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

Intellectual Property Theft

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

Gen. Keith Alexander, Former NSA Director & Cyber Command Commander

IDENTITY THEFT

Data Exploitation

The Washington Post

Hackers who breached corporate wires made millions off insider trading

102

By Drew Harwell August 11 Follow @drewharwell

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.

Most Read Business

Espionage – Deals and Trade

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.

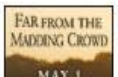
Firms are “high value targets, with access to information on ‘highly sensitive matters such as mergers and acquisitions and patent applications.’”

DealB%k WITH FOUNDER ANDREW ROSS SORKIN

Citigroup Report Chides Law Firms for Silence on Hackings

By MATTHEW GOLDSTEIN MARCH 26, 2015

The Citigroup Center in San Francisco. A study by the bank's cyberintelligence unit recently warned employees of the threat of cyberattacks on big law firms. Justin Sullivan/Getty Images



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

Law Firm Cyber Incidents

2015 ABA Legal Technology Survey Report

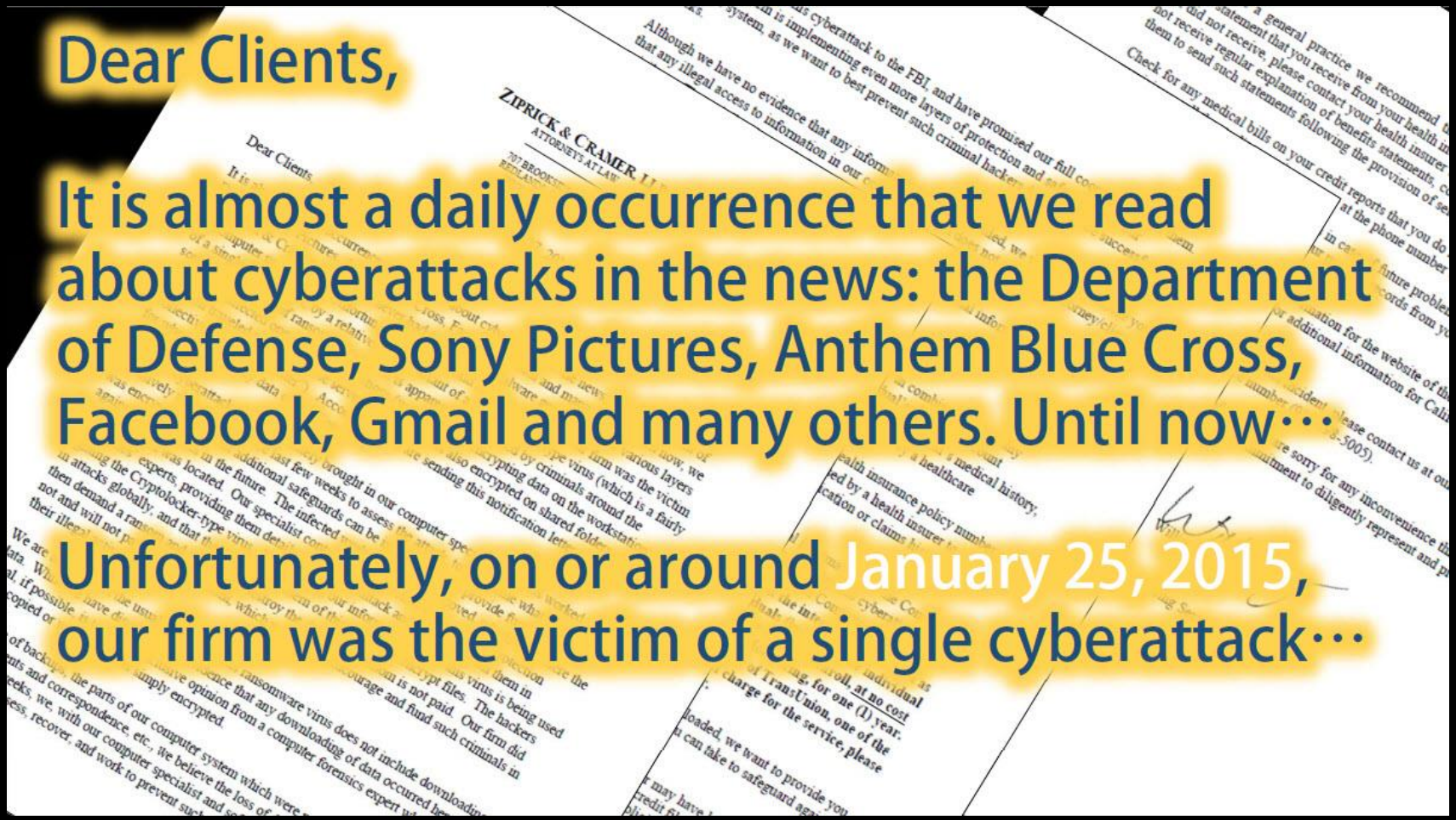
- 15% -- acknowledged breaches
- 30% -- experienced downtime/loss of billables
- 18% -- experienced loss/destruction of data
- 7% -- unauthorized access to non-client data
- 3% -- unauthorized access to client data
- 5% -- notification to clients

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

Law Firm Data Breach Notification



Business Email Compromises

Cyber Extortion, Harassment, Destruction

Network Destruction and Confidential Data Dissemination

SONY'S TOP LAWYERS TARGETED FOR ATTACK

Sony GC's Emails Leaked in Ongoing Hacker Fallout

Sue Reisinger, Corporate Counsel

December 12, 2014 | 3 Comments

SHARE

PRINT

REPRINTS

auris-Fotolia

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

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

Brian Baxter and Nell Gluckman, The Am Law Daily

April 19, 2015 | 0 Comments

SHARE

PRINT

REPRINTS

Photo by Dan Alto/iStock

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

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

ACEDS
ASSOCIATION OF CERTIFIED E-DISCOVERY SPECIALISTS

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.**

ACEDS
ASSOCIATION OF CERTIFIED E-DISCOVERY SPECIALISTS

Commission on Law & Technology Home
Commission Members
Order & Rules
News & Upcoming Events
Blog Spot
FAQs
Helpdesk
Leading Practices
Technology Minute

Delaware Supreme Court Commission on Law & Technology

Leading Practices: Data Security

Working Group	Data Security
Topic	General Principles of Data Security Planning
Date of Publication	June 20, 2014
Version	2.0
Applicable DLRPC (Rules)	1.1; 1.4, 1.6; 1.9; 1.15, 1.18, 5.1; 5.3
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.

Disclaimer: 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

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

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.

Legaltech news

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

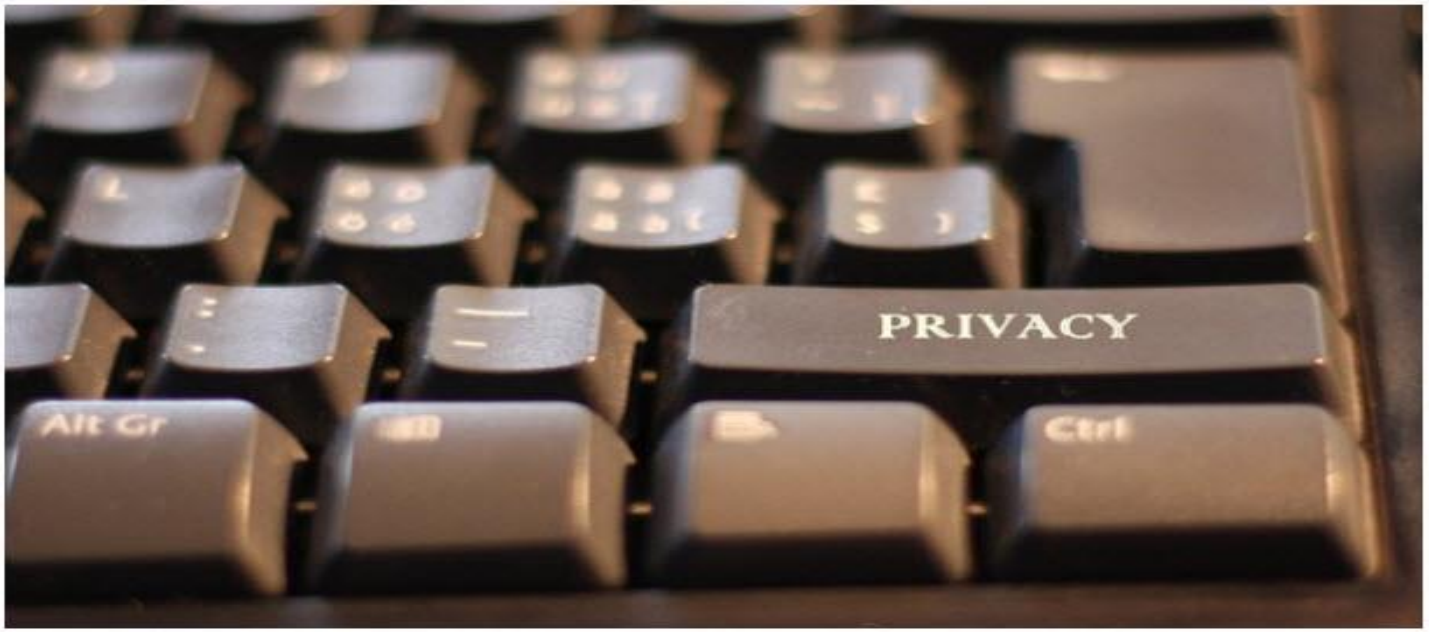


Photo by Sebastien Wiertz, via Flickr

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