BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Privacy Practices

Corporate Security

Many companies—particularly those outside the heavily regulated industries of health care and financial services—may not realize the extent to which they face privacy and security obligations. Moreover, the privacy and security environment is changing so quickly and aggressively that virtually every company should reevaluate its privacy and security risks. Kirk Nahra, of Wiley Rein & Fielding, presents the most pressing issues for companies to focus on for 2007.

A 2007 Privacy and Security Checklist: Focusing Your Attention on The Most Pressing Issues

BY KIRK J. NAHRA

Despite the attention that has been focused in recent years on information privacy and security, by legislators, consumers, the media and enforcement agencies across the globe, privacy and security are not yet mature issues for most American companies. Many companies—particularly those outside the heavily regulated industries of health care and financial services—may not even realize that they face privacy and security obligations. Moreover, even for the most heavily regulated companies, the environment surrounding privacy and security is changing so quickly and so aggressively that virtually every company needs to be re-evaluating its privacy and security risks in 2007. With the enormous range of new obligations and areas of increased sensitivity, where should companies be paying the most attention in 2007?

1. Security Developments.

Protecting the security of personal information must be at the top of the 2007 list *for any company that maintains personal information about customers, employees or any other individuals—encompassing retailers, online merchants, banks, schools, health care entities and the rest of corporate America.* Security, which vaulted to prominence in 2006 as a legal mandate in the overall context of information regulation, remains a critical area, where active enforcement, ongoing breach problems and a variety of new regulatory and standard-setting steps require an aggressive effort to review even

 ISSN 1538-3423

the most reasonable security program, to ensure compliance with an evolving set of standards.

The widespread publicity and vast range of security breaches continued unabated in 2006. In just the past few weeks, we have seen substantial breaches in the news, encompassing a wide range of companies, including government, not-for-profit entities, universities, healthcare entities and a wide variety of retailers. (A full range of security breach incidents is collected by the Privacy Rights Clearinghouse at the Web site, at http://www.privacyrights.org/ar/ChronDataBreaches.htm).

While there are some common themes to these breaches (*e. g*., why is so much personal data stored on laptops, why aren't more steps being taken to protect laptops, how can companies increase awareness of security issues to reduce human error), the breaches also cover a wide range of security problems and industries. These very prominent public events should lead all companies to reevaluate their data protection practices, both ''systemic'' issues, like laptop security and increasing network protections, as well as more basic issues, such as increased employee training on practical security steps and identification of ''internal'' security risks.

In addition, unlike some areas of privacy regulation, security breaches also have led in certain instances to enforcement actions. These actions have been brought by a wide variety of enforcement agencies, some obvious, some not.

For example, continuing a growing line of cases involving a failure to implement reasonable security practices, the Federal Trade Commission recently brought an action under Section 5 of the FTC Act against Guidance Software Inc., based on the FTC's charges that Guidance's failure to take reasonable security measures to protect sensitive customer data contradicted security promises made on its Web site and violated federal law. According to the FTC complaint, Guidance failed to implement ''simple, inexpensive and readily available security measures'' to protect its consumers' data. As a result of these failures, hackers were able to access sensitive credit card information for thousands of Guidance customers. As with many of its previous settlements, the settlement imposes a series of security practices on the company, including implementation of a comprehensive information-security program and audits of the security program by an independent third-party security professional for 20 years.

Companies in all industries must focus attention on reevaluating and improving their information security practices.

The FTC was not the only enforcement agency taking action on security breaches. When Humana confronted two separate security breaches, it found itself facing charges from the North Dakota Insurance Commissioner, resulting in an order requiring Humana to provide credit monitoring services and pay $50,000, to offset costs and expenses incurred by the Department during its investigation. In another case, unencrypted backup tapes and discs containing personal information on 365,000 patients of the Providence Health System were stolen from an employee's car. The Health System reached a settlement recently with the Oregon attorney general, who relied on the state Unlawful Trade Practices Act, requiring Providence to provide credit monitoring and credit restoration services, as well as enhance their security program. Most recently, in December, Ameriprise Financial Services reached a settlement with the Massachusetts secretary of state, where Ameriprise agreed to pay $25,000 to settle an investigation into the loss of a company laptop that contained the personal data of thousands of Massachusetts residents.

So, not only are breaches causing significant reputational harm, but they also can result in government enforcement, even from regulators who have no clear and explicit authority that is specific to security breaches. These regulators often are not the primary regulator of security practices at all. For example, in both the Humana and Providence situations above, one would think that the U.S. Department of Health and Human Services, either through the Office for Civil Rights (which enforces the HIPAA privacy rule) or the Centers for Medicare and Medicaid Services (which enforces the HIPAA security rule), would have been the relevant regulator for a security breach. There is no reason to think that, in 2007 and beyond, these ''other'' regulators won't in fact be the main entities companies have to worry about in the event of privacy or security problems.

Beyond these enforcement actions (with more certainly coming down the pike), companies must be aware of the continuing evolution of security ''best practices.'' For example, for companies that collect credit card information electronically (including a wide variety of small and large merchants and retailers who are not typically at the forefront of information security activities) there will be new ''PCI'' (Payment Card Industry) security standards implemented, with a compliance date in 2008. These standards will require a significant undertaking by any merchant who accepts credit card payments. Similarly, even for the financial services industry (which has been subject to security regulation for a relatively long period of time under the Gramm-Leach-Bliley Act), there have been new standards in place in late 2006. These standards, issued by the Federal Financial Institutions Examination Council, require financial institutions to implement upgraded online security practices, designed primarily to improve customer authentication methods to avoid ''phishing'' breaches.

So, between actual breach problems, active enforcement and new standards, companies in all industries must focus attention on reevaluating and improving their information security practices.

2. Security Breach Notice Issues.

An important corollary to the risks associated with security breaches involves the ongoing legal and strategic issues related to the notification of individuals in connection with security breaches. These notices are becoming commonplace, ranging from notices to a handful of individuals to large scale notices numbering in the hundreds of thousands or larger.

The variety of state breach notice laws continues to create confusion and unnecessary complexity, as companies struggle to meet the requirements of these laws, along with the practical issues related to notices that should be given, even where statutes say no notice is re-

  PVLR ISSN 1538-3423

quired. Identifying whether a risk justifies notice, investigating causes and effects from a breach, crafting a letter that appropriately notifies consumers without unduly creating fear, and determining any resources that will be offered have, unfortunately, become difficult tasks for many companies.

Moreover, the need for urgent action in security breach investigations has placed an even higher emphasis on the need to have a security breach plan in place—in advance of an actual breach incident—that identifies the key steps a company should take to identify the specific details of the breach, stop any ongoing problems and mitigate any realistic risk, along with determining the details of any notice.

Companies also need to recognize that notices may cause their own problems. Sending a notice doesn't avoid lawsuits—the notice meets the obligations of the notice laws, but doesn't prevent affected victims from filing a suit, even if their only knowledge of the breach comes from the notice itself.

As companies struggle with these efforts, Congress in 2007 certainly will revisit the idea of a federal breach notification statutes, with the possibility of streamlining notification obligations by preempting state law, while at the same time broadening the obligations to companies in all states. Companies in any industry where customer or employee data is collected need to be aware of these notice obligations and have a plan in place to deal with the results of a security breach.

3. Re-Examining Data Practices.

In recognizing these ongoing problems with security breaches and the risks and challenges associated with notifying breach victims, one key project emerges for any company that maintains and collects information about individuals—identifying where this data goes, and addressing whether it needs to be in as many places as it is now. While companies often have begun to address new privacy policies for how information is disclosed, many companies have not yet addressed this more basic, and often riskier, set of issues. What kind of information should ever go on a laptop? How long should this information be kept? Are there company policies on removing information from laptops as soon as work is completed, or on removing data if an employee will be traveling? Are there policies on how employees need to safeguard their laptops? While laptops are not the only area of risk, a substantial percentage of the breach incidents in the past year have involved lost or stolen laptops. Many of these incidents have raised an obvious question: why was this data on the laptop in the first place? And, if data is stored on laptops, why aren't the protections better?

Whether it's the Veterans Affairs Department laptop containing information on 26 million veterans and active military personnel (apparently, taken home by an employee who was working from home) or the recent ''loss'' of four Starbucks laptops, containing sensitive employment data on 60,000 employees, companies need to reassess their data management practices. If the data isn't on a laptop, it can't lead to a breach when the laptop is lost or stolen. Companies need to focus on laptops, as well as PDAs (personal digital assistants), Blackberries, CDs, and other forms of disposable or portable media, but also must address the variety of security incidents in the news, and to concentrate attention on areas where problems currently exist—even if these problems, for the time being, only are affecting others.

When re-evaluating data management practices, one risk area stands out: the need to reduce the collection and distribution of Social Security numbers. SSNs clearly are the leading avenue for identity theft. Moreover, SSNs are a clear trigger point for all security breach laws. While companies may focus on security practices, many have not gone back even further in the process to identify where SSNs are collected, to focus attention on whether this information truly needs to be collected, and, if so, to identify stringent controls on where and how often this information is distributed. There are a wide variety of state laws related to the collection, use and disclosure of SSNs. Beyond these laws, companies need to be aware of the enormous sensitivity of this specific piece of data—and should implement a specific project designed to reduce the collection, storage and distribution of SSNs as much as possible.

4. Managing Vendor Risk.

In the same vein, companies continue to struggle with the appropriate means of protecting data when it is provided to vendors. Vendor risks are creating both significant legal risk and practical management challenges, particularly for larger companies that employ large numbers of vendors. Most companies are both ''principals'' and ''agents,'' and therefore are both on the giving and receiving end of the need to develop appropriate contractual protections.

Companies need to be aware that implementing appropriate vendor controls is a legal requirement in most situations. For companies in regulated industries (such as financial services and health care), these requirements are clear, explicit and detailed. For other companies—essentially all of whom are subject to potential enforcement by the Federal Trade Commission—developing appropriate monitoring and oversight mechanisms is an essential component of the ''reasonable and appropriate'' security practices required by Section 5 of the FTC Act. Accordingly, companies need to focus on (1) identifying their vendors that receive personal information; (2) ascertaining whether these vendors need to have this data; (3) developing appropriate contractual protections for any vendor that receives or creates personal information; and (4) identifying an appropriate means of monitoring the activities of your vendors, particularly those who have either large volumes of data or who engage in more sensitive activities.

For many companies, both as principal and agent, the challenge of preparing hundreds or thousands of appropriate contracts as well as monitoring tactics is a daunting challenge. Clearly, companies can become overwhelmed by this challenge, with the result that some companies have thrown up their hands and chosen to essentially ignore the problem. This ''bury your head in the sand'' approach is no longer viable, and there are means of developing appropriate template contract terms and reasonable oversight activities that can make this challenge more reasonable (even though appropriate expert assistance may be required).

One interesting project is emerging to assist with this ongoing dilemma. The BITS group, an offshoot of the Financial Services Roundtable, has taken on the vendor dilemma by developing a set of common guidelines, by which companies can evaluate vendors and vendors can

attempt to standardize their practices, to meet the needs of different customers and reduce the costs of having to meet the demands of these different customers. This project, called the Financial Institution Shared Assessments Program, has been led by several major banks in partnership with major accounting firms. The program is designed to both (1) raise the level of security of financial services, while, at the same time, (2) trying to lower costs for banks, insurance companies and computer-services providers. More information on this program—which could easily serve as a model for other industries—is available at http://www.bitsinfo.org/FISAP/index.php.

Keep an eye over the next few years on how this program is working and whether it becomes a reasonable vehicle for appropriate standards with reduced workload for other industries. Regardless of the effectiveness of this approach, companies need to implement a reasonable strategy in 2007 to manage their privacy and security risks arising from vendor relationships.

5. Expanding The Role of The Privacy Officer.

Moving beyond the world of data security and security breaches, the most visible privacy story of the year may have involved the pretexting problems at Hewlett-Packard, which resulted in civil settlements, criminal charges and significant loss of executive-level jobs. While there were many issues at play in this situation—and we may still not know all the facts, even with the massive media attention—it is clear that companies need to ensure that their privacy officers are involved in key issues that have any impact on personal information. An effective privacy officer, if consulted and involved in significant activities, can be a useful brake on inappropriate activities, even if they are not clearly illegal. Privacy officers are clearly the norm in regulated industries. More and more companies, regardless of industry, are creating a privacy officer position, and filling these positions with well qualified lawyers, compliance experts and others.

At a minimum, privacy officers need to know the rules concerning data privacy and security. To be effective, the privacy officer must know and understand the company and its business, so that he or she can contribute both in the creation of the business model and the evaluation of how these models are working. To be useful, however, the privacy officers need to be involved and to be consulted by senior management when significant steps are being taken. Increasingly, the world of privacy and security is one where knowledge of the law is not enough. While privacy officers can point to the enforcement rules for various privacy laws, they also need to be media savvy and to understand—and be able to communicate to corporate management—that many privacy risks have nothing to do with formal enforcement. Appearances matter in this area, given the vast media, consumer and legislative attention to privacy and security (It should not escape notice that the HP scandal led directly to a new federal law, passed in the waning days of the 109th Congress—related to ''pretexting.'')

So, companies need to pay attention to their privacy officer. Those that don't have a privacy officer should consider whether to get one. They increasingly are becoming the norm in large businesses, particularly those with any consumer-driven businesses. (The International Association of Privacy Professionals, the privacy officer trade association, continues to grow every year, with more than 3,000 members in 23 countries and 1,000 Certified Information Privacy Professionals). As discussed below, given international privacy complications, one of the major challenges for most privacy officers involves employee data—so even companies with no consumer presence but a large employee base should have a privacy officer. In addition, privacy officers need to be a part of the management team: knowledgeable, able and consulted, not only on clear privacy legal issues, but also on the wide range of issues where an understanding of the implications of data practices matters. The HP scandal means nothing less than that more privacy officers at higher and higher levels in the company need to be involved in and consulted for more and more corporate activities.

6. Navigating The Legal Quagmire.

Privacy officers, compliance officials, lawyers and others also need to address how best to comply with the increasing quagmire of laws governing privacy and security. Laws and policies cover multiple industries. An increasing number of laws set out ''general'' standards independent of industry. At the same time, the states are passing laws on a wide range of topics related to privacy and security, and focusing attention on laws that have been on the books for years. These laws often are inconsistent, or impose differing standards. Evaluating how best to meet these complications, as well as trying to figure out what laws apply to you, is becoming one of the most difficult challenges. What do you do if you are governed by one law, and your customer is following another? What if you are governed by 50 (or more) different laws? How do your vendors know what law to follow? Is the typical contract provision stating that the party will follow ''all applicable law'' remotely useful in this context?

Accordingly, companies need to have a more complete understanding of the universe of laws governing their collection, use, disclosure and protection of information. It is only with this knowledge, and a sophisticated understanding of both the business environment and the emerging best practices, that companies can develop a realistic approach to managing privacy and security risk and compliance obligations.

7. Expanding Complexities With Health Care Information.

For substantive privacy issues, there may be no hotter area than the wide range of developments affecting the use, disclosure and distribution of health care information. Several integrated developments are driving this complex problem. First, employers are becoming increasingly involved in the management of their health care expenditures. They are exploring new benefit options, designed to reduce overall expenditures and improve employee health. This has led to the need for more information, to evaluate how these new opportunities are working. At the same time, employers (and many others) are interested in ''wellness'' activities: encouraging, incentivizing and forcing employees into programs designed to improve overall health. Data clearly is needed to drive these activities, if they are to be effective.

At the same time, research is becoming an increasing source of new information in the health care field—and more research needs more data. Also, as medical re-

  PVLR ISSN 1538-3423

search reaches further into the details of the human body, this information can be used for more and more things, some good, some bad, most of which depends on your perspective. So, the sensitivity of uses of medical data is increasing.

In addition, the push toward electronic medical records and personal health records is raising a wide variety of new and old issues. The primary goals of this movement are to improve medical outcomes and decrease administrative costs in the health care industry. To achieve these goals, appropriate privacy practices need to be developed, that both permit the most information to be used while, at the same time, protecting patient privacy and convincing patients that their personal information is protected and won't be misused. This is an enormous challenge, one that involves analysis of existing laws, identification of current best practices, and a significant new debate about the appropriate means of protecting patient privacy. (Full disclosure: I co-chair a working group at the U.S. Department of Health and Human Services that is tasked with developing many of these practices).

As this debate continues, the marketplace is moving ahead. Several large employers recently announced a new program to create personal health records for thousands of employees across the country. On almost the same day, two leading health insurance groups announced a joint program to develop compatible medical records for use by their customers. So, the health care industry—already at the forefront of privacy and security regulation—now is at the forefront of altering our perceptions of how medical information should be used, leading to a new and ongoing debate about the uses and disclosure of medical information. Because virtually all companies use health care information to some extent, whether through insurance, disability, medical leaves, job applications or otherwise, it is critical to monitor these developments and develop an appropriate understanding of how this ongoing evolution will affect your company.

8. Managing Expanding International Regulation.

As an add-on to the complexity of the multitude of U.S. privacy and security laws, the international privacy regulatory environment also is becoming more complicated. We saw various events in 2006 that focused attention on these international issues, starting with the French data authorities imposing restrictions on whistleblower reports and ending with the finding by the European Union Article 29 Working Party that the U.S. government's agreement with the Brussels-based bank consortium known as SWIFT, giving the U.S. government access to a database about people making bank wire money transfers, violated EU privacy law.

For many U.S. companies, the international data environment arises in several different circumstances. For many employers, the first brush is related to employee data. Transmitting employee data across international borders, particularly leaving Europe, is exceedingly complicated. For other companies, the requirements arise in relation to outsourcing contracts and other contractual obligations, where companies are required to make representations about their international compliance or the participation in the Department of Commerce Safe Harbor program.

While no article, particularly a short one, can address the full range of international privacy issues, companies need to focus on a few key issues:

- Do you have data that crosses international borders?
- If so, what kinds of data are involved, and why is this data being transferred?
- Do you outsource any functions that involve vendors located in other countries?

Once these basic data flow issues are addressed, companies can evaluate how they will manage these data flow issues, including what country's laws are involved and how the company proposes to comply with them. This international information dilemma shows no indication of simplifying, particularly as more and more countries create additional privacy and security regulation.

9. Understanding and Revising Your Privacy Policy.

One of the cornerstones of privacy regulation in the United States is the idea of notice: telling your customers and your employees what you do with their data. This component has led to formal privacy notice requirements in many laws, such as HIPAA and Gramm-Leach-Bliley, and the de facto obligation for companies doing business on the Web—despite Congress' inability to agree on a federal Web site notice standard. Its clear that most people don't read their privacy notices, and that the ones who do read them often are confused.

With that said, however, a privacy policy is both a key component of a company's philosophy about privacy and a critical measuring stick for enforcement action, particularly by agencies like the FTC and the state attorneys general, who often rely on vague ''unfair competition'' concepts to bring enforcement action. For example, several of the most recent FTC settlements, including the Guidance settlement discussed above, are premised on violations of a company's privacy policy. These policies may become even more important in the future, both due to various ongoing projects related to ''clarifying'' or ''redefining'' privacy policy obligations, as well as certain new activities, such as the development of personal health records, where compliance with privacy policies may become the primary vehicle for privacy enforcement, in the absence of new laws.

Accordingly, companies need to revisit several key issues related to privacy policies.

- Do you have a policy? (or more than one policy)?
- Is the policy (or policies) accurate and complete?
- Are there things you want to do that are restricted by your privacy policy?
- Can you revise your policy to meet changing business practices?
- Do you need to revise your policy, either to restrict its application, meet new privacy practices or comply with evolving standards?

While these questions are a mandatory start, companies should view their privacy policy as a required short-form definition of a company's privacy philosophy, one that should be visible to the various constituencies for the company, including the employees who need to implement these practices.

10. Keeping an Eye on The Litigation.

It is fair to say that virtually all privacy experts—including this one—have been wrong in our predictions concerning privacy and security litigation. There simply hasn't been much of it, despite the flood of new laws and significant privacy and security problems. While it is not reasonable to expect a flood of privacy and security cases, particularly ones that get past an initial court stage, it is important to understand the litigation landscape and to be aware of new developments in this area.

Why hasn't there been more litigation so far? Three major reasons stand out.

First, while there has been a flood of new privacy obligations, most new laws have been passed without any obvious private right of action. So, under HIPAA and Gramm-Leach-Bliley, for example, there is no clear path for bringing a suit, even if a potential claim surfaced. Courts have rejected efforts to put a HIPAA label on a private claim, even if a ''HIPAA violation'' appears to have been alleged.

Second, within the limited range of suits that have been brought, there is a reasonable trend that makes proof of damages exceedingly difficult. There have been a number of recent cases (one key case to remember is *Smith v. Chase Manhattan Bank*, 741 N.Y.S.2d 100 (App. Div. 2002)), where courts have been skeptical that privacy or security breaches have caused any damage, even enough to justify a complaint going forward.

Clearly, with other fish to fry, the plaintiffs' bar has not been impressed by the potential ''pot of gold'' related to privacy litigation. Nor, despite the modest recent increase privacy and security-related filings, is there any particular reason to think that courts are in any way more sympathetic to claims of damages in connection with potential privacy and security harms.

Third, in many arenas, successful class action litigation follows significant government enforcement activity. In the privacy and security realm, government enforcement obviously has been limited and, in some cases, almost non-existent. So, whereas there are virtually automatic lawsuits filed when the SEC takes enforcement action against a publicly traded company, there have been few ''lead events'' by the government enforcement agencies that have led to follow on class action litigation.

But this may be changing, and it is important for companies to focus on both what kinds of suits are being brought and to pay special attention to any successful claims. With increased enforcement action from a variety of government agencies, plaintiffs may have new ''starting points'' for their claims. The security breach notification laws, while not directly assisting plaintiffs with their damages claims, create awareness of a broader range of security problems. We also are seeing some companies fighting among themselves, often over responsibility for the costs of mitigating a security breach. We also are seeing privacy issues arising in a variety of cases where personal information is relevant, but not the ''cause'' of any specific action. So, there is a lot for companies to pay attention to, and to factor into their overall privacy compliance efforts.

Companies in all industries need to keep a watch on these developments. Because the area is so new and (as of now) so limited, each new case takes on increased importance. Moreover, litigation risks need to be factored into both the development of privacy policies and the legal and practical strategy related to mitigation of privacy and security breaches.

Conclusion

So, there's clearly a lot to do in 2007. Moreover, these items, while more than the tip of the iceberg, are only the most critical areas of broad applicability. Obviously, for companies in certain industries, issues related to marketing (e-mail, telephone and fax), or radio frequency identification (RFID) technology programs will create more substantial obligations. But this list hits the highlights for the broadest reach of companies.

Therefore, regardless of your industry, it is critical to understand the need to focus on these issues, recognize the risks associated with the creation, maintenance and distribution of personal information, and to develop an appropriate strategy towards reducing and managing these risks in the year ahead.

  PVLR ISSN 1538-3423