SCCE
corporatecompliance.org

Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

AUGUST 2018

Meet Laura Ellis

Ethics Program Manager for Global Compliance Enablement
Cisco International Limited
Feltham, UK

by Dov Goldman

Five ways to reduce the likelihood of a third-party breach

» Create an inventory of all third parties and identify which of them have access to your data to reduce the risk of a data breach.

» Use a SaaS solution to centralize third-party documentation and workflows to help reduce risk.

» Designate responsibility and accountability to the board of directors/senior leadership to alleviate risk.

» Collaborate across job functions and form a third-party risk management committee to regularly review/update standard risk management processes.

» Ultimately, information security is more about managing risk and building customer trust than building widgets.

Dov Goldman *(dov.goldman@opus.com) is Vice President, Innovation & Alliances for Opus in New York City.*

Some of the largest organizations in the world remain vulnerable to data breaches. Recent widely reported, large-scale data attacks include household names like Best Buy, Sears, Yahoo!, Domino's, Uber, and of course, Equifax. The Identity Theft Resource Center[1] shared that the number of data breaches reported by US organizations reached an all-time high last year. We need a new perspective on risk management protocols—and we need it fast.

Goldman

How to reduce risk

Companies do not realize the vulnerabilities that come from their third-party relationships. A recent survey done by Soha Systems notes that 63% of all data breaches can be attributed to a third party. Consider the Uber data breach. The original exposure occurred through a third-party coding site used by Uber engineers.

A recent report from Ponemon and Opus, "Data Risk in the Third-Party Ecosystem," found these breaches on the rise. More than half (56%) of respondents experienced a third-party data breach, a 7% increase from last year. In the pharmaceutical and healthcare industries, the increase was even sharper: 61%.[2]

Companies do not have an adequate read on third parties throughout their organizations, which puts the companies at risk. Mistakes can be costly. A 2017 Cost of Data Breach Study found US companies spent an average of $7.35 million per breach in fines, remediation costs, and customer loss.[3]

Here are five tips[4] to reduce the likelihood of a third-party data breach.

1. **Manage all third parties based on their risk**

   Prioritize third parties with access to your data, whether it's non-public information about customers or your company's intellectual property; learn whether these third parties share this data with

others. Creating an inventory of all third parties can reduce risk by as much as 19%. Identify which firms have access to sensitive information and manage them in accordance with risk they expose your company to.

2. **Centralize documentation and workflows**
   Reduce risk by 15% to 20% by using a software as a service (SaaS) solution to centralize third-party documentation and workflows and facilitate visibility into, and evaluation of, the security practices of all third parties.
3. **Designate ownership**
   Assign accountability for your company's third-party risk management program from the board of directors and senior leadership to the third-party relationship manager. This can help alleviate risk by 10% to 14%.
4. **Create standards for success**
   Standards save money and drive efficiency. Collaborate across job functions and form a third-party risk management committee to regularly review and update standard risk management processes and controls to reduce risk by up to 15%.
5. **Monitor risks continuously**
   Consistent risk management program oversight can help reduce risks by up to 18%. Review and update vendor management policies regularly as well as conduct audits and assessments to ensure the security and privacy practices of third parties address new and emerging threats.

The influence of leadership

Although there are many factors that can contribute to a system infiltration, employing these tactics can help prevent companies from experiencing a debilitating third-party data breach. There needs to be buy-in from the executive level for companies to keep their information and customers protected. A recent Forrester research report, "Build a High-Performance, Customer-Obsessed Security Organization," stated that information security is about managing risk and building customer trust—not widgets.[5]

Technology plays a significant role in helping companies remain secure, but leadership must implement a sound risk management framework that evolves with changing business models, maintain a strong relationship with their customers, and ensure they are transparent in their security processes. ✳

1. Identity Theft Resource Center: "2017 Annual Data Breach Year-End Review." Available at https://bit.ly/2s3TGM9
2. Available at https://bit.ly/2kf0mDv
3. Available at https://ibm.co/2Bir60B
4. *Ibid*, Ref #2
5. Christopher McClean: "Build A High-Performance, Customer-Obsessed Security Organization" *Forrester*; July 13, 2017. Available at https://bit.ly/2IDqgiT.