CYBERSECURITY

Are You Mitigating Cyber Risks Related to Your Suppliers, Vendors and Partners?

By Jake Omann, CIC, CPCU
Management Liability Segment Leader

www.usi.com

THE USI ONE ADVANTAGE®

According to the *2018 Third-Party Data Risk Study* produced by risk management software developer, Opus, with cybersecurity think-tank, Ponemon Institute, 61% of organizations in the U.S. confirmed that they had experienced a data breach caused by one of their third-party vendors, up from 56% in 2017 and 49% in 2016. Forty-two percent of organizations reported a breach through a third party in just the last 12 months, with another 22% unsure if they'd experienced such a breach.

Digital consulting firm, Booz Allen Hamilton, lists third-party risk as a top concern in Top Financial Services Cyber Security Trends recognizing that there is a "huge mesh of intertwined capabilities." As businesses become more interconnected, the risk of a third-party data breach at your organization becomes more imminent. It's no longer enough to simply secure your organization's network systems and data. Your risk management program needs to look beyond the perimeter of your organization to properly vet the third-party vendors who have access to your networks and data. Fortunately, your organization can take certain steps to minimize exposure, reduce the likelihood of a third-party breach and mitigate potential damages.

1. Review vendor contracts

Contract clauses addressing data privacy and security can be the subject of intense negotiation, with each party seeking to minimize its risk of exposure. Service agreements should be customized to reflect the sensitivity of the data involved and your organization's need for security, as well as the size, nature and resources of each party. It is critical to consider the following:

- **Safeguards.** The service contract should require the vendor to implement specific, reasonable administrative, technical and physical safeguards and regularly test and monitor their effectiveness. What constitutes "reasonable" will vary, depending on the size of the business and the nature of the data at risk. Massachusetts and California, for example, require vendors to agree to implement security safeguards when entering into service provider agreements. Such contractual provisions may also reduce the risk of exposure to an enforcement action under Section 5 of the Federal Trade Commission (FTC) Act (as it relates to "unfair acts") or similar state laws.
- **Breach notification.** Ideally, the vendor should notify its clients of any potential or suspected breach, not just after it is certain that data has been compromised. Your organization will also want to retain control over how your employees are informed. If the vendor simultaneously notifies employees and management of a possible breach, the organization will miss out on crucial opportunities to prepare employee communications and ascertain the company's own responsibilities under applicable laws.
- **Remediation.** It is also important to expressly provide that the vendor will reimburse the business for costs incurred in notifying affected individuals and mitigating damages, particularly when highly sensitive data is involved. These costs may not be covered under standard indemnification provisions within the contract.
- **Insurance.** Many commercial general liability policies exclude coverage for electronic data. Find out the extent to which the vendor maintains current cyber liability insurance policy coverage to protect the vendor (and clients via indemnification) against substantial monetary losses arising from both first-party and third-party cyber liability risks. Also, consider whether it is appropriate to contractually require vendors to maintain technology errors and omissions or cyber liability insurance, depending on the type of services they are providing and the risks they pose to your data and network.
- **Oversight.** Push for the right to conduct or oversee an audit of the provider's facilities and practices, particularly if highly sensitive data is involved. At a minimum, reserve the right to require the vendor to provide information addressing its security practices at specified intervals throughout the term of the agreement. High-risk vendors should be evaluated more frequently. Larger vendors tend to be more restrictive on the information they are willing to provide, but it is still prudent to request documentation of the security protocols and safeguards they have in place.

2. Conduct vendor due diligence

As more businesses migrate to cloud-based technology, proper vendor management and due diligence is becoming an even more important element of every organization's cybersecurity compliance program. In order to properly vet a service provider, it's critical to identify which services are being provided by the vendor, such as:

- Internet service provider (ISP) or other data network services
- Commercial co-location/cloud hosting (physical, network, and/or system-level only)
- Original application development
- Payment processing services
- Outsourced retail sales/fulfillment/service
- Outsourced commercial business operations processing
- Outsourced healthcare, back-office, or insurance-related services
- Managed security services
- Payroll services
- Business/marketing consultancy services
- IT/technical consultancy services
- Independent audit/compliance services

Also, consider from what locations the services are being provided on your organization's behalf—will they be onsite or offsite at the vendor's location or a third-party location?

Find out if the vendor anticipates sub-contracting some or all of the provided services. If they do, identify by company name and location all sub-contracted vendors who will participate in any aspect of the provided services.

3. Classify your data

In order to understand what's at risk, you must understand what kind of data you have. Start by taking an inventory of your data, then categorizing the data by sensitivity level to help determine how to protect it appropriately. Loss of sensitive data can happen when organizations fail to properly identify or classify data, or when they do not identify all the ways in which data could be manipulated or exposed.

Data and indemnification

An indemnification provision is an example of contractual risk transfer. One party agrees to reimburse or "indemnify" the other party under certain circumstances. Some indemnification provisions also include a duty to defend, which means you agree to pay for the loss and for the other party to defend against the claim (and sometimes even pay the other party to sue you). Indemnification often requires you to "hold harmless" the other party, which acts like a release of responsibility when something goes wrong.

Businesses should identify the sensitivity of the information being entrusted into a vendor's care as a required element of the services being offered when the third party is receiving, handling, processing, storing, and/or transmitting the following:

- Personally identifiable information (PII) associated with your organization's clients, employees, or other involved parties. PII includes, but is not limited to, names, addresses, Social Security Numbers, driver's license information, purchase histories, etc.
- Payment cardholder information (PCI) associated with your organization's clients, including card numbers, expiration dates, magnetic stripe data, etc.
- Other types of financial account/payment information associated with your organization's clients, employees, or other involved parties. This can include bank/brokerage account numbers, automated clearing codes (ACH), balances, debts, etc.
- Private health information (PHI) associated with your organization's clients, employees, or other involved parties. PHI can include paper and electronic health records, treatment data, etc. Additional HIPAA rules will apply.

- Competitive business information associated with your organization's profit-seeking activities, intellectual property, legal/compliance, or other types of data elements subject to client-assigned confidentiality requirements.

When sensitive client data of any of these types are entrusted into a vendor's care, identify the means by which such data is segregated from that of other clients while in system storage (e.g., physical segregation, logical segregation via VLANs/firewalls, separate DB instances, etc.).

As always, accountability is essential. Identify by name and role the vendor's senior manager responsible for developing, implementing, and enforcing information security requirements, as well as the nature and extent of the vendor's overall incident response plan. Include the employee teams who are involved in the incident reporting, escalation, and remediation tasks associated with resolving suspected or confirmed information security incidents.

For more information about mitigating cyber risk at your organization, please contact us at 800-258-3190 or MNWI.Info@usi.com.