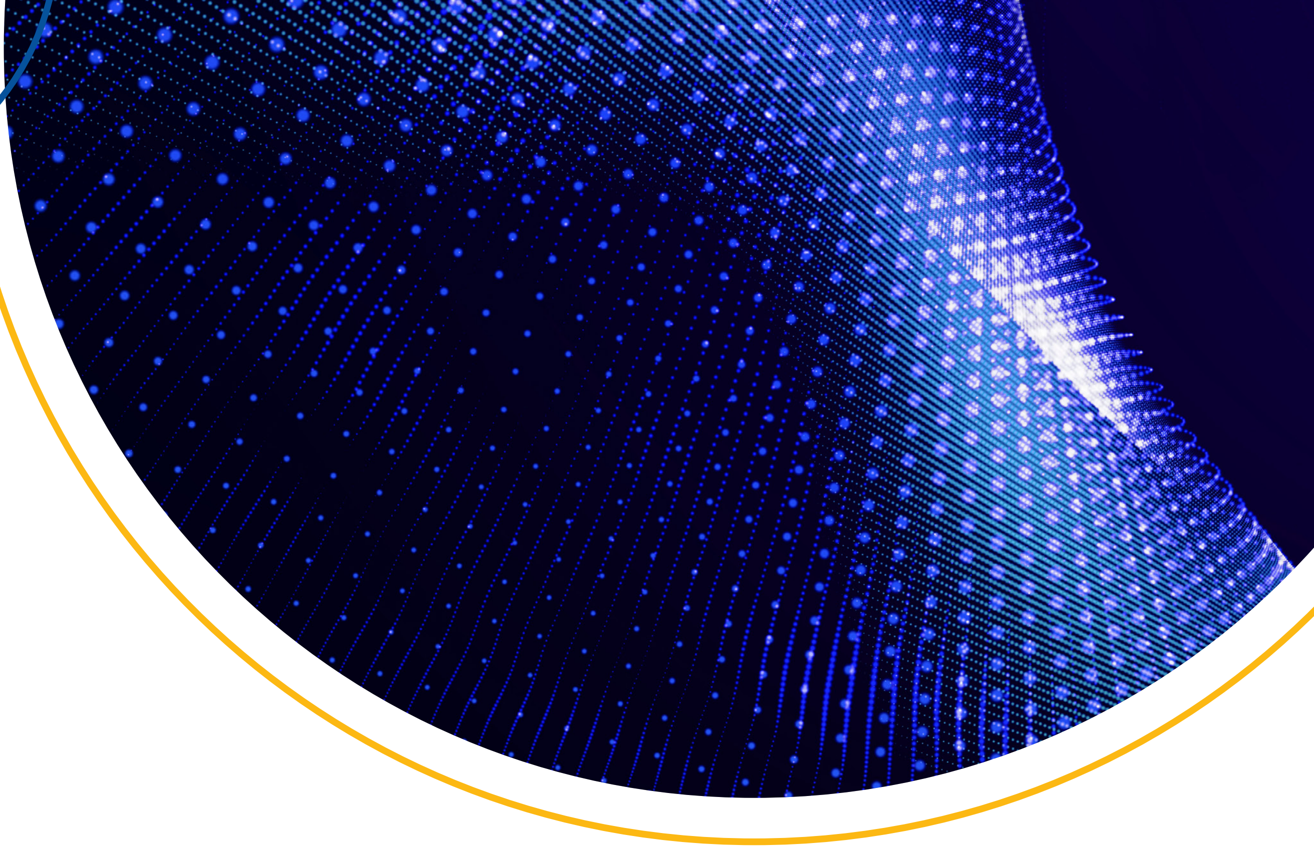
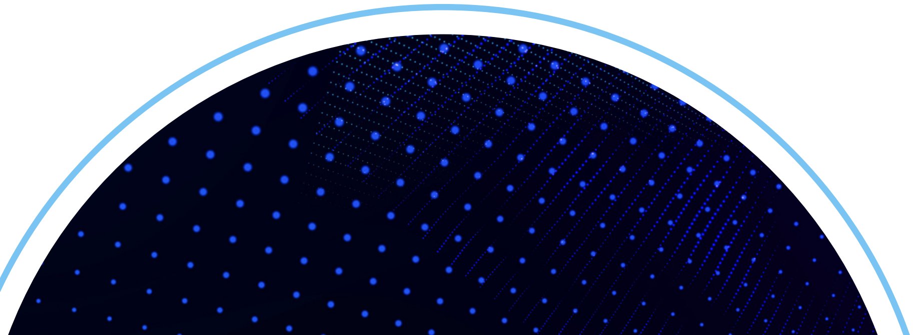


Cybersecurity Risks in the Supply Chain:

Mitigation Tactics

Written by Steve King & the CyberEd.io Security Team



CyberEd.io

Introduction

Since the SolarWinds attack franchised both Open-source and proprietary supply chain attacks, the attack underscored the cyberattack vulnerabilities native to supply chains. Supply chain risk mitigation has since become an essential component of risk management strategies and information security programs. How to manage against this risk in the current tight labor market and constrained budgetary goals is a challenge. If you have the budget, you can't find the skills. If you have the skills, you can't find the budget.

In our own survey of 600 enterprise leaders, we found that only 21% rated the availability of qualified cybersecurity candidates good/excellent, while only 23% believed that the average employee level of cybersecurity knowledge is good/excellent. When queried about the company's greatest roadblock to successful threat detection and response, 21% cited a lack of visibility across the organization, 19% a lack of trained or skilled personnel, and 19% claimed lack of budget

Third-Party Vendor Risks

Third-party exposures always introduce significant data security risks to your organization. This is usually due to poor security practices stemming from a weak security strategy. The unfortunate reality impacting supply chain cybersecurity is that your third-party vendors likely don't take cybersecurity as seriously as you do.

Digital Risks

Digital risks are the by-product of digital transformation - the more digital solutions you add to your ecosystem, the more complex your network dependencies become, and the larger potential network gateways cybercriminals will have to exploit. These exposures are usually caused by software vulnerabilities, such as zero-day exploits or overlooked configuration errors.

Digital risks frequently translate to Ransomware, IP Theft and regulatory non-compliance.

Supplier Fraud

An example of supplier fraud, or vendor fraud, is when a cybercriminal claiming to be a known retailer requests a change to their payment processes. These events are difficult to identify and getting more so quickly with the availability of ChatGPT style models for G-AI and fraudsters who are rapidly adopting advanced social engineering techniques, including Generative AI authored voicemails, phishing attacks, and Deepfake video recordings.

In addition, fraud events impacting global supply chain security aren't limited to the supplier category. A growing number of data breach events are caused by third-party vendors falling victim to various social engineering and fraud tactics.

Kick-started during the pandemic, fraud continues to increase. According to the FTC, Americans lost more than $8.8 billion to fraud in 2022, an increase of 30% in a single year.

Data Protection

Data integrity throughout the supply chain is growing in significance. Security measures should ensure all data states are secure, including those at rest and in motion, but rarely achieve that performance. Data encryption practices are now critical for third-party integrations because hackers know that a target's third-party vendor usually has easy access to their sensitive data.

What You Can Do

By implementing the following best practices, you will reduce the likelihood of common cybersecurity risks in the supply chain by a big number.

Third-Party Risk Assessments

Developing, publishing and adhering to a structured third-party risk assessment schedule will help you discover supply chain security risks before cybercriminals exploit them. These assessments should be completely customizable to accommodate each supplier's unique risk profile.

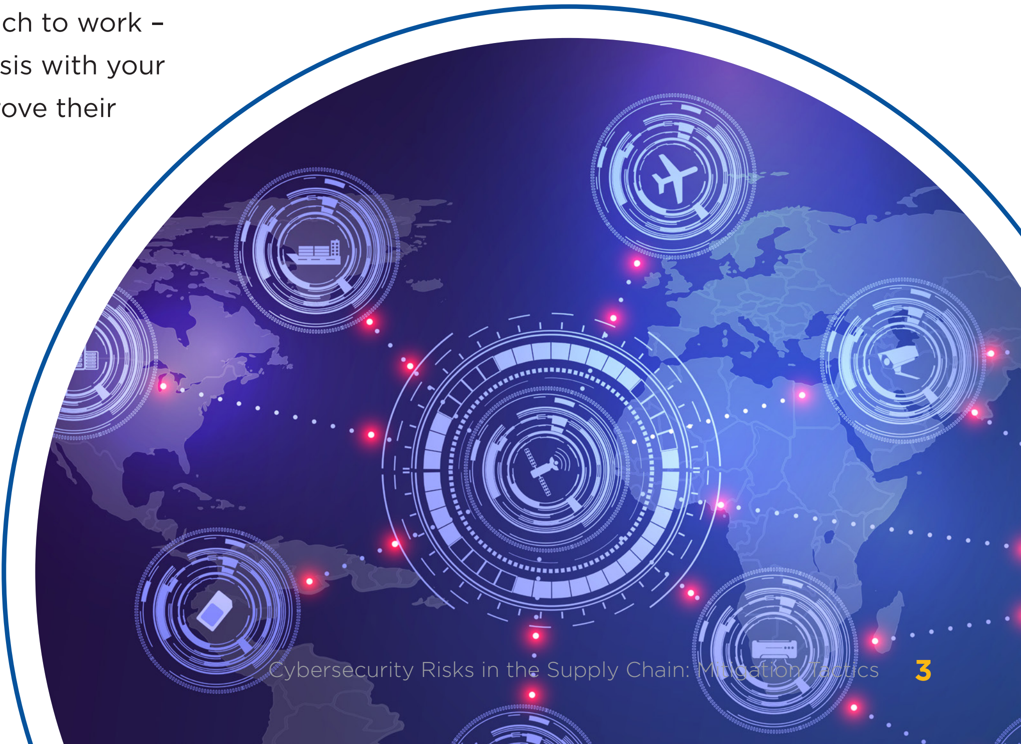
There is an abundance of free risk assessment forms and models available with which to work – sharing the results on a continual basis with your partners may motivate them to improve their security posture as well.

Data Encryption

Defense strategies should never pursue absolute solutions. Mitigating risk is an incremental growth strategy which can be impacted by enforcing encryption practices on all forms of data, especially at the interface of third-party integrations. The Advanced Encryption Standard (AES) should ideally be implemented. Because of its key length options, it's considered one of the hardest encryption types to compromise, which is why it is in use by the government and military.

The Advanced Encryption Standard, also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology in 2001. It deploys a 256-bit encryption method, which is considered a more complex and highly secured method. Facebook and WhatsApp messenger uses the AES encryption of 256-bit for securely transmitting and receiving the one-to-one message.

You don't have to know more about AES, just that it is what it is and generally why it works, as there are lots of "how to" manuals and skilled consultants around to help



Attack Surface Monitoring

Monitoring your attack surface is always a good idea, regardless of supply chain activity as it will identify 3rd party risks along with all others and will heighten your chances of detecting a supply chain attack in time to defend against it.

There are lots of good attack surface monitoring solutions on the market that can discover security vulnerabilities across cloud solutions throughout the third and even fourth-party network. Fourth party networks support operational models known as 4PL where the business outsources the entire supply chain management and logistics to a single vendor with whom you may otherwise never engage. If even part of your operation is outsourced in that model, you will need another layer of security monitoring and a complete vetting of the 4PL solution.

Incident Response Planning

Whether you plan offensively or defensively, a structured, rehearsed and tested Incident Response Plan (IRP) with clear role assignments is critical so that you and your teams can prepare for every supply chain attack scenario with minimal impact on business continuity.

Assign incident response planning to a senior officer and get insurance and policy help from a reputable broker, then run table top exercises with fully functional participants present. There are readily available templates and design kits that can help you build out your own.

Penetration Testing

Penetration testing used to be helpful for isolating Cybersecurity risk, but as the threats have evolved, so have the adversary's ability to get into your network. Pentests are helpful today in identifying exploitable vulnerabilities so that they may be repaired before they are attacked from the outside.

The other useful purpose of a pentest is in exercising IRPs. Response tactics should be routinely evaluated with penetration testing and corrections remedied on a continuing basis. Pentesting will also uncover advanced supply chain security threats that bypass some modern security systems.

Tactical Steps

Supply Chain Risk can take many forms and these five approaches are standard best practices from a macro cybersecurity defense point of view which, when combined with the best practices for the three specific types of supply chain attacks—compromising commercial software, compromising open source software, or embedding malware during the physical production of technology, will harden your defenses against this category of threat.

As soon as you identify a need for a third party, make a list of all of the possible solutions and vet them. In addition to evaluating them on the solution, also take a few moments to evaluate the potential risks. While you'll dive deeper into this at a later stage, it's important to be aware of deal-breakers or high-risk situations.

After choosing your top solution, it's time to drill down into risk. What specific risks are involved? How critical are those risks? Risk factors typically include severity and how likely a problem is to occur. One common formula for cybersecurity risk, and the one endorsed by NIST is Risk = Threat x Vulnerability x Consequence, but a more granular formula and one we promote is Risk = (Threat x Vulnerability x Probability of Occurrence x Impact). In the latter, more refined formula, by adding the 'probability' factor, you can see how a more complete picture of risk can be determined by expanding the formula.

And, also why it is necessary.

From there, you must define what changes or considerations your organization needs to make to mitigate those risks. At this time, you also must define how frequently you need to review this vendor, and what metrics you'll use for evaluating ongoing risk.

For the duration of your relationship with the third party, you'll need to conduct ongoing monitoring. Some of this will be their responsibility, but you'll also want to pay attention to media reports, business updates, and sanctions lists of an international company, breach notifications, and other various methods of gathering intelligence.

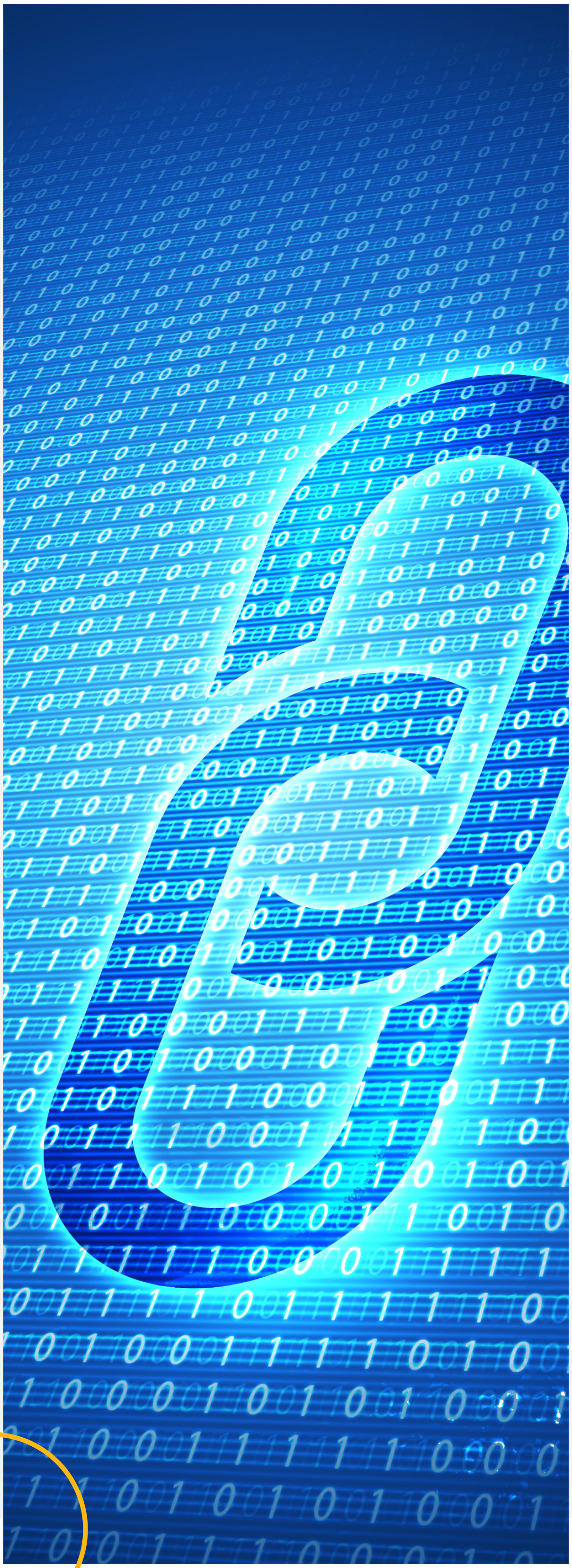
This phase includes maintaining compliance with all applicable laws and regulations. Some of the most common regulations you must comply with include ISO 27001 and 27701 and NIST SP 800-53. It's your responsibility as an organization to ensure that you are aware of all regulatory bodies and requirements to which your company is subjected.

Whether you no longer need the third party or the risk becomes too great to continue, there comes a time to end the relationship. Rather than letting it gather dust and opening yourself up to the possibility of unmonitored breaches, you must develop a specific off-boarding process.
After ensuring that any and all obligations have been met, it's time to end the relationship and completely extract the third party from your business.

If terminating a relationship because the third party exceeds your tolerance for risk, it's time to start sourcing and vetting a new solution. A structured version of that process will help you move efficiently on to your next supplier.

It should go without saying that to succeed in the coming years, you must be aware of — and take strides to mitigate — any third-party risk. While establishing a third-party risk mitigation program doesn't remove all possibility of future breaches, it does reduce the likelihood of a breach imposing a lasting effect on your business.

Conclusion



Effective cyber-risk management requires an accurate and complete understanding of your risk.

Insufficient patching of known vulnerabilities affects many third-party relationships. All companies share the same exposures caused by ignoring the same fundamentals. All told, firms typically “inherit” exposure to three times as many unique types of security issues from third parties than exist in their own infrastructure. There’s clearly a contagion aspect to third-party cyber risk that organizations must recognize and manage accordingly.

If contagion risk is an issue in direct vendor relationships, you can imagine that it becomes a much bigger issue with subsequent-tier indirect partnerships. These cascading indirect relationships need to be vetted with the same rigor and enthusiasm as you bring to your mitigation process for your primary vendor.

Vendor attestation of security through annual questionnaires helps you understand the investments they have made to achieve good risk outcomes within a point-in-time, but that is only some of the information you will need to make better decisions. Objective data helps you understand how well they claim to implement and operate their program, and applying your risk formula to all aspects of your business will quickly identify the information assets with the highest exposures to third party vulnerabilities.

This is the true benefit that a continuous risk monitoring solution can provide.

CLOSE THE GAP.

Talk to a CyberEd Expert today

Visit cybered.io

@cyberedio CyberEd.io CyberEd.io

CyberEd.io

+1-609-356-1499 • info@cybered.io • cybered.io