Example Security Audit Questionnaire

1. Does your firm have cyber security policies, procedures, and standards based on industry standards?
2. Does your firm protect sensitive information received from a third-party firm during transmission between the owning third-party as well as other parties with whom that data is shared (i.e. Encryption, SSL/TLS connections)?
3. Are all devices that store or process a third-party firm's sensitive information protected from the Internet by a firewall?
4. Does your firm have designated Cyber-security personnel?
5. Does your firm have a cyber-security user education and awareness program?
6. Does your firm perform cyber security audits by external 3rd parties at least annually?
7. Do all devices that store or process sensitive information utilize antimalware software with current signature files?
8. Do users that can access devices that store or process sensitive information have a unique user name and complex password to access the system?
9. Do all devices that store or process sensitive information at a minimum have access control that is configured on a least privilege model (a person only has access to the data/device that they need)?
10. Do all devices that store or process sensitive information at a minimum have vulnerability scanning performed at least monthly
11. Are vulnerabilities being remediated in a risk based priority (highest priority vulnerabilities are fixed first)?
12. Do all devices that store or process sensitive information at a minimum have all unnecessary ports and services disabled and the device is used for limited functions (ex. A device acting solely as a file server vs. a file server, FTP server, and web server)?
13. Do all devices that store or process sensitive information at a minimum have patches deployed for high risk operating system and third-party application vulnerabilities within industry best practices (i.e. 48 hours) and medium/low risk patches to be deployed in <= 30 days?
14. Are all laptop devices that store sensitive information encrypted?
15. Do all mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have configuration management provided by a firm owned centrally managed infrastructure including the ability to remote wipe the device?
16. Do all mobile devices (e.g. smartphones, tablets) that store sensitive information at a minimum have access control to the device (complex password to access device)?
17. Does your firm have a Computer Incident Response Team (CIRT) with a formal process to respond to cyber-attacks?
18. When you must share sensitive information with other companies, do you require those companies to follow policies, and procedures for cyber security based on industry standards?
19. Does your firm require 2-factor authentication for remote access (e.g. token used in addition to a username and password for VPN login)?
20. 21. Does your firm perform industry standard logging and monitoring on devices that store or process sensitive information?
21. Does your firm control web access based on the risk (e.g. reputation, content, and security) of the sites being visited (e.g. Web Proxy Controls)?
22. Does your firm have capabilities of detecting and blocking malicious e-mail prior to delivery to the end user?
23. Does your firm actively participate in a cyber-intel sharing forum? (e.g. ISAC, Infraguard)
24. Does your firm perform phishing e-mail testing of its employees?

Standard of Care for Client Data – Legal Obligations

- Currently 48 states have enacted breach notification laws
  - Still talk of a Nationwide breach notification
  - Breach notification requirements could prove devastating to a Law Firm's Reputation
  - Nevada District Ct. finds no standing to sue where the only risk is a potential for future harm
  - CA N.D.: finds standing to sue where costs of credit monitoring, password protection, or threatening e-mails are sufficient to show harm

Ethical Obligations

- ABA Model Rules of Professional Conduct:
  - 1.1: Attorneys must keep abreast of changes in the law – including risks and benefits of technology
    - 1.15 (safekeeping property) may include electronically stored information
  - 1.6: Attorneys must take reasonable precautions with client data (storage and transmission)
  - 5.3: Using cloud based storage – attorney must take reasonable precautions to safeguard client data

- Ethical Obligations - Continued
  - CA (Prof'l Resp. and Conduct Op. 2010-179): Attorney must take reasonable steps to ensure use of technology does not expose confidential client data
  - AZ (Ethics Op. 05-04): Attorney must have expertise to assess HW/SW & Network for data safeguards OR must retain an expert to do so
  - NJ (Ethics Op. 701): Documents transmitted via email over the internet should at a minimum be password protected
  - NY (Ethics Op. 842): use of third-party provider to store client data – MUST exercise reasonable care to protect client data
  - PA (Ethics Op. 2011-200): 15-point list of steps a firm may take to exercise reasonable care of client data storage (cloud based)

Legal Considerations (Discovery)

- WA: Kyko Global, Inc. v Privthi Solutions – 5-factor balancing test
  - Reasonableness of precautions taken
  - Amount of time required to mitigate the error
  - Overall scope of the discovery effort
  - Depth and breadth of the disclosure
  - Impact on the fairness of the proceeding
- MD: Victor Stanley, Inc. v. Creative Pipe, Inc.
  - Search parameters of electronic information not verified
  - Insufficient review prior to disclosure of items
  - RESULT: 165 otherwise confidential documents produced for opposing counsel ruled admissible