Bloomberg Law Reports® Privacy & Information

The Intersection of 21st Century Risk Management and Data: Risk Allocation and Mitigation for Customer Data Breaches

Ethan D. Lenz, CPCU, and Christopher C. Cain, Foley & Lardner LLP

Data. It has always been important for companies, particularly data about their customers. What constitutes customer data has expanded from names, addresses, and account numbers to include tracking the specific products and services each customer bought, shopping preferences, dates of purchases, customer service questions, and so on. Customer data can be very valuable, as companies can "mine" the data with software programs in countless ways; for example, to discern patterns in customer behavior or to more accurately *see* which products are selling better than others and why. Companies can keep more and more customer data, thanks to the continual decline in the costs of storing data digitally. And so the digital data pile has grown—a recent IDC whitepaper estimates that by 2011, there will be 1.8 exabytes of electronic data in existence (each exabyte equals 1 billion gigabytes).[1]

With great amounts of data comes great risk. Specifically, the risk of data security breaches involving customer data, including data known as "personally identifiable information" or "PII" (for example, names, addresses, e-mail addresses, phone numbers, birthdates, and social security numbers). Compromising PII through a security breach damages a company's business reputation and is expensive. A 2009 Ponemon Institute study examined over 40 companies and the costs each organization incurred because of a data security breach and found that, on average, a single data breach cost the affected company $6.75 million in terms of data restoration, lost business, legal fees, customer notifications, and fines/penalties.[2] Moreover, companies cannot escape liability for a data breach by outsourcing data storage to a third party. Data privacy laws hold a company ultimately accountable for a security breach related to its data, regardless of where the data is stored and regardless of who was "guarding" the data.

Too many companies focus only on the benefits of collecting more and more customer data and do not truly focus on basic risk management associated with protecting that data. The primary risk management principle is to deliberately consider risk allocation: to what extent a company retains some or all of its data security risks and to what extent it can transfer some or all of those risks to third parties, such as a service provider (via a services agreement) and/or an insurance company (via an insurance policy). Not surprisingly, most companies would rather shift at least some of the risk to a third party. The trick is to do it properly—many companies have both services agreements and insurance policies related to data security, but they don't provide the risk shifting and protection they could have or should have. Below we examine how to properly shift data sharing risk through provider agreements and insurance policies.

Maximize Contractual Risk Allocation with Third-Party Providers

If a company uses a third-party provider to store and/or manage customer data, take care to ensure the provider's written agreement addresses the following provisions to shift at least some of the data security risk to the provider. First, make your provider legally stand behind the data security standards it boasts about on its marketing brochures and website. Do not just accept the provider's standard language as it is too one-sided in favor of the provider. Insist that the agreement contain specific representations regarding the provider's baseline security measures, security incident management, and hardware, software, and security policies. Make sure you are comfortable with those specifics and ask for changes to them if you are not—many companies with their own in-house data security standards will demand the provider at least meet those. Detailed representations regarding the provider's data security and confidentiality standards serve two key purposes—they give you assurance the provider has good security measures in place, which should minimize the chance of a breach, and if the provider breaches its security representations, then at least you will have a claim for resulting damages. The agreement should also require that the provider's data center be located in, and the services be performed in, the United States, and that no data be made available to those located outside the United States. Otherwise, your data may end up in a remote country and the country may have very lax security and privacy laws. The provider should also allow a client to verify the provider's security capabilities via a physical visit or SAS 70 audit (IT internal controls audit) conducted by a third party, or both.

Second, ask for a strong provider-indemnity provision with appropriate loss limitations. Indemnity is inter-party insurance—parties to an agreement decide that if certain events occur then one party will protect the other party against those events and cover the related damages and costs. In the data security context, the provider should agree to defend, indemnify, and hold harmless the client from any claim where the provider was negligent or breached its data security obligations. Any intentional breach should be fully indemnified, meaning the client has no out-of-pocket costs related to data recovery, damages, legal fees, and otherwise complying with applicable data privacy laws. If a data breach was not because of a provider's intentional act, then the provider may require a cap on its potential liability exposure, which may be reasonable depending on the type of client data in question. Such a cap is typically expressed as a multiple of the total amount paid to the provider (i.e., three times the amount paid to provider). A provider's limitation of liability should not, however, apply to claims for which provider is insured or to third-party indemnity claims.

Lastly, make sure the provider has technology errors & omissions insurance in place to back up its representations and indemnities. As discussed in greater detail below, the provider's commercial general liability insurance is unlikely to provide protection for the provider's liability arising from its data-related services. Therefore, you will want to require the provider to carry appropriate coverage for this risk. While the amount of the coverage a provider should carry will vary depending on the size of the agreement and the services provided, typically limits for the coverage should be no less than $1 million per claim. Furthermore, because this coverage is almost

always "claims-made" (i.e., it only applies to claims made while the policy is in force), the agreement should require the provider to maintain the insurance for some period of time after the agreement terminates (usually, no less than 1 year, and preferably 3-6 years).

Have the Appropriate Insurance Policies in Place

Don't assume your current insurance will cover you for data security breaches, and consider getting a cyber-liability policy customized to your business. A common misconception exists that a company is covered for much or all of the liability associated with a consumer data security breach if the company has a standard form commercial general liability insurance policy (a "CGL Policy"). The typical CGL Policy however, may provide little or no protection for a data breach. Why? A CGL Policy may, and often does, contain specific "exclusions" that will preclude coverage for a data breach claim; for example the CGL Policy likely will: (1) exclude electronic data from the definition of covered property damage; (2) exclude coverage for intangible property damage (data is considered intangible property); (3) exclude personal injury coverage for internet-based businesses; and (4) specifically exclude coverage for liability associated with data security breaches if the insurer views the company's business as having potentially significant liability for loss of customer data as a result of a security breach (these types of additional exclusions will almost always be found in CGL policies issued to providers who are in the business of storing or collecting customer data on behalf of businesses).

Because of the likely gaps in coverage under traditional CGL Policies, insureds with significant technology-based liability exposures should usually consider the purchase of some type of "cyber-liability" or "technology errors and omissions" insurance protection as part of their liability risk management program. At the very least, the cost of such coverage should be determined so that the business can make an informed decision regarding whether the cost of the coverage exceeds its potential benefit in the event the business becomes the subject of a liability suit related to a security breach or similar issue.

While there is no standardization yet among cyber-liability policies, most are written with a "menu" type format, where the insured can pick and choose the coverages that it wishes to purchase, in order to customize the protection to the particular risks faced by its business. Some of the more typical coverage choices that will potentially provide coverage for liability arising from security breaches include:

> *Cyber Professional Liability/Tech E&O*: As noted above, this type of insurance covers liability arising out of the company's performance of professional services. Typically, the scope of the covered professional services is specifically defined in the policy, and must be tailored to cover as completely as possible those services offered by the company (e.g., web hosting, data security, Internet publishing, etc.). This coverage is particularly valuable to providers that are responsible for storing, or otherwise handling, large volumes of third-party customer data. It can, for example cover

liability arising from inadequate security, and resulting loss of use, or misuse of customer data if the provider's storage system is breached and customer data is stolen or destroyed. Furthermore, companies that utilize outside providers for storage or analysis of customer data should almost always require that the provider carry this insurance as part of the provider's agreement.

Network Security Liability: The scope of this type of insurance, which covers liability arising from the unauthorized use or access/breach of an insured's network, can vary significantly from insurer to insurer, and should be carefully evaluated. However, the typical coverage will provide protection against both liability arising from the transmission of computer viruses from the insured's network to an outside network, as well as liability arising from theft of customers' electronic data.

Identity Theft Liability: In some ways, this type of insurance is similar to, and may be included in, Network Security Liability coverage offered by certain insurers. However, identity theft liability coverage is typically limited to liability arising from the theft of electronically-stored personal information of customers (with some coverage forms also including coverage for liability arising from theft of employees' personal information).

Electronic Data Restoration: This type of insurance covers costs associated with restoring third-party electronic data and other information assets after a cyber attack.

While these various types of "cyber risk" insurance coverages certainly have the potential to provide valuable protection to businesses with exposure to cyber-based liability, they are not a perfect solution. The policies are still relatively new and therefore, they have not yet generated significant levels of coverage litigation, and there often are gaps in coverage that only come to light after a claim arises. These gaps in coverage should be minimized, to the extent possible, through careful negotiation of the coverage terms and conditions, so that the coverage is as customized as possible to a company's risk profile (e.g., by ensuring that the covered "professional services" under a technology E&O policy identify the full gamut of services of a provider, ensuring that a network security liability policy covers data at all locations where the company stores that data, etc.)

In addition, there are a number of differences between the typical cyber-liability insurance policy and the typical CGL Policy that can present traps for the unwary. For example, many CGL Policies will provide "first dollar" coverage (i.e., they have no deductible), and will pay for the costs of defending a suit against the insured in addition to the limits of the policy that only apply to any judgments against or settlements entered into by the insured. On the other hand, most cyber-liability policies require the insured pay a deductible before the coverage is triggered, and

are written such that the costs of defending a suit reduce the amount of insurance available to pay for any settlements or judgments.

Finally, as noted above, cyber-liability insurance policies are not standardized, and each insurer that currently writes them has their own version. This is in contrast to the typical CGL Policy, which is written on the same form by a large number of insurers. As a result of this policy divergence, businesses must carefully evaluate of the coverage language offered to them in light of their business needs.

Conclusion

Companies that spend more time on risk allocation and transfer related to their customer data security will realize better protection for that data. Using a third-party provider can be a great way to outsource management and security for that data, but make sure the agreement requires the provider to stand behind its claims so that you have adequate recourse in the event something goes awry. Lastly, examine your current insurance policies and see if they provide protection for data security breaches. If they don't, get appropriate policies in place, customized to your business to mitigate, if not completely offset, the potential costs if a data security breach occurs.

Christopher C. Cain is a partner with the law firm of Foley & Lardner LLP, practicing in the firm's Information Technology & Outsourcing practice. He routinely counsels clients on the legal, technical, and transactional issues arising in technology transactions. Ethan Lenz, CPCU, is a partner in the firm's Insurance Industry practice and has extensive experience providing risk management and insurance coverage-related advice to commercial clients, including in the context of IT agreements. They can be reached at ccain@foley.com and elenz@foley.com, respectively.

---

[1] IDC, *The Diverse and Exploding Digital Universe: An Updated Forecast of Worldwide Information Growth Through 2011* (Mar. 2008), available at http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf (last visited Feb. 26, 2010). *See also* Lucas Mearian, "Study: Digital universe and its impact bigger than we thought," *ComputerWorld* (Mar. 11, 2008), available at http://www.computerworld.com/s/article/9067639/Study_Digital_universe_and_its_impact_bigger_than_we_thought (last visited Feb. 26, 2010).

[2] Ponemon Institute, *Fourth Annual US Cost of Data Breach Study* (Jan. 2009), available at http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf (last visited Feb. 26, 2010).