Legal Due Diligence Checklist For
Cyber-Preparedness of Businesses and Non-Profit Organizations

CIANJ Virtual Event: Living in the Remote Workforce:
How Technology Makes Working From Home Possible
April 30, 2020

By: Brett R. Harris, Esq.[1]
Business, Nonprofit and Technology Attorney
Wilentz, Goldman & Spitzer, P.A.

□ ***Develop Information Security Program –*** administrative, technical and physical security measures

□ ***Assess System Vulnerabilities*** – "ethical hack" by security professionals hired to identify weaknesses

□ ***Investigate and Implement Technology Solutions*** - anti-spam software, firewalls, and email filters; multi-factor authentication; administrative rights management; cryptography; outsourcing of data storage

□ ***Establish Access Levels*** – segregate data and company records to limit access to those within and outside the company with need to know

□ ***Asset Management and Control*** – lost or stolen computers and storage devices are major cause of breaches; portable devices should be inventoried, monitored and controlled remotely

□ ***Develop Document/Data Management, Retention and Destruction Policies*** – should be organization-specific, written, mandatory policy; must set retention periods appropriate for legal, tax and regulatory compliance, operational needs and contractual obligations; need procedures for suspension of destruction processes for litigation holds and e-discovery and laws on spoliation of evidence and obstruction of justice

□ ***Determine "Secure Destruction" Procedures*** - NJ law requires that personally identifiable information in electronic and paper documents must be destroyed, erased or rendered unreadable prior to disposal; need to address disposal of equipment with embedded data, including cell phones and copy machines

□ ***Red Flag Rule Compliance*** - written program must be instituted under FTC's Identity Theft Regulations applicable to creditors (one who arranges for the extension, renewal or continuation of "credit", being the right to defer payment of debt or to purchase property or services and defer payment therefore). Applies to banks, finance companies, automobile dealers, mortgage brokers, utilities, telecommunications companies and those who maintain "covered accounts" not otherwise exempted

---

Brett R. Harris is a shareholder with Wilentz, Goldman & Spitzer, P.A. in Woodbridge, NJ. She is a corporate transactional attorney admitted in New Jersey and New York. In addition to counseling businesses and non-profit organizations in her general corporate practice, she focuses on addressing legal issues raised by technology. She can be reached through the firm's web site at www.wilentz.com, or directly at bharris@wilentz.com or (732) 855-6122. Follow her on Twitter @BrettHarrisEsq for tweets on business and nonprofit matters, technology law and issues of interest to professional women

 Develop Data Breach Response Plan – incident response procedures should be set in advance to minimize overall cost and reputational harm and ensure business continuity; develop by team of management, HR, PR, legal and IT; identify what laws may be implicated by surveying the State residences of those whose personally identifiable information is maintained

 Set Designated Point of Contact– whether titled Privacy Officer or assignment of responsibility to HR Director, Legal Staff or other Executive (typically not IT Administrator), plan ahead so can ensure consistent coordinated message to law enforcement, regulatory bodies, victims, press and business partners

 Negotiate Contractual Provisions relating to Data – When company data will be stored by others (such as cloud computing platforms) or accessed by business partners (for operational matters such as supply, distribution and order fulfillment), have written contracts which address data security and shift burden to notify if breach occurs by third party, given that most state breach notification laws provide for notice by data owner

 Conduct Due Diligence on Outside Vendors– review security programs, back-up and disaster relief plans, privacy policies, and employee training at companies where data will stored

 Background Checks – subject to applicable state laws and Fair Credit Reporting Act requirements, consider requiring for those employees and contractors with network access or clearance for confidential information

 Create "Security Culture" through Training and Policies – make employees cyber-conscious through tips and best practices: web based email systems should not be accessed on unsecured networks; consider encryption for highly confidential information; use robust passwords; do not follow links provided in spam emails; be cautious about pop-up messages and unsolicited emails with downloads; never provide information about the organization's computer systems or account numbers to outsiders; report any breaches immediately

 Implement Social Networking Policies – social networking sites can be access points for intruders and employees may disclose company confidential data or security information through inadvertence or inattention

 Employee Monitoring - after crafting a properly-worded policy, distributed with appropriate notice and consent to avoid employee privacy issues, monitoring can identify pattern of suspicious access to sensitive data

 Exit Interviews of Departing Employees –inventory and return of computers and devices, disabling of access to systems, and require employees to execute Reaffirmation of obligations of confidentiality

 Post-Employment Enforcement – similar to enforcement of non-disclosure agreements and non-competes, when employees are identified as offenders, pursue legal recourse civilly and criminally for deterrent effect

 Investigate Insurance Risk Transfer Options– consider cyberinsurance