TheSecurityAdvocate

Teaching Cyber Security to Lawyers

Scott Aurnou, Esq., CISSP
CIPP/US, CIPT, FIP

Introduction

- Lawyers and law firms handle and store sensitive data on a regular basis
- Attorneys are prime targets for data theft
- Of course, the threats go beyond data breaches

Agenda

- Why are lawyers different?
- What challenges do they present?
- What will actually engage attorneys?
- A sample slide
- A few helpful resources

Lawyers? So what…

- Mistakes in attorney work product can have severe repercussions
- Lawyers' role in vendor risk management, compliance, privacy, cyber liability insurance, incident response, etc.
- Often responsible for – or at lest oversee – administrative controls (contracts, policies, etc.)
- Can even oversee organizational awareness programs through Compliance Dept or General Counsel's office

Challenges

- Difficult to engage with most common security awareness techniques
  - Why?
- "Typical" attorney experience
- Lawyers vs. law firm staff

Some similarities, but…

- Some of the same rules apply, but…
- Information security is still often viewed as confusing, scary and dull
- Convenience is still the enemy
- Training fatigue most definitely applies

Some differences, too

- Lawyers have a different relationship with regulations (HIPAA, GDPR, GLBA, etc.) than other employees
- Of course, attorneys must comply themselves
- But they are also often tasked with ensuring organizational compliance via policies, procedures, contracts, investigations, audits, etc.

Potential problems

- What can go wrong if lawyers don't get it?
- Potential for organizational & professional liability
  - GDPR, CCPA, DFS/GLBA, state data breach laws
- Beyond the risks of data and/or network compromise presented by other users
  - Attorneys commonly deal with confidential and extremely sensitive data

Stuff that probably won't engage lawyers

- Cartoons
- Posters
- Games
  - Phishing exercises should absolutely be done, but **explain why**
- Cutesy stuff: "Hey Fred, let's go phishing!"
- Gimmicks & swag

Stuff that actually might

- Structure is important
- Take a moment or two actually explain the tech and the dangers related to specific risks (behavioral, technical, compliance, etc.)
  - What is the threat and how will this particular control mitigate that threat?
- Analogies, movies and other pop culture references
- If there's a related law or regulation, mention it
  - Include relevant section/paragraph numbers, if applicable
- Humor can work, but steer clear of slapstick and juvenile humor
  - Charles Sevilla books (*Disorder in the Court*; *Law and Disorder*; *Disorderly Conduct*)

Topical is good

Ethics CLEs

- Every attorney wants more ethics credits
- Model Rules of Professional Conduct
  - Published by the American Bar Association
  - Set a standard of reasonable conduct for attorneys
- With recent technical requirements added to the Model Rules, security can legitimately be taught as an ethics course
  - Must be taught with an attorney to get accreditation

The Model Rules of Professional Conduct

- The ABA updated the Model Rules in 2012 to emphasize lawyers' duties with respect to technological competence.
- Changes pertaining to technology were made in August 2012:
  - Rule 1.1 – Competence
  - Rule 1.6 – Confidentiality of Information
  - Rule 5.3 – Responsibilities Regarding Nonlawyer Assistance
- Not changed in 2012, but still relevant to security:
  - Rule 5.1 – Responsibilities of a Partner or Supervisory Lawyer

Rule 1.1 – Competence

- A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

- **Comment 8**: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.
  - The Report accompanying the change expressly noted:
    - "The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent." ABA Commission on Ethics 20/20, Report to Resolution 105A Revised (2012)

- Adopted by 34 states as of June 2019

Rule 1.6 – Confidentiality of Information

- (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
- ***
- (c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

- **Comment 18**: Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]–[4].

Rule 1.6 – Comment 18 Safe Harbor Provision

- "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure."

- Factors to determine reasonableness of the efforts include (but aren't limited to):
  - Sensitivity of the data
  - Likelihood of disclosure if additional safeguards aren't employed
  - Cost and difficultly of employing additional safeguards
  - Extent to which additional safeguards adversely affect the lawyer's ability to represent clients

- Also specifically notes that the Rules do not supersede Federal or state laws "that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information"
  - Safe harbor won't protect you from state or Federal privacy or post data breach reporting requirements

Rule 1.6 – Comment 19 Electronic Communication re: Client

- "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."

- Safe harbor provision: "This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."

- Factors to determine reasonableness of the expectation of privacy include:
  - Sensitivity of the data
  - Extent to which the privacy of the communication is protected by law or a confidentiality agreement
- A client may give informed consent to a method not otherwise permitted

- **Amended portion:** specifically notes that the Rules do <u>not</u> supersede Federal or state laws that require additional steps to safeguard data privacy

Rule 5.3 – Responsibilities Regarding Nonlawyer Assistance

- With respect to a nonlawyer employed or retained by or associated with a lawyer:

- (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
  - (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
  - (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

- The new Comment 3 expressly references cloud storage services
  - A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.

Rule 5.1 – Responsibilities of a Partner or Supervisory Lawyer

- Not changed in 2012, but still relevant to security

- Paragraph (c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:
  - (1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or
  - (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Sample slide (re: “Insider Threats”)

- The threat effectively begins inside the network, subverting your perimeter defenses
  - Includes departing employees
  - Unintentional threats
  - Countermeasures
    - Network monitoring, honeypots, DLP systems
    - Procedures
    - Keeping systems up-to-date and whitelisting can counter attempts to introduce malware inside the system

  - Pertinent Model Rules – 1.1 (Competence); 1.6 (Confidentiality of Information)

A Few Helpful Resources

- Basic security information and updates
  - US-CERT/CISA: https://www.us-cert.gov/
  - NIST Computer Security Resource Center (CSRC): http://csrc.nist.gov/
  - FBI Internet Crime Complaint Center (IC3) alerts: https://www.ic3.gov/media/default.aspx
    - ABA started linking to them in early 2016
- Threat intelligence
  - Legal Services Information Sharing and Analysis Organization (LS-ISAO): https://www.isao.org/information-sharing-group/sector/legal-services-isao/
- ABA Formal Opinions
  - 477R – Securing Communication of Protected Client Information (2017) https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf
  - 483 – Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018) https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf
- Security news
  - https://thecyberwire.com/

Scott Aurnou, Esq.

LinkedIn:
https://www.linkedin.com/in/scottaurnou

Lawline:
https://www.lawline.com/lawyer/scott-aurnou

Instagram:
https://www.instagram.com/saurnou/