TO "REPLY ALL" OR NOT TO "REPLY ALL" - THAT MAY BE AN ETHICS QUESTION

John T. Rogers, Jr.
Rogers Trust Law
Los Angeles, California

Presentation to
The National College of Probate Judges

May 2018

John T. Rogers, Jr.
Rogers Trust Law
350 South Grand Avenue, Suite 3500
Los Angeles, California 90071
213-986-3400
JRogers@RogersTrustLaw.com

TO "REPLY ALL" OR NOT TO "REPLY ALL" - THAT MAY BE AN ETHICS QUESTION

I. E-Mail - Love It or Leave It?

   A. How Secure?

II. History of Cyber-Attacks

   A. Software Viruses

   B. Spam

   C. Phishing

   D. Hacking

   E. "Hactivism"

      1. Wikileaks

      2. Anonymous

   F. State-Sponsored Cyber-Attacks

      1. Russia

      2. China

      3. North Korea

      4. U.S. (it's a two-way street)

         a. Iran - Stuxnet worm

   G. Other Malware

III. What Is Happening Today

   A. Data Breaches

      1. Hospitals - Ransomware

      2. Target

3. Sony

4. WannaCry Attack

5. Entertainment (e.g. HBO's "Game of Thrones")

6. Equifax

a. Complimentary protection

B. Leaks

1. Intentional

a. Edward Snowden - NSA

b. Chelsea Manning - WikiLeaks

2. Foolish

a. Hillary Clinton (?)

IV. Where Do Threats Come From?

A. Internal

1. Employees

a. Deliberate - sabotage

b. Accidental

i. Misdirected e-mail

ii. Unprotected e-mail attachments

(a) Metadata

iii. Lost storage devices (including phones)

2. IT Staff

3. Contractors

B. External

1. Exploitation of Vulnerabilities

a. Poor password practices

V. What to Do?

A. Good Hygiene

1. General

a. Keep software and operating systems updated.

b. Do not install software from unknown sources.

c. Limit who has (and uses) administrator privileges.

d. Ensure that your wireless networks are secure and avoid public wireless connections.

e. Implement hardware and software firewalls and install and maintain anti-virus software.

f. Require (different) passwords for user accounts and routers and other hardware.

g. Use encryption.

h. Educate yourself and your employees on how to avoid malware and social engineering attacks.

2. Two-Factor Authentication

B. Backup Systems

1. Cloud Services

a. Refer to ABA guidelines

2. Redundancy

C. Court Policies

1. BYOD Policies

2. Home Computer

3. The Company Laptop

4. Secure Connections

5. Social Media

D. Consider Outside Audit

E. Cyber Insurance

F. Disposal of Hardware

VI. Ethics Issues

A. ABA Model Code

1. Rule 1.2 - Confidence in the Judiciary

2. Rule 2.4 - External Influences

a. Social media

b. Adverse publicity, e.g. websites

3. Rule 2.5 - Competence, Diligence, Cooperation

a. Compare ABA Model Rules 1.1, 1.6

4. Rule 2.9 - Ex Parte Communications

a. Social media (again)

b. 2.9(C) No independent fact investigations

VII. Conclusion