The Evolving Cyber Threat to Legal Service Providers

Edward J. McAndrew
Ballard Spahr LLP
Partner, Privacy & Data Security
January 15, 2016
Who Are the Bad Guys?

- Individuals
- Criminal Groups or Organizations
- Nation-state Actors or their Affiliates
What Are Their Objectives?

- **Spying** -- those who steal data collected, created or used by governments or private organizations to gain a competitive strategic, security, financial, or political advantage.

- **Stealing** -- those who engage in illegal cyber-events for monetary gain, such as computer intrusions or internal exfiltration of personal, professional, financial, or proprietary information or intellectual property.

- **Terrorism/Extortion** -- state-sponsored and non-state actors who engage in cyberattacks as a form of, or use digital technology to facilitate, acts of terrorism or to effect organizational or individual behavior.

- **Warfare** -- agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country’s strategic military objectives.

- **Hacktivism** -- individuals or groups who perform cyberattacks for personal, political or other nonmonetary reasons.
Outsiders and Insiders

WANTED BY THE FBI
Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

WEN XINYU  SUN KAILIANG  HUANG ZHENYU

WANG DONG  GU CHUNHUI
Intellectual Property Theft

We are witnessing “the greatest transfer of wealth in history.”

Gen. Keith Alexander, Former NSA Director & Cyber Command Commander
An international hacking ring armed with tens of thousands of corporate secrets pocketed more than $100 million from illicit trades, targeting a core vulnerability of the financial system in one of the digital age's most sprawling insider-trading schemes, federal investigators said Tuesday.

Since 2010, more than 30 hackers and traders across the U.S., Ukraine, Russia and other countries coordinated to steal and profit from more than 150,000 press releases, which were scheduled to be delivered to investors from corporate wire services Business Wire, PR Newswire and Marketwired.
Espionage – Deals and Trade

In the News...

HUFFPOST TECH

Daniel Garrie
Managing Partner

The New York Times

U.S.

Spying by N.S.A. Ally Entangled U.S. Law Firm

By JAMES RISEN and LAURA POITRAS  FEB. 15, 2014

The list of those caught up in the global surveillance net cast by the National Security Agency and its overseas partners, from social media users to foreign heads of state, now includes another entry: American lawyers.
Law Firms as a Major Target

• Mandiant estimated that 80 percent of the 100 largest U.S. law firms were subject to successful data breaches in 2011 alone.

• Law firms are “a very target-rich environment, their IT is generally not up to the level it needs to be, the victims themselves are very reluctant to implement any of the defenses that would work against this sort of thing. . . . it’s pretty much the perfect place to steal data from.” -- Richard Bejtlich, Mandiant Chief Security Officer
Law firms are ill-equipped to defend themselves from the growing risk of cyberattacks.

Firms are “high value targets, with access to information on ‘highly sensitive matters such as mergers and acquisitions and patent applications.’”

Every month it seems another American company reports being a victim of a hacking that results in the theft of internal or customer information. But the legal profession almost never publicly discloses a breach.

The unwillingness of most big United States law firms to discuss or even acknowledge breaches has frustrated law enforcement and corporate clients for several years. That frustration bubbled over in a recent internal report from Citigroup’s cyberintelligence center that warned bank employees of the threat of attacks on the networks and websites of big law firms.

*Due to the reluctance of most law firms to publicly discuss cyberintrusions and the lack of data breach reporting requirements in general in the legal industry, it is not possible to determine whether cyberattacks against law firms have increased in the past decade.*
Law Firm Cyber Incidents
2015 ABA Legal Technology Survey Report

- 15% -- acknowledged breaches
- 30% -- experienced downtime/loss of billables
- 18% -- experienced loss/destruction of data
- 7% -- unauthorized access to non-client data
- 3% -- unauthorized access to client data
- 5% -- notification to clients
Law Firm Cyber Incidents
2015 ABA Legal Technology Survey Report

- 42.4 % -- confirmed virus/malware/spyware infections
- 32.9 % -- denied infections
- 22.7 % -- did not know if infected
- 52 % -- firms of 10-49 lawyers
- 44 % -- solos
Dear Clients,

It is almost a daily occurrence that we read about cyberattacks in the news: the Department of Defense, Sony Pictures, Anthem Blue Cross, Facebook, Gmail and many others. Until now…

Unfortunately, on or around January 25, 2015, our firm was the victim of a single cyberattack…
Alert: July 27, 2015

Members of Bar

The Delaware Supreme Court's Commission On Law and Technology has discussed the recent wire transfer scams affecting the Real Estate Legal Practice in Delaware. In order to avoid Delaware Lawyers from becoming victims of this scam, the Commission is issuing the following directive. This is very important and should be shared with any of your staff who may have involvement in real estate closings:

“In light of the recent computer hacking and scams affecting Delaware real estate settlement practices, it may no longer be reasonable to direct settlement proceeds as a result of computerized instructions via email, text or a website without use of a second means of independent verification.”

Richard K. Herrmann
Kevin F. Brady
Co-Chairs
Delaware Supreme Court Commission on Law and Technology
Cyber Extortion, Harassment, Destruction
Network Destruction and Confidential Data Dissemination

Warning:
We’ve 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 data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM (GMT).
Data Link:
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmplaehw36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip
SONY’S TOP LAWYERS TARGETED FOR ATTACK

Sony GC’s Emails Leaked in Ongoing Hacker Fallout

Sue Reisiger, Corporate Counsel
December 12, 2014 | 3 Comments

Sony’s Hacked Emails a Treasure Trove for Attorney-Client Relations

April 10, 2016 | 0 Comments

Internal emails hacked from Sony Pictures Entertainment (SPE) late last year have been released in database form by WikiLeaks. The document dump reveals frank discussions between the company’s in-house lawyers and outside counsel on everything from legal fees and conflict waivers to pitches for business.

The documents were stolen late last year by hackers that the U.S. government has linked to North Korea, but were not readily searchable online at the time. WikiLeaks—the hacktivist collective that has released troves of classified U.S. government documents in the past—published them online last week, calling them “a treasure trove for anyone interested in the inner workings of the legal world.”

Sony Pictures Entertainment Inc. general counsel Leah Weil reportedly argued against a company policy of saving all emails and in favor of instituting a regular purge. Ironically, she made the argument in one of the many Weil emails hacked and made public by a group calling itself Guardians of the Peace.

Photo by Dan Alto/Stock

Sony Pictures Entertainment Inc.
GENERAL COUNSEL AND OTHER IN-HOUSE COUNSEL’S EMAILS STOLEN.

**LEGAL MATTERS**
- Legal and business strategies for Sony
- “email purge” directive
- Litigation strategy
- FCPA investigation
- Legal budget data
- General Counsel’s Board

**DATA SECURITY MATTERS**
- General counsel’s board briefing on data security prior to attack
- Handling of prior data breaches
- Hacktivist response strategy
Four Major Ethical Questions

• Are lawyers acting competently in their use of technology? -- Rule 1.1

• Are lawyers communicating appropriately about data security? – Rule 1.4

• Are lawyers using “reasonable efforts” to protect the confidentiality of client data? – Rule 1.6(c)

• Are lawyers properly supervising other lawyers and vendors? – Rules 5.1 and 5.3
“Reasonable Precautions”

- “Reasonableness of the Lawyer’s Expectation of Confidentiality”
  - The sensitivity of the information.
  - The extent to which the privacy of the communication is protected by law or by a confidentiality agreement.
  - The use or failure to use special security measures required by client.
  - Client’s informed consent to forgo security measures that would otherwise be required by this Rule.

- 2 Important Caveats on “Reasonableness”
  - Listed factors are non-exclusive.
  - Whether a lawyer has an independent legal duty to comply with state and federal laws governing data security and privacy is “beyond the score of these Rules.”
Reducing Cyber Risk

• Identify
• Protect
• Detect
• Respond
• Recover

* National Institute of Standards and Technology Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity
A Key Concept

• Individualized risk assessments should lead to the design of security and incident response plans that fit each individual’s and legal organization’s risk profile, goals, and budget.
# Delaware Supreme Court Commission on Law & Technology

**Leading Practices:** Data Security

<table>
<thead>
<tr>
<th>Working Group</th>
<th>Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>General Principles of Data Security Planning</td>
</tr>
<tr>
<td>Date of Publication</td>
<td>June 20, 2014</td>
</tr>
<tr>
<td>Version</td>
<td>2.0</td>
</tr>
<tr>
<td>Applicable DLRPC (Rules)</td>
<td>1.1; 1.4, 1.6; 1.9; 1.15, 1.18, 5.1; 5.3</td>
</tr>
</tbody>
</table>

**Summary**

This Leading Practice addresses a lawyer’s ethical obligations relating to data security. This Leading Practice is intended to provide a general overview and approach to data security planning. It should be read in light of other Leading Practices that address particular technology applications or issues.

**Disclaimers**

The purpose of this leading practice is to provide the Delaware Bench & Bar with an understanding of an appropriate manner in which this technology may be used. There may be more appropriate uses; and the leading practice discussed might not be appropriate for a specific purpose. It is up to the individual to use well-reasoned judgment in making that decision. The Commission is not responsible for the consequences of the decision-making process.

---

**General Principles of Data Security Planning**

**Introduction**

Data security is a risk management process undertaken to ensure the confidentiality, integrity and availability of data and information systems. Privacy is an objective of data security, and often a legal and ethical requirement imposed upon lawyers and others who create, transmit and possess confidential or sensitive data. There is no single, correct way to mitigate cyber risk. As pertinent to these Leading Practices, there are two overarching principles of data security. First, individualized risk assessments should lead to the design of a Data Security Plan that fits each lawyer or legal organization’s risk profile, goals, and budget. Second, the Data Security Plan should be reviewed regularly to ensure its continued effectiveness.
Best Practices for Victim Response and Reporting of Cyber Incidents
Version 1.0 (April 2015)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, before an incident occurs.

This “best practices” document was drafted by the Cybersecurity Unit to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident. It reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals’ tactics and tradecraft can thwart recovery. It also incorporates input from private sector companies that have managed cyber incidents. It was drafted with smaller, less well-resourced organizations in mind; however, even larger organizations with more experience in handling cyber incidents may benefit from it.
Client Data Concerns Drive Creation of Law Firm Chief Privacy Role

Mark G. McCreary has taken on that role at Fox Rothschild and discusses some of the trends that are making waves in the space.

Gina Passarella, Legaltech News
September 25, 2015 | 0 Comments

For years, Fox Rothschild partner Mark G. McCreary has been advising the chief privacy officers of his corporate clients on data privacy issues from cyberinsurance to data ownership. Now McCreary is the firm's chief privacy officer, taking on the new role in an effort to better manage how his firm responds to increasing and varied data security requirements from its clients.

McCreary said he views the role as a policy position, providing a centralized location for client questions on data privacy, review of firm technology contracts and reviews of data privacy questions on RFPs or engagement letters. McCreary will also be responsible for reviewing and revising firm security and data policies and for training employees.