KRIEG | DEVAULT

Insights

Are you prepared for a Cybersecurity Breach?

August 13, 2015

Today, more than ever before, organizations face the growing challenge to ensure they are empowered and equipped to succeed with breach prevention, preparation, and response. Proactively securing experienced legal counsel should be one of the first steps in any organization's preparation for a future cyber-attack.

A recent article authored by Kacy Zurkus at www.csoonline.com advocates the benefits of having a cybersecurity attorney on retainer. Zurkus posits that cybersecurity law firms provide services from data breach to cybercrime, compliance with privacy laws, security policies, records management, and corporate security planning.

JJ Thompson, chief executive officer at Rook Security, noted, "To not have a cybersecurity attorney on retainer is foolhardy at best." Companies will benefit with proper, thorough advanced planning for potential breaches. Planning should include building a response team, employee training, insurance review, employee manuals and policies.

Beyond technical safeguards, companies can proactively put themselves in a better position from a corporate governance perspective. For example, conducting a legally privileged review of security measures prepared by outside counsel can assist an organization preparing for the inevitable. After the review is completed, outside counsel can prepare a detailed, legally privileged plan providing guidance to shore up a company's security plan. Areas to consider include possible insider threats, physical security in addition to network security, use of VPNs for remote access, and the development a cyber breach response plan. Plaintiffs' lawyers and regulators will likely look to the measures used to prevent cyber-attacks as a basis to assert civil or regulatory liability. A well-prepared plan for combatting cyber-threats would go a long way to protect against such claims.

To learn more about Krieg DeVault's Cybersecurity Practice click here.