What, Me Worry?

Assisting Clients with Cyber Security in the Age of Big Data Breach

by Paul L. Stoller

In December 2013, Target Corporation, the nation's third-largest retailer, announced that it had been the victim of an extensive data breach in which sophisticated hackers accessed the names and credit and debit card information of approximately 40 million of its customers. The effect of the breach was immediate and devastating. In addition to the approximately $252 million in expenses the company incurred relating to the breach, Target reported that its second quarter 2014 earnings dropped 61.7 percent from the prior year – demonstrating the dramatic financial effect the huge data breach has had on its bottom line.

While it was one of the largest and more expensive data breaches in history, what happened to Target is hardly a rarity. Indeed, Home Depot, JP Morgan Chase, Anthem, Premera, and even the Internal Revenue Service subsequently had high-profile data breaches. There are literally hundreds, if not thousands, of data breaches in the United States every year and the frequency and expense of those breaches is increasing. Nonetheless, following the "wisdom" of *Mad Magazine*'s Alfred E. Neuman, many businesses continue to approach their data security with the attitude of "What, me worry?"

Alfred E. Neuman is the fictitious mascot and cover boy of *Mad Magazine*.

Lawyers who serve as counselors and legal advisors to corporate clients should be prepared to discuss with their clients reasonable steps they can take to limit the likelihood of a data breach and their exposure in the event of a breach. That conversation begins with an understanding of the costs companies face from data breaches and the sources of such breaches, which make out the business case to take protective steps. This article addresses those issues and then discusses a number of those steps that lawyers can discuss with their clients.

The Business Case: Financial Costs and Customer Accountability.

Data breaches can be tremendously expensive. A 2015 study by the Ponemon Institute found that the average cost of a data breach in 2014 for U.S. companies was $6.5 million or $217 per record.

This included the out-of-pocket costs for investigation and forensics into the cause of the breach, determination of probable victims, organization of response teams, communications and public relations outreach, notice to affected individuals and other required disclosures, remediation, legal services assistance, identity-theft protection and credit monitoring for victims, settlement payments for private litigation or governmental investigations, and government fines and penalties.

Even beyond the immediate out-of-pocket costs to respond to a data breach, many companies suffer additional loss in the form of lost business and brand damage. That loss can be both short and long term. Short term, in the immediate aftermath of a breach, the company's systems may need to be taken down in order to determine the source and to remediate the breach. Even if the company has no business shut down or if the shut down is brief, customers (and potentially vendors) often stay away immediately after the breach out of fear that doing business with the company may expose their information. Longer term, as Target can attest, some never come back. The Ponemon Institute study found that the average business loss for the 2014 breaches in its study was in excess of $3.72 million.

Obviously, the costs to any individual company depend upon the size of the company, the size of the data breach (in terms of records), and the company's business. But, the direct costs and loss of business have the prospect of being devastating to a business of any size.

Additionally, companies are stewards of their employees' and customers' information. Beyond legal responsibilities to those individuals, companies strive to be good corporate citizens. And, the protection of personal information that, if lost, can be devastating to its employees and customers should be of paramount importance.

Where to Start? Understanding the Risk.

Assisting a client in reducing its risk to and exposure from a potential data breach starts with both the lawyer and the client understanding the client's business, what kind of electronic information it has, and how it handles that information. It also requires understanding the different types of cyber security breaches and how they happen.

The starting point of cyber security is an audit of the company's electronic information, where it is stored, and how it is created and accessed. Depending upon the size and complexity of the client and its information systems, an outside IT specialist may be best equipped to perform this task. Regardless of whether the audit is performed internally or by outside consultants, the company should understand the

types of customer, vendor, and employee data it has, where all of its data is kept, how it is accessed and moved, and the storage and destruction policies for all such data. This includes reviewing information and data that the company intentionally makes available to the public to ensure that the information does not unintentionally provide would-be hackers with the ways and means to breach its systems (examples include where and how a company's information is maintained and who has responsibility for it).

It is also essential for the client to understand the potential sources for a data breach as they can be both internal and external. Internal loss of data can be the result of both negligence and malfeasance. Employees can accidentally disclose data in numerous ways, including the simple unintentional attachment of a file to an email, copying the wrong file(s) to data storage devices, or even by posting information on the company's website. Employees can lose or misplace devices containing electronic data (such as laptops and cell phones). They can also steal the information themselves for personal profit by taking it directly from the company's systems.

With increasing frequency, data breaches are the result of intentional acts by outsiders. Hacking via the Internet is now the largest cause of data breaches. And, many of the more high-profile data breach incidents in the last five years have been the result of hacking by anonymous Internet criminals whose sole design was to steal the data from a company for their own illegal use. In addition to attacks over the Internet to access company data, third-party malicious software (malware), often delivered through email or downloads, is a significant and increasing cause of data breach. Data can also be lost by the physical theft of systems devices, data containers, or even other company property – such as thieves stealing briefcases (or cars containing briefcases) that had within them data storage devices (including laptops) containing company data.

The ability to assess a client's vulnerability to the various sorts of data breaches is certainly beyond the expertise of most attorneys; IT experts will likely be necessary to do a specific assessment for any given client. That being said, understanding how clients are being attacked can help attorneys work with clients to protect themselves from such attacks.

An Ounce of Prevention is Worth a Pound of Cure.

PricewaterhouseCoopers LLP, *CIO Magazine*, and *CSO* magazine conducted a 2014 information security survey which found companies that detected more electronic information security incidents and reported lower average financial losses per incident shared several key attributes.

Those attributes include having an overall information security strategy, employing a chief information security officer or equivalent who reports directly to top management, having reviewed the companies' security measures within the previous 12 months, and understanding the types of security events that had taken place in the prior year. Thus, effectively counseling clients in risk-reduction for such incidents should include addressing as many of those attributes as possible.

As a starting point, it is clear in most situations that companies have an obligation to take reasonable efforts to protect client, customer, employee, and even vendor data that is of a private or confidential nature. What constitutes "reasonable efforts," however, is not so clear. Indeed, courts have struggled with precisely how to determine what is reasonable in this context.

Suffice it to say, that reasonableness will be specific to the types and amounts of data held by the company, the risks it faces, and the actions it takes, including exploring the options available to it.

With those thoughts in mind, there are a number of items attorneys can review with clients to assist them in becoming more secure and reducing the risk of a breach or exposure in the event of one.

Compliance with Regulatory Requirements for Data Protection

Many companies operate within regulated industries, and increasingly state and federal regulators and agencies are requiring companies to take affirmative steps to protect cus-

tomer information. If the client happens to operate within one of those industries, one of its primary priorities should be to comply with the regulations. Compliance with regulations is not necessarily sufficient to avoid a data breach or liability in the event of one. However, applicable regulations should be considered to be minimum thresholds for information protection given that, in the event of a breach, failure to meet them could be determined to be negligence per se and may also subject the client to fines and penalties by the regulators.

Company Information and Data Security Policies

As part of its protection of electronic information, the client should have policies in place for the protection of all the data and information on its systems. The necessary technical steps for the protection of data are certainly beyond the expertise of most attorneys. But, attorneys can counsel those clients to ensure that they have sufficient expertise within their own IT departments to address network security or to work with outside IT professionals who can do so. They can also ensure that the clients have the right employee policies in place and assist clients in reviewing those policies. To that end, counsel should ensure that the company has comprehensive electronic data policies that cover information security, Internet use, email use, social media, and website privacy.

The company's information security policies should address its information systems, identify its information types and where the information is stored, determine the levels of protection for different types of information, and set restrictions on the use of or access to sensitive information, including employer, employee, and customer information. The policy should also identify who within the company is responsible for information protection, the precautions and protections to be used to protect the different types of data, the means by which information will be stored and backed up, steps the company will take to ensure the accuracy of its information is not compromised, the circumstances for disclosure of information, to whom such disclosures may be made, and who is authorized to make disclosures.

A starting point for smaller businesses looking to implement new information-security policies is the U.S. Chamber of Commerce's Commonsense Guide to Cyber Security for Small Business, which is available at **https://www.uschamber.com/sites/default/files/legacy/reports/cybersecurityguide923.pdf**. The guide contains fundamental recommendations for small businesses to protect their information that can be instituted as part of their data protection policies.

It is also advisable, given the increasing number and severity of data breaches, for companies to have a policy or an emergency plan to address how to respond in the event of a data loss or data breach. The policy should include the creation and assembly of a response team for a breach and assign responsibilities for key decisions. Those responsibilities should include the IT response (identifying the source of and closing the breach), dealing with law enforcement, and handling public relations and customer issues (including dealing with any media, providing notice to affected individuals, and responding to customer inquiries). Experian has drafted a Data Breach Response Guide, which is a useful tool for companies in preparing for and responding to a data breach.

Customer Information Privacy Policies

Many companies have existing customer information privacy policies that they promulgate regarding their treatment of the confidential and private information of their customers. Some have similar policies for the information of their employees and vendors. In those policies, the company often tells the customer how important it believes the customer's private and/or confidential information is and how the company will take steps to ensure that the information is protected and not made public. Such policies are laudable and certainly not to be discouraged.

However, the company's privacy policies should be reviewed to ensure that they are consistent with the client's obligations and that they do not overstate its commitments. In particular, the commitments made in those privacy policies will be the minimum standard against which the client's conduct is measured in the event of a breach. Thus, even if the legal requirements on data protection and security are less than what the client promises to do in its privacy policies, the client should be aware that it very likely will be held to the higher standard stated in those policies. There is certainly nothing wrong with a client taking on heightened obligations, but it should do so knowingly.

Having customer information privacy policies in place is critical.

Moreover, the client's representations as to its treatment of confidential customer information should be consistent with what it actual practices in protecting that information. In the event of a breach, the client will be held to the standard of its representations; it should make sure it is living up to them. Indeed, the knowing failure to live up to its representations could expose the client to exemplary damages.

Many of the country's largest companies have existing customer information privacy policies that are available online and can be used as a template depending upon the industry and business practices of the client.

Employee Policies on Data Use and Security

While most breaches are the result of outside hacking and malware, employee actions continue to be a contributing or direct cause in many data breaches, whether by error, inadvertence, or even theft. Since the company's employees are most often the individuals with access to company and customer data, the company should have policies to address employees' use of and access to that information. These include confidentiality, social-media, and bring-your-own-device (BYOD) policies.

For any company that has confidential and/or personal information (whether its own or of customers, employees, or vendors), it is good practice to have a confidentiality policy for its employees. That policy should address the treatment and use of confidential information and under what circumstances it may be disclosed. In addition to an employee confidentiality policy, individual employee confidentiality agreements provide a second layer of protection, further clarity in terms of the treatment of information, and the "teeth" to enforce the confidentiality requirements.

The rise of social media has created a new avenue for data disclosure and confidentiality breaches. While data breaches resulting from employee use of social media were a relative rarity even five years ago, it has become an increasingly prevalent source of breach. The exposure of confidential information through social media can and should be covered in the company's confidentiality policies. Additionally, a separate social media policy can be an important piece of a company's comprehensive data-protection plan.

Finally, employees are increasingly accessing company systems and data through their own electronic devices – their personal phones, laptops, tablets, and data-storage devices. BYOD policies are essential to establish what access (if any) employees may have to company systems and data through their personal devices and the permissible uses of those devices for company business. In the context of data breaches, the use of employee devices is an additional data-exposure risk – employees can intentionally or inadvertently capture company and customer infomation on their devices. Some companies preclude the use of any employee devices, while other companies are more moderate in their restrictions. The precise boundaries of usage are something that should be addressed by the client's officers and directors, but the lawyer should ensure that they are properly documented in a policy that is disseminated to all employees.

Destruction of Data; Document Retention and Destruction Policies

Generally speaking, the costs a company incurs from a data breach correspond to the quantity of records lost in the breach – the larger the number of records, the greater the cost to the company. Given that correlation, one way to reduce loss exposure is for the company to reduce the quantity of data it retains in the first instance. Of course, companies cannot just haphazardly destroy their data. To that end, lawyers can assist clients in the preparation and implementation of document retention and destruction policies, which provide for the orderly and appropriate destruction of data that has lost its business usefulness. A good retention and destruction policy will include an audit of the company's data and records, determine record locations, determine retention criteria and periods for types of information based on business need or legal regulations and requirements, assign custodians, and contain particular provisions relevant to the business of the company to ensure implementation and compliance by the company and its employees.

Additionally, the policy should comply with the company's contractual, regulatory, and other legal obligations to preserve data and information. Through its implementation,

the policy will ensure preservation of the company's important records but also facilitate the reduction of the volume of data it maintains such that less data is available in the event of a breach.

Employee Training and Awareness

Employee training and awareness are essential components of data security, as policies are of little value if a company's employees do not follow them. Employees should receive training not only on the company's various policies for information security but also the risks that give rise to breaches to ensure they understand how their actions could contribute to a breach. Training should be done periodically to ensure that employees remain up to date both on policy changes and new and emerging threats to the company's data security.

Review of Provider Contracts

Many clients utilize contractors to provide services for data storage, data backup, and disaster recovery services. Those relationships and contracts should be examined to ensure they provide the client both proper protection and proper remedies in the event of a data loss. Where the client has such contracts, they should be reviewed to ensure that the provider commitments to information security are consistent with the expectation of the client, its regulatory requirements, its customer data privacy policies, and its representations to its own customers as to data security. Obviously, if the contractor cannot or will not live up to the standards that the company has represented to its customers, the company will either need to find another provider or to adjust its own policies. Additionally, vendor contracts will often include limitations of the vendor's liability in the event of a loss. Often, those limits are far less than the exposure the company faces from its customers in the event of a breach (and not necessarily commensurate with the amount the providers are being paid to store and to protect the data). Those terms should be reviewed and discussed with the client so that it can maximize its security and determine how it is willing to allocate responsibility in the event of a loss by the contractor.

Data Breach/Cyber Security Insurance

In reviewing the client's data-breach protection, the lawyer should review the client's insurance policies to determine whether the client has insurance coverage for losses resulting from a data breach. Most standard commercial general liability insurance policies do not include coverage for data breaches. Thus, most companies who desire coverage in the event of a breach will need to buy specific insurance for it. Many major insurance carriers now offer data breach insurance (also known as cyber liability insurance). That insurance can cover liability arising out of a data breach, defense of claims, costs of responding to the breach, and losses from business interruption. Though not directly a loss-prevention mechanism, the existence of data breach insurance can help minimize losses from a breach. Additionally, the purchase of data breach insurance correlates with a lower incidence of data breach – most likely because those companies with good security practices are more likely to purchase insurance.

Consequently, companies who are serious about their data protection appear to be the ones most interested in having appropriate insurance coverage in the event they suffer a breach. abl

endnotes

1. Because a number of the things companies can do to reduce their risk require more detailed explanation than can be included in this article, the author has provided references and links in the text and footnotes to sources for further detail.
2. Ponemon Institute, 2015 Cost of Data Breach Study: United States (May 2015).
3. PricewaterhouseCoopers, LLC, *Defending Yesterday, Key Findings from the Global State of Information Security Survey 2014*. The 2016 study by PricewaterhouseCoopers, *CIO*, and *CISO* advocates the adoption of risk-based cyber security frameworks, including the implementations of guidelines such as ISO 27001 and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework. PricewaterhouseCoopers, LLC, Turnaround and transformation in cybersecurity, Key findings from the Global State of Information Security Survey 2016, available at www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.
4. *See, e.g., Patco Constr. Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012).
5. Another basic research source for small businesses is the Visa Data Security report, "Tips and Tools for Small Merchant Businesses," available at usa.visa.com/download/merchants/data-security-tips-for-small-business.pdf.
6. Experian Data Breach Resolution, Data Breach Response Guide (2014-2015 ed.), available at www.experian.com/assets/data-breach/brochures/response-guide.pdf.
7. As examples of some of the more extensive customer privacy policies, Apple's is available at www.apple.com/legal/privacy/en-ww/; Amazon's at www.amazon.com/gp/help/customer/display.html?nodeId=468496; and Bank of America's at www.bankofamerica.com/privacy/consumer-privacy-notice.go. In contrast, McGraw Hill provides a shorter form of privacy policy that is no less appropriate: http://www.mheducation.com/customer-privacy-policy.
8. Examples of major corporation social media policies and guidelines can be found online. Walmart's are available at http://corporate.walmart.com/social-media-guidelines; Intel's are available at www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html.
9. The American Bar Association offers a bit dated (2003) version of best practices for document retention and destruction at www.americanbar.org/content/dam/aba/migrated/buslaw/newsletter/0021/materials/recordretention.authcheckdam.pdf. Nonetheless, the process of creation of a policy and the key considerations it describes remain relevant today.
10. Ponemon Institute, *2014 Cost of Data Breach Study: Global* (May 2014) at 22.

about the author

For nearly two decades, **PAUL L. STOLLER** – a shareholder at Gallagher & Kennedy – has represented clients in high-stakes and hotly contested commercial litigation in Arizona and across the country. Paul has represented plaintiffs and defendants in virtually all types of complex commercial litigation matters, including professional liability, data privacy and security, contract, insurance coverage, securities, officer and director liability, racketeering, intellectual property, and antitrust cases. Paul has extensive experience in State and Federal class actions in Arizona and District Courts around the country. Paul has also represented attorneys, law firms, and clients in malpractice cases and with respect to ethical issues.