paloalto NETWORKS®

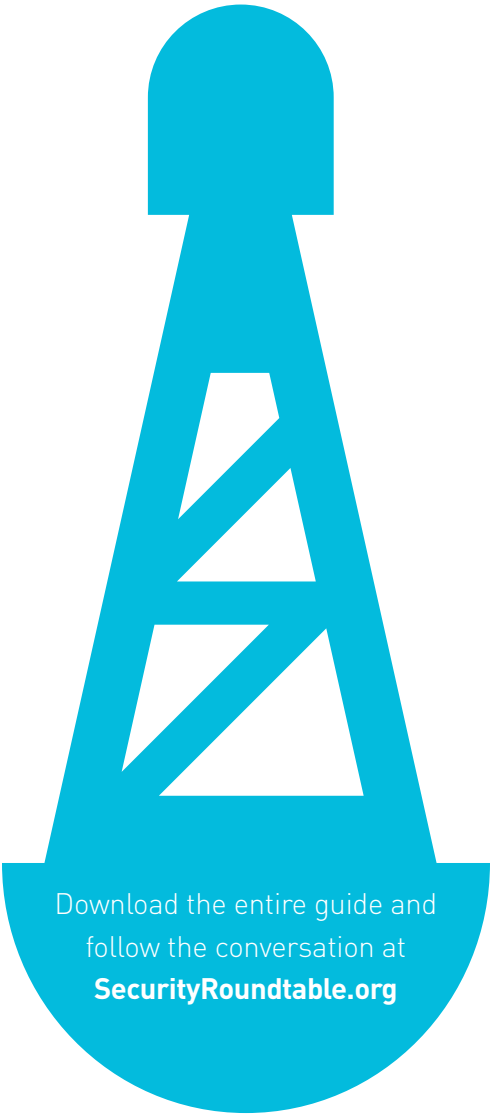
NYSE

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

Georgia Tech Institute for Information Security & Privacy

INTERNET SECURITY ALLIANCE


Download the entire guide and
follow the conversation at
SecurityRoundtable.org

30

Managing risk associated with third-party outsourcing

Covington & Burling LLP – David N. Fagan, Partner; Nigel L. Howard, Partner; Kurt Wimmer, Partner; Elizabeth H. Canter, Associate; and Patrick Redmon, Summer Associate

Third-party outsourcing and cybersecurity risk

Businesses increasingly work with third parties in ways that can render otherwise well-guarded data vulnerable to attack or accidental disclosure. These third parties can include technology service providers; other major business function vendors, such as payroll, insurance, and benefits companies; and accounting and finance, advertising, delivery and lettershop, legal, and other consulting services.

Many of these commercial relationships require sensitive information—whether the business' own confidential business information or the personal information of its employees or customers—to be shared with, or stored by, the third parties. Such relationships also may entail third-party access to a company's networks. There is, in turn, an inherent risk in the third-party services: they can create new avenues of attack against a company's data or its systems and networks—and those avenues require appropriate mitigation.

Perhaps no data security breach highlighted this risk more than the incident incurred by Target. That incident began not with a direct attack on the Target network but with a phishing attack on a Pennsylvania HVAC contractor that had access to Target's external billing and project management portals. The HVAC contractor depended on a free version of consumer anti-malware software that allegedly failed to provide real-time protection. Once the phishing campaign succeeded in installing key-logging malware, the hackers obtained the HVAC contractor's credentials to Target's external billing and project management systems and from there infiltrated Target's internal network, eventually reaching Target's customer databases and point-of-sale systems.

The results of the Target breach are well known: the personal information of up to 70 million customers was compromised, and about 40 million customers had their credit or debit card information stolen. By the end of 2014, the costs to Target from the breach had exceeded $150 million. These costs include the litigation and settlement expenses resulting from lawsuits brought by consumers and credit card issuers. Further, in the quarter in which the data breach occurred, Target's year-over-year earnings plummeted 46 percent. Ultimately, in the aftermath of the breach, Target's CEO resigned.

The Target breach was not an isolated incident. In 2014, a Ponemon Institute survey found that in 20 percent of data breaches, a failure to properly vet a third party contributed to the breach. Even more troubling, 40 percent of the respondents to another Ponemon survey named third-party access to or management of sensitive data as one of the top two barriers to improving cybersecurity. Further, the Ponemon Institute's 2015 U.S. Cost of Data Breach Study reports that third-party involvement in a data breach increased the per capita cost of data breaches more than any other factor. However, despite the cybersecurity risks posed by third-party service providers, many companies fail to systematically address such risks. Only 52 percent of companies surveyed in a 2014 Ponemon Institute report have a program in place to systematically manage third-party cybersecurity risk.

Legal risks

Although there are many commercial and other reasons to adopt strong third-party risk management processes, a variety of legal frameworks require the management of third-party risk. Examples of such statutory or regulatory requirements include the following:

- the Interagency Guidelines Establishing Information Security Standards that implement Section 501 of the Gramm-Leach-Bliley Act and require financial institutions to engage in due diligence in the selection of service providers, to use contractual provisions to manage third-party risk, and, in some cases, to monitor service providers on an ongoing basis (e.g., 12 C.F.R. Pt. 225, App. F at III.D. [2012])
- the HIPAA Privacy Rule, requiring specific contractual provisions in dealing with business associates who handle protected health information, 45 C.F.R. §164.502(e) (2014)
- state regulations, such as the Massachusetts Standards for the Protection of Personal Information, requiring reasonable steps in selecting third parties and the use of contractual provisions to require their compliance with Massachusetts law, 201 Mass Code Regs. 17.03(2)(f).

In addition, the Federal Trade Commission has applied its authority under Section 5 of the FTC Act, 15 U.S.C. §45 (governing unfair acts and deceptive trade practices) to apply to cybersecurity and data security, and has taken action against companies that fail to take "reasonable steps to select and retain service providers capable of appropriately safeguarding personal information" a de facto regulatory requirement. See, for example, GMR Transcription Servs., Inc., F.T.C. Docket No. C–4482, File No. 122–3095, 2014 WL 4252393 (Aug. 14, 2014).

Sources of third-party cybersecurity risk

The cybersecurity and privacy risks generated by third-party engagements include the following:

- breaches of personal data—whether the personal data of customers or employees—and the attendant regulatory obligations (e.g., notification requirements), as well as legal liability, as in the Target breach
- breaches of a business's proprietary data, including the following:
  - competitively sensitive data, privileged information, attorney work product, and trade secrets
  - business partner data resulting in obligations to notify business partners

as well as potential contractual liability to them
  - data that result in financial harm to the company, such as bank account information
  - other confidential, market moving insider information in the hands of third parties such as investment bankers, consultants, and lawyers, such as information regarding nonpublic M&A activity, clinical trial results, or regulatory approvals
- the introduction into internal networks of viruses or other malicious code, as in the Dairy Queen attack, in which vendor credentials were used to gain access to internal networks and eventually install malware targeting point-of-sale systems
- the introduction of other vulnerabilities to IT systems, for instance, by the use of vulnerable third-party applications or code, as occurred in the Heartbleed OpenSSL exploit that potentially exposed the data transmitted to and from secure web servers
- misuse and secondary use of company data such as for direct marketing or data mining for the benefit of the vendor
- "fourth-party" risk, that is, the third-party cybersecurity risks introduced by a vendor's relationships with its own third-party service providers and vendors
- potential director or management liability for breach of fiduciary duty in the exercise of cybersecurity oversight.

To help manage this array of risks effectively, companies may consider whether they have appropriate procedures in place to evaluate and monitor individual vendors, as well as a program to manage and monitor third-party relationships.

Engagement-level management of third-party cybersecurity risk

The appropriate measures needed to scrutinize and monitor third-party service providers will depend to a large extent upon the sophistication of the vendor and the nature of the IT systems and data at issue. Nonetheless, three elements are common to all third-party risk management:

1. due diligence prior to entering an engagement
2. contractual commitments and legal risk management
3. ongoing monitoring and oversight.

Pre-engagement due diligence

A critical element of managing third-party risk is the assessment of the third party's own security practices and posture before any contract is signed. Such diligence is crucial for the identification and evaluation of risks, and, in turn, can ensure that such risks are mitigated before the engagement, including through the use of contractual provisions. The actual evaluation may be more ad hoc (i.e., conversations with key business or technology stakeholders) or formal (i.e., through a questionnaire or even on-site assessment), and the extent of an evaluation may depend on various factors in the prospective relationship, including, for example, whether the service provider will have access to the company's IT systems, the nature of the information that it may access, and whether it will store such information.

Depending on the extent of the relationship and information that may be accessed by the vendor, the following areas of inquiry may be necessary to inform a cybersecurity diligence assessment:

- whether and how often the vendor has experienced cybersecurity incidents in the past, the severity of those incidents, and the quality of the vendor's response
- whether the vendor maintains cybersecurity policies, such as whether the vendor has a written security policy or plan
- organizational considerations, such as whether the vendor maintains sufficient and appropriately trained personnel to

protect the data and/or service at issue and respond to incidents
- human resources practices, particularly background screening of employees, cybersecurity training, and the handling of terminations
- access controls, particularly whether controls are in place that restrict access to information and uniquely identify users such that access attempts can be monitored and reviewed
- encryption practices, including whether information is encrypted at rest, whether information transmitted to or from the vendor is properly encrypted, and whether cryptographic keys are properly managed
- evaluation of in what country any data will be stored
- the vendor's policies regarding the secondary use of customer data, and whether IT systems are created in such a way as to respect limitations on secondary use
- physical security, including resilience and disaster recovery functions and the use of personnel and technology to prevent unauthorized physical access to facilities
- back-up and recovery practices
- change control management, including protocols on the installation of and execution of software
- system acquisition, development, and maintenance to manage risk from software development or the deployment of new software or hardware
- risk management of the vendor's own third-party vendors
- incident response plans, including whether evidence of an incident is collected and retained so as to be presentable to a court and whether the vendor periodically tests its response capabilities
- whether the vendor conducts regular, independent audits of its privacy and information security practices

Contractual risk and negotiation

In addition to evaluating third parties on the basis of their cybersecurity practices, another important risk mitigation tool is the actual contractual language. As with other areas, contractual requirements can be an effective way to allocate risk and responsibility for potential breaches of cybersecurity, including the investigation and remediation of such incidents. Commonly negotiated terms include the following:

- a requirement that the vendor have a written information security program that complies with applicable law or other regulatory or industry standards
- limits and conditions on the use of subcontractors and other third-party service providers
- restrictions on secondary use of data, including making clear that the customer remains the owner of any data transmitted to the vendor and any derivatives of that data
- mandatory and timely notification in case of a security incident
- rights to audit or otherwise monitor the vendor's compliance with the terms of the contract
- in case of a breach, a requirement that the vendor take on reasonable measures to correct its security processes and take any necessary remediation steps
- provisions ensuring an orderly transition to in-house systems or another third party in case of the termination of the relationship.

In addition to such terms, indemnification clauses can be used to shift the risk of data breach onto the third party and to incentivize healthy security practices. To accompany an indemnification clause, it sometimes can be desirable to draft clauses that define when the entity is or is not liable, on which party the burden of proof falls, and how root-cause analysis should be conducted. To ensure capacity to take on the financial costs

of a breach, third parties are frequently required to obtain a cybersecurity insurance policy.

From the business's perspective a third-party vendor should be fully responsible for any liability for data breaches that occur while the data are under the vendor's control. However, vendors often push for caps on their cybersecurity liability. To guide negotiations as to appropriate caps on liability, consider the type of data processed or accessed by the third party (e.g., how sensitive is it, does it relate to employees, consumers, or is it not personally identifying information), the volume of records to be handled by the third party, the ability for the customer to implement security controls such as encryption, the nature and extent of the third-party promises on cybersecurity, and the brand and reputation of the third party with respect to data security. Based on those inputs, a company can then consider the potential losses and sources of third-party liability to evaluate what constitutes an acceptable level of risk in terms of exclusions for indemnifications and caps on liability. A business also may consider offsetting any contractual concessions with corresponding increases in their own cybersecurity insurance coverage.

Ongoing monitoring and oversight

Ongoing monitoring and oversight of third-party service providers is essential given the rapidly changing landscape of cybersecurity threats. Whereas due diligence provides a snapshot of a third party's cybersecurity stance at a specific point in time, continual monitoring and the right to such monitoring are necessary to help ensure that the third party responds and adapts to secure its systems against new threats. Over the life of the relationship, periodic checks, including on-site reviews of vendor, can be important oversight mechanisms. Other monitoring requirements include access to timely and accurate records and reports of the third-party provider's cybersecurity posture.

Although relatively uncommon outside of certain regulated industries, such as the financial and health-care industries, provisions in vendor contracts for regular security audits by an independent third party provide a robust but intrusive form of periodic monitoring. However, it is not always possible to obtain audit rights from a vendor. Alternatively, the vendor could be required to provide up-to-date certifications of compliance with industry standards or regular, third-party audit reports. In addition, to manage fourth-party risk, vendors could be required to perform initial and periodic assessments of their own service providers and vendors if they will be handling sensitive information. If, in the course of an audit, vulnerabilities are identified or practices are found that are not in compliance with industry practices or regulatory requirements, the vendor may be required to notify the customer and correct any outstanding issues in a timely fashion.

As part of ongoing monitoring of vendor cybersecurity, it is useful if the contract with a third-party service provider also includes notification and remediation provisions if the vendor becomes aware of deficiencies in its cybersecurity posture. In addition, as part of the remedies, the outsourcing party may seek the right to terminate the agreement immediately and to receive a pro rata refund of any fees paid or payable. In addition to contractual provisions dealing with the termination, contingency plans to facilitate an orderly end to the third-party relationship and a smooth transition to an in-house solution or another a third-party provider may prove useful.

Conclusion

The measures described above—diligence, contractual terms, and continued monitoring and oversight—are critical elements of a comprehensive cybersecurity program that includes managing third-party relationships. To effectuate these elements, in turn, it often

is helpful to have standardized processes and documentation.

Examples include standardized diligence checklists and questionnaires, template contract addendums addressing cybersecurity issues, and standardized schedules for audits and other forms of monitoring. Because there is no one-size-fits-all approach that is appropriate for every vendor, it is appropriate to implement a tiered approach that scales due diligence, contractual obligations, and oversight processes according to the nature and extent of the cybersecurity risks presented by the vendor relationship. In all events, it is important that organizations periodically review their processes for evaluating and overseeing third-party relationships to ensure that such processes are periodically updated and appropriately tailored to address new and emerging threats.

COVINGTON

Covington & Burling LLP

One City Center
850 Tenth Street, NW
Washington, DC 20001-4956
Tel +1 202 662 6000
Web www.cov.com

DAVID N. FAGAN

Partner
Email dfagan@cov.com

David N. Fagan, a partner in Covington's global privacy and data security and international practice groups, counsels clients on preparing for and responding to cyber-based attacks on their networks and information, developing and implementing information security programs, and complying with federal and state regulatory requirements. Mr. Fagan has been lead investigative and response counsel to companies in a range of cyber- and data security incidents, including matters involving millions of affected consumers.

NIGEL L. HOWARD

Partner
Email nhoward@cov.com

Nigel L. Howard, a partner in Covington's New York office, helps clients execute their most innovative and complex transactions involving technology, intellectual property, and data. Mr. Howard has been at the forefront of initiatives to protect data assets for his clients, helping them achieve a competitive advantage or fend off a competitive threat. He advises clients on their proprietary rights to data and global strategies for protecting these assets. He has represented companies in transactions covering the full spectrum of data-related activities, including data capture and storage, business and operational intelligence, analytics and visualization, personalized merchandizing, and the related cloud computing services, such as Data as a Service and Analytics Infrastructure as a Service.

KURT WIMMER

Partner
Email kwimmer@cov.com

Kurt Wimmer is a Washington partner and U.S. chair of Covington's privacy and data security practice. Mr. Wimmer advises national and multinational companies on privacy, data security, and digital technology issues before the FTC, the FCC, Congress, the European Commission, and state attorneys general, as well as on strategic advice, data breach counseling and remediation, and privacy assessments and policies. He is chair of the Privacy and Information Security Committee of the ABA Antitrust Section and is a past managing partner of Covington's London office.

ELIZABETH H. CANTER

Associate
Email ecanter@cov.com

Elizabeth H. Canter is an associate in the Washington, DC, office of Covington. She represents and advises technology companies, financial institutions, and other clients on data collection, use, and disclosure practices, including privacy-by-design strategies and email marketing and telemarketing strategies. This regularly includes advising clients on privacy and data security issues relating to third-party risk management. Ms. Canter also has extensive experience advising clients on incident preparedness and in responding to data security breaches.

PATRICK REDMON

Summer Associate
Email PatrickRedmon@gmail.com

Patrick Redmon will graduate from the University of North Carolina School of Law in 2016. He graduated from Fordham University in 2007 with a BA in Philosophy and Economics and in 2013 was awarded an MA in Liberal Arts from St. John's College in Annapolis, Maryland. Mr. Redmon is the Managing Editor of the *North Carolina Law Review*.