Cybersecurity – Crisis Management Associated with Data Breaches

Suggested Preventative Measures:

- Inventory all systems in your environment and know what data you possess, the type of data it is (e.g. PII, PCI, PHI), and where it is stored.
- Update your systems with the most current technologies, timely update all patches and update antivirus on endpoints and servers and set them to automatically conduct regular scans.
- Ensure critical systems and files have up-to-date backups.
- Have both an Incident Response Plan and a Security Compliance Plan.
- Conduct an audit of all high-risk vendor agreements to ensure your interests are adequately protected.
- Frequently train employees how to identify phishing and spear-phishing emails and follow the principle of least privilege, that is, do not give employees access to data they do not need.
- Practice and enforce good password hygiene with your employees.
- Utilize the expertise of a reputable Data Security Services provider!

The Evolving World of Cyber Insurance:

The cyber insurance industry is still finding its footing in this new age of cyber attacks. Nonetheless, there are many different types of insurance coverages a business can obtain to protect itself, such as:

- Forensic and Legal Services Costs Coverage
- Regulatory Costs Coverage
- Crisis Management/Public Relations/Notice Costs Coverage
- Computer Extortion Coverage
- Business Interruption Coverage
- Data Recovery Coverage
- Ransomware Coverage
- Social Engineering Coverage
- Telecommunications Coverage
- Credit Monitoring Costs Coverage
- Media/Content Liability Coverage
- Privacy Liability Coverage

But…Beware of Policy Loopholes:

If you elect to purchase cyber insurance for your business, read the policies carefully. Some examples of policy loopholes include:

- An exception may apply to any named insured if a current or former partner, officer, or director of such named insured committed, acquiesced or participated in the actions that gave rise to a claim.
- Certain coverages may require other coverages also be purchased, for example, Ransomware coverage may have to be purchased in conjunction with Computer System Extortion coverage.
- Look for requirements in the policy that call for subjective standards such as "good faith reliance."
- The policy may not apply with respect to any government-ordered seizure or destruction: seizure, confiscation, nationalization or destruction of information or the computer system by order of any governmental or public authority.

If you suffer a data security breach:

1. Call your attorney to represent you, including during audits and litigation.
2. Notify insurance carrier of potential litigation, losses and damages.
3. Based on the advice of counsel, notify the proper governmental department and affected clients in accordance with mandatory reporting requirements. See Florida Statute 501.171, entitled, "Security of confidential personal information," which states: "A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c)." **Please note**: every state has its own requirements and if you have an affected client who resides in another state then that stat's regulations must be accounted for as well.

Offices Tampa, Florida
119 S. Dakota Avenue, Tampa, FL 33606
www.HunterBusinessLaw.com
813.867.2640