



Nearly every week,

a new corporate data-breach victim is revealed in the news headlines.

Indeed, in the last 24 months, Anthem, Premera, Jimmy John's, Neiman Marcus, Home Depot, JPMorgan Chase, and Target have all suffered major breaches. By the time this article goes to print, there will very likely be one or two more major American companies joining that list. These breaches are costly for the companies that suffer them—causing out-of-pocket losses, lost future business, and brand damage. And they can be devastating for the employees, customers, and vendors whose information is stolen in the breach.

Increasingly, lawyers are being asked by business clients to assist them with their cybersecurity. Particularly, lawyers are being asked to review clients' legal obligations as to information security and to recommend changes to policies and procedures to comply with those obligations as well as to strengthen the clients' cybersecurity. This article addresses several steps that lawyers can and should address with clients as part of the client's overall cybersecurity plan.

Making the Case for a Cybersecurity Plan

In the first instance, clients need to understand that they are at risk and what is at stake. As to risk, data-security experts like to say that the United States is now made up of two types of companies—those who know that they have been breached and those who do not yet know that they have been breached.¹ The threat of breach is very real and is only increasing.²

And data breaches are expensive, both in terms of out-of-pocket costs to respond and later in the form of lost business. A

2014 study by the Ponemon Institute found that the average cost of a data breach in 2013 for U.S. companies was \$5.85 million, or \$201 per record.³ The same study found that the average business loss for those breaches was in excess of \$3.3 million. As but one example, Target spent approximately \$148 million to respond to its highly publicized 2013 breach, and then reported a 61.7 percent drop in earnings in the second quarter of 2014 over the prior year. And it recently settled the consumer data-breach case against it for \$10 million and an agreement to implement numerous cybersecurity pro-

tections.

While there is no way to make businesses bulletproof to data breaches, there are steps they can take to reduce their chances of suffering a major breach and to minimize the financial consequences in the event one does occur. A 2014 security survey by PricewaterhouseCoopers LLP, *CIO* magazine, and *CSO* magazine demonstrated that companies that took certain cybersecurity steps were more likely to detect electronic information security incidents and reported lower average financial losses per incident when they happened.⁴ Those steps include having an overall informa-

PAUL STOLLER is a shareholder at Gallagher & Kennedy whose practice focuses on complex commercial litigation, including class actions, data privacy and security, officer, director, and professional liability, antitrust, intellectual property litigation, and insurance disputes.

BY PAUL STOLLER

Cybersecurity Preparedness

Helping Clients Reduce
Risks, Costs of Data Breach





tion security strategy, employing a chief information security officer or its equivalent, 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.

In assisting companies in their development of an overall information security strategy, attorneys can review the following potential steps with their clients to assist them in becoming more secure and reducing their exposure in the event of a breach.

1. Understand the client's information and risks.

The starting point for cybersecurity is to gain knowledge of the client's electronic information. Ultimately, the client must understand the types of customer, vendor and employee data it has, how that data is created, where it is stored, how it is accessed and moved, and when and how it is destroyed. This understanding often comes through a data audit performed by IT professionals. That audit should include the review of information the company makes available to the public to ensure that it does not unintentionally include confidential information or provide would-be hackers with the ways and means to breach the company's systems.

It is also essential that clients understand the potential sources of data breaches—both internal and external—and where their particular risks reside. Internal loss of data can result from acts as simple as the unintentional attachment of a file to an email or a misplaced laptop, but it can also happen by employee theft. External threats include not only hacking via the Internet (currently, the largest cause of data breaches) but third-party malicious software (malware) often delivered through email or downloads (a significant and increasing cause of breaches).

2. Compliance with regulatory requirements.

Clients that operate within regulated

industries are increasingly subject to state and federal laws that require affirmative steps for the protection of customer information. For clients in those industries, a first priority should be to ensure compliance with industry regulations. Important to note, meeting the regulatory standards alone may not be sufficient to avoid a data breach or liability in the event that one



occurs. In fact, best practices for cybersecurity and the methods used by cybercriminals are often well ahead of the law. Nonetheless, applicable regulations should be considered minimum thresholds for information protection, as the failure to meet them could be determined to be negligence per se. In addition, the failure to comply may subject the client to fines and penalties by the regulators.⁵

3. Information and data-security policies.

As part of a cybersecurity plan, lawyers should ensure that their corporate clients have comprehensive electronic data policies that cover data protection, Internet use, email use, social media and website privacy.

Those policies should address the client's IT systems, classify its data types and locations, determine the levels of protection for different types of data, and set restrictions on the use of or access to sen-

sitive data, including employee and customer information. The policies also should identify who at the company is responsible for data security, the precautions and protections to be used to protect the different types of data, the means by which data will be stored and backed up, steps the company will take to ensure the accuracy of its data is not compromised, the circumstances for disclosure of data, to whom such disclosures may be made, and who is authorized to make disclosures.⁶

The company policies should include a data-breach response plan to address how to respond in the event of a data loss or breach. The plan should establish a breach response team whose members are assigned specific responsibilities in the event of a breach. 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).⁷

4. Customer information privacy policies.

Companies should have policies regarding the treatment of customers' confidential and private information and similar policies for employee and vendor information. Those policies should identify the information companies maintain, what use they make of it, how and to whom the information may be disclosed, what steps individuals may take to opt out of certain disclosures, and the steps companies take to protect the information from public disclosure. These policies set the ground rules for the company's use and disclosure of customer information.⁸

Even after they are in place, the privacy policies should be reviewed to ensure that they are consistent with the company's legal obligations, do not overstate its commitments, and are consistent with its actual practices in protecting information. As representations to customers, employees, and vendors, commitments in privacy policies are likely to be the minimum standard



against which a company's conduct will be measured in

the event of a breach. Even if outside legal requirements for data protection are less stringent, the client should be aware that it very likely will be held to the higher standard of its promises in its policies. There is certainly nothing wrong with a client taking on heightened obligations, but it should do so knowingly and be sure to comply with them.

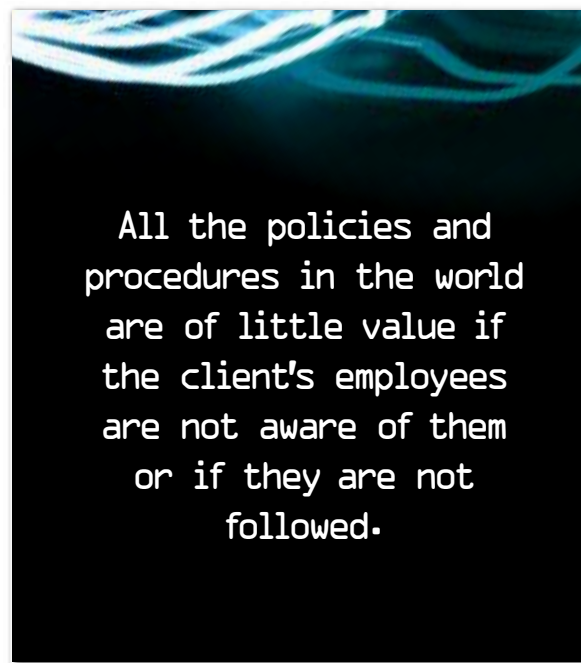
5. Employee policies on data use and security.

Companies also should have policies addressing employee use of and access to company and customer information, including 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 client's treatment and use of confidential and/or personal information and under what circumstances it may be disclosed. Individual employee confidentiality agreements can provide a second layer of protection, further clarity for the treatment of information, and the "teeth" to enforce confidentiality requirements.

As the use of social media has increased, data breaches resulting from employees use of social media have likewise become one of the more prevalent sources of data exposure.⁹ As a result, employee use of social media should be addressed in the company's comprehensive data-protection plan both through inclusion in its confidentiality policies and through a separate social-media policy.¹⁰

Finally, employees are increasingly accessing company systems and data through their personal electronic devices—cellular phones, laptops, tablets, and data-storage devices. The use of these devices on client systems creates an additional data-exposure risk as employees can capture company information on those devices and remove the information from its systems. 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. The precise boundaries of usage are something that should be addressed by the client's management, but the lawyer should ensure that they are properly documented in a policy that is disseminated to all employees.



All the policies and procedures in the world are of little value if the client's employees are not aware of them or if they are not followed.

6. Data/document-retention and -destruction policies, and destruction of outdated data.

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. One way to reduce loss exposure is to reduce the quantity of data a company retains in the first instance. Of course, companies cannot just randomly destroy their data, nor would they want to. However, document-retention and -destruction policies can provide for the

endnotes

1. Nicole Perlroth, *The Year in Hacking, by the Numbers*, N.Y. TIMES, Apr. 22, 2013, available at http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/?_r=2.
2. The California Attorney General reported that, in 2013, known breaches in California increased by 28 percent over the prior year. Kamala D. Harris, Attorney General, Calif. Dep't of Justice, *Calif. Data Breach Report* (Oct. 2014).
3. Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis* (May 2014).
4. PricewaterhouseCoopers LLC, *Defending Yesterday, Key Findings from The Global State of Information Security Survey 2014*.
5. Although the standards are currently voluntary, many regulators have been looking to the National Institute of Standards and Technology's "Framework for Improving

Critical Infrastructure Cybersecurity" (Feb. 12, 2014) as potential basis for cybersecurity standards. Available at: www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

6. A source for smaller businesses implementing new data-protection policies is the U.S. Chamber of Commerce's *Commonsense Guide to Cyber Security for Small Business*, which contains fundamental recommendations for small business data protection policies. Available at www.uschamber.com/sites/default/files/legacy/reports/cybersecurityguide923.pdf. Another basic research source for small businesses is the Visa Data Security report, *Tips and Tools for Small Merchant Businesses*, available at <http://usa.visa.com/download/merchants/data-security-tips-for-small-business.pdf>.
7. Experian has drafted a Data Breach Response

Guide, which is a useful tool to prepare for and to respond to a data breach. Experian Data Breach Resolution,

Data Breach Response Guide (2014-2015 ed.), available at www.experian.com/assets/data-breach/brochures/response-guide.pdf.

8. Many of the country's largest companies have their customer information privacy policies available online. Examples of more extensive policies include Apple's 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: www.mheducation.com/customer-privacy-policy.
9. The 2014 Data Breach Investigations Report by Verizon identifies social media as the third-

appropriate destruction of data that has lost its business usefulness while avoiding potential legal issues that may arise from data and record destruction. Those policies should identify and categorize the company's data and records, determine retention criteria and periods based on business need or legal requirements, assign custodians, determine record locations, and contain particular provisions relevant to the business of the company to ensure implementation and compliance.¹¹ The policies should comply with the company's contractual, regulatory, and other legal obligations to preserve data and information. Properly implemented, they should assist the company in reducing its volume of data such that less data is available in the event of a breach.

7. Employee training and awareness.

All the policies and procedures in the world are of little value if the client's employees are not aware of them or if they are not followed. Consequently, lawyers should ensure that their clients' cybersecurity plans include provisions for employee training and awareness. Training should address not only the company's policies but also cybersecurity risks to ensure employees understand how their actions can contribute to a breach. Training should be done periodically to ensure that employees are up to date both on the com-

pany's policies (and any changes therein) and new means that threaten the company's data security.


8. Review vendor contracts for data protection.

Many companies utilize vendors to provide data-storage, data-backup, and disaster-recovery services. Those relationships and contracts should be examined to ensure that the vendor is taking appropriate steps to protect the company's data; to comply with its regulatory requirements, policies, and representations for the protection of data; and to provide the company with appropriate remedies in the event of a data loss by the contractor. Vendor contracts often include limitations on the vendor's liability in the event of a loss—often at amounts far less than the client's exposure from a breach. Those terms should be specifically negotiated to determine an appropriate allocation of responsibility in the event of a data loss by the vendor.

9. Data breach/cybersecurity insurance.

Finally, insurance provides a potential avenue of loss mitigation in the event that a company suffers a breach. Most standard commercial general liability insurance policies, however, do not include (and often now specifically exclude) coverage for data breaches. Thus, most companies who desire data-breach and cybersecurity coverage will need to buy specific insurance for it, which is now offered by many major insurance carriers.¹²

Conclusion

Although these steps are neither a comprehensive list of all actions a business should take nor a roadmap to complete cybersecurity, they are a good starting point for any lawyer working with clients who desire to reduce their vulnerabilities to data breaches and to minimize their costs in the event of one. And they will help those clients avoid becoming the next news headline about yet another corporate data breach. 

leading cause of data breach, behind only hacking and malware.

10. Examples of corporate social media policies and guidelines can be found online, including Intel (www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html) and Walmart (<http://corporate.walmart.com/social-media-guidelines>).
11. The American Bar Association offers a bit dated (2003) but still useful version of best practices for document retention and destruction: www.americanbar.org/content/dam/aba/migrated/buslaw/newsletter/0021/materials/recordretention.authcheckdam.pdf
12. Significantly, 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.” Ponom Institute, *supra* note 3, at 23.