wiley

NEWSLETTER

Lessons to Be Learned from the Sony Breach

January 2015

Many data breaches generate significant media attention, but we have never seen the kind of impact from an information security breach that we have from the continuing fallout from the breach involving Sony. We've had national security implications, large-scale international negotiation and sanctions issues, enormous commercial fallout, and widespread personal embarrassment from business activities, all along with the "normal" fallout involving personal data of various kinds. And this situation has not yet ended, and may continue almost indefinitely as data continues to spill out from the hackers (whoever they turn out to be).

So, what are the major lessons from this situation?

All companies have data security risks

Sony isn't a financial services company. It isn't a health care company. And, therefore, it isn't required to meet specific and detailed regulatory requirements for data security involving personal data (yes, I know there are exceptions such as the Massachusetts state law, but work with me on this one). At a minimum, we don't think of Sony as a company that uses large volumes of personal data about its consumers or that faces specific regulatory requirements for data security.

But the fact of the matter is—as this breach shows—that virtually every employer has volumes of data about employees, and, because of the "big data" phenomenon, more and more companies also have detailed facts about clients, consumers, business partners and other individuals. Every company has this information. And all of them are subject to breaches, from a growing variety of causes. The conclusion is that every company that, at a minimum, has employees and/or customers must care about data security, at least from a compliance perspective.

This isn't news—the Federal Trade Commission (FTC) has taken the position for more than a decade that every company with employees or customers has specific data security requirements.[1] It's just that many companies don't listen if there isn't a specific law, often until it is too late.

Even for those companies that don't recognize their risks and obligations for personal data, the Sony breach drives home that there is much more to worry about than protecting personal data. The laws focus on personal data—Congress and the FTC don't (generally) care if companies don't protect their own commercial information. But the Sony breach makes clear that this commercial data is (1) valuable; (2) at risk; and (3) can subject the company to enormous problems, even if "compliance" isn't one of them. For those companies where the threat of an FTC enforcement action isn't enough, the risks related to corporate data—something every company has—should drive this emphasis home even more.

There's "data security" and "cyber security"

One reason that the Sony breach caught so much public attention is because of the national security and diplomatic implications of the breach. These risks—which have little to do with personal data—demonstrate why there is a separate debate building in Congress and elsewhere about "cybersecurity." The data security regime is well established, and continues to expand, but those requirements focus on specific kinds of personal data and the risks to individuals in connection with breaches involving that data.

Cybersecurity, meanwhile, focuses more on the interconnections between companies and systems, and the potential concerns to the country and on a broader basis from cybersecurity attacks. The key provisions of federal law and policy for cybersecurity deal with "critical infrastructure," a broad category of companies that are included by virtue of the role they play in our country. Some of these industries—like health care and financial services–are included in both data security regulatory regimes and cybersecurity. Others (e.g., chemical and power companies) are only (or primarily) affected by cybersecurity. And while cybersecurity focuses on the national security impact of potential cyber-attacks, the Sony attack should push companies on a much broader level to apply strong and effective cybersecurity controls, even where not required by law.[2]

Many information security risks aren't "legal" or compliance related

While Sony may face regulatory action and (already) faces lawsuits from former employees, much of the negative attention for Sony and negative business implications have nothing to do with personal data. All of Sony's proprietary information is at risk. One movie was affected in significant ways, and many others may be affected going forward. Senior executives faced personal and business complications from release of business communications. None of these "injuries" is what either data security laws or cybersecurity principles are designed to address. Yet, these are an important reminder of how important it is to protect technology infrastructures, even without facing any regulatory or enforcement pressure.

The compliance risks also matter

Most of the attention to security breaches in recent years has involved personal data—credit cards, Social Security numbers, or medical information that can cause specific financial or other harms to individuals. While there is no reason to think that this attack on Sony was driven by this personal data, the personal information clearly is affected, and a large number of employees (and perhaps consumers) face potential harms as a result of the attack. Already, Sony faces a lawsuit from former employees. Other suits may follow. We can expect various investigations, some of which may focus on personal data. While it is not clear that Sony violated current information security standards, there have been various reports that Sony ignored earlier evaluations of their information security framework. This situation is a reminder of the importance of constant vigilance on information security, and the critical need to fix problems that have been identified. A failure to fix problems both exposes the company to actual risk of a breach, but also makes the impact from these follow-on legal claims much riskier.

Think about all the places your data is

Unlike most breaches, which tend to impact specific data or particular components of a company's operations, the Sony breach is striking by its vastness. From media reports, there seems to be no part of the Sony information technology structure that was not affected. In that sense, this is not a typical case. But it should drive home for all companies the need to think about what data you have and where you keep it. Data obviously falls into many categories, including (at least) proprietary information, internal communications, customer data, and employee data. Each of these categories (and any others) has their own reasons for data being collected and stored, and often fits into company systems in different ways. Companies need to pay close attention to a variety of issues that impact how a potential breach can affect a company—by restricting access to various categories of data, by effective retention policies that restrict how long data is kept (note that the lawsuit that has been filed by employees is in fact by former employees), and in how many places data is stored and retained. It is always important to review traditionally sensitive pieces of information (such as employee Social Security numbers or customers' credit card numbers), and minimize as much as possible the places in a company where these data elements are kept. In my experience, I always find that companies, for example, have Social Security numbers about employees in a large number of places where there is no reason for the numbers to be there. Review your data carefully, and take steps now to restrict how a breach could affect you.

Learn from the mistakes of others

Every security breach connects to some root cause. It might be hackers, malware, insider problems, lost equipment, or otherwise. The true cause of the Sony attack is not yet clear, and may not ever be. But, every breach provides an opportunity for other companies to learn from the problems and/or failings of others. When you see reports of a security beach problem, think about what happened, and how that issue could arise at your company. Reading about lots of stolen laptops? Then make sure that your company's employees know how to protect their laptops, are taught to reduce the information on them, and evaluate the now-typical approach of encrypting all laptops that contain sensitive data. Did your company face a loss of data because of malware sent through a fraudulent e-mail? Then train your employees better on these issues and implement better controls on these emails and the resulting harm. These breaches are a roadmap to how you best can protect your own company, and provide a partial framework for the ongoing need to re-evaluate security controls on an ongoing basis.

Don't forget the insider risk

While the major focus of attention on the Sony breach has involved the alleged role of North Korea, there are lingering reports that the breach was caused by a disgruntled group of former employees. Whether this is true or not (or there is some other cause), this breach should serve as an important reminder of one of the most common sources of security breaches—action by insiders. Many of these “insider” breaches involve behavioral flaws—sloppy activity, a failure to recognize spoofing or other problem e-mails, loss of equipment, etc., which are mainly addressed through better training and smarter controls. In addition, we are seeing frequent and widespread problems where insiders with appropriate access to data are misusing that access for improper and often illegal purposes. We are seeing this problem arise from "lower level" employees (customer service reps, for example), who need access to perform their jobs but then misuse it. We are seeing more sophisticated breaches resulting from technical employees who have broad access to a wide range of data. These breaches can involve personal attacks on individuals, identity theft, health care fraud, and a wide range of other harms perpetrated by insiders. This is a real problem that exists in virtually every industry. Your company must have a plan for addressing these insider threats. This plan must involve (1) better controls on access; (2) education and training on appropriate use of information; (3) an effective employee sanction policy (employees must know that they will be sanctioned for these improper activities) and a real means of policing how employees are accessing data, through audit trails and the like. This problem exists and it creates realistic threats for all companies.

Conclusions

Each year, we have a range of security breaches that capture public attention. Last year, it was the Target breach. At the end of the year and carrying over into the beginning of 2015, the Sony breach is our focus. It is not always clear that this attention translates to action for companies who face these risks on an ongoing basis. It is clear that risks from outsiders are growing. It is also clear that there are a broad range of "other" threats that exist in most companies and that can be addressed to reduce risk. Whether driven by compliance concerns or a more general sense of risk management, companies in all industries need to take these threats seriously, and must engage in thoughtful, creative, and aggressive means of developing an effective approach to information security. These threats are not going away, and your risks will grow until you take smart steps to reduce them.

[1] For a discussion of how every company is affected by data security requirements, please see Nahra, "Privacy and Data Security is for Everyone: Common Matters That All Companies Should Address," Bloomberg BNA's Corporate Law & Accountability Report (July 18, 2014), available at http://www.wileyrein.com/publications.cfm?sp=articles&id=9895 .

[2] For a discussion on how these concepts relate to each other, see Nahra, "Mastering Cybersecurity by Learning Data Security," Bloomberg BNA Privacy and Security Law Report (September 9, 2013), available at http://www.wileyrein.com/resources/documents/Nahra_2013Sep9_BNA_Mastering-Cybersecurity.pdf.