Surviving the service provider data breach

Cybersecurity Law Alert

29 July 2019
By: Edward J. McAndrew

It's summer, and life's a breach. A data breach, that is. It's your service provider's breach, but it involves your (more likely, your customer's) data. So put down the beach reading, for some breach reading.

Service provider cyber incidents have exploded in volume, type, frequency, response time and cost. That makes sense, because the surface attack area for most organizations now expands beyond their networks and devices to those controlled by third parties. From the bad guy's perspective, why hack one organization directly when you can hit a service provider with potentially weaker defenses and the sensitive data of many organizations?

Effective cybersecurity requires organizations to move beyond perimeter defense of their own network to protecting sensitive data in the hands of service providers. If security alone isn't a sufficient motivator, a flood of new cybersecurity laws and regulations now require businesses to bear responsibility for the cybersecurity issues of their service providers. From a security and legal perspective, service provider cybersecurity requires significant attention and coordination by all parties both before and after hitting the breach.

Who "owns" a data breach?

Let's begin with legal responsibility for data breaches involving personal information. Each state's data breach notification law generally applies to all organizations that conduct business in that state and that own, license, maintain, collect, compile, store or manage "personal information" of state residents. A supermajority of states generally define a "breach"
as unauthorized acquisition of electronic data that compromises the security, confidentiality or integrity of "personal information" – the legal definition of which varies by state, but continues to grow broader to include governmental identifiers; financial, health, biometric information, and even login credentials to online accounts. All of this means that more data is legally protected – and the "who, what, when, where and how" of a "breach" may reside on someone else's system.

Even though it may be a service provider's system that is "breached," state data breach notification laws (and a number of federal laws) generally require the "owner" or "licensor" of the breached personal information, or the "covered entity," to notify affected individuals and regulators of the breach. A quick review of sample data breach notices published by at least nine states confirms that many reported breaches were of a service provider's system – not that of the covered entity legally required to report the breach.

Under most state and federal laws, the service provider is merely required to notify the covered entity of the incident, and perhaps to cooperate in investigating the incident and notifying relevant parties. This puts the covered entity on the legal hook for incidents that are often beyond its capability to prevent, detect, investigate and remediate. It also makes it very hard for the covered entity to mitigate any harm to affected parties.

Beyond data breach notification laws relating to personal information, the covered entity and service provider's rights and obligations relating to cyber incidents are often defined by contract. Some key terms include: (1) requirements, representations and warranties relating to the implementation of "reasonable" security controls; (2) data governance and security audit and assessment rights/responsibilities; (3) definitions of protected information and of a "breach" or "incident" that triggers contractual rights and duties; (4) notification, investigation and cooperation obligations upon discovery of a "breach" or "incident"; and (5) indemnification and limitation of liability provisions.

Do "reasonable" cybersecurity controls extend to third parties?

Third-party service provider management is one of the hottest areas of cybersecurity law development. For example, federal laws ranging from the GLBA to HIPAA to the FTC Act either expressly require (or have been interpreted to require) that covered entities impose cybersecurity requirements on their service providers, ranging from particular types of administrative, technical and physical safeguards, risk assessments and audit trails, to incident notification, investigation and remediation requirements.

Roughly half of the states now legally require businesses to implement "reasonable procedures and practices" to prevent and respond to cyber incidents. Most do not define "reasonableness," instead effectively regulating by enforcement action and agency guidance. Some states – such as Alabama, Massachusetts and New York (for financial services companies) – prescribe particular requirements of a "reasonable" cybersecurity program. At least nine states expressly extend these requirements to service providers. While some of these states require the covered entity to supervise and contractually require cybersecurity measures of the service provider, others (such as Alabama) statutorily require the service provider itself to maintain reasonable cybersecurity safeguards.

What's the fallout from a service provider breach?

Service provider cyber incidents are legally perilous for both the service provider and the organization that entrusts it with sensitive data. Covered entities generally cannot contract away all responsibility for cybersecurity or cyber incident response. Once an incident is disclosed, both the covered entity and the service provider may become the focus of regulatory investigation, law enforcement inquiry and allegedly aggrieved civil litigants.

Just last month, the FTC settled a data security enforcement action against a SaaS provider that suffered a breach exposing the personal information of about 12.5 million consumers, which the provider was storing for 130 auto dealers. The same company also settled an enforcement action brought by the New Jersey Attorney General's Office as a result of the breach. This spring, HHS OCR published a fact sheet on direct liability of business associates under HIPAA for violations of the security and breach notification rules.

It is often the covered entity that ends up embroiled in regulatory enforcement actions due to service provider data breaches. Last year, for example, a physician group settled a HIPAA enforcement action based on a website service provider's exposure of patient billing data. Various regulators have brought actions against financial services companies for service provider breaches. The FTC has proposed significant revisions to the Safeguards Rule that will implicate cybersecurity oversight of service providers.

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome. Copyright © 2021 DLA Piper, All rights reserved.
Covered entities and their service providers are ending up as co-defendants in data breach class action litigation brought by consumers, employees and others. Covered entities are also suing service providers that cause them cybersecurity related injury or financial loss. Typical claims in cybersecurity-related litigation include negligence, breach of express or implied contract, unfair or deceptive trade practices, and violations of state data security and data breach notification laws.

As of January 1, 2020, we can add the private data breach cause of action under the California Consumer Privacy Act to the mix. The CCPA claim will likely focus on whether a covered "business" violated "the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information [at issue]." Plaintiff's lawyers will undoubtedly argue that various laws, regulatory guidance and industry standards include cybersecurity management of service providers as a fundamental component of "reasonable security procedures and practices."

In both defensive and affirmative litigation relating to data breaches, the interests and strategies of covered entities and service providers may quickly diverge (if they are not diametrically opposed from the outset). This actual or potential divergence is severely complicating the response and investigation processes related to service provider cyber incidents. Instead of focusing on working together to respond to and recover from the incident, all parties are increasingly assuming pre-litigation postures in an effort to minimize their own exposure. "Every man for himself" may be a reasonable litigation strategy, but it is not often the most effective response to service provider cyber incidents.

How to best protect against service provider incidents?

Take reasonable proactive steps to avoid them wherever possible. But cyber incidents happen. Liability results, though, only if the organization acted unreasonably either before or after the incident occurred. Acting proactively to manage risk and being prepared for those incidents that cannot be avoided is therefore crucial to limiting assorted injuries and liability.

Proactive steps

- Establish policies and practices for managing cybersecurity risk posed by service providers that have access to your systems or legally protected information. Create a matrix of all relevant providers, agreements and provisions for incident response use.
- Catalog all legal obligations and potential liabilities under statute, regulation, contract and common law in the event of a cyber incident involving legally protected information held or accessible by service providers.
- Include cybersecurity-related provisions in contracts that hold service providers to any legal standard that you must meet, while shifting liability risk appropriately. Some examples:
  - Appropriate administrative, technical and physical safeguards, such as identity and access controls; data, device, systems and personnel inventories and mapping; encryption of sensitive data in transit and at rest; patching and updating of software and hardware; physical access restrictions; multi-factor authentication for remote access; limited user privileges; frequent data backups; and periodic cybersecurity training.
  - Audit and assessment provisions that allow you to evaluate the effectiveness of the service provider's cybersecurity program.
  - Proof of adequate cyber insurance coverage.
  - Requirement of quick notification upon discovery of an actual or suspected incident impacting your data or systems, along with investigative cooperation requirements.
  - Robust indemnification clauses.
- Develop an incident response plan that integrates the service provider’s incident response team and process for foreseeable service provider incidents (e.g., ransomware/extortion/loss of service; malicious data breach of legally protected information; non-malicious data exposure/leakage; account takeover/financial fraud).

Key service provider incident response steps

- Activate integrated incident response teams as appropriate for the incident.
- Execute key containment, remediation and investigative steps based on the incident and known facts.
- Ensure that relevant evidence is collected and preserved across both controller and service provider environments.
- Develop and follow integrated response team communications plans.
- Coordinate all external communications and legally required notifications.
- To the extent feasible, coordinate on pre-litigation planning and litigation strategy (particularly for motions to dismiss, ...
class certification and discovery issues).

An earlier version of this article appeared in *The Legal Intelligencer's* Cybersecurity Supplement in July 2019.

**AUTHORS**

Edward J. McAndrew  
Partner  
Wilmington | T: +1 302 468 5700  
Washington, DC | T: +1 202 799 4000  
ed.mcandrew@dlapiper.com