HUNTON& WILLIAMS

CLIENT ALERT

May 2008

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Additional Lawyers
Utaukwa B. Allen
Cédric Burton
James A. Harvey
Jörg Hladjk
Natalie Hunt
Elizabeth Hendrix Johnson
Christopher Kuner
Manuel E. Maisog
Melinda McLellan
Randall S. Parks
Boris Segalis
Aaron P. Simpson
Rachel M. St. John
Bridget C. Treacy
John W. Woods, Jr.

Center for Information Policy Leadership
Martin E. Abrams*
Paula J. Bruening
Fred H. Cate
Orson Swindle*

*Not a lawyer

CSIS's Commission on Cyber Security for the 44th Presidency

Views from Beyond the Beltway: Cyber Security Recommendations from the Experts

By Lisa J. Sotto

Good morning. My name is Lisa Sotto and I am a partner in the New York office of the law firm of Hunton & Williams LLP. I head the firm's Privacy and Information Management Practice and also serve as Vice Chairperson of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee. Thank you for the opportunity to participate in this important dialogue. I am doing so on my own behalf and my views should not be attributed to Hunton & Williams, any client of the firm, or the DHS Data Privacy and Integrity Advisory Committee.

During the last two years, my firm has handled more than 200 data security breaches. The breaches have ranged from the most benign (like a laptop lost in an airport) to the most nefarious (like a maliciously deployed root kit in a corporate server). I will quickly summarize some of the key lessons I have learned from this experience, before offering four recommendations for your consideration.

In this country, an entity that experiences a security breach is required, pursuant to 40 plus state security breach notification laws, to notify the individuals whose data may have been compromised. While we have a patchwork quilt of data breach laws, the result is essentially the same: organizations must disclose their data breaches publicly.

The data breach laws are patterned after the Emergency Planning and Community Right-to-Know Act, which mandates reporting by individual facilities of releases of hazardous chemicals. As a former environmental lawyer, I see many analogies between the current state of data security and the state of the environment as it existed 30 years ago. Data security is a nascent area of the law, as environmental law was years ago. But we managed to make major strides in cleaning up our environment through laws requiring public accountability and through a fundamental shift in corporate behavior. We can do the same for data security.

To some extent we already are. As a result of the data breach notification laws, companies are being held publicly accountable, and therefore are devoting more resources to the protection of personal data. The breach notification laws have, without question, resulted in a significant behavioral shift. But because

there are 40 of them, not to mention local laws, compliance costs are high. In addition, most of these laws apply not only to true breaches, in which sensitive data are targeted by criminals, but also to lost backup tapes and stolen computer equipment, which law enforcement officials and research tell us pose no meaningful risk of identity theft.

As a result, we are diverting scarce resources and inundating the public with often meaningless notices.

As serious as this is today, it is certain to become more significant as data security threats escalate. And they are escalating. In the past year, I have dealt with an increasing number of security incidents that are the result of targeted, malicious attacks. These have involved malware such as worms that originate in Eastern Europe, phishers from Latvia, and system intrusions involving rootkits that go undetected for years. There is growing evidence that both the attacks through which data are collected and the efforts to exploit that information are becoming more organized, more malicious, and more global.

So what should we do to confront this challenge?

First, a federal breach notification law is needed not only to establish nationwide requirements and preempt inconsistent state and local enactments, but also to require public disclosure only of breaches that present a reasonable risk of harm. Such a law would permit businesses and individuals alike to focus their prevention and response efforts on real threats, and on new and emerging attacks, rather than on lost equipment that happened to contain personal data.

Second, we must expand our efforts to work together to make stolen data harder to exploit. There is undoubtedly a role for law here—for example, federal financial regulators have already taken steps to require multifactor authentication. But, in the long run, education, research and the sharing of best practices will be far more important.

Third, businesses must approach information security in a more holistic manner. Information security needs to become part of the corporate ethos and part of a broader risk management strategy. That means companies must have appropriate security-related policies and procedures, conduct background screening on new hires, train employees on data security, make vendors responsible for safeguarding data, and implement appropriate technical and physical controls. These controls must evolve as the risk changes and data thieves become more and more sophisticated. Businesses must protect personal information in the same way they have always sought to protect sensitive business information, like the Coke formula. If we don't fundamentally change the corporate culture to keep looking for the solution to tomorrow's attack, we will always be fighting yesterday's battle.

Finally, data security cannot be left solely to industry. We also need to educate consumers so they can take steps to protect their own data. Without greater awareness and education around the issue of data security, there will always be weak links in the chain—and experience tells us that attacks evolve to take advantage of these weaknesses. Current research suggests that individuals are the most common source of the information that is used to steal their identities and commit financial fraud. Attacks directly targeting individuals, such as phishing and malware, are growing, in large part because they are proving successful. It won't matter how well we secure corporate and other institutional repositories of personal data. If individuals don't protect their own data, and don't take advantage of the many tools (such as free credit reports and bank and credit card statements) available only to them to detect fraud early, the battle will be lost.

Thank you for allowing me to participate in this important discussion. I look forward to your questions.