COMPLIANCE & ETHICS PROFESSIONAL

FEBRUARY 2019

CEP MAGAZINE

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

JACKI CHESLOW, CCEP, CCEP-I
DIRECTOR, BUSINESS ETHICS & COMPLIANCE, RECORD & INFORMATION MANAGEMENT, AVIS BUDGET GROUP

DRIVE THE CHANGE IN YOUR ORGANIZATION (P14)

SCCE™

CYBERATTACKS IN A GLOBAL SUPPLY CHAIN: HOW COMPLIANCE OFFICERS CAN MITIGATE RISK

by Matan Or-El

Matan Or-El

(jan@eskenzipr.com) is co-founder and CEO of Panorays in New York City.

Cyberattacks in the supply chain are being industrialized to not only target one company, but many companies across a single industry. Cyberattacks hit two-thirds of firms, according to research by CrowdStrike,[1] and the impact reverberates from financial to operational disruption and the actual loss of customers.

Cybercriminals are now taking advantage daily of easy access provided by privileged accounts. Attackers target the weakest part of a supply chain, which means that even when an organization has top-notch security protocols in place, there's no guarantee that these same standards are held by the vendors that already have access to the supply chain. Given this, it's no surprise that about 80% of all cyberattacks happen in the supply chain, according to the SANS Institute as cited by KPMG in their report, "Digital Supply chain — the hype and the risks."[2]

The sheer number of supply chain attacks proves that compliance and ethics officers must proceed with caution when it comes to auditing current vendors and vetting new ones. A multilayered approach must be implemented when working toward mitigating risk in the supply chain.

Perform an audit of every vendor

Whether or not a company has vendors that it's been working with for years, an audit should still be performed for every supplier. The level of risk will depend on the nature of the relationship with the vendor; for example, a vendor with full access to a company's IT system will carry more risk than a vendor without credentials. The audit should be thorough and dig deep enough to understand whether suppliers' actions are aligned with the company's security best practices and any legal policies. Even where there is an established relationship of

trust and respect between supplier and client, this is a vital step in the process that could cause damage if overlooked.

Verify the vetting process

Compliance and ethics officers must ensure an airtight vetting process. Paper audits are not practical, because they require lots of manual work, are time-consuming, and are already obsolete by the time the audits are received. The vetting process has to include more than just one audit in a calendar year or initially when the relationship began. It has to be an ongoing process that is reviewed daily, which means the paper process has to be dispensed with, and automation has to be instituted. The latest technologies are not only able to monitor the security posture of third-party vendors continually; they can also alert teams to a change in that security posture, if it occurs.

This approach allows companies to streamline their processes and fast-track vendors as needed instead of struggling through months to verify partners.

Knowing your partners is essential. Each relationship should be reviewed and categorized according to the type and criticality of the data they are able to access and the pathway to it. Identifying the riskiest vendors is vital to define a well-prioritized mitigation road map. The security team can then determine how best to marshal their resources.

Continuous monitoring is critical and can be done automatically by scanning a partner's digital assets against potential threats. This type of test is known as the hacker's view, because it looks for all the same vulnerabilities that a hacker would search for to get into a network. Screening the connections made through servers is essential to spot anomalous traffic that is sending information to a hacker's command-and-control servers. This ongoing scanning does not require any action on the part of third-party vendors and can be performed quickly and efficiently.

Leave zero room for interpretation

It may be tempting to assume that a supplier's definition of security is the same as yours. After all, the mere term itself packs a big punch and should certainly warrant a need for best practices. However, every organization and vendor operate differently, and the idea of security may just as well vary from one team to the next. It's important to leave zero room for interpretation. A full, digital risk management plan, complete with best practices and protocols that can be conveyed to the vendor, should be in place. Even the simplest security procedures should be spelled out, such as requiring the encryption of all data sent to and received from a vendor, as well as data stored on backup tapes, external hard drives, and laptops.

It's important to require vendors to adhere to not only the top security practices, but also to digital privacy regulations as well. With the UK's General Data Protection Regulation, along with a myriad of others in the US, oversight of these regulations is crucial. One misstep from a vendor could cost the host company a great deal in terms of fines and reputation.

Companies should spell it out in detail along with any consequences in any contract. Although most standard contracts provide the typical requirements, there is also flexibility that can be had with written clauses regarding liability in the event of data or regulation breach. This might mean visiting a supplier on site to find out the exact details surrounding any potential breach. Such an investigation could involve determining what has been stolen, how the breach occurred, and the authority to work directly with the vendor to mitigate similar risks moving forward. A full mitigation plan, including step-by-step procedures following an event, should be created and given to vendors and partners to agree to at the beginning of the relationship.

Companies should also have an open-door policy that suppliers can use to raise any red flags or potential concerns throughout the relationship.

Each relationship should be reviewed and categorized according to the type and criticality of the data they are able to access and the pathway to it.

Supply chain attacks are inevitable

Supply chain attacks are the new normal, as companies like [24]7.ai, Ticketmaster, Lord & Taylor, and many others have unfortunately discovered. Currently, there is no single foolproof method of keeping hackers at bay, which

means that compliance and ethics officers must be prepared for a breach or another type of attack to occur and have detailed plans for responding. Much like a fire drill, compliance and ethics officers should run through procedures with the security team so they can prove that the company did everything possible to stop an attack, mitigate damage, and inform customers. CEP

Endnotes

1. CrowdStrike, "Securing the supply chain," July 2018, http://bit.ly/2Qnf11L
2. KPMG, "Digital Supply Chain — the hype and the risks," February 2018, http://bit.ly/2B8p3JW

Takeaways

- Compliance and ethics officers must work toward mitigating the risk of cyberattacks in the global supply chain by creating a detailed vendor risk management plan.
- The vetting process for each vendor must be thorough; time spent vetting can be greatly decreased when companies choose to automate the process.
- An audit should be performed on every vendor before and throughout the business relationship on a continuous basis.
- Companies should ensure that each vendor is also compliant with best practices and legal policies and is aware of liabilities and consequences of not adhering to those rules.
- Companies should reduce the data they share with suppliers to what suppliers require, rather than unlimited data access.