DOS AND DON'TS OF DATA BREACH AND INFORMATION SECURITY POLICY

A White Paper of the Centre for Information Policy Leadership at Hunton & Williams LLP

Fred H. Cate, Martin E. Abrams, Paula J. Bruening & Orson Swindle[1]

Breaches of personal data held by both public and private entities continue to soar. 656 were reported in 2008, up 47 percent from 2007. Between 2005 and 2008, the United States alone accounted for 1,572 reported breaches involving more than 247 million records.[2] Well-publicized breaches in Japan, Germany, the United Kingdom, and other countries involved millions of additional records.

Concern over data breaches has led to the adoption of notice requirements in 44 states and the District of Columbia, in federal regulations, and in the recent stimulus bill—the American Recovery and Reinvestment Act. Data protection commissioners in the United Kingdom, Canada, New Zealand, and Australia have recently published "guidance" concerning security breaches and the role of notification. The European Union has begun the process of considering a draft directive governing electronic communications services that contains provisions governing security breaches, including a security breach notification requirement. The Federal Trade Commission (FTC), the Asia-Pacific Economic Cooperation (APEC) forum, and the Organisation for Economic Co-operation and Development (OECD) are hosting a multinational workshop on "Securing Personal Data in the Global Economy" in Washington on March 16-17, 2009.

DOS AND DON'TS OF DATA BREACH AND INFORMATION SECURITY POLICY

1. **Don't equate data breaches with identity fraud or other consumer harms.**
2. **Don't become so preoccupied on data breaches that you lose sight of other, far more serious, security risks.**
3. **Don't count the cost of poor security just in economic harm to individual consumers or businesses.**
4. **Don't trivialize breach notices by requiring them when there is no reasonable risk of harm.**
5. **Don't go it alone.**
6. **Do take data security seriously.**
7. **Do create incentives for good behavior.**
8. **Do collaborate to succeed.**
9. **Do anticipate, don't just react to, threats.**
10. **Do be realistic.**

In anticipation of that workshop, the Centre for Information Policy Leadership at Hunton & Williams LLP (the Centre) is releasing this white paper with ten key recommendations for data breach

[1] Fred H. Cate is Distinguished Professor, C. Ben Dutton Professor of Law, and Director of the Center for Applied Cybersecurity Research at Indiana University, and a Senior Policy Advisor in the Centre for Information Policy Leadership at Hunton & Williams LLP (the Centre). Martin E. Abrams is Executive Director of the Centre. Paula J. Bruening is Deputy Executive Director of the Centre and member of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. Orson Swindle is a Senior Policy Advisor and Chair of Security Initiatives in the Centre, member of the CSIS Commission on Cybersecurity for the 44th Presidency, and former Commissioner of the Federal Trade Commission.

[2] Identity Theft Resource Center, http://www.idtheftcenter.org/.

and information security policy, drawn from published research and extensive experience with data breaches, breach notices, and information security more broadly. The Centre is a member-driven organization that operates within the privacy and information management practice at Hunton & Williams LLP. Through collaboration with industry leaders, consumer organizations and government representatives, the Centre provides leadership in developing policy to help ensure privacy and information security while balancing economic and societal needs and interests in today's global information age.[3]

The views expressed herein are those of the authors alone and should not be attributed to any other person or organization.

1. Don't equate data breaches with identity fraud or other consumer harms.

Research suggests that data breaches actually play little role in most identity fraud. Consider the ChoicePoint breach. The frenzy of state breach laws was fueled by the disclosure in early 2005 that thieves had deliberately targeted sensitive personal data on 163,000 individuals held by ChoicePoint. The FTC imposed a $10 million fine and required the company to establish a $5 million restitution fund—the largest settlement in the Commission's history.[4] In June 2008, more than three years after the breach, the FTC notified ChoicePoint that it had transferred the balance of the $5 million redress fund to the U.S. Treasury after finding that only 131 consumers had presented valid claims for a total of $141,753.[5]

This result is consistent with research showing that the vast majority of breached data is never used to commit fraud. The Government Accountability Office (GAO) reported in summer 2007 that of the 24 largest data breaches publicly reported in the United States between January 2000 and June 2005, in only three was there evidence of any resulting misuse of an existing account, and in only one was there any evidence of what the FTC calls "true" identity theft.[6]

The 2009 Javelin Identity Fraud Survey shows that of the 35 percent of self-identified identity fraud victims who said they knew how their information was compromised, data breaches accounted for only one in ten (11 percent), substantially less than other causes, such as lost or stolen wallet or checkbook (43 percent).[7]

The consistent research concerning the link between data breaches and identity frauds suggests that data breaches should not be equated with harm to consumers.

[3] This paper, related resources, and additional information about the Centre are available at www.informationpolicycentre.com.

[4] Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, Press Release, Jan. 26, 2006.

[5] Email to F. Cate from Tina Snow, Assistant Chief Privacy Officer, ChoicePoint, June 11, 2008.

[6] U.S. Government Accountability Office, *Report to Congressional Requesters, Personal Information* (GAO-07-737) (2007).

[7] Javelin Strategy & Research, *2009 Identity Fraud Survey Report* at 46.

2. Don't become so preoccupied on data breaches that you lose sight of other, far more serious, security risks.

The variety and complexity of technological tools used by information thieves are astounding: rootkits that take control of individual systems; botnets that connect compromised machines to work in tandem stealing data or attacking servers; wireless communication interception and diversion; domain name server attacks that divert unwitting users to fraudulent websites and steal online information; and dozens of other measures. Industry and individuals spend billions of dollars each year combating spyware, which steals more sensitive data than have been revealed by all reported security breaches combined. Socially engineered attacks such as "phishing" are expanding and proving increasingly effective at persuading individuals to part with their own sensitive data. Seven in ten U.S. internet users say they have been fooled by phishing messages.[8] Corrupt components have been found in wireless routers and cable modems, the vast majority of which are made outside of the United States. Malicious code generally, such as viruses and worms, is expanding in number, severity, and variety of platforms attacked. Security breaches affect fewer people and pose less significant risks than many other attacks.

In the limited area of identity frauds, which are not the primary risk posed by security threats, the Javelin survey suggests that even when data breaches result in identity fraud, they impose far lower costs than fraud resulting from other activities that have attracted less attention from legislators. According to the 35 percent of identity fraud victims who responded that they knew how their information was compromised, frauds attributed to a lost or stolen wallet or checkbook resulted in losses more than three times greater than those attributed to data breaches. Frauds attributed to data taken by friends, family members, or in-home employees were both more frequent than those linked to breached data and resulted in losses more than five times higher.[9]

3. Don't count the cost of poor security just in economic harm to individual consumers or businesses.

We increasingly depend on information and information networks in every area of our society. Because of that dependence and interconnectedness, security compromises threaten not just individual consumers and businesses, but our entire economy and even our national security.

According to the SANS Institute, cybercriminals used technological attacks to extort "hundreds of millions of dollars from multiple critical infrastructure companies" in recent years.[10] In January 2008, the CIA issued a rare public warning that attackers had broken into the computer networks of utility companies and then made demands, in at least one case causing a power outage affecting "multiple cities."[11] One year later the FBI identified cybersecurity risks as "the most critical threat we face . . . [o]ther than a nuclear device or some other type of destructive weapon."[12]

General James Cartwright, USMC, former head of the U.S. Strategic Command and current Vice Chairman of the Joint Chiefs of Staff, testified before Congress last year that "America is under

[8] America Online & National Cyber Security Alliance, *Online Safety Study* (2005).

[9] Javelin Strategy & Research, supra at 49.

[10] Andy Greenberg, "Congress Alarmed at Cyber-Vulnerability of Power Grid," *Forbes*, May 22, 2008.

[11] Ellen Nakashima & Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *Washington Post*, Jan. 19, 2008, at A4.

[12] "US security experts fear 'cybergeddon'," ABC Premium News (Australia), Jan. 7, 2009.

widespread attack in cyberspace. . . . Unlike the air, land and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battle space."[13] In the face of such aggressive, sophisticated, and costly information security attacks, breaches appear comparatively insignificant and breach notices seem a paltry response.

4. Don't trivialize breach notices by requiring them when there is no reasonable risk of harm.

Most security breach laws define the term "breach" so broadly that they require notices even when there is no risk or nothing individuals can do to guard against risk. So when devices or media on which personal information is stored (e.g., laptops, optical disks, and USB drives) are lost or stolen, as they inevitably often are, U.S. laws require that notice be sent even though individuals are not at appreciable risk.

Many of the largest "breaches" reported to date turn out not to involve access to data at all. For example, the May 2005 theft from a Department of Veterans Affairs' employee's home of the laptop containing Social Security Numbers and birthdates for 26.5 million veterans and active-duty military personnel constitutes the largest public sector data breach in U.S. history. It triggered months of press attention, led to the notification of all 26.5 million individuals and the firing or disciplining of numerous employees, and it cost the government millions of dollars. But when the laptop was recovered two months later, the FBI reported that the data had never been accessed. The thieves had stolen the laptop for the laptop, not for the data it contained.[14]

Similarly, that same month a box containing four back-up tapes of data about millions of CitiFinancial customers disappeared while being shipped via UPS. At the time, the loss of the box was heralded by the press as the United States' largest private-sector security breach, and CitiFinancial provided notice and credit monitoring services to every individual with data on one of the four missing tapes. The tapes have never been recovered. There has been no higher than normal incident of identity theft involving the individuals whose data was on the tapes. In fact, there is no evidence that any of the data on them was ever accessed by anyone. Rather, the box containing them is just another of the thousands of packages lost each year while in transit. Because the tapes contained personal data, the loss of the box in which they were being shipped constitutes a "breach" under U.S. law.

The misdelivery of mail, faxes, and email similarly has been regarded as breaches, even in the absence of evidence that the personal data they contain was accessed by anyone. Requiring notices in these similar situations invites the public to worry without cause and causes the public to ignore notices, thereby diminishing their utility when they really are needed. Moreover, the financial and reputational costs of these unnecessary breach notifications can be significant. Not all breaches are the same, and the sending of notices is, as the United Kingdom Information Commissioner has recently written, "not an end in itself."[15]

---

[13] Peter Brookes, "The cyber challenge; Cyber attacks are growing in number and sophistication," *Armed Forces Journal*, Mar. 2008, at 10.

[14] See Fred H. Cate, "The Identity Theft Scare," *Washington Post*, Oct. 14, 2006, at A21.

[15] Information Commissioner's Office [of the United Kingdom], Guidance on Data Security Breach Management 3 (Mar. 27, 2008).

5. Don't go it alone.

Information security is a global issue. Just as the Internet and other information networks cross borders without regard for national and provincial boundaries, so too do security threats and vulnerabilities. Viruses, worms, phishing, stolen data—all routinely cross borders. Attacks are deliberately launched across borders to take advantage of safe haven rogue states and the difficulties in cross-border law enforcement.

Any effort to deal effectively with security threats will necessarily have to be multinational in scope, which makes it even more ironic that breach laws in the United States are enacted at the state level. Concerted multinational action is necessary to arrest and prosecute perpetrators and to isolate countries that may harbor them.

Multinational action is also necessary to harmonize security regulations, so that data are protected appropriately and individuals' rights remain substantially the same irrespective of where the data happen to be located. Harmonization is also necessary to facilitate efficient and effective compliance. There is a great deal to be learned from the experience of other nations.

6. Do take data security seriously.

The flurry of state breach laws suggests how weak the government's response to the problem of information security has been. Federal regulation of the private sector has been limited to specific sectors, and even there has been amorphous. The government's own cybersecurity has been repeatedly criticized by congressional oversight committees and the GAO. Promised investment in information security research by the Department of Homeland Security (DHS) has not materialized and key positions have gone empty. The government has invested very few resources in enhancing information security, and even the much-touted increase in funding promised by the Obama Administration still amounts to the same federal investment scheduled for FY2010 that we currently spend in Iraq in a day—a surprising comparison given how greatly national security officials believe cyberattacks threaten our national interests.

The critique Bruce Berkowitz and Robert Hahn first applied to national cybersecurity policy in 2003 remains equally valid today: the government's approach "lacks at least three features taken for granted in most other areas of public policy. This may be the most fundamental shortcoming of U.S. policy for cyber security up to now."[16] "First," they argue, there has been no realistic "assessment of the threat." That may be beginning today with the Obama Administration's 60-day review of cybersecurity, but 60 days is only a first step to make up for a decade of comparative inattention. "Second, the strategy lacks a clear link between objectives and incentives." And finally, Berkowitz and Hahn conclude, "the strategy rejects regulation, government standards, and use of liability laws to improve cyber security *in toto*." Given the magnitude of the risk, federal policy might still best be described as too little, too late.

[16] Bruce Berkowitz & Robert Hahn, Cyber Security: Who's Watching the Store?, AEI-Brookings Joint Center for Regulatory Studies, Regulatory Analysis 03-5, at 6 (2003).

7. Do create incentives for good behavior.

While it is almost always preferable to allow markets to create appropriate incentives for desired behaviors, there are occasions where government intervention is necessary. Information security is one of those instances. The threats are too broad, the actors too numerous, the knowledge levels too unequal, the risks too easy to avoid internalizing, the free-rider problem too prevalent, and the stakes too great to believe that markets alone will be adequate to create the right incentives or outcomes.

Unsecured computers and networks, as well as unsecured data, threaten us all, yet individuals connect to broadband networks and install home wireless routers with no security and little awareness of how to provide adequate security or the importance of doing so. They visit unsecured websites, download suspect files (even installing peer-to-peer software to facilitate doing so and also providing the world with unhindered access to our machines), share passwords, fail to install or update antivirus software, connect to insecure wireless networks, and install unverified programs and equipment in our homes and offices, often in violation of corporate policies.

Meanwhile, few institutions adequately value the cost of lost or missing data, unless it concerns their own trade secrets or proprietary information. Too many businesses sell digital products and services that are not secure, and use personal information in ways that make it vulnerable to error and abuse. When appropriate security is provided it is often through means so complex or so cumbersome that they baffle consumers and frustrate individuals' efforts to secure data and systems. While cyber attacks are growing increasingly sophisticated and malicious, many of the most successful take advantage of our simple failure to do the things that individuals and institutions know they should to protect themselves. Clearly, better incentives are necessary. Where markets fail to produce appropriate incentives, we usually look to law, yet, as Berkowitz and Hahn observe, the government has largely rejected "regulation, government standards, and use of liability laws to improve cyber security *in toto*. These are all basic building blocks of most public policies designed to shape public behavior, so one must wonder why they are avoided like a deadly virus (so to speak)." Without more appropriate standards and oversight, we will never achieve the broad accountability that effective cybersecurity requires.

8. Do collaborate to succeed.

The perpetrators of information security attacks are getting more organized and more efficient. They are increasingly specializing, and using the Web to distribute both the tools to commit cybercrimes and the proceeds. Names, credit card numbers and Social Security Numbers can be purchased online in lots of 100 or 1,000. As evidence of the increasing specialization and mass availability of malicious software, consider that 42 percent of phishing websites observed in the first half of 2007 originated from just three phishing toolkits.[17] Organized crime, terrorist organizations, and even state-sponsored groups are increasingly responsible for today's most insidious attacks.

Yet the response has not kept up with the sophistication and efficient organization of these attacks. The U.S. lacks good data on the frequency and severity of attacks. Organizations that successfully fend off an attack are not required to notify similarly situated entities, even though evidence shows

[17] Stefanie Hoffman, "Storm Warning," *Varbusiness*, Jan. 28, 2008, at 32.

that attacks driven off from one site just move to a less well protected similar site. Customers receive billions of notices, but there is neither centralized reporting nationally (much less globally) of attacks and attack strategies, nor is there broad-based collaboration to identify and repel attackers.

The government needs to facilitate the information-sharing and collaboration necessary to enhance security effectively. At minimum this means reducing barriers to collaboration wherever they occur, but it probably also requires mandatory reporting to the government or some other central clearinghouse of threats. The sector-specific Information Sharing and Analysis Centers created, but never funded, by DHS could serve as a useful model, but they need to be expanded and invigorated.

9. Do anticipate, don't just react to, threats.

Security often tends to be backwards-looking, responding to the most recently deployed threat. To a certain degree that is inevitable, but to succeed we need to not only reduce the time between attack and response, but where possible anticipate and counter attacks even before they are witnessed.

Enhanced collaboration is an important step. Funding research is another. More than just more resources, however, the government needs to focus those resources more wisely to identify potential new attacks, prioritize them based on their likelihood of developing and the damage they might cause if successful, and then deploy countermeasures.

Getting ahead of the curve is critical to protecting data, individuals, and our broader economic and social interests. To be blunt, cyber attacks have simply been too easy. It is time for government to lead a concerted effort to raise the stakes.

10. Do be realistic.

Information security has been dominated in recent years by a sense of unreality. Businesses make unrealistic promises in an effort to attract consumers or sell security solutions. State and federal agencies have been preoccupied with breach notices to the extent that they feel like a solution in search of a problem. Politicians have made bold statements about the importance of data security, while appropriating a pittance to fund a herculean task. Meanwhile data breaches continue apparently out of control, suggesting that even if they are not the direct cause of broad harm to individuals and the economy, they are at least a symptom of a larger scale problem with institutions being stewards of data rather than merely possessors of it. And individuals behave with an almost breathless irresponsibility towards the security of their own and other's data and systems, largely insulated from the practical effects of their carelessness by laws and competitive businesses practices that shift financial responsibility to banks and retailers.

It is time we develop a more realistic view of information security threats and of the steps and resources necessary to combat them. And it is time we develop more realistic expectations. In a very real sense, society is in an arms race against security threats. It is a race that we realistically cannot win—there will always be lost and stolen data; there will always be new threats—but that we cannot afford to lose. Staying in the race will require substantial investment, constant reevaluation of tactics and strategies, and sustained commitment.