WHITE PAPER

What Every GC Needs to Know About Third Party Cyber Diligence

ACC Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

www.acc.com

What Every GC Needs to Know About Third Party Cyber Diligence

The Proliferation of Third Parties

In the age of the Internet of Things, every organization is increasingly dependent on third party vendors and partners throughout every facet of business. IT departments that, not long ago, managed systems and infrastructure, now manage vendors. By one report, the cloud is growing seven times faster than the rest of IT[1] and in a recent survey of 1,002 technical professionals across a broad cross-section of organizations, 95 percent of respondents reported using the cloud.[2]

Beyond IT-related services, practically every function of the enterprise is likely to engage with outside business partners ranging from consultants to law firms. Most of these third parties will have some level of access to your organization's systems and most sensitive data. Even vendors who provide what would be considered "non-technical" services, like mechanical contractors, are today likely to have access to your corporate network.

Yet, in a recent study, 67 percent of respondents say their company did not have an inventory of all third party vendors.[3] It should come as no surprise that more than half of all data breaches can be attributed to third parties.[4] Yet the ACC Foundation found that only seven percent of surveyed in-house counsel are very confident that their third party vendors are protecting the company from cybersecurity risks.[5]

The Role of the General Counsel

THE IT TEAM IS IN CHARGE OF CYBERSECURITY...UNTIL A BREACH HAPPENS.

Cybersecurity is everyone's concern, but the unique role and responsibilities of the general counsel in the organization's overall cybersecurity strategy, and particularly in regards to third parties, is quickly being defined. As the organization's chief advisor on legal responsibilities and mitigating risks, the general counsel is ultimately responsible for ensuring an appropriate and effective cyber diligence process that governs the selection, contracting, and on-going management of third party relationships.

Here are 10 important considerations for every general counsel:

1. *Do you have the right contracts*? The average cost of a data breach in 2016 was over US$7 million.[6] If you have a breach caused by a third party, it will be critical that your contract is sufficient and accurately reflects the nature of the relationship. Also, relationships change over time. What and how services are provided change as well. An effective diligence process is necessary to ensure contracts are appropriate.

2. *New regulations require third party cyber diligence*. There are a host of regulatory requirements impacting a large swath of organizations that explicitly mandate, or in spirit, require, third party cyber diligence including, but not inclusive: GDPR, NY DFS, Federal Contracting Rules, HIPAA, and State Data Safeguard Rules.

3. *If you're not required to conduct cyber diligence today, you probably will be tomorrow*. Cybersecurity legislation was introduced or considered in at least 28 states in 2016 and governments around the world are introducing new regulations.[7]

4. *Your law firms are a prime target*. Selection of outside counsel is the one decision that is typically the sole responsibility of the general counsel. And because law firms hold organizations most sensitive information, they have become a prime target for hackers. According to a report by security consulting firm Mandiant, 80 percent of the 100 largest American law firms have had some malicious computer breach.[8]

5. *You probably have a legal obligation*. Every day, organizations enter binding agreements with customers, employees, and partners that create legal obligation to protect their information using at least a reasonable standard of care.

6. *Cyber issues caused by third parties impact stock performance*. The SEC has long-recognized that cybersecurity breaches increasingly result in material, financial, and reputational consequences that directly impair stock performance. Time and time again, we have seen third parties jeopardize company valuation and stock performance.

7. *What's in your 10-K?* While companies often include threats resulting from third party vendors and partners in their 10-Ks, they often fail to have appropriate controls in place to safeguard against these risks.

8. *Likelihood of litigation*. All companies, their directors, and their officers face the growing likelihood of becoming the subject of regulatory actions from state and federal authorities, as well as lawsuits by customers, employees, partners, and shareholders arising from cybersecurity-related issues. Management and directors must meet increasing expectations to guard against cybersecurity threats, including those resulting from third party vendors and partners.

9. *It's a professional responsibility*. The ABA Standing Committee on Ethics and Professional Responsibility has expanded guidance to all lawyers on what steps should be taken to enhance confidentiality of sensitive information including conducting due diligence on vendors.

10. *It's best practice*. The American Institute of CPAs have issued guidance that third party diligence is a critical component AICPA's cybersecurity risk management reporting framework.

Creating Effective Third Party Cyber Diligence

CONSISTENCY

Many organizations do not have a formal process for conducting third party cyber diligence and those that do are often very inconsistent. Frequently, cyber diligence programs are limited to the third parties perceived to represent the greatest risk. Variables, such as the value of the contract or type of process being performed, often determine if any sort of diligence will be conducted. In reality, the third parties that pose the greatest risk to your organization are often the smallest partners. This ad hoc approach is also inconsistent and makes it nearly impossible to demonstrate consistent execution of controls during investigations, audits, or litigation. Every third party should go undergo a formal diligence process to determine and document their system access and the type of information they can view. Assessments should be conducted at onboarding and annually to identify changes in the relationship that might require more robust cyber diligence and modifications to the terms and conditions that govern the relationship.

RECOGNIZED STANDARDS

There are many different standards that can be used in evaluating cybersecurity posture. This lack of a single uniform standard makes effective evaluation challenging and is difficult for third parties to respond. To address these challenges, the US Department of Commerce's National Institute of Standards and Technology (NIST), along with industry collaboration, issued a framework for improving critical infrastructure cybersecurity. The NIST Framework created a set of industry standards and best practices, including a shared vocabulary about cybersecurity to help decision-makers manage cybersecurity using a risk-based approach. The NIST Framework is quickly becoming the de facto standard of care.

CONCLUSION

The ability to demonstrate a consistent diligence process, based on recognized and relevant security standards and legal requirements provides the foundation of an effective third party cyber diligence program. It provides documented evidence of controls and enables the legal team to demonstrate the adequacy of the program and defend its reasonableness with regulators and courts. This should be a top priority for the general counsel whose organization has not instituted a formal process for conducting cybersecurity diligence on their third parties at onboarding and at regular intervals.

For organizations that have a diligence process, the general counsel should ask these five questions:

1. Does the current process address every third party, including outside legal counsel, that has access to your systems and data?
2. Are third parties measured against appropriate/required security frameworks?
3. Does the current process provide detailed evidence of controls to sufficiently meet the scrutiny of a regulator or outside auditor?
4. Does the current process assure third parties have adequately addressed cyber threats that emerge between formal audits?
5. Are third party relationships inspected periodically to ensure the appropriate degree of diligence is being performed?

[1] Network World February 2017.

[2] Rightscale Cloud Computing Trends: 2017 State of the Cloud Survey.

[3] Data Risk in the Third-Party Ecosystem Ponemon Institute.

[4] PWC Global State of Information Security Survey 2016.

[5] ACC Foundation. (2016). The State of Cybersecurity Report: An In-House Perspective.

[6] Ponemon's 2016 Cost of Data Breach Study: United States.

[7] National Conference on State Legislatures.

[8] ABA Journal March 1, 2017 Law firms Must Manage Cybersecurity Risks.