P rivacy and data security are on everyone’s mind these days. Whether it is the revelations about the government collecting information about your phone calls and emails, the security breaches at Target Corp. and other retailers that threaten your credit card information or the constant barrage of personal data deriving from Facebook, Twitter, Instagram and the like, every person must be invested in the effort to protect personal information from the threats posed by data thieves and others.

At the same time, more and more companies need to worry about the increasingly complicated array of privacy and data security regulations being imposed on businesses of all kinds, whether in the United States or around the globe. Many service providers—including those in the records management and data storage industry—need to understand virtually all of these rules, because the obligations are imposed directly on these businesses and indirectly through the company’s clients (which could be in any industry and subject to any of these laws).

What are the key areas for companies to pay attention to on privacy and data security in 2014?

**BETTER SECURITY PRACTICES**

The Target breach has highlighted the need for better security practices in general across all industries. While the Target breach seems to have involved sophisticated computer hackers, the breach exploited system weaknesses that could have been identified through more aggressive security practices. And, while the Target breach has generated enormous media attention, we can read about security breaches—in all kinds of industries and affecting all kinds of data—on virtually a daily basis. The magnitude of this Target breach also distracts from the reality of most security breaches: They are much smaller, often involving dozens or hundreds of individuals, but also can involve virtually any kind of business that maintains personal information about employees or customers. If a business has not had a breach yet, it is likely because it hasn’t been looking for it.

It is clear that (1) every business faces realistic risks of security breaches; (2) these breaches result in complicated analysis and regulatory and operational challenges resulting from contractual entanglements and numerous state laws; and (3) many of these breaches could have been prevented through more effective security practices. It is critical for companies in all industries to review their security practices regularly and to stay on top of changing business practices, technologies and security risks. Watch what is happening to others, pay close attention to how your business operates and make sure you have identified changes in your operations and are monitoring your employees regularly.

**SECURITY LAWS & REGULATIONS**

While better security is a smart goal independent of legal requirements, an increasing number of laws and regulations are dictating specific kinds of security practices.

Specific and detailed sets of information security requirements are imposed on businesses in certain industries and, typically as well, on their service providers. The prototype is the Security Rule from the Health Insurance Portability and Accountability Act (HIPAA). This regulation, initially applied only to “covered entities,” meaning primarily to health care providers and health plans. Now, with recent changes that went into effect in September 2013, these rules apply not only to these covered entities but also to any service provider of these covered entities (called “business associates” under HIPAA) where the business associates stores, accesses or maintains any individually identifiable patient information.

These rules also extend downstream to service providers to the business associates and down the chain indefinitely. Companies in the storage and records management industries need to ensure they are following these rules if they have clients in the industry or serve clients who provide services to the health care industry.

The financial services industry—through the Gramm-Leach-Bliley Act—provides similar requirements for financial services companies and their service providers. At the same time, while these provisions apply to a wide range of entities (given the breadth of the number of companies that are service providers), there also is “default” regulation of data security practices through the Federal Trade Commission (FTC). For almost a decade, the FTC has taken enforcement action against entities that have not implemented reasonable and appropriate data security practices. Using the standards established in the Gramm-Leach-Bliley Act, the FTC has moved ahead with dozens of cases involving inappropriate security practices, starting with the B.J.’s Wholesale case in 2005.

Today, the FTC’s authority to bring this kind of case is in question. Two FTC targets have directly challenged its ability to engage in enforcement activities in connection with data security. The
In addition to these laws that regulate security practices, a parallel set of laws also has had an equally significant impact on security practices: the wide variety of state and federal provisions requiring notification to individuals and others in the event of a security breach.

first case, involving Wyndham Hotels, is proceeding in federal court. The second, involving a company called Lab MD, is working its way through the FTC administrative enforcement structure. Both cases directly present the question of whether the FTC is authorized to engage in enforcement activity related to data security independent of specific data security statutory authority, relying on its general consumer protection authority. (The Lab MD case also presents the separate and important question of whether the FTC can act in a situation where the Department of Health and Human Services has primary enforcement authority under HIPAA).

These cases will have a substantial impact on the regulation of data security in the United States. If the FTC wins these cases, it will have the ability to act without fear of later court action. Conversely, if the FTC’s authority is struck down, one of two things (or perhaps both) will happen. First, we could see a substantial vacuum in data security enforcement authority, with increased risks to individuals. This will create a meaningful enforcement gap, both in terms of regulating U.S. data security practices and in the consequences for the actions of European Union regulators and others to evaluate the strength of the U.S. data protection regime. The key question (and second step) will become whether this gap will finally force Congress to act in an area where it has tried but failed to pass meaningful legislation for several years.

While efforts to pass legislation continue in any event (either as a standalone data security bill or as part of a broader cyber security package), striking down the FTC’s authority will create substantial additional pressures on Congress to act. The likelihood of new legislation—perhaps much stricter legislation than the current FTC view—becomes much higher if the FTC can no longer act as a de facto data security regulator.

Breach Notification

In addition to these laws that regulate security practices, a parallel set of laws has had an equally significant impact on security practices: the wide variety of state and federal provisions requiring notification to individuals and others in the event of a security breach. Forty-six states and various other jurisdictions have laws requiring notification to individuals in the event of certain security breaches involving particular categories of information, such as Social Security numbers, credit card numbers and bank account numbers. The HIPAA law also now includes a breach notification regulation specifying notification requirements for breaches involving protected health information unless the information has a “low probability of compromise” following a breach. These laws generate substantial publicity through notification to individuals and, frequently, state regulators and typically lead to lawsuits and investigations. Therefore, many of these practices have little about specific security requirements, they provide a substantial motivation to improve security practices in an effort to avoid having breaches that require notification.

Where a breach triggers these requirements, or where a company determines that it should give notice regardless of the

specific legal requirements, these laws are challenging and cumbersome. Each law has as its core legal requirements, and these requirements are inconsistent or just different.

Make sure you have carefully thought through the applicable requirements and have sought competent and experienced assistance in guiding you through this legal quagmire.

New Legislation

In addition, there is a strong movement in Congress to pass national legislation that would dictate specific security practices across industries and would require data breach notification for any company at a national level. These proposals (led by Sen. Patrick Leahy) and other legislative activity under HIPAA, a revised version of legislation from prior years, and a new proposal by Sens. Carper and Blunt, the Data Security Act of 2014) have been given additional momentum because of the publicity related to the Target breach. Watch these bills carefully as they move through Congress. If passed, they will impose uniform national requirements on companies to (1) provide reasonable and appropriate data security practices and (2) notify individuals on a national basis about security breaches in specific defined situations.

Cyber Security

There also is a parallel movement to address concerns about cybersecurity. Beginning in 2012 and continuing throughout 2013 and on to today, Congress and the Obama administration have attempted (with little success) to develop a legislative and regulatory approach to cyber security issues. While Congress developed a series of legislative proposals, none of these may reach the White House. The Obama administration has tried to issue an executive order addressing the development of an overall cyber security framework. The overlaps between cyber security and data security are important for any company to understand. Data security principles, stemming from statutes like HIPAA (for the health care industry) and the Gramm-Leach-Bliley Act (for financial services firms), coupled with the FTC’s enforcement directives on data security (for everybody), have existed for many years and have focused on technical, administrative, and physical safeguards for effective protection of personal information, whether in paper or electronic form (or any other form). These laws typically were a follow-on corollary to privacy principles dictating how this information can be used and disclosed.

Cyber security, by contrast, is less of a "personal information" issue and more of a "protection of our national infrastructure" issue, with undertones of national security. As noted in the executive order, "Repetitive cyber intrusions into critical infrastructure demonstrate the need for improved cyber security. The cyber threat to critical infrastructure and our financial system, the integrity and reliability of which are vital to the strength of the U.S. economy, has become whether this gap will finally force Congress to act in an area where it has tried but failed to pass meaningful legislation for several years.

When efforts to pass legislation continue in any event (either as a standalone data security bill or as part of a broader cyber security package), striking down the FTC’s authority will create substantial additional pressures on Congress to act. The likelihood of new legislation—perhaps much stricter legislation than the current FTC view—becomes much higher if the FTC can no longer act as a de facto data security regulator.

Breach Notification

In addition to these laws that regulate security practices, a parallel set of laws has had an equally significant impact on security practices: the wide variety of state and federal provisions requiring notification to individuals and others in the event of a security breach. Forty-six states and various other jurisdictions have laws requiring notification to individuals in the event of certain security breaches involving particular categories of information, such as Social Security numbers, credit card numbers and bank account numbers. The HIPAA law also now includes a breach notification regulation specifying notification requirements for breaches involving protected health information unless the information has a “low probability of compromise” following a breach. These laws generate substantial publicity through notification to individuals and, frequently, state regulators and typically lead to lawsuits and investigations. Therefore, many of these laws say little about specific security requirements, they provide a substantial motivation to improve security practices in an effort to avoid having breaches that require notification.

Where a breach triggers these requirements, or where a company determines that it should give notice regardless of the
ADDRESS RISK

Security breaches continue to run rampant. Breach notification laws force disclosure of a wide variety of breaches. Legal requirements for protecting sensitive personal information continue to grow. Investigations and enforcement put additional pressures on companies that maintain or access personal data. And law suits present complicated challenges with threats from both individual consumers and business partners.

Companies—in all industries—need to focus their attention on protecting the privacy and security of the data they maintain, whether it be about employees, customers and any other individuals. This information is regulated and valuable.

Addressing these concerns—particularly on the security front—requires an ongoing and organized effort to attend to risk. This effort must evaluate how data are collected, where they go and what is done with them. It must review technological developments, operational changes and business developments; it cannot remain static. A good security plan from three years ago is a bad plan today.

Make sure that you are thinking about these issues regularly and spending your time and resources effectively to reduce ongoing risks to your clients, your business and the individuals whose data you maintain. 

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., a member of the advisory board for Privacy & Security Law Report and the editor of The Privacy Advisor. He provides privacy, data security and cyber security advice to companies in a range of industries. He can be reached at 202-719-7335 or at knahra@wileyrein.com.