Westlaw Journal
BANK & LENDER LIABILITY
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 17, ISSUE 6 / AUGUST 1, 2011

Expert Analysis

Once More Into the Breach: Are We Learning Anything?

By Cynthia Larose, Esq.
Mintz Levin Cohn Ferris Glovsky & Popeo

> I'm a guy who doesn't see anything good having come from the Internet. ... [The Internet] created this notion that anyone can have whatever they want at any given time. It's as if the stores on Madison Avenue were open 24 hours a day. They feel entitled. They say, "Give it to me now," and if you don't give it to them for free, they'll steal it.
>
> *–Sony Pictures Entertainment CEO Michael Lynton, May 14, 2009*[1]

How ironic. This comment two years ago by Lynton created a minor firestorm and drove him to post a lengthy rebuttal on The Huffington Post,[2] but at the time, Lynton was referring to content piracy, not data breaches.

Given the events since Sony's massive data breaches in April[3] (and subsequent breaches in May and June), he might as well as have been referring to user information held by Sony and its various properties. As a matter of fact, the Sony Pictures hackers said, "Sony stored over 1 million passwords of its customers in plain text, which means it's just a matter of taking it."[4]

Since the April PlayStation Network breach that exposed more than 100 million user accounts, Sony has been hacked more than 10 times. Sony Europe,[5] Sony BMG Greece,[6] Sony Thailand,[7] Sony Music Japan[8] and Sony Ericsson Canada[9] all suffered some intrusion and compromise of user information.

The most recent was also the most "spectacular."

On June 3, various websites associated with Sony Pictures were attacked by a "hacker team" known as LulzSec[10] and user information was posted to LulzSec's website and announced on Twitter.[11] According to the group, it was able to access more than 1 million user accounts via a database storing the information in clear text.[12]

If misery loves company, Sony executives have been happier of late. A litany of reported data breaches, similar to the Sony hacks, run the gamut from global

financial institutions like Citigroup and the International Monetary Fund to the U.S. Senate, Public Broadcasting Service and, reportedly, the CIA.[13]

The cost of remediating these breaches is into the billions. By May 24, Sony publicly stated that it had already spent $170 million to cover costs that included identity theft insurance for customers, improvements to network security, free access to content, customer support and an investigation into the hacking incidents.[14]

And that is long before the most recent breaches and class-action lawsuits started in the United States and Canada. Multiple suits have been filed in jurisdictions across the United States, and on April 2 a Canadian law firm filed a $1 billion class-action suit against Sony Entertainment and its associated companies.[15]

California plaintiffs' lawyer Ira Rothken filed a motion to consolidate all of the Sony lawsuits in the U.S. District Court for the Northern District of California into one large class-action suit.[16] Proving damages has been challenging in these types of cases in the past, but victims in the Sony suits are seeking payment for the fair market value of their leaked information, assuming that the underground market for such information arguably sets "fair value."

Bad decisions about handling breaches when they are occurring or in the aftermath are often made because of lack of planning.

Even as all of these stories evolve, and new ones emerge (see, for example, the Sega breach most recently[17]), what are the take-away lessons? Computer security is not a problem that can be "solved."

It is a risk-management issue and network security presents risks of doing business in a "connected" world. Approaching data privacy and security from a risk-management perspective shifts the focus from the attempt to find "solutions" to threats that are ever-changing and evolving to those risks that are part of the business operation and that can be managed and mitigated. Risk assessments have long been part of the "best practices" for organizations focused on information security.

For example, the Government Accountability Office published an "Executive Guide on Information Security Management" in 1999 that included "Practices of Leading Organizations."[18] However, too many businesses have not undertaken this straightforward exercise of targeted and focused risk assessments and analysis with respect to their own data-privacy and security operations.

The requirement for a "risk assessment" is popping up in data-protection legislation such as HIPAA/HITECH[19] and the Massachusetts security regulations.[20]

Entities covered by these regulations (such as business associates of health care providers or those with personal information of Massachusetts residents) are required to conduct and document risk assessments tailored to their businesses before imple-menting privacy and security measures consistent with the applicable law.

The failure to appreciate the full dimensions of data privacy and security can lead to poor data-protection management and exposure to unnecessary risks.

Application of basic risk-management foundations — governance, risk management, and compliance — to enterprise data privacy and security must be at the top of the list for any board of directors. Without application of sound risk-assessment principles, a company may make the wrong allocation decisions and spend too much on secu-

rity that is not necessary without addressing the human elements (communications and training) that can pose the greater risk.

Protection of data in all its forms — electronic or paper — should be a business priority. We are still learning many facts about the Sony breach, and further details of the other myriad hack attacks of the last few weeks have yet to be disclosed or uncovered.

Some attacks appear to have been highly sophisticated operations;[21] the Sony Pictures and Sega breaches involved very basic tactics that exposed vulnerabilities that should have been discovered by the attack victim in routine and regular scans of the online operations. Customer data was reportedly stored in clear text, visible to anyone who got beyond rudimentary access control measures.

Companies should determine what information they collect from customers, how long it is stored, whether such storage is necessary, who has access, and whether existing policies and procedures need revising.

Databases with customer data, particularly user IDs, passwords and similar information, should be secured and segregated and preferably encrypted. Data masking is another option and is effective even without encryption.

Companies should be examining their own operations and databases in light of these recent data incidents to determine what information they collect from customers and how that information is stored, how long the information is stored and whether such storage is necessary, who has access, and whether existing policies and procedures need revising.

Data breaches should be included in disaster-response planning — bad decisions about handling breaches when they are occurring or in the aftermath are often made because of lack of planning. If a business uses a cloud service or external Web host, contract language should be included that guarantees accessibility to resources to shut the services down immediately because data — and the leakage of that data — is in someone else's control.

The failure to take action now could be laying the groundwork for a negligence claim in future lawsuits.

NOTES

1 Dave Rosenberg, *Sony Pictures CEO hates the Internet,* CNET News, May 16, 2009.

2 Michael Lynton, *Guardrails for the Internet: Preserving creativity online*, Huffington Post, May 26, 2009.

3 Liana B. Baker & Jim Finkle, *Sony PlayStation suffers massive data breach,* Reuters, Apr. 26, 2011.

4 http://lulzsecurity.com/releases/sownage_PRETENTIOUS%20PRESS%20STATEMENT.txt.

5 David Murphy, *Sony Europe Hacked: 150 Accounts Compromised*, PCMag.com, June 4, 2011.

6 Bianca Bosker, *Sony BMG Site Hack Exposes User Data,* Huffington Post, May 23, 2011.

7 Amy Lee, *Sony Faces New Hacks as PlayStation Network Comes Back Online*, Huffington Post, May 20, 2011.

8 Posting of Chester Wisnieski to Sophos Naked Security blog, http://nakedsecurity.sophos.com/2011/05/24/sony-music-japan-hacked-through-sql-injection-flaw/ (May 24, 2011).

9 *Sony Ericsson Canada Store Hack: 2,000 Names, Emails, Passwords Compromised*, Huffington Post, May 25, 2011.

10 www.lulzsec.com.

11 https://twitter.com/#!/LulzSec/status/76379897790070784.

12 Christine Warren, *Sony Pictures Website Hacked,* Mashable, June 2, 2011.

[13] Posting of Jeremy Simon to Halock Security Labs blog, http://blog.halock.com/blog/pci-compliance/summary-of-recent-data-breaches (June 16, 2011).

[14] Dan Goodin, *PlayStation network breach will cost Sony $171M*, The Register, May 24, 2011.

[15] Press Release, McPhadden Samac Tuovi LLP, Canadian Sony PlayStation Network Class Action (May 2, 2011), *available at* http://www.mcst.ca/LinkClick.aspx?fileticket=RlXFlfrf51k%3d&tabid=463.

[16] *Johns v. Sony Computer Entmt. Am. LLC*, No. 4:11-cv-2063 (N.D. Cal.).

[17] Matthew Schwartz, *Hack Attack Exposes 1.3 Million Sega Accounts,* InformationWeek, June 20, 2011.

[18] http://www.gao.gov/special.pubs/ai00033.pdf.

[19] Breach Notification Interim Final Regulation, 74 Fed. Reg. 42,740 (August 2009).

[20] Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, Mass. Regs. Code tit. 201 § 17.00.

[21] Charles Arthur, *IMF cyber-attack led by hackers seeking 'privileged information,'* The Guardian, June 12, 2011; Larry Dignan, *Lockheed Martin confirms attack, allays concerns for now*, ZDNet, May 29, 2011.

Cynthia Larose is a member of **Mintz Levin Cohn Ferris Glovsky & Popeo**'s corporate and securities section in Boston, chair of the privacy and security practice, and a certified information privacy professional. She was recognized by "Chambers USA: America's Leading Lawyers for Business" as a nation-wide leader in the privacy and data security field, 2010–2011. She represents companies in information, communications and technology, including e-commerce and other electronic transactions, counseling clients through all stages of the "corporate lifecycle."