CAHILL

July 20, 2020

Maintaining Cybersecurity with Third Parties and Vendors Receiving Sensitive or Private Data

In May 2020, a prominent media and entertainment law firm fell victim to a ransomware attack, risking the widespread release of sensitive, valuable, and potentially damaging information belonging to its clients, which include A-list celebrities like Lady Gaga and Robert De Niro.[1] The hackers' ransom demands have exceeded $40 million, with threats to release personal client information to the public if their demands are not met. Then, in early July, the hackers reportedly placed documents belonging to Nicki Minaj, Mariah Carey, and LeBron James up for auction on the dark web.[2] This high-profile extortion effort serves as a stark reminder of the significant and growing cyber risks that exist with the many third parties that use, secure, and process sensitive data for others.

On July 15, 2020, Twitter experienced what it has described as a "coordinated social engineering attack," in which unauthorized entities gained access to the Twitter accounts of prominent cryptocurrency leaders and companies as well as some of the highest profile people in America, including Barack Obama, Bill Gates, Kanye West, and Elon Musk. The compromised accounts then sent tweets intended to deceive Twitter users into sending money to a specified Bitcoin address. Private "direct messages" sent and received by these accounts may also have been accessed.[3] This incident again underscores the potential havoc that cybersecurity events of third parties can wreak upon an organization.

Cyber risks are increasing generally, as more and more valuable data becomes accessible to hackers. As the Internet of Things becomes more ubiquitous, sensitive data is increasingly stored on connected devices such as laptops, tablets, routers, smart watches, manufacturing equipment, and even automobiles. While these are valuable tools for organizations, their proliferation has led to greater network vulnerability, increasing the possibility of a cybersecurity incident. According to the "2019 Year End Report" by Risk Based Security, a firm specializing in vulnerability intelligence and breach data, the total number of records exposed by cybersecurity breaches increased by 284% compared to 2018. At the same time, companies increasingly look to outsource non-core functions, creating new security risks through the electronic flow of private and sensitive data to third parties. The Ponemon Institute, an organization dedicated to the advancement of responsible information and privacy management practices, published a 2019 report entitled "The Cost of Third Party Cybersecurity Risk Management," which estimates that over half of all data breaches in the U.S. are attributable to hacks of third party information systems, rather than hacks of the data owner's information systems directly. In addition, a July 10, 2020 Risk Alert entitled "Cybersecurity: Ransomware Alert," from the Security and Exchange Commission's Office of Compliance Inspections and Examinations observes an "apparent increase" in the sophistication of ransomware attacks against SEC registrants and their service providers.[4]

Even for a company with state-of-the-art information security, relationships with vendors that process, store, or otherwise receive sensitive company data pose significant unknown and potentially serious risks from cyber hacks and malware, such as ransomware that renders a company's data inaccessible until an extortion payment is made. What follows are some best practice tips to keep in mind when sharing data with outsiders and selecting third parties that will receive company data.

[1] https://www.law.com/americanlawyer/2020/05/15/lady-gagas-law-firm-got-hacked-now-what/

[2] https://www.computerweekly.com/news/252485589/Sodinokibi-gang-begins-dark-web-celebrity-data-auctions

[3] https://www.newsweek.com/twitter-bitcoin-hack-direct-messages-stolen-1518247

[4] https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf

I. The Data Ecosystem

For almost all companies today, sensitive company information is stored and managed by a number of different entities, so managing cyber risk involves more than simply protecting against a direct attack. In the regular course of business, companies have ongoing relationships with a myriad of partners, suppliers, and service providers, with whom sensitive information must be shared. Organizations also use third parties, known as "data processors," whose specific service to the company is the processing and storage of company data. While this third-party access to company data can be both beneficial and practical, a company must appreciate that any sharing of sensitive or private data outside the organization increases the risk of exposure to a cybersecurity incident in important and potentially unanticipated ways.

II. Understanding Third-Party Cyber Risk

Before exploring third-party risk, it is important to emphasize that an optimal cybersecurity program begins with robust internal policies, procedures, and controls, with a strong tone-at-the-top to reinforce policies, as well as training and engagement by all employees. Established security standards and protocols can guide program elements, or a company can engage with outside vendors to review and certify security according to a variety of developed frameworks, including the NIST Cybersecurity Framework,[5] International Organization for Standardization (ISO) 27000,[6] NIST 800-171,[7] and CIS-20.[8] These standards can provide helpful guidance that can be customized and supplemented depending on the type of data being shared and any unique requirements of the party sharing the data. It is essential to have top-level support from senior leaders who understand the importance of cybersecurity, appropriately resource and promote a coherent program, and consider cybersecurity risk factors when weighing other business decisions. The program should include regular audits and vulnerability assessments, as well as periodic cybersecurity awareness training for all employees.

The foregoing should be considerations anytime an organization assesses the risks of sharing sensitive company or customer data outside an organization. Regulatory requirements for dealing with vendors and third parties also should be considered. A company's clients may have baseline and other security requirements for company vendors that must be considered. Vendor contracts also will require negotiation or reporting requirements and liability for risks of breach, misuse, or sale. These considerations should be weighed whenever sensitive data is being shared with anyone outside, and not limited to relationships with conventional data vendors and processors. Indeed, they are inherent in most corporate relationships, including with outside consultants, accountants, and law firms – virtually anyone receiving sensitive or private company data.

III. Managing Third-Party Cyber Risk

Considering the potential harm that a third-party breach or other misuse of shared data can cause, organizations should devote serious time and effort to address these threats before they arise. In addition, companies may be obligated, under certain regulations, to verify the security and privacy capabilities of such third parties. The General Data Protection Regulation (GDPR), governing data protection in the European Union, has codified this obligation, and many regulatory regimes around the world have or likely will follow suit. Increasingly, the privacy assessments required by the GDPR are being coordinated or reviewed by outside counsel.

[5] https://www.nist.gov/cyberframework

[6] https://www.iso.org/isoiec-27001-information-security.html

[7] https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

[8] https://www.cisecurity.org/controls/cis-controls-list/

Organizations should create a vendor inventory to identify precisely which outside entities have access to what information. The inventory should include a data classification exercise, which involves categorizing data shared with third parties according to importance and sensitivity and determining the level of security required for vendors in possession of data in each category. This is often more difficult than it might seem, as there can be many non-obvious, smaller vendors involved in the ecosystem. In addition, vendors themselves may be sharing their customers' data with their own subcontractors, increasing the risk of unauthorized disclosure even further. Companies should consider whether each vendor actually needs all of the access that has been granted, and endeavor to limit access going forward only to the data the vendor requires in order to provide its service. Further, the company should evaluate the sufficiency of each vendor's cybersecurity program. For existing vendors, companies should review and reassess security and privacy practices at least annually.

When selecting third-party vendors, companies should perform a Third-Party Security Assessment, confirming that any vendor that would have access to company data has adequate controls to prevent the accidental leaking of sensitive data and to protect against deliberate attacks, including phishing campaigns and malware. Such assessments are often performed by a consultant and should include an analysis of potential vulnerabilities. The prospective vendor may also be required to complete a cybersecurity questionnaire. In performing this diligence, companies should consistently apply well-defined criteria to determine the security risks, considering factors like encryption, staff anti-phishing and malware training, contingency and incident response planning, access and authentication, and overall system security. Legal obligations for data security and privacy under various regulations must also be considered, including those under GDPR, the New York State Department of Financial Services, the Health Insurance Portability & Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA). Outside counsel can be enlisted to evaluate vendor compliance with all applicable regulations and to review vendor compliance and security assessments. Finally, vendor cybersecurity diligence should go beyond these technical considerations to assess the vendor's commitment to and appreciation for the importance of cybersecurity. While vendors may resist intrusive client security requirements or liability protections, most know of the increasing customer security expectations and understand that those expectations are not likely to decline in the future.

Once a potential vendor has been properly vetted, a company can take important measures at the outset of the relationship to manage third-party risk, namely through the inclusion of certain contractual provisions. Contracts with vendors should establish data protection requirements and agreed-upon standards for assessing the third party's cybersecurity efforts and provide for notice of breaches and other reporting periods consistent with existing contractual and regulatory requirements. Contracts should incorporate data access and security protections and should include mandatory audits to ensure compliance with adequate security standards. Audit attestation requirements also can help improve a company's insight into a vendor's potential vulnerabilities.

During the relationship, a company should share only the data necessary for the third party to provide the service for which it was retained. In addition, it should conduct periodic audits to confirm compliance with the agreed-upon contractual terms. It is also vital to maintain open, ongoing communication with vendors. Companies using vendors must resist the "set it and forget it" mindset. Regular discussions regarding potential vulnerabilities and opportunities for improvement can be an important tool in third-party risk management.

IV. Limiting Liability for Third-Party Breaches

As discussed above, using a vendor does not relieve a company of its cybersecurity obligations and the liability that results from a breach. Third-party breaches are as damaging as direct breaches. Unfortunately, just as with direct breaches, third-party breaches can still occur even when the most sophisticated and robust cybersecurity technologies, policies, and procedures are in place. Therefore, companies must plan for a breach and take steps to mitigate their losses.

Organizations can also limit the liability stemming from third-party breaches through contractual agreements. For example, third-party service provider contracts should require prompt notification if a security breach occurs, and the vendor should be contractually required to maintain an adequate cybersecurity response plan. Notification periods should be consistent across all contracts, and failure to timely notify of a breach should constitute a material breach under the contract, allowing the company to cut ties with a vendor that fails to provide this crucial notification. Furthermore, companies should ideally have broad indemnification language in third-party vendor agreements, holding the vendor responsible for costs and liability arising out of or in connection with a vendor data breach. Finally, companies should consider purchasing insurance that covers loss due to third-party cybersecurity breaches.

V. Using Data Processors

Use of third-party data and payment processors can significantly streamline operations and help an organization focus on its core missions. In the case of credit and payment card processing, it also can eliminate the risks presented by receiving customer card numbers that can be stolen by hackers. Nevertheless, organizations must be aware of the risks associated with the use of these data processors, which represent another category of third-party vendor that exposes a company to significant cybersecurity risk.

Companies can consider a variety of factors in selecting and using data processors, including cloud storage providers, to mitigate the risk of compromising sensitive data and suffering losses. Data processors differ from other vendors because they do not control or otherwise use company information in connection with providing a service. Rather, the service is limited to the storage and processing of data. The customer, referred to as the "data controller," decides the purpose of and manner to be followed in processing the data. And companies acting as controllers should insist that data processors comply with specified contractual requirements and standards in doing so. For example, data processors should be contractually bound to act only upon the data controller's instructions and to perform specific security measures. Data controllers also should require all individuals processing data to be subject to a duty of confidence, and that sub-processors are used only pursuant to predetermined controls. The controller should also contract with data processors regarding appropriate protocols tailored to satisfy applicable information security rules and regulations. In addition, the contract with the data processor should cover the deletion and return of company data, as well as obligate the data processor to submit to specified audits and inspections.

VI. Conclusion

Providing data to outside service providers, for whatever reason, brings with it serious risk. Regardless of the state of the data provider's internal security program, it should also include an external component, including routine audits, assessments, and training. Third-party vendors should be selected with care and their controls and internal practices investigated prior to signing them on. Contracts with third-party vendors should include pre-agreed data protection requirements and standards. Provisions addressing response to breaches and indemnification for related losses should be included in these contracts where feasible. Companies that retain data processors should also take into account the processor's limited role when utilizing them.

* * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to call or email David R. Owen at 212.701.3955 or dowen@cahill.com; Kenneth Ritz at 212.701.3661 or kritz@cahill.com; or email publications@cahill.com.