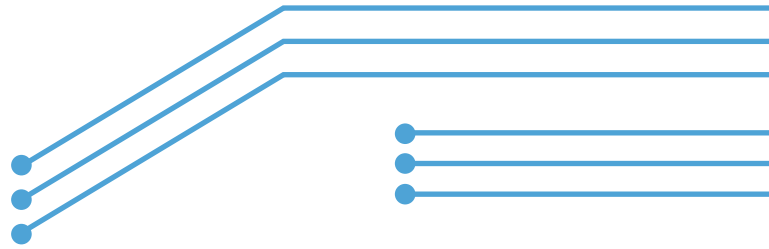
TEN YEARS LATER:

Data Governance in the Decade of the Data Breach

RONALD I. RAETHER



It has been 10 years since the term "data breach" first hit the media and became recognizable by the public. Notices issued in 2005 by companies in response to California SB 1386[1] ushered in a public understanding of the importance of data security that those of us dealing with technology had appreciated long before then. Legislatures in 47 states passed breach-notification statutes building on the California law.[2] Congress held hearings questioning the executives of the affected companies, and Congress discussed federal legislation. Many of us prepared for the expected surge in data security laws and heightened importance of the issue in the boardroom.[3] We waited. Following the TJ Maxx event in 2007 and the Heartland Payments event in 2009,[4] we again expected the surge. Now with Target, Home Depot, Sony 2.0, and Anthem in 2013 and 2014,[5] we are anticipating change yet again.

Ten years later, have we made any progress? I would say yes. For example, Congress passed the Health Information Technology for Economic and Clinical Health Act in 2013.[6] Credit issuers developed and contractually required more in-depth security requirements found in the Payment Card Industry Data Security Standard (PCI DSS), which have been improved in the past 10 years[7]. However, the progress has not been a surge. Rather, there has been slow progress in understanding the issues and adopting appropriate responses. No business today can claim ignorance to the issue of data security. But many businesses are in denial, believing they will never be a target, and they are unwilling to address security for fear that doing so will impede profitability. Other businesses implement programs that meet a general industry standard without any consideration to the issues unique to that business. Security thus becomes a check-the-box effort.

It is time for a change in how businesses consider and manage data security. I am not just referring to the tools and tactics but instead how data security is considered within the organization and the boardroom. We have often overheard information technology professionals complain about their nominalization within the organization. In reality, companies that fail to see technology as an essential component of the business and instead treat technology as infrastructure (like facilities management) will fail in the modern economy. Even IT professionals sometimes fail to see that information security is as critical to a company's success. What is the net value to the bottom line of new functionality that permits criminals to steal the identity of your valued customers, take your intellectual property, and diminish your good will?

It is not enough to focus on the products or services a company provides. Companies must create and implement effective procedures for information privacy and security risk management. Companies should employ a layered security approach, or what is commonly called security in depth. This can include perimeter security, intrusion detection systems, egression device monitoring, and the like. With this layered approach, when one security element fails, several others are in place to prevent, if not mitigate, the resulting harm. Many companies ignore this approach and relegate information security to an insignificant voice in the debate concerning the best use of company resources. Even for those companies that adopt security in depth, there is an over-reliance on technology. The board or the business leaders may think of data security like infrastructure: "Just get my phones to work—I do not want to know how—and do so at the lowest cost." This approach is foolish and, most important, will not protect critical assets.

So what does this have to do with our role as counsel? Lawyers are problem solvers. Information security presents a significant problem for many companies, and the issue is only growing in importance and complexity. As legal counsel, our responsibility is to understand the issues and provide measured advice and solutions in helping to manage these risks. This article will walk through some of the basic foundations of sound data security with an emphasis on where attorneys can best provide aid.

Critical Assets: Data Classification and Mapping

It should come as no surprise that the first questions to ask are: (1) what sensitive information do I have (i.e., data classification), (2) who uses the information, (3) where is it stored, and (4) how is it transmitted (collectively, data mapping)? Most companies have performed at least the data classification task—what information do I have. Many companies cannot answer the other questions and certainly not over time. But knowing who has access, where the information is stored, and how it is transported are critical to sound data security.

An analogy may prove useful. I have three daughters. I buy jewelry for my wife and toys for my daughters. Would I treat my daugh-

ters' toys in the same manner as my wife's jewelry—which, for me, would mean leaving the jewelry in the driveway after a long day? Obviously we would not. Yet many companies do so by not knowing the location and treatment of their critical data and thus treating all information the same.

The concepts of data categorization and mapping are critical for complying with statutes like the Gramm-Leach-Bliley Act (GLBA)[8] and the Health Insurance Portability and Accountability Act (HIPAA).[9] Likewise, companies that accept credit cards must segregate and know the location of payment information to comply with the PCI DSS standards.[10] For these companies, a breach of financial protected personal information, protected health information or credit card data presents serious consequences and difficult questions about sufficiency of the company's data security regime. However, the questions are just as difficult when asked by a board about the loss of intellectual property. It is critical to know the location and protection strategy of data. Indeed, having sound data mapping practices can allow a company to concentrate its efforts on protecting its "jewelry."

Existing Laws Provide Some Basic Data Protection Policies

We can look at the security requirements included in GLBA, HIPAA, and PCI DSS to understand the importance of data classification and mapping. At the core of each of these standards is a layered approach to data security involving sound technology and administrative controls.

GLBA provides a useful point of focus for a variety of reasons, including its continuing use as a guide for developing standards for HIPAA, state laws, and even private party contractual requirements. GLBA regulates the collection, use, and disclosure of consumer financial information by "financial institutions" (e.g., nonbank mortgage lenders, loan brokers, and some financial or investment advisers). The major components regarding privacy protections include the Financial Privacy Rule and the Safeguard Rule, which were promulgated by the Federal Trade Commission (FTC). The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice upon the establishment of the consumer relationship and then provide further notice in each subsequent year. Generally, the privacy notice must explain the information collected about the consumer, where that information is stored, how that information is used, and how that information is protected. The notice also must identify the consumer's right to opt out of the information being shared with unaffiliated parties.

The Safeguard Rule requires financial institutions to develop a comprehensive written information security plan that contains reasonable administrative, technical, and physical safeguards and measures for continuing to evaluate the plan and force adjustments to the plan based on the evaluation. Generally, the plan must include:

- A designation of one or more employees to coordinate the information security program
- The identification of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessments of the sufficiency of any safeguards in place to control those risks
- Implementation of information safeguards to control the risks identified through risk assessment, and regular tests of the effectiveness of the safeguards' key controls, systems, and procedures
- Oversight of service providers; requiring them to protect the security and confidentiality of customer information
- Evaluation and adjustments to the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances

Each of these requirements is addressed through relevant physical, technical, and administrative (e.g., training) controls. In turn, accountability through a sound governance structure is essential.

Technology

Any layered security program must include and account for the benefits and risks associated with technology. Use of technology to safeguard company data as part of a layered information security program should likewise balance technology with the business model and its associated risks. Mobile devices, wireless networks, and remote company server access all play a key part in the ever-expanding virtual office space, increasing efficiency and flexibility. Companies must balance the benefits of technology with appropriate enterprise risk management to isolate and minimize security threats, as well as to mitigate resulting harms. Information technology "doors" should be locked and monitored the same way as those to any office suite. Centralized control is essential.

Perimeter defense and access controls (similar to a castle's walls, drawbridge, and moat) should include a barrier between the bad guys outside and the valuable data inside, but they also should provide a line of demarcation along which companies can position resources and focus their attention. Firewalls are a first line of defense. Companies should also consider implementing intrusion detection systems, routing technology, and credential controls for a robust defense.

To keep abreast of corporate enterprise risk, companies should also implement oversight and surveillance technologies. Such technologies, if implemented and maintained, not only can provide intelligence for short-term notice of a potential risk but also long-term systemic reporting capabilities to assess ongoing performance issues and opportunities for improvement. System and information monitoring software, audits and logging of activity, and data backup all help support a full-layered approach to information security.

Administrative Controls—People

Even the best-designed and most robust technological security measures can be compromised by its users. People within a company have access to data and systems that can impact security well beyond their office space or assigned job responsibility. Edward Snowden was a civilian government contractor to the National Security Agency—one of hundreds, maybe thousands. The Target breach may very well have begun with an air-conditioning service provider clicking a link in a company email and unwittingly launching malware. Indeed, a company's greatest resource is its people and its business relationships. Conversely, they also present the company's greatest risk.

Contractors are used extensively in meeting workforce demands. A company should have policies of varying degrees to manage the risk associated with contractors (nonemployees) to include what work is reserved exclusively for employees and what can be assumed by contractors. The policies should include background checks, access permissions, policies, and contractor agreements. Such agreements and policies should include clear requirements for what is

acceptable and unacceptable work practice and use of information. Furthermore, a company should demand that contractor companies and independent contractors comply with the same security framework imposed within the company.[11] The third-party also should be obligated to assist in mitigating any harms resulting from a breach or other act by the contracting company or its personnel. Where appropriate, companies should secure the right to audit their third party contractors—and then actually complete such audits.

Finally, employees can be just as much, if not more, of a risk. The obvious security protocol is for companies to have clear policies and procedures for all employees. But this is not enough. A company must regularly train and audit compliance with those policies and procedures to make sure employees not only understand but also comply with the security measures. In May, a Colorado company was fined $125,000 by the Office of Civil Rights for HIPAA violations for allegedly disposing of unsecured protected health information in a dumpster.[12] In July 2014, a hospital system agreed to pay $800,000 and adopt a corrective action plan to address alleged deficiencies in its program for HIPAA compliance when its employees left 71 cardboard boxes of medical records unattended and accessible to unauthorized persons on the driveway of the physician's home, even with notice that the physician was not at home.[13] A trained employee with appropriate oversight and controls would not have made such obvious and notably low-tech mistakes. At a minimum, a company would have a reasonable defense to the actions if they had. Companies must maintain an active employee training program with an ongoing awareness program, which includes reminders and updates on new or emerging threats to company information security. (Regulators have told me time and again that they could educate on just the value of training and awareness programs as safeguards against data breach.) Companies must see information technology as part of their business rather than just infrastructure, and information security must be fully integrated with daily employee duties to successfully address threats at all fronts.

A company should have policies of varying degrees to manage the risk associated with contractors (nonemployees) to include what work is reserved exclusively for employees and what can be assumed by contractors. The policies should include background checks, access permissions, policies, and contractor agreements. Such agreements and policies should include clear requirements for what is acceptable and unacceptable work practice and use of information.

Data Governance

Before employees, contractors, and other third parties can help manage a company's risk accordingly, a company must set forth its requirements in written policies. A data governance plan is a living, documented set of guidelines for assuring the proper management of a company's digital information. Without a written expression of a company's expectations—to include the manner in which it will collect, store, and use personally identifiable information—a company cannot reasonably expect its employees and business partners to likewise meet those expectations. Furthermore, when a breach occurs, regulators and law enforcement will have an easier time understanding a company's efforts to properly manage risks to information if a written policy and supporting procedures are in place. This is especially true in regulated sectors such as health care, financial services, and with publicly held companies. After a breach occurs, a company's ability to demonstrate that it has current and substantial policies and procedures may help to mitigate, to some degree, potential liability if followed. However, companies must grasp the idea that written policies are not an end but only a means to information security.

Pulling It All Together

The above may seem obvious. However, 15 years ago we were asking project managers why security was not part of the functional specifications when a product was designed; today, we are asking board members why data security is not part of a company's strategic and financial considerations. Yet many organizations still are not taking the above steps. Or if they do so, the organization goes through the motions but with no true mitigation of risks. Why is this often the case? In short, information security is a secondary thought not only in the IT department but also in the boardroom. It is seen as a cost center and not important to financial performance. This perspective is naive at best and more likely driven by short-sightedness.

Let me provide a simple example. A firewall is in fact not a wall; it is more like a door. The device determines which packets of information get into the company's network based on whether the sniffed data includes expected credentials (a white list) or known malware or bad data (a black list). How does a company decide how those lists are created and managed? What happens if the rules keep out a customer? What if changing the rules to make sure no customers are blocked means letting in some malware? We see this same issue also come up with customer support personnel. Since these employees are evaluated based on caller satisfaction, it is easy to understand why a hacker can convince one of these employees to provide passwords and other sensitive information over the phone.

These are not just hypothetical examples. Hackers were able to compromise an individual Instagram account by convincing a consumer representative to forward the victim's cell phone to his phone.[14] The Instagram account was protected by two-factor authentication. You may understand two-factor authentication as (1) a password (what you know) and (2) sending a PIN to your cell phone (something you have). The hacker circumvented this security by convincing the cell services customer support representative to forward calls and text messages from the victim's phone to the hacker's device. Thus, when Instagram sent the PIN, it went to the hacker. How could this happen? The call center representative likely did not want to make the caller upset, not knowing the caller was a criminal. I suspect that the employee's performance goals were dependent on customer satisfaction surveys without any consideration to security.

Indeed, data security is often left out of these decisions or heavily

discounted. Information security officers report to management or to IT departments, creating conflicts of interest. When a business leader decides to not invest in security, or chooses functionality at the risk of security, there is not a corresponding recognition of the risk in the balance sheet. Rather, the decision-maker likely hopes that the breach (and corresponding costs) will not happen on his or her watch or will occur at a later point in time after he or she has received the annual bonus and has moved on.

The solution is not easy, as it requires cultural changes. To start, information security personnel need to identify the risks and present practical solutions. Information security causes itself to be marginalized when it obstructs advances and is not part of the solution. However, information security must be empowered and have a voice. The most effective information security regimes have some relation with general counsel or another individual that can take concerns to the board. Finally, decisions to forgo a recommended security feature must be recognized in financial projections and models. How to do so can be tricky. Requiring the business to purchase cyberinsurance and the resulting underwriting process is one solution. Another is to set a value of the risk created by the decision based on the likelihood of an event and corresponding costs, and then use that value when forecasting profitability of the business. In the end, accountability is the means; the goal is assuring the best risk-management decision to see the company to long-term success.

Summary

Companies need to understand how internal threats and company personnel can affect data security and information privacy. Companies should implement security through a multilayered approach while understanding what information can be shared across different internal business sectors. A company needs to understand and communicate its information-management practices, make sure employees and contractors comply with that understanding, implement and enforce policies, and communicate openly and honestly with its business partners and customers. Companies must also account for how the evolving connectivity enabled by the Internet of Things changes and impacts privacy and security. In the end, companies must not only discuss these issues but also include a governance structure that gives voice to these issues and implements the most effective solutions. Doing so puts a company in the best position possible to respond to a breach when—not if—it happens. ⊙

Ronald I. Raether is a partner at Faruki Ireland & Cox PLL, with offices in Laguna Beach, California, and Cincinnati, Ohio. Raether can be contacted at rraether@ficlaw.com.

Endnotes

[1]S.B. 1386, Cal. Civ. Code 1798.82 and 1798.29 (2013).

[2]*Security Breach Notification Laws*, National Conference of State Legislatures, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited May 12, 2015).

[3]Ronald I. Raether, *Security Before and After a Data Breach*, Business Law Today 57-62 (Nov./Dec. 2006), *available at* www.ficlaw.com/links/raether/RIR_security_before_and_after.pdf.

[4]*Jan. 17, 2007 Press Release*, The TJX Companies, investor.tjx.com/phoenix.zhtml?c=118215&p=irol-newsArticle&ID=951253 (Jan. 17, 2007); Kim Zetter, *Card Processor Admits to Large Data Breach*, Wired.com, *available at* www.wired.com/2009/01/card-processor/ (Jan. 20, 2009).

[5]*Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores*, Target Pressroom (Dec. 19, 2013) *available at* pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores; *Home Depot, The Home Depot Reports Findings in Payment Data Breach Investigation* (2014) *available at* corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf; Rachel E. Silverman & Ben Fritz, *Data Breach Sets off Upheaval at Sony Pictures*, WSJ.Com, (Dec. 4, 2014), *available at* www.wsj.com/articles/data-breach-sets-off-upheaval-at-sony-pictures-1417657799; *Statement Regarding Cyber Attack Against Anthem*, Anthem.com (Feb. 5, 2015), www.anthem.com/health-insurance/about-us/pressreleasedetails/WI/2015/1813/statement-regarding-cyber-attack-against-anthem.

[6]Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), *codified at* 42 U.S.C. §§ 300jj *et seq.*; §§ 17901 *et seq.*

[7]*See, e.g.*, *Payment Card Industries, PCI Security Standards Council on Minor Corrections to PCI DSS and PA-DSS Standards Documentation* (2009), *available at* www.pcisecuritystandards.org/pdfs/statement_090810_minor_corrections_to_standards.pdf. In 2009, Nevada enacted a law requiring compliance of merchants doing business in that state with the current PCI DSS, providing a safe harbor for compliant companies. Nev. Rev. Stat. § 603A.215 (2009).

[8]Pub. L. 106-102, 113 Stat. 1338 (1999).

[9]Pub. L. 104-191, 110 Stat. 1936 (1996).

[10]A complete list of documents, including standards, published by PCI DSS can be found at www.pcisecuritystandards.org/security_standards/documents.php.

[11]Ronald I. Raether, *Data Security and Ethical Hacking: Points To Consider for Eliminating Avoidable Exposure*, Business Law Today, 55-58, (Sept./Oct. 2008) *available at* www.ficlaw.com/links/raether/RIR_EthicalHacking.pdf.

[12]*Department of Health and Human Services Office for Civil Rights, Resolution Agreement* (2015) *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cornell/cornell-cap.pdf.

[13]*Department of Health and Human Services Office for Civil Rights, Resolution Agreement* (2015) *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/hhs-parkview-resolution-cap.pdf.

[14]Sean Gallagher, *Cell Carrier was Weakest Link in Hack of Google, Instagram Accounts*, Arstechnica.com (Nov. 3, 2014), *available at* arstechnica.com/security/2014/11/cell-carrier-was-weakest-link-in-hack-of-google-instagram-accounts.