Hack This: Cyber Security Practices and Ethical Duties for IP Law Firms

Presented by

Steve Hatch &

Michael E. McCabe Jr., Esq

OM01

9/15/2016

11:00 AM - 12:00 PM

Hack This: Cyber Security Practices and Ethical Duties for IP Law Firms

Steven Hatch

Michael E. McCabe, Jr.

Sept. 15, 2016

Your connection
to knowledge, resources and networking

Objectives

- Understand the law firm cyber threat.
- Identify ethical and legal duties implicated by cyber security breaches.
- Raise awareness of technologies to combat the cyber threat
- Learn what to do if your law firm has been cyber breached.
- Learn about cybersecurity insurance policies for law firms.

The Law Firm Cyber Threat

- The soft underbelly of corporate security
- Untargeted and targeted threats
- Perimeter penetration vs end user computing
  - Malware Payload and/or Social Engineering
    - Ransomware
    - Phishing & Spoofing
    - Whaling
- Too small or obscure to warrant interest of hackers
- Learn of a deal - research & infiltrate the players
- Sharp increase targeting 100 employees and less
- $1B Industry

3

Ethical Duties

- Duty of competence.
- Duty of confidentiality.
- Duty of communication.
- Duty of supervision.
- Duty to others (e.g. opposing parties).
- Compliance with Outside Counsel Guidelines.

4

Duty of Technical Competence

- ABA Model Rule 1.1:
  - Lawyers must provide competent representation.
  - "competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
  - Comment 5 to Model Rule 1.1 explains that competence "includes . . . use of methods and procedures meeting the standards of competent practitioners.

5

Duty of Technical Competence

- ABA Model Rule 1.1 amended in 2012 to impose duty of "technical competence"
- Comment 8 states:
  - "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . ."
- At least 13 states have adopted.

6

Duty of Confidentiality

- "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . ."
  - ABA Model Rule 1.6
- "A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure . . ." ABA Model Rule 1.6, cmt. 16

7

Duty of Communications

- ABA Model Rule 1.4 requires communications with clients "about the means by which client objectives are to be accomplished."
- This includes usage of technology.
- Also imposes duty on lawyer to tell client if confidential information has been breached.

8

Duty of Supervision

- ABA Model Rule 5.1 require partners and supervisory lawyers to ensure that subordinates are practicing ethically.
- ABA Model Rule 5.3 imposes same duties regarding non-lawyer assistants.
- Lawyers may be responsible for ethical breaches of others, even if they were not personally involved.

9

Duty to Third Parties

- Law firms often possess third-party property and confidential information.
- Same ethical duties apply.
- Additional legal duties to third parties and courts.
  - E.g. Maintaining security of opponent's confidential information covered by a court's protective order.

10

Cyber Security Ethics Math

- Competence +
- Confidentiality +
- Communications +
- Supervision +
- Third-Party Rights =
  - Cyber migraine.
  - The new normal.

11

Cyber Security Ethics Takeaways

- Can't just "leave it up to IT."
- Top down commitment.
- Understanding limits on lawyer's competence.
- Get appropriate assistance.
- Continue security awareness.
- Teach, supervise and communicate with client and subordinates.
- Ongoing review of threats and solutions.

12

Ethics in the Cloud Checklist

- Duties of competence, confidentiality and communication apply in the cloud
- Does cloud provider use robust security measures?
  - Verification procedures limiting access to the data; safeguards such as data back-up and restoration, a firewall, or encryption; periodic audits by third parties of the provider's security; and notification procedures in case of a breach.
- Is data stored in a format that renders it retrievable as well as secure?

13

Ethics In the Cloud Checklist (Cont'd)

- Is data stored in a proprietary format and is it promptly and reasonably retrievable by lawyer in a format acceptable to the client?
- Does provider have an enforceable obligation to keep the data confidential?
- Where are the provider's servers located and what are the privacy laws in effect at that location?
- Provider's disaster recovery plan?
  - *See* N.H. Bar Ethics Op. No 2012-13/4

14

Ethics Risk Points Beyond the Cloud

- SmartPhones
- Laptops
- Remote access
- Wireless networks
- USB drives
- Working from home/third-party systems.

15

Contractual Duties - OCG

- Clients may help force change.
- Corporate legal departments, via Outside Counsel Guidelines, including stringent requirements to ensure adequate data privacy, security requirements, and compliance with other legal statutes.
- Law firms that agree to OCG must be sure the requirements are communicated and implemented.
- OCG compliance is a firm issue, not a partner or practice group issue.

16

Cyber Threat Protection

- Leadership awareness
- Cover the basics
  - Anti-Virus, SPAM, Back-up
  - Least user rights
  - Patching & pattern updates
- Intrusion Protection Systems / Perimeter security
- Develop a response plan
- User awareness training
  - Whether in the office or in Moscow

17

Available Countermeasures

- Strong passwords
- Ransomware detection scripts
- Multi-factor authentication
- Mobile device management
- Email hygiene with targeted thread protection
- Microsoft BitLocker / encryption at rest
- Microsoft AppLocker & DeviceGuard
- User training, testing and retraining
- The Cloud

18

What to do if Your Firm Has Been Cyber Breached

- Assess damage.
- Communicate with affected parties.
  - Clients.
  - Courts.
  - Opposing parties.
- Remedial measures.
- Training of staff (legal and non-legal)

19

Cyber Liability Insurance

- What is covered?
  - Terrorism exclusion?
  - Intentional conduct by insiders excluded?
- Recent case:
  - CNA denied claim under policy for the exclusion for "failure to follow minimum required practices" which precludes coverage if the insured does not "continuously implement the procedures and risk controls identified in the Insured's application for this Insurance."

20

Resources and Checklists

- General knowledge – www.sans.org
- User awareness training – www.knowbe4.com
- Email threat protection – www.mimecast.com
- Multi-factor authentication – www.duo.com
- Mobile device management
  - Microsoft Intune – www.Microsoft.com
  - Citrix XenMobile – www.citrix.com

21

Resources and Checklists (Cont'd)

California Data Breach Report - https://oag.ca.gov/breachreport2016

Safe and Secure: Cyber Security Practices for Law Firms (CNA 3/2015) - https://www.cna.com/web/wcm/connect/61aec549-ac28-457b-8626-aa791c782459/Safe_Secure_Cyber_Security_Practices.pdf?MOD=AJPERES

22

Questions?

- Steven Hatch
  - Phone 732.204.7411
  - Email shatch@Helient.com
- Michael E. McCabe, Jr.
  - Phone 410.659.4981
  - Email mmccabe@fblaw.com
  - ***IPethics & INsights*** @ www.IPethicslaw.com

23

Remember

Your opinion matters!

Please take a moment now to evaluate this session.

Thank You!

24