

What the Sony Cyberattack Can Teach Lawyers About Data Security

By Edward J. McAndrew, Esquire

The late-2014 cyberattack on Sony Pictures Entertainment, Inc. illustrates a growing cyber threat that is much different and perhaps more concerning than the consumer privacy data breaches that have garnered headlines. The Sony attack involved digital espionage and massive data theft relating to some of Sony's most sensitive business and legal matters. The hackers also stole information about the professional and personal dealings of Sony's employees.

What truly distinguishes the Sony attack, though, is that the hackers did not stop at spying and stealing. They used malware to destroy Sony's computer network. They published portions of the stolen data online, in an attempt to threaten, extort, and inflict financial, legal, and reputational injury on Sony and its employees. They threatened to harm Sony employees and their families.

Sony's lawyers were high-value targets in the attack. The hackers stole, and later published online, the emails of Sony's general counsel and other in-house counsel. What was disclosed should be every lawyer's personal data breach nightmare — legal and business strategies for the company, including an "email purge"; discussions about potential litigation against the company; information relating to a sensitive Foreign Corrupt Practices Act investigation; and even the percentages of the legal budget committed to different matters.

The hackers displayed a particular interest in publicizing the Sony lawyers' communications and actions relating to data security. The hackers disclosed that

Sony's general counsel conducted at least one briefing to Sony's Board of Directors about data security issues in June 2014 — putting the Board on actual notice of such matters months before the massive cyberattack. There were also discussions about prior hacking incidents and data breaches at Sony, including the highly publicized 2011 attack on its PlayStation Network that impacted over 77 million users. Sony lawyers advised the company not to disclose some of these past data breaches. The lawyers also discussed the hacking group Anonymous and how to respond to past hacking incidents via social media. Thus, what was put on public display was some portion of the approach taken by Sony, its Board, and its lawyers to data security.

A primary legal and ethical question now is whether Sony and its lawyers made "reasonable efforts" to secure their data. That question may be asked in lawsuits, government investigations, and perhaps bar inquiries. What happened to Sony can happen to any of us, and the question will be the same.

For us, the question would come directly from the Delaware Lawyers' Rules of Professional Conduct. Rule 1.6(c) requires lawyers to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Although this Rule focuses only on client-related information, the data security approach it requires applies equally to securing a lawyer's own data and digital tools.

What is "reasonable" is, of course, often highly fact-specific. Comment 19

to Rule 1.6 lists various factors relevant to whether data security efforts are reasonable, "including, but [] not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or important piece of software excessively difficult to use)." Comment 20 offers similar advice as to client communications.

In 2014, the Commission on Law and Technology published "Leading Practices: Data Security" on its website to assist lawyers on data security issues.¹ The "Leading Practices" are drawn from a variety of sources that have been widely adopted across public and private sectors for businesses of all sizes. Utilizing these "Leading Practices" will enable lawyers — regardless of practice type or organizational size — to engage in the type of risk management process and planning for cyber incidents that is increasingly seen as a "reasonable" approach to cyber threats. The Commission intends to add to its website additional resources that may aid lawyers in undertaking "reasonable efforts" to secure their own and their clients' data from the constantly evolving cyber threat. 

1. Delaware Supreme Court Commission on Law & Technology Website, available at: <http://courts.delaware.gov/declt/datasecurity.stm>.

Ed McAndrew is the Cybercrime Coordinator in the United States Attorney's Office for the District of Delaware and the leader of the Commission on Law and Technology's Data Security Working Group.

Workers' Compensation

Celebrating 25 Years of Excellence

Sponsored by the
Workers' Compensation Section
of the Delaware State Bar Association
and the Industrial Accident Board

Wednesday, May 6, 2015
8:30 a.m. - 5:00 p.m.

Featured Speaker
Professor Lex K. Larson,
Editor in Chief
*Larson's Treatise on
Workers' Compensation*

Chase Center on the Riverfront
815 Justison St., Wilmington, Delaware

6.5 hours CLE credit
including 1.0 hour Enhanced Ethics
for Delaware and Pennsylvania attorneys
6.0 Delaware Insurance Continuing Education
licensee credits (including 1.0 credit hour Ethics)

Visit www.dsba.org for registration information.

Is there a major milestone
in your future, or the
future of your law firm?

An anniversary, a
memorial or a celebration?

Consider a tax deductible
gift to the Delaware Bar
Foundation Endowment
Fund, a gift that will continue
to give to those most in need.



DELAWARE BAR
FOUNDATION

Melissa Flynn
Executive Director
Phone: (302) 658-0773
www.delawarebarfoundation.org

Delaware's Premier Litigation Support Team



Stephen M. Conyers, CPA
Stacey A. Powell, CPA, CFE, CICA
Edward P. Byrnes
William A. Santora, CPA

- Review & Analysis of Documents
- Damage Calculation
- Detailed Expert Report Preparation
- Deposition & Court Testimony
- Rebuttal Reports
- Forensic Accounting



 **Santora CPA Group**
Right, By Your Side

Call 302-737-6200 or toll free 800-347-0116

**Available For Labor & Employment And
Noncompete/Nonsolicit Arbitrations and Mediations**

Sheldon N. Sandler, Esquire
Over 40 years' experience in labor and employment matters

- Fellow, College of Labor & Employment Lawyers
- *Chambers USA* - Senior Statesman
- *The Best Lawyers in America*, Labor & Employment Law, since 1983
- AV Preeminent Rating - LexisNexis Martindale-Hubbell
- The Most Powerful Employment Attorneys in America, Lawdragon 2010
- Delaware Super Lawyers, Employment & Labor
- Who's Who Legal, since 2007
- Past Chairperson - 3rd Circuit Lawyers Advisory Committee



ssandler@ycst.com
302.571.6673

 **YOUNG CONAWAY
STARGATT & TAYLOR, LLP**
Attorneys at Law