CYBER SECURITY AND LAW FIRM RISK MANAGEMENT

Oregon Eminent Domain Conference
June 10, 2016
Portland

Mark J. Fucile
Fucile & Reising LLP
mark@frllp.com
503.224.4895
www.frllp.com
OVERVIEW

► Confidentiality, Competence and Cloud Computing
► Law Firms and Data Breach Risk
► Email Security after Edward Snowden
LOGISTICS

► Materials
► Questions
CLOUD COMPUTING: CONFIDENTIALITY

► December 2013 Amendment to Oregon RPC 1.6:

“(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.”
CLOUD COMPUTING: COMPETENCE

► OSB Formal Op. 2011-188:

“[L]awyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential.”
“Lawyer may store client materials on third-party server so long as Lawyer complies with the duties of competence and confidentiality to reasonably keep the client’s information secure within a given situation.”
CLOUD COMPUTING:
USE OF VENDORS

OSB Formal Op. 2011-188:

“... [T]his may be satisfied through a third-party vendor’s compliance with industry standards relating to confidentiality and security, provided that those industry standards meet the minimum requirements imposed on the Lawyer by the Oregon RPCs.”
“As technology advances, the third-party vendor’s protective measures may become less secure or obsolete over time. Accordingly, Lawyer may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials.”
CLOUD COMPUTING: CONSEQUENCES

► Regulatory Discipline
► Breach of Fiduciary Duty
► Malpractice
CLOUD COMPUTING: COVERAGE?

- PLF Basic Plan
- PLF Excess Plan
- Private Carriers
DATA BREACH RISK: LOW & HIGH TECH

► Low Tech Risks

► High Tech Risks
DATA BREACH RISK: SAME DUTIES

► RPC 1.1~Competence

► RPC 1.6(c)~Confidentiality

► 2011-188~Weaving them together
DATA BREACH RISK: PLUS STATUTORY DUTY

► Oregon Consumer Identity Theft Protection Act

► ORS 646A.600-.628
DATA BREACH RISK: PLUS STATUTORY DUTY

▶ ORS 646A.622(1)

“Any person that owns, maintains or otherwise possesses data that includes a consumer’s personal information that is used in the course of the person’s business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of data.”
DATA BREACH RISK: PLUS STATUTORY DUTY

ORS 646A.602(11)

♦ Defines “personal information” broadly

♦ Includes Social Security numbers, drivers license numbers, financial account numbers
DATA BREACH RISK:
“BREACH OF SECURITY”

ORS 646A.602(1)(a)

“‘Breach of security’ means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains.”
DATA BREACH RISK: NOTIFICATION OF BREACH

► ORS 646A.604

♦ Generally requires notification
♦ Notice also required by the “communication rule,” RPC 1.4
♦ PLF has a template (www.osbplf.org)
DATA BREACH RISK: COVERAGE

- Expenses of notice, mitigation and potential claims
  - PLF Basic Plan
  - PLF Excess Plan
  - Private Carriers
DATA BREACH RISK: BEFORE AND AFTER

Before
♦ Don’t assume it won’t happen
♦ Get advice on the high tech part
♦ Take reasonable precautions on the low tech part

After
♦ Get help on the high tech part
♦ Get help on notice issues
EMAIL SECURITY: “REASONABLE EFFORTS”

► RPC 1.6(c)

► ABA Model Rule 1.6, Comments 18-19


EMAIL SECURITY: “REASONABLE EFFORTS”

► What’s reasonable depends on the circumstances and the sensitivity of the information being transmitted

► Public wi-fi?

► Encryption?

► Non-electronic?
QUESTIONS?