The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2015
THURSDAY, JANUARY 8, 2015
An ALM Publication

E-DISCOVERY AND CYBERSECURITY

The Sony Hack: Lessons for Law Firms and Their Clients

BY JANA LANDON

Maksim Kabakou/Fotolia

Have you heard about Sony? Of course you have. The Sony attack has been in the headlines for over a month; new facts about how the hack occurred and the scope of the data that was compromised—and what it contained—are emerging every day.

While it would be easy to write this off as yet another cybercrime incident, this particular event differs from previous headline-grabbing data breaches because it gives us a sketch of what skilled hackers can do when they focus on attacking, not just a particular asset, but an entire company. To recap briefly: According to published reports, a group called the Guardians of Peace (GOP) first made their presence known on the Sony systems Nov. 25. GOP's first message to Sony was: "We already warned you, and this is just a beginning. We continue till our request be met. We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release the data shown below to the world." Over the next few days, Sony learned that the data stolen by GOP included celebrities' information, internal budgets and contract figures. The alleged motive: To stop Sony's scheduled Dec. 25 release of "The Interview," a Judd Apatow movie, the plot line of which centers on the assassination of North Korea's leader, Kim Jong-un.

Although final figures will not be known for some time, most reports are putting Sony's damages north of $100 million, far greater than the average cybersecurity breach, which costs a company approximately $3 to $5 million. This event contains lessons for both firms and clients regarding what the future of a comprehensive data hack looks like in 2015 and what the risks are.

Cybercrime: Not Just for Retailers Anymore

Instead of simply looking for credit card data, Social Security numbers, or some of the other common assets compromised in past data breaches that have made the news (Home Depot, Target and, most recently in December, Staples), this targeted breach grabbed digital assets and threatened to release information that would embarrass the company. On Dec. 1, unreleased Sony Pictures films appeared on various file-sharing sites. Dec. 2 and 3 saw the leak of the salaries of many top executives inside Sony and its financial firm, Deloitte. In the following days, marketing slide decks, celebrity aliases and, of course, emails from Sony Pictures executives, many of them maligning various stars, were leaked to the Internet.

This is in line with a new type of "cyber ransom" that companies large and small are experiencing. For example, on Nov. 2, an Illinois hospital received an anonymous email that contained protected health information of some of its patients. The email sender threatened to release this information to the public if they did not receive a substantial payment from the hospital. Similar attacks may lock up all computer systems at a business and hold them hostage. The new

target may not be credit card numbers, but rather smaller hits on organizations themselves that hackers are counting on being easy targets for exploitation.

Many companies, especially smaller ones and law firms, have not invested in robust security software and protocols because they did not see themselves as targets. In fact, the opposite may be true—banks, retailers and other obvious handlers of consumer data may be harder to hack than smaller companies and law firms, precisely because they know they are targets. Indeed, the business itself may be the asset when one takes into account the real costs associated with business interruption or destruction of data.

Simply put, attorneys should be aware that every business has information that is important to it and that businesses must protect. Law firms in particular should consider themselves prime targets for cyberattacks because they hold information relating to mergers and acquisitions, intellectual property and other valuable assets, not to mention their own client lists, emails, etc. All companies should assume they will be the target of a cyberattack, identify key assets and take sufficient precautions to protect those assets.

Keeping Goodwill and Controlling the Message

Of course, some of the juiciest leaks from the Sony breach have been emails in which executives bad-mouth everyone from Angelina Jolie to President Obama. While they make fantastic fodder for gossip websites and entertainment magazines, they demonstrate that the biggest asset loss may not be data, but instead goodwill from customers and clients. Moreover, in the days following the first indicia of the attack, Sony's PR message has been, in a word, garbled. It has ranged from low-key (stating they were "working diligently" to fix the problem) to reactive (pulling "The Interview" from theaters) to defensive (a strongly worded letter from Sony attorneys to news organizations demanding that they stop publishing information).

This demonstrates something that the tech industry and attorneys have known for a long time: People use work email and their mobile devices to discuss personal matters or observations that they would not want made public. While strong detection and technological intervention are good, not having the embarrassing emails in the first place is even better. Every organization, regardless of size, should have email best practices in place and should engage in top-down training for employees.

Additionally, companies and law firms should consider making—and regularly updating—a robust cyberincident response plan, which should include a public relations/notification component. Any plan should also address who needs to be notified of data breaches (for example, certain states require that individuals be notified within a certain time frame), but also lay out who will be responsible for delivering the message to the public and through which channels these messages should come.

Employee Breach Lawsuits: A New Trend?

Finally, it is not just clients and customers who may take legal action against a company after a data breach. Two class action lawsuits were filed recently in state and federal court by former Sony employees alleging that Sony failed to secure its networks against external attacks and did not take adequate steps to protect employees once the company became aware that employee data was compromised. The cases are *Dukow v. Sony Pictures Entertainment*, No. BC-566884 (Super. Ct. Cal. Cty of Los Angeles, Dec. 16, 2014); and *Corona v. Sony Pictures Entertainment*, (C.D. Cal. Dec. 15, 2014) (No. 14-CV-09600). The *Corona* matter alleges that Sony knew its data systems were at risk and made a business decision to accept the risk of losses, thereby exposing to the hackers over 40,000 records containing sensitive information. Both complaints also allege violations of various state privacy statutes. Importantly, they also cite an April 2011 breach in Sony's PlayStation video game network as a warning flag that Sony's network was vulnerable; therefore, Sony knew or should have known that a breach was possible.

Most state and federal regulations require that organizations use reasonable care when protecting sensitive information. An excellent way for any business to show this is, of course, to have a robust business continuity plan that may include a cyberincident response plan. Organizations may also want to consider obtaining cybersecurity insurance to minimize their exposure in case of a breach; in addition to offering policies, insurers are now offering assessment tools.

Although the consequences of the Sony hack are still unfolding, it is clear that the risks facing organizations—both law firms and their clients—do not look the same as they did a few short years ago. It is important to make sure that your company has a solid script in place to make sure that the next cyber-drama is not yours.

Jana Landon *is counsel in Stradley Ronon Stevens & Young's Philadelphia office and co-founder and chair of the firm's e-discovery team. Her practice focuses on advising lawyers and clients on legal, technical and strategic issues regarding electronic discovery and information governance, as well as representing clients in complex insurance coverage and products liability matters. She can be reached at jlandon@stradley.com or 215-564-8049.*