Posted On: 4/6/2010

Data Breach Legislation 101: Top Principles for Mitigating Brand Risk

Mary Hildebrand, Esq., Lowenstein Sandler, PC; and Matthew Savare, Esq., Lowenstein Sandler PC

Over the last five years, there have been a number of high-profile, electronic data breaches that have sent shock waves through the public; and increasingly, the hospitality industry has been the target and victim of data breaches, both in the digital and the physical world.

Explaining the problem

Although it is difficult to pinpoint exactly why criminals are increasingly targeting hotels and resorts, several explanations do surface. First, hotels and resorts typically do not employ the most robust electronic and physical safeguards to protect their computers and networks and criminals take the path of least resistance. For example, Forbes reported an incident where hackers gained access to a hotel's network by exposing a vulnerability that had been routinely patched by other software vendors for their clients 10 years prior. Evidently, the hotel or the software vendor it hired did not update the network to solve this security glitch.

Second, hospitality companies generally obtain a great deal of personal and financial information from their guests, including names, addresses, and credit card information.

Finally, the hospitality industry, unlike other sectors of the economy, lives and breathes in the real world. As more and more people work remotely, they often bring laptops and other mobile devices or work on hotel machines, which are often not secured. This has invited trouble. For example, in June 2006, a Humana employee working on a hotel computer failed to delete a file he created that contained the personal information of Humana customers enrolled in the company's Medicare prescription drug plans. It is estimated that 17,000 records could have been compromised. Similarly, in September 2006, a GE employee's laptop was stolen from his hotel room. The laptop contained the names and Social Security numbers of approximately 50,000 current and former GE employees.

Legislative efforts to curtail data breaches

In response to numerous, well-publicized data breaches, virtually every state in the country, including New York, California, Hawaii, Florida, Puerto Rico, and the Virgin Islands, have enacted data security breach notification laws. These laws typically require notification after a data breach. However, some states, like Massachusetts, have revised their regulations and impose several compliance obligations to prevent data breaches.

Massachusetts' amended data privacy regulations, which are some of the most comprehensive and restrictive in the nation, became effective on January 1, 2010. These regulations apply to all "persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." In other words, the regulations are not restricted to companies that are located or operate in Massachusetts. Other states, such as New Jersey, have similar laws that aim to protect their residents, even if the company does not do business in the state. Thus, the clear trend is for states to impose broad-based regulations that transcend particular industries and localities.

Even if a hotel or resort does not fall within the scope of Massachusetts' new regulations, the rules are instructive for at least two reasons. First, other states have enacted similar laws with respect to their residents, so it is likely that the hotel or resort is subject to the data privacy laws of more than one state. Since Massachusetts employs one of the most restrictive regulatory regimes in the country, complying with its regulations will assist in complying with the laws of other states. Second, as described below, the requirements under Massachusetts law, although stringent, do offer some useful best practices to help reduce the incidence of data breaches.

Risk mitigation principles
Given the myriad privacy statutes currently in effect, there is no single compliance checklist. However, the following principles, many of which are taken from the new Massachusetts' regulations, are useful to reduce your company's exposure to data breaches:
1. As required under Massachusetts law, companies should develop, implement, maintain, and monitor a comprehensive, written information security program. The security program should be "reasonably consistent with industry standards," and contain "administrative, technical, and physical safeguards" to protect the security and confidentiality of personal data. Businesses may tailor their programs based on their size, scope, and type of business, etc. However, in their security programs, companies should do, at a minimum, the following:

- Designate one or more employees to maintain the program
- Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the personal information;
- Develop comprehensive security policies for employees;
- Impose disciplinary measures for violations of the program;
- Prevent terminated employees from accessing personal information by immediately prohibiting physical or electronic access to such data;
- Take "all reasonable steps" to verify that any third-party service provider with access to personal information has the ability to protect such data in accordance with the regulations;
- Limit the amount of personal information collected to only that which is required for the legitimate business purpose for which it was collected; limit the time within which the data is kept; and limit access to such information to only those who are reasonably required to have it;
- Create a comprehensive inventory of paper and electronic records; computers, including laptops and portable devices; and storage media that contain personal information;
- Impose reasonable restrictions and safeguards upon the physical access to records containing personal information;
- Monitor and upgrade the program regularly to ensure compliance;
- Audit the scope of the security system described below at least once a year or whenever there is a material change in business practices that may affect the security of personal information;
- Document actions taken in response to any breach of security.

2. As required under Massachusetts law, companies should establish and maintain a security system, under which the company:

- Creates secure user authentication protocols, including strict control of user IDs and passwords;
- Develops secure access control measures that restrict access to personal information to only those who need the information to perform their obligations;
- Encrypts, to the maximum extent technically possible, all data containing personal information that will travel across public networks such as the Internet, and encrypt all such data that will be transmitted wirelessly or that is stored on laptops or other portable devices;
- Monitors systems for unauthorized use of or access to personal information;
- Utilizes reasonably current firewalls and security patches on all systems connected to the Internet that contain personal information;
- Uses reasonably current security software, which must include malware protection and current patches and virus definitions; and
- Educates and trains its employees on the proper use of the security system and the importance of the security of personal information.

3. Although most of the focus regarding data breaches is on electronic data, many breaches still concern physical documents. As such, filing cabinets, desks, and rooms containing sensitive information should be locked.

4. All paper and electronic files that are to be discarded should be obliterated. For example, paper documents should be cross-shredded or destroyed by a third-party vendor; removable media such as thumb drives or CDs should be thoroughly destroyed, not simply erased or reformatted.

5. Companies should create strict internal procedures that dictate how they will respond to security breaches. Frequently, as under the law of New Jersey, such responses are dictated by statute or regulation.

6. Companies using outside vendors to collect, store, process, transmit, or destroy their data should:

- Investigate and determine if their vendor's privacy and security policies and practices are adequate;
- Delineate the vendor's specific obligations, rather than simply stating that the vendor will comply with all

applicable laws;

- Perform privacy audits on the potential and existing outsourcers on a periodic basis; and
- Attempt to establish a strong working relationship with the vendor's privacy officer.

7. Companies should consider obtaining cyber-insurance, which covers a broader range of privacy and identity theft claims than general liability policies.

Mary J. Hildebrand is a member of the law firm Lowenstein Sandler, PC. She focuses on strategic planning, commercialization, protection, and management of intellectual property and technology assets in the United States and many foreign jurisdictions. Her e-mail address is mhildebrand@lowenstein.com.

Matthew Savare practices intellectual property, media, entertainment, and privacy law with Lowenstein Sandler PC. His e-mail is msavare@lowenstein.com.