Cybersecurity: Raising awareness to prevent a third-party or supply chain attack

February 2019

Mark Giuliano
Chief Administrative Officer
Invesco

Contents

Executive summary

"Third-party (or supply chain) cyber risk has become a significant concern because it provides an opportunity for adversaries to get into what might already be a fairly well-protected organization."

Mark Giuliano
Chief Administrative Officer
Invesco

High profile cyberattacks—often involving serious breaches of sensitive corporate and client data—have become commonplace in daily news reports around the world. One method increasingly used by nefarious actors is penetrating a company's systems through a less well-protected third-party vendor or contractor, also known as supply chain attack. Instead of hiring and training employees to perform functions such as accounting and human resources, companies are turning to highly specialized providers, and especially cloud companies, to perform these functions to save time and money. These third party vendors are often granted access to the hiring company's systems and can be used as unwitting Trojan horses to breach data security firewalls.

Effective cybersecurity is everyone's responsibility as employees are the first line of defense against an attack. Employees also create the biggest vulnerability, as email-based phishing, also known as business email compromise, and viruses are still the most prevalent types of cyberthreats to a company's business. Accordingly, it is important for employees to be aware of the best practices for cybersecurity regarding third-party vendors.

Supply chain risk: A significant and growing threat

This paper focuses on third-party risk, or the vulnerability that occurs when one company hires another company to provide a service. This is also called supply chain risk, because the third-party can hire a fourth-party, and the fourth-party can hire a fifth-party (Nth party risk) and so on. Because of this supply chain, it becomes increasingly difficult for the original hiring company to keep track of its data and keep the data safe. Cybersecurity is costly and time-consuming and not all vendors have robust practices in place, which is why adversaries will often take advantage of the vendor link.

According to a 2019 security predictions report by cybersecurity firm FireEye®, supply chain attacks are an increasingly important concern[1]. The new report explains that the supply chain allows thieves to steal information from several targets at once and usually remain unnoticed. It also warns that as data increasingly moves to the cloud, attackers are moving with it. FireEye says companies' increasing use of the cloud is causing a "massive" increase in attacks there.

After years of identity theft, the US Federal Trade Commission in 2011 began enforcing its Fair and Accurate Credit Transactions Act of 2003's Red Flags Rule. The Red Flags Rule requires that each financial institution or creditor implement a written program to detect, prevent and mitigate identity theft in connection with the opening or maintenance of consumer accounts.

In 2016, the Securities and Exchange Commission (SEC) enforced this law with a $1 million fine against a Fortune 500 financial services firm after cyberintruders impersonated independent representatives and gained access to the personal information, such as social security numbers and addresses, of at least 5,600 clients.

According to the SEC, the company's identity theft prevention program was implemented in 2009 and hadn't been reviewed or updated. In fact, hackers reportedly got around an authentication procedure by calling the company's own technical support team to reset passwords and change security questions. This is where employee cyberthreat awareness is important, as this company's employees unknowingly assisted the hackers, thereby enabling the breach, instead of disabling it.

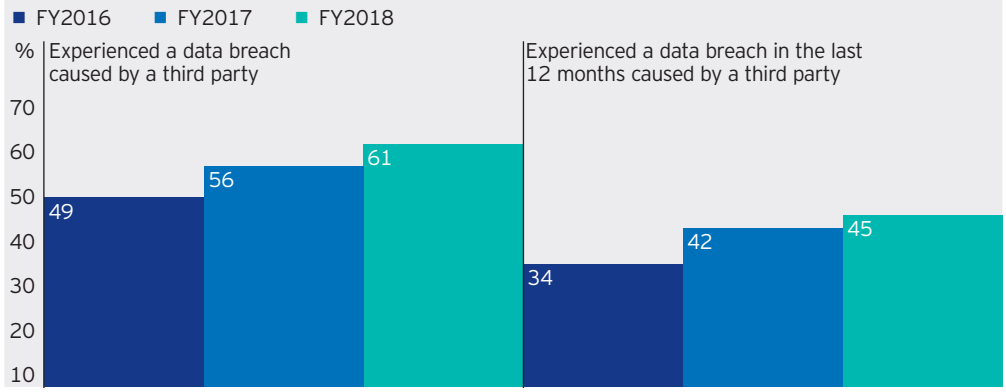
Another example of a third-party breach involving a large US retailer happened in 2013 when hackers stole personal data from nearly 40 million credit and debit card customers through a third-party HVAC contractor. The attackers reportedly used network credentials stolen from the Pennsylvania-based subcontractor that had worked at several of the US retailer's locations. The breach cost more than $200 million and included settlements in several states.

This assessment is also supported by a 2018 survey of over 1,000 IT and IT security experts in the US and UK conducted by the Ponemon Institute[2]. The survey found that almost two-thirds of of respondents' companies had experienced a data breach caused by a third party, up from 49% in 2016 (figure 1).

"Instead of hitting big corporations, they're going after the little guys, who are not as sophisticated in their security posture."

Stacy Scott
Managing Director of cybersecurity firm Kroll, a division of Duff & Phelps

Figure 1: Has your organization ever or in the past 12 months experienced a data breach caused by a third party?
Yes responses presented



Source: Ponemon Institute, November 2018

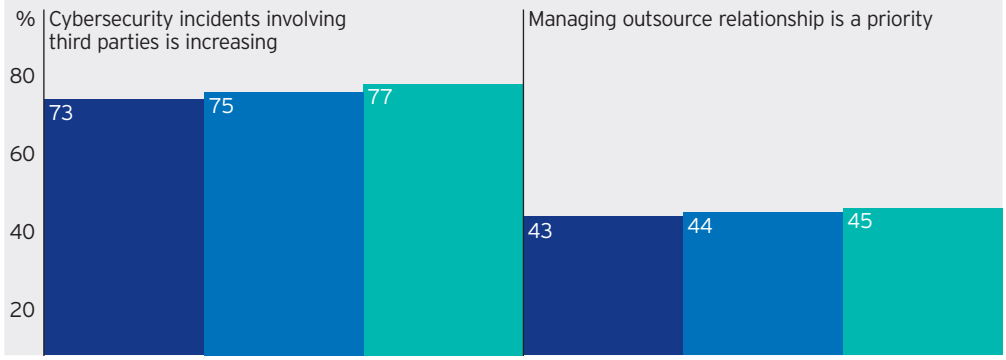
"To stay ahead of threats in 2019, organizations need to begin shifting from a compliance-based approach to a security-based approach," according to the FireEye report. A 2019 threat predictions study by online security firm Kaspersky, confirms this view, identifying supply chain attacks as a major threat and noting that they are forcing companies to vet their service providers' cyberhygiene more rigorously.[3]

This view, too, is supported by data from the Ponemon Institute survey, in which 77% of respondents indicated that cyber threats from third parties were increasing (figure 2).

"Security in a company is every employee's responsibility. Everyone has a responsibility to keep clients' and employees' data safe."

Mark Giuliano
Chief Administrative Officer Invesco

Figure 2: The gap in third-party risk
Strongly agree and agree responses combined



Source: Ponemon Institute, November 2018

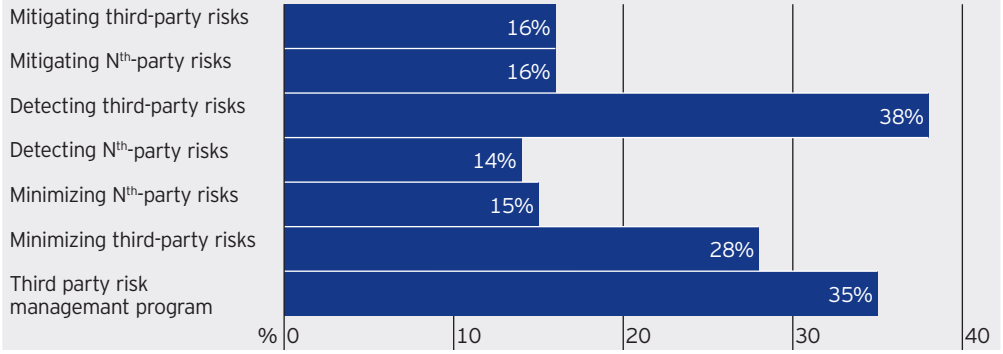
What is cyberhygiene?

Cyberhygiene refers to the practices and procedures that a company uses to ensure its data is safe from theft or attacks. Companies should ensure that vendors and contractors with access to client data have routines in place to keep their systems healthy and secure. There are many different frameworks companies can implement to help secure against an attack. The US Commerce Department's National Institute of Standards and Technology (NIST) publishes several publications that recommend security controls that can be implemented by organizations to protect information. While Scott said her company prefers the NIST 800-53 framework, which recommends security controls for federal agencies to promote information security, there are other NIST framework systems such as NIST Cybersecurity Framework (NIST-CSF) and ISO 27001 that are highly regarded as comprehensive frameworks for securing data.

Cyberhygiene is a set of practices and procedures for managing cybersecurity risks facing organizations today.

The Ponemon Institute survey results, however, suggest that most companies still have a long way to go with respect to preventing, detecting and mitigating supply chain risk. For example, only 16% of respondents believed that they had effective supply chain risk mitigation procedures in place (figure 3).

Figure 3: How effective are organizations in dealing with third party and Nth party risks?
1=not effective to 10=highly effective, 7+ responses reported



Source: Ponemon Institute, November 2018

How to minimize supply chain risk

The mitigation of third party risk has become even more important in light of the European Union's General Data Protection Regulation (EU-GDPR) that went into effect May 25, 2018 and the California Privacy Act. These sweeping regulatory changes, the most significant in 20 years affecting data storage and transmission, are forcing companies to secure data management or potentially face huge fines.

IT security experts recommend a number of critical steps for companies seeking to minimize supply chain risk:

Inventory
Create an inventory of all third parties who have access to client data. Make sure the IT department knows about all vendor relationships and about any fourth-party or fifth-party relationships.

Evaluation
In addition to contracts, vendors should be reviewed and assessed based on what kind of data they hold and what kind of access they will have to the hiring company's system. IT departments typically arrange vendors by tiers, with Tier-1 vendors being those that hold significant client data and have access to the hiring company's systems.

This process usually starts by requesting vendors to complete a questionnaire in which they must describe how they protect, store, transfer and delete data. They can also reveal any possible fourth- and fifth-party relationships.

Then it's critical for the hiring company to perform due diligence, either by hiring an independent company to assess risk, or by doing it themselves through a strict set of guidelines and procedures. Due diligence requires the hiring company to perform an on-site review and to talk to the leaders and employees who are responsible for data protection and compliance.

Frequent review
The contracts that are agreed upon by the two companies should be reviewed regularly, and updated, if necessary. The third-party risk management group should also regularly review the security practices of their third-parties and their contractors to make sure they're aware of any new threats.

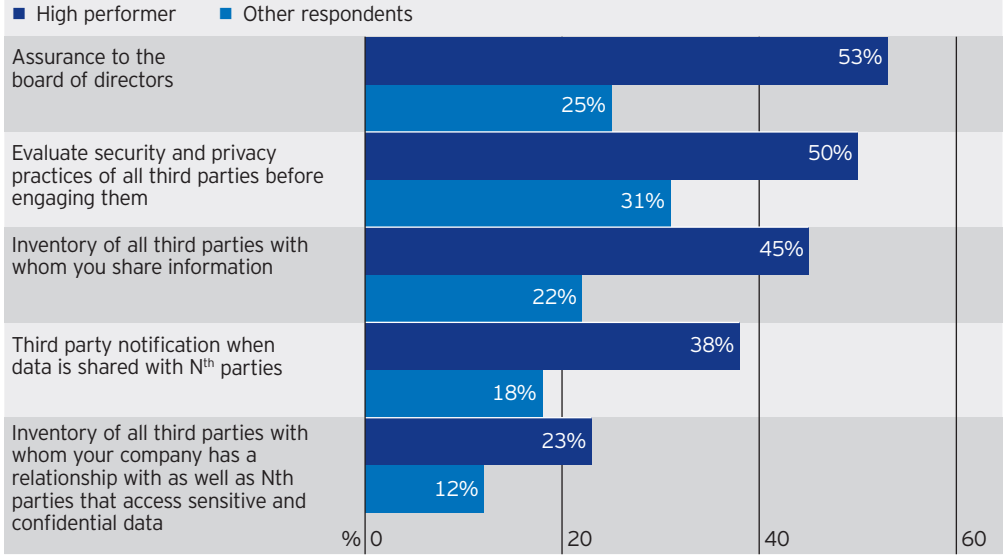
Notification
Companies should include in their contracts a requirement to be notified when their data is shared with a fourth- or fifth-party contractor.

Board oversight
The Opus report specifically recommends involving high-level board or senior leadership to help ensure that more resources will be allocated to third-party risk management.

Good cyberhygiene requires time and capital, which is why not all companies can successfully navigate and ensure complete cybersecurity. Global banks are among the companies leading the pack when it comes to managing supply chain risk. This is in part due to the fact that they are among the most frequent targets of cybercrime attempts. The big banks spend a lot of time trying to understand how to respond before a crisis occurs. Also, banks tend to see the bad actors in the financial services industry first, so asset managers and others can benefit from looking at how the banks respond.

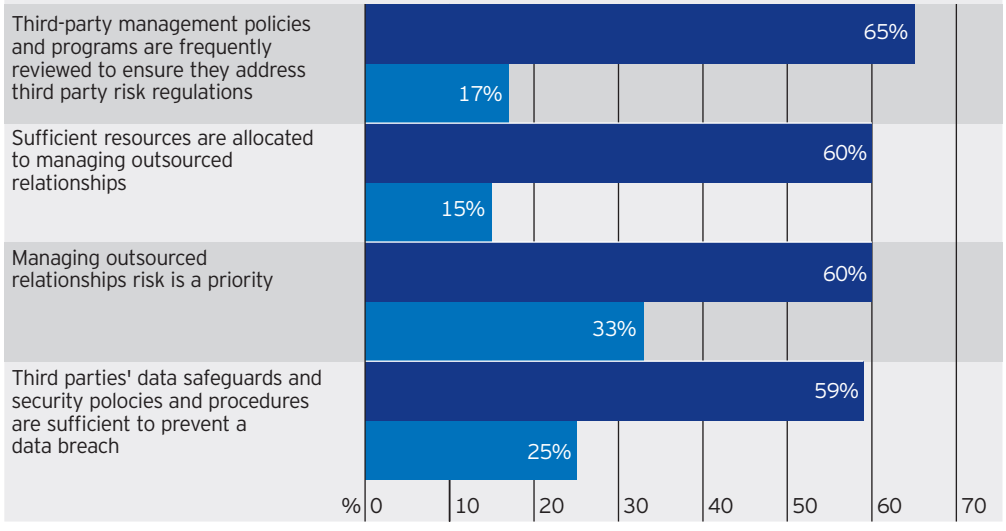
Awareness
While implementing and maintaining an effective cyberhygiene program can be labor and cost intensive, the potential risks associated with cyberattacks present a compelling case for doing so. The Ponemon survey data demonstrates that "high performing" companies (i.e., those that had avoided a third-party data breach in the prior 12 months or ever) were significantly more likely to have implemented strong supply chain risk governance processes (figures 4 and 5).

Figure 4: Differences in governance practices in high-performing organizations and the overall sample of organizations
Yes responses reported



Source: Ponemon Institute, November 2018

Figure 5: Differences in other governance practices
Strongly agree and agree responses combined



Source: Ponemon Institute, November 2018

What every vendor contract should include

"Cyberinsurance has really become something that companies are considering much more aggressively."

Mark Giuliano
Chief Administrative Officer
Invesco

Tier-1 vendor contracts should be reviewed annually and should include auditing certifications such as a Statement on Standards for Attestation Engagements 18 (SSAE 18, which replaced SSAE 16 in 2017), a regulation created by the Auditing Standards Board. These contracts should also include a Service Organization Control report (SOC 1), which is written documentation of the internal controls relevant to an audit of a customer's financial statements. SOC 2 focuses on a business' non-financial reporting controls. These certifications are increasingly used by vendors to market themselves to clients. They are costly and time consuming to acquire. Most Tier-1 vendors should have these, but it's possible that a vendor is highly specialized and doesn't have these certificates, in which case the hiring company must include a ***right-to-audit clause*** in the contract.This allows the hiring company to request an audit of the vendor's controls for accessing, creating, storing, sharing or deleting data, at any time during the length of the contract.

The second important requirement in vendor contracts is a ***notification clause,*** which states that if there is a breach, the client must be notified within a certain time period.

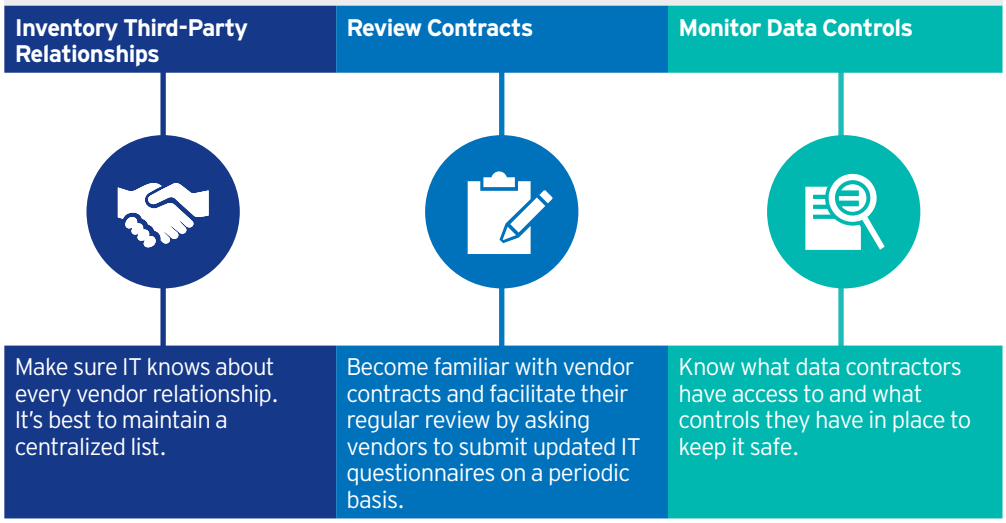
The third piece to look for in vendor contracts is ***liability coverage.*** Increasingly, the hiring company will ask for cyberliability insurance, which is a relatively new insurance product and very expensive, as insurance companies are still working through what they will cover in the event of a breach.

Good cyberhygiene requires time and capital, which is why not all companies can successfully navigate and ensure complete cybersecurity. Global banks are among the companies leading the pack when it comes to managing supply chain risk. This is in part due to the fact that they are among the most frequent targets of cybercrime attempts. The big banks spend a lot of time trying to understand how to respond before a crisis occurs. Also, banks tend to see the bad actors in the financial services industry first, so asset managers and others can benefit from looking at how the banks respond.

Conclusion

Awareness and responsibility among all employees will help businesses maintain flexible defenses against the continually evolving threats to their systems. The best practices for cyberdefense, including defenses against supply chain attacks, should be understood by all business leaders and employees for better prevention and reaction. Some sources for learning about best practices include *cyberreadinessinstitute.org*, *CREATe.org* or *NIST.gov*.

Three key steps to help guard against supply chain risk



1 Facing Forward: Cybersecurity in 2019 and Beyond, FireEye, December 2018.
2 Data Risk in the Third-Party Ecosystem (Third Annual Report), Ponemon Institute LLC, November 2018.
3 Threat Predictions for 2019, Kaspersky Lab, December 2018.

About risk
The value of investments and any income will fluctuate (this may partly be the result of exchange rate fluctuations) and investors may not get back the full amount invested.

Important information

This document has been prepared only for those persons to whom Invesco has provided it for informational purposes only. This document is not an offering of a financial product and is not intended for and should not be distributed to retail clients who are resident in jurisdiction where its distribution is not authorized or is unlawful.. Circulation, disclosure, or dissemination of all or any part of this document to any person without the consent of Invesco is prohibited.

This document may contain statements that are not purely historical in nature but are "forward-looking statements," which are based on certain assumptions of future events. Forward-looking statements are based on information available on the date hereof, and Invesco does not assume any duty to update any forward-looking statement. Actual events may differ from those assumed. There can be no assurance that forward-looking statements, including any projected returns, will materialize or that actual market conditions and/or performance results will not be materially different or worse than those presented.

The information in this document has been prepared without taking into account any investor's investment objectives, financial situation or particular needs. Before acting on the information the investor should consider its appropriateness having regard to their investment objectives, financial situation and needs.

You should note that this information:
- may contain references to amounts which are not in local currencies;
- may contain financial information which is not prepared in accordance with the laws or practices of your country of residence;
- may not address risks associated with investment in foreign currency denominated investments; and
- does not address local tax issues.

All material presented is compiled from sources believed to be reliable and current, but accuracy cannot be guaranteed. Investment involves risk. Please review all financial material carefully before investing. The opinions expressed are based on current market conditions and are subject to change without notice. These opinions may differ from those of other Invesco investment professionals.

The distribution and offering of this document in certain jurisdictions may be restricted by law. Persons into whose possession this marketing material may come are required to inform themselves about and to comply with any relevant restrictions. This does not constitute an offer or solicitation by anyone in any jurisdiction in which such an offer is not authorised or to any person to whom it is unlawful to make such an offer or solicitation.