Marsh

Three best practices to reduce supply chain cyber exposure

Cyber-attacks on service providers and vendors — often referred to as supply chain cyber-attacks — continue to grow. It is impossible to completely eradicate supply chain vulnerabilities. Your organization can, however, minimize risk and reduce potential exposure in advance of a compromise, engage outside resources to provide support during an event, and perform a post-mortem analysis after an event that takes into account losses and reduces the likelihood of another attack.

This guide provides straightforward, practical recommendations on addressing three critical focus areas.

Best practice #1

TAKE STEPS TO IDENTIFY AND MINIMIZE SUPPLY CHAIN/VENDOR EXPOSURE

Create a vendor inventory

Accounting for third parties in your risk management program is critical. Create an inventory of:

- Any third-party vendor with authorized access or connectivity to your organization's IT network. This can be through perpetual, part-time, or ad-hoc access to the IT network, such as an operational technology (OT) manufacturer that provides maintenance to your production system.
- Any third party with access to your organization's data, including personal healthcare information (PHI) related to employee benefits; employee payroll data that contains employee salary, social security numbers, addresses, or other personally identifiable information (PII); and proprietary or protected data. One example is a payroll provider that is given a payroll file every week to generate employee pay.
- Consultants with access to your IT network and/or data. External consultants, for example someone working in your office on your production improvement program, should only be allowed to access work-required applications and data. A best practice is to establish their accounts in a way that is different to regular employees, allowing you to easily identify them. You should require the use of multi-factor authentication.

Assess your vendor risk

Your vendor inventory should include a detailed description of the service(s) provided, and the last time the vendor's risk posture was reviewed. The risk from the third-party vendor needs to be assessed, ideally by a cross-functional team that includes representatives from legal, compliance, privacy, information security, risk, and procurement, among others. A clearly defined risk assessment and a vendor approval process is also important to help understand vendor risk. One example is a vendor inadvertently allowing unauthorized files or malware to enter your organization's network.

Your organization may want to consider an external cyber risk assessment, which can be used to assess the external risk posture of vendors with access to your data and/or IT resources. At a minimum, a third-party vendor's risk should be evaluated annually, or potentially more frequently, depending on how critical they are to your operations. You may also want to assess the risk posture of any new vendors and suppliers prior to utilizing their services.

Use contractual protections

Work with your legal counsel, to consider incorporating risk management into your vendor contracts such as the following:

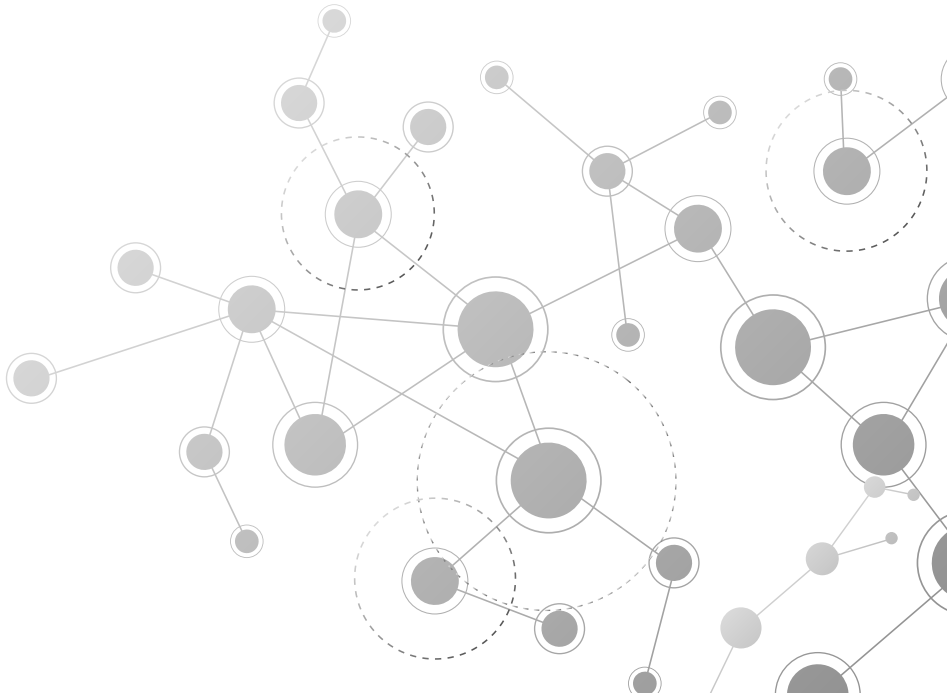
- Obligate the vendor to timely notify you of any cyber incident or data breach and to fully cooperate in providing all information necessary for a complete investigation.
- Consider requiring the third-party vendor to carry cyber insurance (and technology errors and omissions insurance for technology vendors) to cover any losses related to the service they provide to your organization.
- Obligate the vendor to return or destroy data upon the termination or expiration of the contract. Establish and follow internal procedures for contract terminations/expirations so that all data access is revoked and data possessed by the vendor is certified to have been deleted/destroyed.
- Consider requiring the vendor to practice cybersecurity standards — no less than what your organization requires of itself.

Communicate, communicate, communicate

Collaborate frequently with any third-party vendors that have access regarding their cyber risk posture and services. Be aware of the ecosystem that exists between you, your third-party vendors, and your vendor's vendors (fourth-party vendors) that your vendors may rely upon.

Minimize access

Follow the principle of least privilege. Many third-party data breaches occur because the third-party vendor is given unnecessary access to data and/or IT systems. Use network segmentation to separate third-party vendors from unrequired critical applications and data. Consider dividing third-party vendors that have access to the organization's IT network into separate segments based on the services/functions they provide.



Best practice #2

ENGAGE OUTSIDE RESOURCES WHEN A VENDOR IS COMPROMISED

Mitigate first

When your systems are compromised following a cyber incident, mitigation is the top priority. Depending on the nature of the compromise, mitigation could involve patching, upgrading software versions, moving applications behind firewalls, disabling internet access, and checking for indicators of compromise (IOCs). The discovery of such indicators should trigger a full digital forensics investigation to understand the impact on systems and data.

Provide notice to your insurance carrier

Consult with your broker and notify your cyber insurance carrier as quickly as possible. Most cyber insurance policies provide coverage for incident response services, including legal and forensics assistance. These are frequently subject to prior consent and most carriers have vendor panel requirements.

Engage legal counsel

Retaining expert counsel is important, especially in cyber compromises caused by a third-party vendor. Counsel can advocate on your behalf for the vendor's cooperation with the investigation. Your organization can benefit from that wider perspective and deeper knowledge when counsel also has experience representing similarly situated clients. In the event that the vendor's compromise results in a breach of PII that triggers breach notification laws, counsel can assist you in determining any involvement the vendor should have in the data breach response process.

Enlist forensics' expertise

A key issue in a vendor-caused data or network compromise is the extent to which the third party will provide forensics findings to its clients. It is often difficult for organizations to determine the sufficiency of the vendor's investigation and understand the full impact on your data. You can attempt to minimize this uncertainty by requesting a summary of the vendor's forensics report, as well as obtaining legal guidance on the advisability of obtaining a third party forensics firm to review the vendor's forensics findings and representations. If the vendor compromise has impacted your systems (for example, IOCs were discovered) you will need your own forensics investigation.

Best practice #3

FOLLOWING A VENDOR OR SUPPLIER COMPROMISE, ASSESS AND RE-EVALUATE PLANS AND VENDORS, AND LEVERAGE YOUR CYBER INSURANCE

Learn post-mortem lessons

Revisit the prevention steps discussed above to reduce the chance that your organization will be exposed again to vendors' security vulnerabilities.

Review and update response plans

Evaluate incident response, disaster recovery, and crisis management plans in the context of the vendor compromise and determine what worked, what did not, and any adjustments that may be needed.

Replace the vendor

Reconsider using the same vendor that caused the problem and investigate the use of other, lower risk providers.

Use cyber insurance to cover the claims expenses

Determine whether the vendor's or supplier's compromise caused a loss of revenue due to system downtime, created out-of-pocket expenses, or caused extra expenses that could be claimed under your cyber insurance policy's business interruption coverage. Consider whether contractual indemnification or other provisions address recouping losses from the vendor. Expect liability exposure if regulated data was exposed. Engage forensic accountants as needed to evaluate losses and prepare the proof of loss.

In summary

Cyber-attacks against the supply chain continue to grow — and some are simply impossible to eliminate. With that in mind, consider an approach rooted in cyber risk management. Whereas a traditional cybersecurity approach focuses primarily around mitigation, cyber risk management understands that not all risks can be removed and not all attacks can be prevented, especially when it comes your supply chain. Instead, focus on minimizing risk and reducing your potential exposure.

Katherine Keefe
Cyber Incident Management Leader
US & Canada Cyber Practice
Marsh Specialty

+1 215 301 4030
katherine.keefe@marsh.com

James A. Holtzclaw
Senior Vice President
US Cyber Risk Consulting
Marsh Advisory

+1 202 297 9351
james.holtzclaw@marsh.com

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $17 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.

1166 Avenue of the Americas, New York 10036