A Brief Survey of Current and Future Developments in Privacy, Data Protection and Cyber Security Law

By Patrick X. Fowler, Partner, Snell & Wilmer LLP

The challenges confronting corporate counsel regarding privacy, data protection and cyber security have never been more daunting: dealing with the threat of increasingly sophisticated cybercriminals, responding to data breach incidents, keeping up with a myriad of evolving national and international laws, regulations and industry standards, all while wondering if your data has been targeted by a government surveillance program.

And they're not letting up in 2014. New online privacy laws in California already went into effect on January 1. In February, the federal government is expected to publish a new "cybersecurity framework" for critical infrastructure in the U.S., and that framework, like it or not, may well set a future *de facto* standard of care for establishing liability. In addition, in response to the massive retail customer data breach that occurred late last year, Congress may finally pass a national personal data privacy and security law.

I. Data Breaches, Cyber-Crimes and Data Center Outages: By the Numbers

A. The High Cost of Fending Off the Barbarians at the Gate, as well as Those Already Inside the Walls

When it comes to data breaches, no one is immune. Organizations of all shape and sizes, from government agencies to internet startups, retail brands to respected financial institutions have reported major data breaches in the past year. According to figures kept by the Open Security Foundation, there were 1,390 data breach events reported in 2013.[1] One study found that 41% of US data breaches were due to malicious or criminal attacks, with 33% caused by human factors (negligence) and 26% from system failures or glitches.[2]

Smaller companies no longer operate under the hackers' radar. In 2012, 50% of all targeted cyber-attacks were aimed at businesses with fewer than 2,500 employees, and *the largest growth area for targeted attacks was businesses with fewer than 250 employees:* 31% of all attacks targeted them.[3] Applying the time-tested strategy of following the path of least resistance, attackers thwarted by a large company's defenses will try instead to breach the lesser defenses of a small business that has a relationship with (and perhaps easier electronic access to) the attacker's ultimate target.

Perhaps more troubling is how long it took to spot the breaches. Verizon noted in its 2013 study that *66% of breaches took months or years to discover*.[4] The median number of days between the breach and its discovery was 243 days, or about eight months (which was actually a marked improvement over the prior year).[5] And when the breaches were finally detected, 63% of the discoveries were made by someone *outside the organization*.[6]

The average organizational cost of a data breach was $5.4 million.[7] This included detection and escalation costs ($395,000), notification costs ($565,000), post-breach costs ($1.4 million) and lost business costs ($3.03 million).[8] When viewed in a "per capita" context, the average per record cost of a data breach in 2012 was $194, as compared to $188 per record in 2011.[9]

B. Cyber-Crimes Apparently Do Pay

While cyber-crimes comprise just one slice of the data breach pie, it is a huge portion. The annual cost of cyber-crime and cyber-espionage to the U.S. is as much as $100 billion.[10] The reported average cost to resolve a single successful cyber-attack (one that results in the infiltration of a company's core networks or enterprise systems) ranges from $300,000[11] to more than $1 million,[12] with an average annualized cost of cyber-crimes to be more than $11.5 million.[13] The average time to resolve a cyber-attack was 32 days in 2012 (as opposed to 24 days in 2011).[14] However, malicious insider attacks can take more than 65 days to contain.[15] Moreover, with the recent emergence of so-called "ransomware" such as CryptoLocker (malware that encrypts user data and holds it for ransom[16]), the threat of cyber-crime is not likely to diminish.

C. When the Power Goes Out: The Cost of Data Center Outages

Aside from data breaches and cyber-crimes, companies that rely on remote data centers for web hosting, data processing and/or information storage (i.e., cloud computing) can suffer significant losses when the data center goes off-line, even temporarily. In 2013, the average cost of an unplanned data center outage was reported to be slightly more than $7,900 per minute, a 41% increase from 2010. The average reported outage length was 86 minutes, resulting in an average cost per outage of approximately $690,000 (compared to 97 minutes and $505,000 in 2010).[18]

---

[1] Open Security Foundation / DataLossDB.org http://datalossdb.org/statistics

[2] Ponemon Institute "2013 Cost of Data Breach Study: Global Analysis", May 2013

[3] Symantec Corporation, "Internet Security Threat Report", Vol. 18, April 2013 http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[4] Verizon, 2013 Data Breach Investigations Report

[5] Mandiant, M-Trends 2013: Attack the Security Gap, March 2013 https://www.mandiant.com/resources/mandiant-reports/

[6] Id.

[7] Ponemon Institute "2013 Cost of Data Breach Study: Global Analysis", May 2013

[8] Id.

[9] Id.

[10] Center for Strategic and International Studies, "The Economic Impact of Cybercrime and Cyber Espionage." July 2013 http://www.mcafeee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

[11] IBM X-Force 2012 Mid-Year Trend and Risk Report, September 2012

[12] Ponemon Institute "2013 Cost of Cyber Crime Study: United States", October 2013

[13] Id.

[14] Id.

[15] Id.

[16] http://www.pcworld.com/article/2084002/how-to-rescue-your-pc-from-ransomware.html

[17] Ponemon Institute, 2013 Study on Data Center Outages, September 2013

[18] Id.

continued on page 6

continued from page 5

II. A Patchwork of Privacy and Data Breach Notification Laws and Rules

The lack of a comprehensive, uniform set of privacy and data protection laws has been an on-going source of frustration for corporate counsel. The U.S. does not have a national privacy and data protection law — at least not yet. Instead, 46 states, along with several territories, have enacted non-uniform laws that provide various types of protection for personal information. There also exists a hodge-podge of federal laws protecting particular types of records (e.g., health records, school records, financial records).

A. California Continues to Expand the Universe of Privacy Laws

Already in 2014, California has added two new laws to its online privacy protection scheme.[19] Effective January 1, website and mobile application operators must update their privacy policies to disclose how the site responds to so-called "Do Not Track" signals designed to tell websites or mobile applications that the user does not want the website operator to track his or her visit to the site. The law applies to all companies that collect tracking information from California residents, and accordingly applies to companies that do business in California and track California residents, even if the company does not have a physical presence in California. (Notably, California has not mandated that website and mobile application operators actually honor a "Do Not Track" signal — only that the user be provided with a disclosure about how the website will respond to such signal.)

The other addition to California's privacy policy requirements requires website operators to disclose whether third parties may collect personally identifiable information about the user's online activities over time and across different websites.

B. Congress Mulls Several National Privacy and Data Protection Bills

In response to the massive security breach announced by Target late last year, at least three different data protection and breach notification bills have been introduced in the Senate.[20] One such proposal, the Personal Data Privacy and Protection Act of 2014, re-introduced by Sen. Patrick Leahy (D-Vt) for the fifth time, would nationalize data breach notification laws and impose new data protection requirements on businesses that hold personal data on more than 10,000 individuals. Similar bills have been introduced many times in past sessions without success. However, given the confluence of several recent highly publicized events involving aspects of privacy, data breach and cyber security and the alleged lack of consumer protection, the chance for passage of some reactionary federal legislation in this area is greater than in the past several years.

C. The Federal Government's Proposed Cybersecurity Framework for Critical Infrastructure

In February 2013, President Obama issued Executive Order 13636 titled "Improving Critical Infrastructure Cybersecurity"[21] It contained several key features: (1) requiring government entities to share cyber threat information with the private sector, (2) the impact of cybersecurity activities on privacy and civil liberties must be assessed, and most importantly, (3) the creation of a comprehensive, but voluntary cybersecurity framework for companies involved in critical infrastructure to adopt.

Critical infrastructures have been defined by the federal government as including 16 different "sectors." These are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, material and waste, transportation systems, water and wastewater systems.

The National Institute of Standards and Technology (NIST) (part of the Department of Commerce) was charged with developing this framework within a year. NIST conducted several workshops across the country and before it released the preliminary framework last summer[23], it consulted with more than 3,000 interested parties on best practices for securing IT infrastructure. The final version is expected to be released sometime around February 2014.

Suffice it to say that the potential impact of the framework, once issued, is significant. Given that level of broad input and degree of consultation in creating the framework, at least one commentator has observed that once finalized and released, the framework will be recognized as an industry standard.[24]

While it is intended to be — at least initially — a voluntary program for owners and operators of critical infrastructure, the federal government is already taking steps to encourage adoption of the framework, such as considering changes to the federal acquisition regulations. Additional incentives are being contemplated, such as those involving insurance, possible liability limitations for companies that adopt it, and making adoption a condition for receipt of federal grants. Consequently, companies that work within the critical infrastructure sectors would be wise to review the framework and evaluate their ability to adjust their cyber security policies and practices to meet it.

III. Conclusion

The technical, societal and legal developments in the realm of privacy, data protection and cybersecurity continue to unfold in remarkable and unpredictable ways. Given the pace and significance of these changes, it is essential for companies and their lawyers to keep a close eye on them.

---

[19]http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370&search_keywords=

[20]http://www.bankinfosecurity.com/breach-notice-bills-pile-up-in-senate-a-6398 (January 15, 2014)

[21]http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf 0

[22] http://www.dhs.gov/critical-infrastructure-sectors

[23]http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf

[24]http://www.informationweek.com/government/cybersecurity/nist-cybersecurity-framework-dont-underestimate-it/d/d-id/1112978 (December 9, 2013)