The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

September 2013 Volume 21, No. 9

The Tensions And Overlaps Between Cyber And Data Security

Kirk J. Nahra

WILEY REIN LLP

Cybersecurity is a hot buzz word in Washington these days. Congress debates the impact of cybersecurity risks on a wide range of national concerns. The U.S. Food and Drug Administration (FDA) warns about the risk of cyber attacks on medical devices. The White House is implementing an Executive Order (EO) to develop a cybersecurity framework. The news media reports almost daily on cyber attacks, with ever-increasing levels of frantic concern.

But what is cybersecurity? And how is it similar to (and different from) its older sibling (with a more detailed legislative and regulatory history), data security?

Essentially, these concepts are roughly the same, driven by different concerns (personal privacy versus national security). The main differences are the scope of where attention is focused in regulations and the core purpose of the regulations. Data security regulation has sought to prevent the disclosure of personal information; cybersecurity concerns focus on keeping "critical infrastructure" functioning.

But any company affected by cybersecurity concerns (whether in "critical infrastructure" or not) should understand that the core regulatory framework for compliance and best practices is driven by the world of data security, where detailed laws and regulations (as well as enforcement authority) apply to virtually all companies, regardless of industry. Businesses may find the cybersecurity threat to be an effective motivator for action, whether through new resources or gaining heightened management attention, but the risks from cyber attacks essentially mirror the risks that have been addressed through data security regulation for more than a decade.

Kirk J. Nahra

Where Does The Data Security Framework Come From?

Data security is highly regulated today across many industries and most companies. Most current data security requirements stem from two related developments – security requirements as an offshoot of laws regulating the privacy of personal data and breach notification requirements stemming from risks to individuals associated with data breaches. These requirements are all driven by personal data – and are designed to impose requirements on companies as a result of their control and use of personal data.

The two most prominent data security schemes stem from the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB), applicable to the health care and financial services industries, respectively. Both statutes required the development of privacy and security policies and procedures to protect the confidentiality of personal data held in these industries. Both developed privacy regulations first, with separate security principles following afterwards. Both applied these requirements to service providers, either through contract or (as with HIPAA now) directly.

These requirements also follow core principles of "fair information practices," followed in Europe and more generally by the U.S. Federal Trade Commission (FTC). One of the key components of these fair information principles (again, driven in the first instance primarily by privacy concerns) is that privacy protections are ineffective to protect personal privacy if security controls are not appropriate. Once again, security is an offshoot of direct concerns about personal privacy.

The HIPAA and GLB regulations apply specific and detailed security requirements for covered businesses. GLB covers a wide variety of "financial institutions," including banks, insurers, credit card companies and many others. The HIPAA rules (as of September 2013) will apply directly to:

- HIPAA "covered entities" (meaning health care providers, health plans/health insurers and health care clearinghouses);
- Employee benefit plans that provide health care benefits to employees and dependents;
- Service providers to either of these two categories (called "business associates"); and
- Service providers to these service providers, and on down the chain indefinitely.

This means that detailed information security requirements, with specific enforcement risks, apply to an enormous range of companies across the country, essentially anyone in the chain who touches protected health information.

That's not all. The FTC, through a line of enforcement cases beginning with the *BJ's Wholesale* case in 2005, has developed an enforcement approach that imposes the obligation to develop and maintain "reasonable and appropriate" information security practices for companies in either of two categories:

- Companies that have individual customers; and
- Companies that have employees.

That's pretty much everyone in every industry, regardless of size. These companies all face specific legal obligations to develop and implement at least reasonable and appro-

***Kirk J. Nahra**, a Partner with Wiley Rein LLP in Washington, DC, chairs the firm's Privacy Practice and co-chairs the Health Care Practice. He assists a wide range of companies in meeting their obligations under the HIPAA rules and numerous other privacy and security laws across the country and internationally. He can be reached at (202) 719-7335.*

priate information security safeguards, including a comprehensive written information security plan, with many companies subject to additional requirements.

The FTC's view (now being challenged in an important court case involving Wyndham Hotels) is that any company that fails to implement such reasonable and appropriate information security safeguards has acted in violation of the FTC's consumer protection authority.

There are state-level laws being developed as well. The most substantial to date is the Massachusetts approach, which requires any company that maintains specific information about Massachusetts residents (putting aside the question of whether companies can figure this out) to implement a written comprehensive information security program to protect that information, covering a significant range of specified topics, including physical security, encryption and agreements with service providers.

The Massachusetts approach leads directly to the second key area of information security obligations, again applicable to essentially any company that has customers or employees. There are laws in 46 states requiring consumer notification in the event of security breaches involving certain kinds of personal data (such as Social Security numbers and credit card numbers). These laws often do not dictate specific data security requirements, but impose difficult and public obligations in the event of a security breach. The purpose of these laws is twofold: to provide notification to individuals in the event of a breach involving their personal information (primarily to permit activity to prevent future losses) and to offer incentives to implement better overall information security, to avoid the burden, publicity and potential enforcement associated with these breaches.

The Cybersecurity EO And Debate

Cybersecurity, as a regulatory and legislative issue, is being driven by a different set of concerns. As the Cybersecurity EO indicates:

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

This approach has led the debate about cybersecurity to focus on three areas: "critical infrastructure," impact on national security and development of information-sharing approaches. These efforts have been subject to enormous controversy, with the primary "result" of the debate so far being only this EO. But it is critical to recognize that what will result from this debate – whether through new legislation, detailed regulations or various voluntary standards – will be an effort to implement effective physical, technical and administrative information security practices to ensure that technological systems of companies, in at least the "critical infrastructure" areas, maintain appropriate security practices. These standards will mirror and borrow heavily from the existing data security framework, building on the principles set forth in HIPAA, GLB, state laws and the FTC's approach, but applying these principles with an eye toward the protection of information systems, rather than a focus on personal data, per se. However, unlike privacy principles, which apply only to personal information and make little sense in the context of other kinds of information, these cybersecurity principles will apply to the same systems and activities as any requirements applicable to personal information – since companies typically use the same information technology systems for their personal information as for all other information to conduct their business activities.

So, while there has been an enormous debate about the imposition of new principles, many companies already face these obligations (from the starting point of data security rather than cybersecurity), but the impact is largely the same. If a company has developed an appropriate information security approach to meet the requirements of the HIPAA rules, for example, it is most of the way toward meeting the proposed requirements of a cybersecurity framework (with the addition of various information-sharing activities in the cybersecurity area that typically are not included in data security principles).

Conclusions

For companies in virtually all industries, the resurgent debate over cybersecurity should be evaluated with these points in mind:

- Most companies develop appropriate information security policies and procedures because the company knows that it cannot function effectively without these programs. If your technology systems do not work – and are subject to security problems – your business suffers. Self-interest motivates most of these activities, without any particular focus on the kinds of information at stake, but with an overall view toward protecting business interests.
- Companies affected by specific information security regulatory frameworks – whether, HIPAA, GLB, state law or the various other existing frameworks – typically treat these obligations as a compliance issue. For some, that means effective and thorough safeguards. For others, compliance may take a back seat, with a minimalist approach – at least until a specific problem emerges.
- The cybersecurity debate will affect who focuses on these issues and how they are addressed. The cybersecurity debate – because of its focus on national security – has caught the attention of senior management in a wide range of companies who have not previously focused on these issues. Cybersecurity may be a focus point for increased resources, even where all the same requirements already exist. At the same time, by concentrating on particular "critical infrastructure" industries, the cybersecurity debate has focused attention on certain industries where the concern about personal data has been much more limited. The manufacturing and chemical sectors, for example, may have few individual customers in some settings or little data about those individuals, but all have employees. However, by being a target of attention in the cybersecurity debate, these companies will be getting specific attention in these areas even if this has not happened in the past.
- Last, the great equalizer remains the security breach. Breach notification laws focus on personal data – and it is only through dealing with these breaches that many companies have truly focused attention on information security requirements. Now, the cybersecurity debate clearly expands the kinds of information that can be affected by a breach and have resulting impact. The breach notification laws are not concerned about corporate information – but cybersecurity will address any impact from these kinds of harms, regardless of the information or systems involved.

So, while it is important to get the details right, and to ensure that the level of attention does not overwhelm the ability of companies to implement effective information security practices, companies should realize that, for most of them, most of the areas subject to the cybersecurity debate already are in place. This debate – even with the different focus than the information security requirements – should serve to improve overall information security practices, to the benefit of companies, their customers and employees.