The Need for Enhanced Risk-Based Information Security Policies with a Remote Workforce

By: Kevin D. Pomfret

03.31.2020

For some time, government agencies such as the National Institute of Standards and Technology (NIST) have recognized that a ?one size fits all approach? is not practical from an information security standpoint. Instead, companies were encouraged to take a risk-based approach and develop information security policies that were aligned within the context of their business operations. As a result, while both an international public company, with a large distributed workforce and offices across the globe, and a smaller company with one or two offices and a limited number of employees, were expected to have adequate information security in place, the determination of what was considered adequate was significantly different because their risk profiles were very different.

However, one of the impacts of COVID-19 is that businesses are now operating with most, if not all, of their staff operating from home. This changes the information security risk profiles for many organizations. As a result, companies of all sizes should review their existing information policies and procedures to verify that they address the additional risks associated with what are essentially numerous satellite offices. In addition, they should continue to keep abreast of cybersecurity developments as there are reports that criminals and nation states are attempting to take advantage of the new entry points into organizations through the distributed workforces.

Here are some measures to consider:

- Putting enhanced security features, such as multi-factor identification and encryption, into place;
- Updating policies and training associated with personal and sensitive data for remote workers. (In the interim, it might be helpful to send all employees this useful link from NIST.);
- Reviewing cybersecurity insurance policies to ensure that coverage applies to remote operations and whether limits are adequate;
- Building redundancy into authorizations for money transfers, so as to counter increasingly

sophisticated spear phishing efforts targeting finance departments; and

- Updating (or developing) the company?s incident response plan in the event of a cyber incident, as in such matters every minute counts, and notification and coordination will get more challenging with a distributed workforce (and advisors).

Another benefit to updating information security policies and procedures is that it may provide additional legal protections in the event of a data breach. For example, a recent Ohio law provides safe harbor from the state?s data breach provisions for companies that have implemented cybersecurity measures that conform with recognized information security frameworks: many of which provide for a risk-based approach.

If you have any questions about this topic, please contact Kevin Pomfret.

Please note: This alert contains general, condensed summaries of actual legal matters, statutes and opinions for information purposes. It is not meant to be and should not be construed as legal advice. Readers with particular needs on specific issues should retain the services of competent counsel.

Please click here for additional legal updates from Williams Mullen regarding COVID-19.

Related People

- Kevin D. Pomfret ? 703.760.5204 ? kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity