Attention Title Companies

Beware and Avoid the Myths about Data Privacy & Security

Data breaches and compliance failures continue to threaten companies and put individuals' personal identities, payment card data, finances, and medical information in jeopardy. For companies that experience those breaches, reputational harm can have a significant impact on their business and brand reputation. This is true in most industries, in particular those that handle significant amounts of personal information, such as title insurance and settlement companies ("title companies").

For title companies, this is not only a matter of legal compliance, risk management and good business. The American Land Title Association (ALTA) has included adopting and maintaining reasonable safeguards to protect nonpublic personal information in accordance with applicable law as one of the seven "best practice pillars"[1] it expects of its members. Shelley Stewart of Southern Title in Florida commented that while these pillars are not mandated by ALTA, "compliance with them makes a difference to banks and other institutions looking to partner with title companies." There are safeguards required under federal law as well as state laws which can be more specific and expansive. However, perceptions about risk can inhibit appropriate action. Some of those perceptions derive from common myths about data security that all firms, including title companies, should avoid.

Myth #1: Our title company is too small to be a target.

The size of a company, whether measured by annual sales volume, number of employees, locations or certain other metrics, is not always the best measure of data risk. A small medical transcription company with 8-12 employees could easily maintain sensitive personal information on thousands of individuals. A neighborhood restaurant can process credit card data for hundreds of customers each week. Likewise, a title company can close hundreds or thousands of transactions a year, each of which containing substantial amounts of very sensitive personal information. This, coupled with the perception (reality) that a business does not have strong safeguards, may present an attractive target for an outsider, as well as from insiders within the organization intent on doing harm.

This point was made clear in a recent L.A. Times article, and should not be overlooked. Certain small businesses may be even more likely to be targets than larger organizations, even if their breaches do not make national headlines. These companies are viewed as having significant amounts of personal data, with less sophisticated safeguards in place and fewer resources to react to an attack.

> ***"But for every high-profile case, there are dozens of threats to confidential data held by everyday enterprises."***
>
> ***--L.A. Times***

Myth #2: We are located in State X, and laws in other states do not apply to us.

When it comes to certain data privacy and security requirements, state laws are

[1] ALTA Best Practices Framework: Title Insurance and Settlement Companies, published July 19, 2013. http://www.alta.org/bestpractices/index.cfm

important, and many have strong protections and enforcement. Even if that is not the case, consumer personal information also enjoys significant protection by the Federal Trade Commission (FTC). The FTC regularly enforces the requirements that businesses not engage in unfair and deceptive trade practices, which include those practices that relate to consumer personal information. This includes statements companies have on their websites, describing the steps they take to protect the personal information of the customers visiting their sites. These protections also include taking steps to identify "red flags" that may indicate the existence of identity theft.

However, businesses cannot look solely to federal law and the state laws in which they are located. They also may need to consider the laws of other states that apply their laws beyond their borders. For example, the Massachusetts data security regulations (201 CMR 17.00) set forth extensive privacy and security requirements that apply to companies that "own or license" personal information about Massachusetts residents. According to the regulations, the term "own or license" refers to circumstances where a company: ***receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment***. Thus, a business that maintains personal information concerning a Massachusetts resident arguably must comply with those data security regulations, even if the business does not have a location in the Bay state or does not do business in the state.

For this reason, like other businesses, title companies need to look closely at the kind of personal information they maintain, as well as the state(s) of residency of the individuals about whom the information relates, in order to have a more complete understanding of their obligations.

Myth #3: We do not own the data; the banks do and they have the reporting obligations.

It is true that many of the 47 state data breach notification laws generally provide that the obligation to notify affected individuals rests with the entities that own the personal information. It also may be true that the data is owned by banks and other entities involved in transactions that title companies service. The determination of which entity owns the personal information may not always be an easy one. But, either way, if a title company experiences a data breach pertaining to the personal information of its customers or employees, it will have notification obligations (even if only to the bank) and how it responds to those obligations could have significant impact on its business. Increasingly, service agreements establish contractual obligations on vendors, such as title companies, to take certain steps in the event of a data breach.

> ***Entities that maintain personal information and discover a breach of that information must notify the owner(s).***

Frequently, the investigation and response to a data security incident involving a service provider and the owner of the personal information requires coordination between those two entities. Determining what happened, who will provide the notice, what the notice will say, whether to provide credit monitoring, and so on, all can cause significant delays in the notification process, particularly when two or more entities are involved and where their interests may not be exactly aligned. It is critical that title companies be prepared for dealing with these situations ahead of time.

Myth #4: We have a privacy policy in our handbook and require strong passwords, so we are good.

Having a well-drafted handbook policy and a requirement for strong passwords is a good

start. But those two items by themselves are insufficient to satisfy just about any of the data security standards required under federal or state law. For example, a handbook policy likely would not have prevented the "phishing" attack in 2014 that caused a title company to have to notify its customers of a data incident.[2] In states such as California, Connecticut, Florida, Maryland, Massachusetts, and Oregon, a written information security program (WISP) in one form or another is required. Although the FTC has not articulated detailed and comprehensive data security standards, a comprehensive WISP covering customer and employee information will be a good step toward compliance.

A WISP can be a competitive advantage by providing comfort to existing and potential customers concerning the safeguarding of personal information.

For title companies that handle payment cards, some level of PCI compliance is required. Depending on the manner and volume of payment cards processed, the business can have significant PCI obligations. Note, however, that those obligations extend only to the payment card data, and most businesses stop their data security compliance there. However, those same businesses also have large amounts of other customer data – such as that contained in financial and closing documents, marketing information and other lists – that warrant similar protections. So, PCI compliance alone, like a handbook privacy policy, is not sufficient.

WISPs start not with policies, but assessments. That is, even before an organization puts pen to paper or finger to keyboard to create a policy or policies, it must assess a number of factors concerning the risk posed by the personal information it keeps. This includes learning more about the kinds of personal information the company maintains, who has access to it, how and where is it being stored, along with a number of other considerations. At that point, the company is in a better position to address the administrative, physical, technical and organizational risks to that information in the form of policy…a WISP.

Depending on the business, a WISP can be a competitive advantage by providing comfort to existing and potential business partners, concerning the safeguarding of personal information. A WISP also will better position a company when defending claims related to a data breach and a federal or state agency investigation, help the company manage and safeguard critical information, and may even avoid whistleblower claims from employees.

Myth #5: Our IT Department is on top of this.

No doubt, an organization's IT Department is critical to the process of safeguarding all of the organization's information assets. However, leaving that responsibility solely in the hands of the IT department can be problematic for a variety of reasons:

- The increasing complexity of IT systems often makes it very difficult for upper management to understand an organization's needs and whether its IT department is addressing those needs or has the expertise to do so.
- Putting data privacy and security in the silo of an IT department may stifle collaboration among other departments, making it difficult to identify risks as well as solutions.
- IT departments may not be in a position to keep up to date with legal developments or know the best way to apply them.
- Fearing discipline, IT departments may not be as quick to address data incidents or may be too aggressive in downplaying risk of harm.

[2] http://www.databreaches.net/fidelity-national-financial-notifies-title-insurance-customers-of-breach/

Data privacy and security is an enterprise-wide issue that requires the involvement of key stakeholders in the organization.

Myth #6: Our insurance covers these situations.

Like many other risks, information risk can be addressed in part through insurance. Increasingly, carriers are developing products designed to deal with personal information risk and specifically data breach response. Acquiring this kind of coverage certainly should be considered by any organization as part of its plan to address information risk.

But, don't assume your current policies will cover you in the case of a data breach. When a company claimed data breach coverage under its commercial general liability policy, a New York court disagreed. However, faced with similar claims under a comparable policy, a U.S. District Court for the Central District of California found coverage existed under the policy.

Do not assume your current policies cover data breaches.

Thus, companies have to be careful about understanding the coverage they have and the coverage they select; they should be working closely with their brokers and appropriate counsel.

Coverage known as "cyber" coverage is not necessarily going to cover costs incurred by the company to respond to a data breach, and has to be considered in coordination with other coverage. And, even if the policy addresses costs the company incurs to respond to the breach (notification, legal, media, credit monitoring, etc.), it may not cover exposure from litigation and regulatory investigations. For title companies considering such insurance, it will be important to confirm application of the coverage to all of the personal information they handle.

* * *

Cybersecurity is a significant challenge for all businesses and governments. There is no "silver bullet" to accomplishing it, nor will even the most comprehensive set of safeguards be 100% secure. On the other hand, ignoring the problem or succumbing to myths that cloud thinking on how to tackle the challenge should be avoided.

About the Author

Joe Lazzarotti is a partner with the Jackson Lewis law firm and head of its Privacy, eCommunications and Data Security Practice Group.