Cybersecurity Concerns for Attorneys

NEW YORK STATE BAR ASSOCIATION
BRIDGE THE GAP CLE
NEW YORK, NEW YORK
AUGUST 27, 2015

DeVore & DeMarco LLP
Attorneys and Counselors at Law

Today's Topics

- My Background
- Cybersecurity Pitfalls for Lawyers
- Legal and Ethical Cybersecurity Requirements
- Practical Cybersecurity Tips for Lawyers

My Background

- Partner, DeVore & DeMarco LLP
  - Boutique law firm in New York City
- Cyberlaw Practice
- Previously, Assistant U.S. Attorney, Southern District of New York, 1997-2007
  - Founder and Chief, Computer Hacking and Intellectual Property Unit (CHIPS)

Cybersecurity Pitfalls

- Compromise of Client Information
  - Gatekeepers: Lawyers often possess, store, and maintain numerous kinds of confidential information
    - Intellectual Property
    - PII
    - Privileged materials
  - Vulnerabilities
    - Hacking: Outside intrusions or targeted attacks
    - Inadvertent loss or insider theft

Cybersecurity Pitfalls

- Social Media and the Internet
  - Publicly accessible information and social engineering
  - Using Social Media and Internet for investigative purposes
  - Unsafe Browsing
  - Ethics
    - Breach of Confidentiality for public disclosure
    - Privilege of Communications
    - Solicitation and Attorney advertising
  - If ever in doubt, refer to the NYSBA Social Media Guidelines

Cybersecurity Pitfalls

- Cloud Storage and Removable Storage Media
  - Lackluster security features and ability to minimize downstream sharing
  - Lack of audit capabilities
  - Lack of control and transparency in storage and retention
  - Inadvertent storage in publicly accessible areas

Cybersecurity Pitfalls

- Email and Digital Communications
  - Inadvertent distribution of confidential client information
  - Phishing attempts and malware
  - Privileged and confidential communications

Cybersecurity Pitfalls

- Mobile Devices
  - Increased portability of mobile devices increase risk of loss or theft
  - Comingling of Client, Firm, and Personal data and inadvertent disclosure – particularly in email
  - Potential for rogue connectivity and compromise

Legal and Ethical Cybersecurity Considerations for Lawyers

- **ABA & NY Rule 1.1** – Duty of competent client representation
  - Technology is an increasingly important aspect of legal practice – both in form and in substance – and lawyers owe their clients a duty of competence with technology in their representation.
- **Communication**
  - **ABA & NY Rules 1.4** – duties regarding of client communication to client
    - Involves and arguably requires effective use of technology by attorneys
- **Confidentiality**
  - **ABA & NY Rule(s) 1.6** – Confidentiality of Client Information
  - **NY County 733 (2004)** – "An attorney must diligently preserve the clients confidences, whether reduced to digital format, paper, or otherwise.
  - **NY CPLR 4548**
    - Privileged communication does not lose its privileged character solely because it is communicated by electronic means or because "persons necessary for the delivery or facilitation of such electronic communication may have access to" its contents.

Legal and Ethical Cybersecurity Considerations for Lawyers

- Email and Attorney-Client Communications
  - **NSYBA Ethics Comm. Opinion 709 (1998)** – Ethics of Transmitting Confidential Information Online (Email)
    - Lawyers may transmit confidential information by Email, but "must always act reasonably in choosing to utilize Email for confidential communications."
    - But where a lawyer is on notice that the confidential information is "of an extraordinarily sensitive nature that it is reasonable to use only a means of Communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet Email."
  - **NSYBA Ethics Comm. Opinion 820 (2008)** - A lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising (*i.e.* Gmail), where the e-mails are not reviewed by or provided to human beings other than the sender and recipient … "Unless the lawyer learns information suggesting that the provider is materially departing from conventional privacy policies … or puts confidentiality at risk, the use of such e-mail services comports with DR 4-101" (Rule 1.6).

Legal and Ethical Cybersecurity Considerations for Lawyers

- Cloud Storage and Attorney-Client Materials
  - **NSYBA Ethics Comm. Opinion 842 (2010)** – Ethics of Storing Confidential Information Online
    - "A lawyer may use an online "cloud" computer data backup system to store client files provided that the lawyer takes *reasonable care to ensure that the system is* ***secure*** *and that client* ***confidentiality will be maintained***.
    - "**Reasonable care**" includes consideration of the following:
      - Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
      - Investigating the online data storage provider's security measures, policies, recoverability methods and other procedures to determine if they are adequate under the circumstances;
      - Employing available technology to guard against reasonably foreseeable attempts to infiltrate the Data that is Stored; and/or
      - Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes providers.

Practical Cybersecurity Tips for Lawyers

- **General Computer Security Awareness**
  - Run Updates and Security Patches on computers or laptops
  - Use robust, complex, and varied passwords for user accounts
  - Minimize or eliminate use of USB drives and removable media devices
  - Minimize use of P2P applications on devices connected

Practical Cybersecurity Tips for Lawyers

- **Email Best Practices**
  - Avoid use of private email accounts for business purposes
  - Use different passwords for email and other system access
  - Double-check recipients to avoid auto-complete and inadvertent receipt
  - Don't use your email as your file repository -- do not leave emails with confidential information stored in accounts for longer than necessary.
  - Encrypt or password protect privileged or confidential attachments – and do not include the password in the email.

Practical Cybersecurity Tips for Lawyers

- **Mobile Device Security**
  - Passwords – use them, vary them, don't write them down
  - BYOD
  - MDM solution
    - Access Control
    - Data Segregation – Personal Data and Client Data remain separate
    - Remote Beacon/"Find my iPhone"
  - Anti-Virus and Anti-Malware
  - Understand the settings and privacy features of your mobile device
  - Encryption*

Practical Cybersecurity Tips for Lawyers

- **Data Encryption**
  - In Transit:
    - HTTPS and SSL – Look for indicators in browsers
  - At Rest:
    - Full Disk Encryption
      - Apple iOS8 and above is encryption by default
      - Consider hard disk encryption for Laptops, Tablets, and other mobile devices
    - Utilize encryption software
  - What Data to Encrypt and When
    - Any Client or sensitive Firm information stored on servers
    - Any Client or Firm information sent by Email
    - Any removable storage media containing Client or Firm information

Practical Cybersecurity Tips for Lawyers

- **Cloud Storage**
  - Assess *what* data will be stored in the cloud
  - Do your due diligence – use the "reasonable care" steps to ensure that the system is secure and client confidentiality will be maintained.
  - Consider the location of data storage and issues with cross-border data flows and international privacy laws

Practical Cybersecurity Tips for Lawyers

- **Public and Private WiFi and International Travel**
  - **Before Travel**
    - Secure devices with robust passwords
    - Configure devices so that wireless and Bluetooth connections are not established automatically;
    - Ensure that P2P connectivity has been disabled on all devices
    - Utilize hard disk encryption whenever possible
  - **While Traveling**
    - Lock doors in taxis, limousines, and rental vehicles, and check them upon exiting
    - Keep mobile devices out of site while using any public transportation
    - Use only trusted, password protected Wireless connections or hotspots, and never connect to public, free, open WiFi hotspots.
    - Use VPN connections to access corporate networks, and SSL to access private information.
    - Do not use public computers to access any company or personal email accounts

Questions?

DEVORE & DEMARCO LLP
ATTORNEYS AND COUNSELORS AT LAW

Joseph V. DeMarco
DeVore & DeMarco LLP
99 Park Avenue, Suite 1100
New York, New York 10016
Phone: (212) 922-9499
Fax: (212) 922-1799
jvd@devoredemarco.com