Strafford

Presenting a live 90-minute webinar with interactive Q&A

Data Privacy and Security: Legal Strategies Amid Growing Liability Threats

Crafting and Implementing Policies and Responding to Breaches

THURSDAY, NOVEMBER 3, 2011

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Yonaton Aronoff, Senior Counsel, **Foley & Lardner**, New York

Robert D. Brownstone, Technology & eDiscovery Counsel, **Fenwick & West**, Mountain View, Calif.

Brian L. Hengesbaugh, Partner, **Baker & McKenzie**, Chicago

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
September 2011 • Volume 11 • Number 7

Ten steps every organization should take to address global data security breach notification requirements

By Brian Hengesbaugh, CIPP, Michael Stoker and Daniel Krone

Data security breach notification is rapidly becoming a significant compliance risk for global enterprises. A data security breach can disrupt business operations, damage brand reputation and customer relationships, and attract government investigations and class action lawsuits. Among other benchmarks, the Ponemon Institute estimates that a data security breach now costs an organization approximately $214 per compromised record or $7.2 million on average per incident. As such, data security breach is moving into the "upper right quadrant" on the compliance chart that maps likelihood of an incident against the severity of its potential harm. This article summarizes the rapid expansion of global data security breach notification requirements and identifies 10 key steps every global enterprise should take to address such obligations.

A. Expansion of Global Data Security Breach Notification Requirements

From the adoption of the first data security breach notification law in California in 2003, there has been a significant expansion of breach notification requirements adopted in the U.S. and abroad. It is critical to understand the scope and application of these laws in order to make reasonable decisions about how to allocate resources to manage the corresponding risks.

1. U.S. State Breach Notification Laws

Almost every U.S. state has now adopted a breach notification law. The specifics of the laws can vary substantially, but in very general terms, the laws mandate that when certain sensitive personally identifiable information (sensitive PII) is subject to unauthorized access or acquisition in unencrypted form, the business that "owns" such data must notify affected state residents, state agencies, consumer protection agencies and, in some instances, statewide media. If a service provider maintains the sensitive PII on behalf of its customer (the data owner), the service provider generally must notify the data owner which, in turn, must make the required notices.

In practice, the variations in these laws can present significant challenges. For example, the scope of covered "sensitive PII" varies among the states. Some states, such as Illinois, focus on the key data fields of name plus Social Security numbers, bank account numbers and credit or debit card numbers. Other states, such as North Dakota, have laws that cover a broad range of other data fields, such as date of birth, electronic signature, unique physical representation (e.g., a photo), employer identification number and the like. Collectively, across the patchwork of state laws, there are more than 30 different categories of sensitive PII that can trigger a breach notification obligation.

There are also variations as to what constitutes a notifiable "breach." For example, Colorado does not require notice unless misuse of the data is likely (i.e., a "risk of harm" threshold applies before notice is required). In contrast, Arkansas mandates notification whenever there is a reason to believe that covered information has been subject to unauthorized acquisition of data, regardless of any risk of harm.

Other variations apply regarding mandatory content in the notice. For example, North Carolina mandates that the notice to the individual ***must*** describe the nature of the incident. In contrast, Massachusetts specifies that the individual notice ***must not*** describe the nature of the incident. Such direct conflicts generally drive towards different notices to different state residents, although such divergent requirements pose obvious challenges in situations where notice is also provided via the organization's website (given that both North Carolina and Massachusetts residents will view the same website).

Perhaps the most acute challenges arise on the timing of the notice. Some states establish specific timelines for notification in certain cases (e.g., California requires notice in five days for certain health records). In contrast, other states, such as Arizona, impose affirmative obligations to conduct a reasonable investigation regarding the incident ***before*** notifying the affected individuals. In practice, a reasonable investigation could actually require substantially more than five days to complete, particularly if the situation involves a hacking incident or other complex scenario. The organization thus may not be able to satisfy both Arizona and California law on timing, even though both laws may apply to the same incident.

More fundamentally, as a practice point, it is critically important for an organization to perform a reasonable investigation—and to know what it is talking about—before it notifies affected individuals. Premature notification may seem like a good idea in the short term, because it helps avoid questions about "why did the company wait X days to notify?" It is not, however, a strategy that is in the best interests of the affected individuals or the organization. Among other concerns, premature notification can cause more harm than good, as the population of individuals initially notified may be excessively large or inappropriately narrow, depending on whether a reasonably complete investigation would show that more or fewer individuals were actually affected, and the substance of a premature notice to individuals may be materially misleading (e.g., if a reasonably complete investigation would reveal that more data fields, or fewer data fields, actually were affected). Simply put, a "ready, fire, aim" approach to breach notification does not work well.

2. Federal Breach Notification Laws

There is also a growing body of federal breach notification laws. In particular, healthcare providers and other "covered entities," as well as their "business associates," have duties to notify breaches of unsecured protected health information (PHI) under the Health Information Technology for Economic and Clinical Health Act (HITECH), an amendment to the Health Insurance Portability and Accountability Act (HIPAA). HITECH requires various forms of reporting to the Department of Health and Human Services (HHS); notice to the media if more than 500 individuals affected, and notification to the individuals. A similar set of requirements apply to vendors of personal health records pursuant to Federal Trade Commission (FTC) regulations issued under HITECH.

In the financial services area, the federal functional regulators have issued Guidelines on Response Programs for Unauthorized Access to Customer Information. These include obligations to maintain a response program and to notify the applicable regulatory agency and customers if misuse is possible. Comparable regulations have been issued by the FTC that are applicable to entities that provide certain financial products and services to consumers, and other requirements have been issued at the state level that are applicable to insurers.

Various additional bills on data security breach have been introduced in congress recently. It is difficult to predict when such legislation will be enacted, but in general, such legislation probably will be adopted at some point. This would follow a similar trajectory to how a patchwork of state electronic signature laws were pre-empted by the federal E-SIGN Act in 2000, and how a similar patchwork of state anti-spam laws were pre-empted by the federal CAN SPAM Act in 2003.

3. Emerging Non-U.S. Breach Notification Laws

Non-U.S. jurisdictions are quickly "jumping on the bandwagon" with the adoption of breach notification requirements. This may become particularly problematic for global enterprises, because non-U.S. jurisdictions often adopt "omnibus" privacy regulations that apply to a much broader range of data about individuals than the "sensitive PII" regulated under laws in the United States.

For example, **Germany** has now adopted breach notification requirements under three different laws. Under the Federal Data Protection Act, a breach notification requirement applies to a wide array of personal data, including: (i) sensitive personal data (defined as any information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life); (ii) personal data specifically protected by professional secrecy duties (e.g., in the medical, insurance or legal industry); (iii) personal data concerning criminal acts, administrative offenses, or the suspicion of the same; and (iv) personal data in relation to bank or credit card accounts. Under the Telecommunications Act and the Telemedia Act, notification is required if the breach involves contract data (e.g., customer's name and address, billing information, or the like) and traffic data (i.e., data in relation to connections such as the caller's number, the number called, IP addresses, duration of a call, and the like). The good news is that, due to certain constitutional prohibitions on self-incrimination, data protection authorities in Germany are limited in their ability to pursue criminal and administrative sanctions actions against organizations that provide them with mandatory notifications about data security incidents. This serves as an incentive for organizations to notify data protection authorities about such matters, even though such notifications do not preclude the authorities from pursuing actions on broader privacy matters, nor do they limit affected individuals from pursuing claims against the organization.

Russia has also recently adopted a breach notification requirement as part of its data protection law that applies to unauthorized access to any "personal information." Personal information is broadly defined as "any information concerning an individual that may be identified on the basis of that information, including his or her family name; first name; patronymic; the year, month, date and place of birth; address; family; social; property status; education; profession; incomes, and other information." The notification must be provided to individuals, although the organization is obligated to respond to any requests for information raised by the data protection authority. Perhaps more notably, Russia requires data security incidents to be "cured" immediately, and appears to impose a duty to notify affected individuals within three days after such cure. Although these statutory requirements have not been interpreted through cases or official advisory opinions from the data protection or other authorities, the combination of the broad scope combined with the strict timelines for notification may pose acute challenges in practice.

A wide range of other jurisdictions have also adopted breach notification requirements in certain sectors. For example, telecommunications providers in the **European Union** are subject to breach notification obligations pursuant to the European Commission Directive on Privacy and Electronic Communications, and broader notification requirements are expected as part of the revision to the European Commission Directive on Data Protection. In **India**, certain "intermediaries" must report a cybersecurity incident to the Indian Computer Emergency Response Team (CERT) within the Department of Information Technology. A notifiable "cybersecurity

incident" is defined to include any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data or information without authorization.

Other requirements are also emerging. For example, **Chile** has established a general consumer protection requirement that any actions that may harm consumers (such as data security breaches) must be notified to the Chilean consumer protection agency. **Mexico** also has recently adopted a data security breach notification obligation as part of its data protection law. In addition, other countries, such as **Brazil**, have active consumer protection agencies that generally are willing to pursue actions against global enterprises for data security breaches or other incidents when they affect local consumers.

4. Other Breach Notification Duties

Beyond regulatory obligations, breach notification duties can arise pursuant to contractual obligations between relevant parties. Perhaps most notably, merchants that accept credit cards and their service providers have various duties to notify data security breaches pursuant to Payment Card Industry (PCI) requirements. The required timing for these notifications can often be significantly shorter than those that apply under regulatory duties (e.g., merchants often have duties to immediately notify merchant banks about potential incidents).

B. Ten Steps To Help Address Data Security Breach Notification Requirements

What should organizations do in the face of an expanding array of global data security breach notification requirements? The specifics of an organization's actions should be tailored to reflect its industry; geographic footprint; data collections and transfers; history of data security incidents; degree to which it shares data with service providers and external parties across its "extended" enterprise, and other factors. However, basic steps that all organizations should take include the following:

1. Establish the Appropriate "Tone at the Top." Senior management should explicitly state that data security is "mission-critical" and a core value for the enterprise. Given that data security vulnerabilities exist throughout the organization, such clear communications can be essential for strengthening compliance with data security controls and ensuring expedited reporting "up the chain" of potential incidents.

2. Identify What Sensitive PII the Organization Obtains, and Confirm Whether Such Collections Could Be Minimized. This assessment will require both an understanding of the scope of applicable breach notification requirements, as well as a firm understanding of the organization's operations. In practice, it is important to minimize such sensitive PII collection, use and disclosure wherever possible as a means of managing risk. If the data is not collected, there is no risk.

3. Conduct an Information Security Assessment, and Establish Appropriate Controls. The organization should review where Sensitive PII resides internally and within the extended enterprise. The organization should establish a written information security policy and implement and maintain data security controls that are appropriate in light of applicable data security obligations under state, federal, and non-U.S. laws, as well as contractual obligations and industry best practices. Sensitive PII should be subject to appropriate encryption where feasible, due to exemptions from breach notification duties under many laws for properly encrypted Sensitive PII.

4. Manage Service Provider Relationships As Part of the "Extended Enterprise." A key source of potential risk for an organization is the service providers that store or access sensitive PII on its behalf. Typically, if a breach occurs at the service provider level, the organization must provide required notices. Managing this risk requires a focused effort in the contract negotiation process (to structure appropriate privacy, information security, audit, liability terms), and ongoing review to ensure security measures are followed in practice, and to ensure that the organization will have adequate control in the event of an actual incident.

5. Establish and Implement an Incident Response and Breach Notification Policy. The organization should adopt an incident response policy that provides procedures for responding to a potential incident, and addressing any applicable breach notification duties. This policy should establish streamlined procedures (given the time pressures of actual incidents), although it should also include details regarding methods of notification and other jurisdiction-specific provisions that can facilitate compliance with notification obligations.

6. Shop Early For Incident Response Providers. Organizations should consider identifying early those service providers that will be critically-important in the event of an actual breach, such as forensics firms, public relations firms, call center providers and notification delivery services. However, organizations should take steps to preserve any privileged work product that may be created in the course of any investigations pertaining to a data breach, including involving counsel in the selection and retention of such service providers if appropriate.

7. Enhance Communication and Training. The most carefully drafted policies and procedures may be ineffective if they are not properly communicated throughout the enterprise, or if proper training is lacking. Training should be appropriate to the role of the individual, but every individual within an organization should receive at least minimal training so as to know how to report a potential breach "up the chain" to appropriate managers.

8. Conduct Incident Response "Scenarios." The organization should also conduct "scenario" training with key incident response team members to allow them to develop a feel for an actual incident response. Key issues to test in the scenarios relate to the timing of any notification, as such experience can be critically helpful in the context of an actual incident.

9. Update Record Retention Policies. The organization should update its record retention policies to maintain sensitive PII only so long as necessary and securely dispose of sensitive PII when it is no longer needed for its identified purpose. Note that there are various state, federal and non-U.S. laws that establish standards for the secure disposal of such information, but if performed properly, this can be an important aspect of managing data security breach risk.

10. Conduct Ongoing Review. The organization must conduct ongoing reviews to confirm that its existing controls—including its written information security policy, technical data security measures, and incident response policy—reflect current technology, business activities and information security threats. Such reviews should include periodic security assessment testing on its technical data security measures. The ongoing battle between the information security professionals and data thieves and risks, as well as legal standards, are ever-changing. Controls that are appropriate today may not be appropriate tomorrow, and regular assessment will help prevent and manage data security incidents.

C. Conclusions

Data security and breach notification is an issue that now warrants priority attention from all global organizations. The 10 steps outlined above should serve as a high-level roadmap for organizations to manage this increasingly important risk. As in other areas of risk management, the implementation of appropriate policies and procedures

can produce significant cost savings for the organization over time, both in terms of preventing security incidents as well as effectively managing them when they invariably arise.

Brian Hengesbaugh*, CIPP**, *is a partner with Baker & McKenzie in Chicago, and a member of the firm's Global Privacy Steering Committee. He focuses on domestic and global data protection and privacy, data security, electronic signature, e-commerce, and social media issues.* ***Michael Stoker *is a senior associate with Baker & McKenzie in Chicago, focusing on data security, information technology, intellectual property, sourcing, and e-commerce.* ***Daniel Krone*** *is a senior associate with Baker & McKenzie in Munich, focusing on all aspects of data security, information technology, and digital media.* *The authors would like to thank our colleagues for their invaluable contributions to this article: Michael Mensik (Chicago), Michael Wagner (Chicago), Sergio Legorretta-Gonzalez (Mexico City), Edward Bekeschenko (Moscow), Christoph Rittweger (Munich), Antonio Ortuzar Jr. (Santiago), Esther Flesch (Sao Paulo) and Theodore Ling (Toronto).*