ALSTON&BIRD

WWW.ALSTON.COM

Privacy & Security ADVISORY ■

JANUARY 25, 2016

The Importance of Strategic Vendors in Breach Response

By Jim Harvey and Karen Sanzaro

Cybercrime and data security incidents are on the rise. Publicized cyber incidents have become so prevalent that it would be difficult to find someone who has not received at least one breach notification letter in the mail. While most companies are devoting increased efforts and resources to manage this risk, cyber criminals are constantly devising new and more creative means of attack, including targeting larger companies via their smaller and often less technologically sophisticated third-party service providers.

Data security breaches are nearly inescapable in the current environment, and the ensuing investigation and remediation process can be quite costly and complex, requiring access to and interpretation of a morass of highly technical data. The process is further complicated if (as is frequently the case) the breach implicates a company's third-party service provider or the services provided by the third party. This is an even greater concern when the service provider relationship is extensive or the services are strategic or essential to a company's ongoing operations, such as IT infrastructure services and certain cloud-based service offerings. In these circumstances, the company has the customer relationships and (in most cases) the compliance and notification responsibility, but has to rely on the cooperation and assistance of its service provider in order to obtain the information necessary to meet its compliance obligations and to otherwise mitigate the effects of the breach and preserve its customer relationships. If the service provider is the one that experienced the breach or was responsible for the security activities that gave rise to the breach, the incident response process may be further complicated because the service provider's objectives in this circumstance may be in conflict with the needs of its client.

Despite the ubiquity of cyber threats and the increased awareness by businesses of the need for robust cybersecurity and vendor management policies, many such policies still do not adequately take into account the risks posed by third-party service providers or contemplate appropriate breach response activities for security incidents involving service providers or otherwise requiring the cooperation of critical service providers. While regulators have acknowledged the risks presented by third-party service providers for quite some time, the guidance generally addresses pre-breach activities, emphasizing the need for due diligence, ongoing oversight, robust contract protections and breach notification requirements. To date, regulators (and many businesses) have not focused on the specifics of managing the vendor relationship *after* a breach has occurred.

Risk-based advance preparation and planning—conducted together with your vendors—will help ensure a more efficient and effective response in the event a security incident occurs, and will benefit all parties involved.

Vendor-Related Breaches

A significant number of cybersecurity incidents involve third-party service provider relationships. In fact, several recent high-profile breaches were attributable to access gained from a company's service provider. In the Target breach (reported December 2013), approximately 40 million credit and debit card accounts were exposed to hackers who were able to gain access to Target's network using credentials stolen from a third-party HVAC vendor.[1] The HVAC vendor maintained a connection to the Target network for electronic billing, contract submission and project management. Similarly, in the Home Depot breach (reported September 2014), hackers used credentials stolen from a third-party vendor to access point-of-sale data on Home Depot's network, resulting in access to approximately 56 million payment card accounts and 53 million email addresses.[2] Hackers responsible for one of the Office of Personnel Management (OPM) breaches used credentials obtained from a contractor used by OPM to conduct background investigations to gain access to OPM systems and vast amounts of potentially sensitive data. These examples illustrate the potentially significant risks posed by third-party relationships, though the vendors' involvement in the post-breach activities in this type of incident is more limited. The complications increase exponentially when the vendor is critical to a company's breach response or when there may be some question about which party's actions or inactions resulted in the breach.

Regulatory Guidance

Regulators in the United States—particularly in the highly regulated financial services and health care areas—are increasingly focused on the cybersecurity risks posed by third-party service providers. Most regulator guidance in this area advises companies to factor third-party service providers into their cyber risk planning using a risk-based approach. The guidance, however, generally focuses on breach prevention activities (pre-breach planning and vendor diligence and management), rather than the specific activities that should take place *after* a breach occurs.

Financial services

Financial institutions are subject to a number of laws regulating the security of consumer financial data,[3] and financial services regulators have issued a plethora of guidance addressing third-party risk management, stressing the need for robust vendor management policies, comprehensive due diligence, contracting requirements and ongoing supervision and monitoring. For example, the Federal Financial Institutions Examination Council (FFIEC) and Office of the Comptroller of the Currency (OCC) have published guidance specific to the risks posed by third-party service providers. The FFIEC has issued guidance on the outsourcing of technology services ("Outsourcing Guidance") and on the supervision of service providers ("Service Provider Guidance"), in addition to other more general guidance that also speaks to the potential cybersecurity risks associated with third-party service providers.[4] The FFIEC has also developed a cybersecurity assessment tool for financial institutions that includes the use of third-party vendors as a risk factor.

---

1 See Congressional Testimony from Target CFO John Mulligan.

2 See press releases issued by The Home Depot on Sept. 18, 2014 ("The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores") and Nov. 6, 2014 ("The Home Depot Reports Findings in Payment Data Breach Investigation").

3 E.g., the Gramm-Leach Bliley Act; Regulation S-P (applicable to broker/dealers).

4 See, e.g., FFIEC's Business Continuity Planning IT Examination Handbook, which was updated in February 2015 to include Appendix J (Strengthening the Resilience of Outsourced Technology Services). Appendix J includes a section dealing with cyber resilience that emphasizes the need to incorporate the potential impact of a cyber event into business continuity planning. It notes that banks and their providers should consider "identifying and making advance arrangements for third-party forensic and incident management services," but does not go into further detail.

The FFIEC's Outsourcing Guidance emphasizes the importance of performing comprehensive due diligence in selecting third-party service providers and specifies the types of provisions that the outsourcing contract should include (e.g., an obligation to disclose security breaches). The Outsourcing Guidance includes more specific direction when entering into cloud-based relationships (e.g., requiring encryption of data stored and in transit and an assessment of risk mitigation measures in multitenant environments) and when engaging a vendor to provide managed security services, such as intrusion detection and prevention (e.g., maintenance of an incident response plan that includes a remediation process).

The OCC issued well-publicized risk management guidance for third-party relationships in October 2013 in response to concerns "regarding the quality of risk management on the growing volume, diversity, and complexity of banks' third-party relationships…" (the "OCC Guidance"). Like the FFIEC's guidance, the OCC Guidance focuses on risk management planning, vendor due diligence, contract requirements and ongoing monitoring and oversight. It discusses the need to assess the vendor's information security program and ability to respond to cyberattacks as part of the due diligence and oversight. It also speaks to vendor-caused breaches, noting that vendor contracts should stipulate: (1) that intrusion notifications include estimates of the effects on the bank and specify corrective action to be taken by the vendor; (2) whether and how often the bank and the vendor will jointly practice incident management plans; and (3) whether and how often the bank and the vendor will jointly practice business continuity and disaster recovery plans. Even so, the guidance is still relatively high level.

Health care

The main regulations governing data security in the health care space are the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act. Notably, the HITECH Act amended HIPAA to impose direct liability on third-party vendors (referred to under HIPAA as "business associates"). Thus, business associates are directly liable for certain things, including compliance with the data security safeguards and breach notification rules. Other than a business associate's obligation to notify the covered entity[5] in the event of a breach, the HIPAA and HITECH regulations do not offer any specific guidance on what measures a covered entity should take in response to a security breach by one of its business associates.

Other industries

Outside of the highly regulated financial services and health care industries, both the Federal Trade Commission (FTC) and California attorney general's office have been relatively prolific issuers of privacy and data security-related guidance. Neither, however, have issued any materials that include specific guidance on how businesses should respond to a vendor's security breach after the fact. For example, recent FTC guidance advises businesses to "keep a watchful eye on your service providers," document security-related requirements in the service provider's contract and monitor the service provider for compliance on an ongoing basis. Other FTC guidance takes vendor relationships into account, but does not generally speak to breach response activities (other than guidance on certain notification obligations). The California AG's "Cybersecurity in the Golden State" (February 2014) is notable for its absence of any reference to the potential data security risks posed by a business's vendors.

---

[5] Covered entities (i.e., health care providers, health plans and health care clearinghouses) are regulated entities under HIPAA, with responsibility for ensuring the safety of their protected health information (PHI). Covered entities may engage business associates to provide services that require access to PHI subject to certain requirements (such as entering into a written agreement with the business associate), in which instance the business associates become directly liable under certain provisions of HIPAA and the HITECH Act.

Real World Breach Response

The key item that most regulatory guidance does not confront in any detail, with the minimal exception of the OCC Guidance, is the enormous complexity of breach response, which may be exacerbated by the involvement of a vendor in a significant manner. The guidance is generally concentrated on breach prevention activities, leaving it up to companies to consider and plan for the fundamental aspects of breach investigation and remediation involving a third-party vendor. These considerations include designating which party will actually conduct the investigation, how frequently such party will report on the status of the investigation, the ability of the non-investigating party to independently access and assess evidence produced by the investigation and the timing of the investigation. Without advance agreement on these details, a company could well be left at the mercy of its vendor, whose actions under such circumstances will include both responding to the customer's crisis and protecting its own enterprise and legal interests.

In the event of a complex third-party intrusion, a company must first investigate the situation to find out what is causing the unauthorized data access or exfiltration and, depending on the circumstances, take steps to eliminate that access and/or exfiltration. This has to be done as quickly as possible, as potentially millions of dollars in company valuation, customer trust, legal expense and damages and systems repair costs frequently hang in the balance. Once the situation has been brought under appropriate control, the company can then turn to remediation of its data, network and systems to repair the damage done by the attack and prevent similar attacks in the future.

While this may sound relatively simple and straightforward, in practice it is usually quite complex. First, the relevant information from the network and affected systems has to be gathered in a forensically sound manner, as those materials likely constitute a crime scene and may be introduced as evidence in litigation, government investigations or other adversarial proceedings. Second, after the relevant systems are identified and preserved, they have to be analyzed to determine exactly what happened. Investigative inquiries generally seek to answer the following questions: did the criminals have access to personally identifiable information or other sensitive (or valuable) data; did they create copies of data to which they gained access; did they actually remove data that they copied; did they alter information resident on the system; did they create a means to re-enter the system; how did they get in; how did they get out; were any laws that require notification to third parties triggered; do other, similar means of entry into the system exist. In connection with such inquiries, it is frequently necessary to:

- Deploy software agents on the network to search for malware and other indicators of compromise.
- Create monitoring capability for traffic entering or exiting the network and all changes to systems on the network.
- Possibly investigate live memory (RAM), which requires that the machine not be turned off (lest the memory be sacrificed).
- Engage in forensic deep dives on individual systems to attempt to discern the tactics of the criminals.

To complicate matters further, sophisticated criminals are also likely deploying multiple antiforensic techniques to cover their tracks. These include tactics such as encrypting exported files and then deleting those files after exportation, repairing changes to log files, masquerading as authorized users on the network and many other tactics designed to obfuscate their presence and activities on the system.

The complexity of these investigations leaves companies struggling to satisfy the competing needs to notify regulators and the public as quickly as possible, while also providing detailed, understandable and reliable information to their customers, employees, shareholders, regulators and (where applicable) investigators for credit card brands (PCI forensics investigators, or PFIs). Given the complicated nature of these investigations, and the corresponding notification requirements, it becomes clear why the presence of a third-party vendor on whom a company must rely has the potential to complicate and slow the execution of the investigation, containment and remediation of the incident.

While vendors may be critical to the investigation and remediation and may have been contractually responsible for the systems that gave rise to the breach, the underlying compliance obligation to regulators, the public and practically every interested constituency (whether by statute, regulation or expectation) remains with the company—it is not possible to outsource compliance.[6] While vendors may profess a desire and genuinely attempt to do the right thing, the essence of the situation is that the vendor is motivated to both preserve and enhance the customer relationship, while hopefully avoiding facts or circumstances that might be used to argue that it breached its duties established by the underlying agreement (to the extent those facts exist). The risk with these dual concerns, though, is that any motivation of any involved party for any purpose other than immediate investigation, containment and remediation of the incident may delay those activities and potentially reduce their efficiency and effectiveness.

Companies also need to determine exactly how the investigation, containment and remediation will occur. It is unlikely that a vendor will simply throw open the doors of its network and systems and allow unfettered access to address the situation. While this reluctance may be well-placed (either due to obligations to third parties also residing on those systems or to an unwillingness to reveal the vendor's own detailed security policies and procedures), it raises the question of exactly how a company can accomplish the required activities in a complex breach response scenario. Companies can avoid (or at the very least minimize) these potential complications for critical vendor relationships by considering and documenting each party's rights and obligations regarding breach response activities as part of the contractual documentation *before* a breach occurs, rather than sorting out the details on the fly in the midst of an extreme crisis.

Vendors may also have countervailing obligations to other third parties that conflict with the need to move as quickly as possible and provide unfettered access to as much information as possible. If any of the breached entity's systems are on shared networks, or worse yet shared systems or applications, obligations of the vendor to the party (or parties) with whom the system is shared may frustrate, if not entirely prevent, unfettered access to that system by the company and its investigators. This then creates a situation where the company has to rely on the vendor to either obtain authorization from the third party (which could take days) or to conduct some sort of information gathering and investigation on behalf of the company, which may slow, or decrease the effectiveness of, the investigation and related activities.

Consideration also needs to be given to the privileged aspect typical to many of these investigations. Companies often have inside or outside counsel hire investigators that operate at the direction of counsel for the purpose of conducting a privileged investigation. If the vendor, or worse yet the vendor's investigator, will be carrying out activities that would have otherwise been carried out by a company's privileged investigator, consider what impact that may have on the privileged nature of the investigation in the first place. While one might construct a joint interest privilege agreement that could theoretically address certain of these issues, that agreement itself will likely take valuable time (hours, but more likely days) to draft and negotiate with the vendor and possibly other involved third parties. Moreover, if the vendor insists on a confidentiality agreement being signed by the company's investigator, that agreement needs to be considered in light of conducting the investigation on a privileged basis. While it is difficult to predict all of the potential complications that might arise with the privilege in these scenarios, the issue should be top of mind as the engagement is structured and the activities conducted.

---

[6] Note that vendors may have direct compliance obligations (e.g., business associates under HIPAA/HITECH and data processors under the newly enacted General Data Protection Regulation (GDPR) in Europe, which, among other things, will impose (when it takes effect, likely early 2018) direct obligations on data processors to implement risk-based security measures). In addition, in certain instances, financial services regulators have authority to examine and regulate third-party vendors performing regulated functions on behalf of a bank. This does not, however, lessen or obviate a company's own compliance obligations, which are generally more extensive than those placed on subcontractors.

Practical Pointers

Advance planning is key in managing risks arising from third-party service providers. In addition to the due diligence, oversight and contract provisions recommended in the current regulatory guidance, below are some practical considerations to factor into cyber risk management and incident response strategies that can help companies be better prepared in the event of an actual security incident:

- Adopt vendor management processes that provide for assessment of a third party's cybersecurity capabilities as part of initial due diligence and ongoing oversight.
- Actively include strategic service providers in incident response planning and tabletop exercises.
- Regularly test (and update) a response plan for third-party breaches.
- Include appropriate audit rights and other provisions in vendor contracts to provide for the necessary ongoing oversight, as well as requiring participation in incident response planning.
- Minimize the presence of shared networks and systems where relevant sensitive information is stored or processed.
- Include appropriate post-breach investigation and remediation "rules of the road" in vendor agreements, such as:
  - The vendor's obligation to preserve relevant evidence (in a forensically and legally sound fashion).
  - The company's right to investigate/engage a forensic investigator and related privilege considerations.
  - Whether and how the company and its forensics investigators (and PFIs, if required) will be allowed to directly access the evidence.
  - Whether and how the company (and its investigators) will be afforded physical access to systems and the network (including installation of software), with particular attention to negotiation of required confidentiality agreements before the crisis occurs.
  - How quickly (and completely) the vendor will respond to requests for information and how that will be measured.
  - Under what circumstances the vendor may separately charge for some or all of the resources that it dedicates to the breach response.
  - Liability allocation for the post-breach activities and any third-party claims (including regulatory fines or penalties) arising out of the breach.

If you have questions or would like assistance in evaluating your vendor management and incident response policies, please contact Jim Harvey or Karen Sanzaro.

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Security Group

Atlanta

Kacy McCaffrey Brake
kacy.brake@alston.com
404.881.4824

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

Angela T. Burnette
angie.burnette@alston.com
404.881.7665

David Carpenter
david.carpenter@alston.com
404.881.7881

Lisa H. Cassilly
lisa.cassilly@alston.com
404.881.7945

Julia Dempewolf
julia.dempewolf@alston.com
404.881.7169

Maki DePalo
maki.depalo@alston.com
404.881.4280

Clare H. Draper IV
clare.draper@alston.com
404.881.7191

Peter K. Floyd
peter.floyd@alston.com
404.881.4510

James A. Harvey
jim.harvey@alston.com
404.881.7328

John R. Hickman
john.hickman@alston.com
404.881.7885

William H. Jordan
bill.jordan@alston.com
404.881.7850
202.239.3494

David C. Keating
david.keating@alston.com
404.881.7355

W. Scott Kitchens
scott.kitchens@alston.com
404.881.4955

Dawnmarie R. Matlock
dawnmarie.matlock@alston.com
404.881.4253

Bruce Sarkisian
bruce.sarkisian@alston.com
404.881.4935

Peter Swire
peter.swire@alston.com
404.881.4259

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael R. Young
michael.young@alston.com
404.881.4288

Los Angeles

David Caplan
david.caplan@alston.com
213.576.2610

Kimberly K. Chemerinsky
kim.chemerinsky@alston.com
213.576.1079

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

Katherine E. Hertel
kate.hertel@alston.com
213.576.2600

Sheila A. Shah
sheila.shah@alston.com
213.576.2510

Dominique R. Shelton
dominique.shelton@alston.com
213.576.1170

Evan Sippel-Feldman
evan.sippel-feldman@alston.com
213.576.1098

Washington, D.C.

Louis S. Dennig IV
lou.dennig@alston.com
202.239.3215

Kimberly K. Peretti
kimberly.peretti@alston.com
202.239.3720

Karen M. Sanzaro
karen.sanzaro@alston.com
202.239.3719

Eric A. Shimp
eric.shimp@alston.com
202.239.3409

Paula M. Stannard
paula.stannard@alston.com
202.239.3626

Jason R. Wool
jason.wool@alston.com
202.239.3809

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON&BIRD