INFORMATION SECURITY IN THE LEGAL INDUSTRY

Making a case *for* and not *out of* cybersecurity

Jennifer Chermoshnyuk Patrick Coleman Dennis Dore David Krasnove

ABSTRACT: Our project explored the business culture, information security practices, and potential risks at several law firms in the Seattle area. The business culture and information security practices at these firms are analyzed through a participant survey and a facilitated discussion with lawyers, IT, and InfoSec professionals from participating firms. Based on information collected, the culmination of the project was a few business-oriented security recommendations that emphasized proactive risk remediation and business opportunities.

Law firms are finding themselves on the front line in the cyber war: Where strategic action is better than tactical reaction.

HYPOTHESIS:

- External client pressures and reputational risk are largest driver toward improved IA
- Maturity of IA program varies between firms; largest influence toward maturity is "Tone from the Top" – prioritization of partners and firm management
- Information Security notion of "Need to Know" or Least Privilege is antagonistic to the open knowledge sharing or "Deliver the Whole Firm" mantra for each client for lawyers.
- Some simple but valuable starting places to improve IA exist; more frequent communication is the first step

WHY LAW FIRMS?

New Territory

Information security in the legal profession has not been well studied academically. Although law firms are attractive targets, the American public does not generally perceive that a data breach at a law firm would be as personally impactful as that of an online retailer, governmental entity, or financial institution. Law firms have largely been absent from the recent publicity and academic study of data breaches.[1]

Not Regulated

Lawyers are certified by State Bar Associations, and they act on guidelines from the American Bar Association (ABA). [2] However, there is no particular body that regulates how information security is practiced at law firms. A notable difference from their client industries such as finance, healthcare, and transportation.

Similar Objectives

Lawyers, by nature, are concerned with ethics and risk management. This along with competitive market forces, increased auditing, and client pressure, is rapidly pushing law firms away from their culture of openness and toward more mature IA/IG programs with increased focus and spending on information security.

Knowledge Sharing – Offer the whole firm to every client

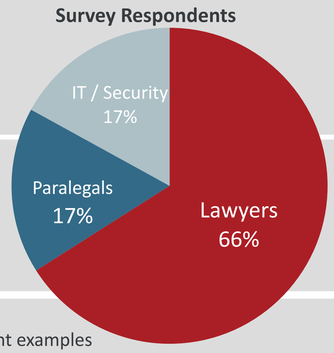
Information Assurance – Least privilege

METHOD:

- Assess knowledge and practices of the legal community through a research survey
- Curate background reading materials to brief the legal community prior to facilitated roundtable lunch discussion
- Facilitate an IA / Cyber Security roundtable to discuss survey observations, reading themes, the current state of IA in law firms, and ideas and changes to consider
- Provide firms with a summary of our findings and recommendations for simple actions to shift IA culture from reactive toward proactive

SURVEY

- Perception of legal industry threat landscape
- Information Assurance (IA) trends
- Cybersecurity strategy, policies and procedures
- Legal ethics: "reasonable effort"
- Open knowledge vs. "need to know"
- 24% of recipients participated in the survey



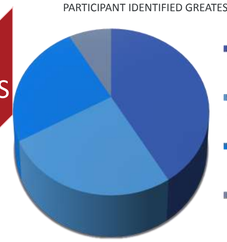
READING

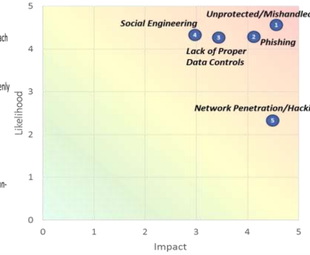
- Top Risks: Key risks specific to law firms
- Legal Ethics RPCs 1.1, 1.6, and 1.15
- Main Drivers: clients, specific threats/vulnerabilities
- Open KM culture threatened by least privilege
- Industry appropriate solutions : Non-Attorney SMEs
- Certifications (ISO 27001, PCI, etc.)

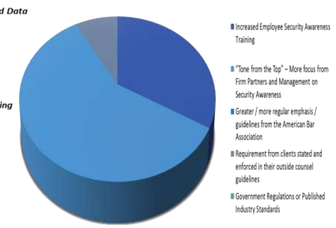
ROUND TABLE

- Security needs to support and enable efficient practice of law
- Law firm culture: What do you mean it's need to know – I want examples
- ***Availability*** is paramount
- Client demands, new threats are forcing cultural and technical change
- Legal industry aware they are behind the curve: change is imminent

FINDINGS







Rank	Risk title	Risk Description	Recommendation
1	Unprotected/ Mishandled Data	If data is shared outside the firm unencrypted, Misdirected in email or cloud service i.e. Dropbox, then a loss/breach of client data will occur	Increase awareness through training Enhance monitoring of data transfer Create IA Steering Committee to create solutions that "enable business" but reduce risk.
2	Lack of Proper Data Controls	If proper controls and classifications are not available, then data will be mishandled and breached	Formalize data classification Increase awareness through training. Augment incident response capabilities to appropriately address loss scenarios.
3	Phishing	If an adversary penetrates the network through phishing/ Spear phishing attack, then control might be yielded and data availability would be impacted	Increase awareness through training and perform spot checks if necessary.
4	Social Engineering	If social engineering is successful, then control might be yielded resulting in a data breach	Staff training. Regular vulnerability/penetration testing Encrypt data at rest according to value. Harden network devices and hosts. Perform an architectural review.
5	Network Penetration/ Hacking	If an Adversary penetrates a device or system, then control would be yielded resulting in a breach	Determine the most appropriate way to retrieve forensic data while maintaining business performance. Increase awareness and reporting of incidents through training.

1 This project was completed prior to the release of information on the data breaches suffered by 40 firms in March of 2016 and before the news of the Mossack Fonseca, better known as "The Panama Papers" breach.

2 To date, 25 State Bars have adopted the ABA's Model Rules for Professional Conduct (RPC) which include RPC 1.1 requiring technical competency by lawyers and RPC 1.6 which requires attorneys to take reasonable efforts to protect client confidentiality, including measures related to data security. WA State effective 09/01/2016.