The Blackbaud Breach – Focus on Vendors

The Blackbaud Breach

In July of this year, Blackbaud, a U.S. based cloud computing provider and one of the world’s largest providers of administration, fundraising, and financial management software, notified its clients that it had discovered and stopped a ransomware attack. In a public statement, Blackbaud described the attack:

In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. Because protecting our customers’ data is our top priority, we paid the cybercriminal’s demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. The subset of customers who were part of this incident have been notified and supplied with additional information and resources.

Since its July announcement, nonprofit organizations throughout the world have issued their own notices of breach to their stakeholders, relying in large part on Blackbaud’s description of the breach.

Key Takeaways from the Breach

While data breaches are an almost daily occurrence, the Blackbaud breach is notable for a couple of reasons. First, even though it was able to prevent the ransomware attack, the cybercriminal exfiltrated unencrypted data from Blackbaud’s servers, in reaction to which Blackbaud elected to pay a ransom for the criminal’s agreement to destroy the data – given the reliability of criminals, a somewhat dubious promise. The response indicates that Blackbaud was threatened with a new, but increasingly common, tactic in ransomware attacks – the cybercriminal will couple a ransomware attack with theft of data, and threaten to make the data public unless it receives payment. As more and more companies are able to reconstruct compromised systems through backups and other means, cybercriminals have found a new way to monetize their attacks.

More importantly, the fact that this breach created a waterfall of breach disclosures reflects the impact of vendors on today’s data environment. Blackbaud provides comprehensive data, financial management, fundraising, payment, and other services to schools, museums, faith communities, foundations, healthcare organizations and nonprofit organizations, and those entities rely on Blackbaud for critical functions that are essential to their missions.

The Role of Vendors
Firms increasingly rely on vendors for data management functions. The 2018 Ponemon Institute survey of data breaches reported that at least 56% percent of organizations participating in the survey experienced a data breach due to a vendor’s security shortcomings. At the same time, companies are increasingly reliant on vendors—a recent Bomgar survey reported that, on average, companies allow 89 vendors to access their networks weekly, and that 71% of respondents expect to become more reliant on third parties in the coming years.

The Problem is Getting Larger

The increase in reliance on vendors comes against a backdrop where vendors account for some of the largest breaches, including highly publicized breaches, such as Equifax (147 million consumers), Target (110 million affected parties), Home Depot (109 million consumers) and Marriott International (500 million guest records).

Bomgar’s 2018 survey reflected a growing problem in the selection and oversight of third-party vendors: 74% of the respondents reported that third-party vendor selection overlooks potential key risks, and 64% said that their organization focuses more on cost than security when outsourcing. The lack of oversight, combined with increased reliance, leads to growing security threats to both businesses and employees.

What Should Companies Do?

Companies can and should take affirmative steps to ensure that a vendor will protect, rather than expose, sensitive information. Key steps include:

- **Due Diligence:** Before hiring a vendor or service provider, identify potential implications for data operations. This usually entails review by outside counsel, as well as communication between data security personnel and business or operations groups.
  - Determine what types of services the vendor will perform and the necessary access to data systems. A company can lower risks by minimizing vendor exposure to any highly sensitive data or systems. If a third party will access a crucial database, review and weigh the risks with stakeholders, including executive leadership.
  - Review the vendor’s policies, procedures, internal controls, and training materials to determine whether it has robust privacy and security infrastructure, and can adapt to evolving data security obligations.
  - Confirm that the vendor complies with relevant privacy-related laws, regulations, and industry standards. This is particularly important for companies that are subject to the new generation of data privacy laws, like the California Consumer Privacy Act.

- **Vendor Assessment Questionnaires:** Companies should create assessment questionnaires to assist in due diligence evaluations. The assessment should address key issues:
  - How will the services be provided?
  - What IT systems, data, and network design does the vendor use?
  - What are the vendor’s current information security procedures?
  - Will the vendor subcontract any services? If so, what are the subcontractor’s security procedures?
  - How often, and to what extent, does the vendor perform risk assessments? Do they use automated tools for some aspects of risk assessments? Which tools and how they use them?
  - What is the vendor’s incident response plan? If it has suffered data breaches in the past, how effectively and how quickly did it respond?
Has the vendor been subject to regulatory enforcement actions related to data privacy?
Has the vendor engaged in any litigation related to data privacy issues?

The answers to these questions will guide a firm in determining whether the decision to engage a vendor for sensitive functions is warranted and reasonable.

**Vendor Contracts:** Vendors seek to minimize their risks by limiting their privacy and data security commitments and transferring data privacy liability to the company. While vendors may have leverage in negotiations, key contract provisions should be addressed:

- Require the vendor to comply with all applicable regulations and standards. For example, a company that is subject to the California Consumer Privacy Act must ensure that a vendor can comply with the disclosure, deletion and other provisions of that Act.
- Establish a minimum standard of care for privacy and data security that meets the company’s risk tolerance – this may be stricter than current applicable laws and standards.
- Require the vendor to dispose of or at least properly secure all its copies of organization-related data upon termination of the agreement.
- Require the vendor to mandate the same privacy and data security obligations for its subcontractors or other service providers and work to ensure their compliance.
- Set meaningful timeframes for identifying and addressing vulnerabilities and risks, and for reporting security incidents.

**Oversight.** Companies must monitor a vendor’s risk potential on an ongoing basis. Conducting routine vendor oversight can help organizations demonstrate that they acted reasonably, particularly if a data breach or another type of security incident results in regulatory action or litigation.

Reliance on vendors is necessary part of business; however, companies must take concrete steps to limit the potential liability that comes with assigning key functions to third parties.

**Robert E. Braun** is the co-chair of the Cybersecurity and Privacy Law Group at Jeffer Mangels Butler & Mitchell LLP. Bob helps clients to develop and implement privacy and information security policies, negotiate agreements for technologies and data management services, and comply with legal and regulatory requirements. He helps clients to develop and implement data breach response plans, and he and his team respond quickly to clients’ needs when a data breach occurs. Contact Bob at RBraun@jmbm.com or +1 310.785.5331.

**JMBM’s Cybersecurity and Privacy Group** counsels clients in a wide variety of industries, including accounting firms, law firms, business management firms and family offices, in matters ranging from development of cybersecurity strategies, creation of data security and privacy policies, responding to data breaches and regulatory inquiries and investigations, and crisis management. The Cybersecurity and Privacy Group uses a focused intake methodology that permits clients to get a reliable sense of their cybersecurity readiness and to determine optimal, client-specific approaches to cybersecurity.