integro

KILPATRICK TOWNSEND

BEYOND BREACHES: GROWING ISSUES IN INFORMATION SECURITY

By Jon Neiditz and David Cox

Some of the biggest threats to information security involve controlling, damaging and interrupting systems, denying access to critical data and destroying data, rather than breaches. Organizations need to make sure that their security strategies and programs – including their insurance coverages – address their biggest threats. In this first installment, we identify some of the threats, including breaches and beyond; in subsequent installments we will look at security and coverage implications in more depth.

1. How Data Breach was Defined

The popular notion of a data breach today was arguably forged by the California Legislature in 2002, when California became for several years the only jurisdiction in the world to require notification of individuals about breaches of some types of their personal information.[1] This innovative law attracted little national attention until three years to the month after that legislation was introduced, when in February of 2005 ChoicePoint announced that it had suffered a breach of the data of 30,000 Californians, and the world soon learned that the only reason Californians were so unlucky was that no other state required notification. Statutes generally modifying – but all fundamentally following – the California model spread like wildfire across the country, and other high-profile breaches followed. Through their similarity and the similarity of the breaches they therefore forced companies to disclose, those statutes arguably reified – constructed and then petrified – what we think of today as a data breach.

Generally, we think of a breach as unauthorized access to or acquisition of unencrypted,[2] notice-triggering personal information that compromises the integrity, confidentiality or security of that information, or causes some type of harm. Breach notification statutes made these types of incidents public, enabled studying their costs and – because they involved personal information and threats of fraud and identity theft – offered valuable warnings to assist victims in protecting themselves, and became good foci for consumer protection initiatives of regulators such as the FTC. Other types of incidents – such as attacks that resulted in theft of data or other assets that were not notice-triggering, or attacks that brought down information systems or made critical data unavailable – received less popular attention.

The information security world, on the other hand, has always been more focused on intrusions, business interruptions and exfiltrations more generally. Organizations' information security programs typically involve levels of seriousness of incidents and responses based on all of those levels. Moreover, both security frameworks and standards such as NIST and corporate security processes have evolved more rapidly than law can generally evolve (wildfire not being the norm); they have moved since the turn of the Century from relatively rigid compliance programs focused on preventive safeguards to more adaptive programs responding to ever-changing risks and focused on detection and response as well as prevention.

Within organizations, the breach response team that includes the legal department (as opposed to the IT security incident response process) is generally only brought in on certain types of incidents, such as incidents when there is unauthorized access to or acquisition of notice-triggering personal information. Trade secrets lawyers, for example, are often not notified when there has been access to critical company secrets, and attacks such as DDOS and ransomware are challenging many compliance-focused breach response processes, because they generally don't involve the exfiltration of personal data.

Meanwhile, given growth of the value of data, including personal data, the metaphor of "data as the new oil" became popular. The visibility of notice-triggering breaches of personal data led to studies of "the

1 S.B. 1386, introduced on February 12, 2002, and becoming effective July 1, 2003.

2 Tennessee has recently received a great deal of attention for requiring notice of breaches of encrypted information, but since Tennessee's statute retains the original California language that a breach is an event that "compromises the security, confidentiality, or integrity" of personal information, and since encryption generally works, the impact of the change is much less than often stated.

cost of data breach."[3] Understandably, given the visibility of personal data breaches, scholars like Professor Dennis Hirsch extended the oil metaphor to the data breach as oil spill.[4] In the next section, we will show that talking about "the cost of data breach" has about as much predictive value for any security incident as talking about "the cost of crime" has for any criminal act: none whatsoever.

2. The Diversity of Security Incidents and Response Strategies

As long as we think of security incidents principally as "spills" of personal data, our security programs and coverages will not offer us the protection we need. Instead, harm associated with security incidents should begin with examination of the many types of incidents and harm now encountered, and the various ways in which those harms are being prevented or avoided. Consider five kinds of data security incidents:

One of the most benign types of data security incident is a credit card breach. If you deal with it in the best way, you get your customers watching, and prevent all of the harm by just getting them to change the numbers at the first sign of any misuse. Whether or not you succeed in preventing fraud and fraud recovery costs, there is a good security regime in place, PCI-DSS, that can extract fines and penalties for noncompliance with that regime, there are legal limits on consumer liability, and there are zero liability policies of the major card brands. This is not to say that companies have not managed to cause some consumer harm in this area, but it was harm that was almost entirely avoidable even after the breach.[5]

A similar type of breach that is not generally notice-triggering is breaches of email addresses. Like credit card breaches, the harm associated with breaches of email addresses can be prevented through effective warnings. Unlike credit card breaches, however, where the consumer is protected by law and by zero-liability policies, the harm associated with email address breaches may be enormous, depending on the circumstances, because email addresses may be used in social engineering attacks, for example, against the critical infrastructure, as discussed below. Preventing harm is harder after an email breach than after a credit card breach because of the effectiveness of phishing attacks, but harm is still avoidable.

Then there is the type of personal information data breach where the harm cannot be prevented through warning. The social security number in the U.S. – our broken system of identity management[6] – is the most frequently cited example. Here the best remedy is monitoring for abuse, and that remedy is not sufficient in preventing either the scope or the duration of the potential harm.[7] So that would be the oil spill, unless the information is not misappropriated or misused, whether as a result of protective actions or due to happenstance.

Commercial espionage involves the theft of "crown jewels," knowledge assets including trade secrets and company-confidential information that may consist of non-personal information such as product design, development and pricing; pre-release financial reports; strategic plans and confidential information about contemplated transactions; source code; or research and development secrets. When it does involve personal information, the information targeted is likely not to be the personal information protected by breach notification laws, but rather, for example, profiles of high-value customers. The harm in these cases may be principally to competitive enterprises, rather than to the individuals whose information is stolen.

Finally, let us consider the many types of security incidents that may harm individuals far more than future threats of fraud or identity theft, and may harm enterprises as well, but do not involve the exfiltration of personal information, notice-triggering or otherwise, or the exfiltration of corporate information. First of all, consider attacks on critical infrastructure areas such as health care or the energy grid, including through ransomware, distributed denial-of-service (DDOS) or other attacks that may bring power or medical systems down in ways that put lives directly and immediately at risk. The current and decreasing centralization of the energy grid has made it a big target for such attacks, but also has permitted the assembly of robust and layered safeguards and detection and response systems. That centralization and those robust systems are less often found in the U.S. health care system, which is now facing new ransomware attacks every week. Yet even though ransomware is clearly the biggest information security threat faced by healthcare providers[8], those providers redundant information security regulatory regimes – from HHS and the FTC – focused principally on the protection of personal information against breach, and the notification

3 See, e.g., http://www.ponemon.org/blog/tag/cost%20of%20data%20breach
4 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393792
5 http://datalaw.net/an-open-letter-to-the-next-four-retailers-to-suffer-big-data-breaches/
6 https://www.teachprivacy.com/ftc-can-readily-halt-identity-theft/
7 http://datalaw.net/why-anthem-is-the-worst-breach-yet-and-how-we-could-protect-everybody-if-we-cared/
8 Indeed, Kaspersky has just pronounced it the top cybersecurity threat generally: http://www.zdnet.com/article/ransomware-is-now-the-top-cybersecurity-threat-warns-kaspersky/

of consumers so that they can protect themselves against breach; there are no notice requirements for consumers regarding ransomware or DDOS attacks, even though by choosing a facility under such an attack you may be subjecting yourself to much greater risks than of a data breach. This is a clear case in which the "oil spill" metaphor is hurting more than it helps.

As noted earlier, ransomware in healthcare may be related to data "spills" insofar as an employee email breach – also not governed by HIPAA, nor is it governed by any but a few state breach notification laws[9] – may be used in the social engineering prior to a ransomware attack. If one looks, on the other hand, at the most threatening security incidents of the present and future, they like ransomware are principally about the control of systems rather than "spills" of personal information. The threats posed to cyber-physical systems in the Internet of Things – connected cars caused to crash, connected medical devices caused to malfunction, attacks by connected buildings – constitute a major area of risk of harm to individuals going forward not necessarily dependent on breaches of personal information. And beyond the IoT, of course, looms the present and future specter of cyberwar and the harms to individuals caused not only by nation states but by private groups and organizations through assuming control of information systems in ways that are immensely harmful to individuals in a multitude of ways having nothing to do with breaches of their personal information.[10]

3. Toward Cyber-Risk Strategies as Diverse as the Risks

This brief exploration of the harms associated with information security incidents demonstrates that, although many such harms are real and undeniable, to argue that there is a generalizable harm or cost to individuals associated with a security incident or data breach is like arguing that there is such a generalizable harm or cost associated with all crimes and torts in the physical world; one could come up with an average cost or even an average type of harm, but it would have absolutely no predictive power with respect to any incident or state of an organization's information security.

Attacks on information systems can cause harms previously caused by natural disasters, invading armies, bank robbers, explosives, murders, thieves, and of course oil spills (the ones that kill marine life as well as the metaphorical ones). Data does not pose one kind of benefit or harm; it poses almost every kind of benefit and harm, and not just in a parallel world but – in part thanks to cyber-physical systems – in the physical world. Yet law and history have narrowed our view of the harms caused by security incidents. Organizations and their insurance advisors have to look beyond these limitations to address organizations' most critical information-related risks.

4. Potential Insurance Coverage Gaps for these Risks

The cyber insurance market, and risk management professionals, have focused on the immediate and obvious losses arising out of data breaches for the past decade, including the first party costs of a breach, and the third party liability for the release of others' information (PHI, PII, payment card information). Such losses are a major concern. However, many cyber policies focus on the popular notion of a data breach, discussed above, to the detriment of risks and losses "beyond breach." Below is a non-exhaustive list of the ways a cyber policy may provide only limited, or no, coverage for such losses:

- Limited or no coverage for a company's loss of revenue arising from reputational harm rather than network interruption;
- Narrow definitions of "privacy" or "security" acts;
- Trade secrets exclusions;
- Limited data asset recovery coverage;
- "Acts of foreign enemies" exclusions; and
- Bodily injury/property damage exclusions.

Evolution of cyber coverage to address losses beyond the standard first party coverage and third party liability coverages generally available in the market will require policyholders and their brokers to be creative in negotiating wording, and possess the requisite specialized knowledge to help carriers become comfortable with their risk profile. It is clear that for the time being, the industry is playing catch-up.

About Integro

Integro is an insurance brokerage and risk management firm. Clients credit Integro's superior technical abilities and creative, collaborative work style for securing superior program results and pricing. The firm's acknowledged capabilities in brokerage, risk analytics and claims are rewriting industry standards for service and quality. Launched in 2005, Integro and its family of specialty insurance and reinsurance companies, some having served clients for more than 150 years, operate from

9 California, North Carolina, Rhode Island and Wyoming, all requiring information such as name to be breached in addition to email address to trigger notice.

10 This point is not principally about China. At least 20 governments now have cyberwar programs.

offices in the United States, Canada, Bermuda and the United Kingdom. Its U.S. headquarter office is located at:

1 State Street Plaza, 9th Floor
New York, NY 10004
877.688.8701
www.integrogroup.com

Kilpatrick Townsend is a leading knowledge asset protection law firm that helps its clients protect their most important information. The firm's Cybersecurity, Privacy & Data Governance Practice takes a comprehensive, multidisciplinary, and integrated approach to helping clients anticipate and obviate information risks, appropriately monetize information, comply with law, and contain and obtain coverage for incidents. Jon Neiditz co-leads the practice, is listed as one of the Best Lawyers in America® in Information Management Law, and blogs at *datalaw.net* and *linkedin.com/in/informationmanagementlaw*.

For more information, contact:
James Sheehan, J.D.
Integro Insurance Brokers
617.531.6865
james.sheehan@integrogroup.com

The content contained herein is not intended as legal, tax or other professional advice. If such advice is needed, consult with a qualified adviser.

CA Lic. #0E77964