Data Security

In recent years, shareholders have begun to directly target board members and company officers when data breaches occur. This began with TJ Maxx (2010), Target (2013), Wyndham (2014) and continues to be a growing trend. Current examples include litigation against Adobe, LabCorp, Google, Facebook and SolarWinds.

Litigation targeting execs isn't the only problem, the damage done by hackers can be extreme, such as hackers exploiting vulnerabilities of a simple sensor that took down Colonial Pipeline, a major energy supplier in the Eastern portion of the US.

There is growing consensus, in both the business and legal world, that dealing with data security revolves around several key strategies, including designating a specific board committee responsible for data integrity, contingency planning for how to handle data breaches, and significant vetting of vendors and suppliers.

To help our customers, we are providing independent 3rd party penetration reports on our website. Further, we have self-certified to United States cybersecurity standards outlined in NIST 8259A. It is our intent to be transparent and proactive in providing this type of information such that your firm can properly handle data security.

Penetration Testing Reports

NIST 8259A Compliance

Patents Pending

Feel free to pass this on to interested colleagues