“Is cyber-crime impacting your ethical obligations to your clients?”
Outline

- **Why are Lawyers being Targeted?**
- **Statistical Information to be Aware of**
  - Training, Audits, Oversight, and target
- **Cyber-Attacks**
  - Identity Theft
  - Consequences of identity theft
- **Internet Threats**
  - Sniffing
  - Spoofing
  - Anti-Virus and Anti-Malware
  - Ransomware
  - Social Engineering
- **Email Security 101**
- **Tools for Control**
  - Firewalls
  - Encrypted Hard Drives
  - Encrypted Communication
  - Education
Outline

- **Ethics of Client Communication**
  - Minimum standards you should meet for your clients?
  - What are clients expecting?

- **What standards are your clients held to for data handling regulations?**
  - Understanding minimum standards
    - HIPAA, Gram Leach Bliley Act, Sarbanes Oxley, GDPR

- **Understanding ABA Opinion 477R**
  - What makes information sensitive?
  - What is the likelihood information is disclosed?
  - Are implementing cybersecurity measures cost-prohibitive?
  - Are safeguards difficult to deploy?

- **Ethical Conduct Under the ABA Model Rules and Federal Rules of Civil Procedure**
  The ethical requirements for attorneys as they relate to modern technology are described in several different sets of rules, including:
  - ABA Rule 1.15 - Appropriately Safeguarding Client Property
  - ABA Rule 1.3 - Diligence and Promptness
  - ABA Rule 1.6 - Duty of Confidentiality
  - ABA Rule 3.4 - Fairness to Opposing Counsel

- **Trend Changing for the Legal Community**
  - Ethical Consideration with Client Communication

- **Improving your Firm’s Security**
Why are Lawyers being Targeted

Lawyers have been underserved in the technical security arena. Why?

- **Limited reporting requirements** has caused lack of awareness in this industry:
  - Lack of knowledge has created **Slow Technological Movement**
  - Lawyers not wanting to create **Impediments** with **Client’s Communications**
  - **Vulnerability** in this sector has created greater **Criminal Focus**
  - **Security Companies** have **Limited Efforts** in the legal field due to **Limited Emphasis** on cyber-security
Statistical Concerns:

- **Training** - Less than 50% of firms have documents cyber-security **training policies** with staff.
- **Audits** - 54% of Firms are receiving a Cyber-Security **Audit** by 1 or more **Clients**.
- **Oversight** - 76% of firms do not have a dedicated person **monitoring for cyber-attacks**.
- **Targeted** - 22% of firms have had **targeted attacks** in 2017... this does not encompass all breached – just targeted.

*Stop being a Victim*

“2018 Logicforce Force Technical Stats”
Cyber-attacks

- **Cyber-attacks:**
  - Typically focus on servers, computers, tablets and mobile phones
  - Having a device infected by a virus or other security threat has **effected 57%** of Americans

Identity Theft:

- 143 million Americans were affected by cybercrime in 2017, affecting more than half online U.S. adults

**Consequences to identity theft**

- Can block your access or delete your personal documents and pictures;
- Can target clients information
- Can cause destroy **business reputation**
Sniffing and Spoofing

Sniffing

- What is this and why should I care?
  - Passive cyber-attack of collecting and utilizing data in a nefarious manner
  - This can be captured at any network point on unencrypted data
  - Victims are usually unaware for months or years
  - Network and encryption protocols are essential to the protection from

Spoofing

- Not a Halloween prank but can be devastating to your firm or reputation:
  - The act of not just viewing but Altering Data or Impersonating the Sender of the information
Statistics which should encourage stricter protocol’s

Why is software updating critical to network protection:

- Every 4.2 Seconds a new Malware Specimen is Introduced
- 77% of compromised Attacks in 2017 were Fileless (exploiting files already installed)

Anti-Virus & Anti-Malware

A variety of malware and virus protection programs are available:

- Maintenance - None of these Solutions are effective if they are not Updated and Maintained
- Maintenance - More than 30% of all computers are Not Protected on a regular basis
- Maintenance - Ensure you are Updating the most Recent Patches, daily or statistically you are at risk
Ransomware

Utilization of Encryption of your data, restricting you from accessing the information:

- 184 Million Attacks in 2017
- 1 in 5 Businesses who paid the ransom never got their data back
- 34% of affected took a week or longer to get data back once Ransom was paid and 17% never received data
- Total number of Ransom attacks grew 56% in the last 4 quarters

What to do...

- Train employees about what to look for and the risk
- Use Scanning technology
- Backup your own data and utilize data encryption
- Never pay the Ransom
Social Engineering

Social engineering is an attack vector which relying on human interaction - involves manipulating people into breaking normal security procedures:

- 43% of the documented breaches involved social engineering attacks
- 66% of malware came from malicious email

What should a business do...

- Train employees about what to look for and the risk
- Implement Strict Security Protocols
- Utilize Encryption and Verification
Email Security 101

- **What is the process to encrypt?**
  - Encryption is simple to deploy on most email platforms.
  - Standard email does not provide the security needed to be protected
  - *(Gmail, Outlook, O365)*

- **How does encryption prevent interception?**
  - How does encryption work?
  - Will encrypting email content protect me from a data breach?

- **Is encryption difficult to set-up?**
  - Encryption system have become simpler and more user friendly.
  - They will work with your current email system.

- **Will this create challenges when communicating with my client?**
  - Will my client be upset with the additional steps they need to take?
  - What are the implications if I don’t encrypt?
Identillect Secure Communication

Committed to advancing client trust for digital Communication:

Identillect’s Team of Cyber Security Professionals are dedicated to the integrity of the legal community's ethical communication to their clients.
Tools for Control

- **Firewalls** - firewalls are created and designed to block malicious software and corrupt files from entering your computer.

- **Encrypted Hard Drives** - a technology which encrypts the data on a hard drive using sophisticated mathematical functions, only accessed by individuals with appropriate access. (How many have had your laptop lost or stolen)

- **Encrypted Communication** - encrypting, or disguising, the content of email messages in order to protect potentially sensitive information from being read by anyone other than intended recipients. **(THE MOST EFFECTIVE MEASURE TO PROTECT CLIENT INFO)**

- **Education** - Security Education and Training Awareness (SETA) - educational program designed to reduce the number of security breaches that occur through a lack of employee security awareness.
Ethics of Client Communication

Minimum standards you should meet for your clients?
- This is a moving target...
- Affected by regulatory change
- Affected by increased data breaches
- Affected by industry trends

What are clients expecting?
- Expectation of confidentiality
- Expectation you know how to protect them
- Expectation you have appropriate security measures in place
Regulations effecting the legal industry

- **ABA Formal Opinion 11-459 & 1.6** - Importance of communicating the *inherently unsecure nature of unsecured email* communications with the client.

- **ABA Formal Opinion 477 & 483** - A lawyer shall make *Reasonable* Efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access.

- **GDPR General Data Protection Regulation** - *Reasonable* efforts to prevent inadvertent or unauthorized disclosure of information.
Client Regulatory Requirements

Client Regulatory Requirements Affect their Legal Representation:

State & industry-specific data handling regulations require encryption when communicating personal identification information (PII)

Examples:

- Gramm-Leach Bliley (GLBA)
- Sarbanes Oxley (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- State Data Handling Regulations

Personal Identifiers

1. Names
2. Geographical locations
3. Dates
4. Phone numbers
5. Fax numbers
6. Email addresses
7. SSNs
8. Medical record numbers
9. Health plan numbers
10. Account numbers
11. Certificate/license #’s
12. VIN/License numbers
13. Device identifiers and serial #’s
14. URLs
15. IP Addresses
16. Biometric identifiers
17. Full face photographic images
18. Unique identifying number
Factors to Consider when Employing Security Measures

- 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
- the extent to which the safeguards adversely affect the lawyer’s ability to represent clients

“The ABA’s latest guidance on cybersecurity is a must read that should give pause to every lawyer, law firm IT department and law firm manager,” writes this IP/ethics commentator.

Implementing the ‘right’ cybersecurity measures for a given representation is fast becoming – if it is not here already – a lawyer’s ethical duty.”
ABA Model Rules

Rule 1.15: Safekeeping Property: A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation. Property shall be identified and appropriately safeguarded.

Rule 1.3: Diligence: A lawyer shall act with reasonable diligence and promptness in representing a client.
ABA Model Rules

Rule 1.6: Confidentiality of Information: A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.

- 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.

Rule 3.4: Fairness to Opposing Party & Counsel: A lawyer shall not unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value.
As Cyber Threats increase changes are made to rules/opinions:

- 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.

- Define Reasonable: At the intersection of a lawyer’s competence obligation to keep “abreast of knowledge of the benefits and risks associated with relevant technology to protect client communication”.

- Reasonable for Technology: lawyers must exercise reasonable efforts when using technology in communicating about client matters.

- Risk Assessment and Effectively: “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify they are effectively implemented, and ensure that they are continually updated in response to new developments.
Ethical Consideration with Client Communication

- If electronic communication is utilized to communicate with clients and we know standard electronic communication is not secure, you must notify your client of the risks.

- The lawyer and client then should decide whether another mode of transmission, such as high-level encryption or personal delivery is warranted.

- Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client.

- Either Security should be used, or the lawyer should provide full disclosure of the potential risks.
Improving your Firm’s Security

- **Protecting your Firm**
  - Enhance security measures for your business and meet the compliance standards

- **Securing communication for your Firm**
  - Ensure all communications are secure

- **Educating your clients**

- **Educating your Staff**
  - Ensure you develop a secure education program for all employees with regular updates

Don’t be a victim!

*Let Identillect help you take security to the next level*
“Is cyber-crime impacting your ethical obligations to your clients?”

Please contact us to schedule a follow-up discussion:
Todd Sexton, MBA, CEO
Identillect Technologies
949-215-1244
todd.sexton@Identillect.com