Securing Client Data: Ethical Rules and Practical Tips

James D. Lamm
Karin C. Prangley
December 14, 2019

James D. Lamm

- Estate planning and tax attorney at the Gray Plant Mooty law firm in Minneapolis, Minnesota
- ACTEC Fellow

2

Karin C. Prangley

- Senior Vice President, Private Wealth Management at Brown Brothers Harriman in Chicago, Illinois
- ACTEC Fellow

3

Introduction

- The practice of law, at its core, is all about receiving, processing, and transmitting information
- Over the past 60 years or so, the practice of law has evolved with each major advance in information technology

4

Introduction

- Major information technology advances:
  - Photocopiers (1959)
  - Fax machines (1964)
  - Personal computers (1981)
  - Cell phones (1983)
  - Internet (commercially available 1989)
  - Email
  - Cloud storage and services

5

Introduction

- Estate planning lawyers acquire:
  - Social security numbers
  - Bank and brokerage account numbers
  - Net worth statements
  - Tax returns
  - Confidential family and business information
  - Maybe an inventory of digital assets (which may include usernames and passwords… although that's not recommended)
- This information is valuable to criminals

6

Introduction

- Lawyers know how to protect that information when it's on paper:
  - We take precautions transmitting important paper (*e.g.*, stock certificates, bonds, and original legal documents)
  - We lock the doors to our law firms and restrict who can enter
  - We train staff to respect client confidences

7

Introduction

- Today, we need to protect confidential information in the digital world:
  - Take precautions transmitting confidential client data
  - Lock confidential devices and data with passwords and encryption, and restrict who can access them
  - Train staff to practice safe computing and respect confidential client data

8

Introduction

- Every day, about 5.9 million data records are lost or stolen
  - 55% of breach incidents are done by a malicious outsider
  - 33% of breach incidents are a result of accidental loss
  - 5% of breach incidents are done by a malicious insider

9

Introduction

- In 2018, the FBI's Internet Crime Complaint Center received reports of 351,936 malicious cyber incidents in the U.S. (reported losses: $2.7 billion)
  - The FBI believes the actual number of malicious cyber incidents in the U.S. is about 10 times that number
  - The chance of arresting a cybercriminal was estimated to be 0.31% in 2016. Taking into account that cybercrime victims often do not report, the effective enforcement rate estimate may be closer to 0.05%.

10

Introduction

- In 2018, 76% of businesses in the U.S. surveyed by CyberEdge Group were compromised by a successful cyberattack in the past 12 months
- 65% of businesses surveyed expect they will be compromised by a successful cyberattack in 2019

11

Introduction

- About 50% of all cyberattacks are against small businesses
- 60% of small businesses that are victims of a cyberattack go out of business within 6 months
- The legal industry is predicted to be one of the 10 most cyberattacked industries for 2019 to 2022

12

Introduction

- Over 90% of successful cyberattacks and data breaches start with a phishing email
- About 1 in 50 emails are estimated to contain malicious content
- "Amateurs hack systems, professionals hack people."—Bruce Schneier

13

Ethical Rules

- ABA Model Rule 1.1:

  "A lawyer shall provide competent representation to a client."

14

Ethical Rules

- ABA Model Rule 1.1, comment 8:

  "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

15

Ethical Rules

- ABA Model Rule 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."

16

Ethical Rules

- ABA Model Rule 1.6(c), 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."

17

Ethical Rules

- ABA Model Rule 1.6(c), comment 18:

  "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."

18

Ethical Rules

- "Reasonable efforts" factors:
  1. Sensitivity of the information
  2. Likelihood of disclosure if additional safeguards are not employed
  3. Cost of employing additional safeguards

19

Ethical Rules

- "Reasonable efforts" factors:
  4. Difficulty of implementing the safeguards
  5. Extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, difficult to use)

20

Ethical Rules

- ABA Model Rule 1.6(c), comment 18:

  "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."

21

Ethical Rules

- ABA Formal Opinion 99-413:

  "A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct."

- Updated by ABA Formal Opinion 477R

22

Ethical Rules

- ABA Formal Opinion 11-459:

  "A lawyer sending or receiving communications with a client via e-mail … ordinarily must warn the client about the risk of sending or receiving electronic communications … where there is a significant risk that a third party may gain access."

23

Ethical Rules

- ABA Formal Opinion 11-459:
  - Obligation to warn a client who uses an employer-provided device or email account
  - Also consider other situations where a third party may have access to emails, including shared email accounts and shared devices

24

Ethical Rules

- State ethics opinions on email:
  - Some states require advising a client that email is not absolutely secure
  - Some states require client consent to use unencrypted email
  - Some states require appropriate precautions when using public Wi-Fi

25

Ethical Rules

- ABA Formal Opinion 477R (May 22, 2017) (update to Formal Opinion 99-413):

  "A lawyer generally may transmit information relating to the representation of a client over the Internet … where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access."

26

Ethical Rules

- ABA Formal Opinion 477R:

  "The use of unencrypted routine email generally remains an acceptable method of lawyer-client communication. However … it is not always reasonable to rely on the use of unencrypted email."

27

Ethical Rules

- ABA Formal Opinion 477R:

  "Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable."

28

Ethical Rules

- ABA Formal Opinion 477R:
  1. Understand the nature of the threat
  2. Understand how client confidential information is transmitted and where it is stored
  3. Understand and use reasonable electronic security measures

29

Ethical Rules

- ABA Formal Opinion 477R:
  4. Determine how electronic communications about clients should be protected
  5. Label client confidential information

30

Ethical Rules

- ABA Formal Opinion 477R:
  6. Train lawyers and nonlawyer assistants in technology and information security
  7. Conduct due diligence on vendors providing communication technology

31

Ethical Rules

- ABA Formal Opinion 480:
  - Lawyers who post public comments on blogs, listservs, and social media may not reveal information relating to a representation, including information contained in a public record, unless authorized by an exception to ABA Model Rule 1.6

32

Ethical Rules

- ABA Formal Opinion 483:
  - When a data breach occurs that involves client information, lawyers have a duty to notify current clients of the breach and take reasonable steps consistent with their ethical obligations under the Model Rules
  - Obligation to monitor for a data breach

33

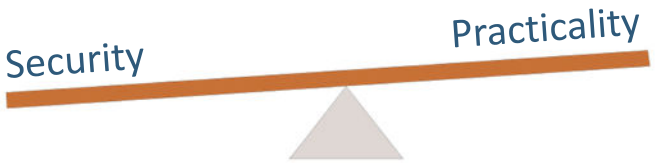
Fiduciary Counsel Beware!

- Fiduciary Counsel may have added duties from their regulators.
  - 23 NYCRR 500. Mandates that organizations implement controls, including *encryption*, based on a risk assessment to protect non-public information that has been held or sent over external networks by the organization.
  - GDPR: Requires businesses who offer products or services to EU residents to protect the personal data and privacy of EU citizens.

34

Ethical Rules

- Security should be balanced with practicality



35

Practical Tips for Cybersecurity

1. What should we do about cybersecurity?
2. How should we send confidential information by email securely?
3. How should we work securely when we're not in the office?
4. How should we keep track of passwords?
5. What else should we be doing to practice safe computing?

36

Practical Tips for Cybersecurity

1. What should estate planning attorneys do about cybersecurity?
   a. Train yourself and train your staff on a recurring basis about phishing attacks and other cybersecurity risks
   b. Hire a consultant to do periodic cybersecurity risk assessments and implement the recommendations

37

1.a. Cybersecurity Training

- Three cybersecurity resources:
  i. IRS Publication 4557
  ii. FCC Cyber Security Planning Guide: https://tinyurl.com/y64zxqvx
  iii. NIST Cybersecurity Framework: https://tinyurl.com/kxa9vfa

38

1.a. Cybersecurity Training

- Four of the top companies that train attorneys and staff on phishing and other cyber risks:
  i. https://www.cofense.com/
  ii. https://www.infosecinstitute.com/
  iii. https://www.knowbe4.com/
  iv. https://www.proofpoint.com/

39

1.b. Cybersecurity Risk Assessment

- Periodically do cybersecurity risk assessments to:
  i. Test hardware security measures
  ii. Test software security measures
  iii. Review cybersecurity policies
  iv. Review security training for all employees

40

1.b. Cybersecurity Risk Assessment

- Consider using a different cybersecurity consultant for the next assessment for a different perspective
- Consider having one consulting firm do the assessment and a different firm implement the recommendations to avoid a potential conflict of interest

41

2. Sending Confidential Information

2. How should estate planning attorneys send confidential information by email securely?
   a. Encrypt attachments
   b. Use a third-party encrypted email service

42

2.a. Encrypt Attachments

- Encryption scrambles the data so that the original data cannot be recovered without knowing the key to decrypt it
- Weak encryption: the data can be decrypted relatively easily without knowing the key (by guessing)
- Strong encryption: practically impossible to decrypt without the key (if a strong password is used)

43

2.a. Encrypt Attachments

- Weak encryption examples:
  - Some Adobe PDF documents:
    - 40-bit RC4 encryption since 1996
    - Today, 40-bit RC4 encryption can be decrypted in minutes
    - Instead, use 128-bit or 256-bit AES encryption plus a strong password to secure client data

44

2.a. Encrypt Attachments

- Weak encryption examples:
  - Some Microsoft Office documents:
    - Encryption for file formats .doc, .xls, and .ppt uses weak RC4 encryption that can be decrypted in less than 10 min.
    - Encryption for file formats .docx, .xlsx, and .pptx uses AES encryption (use with a strong password to secure client data)

45

2.a. Encrypt Attachments

- Weak encryption examples:
  - Zip archives:
    - ZipCrypto encryption released in 1989
    - Today, a home computer can decrypt ZipCrypto in minutes
    - Instead, use AES encryption plus a strong password to secure client data

46

2.a. Encrypt Attachments

- Strong encryption example:
  - Advanced Encryption Standard (AES)
  - U.S. government uses AES to protect national security information
  - AES encryption is widely-used in popular software programs and devices

47

2.a. Encrypt Attachments

- Strong encryption example:
  - 128-bit AES encryption has

340,282,366,920,938,463,463,374,607,431,768,211,456

possible key combinations

48

2.a. Encrypt Attachments

- Strong encryption example:
  - Take one 128-bit AES-encrypted file with a strong password
  - 7 billion people on the planet
  - Give each person 10 computers that each can guess one billion passwords per second

49

2.a. Encrypt Attachments

- Strong encryption example:
  - 70,000,000,000,000,000,000 password guesses per second
  - Let's say we get lucky and guess the password after trying only 50% of the possible password combinations
  - It would take 77 billion years to guess the password!

50

2.a. Encrypt Attachments

- Weak passwords undermine the protection of strong encryption:

51

2.a.i. Encrypt PDF

- Use an encrypted PDF attachment—it's an easy way to securely send confidential information to a client
  - Easy for you to create with software you probably already have at your office
  - Easy for a client to access with software already installed on the client's phone, tablet, and computer

52

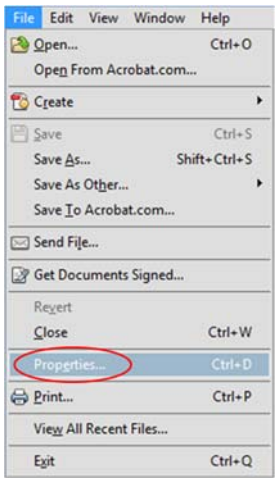
2.a.i. Encrypt PDF

- Print or scan to PDF using free or paid (*e.g.*, Adobe Acrobat) software
  - Change the security settings to "password security" and select "require a password to open the document"
  - Select AES encryption, which is available in Adobe Acrobat 7.0 or later file formats

53

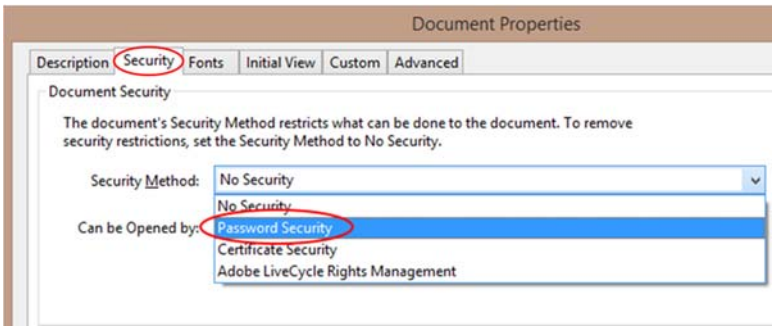
2.a.i. Encrypt PDF

- Adobe Acrobat: (full version)



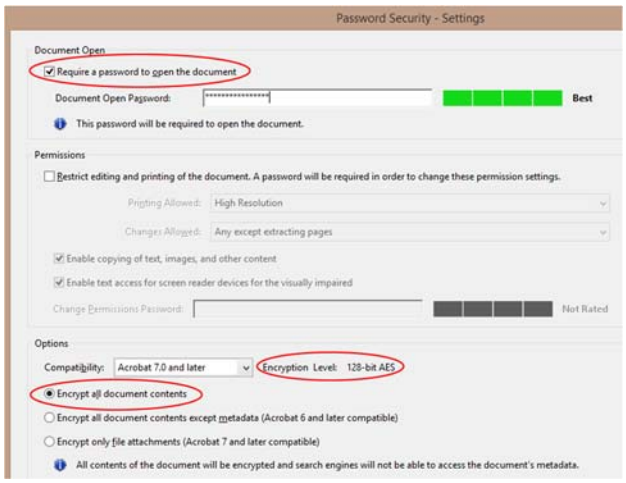
54

2.a.i. Encrypt PDF



55

2.a.i. Encrypt PDF



56

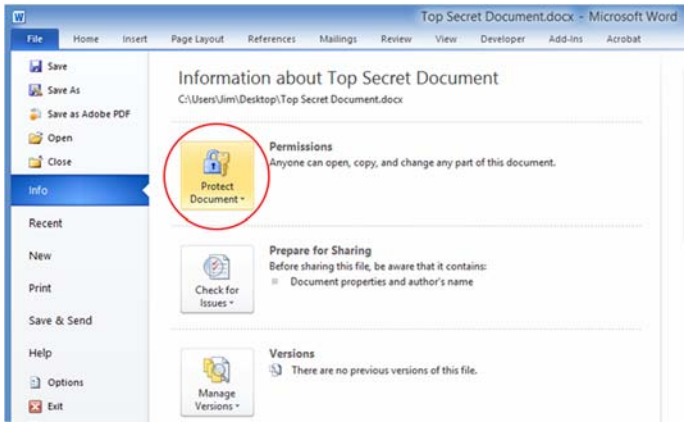
2.a.ii. Encrypt MS Office Files

- Use an encrypted Microsoft Word, Excel, PowerPoint document to securely send confidential information to a client
  - For AES encryption, ensure the file is saved in .docx, .xlsx, or .pptx format
  - File → Info → Protect Document → Encrypt with Password

57

2.a.ii. Encrypt MS Office Files

- Microsoft Word:



58

2.a.ii. Encrypt MS Office Files

59

2.a.iii. Encrypt Zip Archives

- Use an encrypted Zip archive to securely send one or more confidential data files in their native file format to a client
  - Encrypt the data using strong encryption (select AES encryption)
  - Optionally, compress the data files (makes it a smaller size)

60

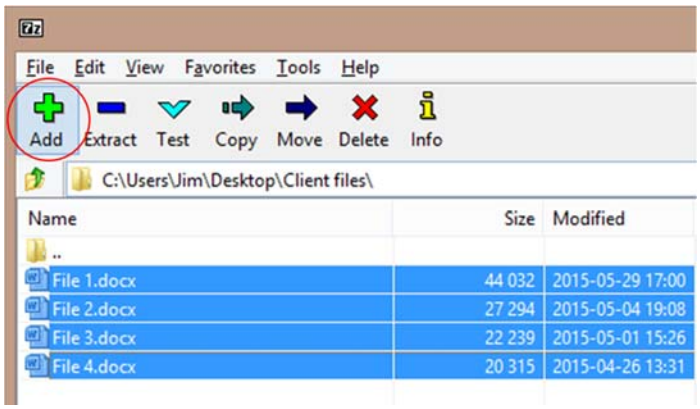
2.a.iii. Encrypt Zip Archives

- Windows software to create encrypted archives: 7-Zip, PeaZip, IZArc
- macOS software to create encrypted archives: Keka (free) and BetterZip ($24.95)
  - If you use Keka, you must take an extra step to enable AES encryption: https://tinyurl.com/y5j74o4m

61

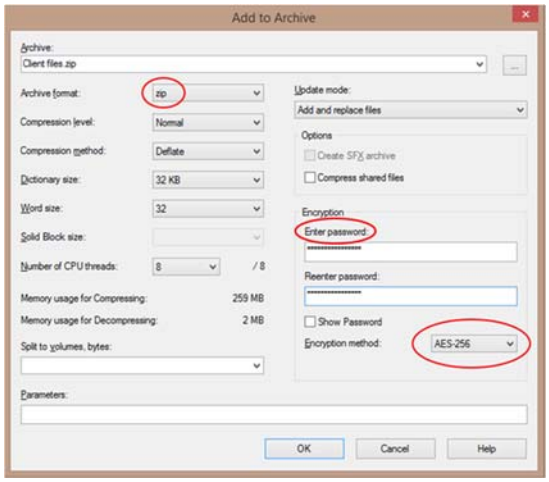
2.a.iii. Encrypt Zip Archives

- 7-Zip for Windows:



62

2.a.iii. Encrypt Zip Archives



63

2.b. Encrypted Email Services

- Encrypt email using a third-party service:
  - Virtru
  - ZixMail
  - Mimecast Email Encryption
  - Rpost RMail
  - Cisco Registered Envelope Service
  - Sophos SPX Email Encryption

64

3. Securely Working Remotely

3. How should estate planning attorneys work securely when we're not in the office?
   a. Use a secure connection to your office computers and documents
   b. Use a secure connection to the Internet
   c. Encrypt your devices and your data

65

3.a. Secure Office Connection

- Connect securely to your office computers and documents with:
  i. Cloud-based document management system
  ii. Virtual Private Network (VPN)
  iii. Remote Desktop Services (RDS)
  iv. Virtual Desktop Infrastructure (VDI)

66

3.b. Secure Internet Connection

- Use a Virtual Private Network (VPN)
  - Encrypts the connection between your device and the VPN provider (prevents others using the same public Wi-Fi network from seeing your data)
  - But, some public Wi-Fi hotspots block VPN services (use your cell phone to create a secure personal hotspot instead)

67

3.b. Secure Internet Connection

- Popular VPN providers:
  - NordVPN
  - Private Internet Access VPN
  - TunnelBear VPN
  - Many other VPN providers

68

3.c. Encrypt Devices and Data

- Encrypting an entire storage device:
  - Encrypt the system drive where the operating system is installed (recommended for laptops that store confidential client data)
  - Encrypt a hard drive, SSD, USB flash drive, etc.
  - Encrypt a virtual volume

69

3.c. Encrypt Devices and Data

- Encrypting an entire storage device:
  - Windows BitLocker (free):
    - Windows 8 or 10: Pro or Enterprise
  - macOS FileVault (free)
  - VeraCrypt (free for Windows, macOS, Linux)
  - How to encrypt your laptop: https://tinyurl.com/qbccuvv

70

4. Remembering Passwords

4. How should we keep track of passwords?

- Use a password manager:
  - LastPass: https://www.lastpass.com
  - 1Password: https://www.1password.com
  - Dashlane: https://www.dashlane.com

71

5. Safe Computing Tips

5. What else should we be doing to practice safe computing?
   a. Keep your operating system, anti-virus, anti-malware, and other apps up-to-date
   b. Back up your data regularly to protect against a ransomware attack, virus, malware, theft, or a hardware failure

72

5. Safe Computing Tips

c. Use appropriate security software on your devices (firewall, anti-virus, anti-malware, etc.)

d. Encrypt your home and office Wi-Fi networks (use the WPA2 protocol): https://tinyurl.com/ya4dvyjj

e. Use a VPN when using public Wi-Fi

73

5. Safe Computing Tips

f. Use separate, strong passwords for each of your user accounts, and use a password manager to keep track of them securely

g. Use two-factor authentication for remote access to your office systems and for as many of your online accounts as possible

74

5. Safe Computing Tips

h. Encrypt confidential client data before it leaves your office by email, on a laptop, on a USB flash drive, etc.

i. Don't leave mobile devices unattended

j. If you've been infected with a virus or malware, get help *(see* https://tinyurl.com/ycktycqt)

75

5. Safe Computing Tips

k. If you've been attacked with ransomware, get help at https://www.nomoreransom.org

l. Think before you click on any link or attachment that you receive, even if it comes from someone you know and trust. When in doubt, check it at: https://sitecheck.sucuri.net/ or https://www.virustotal.com

76

Questions and Answers

James D. Lamm
Karin C. Prangley

77

Copyright Information

-

78