

**State Bar of California 19th Annual Ethics Symposium
Thomas Jefferson School of Law
April 25, 2015**

The Net:
Law Firm Cybersecurity

The State Bar of California
Statewide Ethics Symposium

Thomas Jefferson School of Law
San Diego, CA
April 25, 2015

Speakers

- ▶ *Wendy Wen Yun Chang*, Moderator, Advisor, COPRAC; Advisor, Rules Revision Commission; Partner, Hinshaw & Culberston LLP, Los Angeles
- ▶ *Richard Egger*, Member, COPRAC; General Counsel and Partner, Best Best & Kreiger, LLP, Ontario
- ▶ *Tanya L. Forsheit*, Partner, Baker & Hotstetler LLP, Los Angeles
- ▶ *Scott B. Garner*, Chair, COPRAC; Partner, Morgan Lewis & Bockius LLP, Irvine
- ▶ *Wes Hsu*, Chief, Cyber and Intellectual Property Crimes Section, U.S. Attorney's Office - Los Angeles

Cybercrime for Law Firms

» Wes Hsu
Chief, Cyber and Intellectual
Property Crimes Section
U.S. Attorney's Office – Los
Angeles

A Little Bit About Us

What is a CHIP unit?

State Bar of California 19th Annual Ethics Symposium
Thomas Jefferson School of Law
April 25, 2015



“Law firms have tremendous concentrations of really critical private information, and breaking into a firm’s computer system ‘is a really optimal way to obtain economic and personal security information.’”

Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI’s Cyber Division (quoted in ABA Journal, Ed Finkel, Cyberspace Under Siege, Nov 1, 2010).

Which Law Firms Are Targets?

- ▶ Only firms with:
 - Litigation
 - Transactions
 - Sensitive Information
 - Employees

What are the Threat Vectors?

- ▶ Phishing, Spear Phishing, Whaling
 - Not necessarily at the firm!
- ▶ Technically Sophisticated Adversary
 - who is on the other side of your litigation/transaction
- ▶ Hacking for Hire
- ▶ CryptoViral Extortion
- ▶ Compromised Vendors
- ▶ Password Resetting
- ▶ BYOD—where is the perimeter?

State Bar of California 19th Annual Ethics Symposium
Thomas Jefferson School of Law
April 25, 2015

Types of Breach

- ▶ Theft of information
- ▶ Destruction of Infrastructure
- ▶ Blocking access to information

The screenshot shows the ABA Journal website with a dark blue header. The main navigation bar includes 'MAIN', 'BLAWGS', 'SPECIAL', and 'MORE'. A search bar is present with a 'Submit' button. The article title is 'Lawyer who clicked on attachment loses \$289K in hacker scam', posted on Feb 19, 2015. The author is Debra Cassens Weiss. The article text describes a lawyer named John who lost \$289,000 after clicking on a malicious email attachment. A sidebar on the right contains a promotional banner for 'Who's Really Watching Your Firm's 401(k)?' with a phone number and website, and a 'Most Read' list of related articles.

ABA JOURNAL

COMCAST + TIME WARNER CABLE
NET NEUTRALITY FOR MORE PEOPLE LEARN MORE COMCAST

MAIN BLAWGS SPECIAL MORE

Home Daily News Lawyer who clicked on attachment loses \$289K

INTERNET LAW

Lawyer who clicked on attachment loses \$289K in hacker scam

POSTED FEB 19, 2015 06:53 AM CST
BY DEBRA CASSENS WEISS

A lawyer who clicked on an email attachment lost \$289,000 to hackers who likely installed a virus that recorded his keystrokes.

The anonymous lawyer, identified only as John from the San Diego area, told ABC 10 News how it happened.

On Feb. 9, John received an email with an address ending in usps.gov. Thinking he had received a legitimate email from the U.S. Postal Service, he clicked on the attachment.

Hours later, John tried to access his law firm's account with Pacific Premier Bank, the story says. He was transferred to a page asking for his PIN, rather than his usual login, and received a call from a person identifying himself as a bank employee.

The caller said the bank noticed John was having trouble accessing the account and told him to type in his PIN, along with another number, which turned out to be a wire transfer code. Then a page appeared saying the site was down for maintenance.

John received another call from the supposed bank employee two days later. "He asked me to enter the information several times, but told me it wasn't working. He then said I was locked out of my account for 24 hours," John told ABC 10 News. "That's when alarm bells started to go off."

Within hours, John discovered that \$289,000 had been transferred from the account to a Chinese

At the end of the day...
Who's Really Watching Your Firm's 401(k)?

800.826.8901
www.abaretirement.com

ABA Retirement Funds

Most Read Most Commented

- 1 Lawyer who clicked on attachment loses \$289K in hacker scam
- 2 Once rivals, two Minnesota law schools announce plans to merge
- 3 Alvin the dead cat is among many travails that led to blown deadline, lawyer says in court filing
- 4 "Think of my name and sequel": Lawyer admonished for angry email exchange referencing "Deliverance"
- 5 Merging law schools, merging firms: What does it mean?
- 6 Day man refuses to serve on a jury in courthouse where clerk won't perform same-sex weddings
- 7 "Social media blitz" in custody case yields possible suspension for Louisiana lawyer
- 8 Ginsburg offers second reason for

State Bar of California 19th Annual Ethics Symposium

Thomas Jefferson School of Law

April 25, 2015

The screenshot shows a web browser window displaying a Law360 article. The article title is "BigLaw Firm Names Used In Phishing Emails" by Emily Field, dated January 12, 2015. The text discusses how email scammers have used the names of prominent law firms like Reed Smith LLP and Baker & McKenzie LLP to send phishing emails. It mentions that the emails were sent in bulk on January 8 and contained links to malware. The article also notes that the targeted firms included Skadden Arps State Meagher & Flom LLP, Hogan Lovells and Sidley Austin LLP. A quote from a Reed Smith spokeswoman states, "We continue to monitor the situation and will react as warranted." Another quote from a Hogan Lovells spokesman says, "Once aware of this issue, Hogan Lovells immediately notified law enforcement and has been working to have any of the computers associated with the infection attempts removed from the Internet."

The screenshot shows a web browser window displaying a wellivesecurity.com article. The article title is "American law firm admits entire server of legal files fell victim to Cryptolocker" by Rob Waugh, posted on February 10, 2014. The article includes a photograph of a person's hand holding a white USB drive. The text states that a small American law firm has admitted that every document on a server at the Charlotte-Mecklenburg company has fallen prey to the Cryptolocker ransomware. The infection arrived via a phishing email, according to Paul Goodson, who heads the firm in North Carolina state capital Charlotte. The page also features social media sharing options, a search bar, and a sidebar with related articles and a newsletter sign-up form.

State Bar of California 19th Annual Ethics Symposium
Thomas Jefferson School of Law
April 25, 2015

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK)



DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

OK

Anatomy of a Typical (Law Firm) Hack

- ▶ Starts with phishing



Targeted email to individual with control of funds/information

Anatomy of a Typical (Law Firm) Hack

- ▶ Once credentials obtained, exfiltration



What information?
Client Trade Secrets
Negotiation Strategy
Other Credentials?

Breach Response:
Law Enforcement

What Does a Data Breach Look Like?



What Does a Data Breach Look Like (2)?



Before



After

Anatomy of a Law Firm Hack: Immediately After the Data Breach

- ▶ What happens next?
 - Attack connected systems (client?)
 - Destruction/Extortion?
 - Use Stolen Information in Litigation/Transaction
- ▶ What Happened?
 - Nature of breach
 - Take infections offline
 - How widespread was breach
- ▶ Eradicate infection
- ▶ Secure your network, close any doors
- ▶ Restore from backups compromised or stolen information

Reporting to Law Enforcement

- ▶ What does law enforcement need?
 - All log files
 - All employee times spent addressing the attack
 - All other consequential damages
 - Did you hire a remediation firm?
- ▶ When should law enforcement be notified
- ▶ What law enforcement agency should be notified

The Ethical Rules

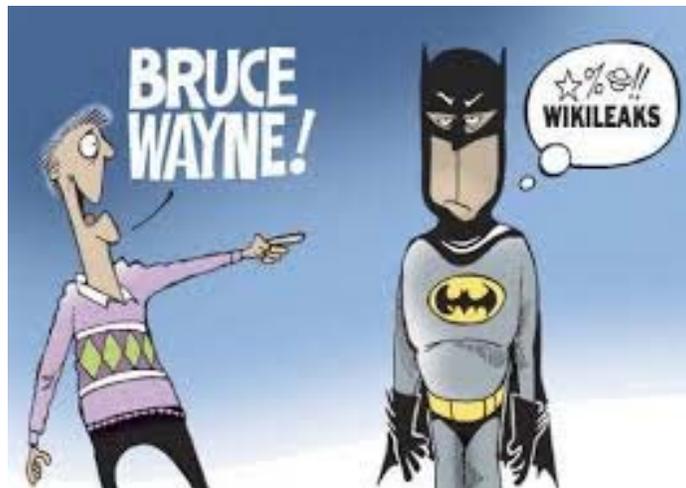
Duty of Competence



Duty of Competence

- ▶ Rule 3-110
 - “(C) If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) professional consulting another lawyer reasonable believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required.”
 - Discussion: “The duties set forth in rule 3-310 include the duty to supervise the work of subordinate attorney and non-attorney employees or agents.”

Duty of Confidentiality



Duty of Confidentiality

- Bus. & Prof. Code § 6068(e)(1): It is the duty of an attorney “[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.”
- Rule 3-100: Member may not reveal information protected by Section 6068(e)(1) without client’s informed consent.
- The duty of confidentiality extends to former clients. *People v. Speedee Oil Change Sys., Inc.*, 20 Cal. 4th 1135, 1147 (1999); *see also* Model Rule 1.6, cmt. [20].

Duties of Competence and Confidentiality – Technology

- Blending of duties of competence and confidentiality
- “[T]he manner in which an attorney acts to safeguard confidential client information is governed by the duty of competence.”
 - Cal. State Bar Formal Opn. No. 2010-179.

Reasonable Precautions



Reasonable Precautions

- Attorney “must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.” (Cal. State Bar Formal Opn. No. 2010-179 (quoting Model Rule 1.6, Cmt. 17).)
- Reasonableness of precautions takes into account “the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.” (Cal. State Bar Formal Opn. No. 2010-179.)

“Reasonable Efforts” under Model Rule .16

- Model Rule 1.6 cmt. [18] lists factors to consider in determining whether the lawyer made reasonable efforts, including:
 - 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).

State Bar Formal Opinion 2010-179

- Factors to consider before using a specific technology:
 - The attorney’s ability to assess the level of security afforded by the technology.
 - Legal ramifications to third parties of intercepting or accessing confidential information.
 - The degree of sensitivity of the information. (The greater the sensitivity, the less risks attorney should take.)
 - Possible impact on the client of an inadvertent disclosure, including possible waiver of privileges.
 - The urgency of the situation.
 - Client instructions and circumstances.

State Bar Formal Opinion 2012-184

- State Bar Opn. 2012-184 discusses factors to consider when selecting a cloud-based vendor:
 - Credentials of vendor.
 - How secure is data.
 - Whether vendor transmits information in the cloud across jurisdictional boundaries.
 - Attorney's ability to supervise vendor.
 - Terms of service with the vendor.

- While 2012-184 is in a VLO setting, its rationale can be applied to give guidance in cloud based vendor selection generally.

Reasonable care is a sliding scale

- ▶ Firm policies and protocols
- ▶ Educate employees
 - Safe and ethical use of technology
 - Avoiding phishing etc.
 - Recognizing signs of intrusion
 - Culture of compliance/management priority
- ▶ Investment in safeguards: employees, software and hardware
- ▶ Monitor your network
- ▶ Encryption
- ▶ VPN

Breach Response: Ethics Rules

Reporting to Law Enforcement?

- ▶ Does the duty of confidentiality permit this absent client consent?

Client Disclosure Obligations Following a Breach



Duty to Communicate

- ▶ Rules of Professional Conduct Rule 3–500
- ▶ A member shall keep a client reasonably informed about significant developments relating to the employment or representation
 - Do you know what happened?
 - Breach vs. "incident"
 - What information was compromised?

*Neel v. Magana, Olney, Levy,
Cathcart & Gelfand*
(1971) 6 Cal.3d 176

Attorneys have fiduciary obligation to disclose material facts to their clients.

Avoiding the Representation of Adverse Interests



Rules of Professional Conduct Rule 3-310(b)

A member shall not accept or continue representation of a client without providing written disclosure to the client where:

- ▶ (1) The member has a legal, business, financial, professional, or personal relationship with a party or witness in the same matter; or . . .
- ▶ (4) The member has or had a legal, business, financial, or professional interest in the subject matter of the representation.

ABA Formal Opinion 08-453

- ▶ Model Rule 1.7 defines a conflict as including a situation where “there is a significant risk that the representation of one or more clients will be materially limited by the lawyer’s responsibilities to another client, a former client or a third person, or by a personal interest of the lawyer.”
- ▶ Opined that “[a] lawyer’s effort to conform her conduct to applicable ethical standards is not an interest that will materially limit the lawyer’s ability to represent the client. . .”

New York State Bar Association Opinion 789 (2005)

- ▶ Clients are entitled to counsel who comply with applicable standards of professional responsibility.
- ▶ Lawyers are entitled to seek advice on how best to comply with those standards.
- ▶ Lawyers are not obligated to tell a client how the lawyers have reached a conclusion concerning professional responsibilities.
- ▶ See also State Bar Formal Opinion 2012-183

Is client consent required for continued representation?



Rules of Professional Conduct Rule 3-310(c)

A member shall not, without the informed written consent of each client:

- (1) Accept representation of more than one client in a matter in which the interests of the clients potentially conflict; or
- (2) Accept or continue representation of more than one client in a matter in which the interests of the clients actually conflict; or
- (3) Represent a client in a matter and at the same time in a separate matter accept as a client a person or entity whose interest in the first matter is adverse to the client in the first matter.

State Bar of California 19th Annual Ethics Symposium
Thomas Jefferson School of Law
April 25, 2015

- ▶ But what about 3-310(b)?
- ▶ How to reconcile the two rules in this setting?
- ▶ And what impact, if any, does the rationale of the in-firm privilege cases have on the question of whether consent is required?
 - Federal In firm cases vs. *Edwards Wildman*

Thelen Reid & Priest v. Marland
(N.D. Cal. 2007) 2007 U.S. Dist.
LEXIS 17482

- ▶ Recognizing that law firms seek advice about their legal and ethical obligations in representing a client, including from their own lawyers
- ▶ Although consultation with an in-house ethics advisor is confidential, the firm should disclose to the client the firm's conclusions with respect to those ethical issues if it concludes the client may have a claim against the firm

ABA Formal Opinion 08-453

“[C]lient consent may be sought only when the firm reasonably believes that one or more lawyers in the firm can provide competent and diligent representation to the client notwithstanding the consulting lawyer’s conflict.”

RFF Family Partnership v. Burns & Levinson LLP (2013)
465 Mass. 702, 991 N.E.2d 1066

“It may not always be clear when the interests of the client and the law firm have become so adverse that withdrawal is required in the absence of client waiver. . . . [A] law firm is not disloyal to a client by seeking legal advice to determine how best to address the potential conflict, regardless of whether the legal advice is given by inhouse counsel or outside counsel.”

*Edwards Wildman Palmer LLP v.
Superior Court*
(2014) 231 Cal. App. 4th 1214

- ▶ Attorney consultation with its in house counsel is protected by the attorney client privilege.
- ▶ Court declined to opine on the ethics questions other than to acknowledge the duty of disclosure to a client of significant development.

Breach Response:
Privacy Laws

State Bar of California 19th Annual Ethics Symposium
Thomas Jefferson School of Law
April 25, 2015

BakerHostetler

The Net: Law Firm Cybersecurity
The State Bar of California
COPRAC
Statewide Ethics Symposium

BAKER & HOSTETLER LLP
Tanya L. Forsheit, Partner

000006700 51

Security and Control

BakerHostetler

- Assess
- Protect
 - Confidentiality
 - Prevent unauthorized access
 - Integrity
 - Prevent unauthorized and unintentional alteration or deletion
 - Availability
 - Maintain availability to authorized users
- Respond

000006700 52

Accountability and Education

BakerHostetler

- Communicate and educate
 - Employees
 - vendors
- Establish goals and measure performance
- Monitor for compliance
- Procedures to address requests, complaints and disputes
- Enforcement and corrective action

600006700

53

Costs of Incident Response

BakerHostetler

- Forensics
- Notification costs
- Credit monitoring
- Call center
- Crisis response
- Legal fees
- Defense costs/settlement expenses
- PCI fines/assessments & regulatory fines

CATEGORY	DESCRIPTION	COSTS
1). Notification Costs	<ul style="list-style-type: none"> • Address list management • Printing, Inserting, Mailing • Post-Mailing Call Services • Returned Mail 	\$2,308,350
2). Credit Monitoring	<ul style="list-style-type: none"> • Flat Fee —\$4 • Redemption — \$15 @15% redemption rate 	AVG: \$5,512,500

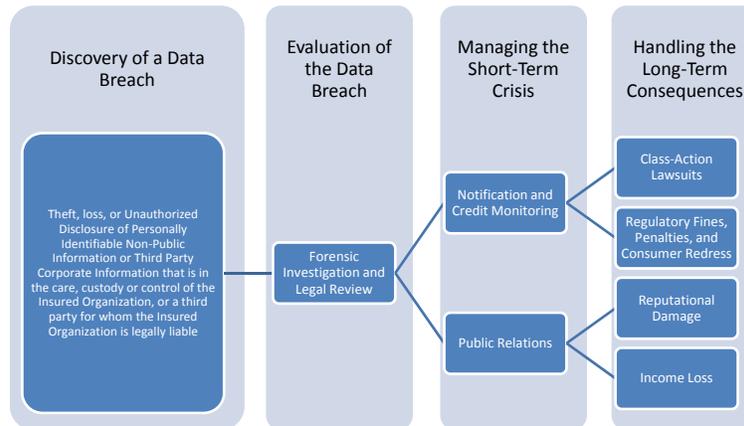
600006700

54

State Bar of California 19th Annual Ethics Symposium
Thomas Jefferson School of Law
April 25, 2015

What Should Happen If There Is a Suspected Security Incident or Breach, and When and How?

BakerHostetler



600006700

55

Notification Laws

BakerHostetler

- 47 states, D.C., & U.S. territories
- HIPAA
- Laws vary between jurisdictions
- Varying levels of enforcement by state attorneys general
- Limited precedent
 - What does “access” mean?
 - What is a reasonable notice time?



600006700

56

Other Challenges

BakerHostetler

- FTC (and FCC?) enforcement priorities
 - Security, deceptive privacy policy statements, mobile applications, big data, US-EU Safe Harbor
 - Recent FCC fines
- State laws
 - Reasonable security & expanding scope of notification laws
 - Active enforcement – State Attorneys General
- Legislative
 - Cybersecurity Framework, White House report

600006700

57

Objectives for a Data Breach Incident Response Plan

BakerHostetler

- **“Living Document”**
 - Routinely updated to keep current
- **Clear and easy to use in the midst of a crisis incident**
 - Succinct
 - Organized by sections
- **Not a “phone book” but not a “leaflet”**
 - Background information on regulations and laws
 - Detailed procedures and steps on incident management
 - Contact details of the Incident Response Team (IRT)
- **Document all discoveries for evidentiary needs**
- **Practice for events**

600006700

58

2014 Global Law Firm Cyber Survey ©Marsh & McLennan Companies

- ▶ 79% surveyed firms in aggregate view cyber/privacy as one of top 10 risks
- ▶ 72% surveyed have not assessed and scaled cost of data breach based on info they retain
- ▶ 41% surveyed have not taken measures to insure against cyber risk and 10% don't know if they have or not
- ▶ 62% surveyed have not calculated effective revenue lost or extra expenses incurred after attack.

Thank you for coming today.

Wendy Wen Yun Chang, wchang@hinshawlaw.com
Richard Egger, Richard.Egger@bbkllaw.com
Tanya Forsheit, tforsheit@bakerlaw.com
Scott B. Garner, sgarner@morganlewis.com
Wes Hsu