Read Our Latest COVID-19 Updates

The Low Tech Approach to Help Reduce Your Company's Data Breach Risk

By: John C. Babione, CEDS, CIPM, CIPP/US

Headlines about Meltdown and Spectre, two recently discovered computer chip security vulnerabilities, add to the long list of reasons to worry about the risk of data breach. But they also serve as reminders to be vigilant because there are many ways businesses may become vulnerable to a data breach.

Human nature encourages business owners and employees to underestimate their chances of being the victim of a data breach by reasoning that their business is "not large enough" or "not important enough" to be a target. Unfortunately, in today's world of cybercrime, many attacks are part of automated processes where criminals use technology to scan the internet looking for vulnerabilities. If you have an unpatched security flaw, criminals may catch your business in their "net" without specifically targeting you. To make matters worse, there are many other ways your business may become a victim regardless of your size or perceived importance, such as your relationship to another entity that may be the actual target. If your business is the "weak link" used to connect to and breach your business partner, that will damage or end that relationship.

While firewalls, vulnerability patching and other technical defenses are a critical part of a well-planned strategy to protect against data breach, there is a low-tech approach you should employ simultaneously to reduce your financial risk – Information Governance. Information Governance, or IG, involves strategically planning how your business collects, stores, uses and disposes of information. Besides many other business benefits, implementing a well-crafted IG plan significantly lowers the financial risk from data breach in two critical ways. First, IG may prevent a cybersecurity "incident" from becoming a "breach." Second, if a breach occurs, part of your IG plan should include a response plan which will reduce the costs to respond compared to the calamity of facing a breach without a plan in place.

Regarding prevention, while most security experts agree that it is virtually impossible to stop 100% of cyber-attacks, those attacks that get through your defenses do not necessarily have to become an expensive data breach. The legal definition of what qualifies as a breach involves a fact sensitive analysis depending upon the laws governing your industry and jurisdiction. But to generalize, if you can keep the hacker from getting to sensitive data covered by state data breach laws and other privacy-related regulations applicable to your business, you likely save your company significant money by limiting the event to an internal incident. If instead the attacker gets to the sensitive data and you have a breach, the consequences are much more expensive and public, including: significant investigation and legal costs, breach reporting costs, damage to your brand, lost customers, potential lawsuits and business downtime.

Here are two examples of how IG might help with breach prevention:

- IG will include analysis of the information your company is collecting to determine if you truly need it for business reasons. For example, your employees may be collecting customers' full driver's license numbers or copying licenses as part of a standard process to confirm identify. However, there are likely other ways to accomplish the same objective without accumulating this sensitive information. If your company does not collect or retain this data, then hackers cannot access it and there can be no breach.
- IG will direct company employees how to protect data that is collected. Your employees may be storing financial account numbers, social security numbers or other sensitive data in their email folders or in unsecured network drives. If they instead stored that information within an encrypted file management system, the encryption may prevent an incident from becoming a breach if the hacker cannot access the data.

Although breach prevention is reason enough to implement IG, there are other benefits such as improved business efficiencies from organizing company data flows. In addition, IG moves an organization toward the state of "Litigation Readiness," which involves proactively managing data before becoming involved in litigation. This allows a more cost-effective defense when litigation arises.

For more information on Information Governance, Litigation Readiness and discovery of electronically stored information (ESI), please contact the members of Wooden McLaughlin's E-Discovery Practice listed below. And, visit our new blog – Wooden's GPS for E-Discovery – found at WoodenLawyers.com.

John C. Babione, John.Babione@WoodenLawyers.com

James M. Boyers, Jim.Boyers@WoodenLawyers.com

Robert J. Simmons, Robert.Simmons@WoodenLawyers.com

Attorneys

- John C. Babione

Practice Areas

- E-Discovery & ESI