Law Firm Cyber Security Tips

Encompassed within a lawyer's duty of confidentiality (Ala. R. Prof. C., Rule 1.6) is a duty to ensure clients' information is protected in all of your data sources. Cyber security has become necessary in the ever-evolving practice of law. It is far better to be proactive than reactive when it comes to cyber security.

- **Cyber Security Obligations:**
  - Types of Data
  - Client specific needs (i.e. HIPAA)
  - Ethical Obligations

- **Logistical Needs**:
  - Dedicated computer for work. Do not use your work computer or email for personal matters.
  - Secure communications
  - Training
  - Knowledge regarding types of threats
    - Think before you click
    - Beware of Fraudulent websites
    - Don't respond to scammers
    - Use antivirus software
    - Only sue trusted software

- **Encrypt Everything**: According to an ABA survey conducted in 2012, all forms of encryption – including file encryption, email encryption, and full disk encryption – are the least often used security feature among law firms. Encryption is a relatively simple and effective risk management tool. Lost and stolen devices are the most common cause of data breaches in law firms. Encryption protects your information even if your device has been accessed improperly.

- **Cloud Computing**: You must use due diligence in selecting a cloud provider by asking the right questions. You should ensure the provider employs adequate security to protect your data. You should only use a cloud provider that can provide you with reasonable assurance that your data will be secured.

  - **TIP**: If the provider cannot give you such assurance, then you should decline their services.

- **Staff Training:** Educating staff on confidentiality issues and avoiding data breaches can greatly reduce the risk of a data breach in your firm. It's important for employees to understand that spam filtering and anti-virus will never be 100% effective in stopping malware.

- **Passwords**: Having a different password for every account can be confusing and frustrating. However, maintaining clients' confidentiality is of utmost importance. You should develop a uniform password policy, which includes certain criteria. Passwords should be a complex combination of letters, numbers, and special characters. You should change your password routinely and never duplicate a password.

  - **TIP**: Utilize a password manager to create, track, and securely store your passwords.
  - **TIP**: Choose strong passwords
  - **TIP**: Never tell anyone your passwords (not even IT staff)
  - **TIP**: Enable multi-factor identification

- **Recovery Plan**: Regardless of the policies you have in place and the security measures you employ, you should be prepared for a security breach. Have a business recovery plan in place and test it annually. Routinely back-up your data and maintain a copy of data in an off-site secure location.

  - **TIP:** Consider obtaining cyber liability insurance coverage.

- If you need additional information please contact PMAP at autumn.caudell@alabar.org or 334-517-2120.