WARD AND SMITH, P.A.
ATTORNEYS AT LAW

# Is Your Customer Data Your Greatest Asset or Your Greatest Liability (or Both)?

October 4, 2016

Customer data can be a treasure trove for an organization. Many businesses believe customer and prospect data to be their most valuable asset. Unfortunately, some have discovered that, unless handled with care, it can also be their greatest liability.

Organizations of all kinds collect, store, analyze, use, and share consumer data for myriad reasons. Consumer data may help an organization maintain contact with a customer or prospective customer. Properly analyzed, it can often predict customer behavior, allowing an organization to tailor its communications and offerings. It can reveal patterns that help increase revenue, minimize expenses, and ultimately drive profitability. Data can be leveraged and monetized by sharing with affiliated and non-affiliated entities. Given the immense value of consumer data, it is no surprise that some of the most valuable companies in North Carolina and the world are data analytics firms.

Over the past few years, however, it has become widely acknowledged that such valuable data can also be a liability of the greatest magnitude. The costs of the largest data security breaches have made headlines. But these sensational headlines sometimes create the misleading impression that only large organizations incur massive costs, and that the losses are solely attributable to hackers.

**The Risks, by the Numbers**

One of the best sources of information about risks associated with consumer data isNetDiligence's annual study of "cyber insurance" policy claims. Although the information is limited to incidents for which the targets had insurance coverage, and is limited to covered losses, it is still an excellent source of data. The most recent study, covering claims data from 2012 to 2015, showed the average insurance claim amount was $673,767, with average legal fees of $434,354.

**Smaller Organizations Face Increasing Risks**

In the NetDiligence study, organizations were categorized by size (revenue), which provides some interesting insights. The smallest organizations represented the largest raw number of incidents, probably due to the fact that there are simply more small organizations than there are large ones. While the three smallest categories of organizations accounted for a combined 71% of the reported incidents in 2015, they were responsible for only 38% of records exposed. It was surprising, however, that, according to NetDiligence, some of the largest claims came from smaller organizations. This may be a result of the smaller organizations being less aware of their exposure or having fewer resources to provide data protection and security awareness training for employees.  By contrast, mid- and large-revenue organizations accounted for only 17% of incidents, but were responsible for 60% of the consumer records exposed.  This seems intuitive, because larger organizations would be expected to have more consumer records, on average, than smaller organizations.

**Risks Are Spread Across Industries**

The NetDiligence study also reveals a good deal about the source of recent risks.  While risks in prior years were concentrated in certain industries, they are becoming less concentrated year by year.  According to the study, recent losses were more evenly dispersed among business sectors, with healthcare reporting the most at 21% and financial services coming in second at 17%.  In other words, the categories of affected data resulting in the highest losses, from all industries, were health information and financial data, but the majority of losses were incurred outside of these two historically most targeted industries.

**Vendors: The Weak Link?**

Vendors are a common source of privacy and data security risk.  Vendors include service providers and others with access to an organization's data or systems.  In 2015, 25% of claims were attributable to vendors.  Of those claims, approximately half were hacking incidents, with the other half largely accidental or intentional disclosures.  Another interesting observation is that the vendor events exposed significantly more consumer records than events that occurred at the organization itself, indicating that failures by vendors may tend to be more systemic than failures at the level of the primary organization.

Healthcare providers and other HIPAA-covered entities, financial institutions, and defense contractors have long been required to extract certain contractual agreements requiring security protection from their vendors.  Following the breach of a Target vendor resulting in a massive theft of Target's customer data, organizations of all kinds began imposing contractual privacy, security and, importantly, indemnity terms on vendors, and these terms are sometimes heavily negotiated.

**Data Use Violations: A Bigger Risk Than Breach?**

Data-related liability in the context of nefarious hackers breaching security systems from foreign lands dominate the headlines, but much less dramatic circumstances lead to large numbers of significant incidents every year.  An analysis of what triggered the losses that gave rise to cyber liability claims in 2015 reveals that targeted security breaches are not the only source of loss.

There were many reported causes of claims, and while the most expensive were malicious hacking attacks, the second greatest cause was the wrongful collection of data—in other words, data use (or "privacy") claims.  Data use violations involve the intentional collection, storage, use, or sharing of consumer information in a way that violates the law, a contract, or an individual's right.  Organizations and individuals throughout the United States are collecting, using, and sharing data in ways that expose them to liability, often without realizing it.  One of the most frequent violations involves collecting consumer information without consent, followed closely by using consumer information for purposes that were not consented to at the time of collection.

**An Ounce of Prevention**

Perhaps nowhere else is the axiom "an ounce of prevention is worth a pound of cure" more appropriate than in the context of the modern explosion in the collection and use of customer data.  Preventing a data security- or privacy-related loss involves more than just purchasing defensive technology.  According to reports, simply adopting and implementing good policies and procedures for correctly collecting, storing, using, and sharing data would have prevented a large portion of the reported losses.  Data governance policies should be carefully crafted and followed, and should cover the following areas:

- Document retention and data destruction
- Consumer consent practices and electronic signatures
- Payment card information
- Employee email and telephone monitoring
- Website and application monitoring and advertising
- Email marketing
- Telephone and text message marketing
- Fax marketing
- International consumers and international data transfers
- Password administration and limited access
- Background checks and credit reports
- Identity theft and "red flags"
- Employee and consumer health information
- Educational records
- Sharing customer information with affiliates
- Sharing customer information with non-affiliates

The policies should address the following:

- Designated categories of data based on sensitivity (low risk, high risk, etc.) and business necessity (critical, valuable, low-value, etc.); and,
- Established guidelines for collecting, using, storing, and sharing various categories of data.

**Telling the World**

Organizations frequently publish privacy policy statements to inform their customers and others about their privacy practices.  Financial institutions, healthcare providers, and website operators are all required by law to make such statements publicly available.  Many organizations, unfortunately, misunderstand the purpose of this document.  A privacy policy statement is not the same as an internal policy or procedure; it is a public-facing disclosure that should be simple and flexible.

Organizations are often their own worst enemies in misconstruing the purpose of privacy statements.  They frequently draft and distribute privacy policy statements that include lofty language and make promises the organizations are not required to make, only to later fail to fulfill those unnecessary promises, thereby creating unnecessary liability.  Practices that do not live up to the statements made in a privacy policy statement are the number one source of Federal Trade Commission enforcement actions.

**Not If, But When**

It is natural for an organization, just like an individual, to hope that it is immune from risks that others face. If, however, the federal government, the United States military, and major multinational corporations are susceptible to major privacy and data security incidents, your organization probably is as well.  Therefore, it is most reasonable to think of a data security or privacy incident not in terms of "if," but rather "when."

Breaches and intentional, but unauthorized, data disclosure events trigger reporting obligations to federal and state officials, customers, and sometimes the media, and often result in regulatory enforcement actions and litigation (including class action lawsuits).  There are, however, steps that an organization can take to prepare for such unwelcome events and that can help mitigate resulting losses.  Two of the most important steps an organization can take are:

- Purchase cyber insurance; and,
- Adopt a breach response plan.

Cyber insurance is a term that refers to a category of insurance policies that transfer, in return for the payment of a premium, some of the financial risk of a data security incident to an insurance company.  Cyber insurance policies are not standardized, and they vary dramatically in the scope of coverage.  For example, the direct loss of funds from a hacked bank account is almost never covered by a cyber insurance policy, but many potential liabilities and defense costs can be covered.  It can be helpful to have the assistance of a knowledgeable attorney when evaluating cyber insurance coverage options.

Having an incident response plan in place is always a good idea.  Once an incident has occurred, the required timeframes for reporting the incident and mitigating any resulting harm can be very short (sometimes less than a week).  Having a plan in place, and a designated team ready to implement the plan, can make a tremendous improvement in your organization's response and potentially limit losses associated with the incident.  Additionally, incident response assistance (such as forensic computer expertise, call centers, printing and mailing services, and public relations) can be vetted and prices negotiated in advance, with potentially massive savings.

**Ready or Not, It's Time**

Complying with privacy laws, mitigating risks, and preparing for the possibility of a loss may seem daunting.  Given the scope and magnitude of the risks, however, it is simply a necessity in today's environment.  The task is manageable with some professional guidance, and the peace of mind that preparation can bring is well worth the effort.

--

*This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.*

*We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.*