How Vulnerable Is Your Business to a Cyber Attack or Data Breach?

Description

By Colin Coleman, John Ottaviani, and Brian Reilly

January is a good time for all businesses to review and update their cybersecurity policies and practices.

We are only a few days into 2019, and already we are hearing breaking news about new data breaches. The German government suffered a breach involving many prominent politicians and celebrities. Not all of the breaches are by hackers. Singapore Airlines announced that changes to its software in early 2019 allowed some members of its frequent flyer program to view the personal information of other members. These breaches were all preventable with proper diligence by the affected organizations.

January is typically a time for businesses to make plans for operations, marketing and sales for the upcoming year. It is also an excellent time for all businesses to review and update their information security policies, practices, and technology. Although the needs of each business will be different, businesses should focus on the following areas:

Review and Update Your Policies, Procedures, and Technology. Consider the cyber-security risks associated with your lines of business, products and services, systems, devices, employees and vendors, particularly new ones. Do you need to update your business's policies to address growing cyber risks? Is your business dealing with new kinds of personal or confidential information than in the past? Are the appropriate contract provisions in place, particularly with vendors, to protect personal information adequately? Now is the time to review and update your business's policies, and to add new policies, procedures, and technologies to fill in any gaps.

Maintain and Improve Awareness. Adopting the best policies and technology to protect your business can only go so far. That is why employee security awareness and data loss prevention training are critical to minimize data breaches. However, threats change, systems change, and people forget. Businesses should conduct frequent trainings to help employees recognize and respond appropriately to suspicious behavior. While the details may differ, your business should conduct training at all levels of the organization. Now is the time to plan and schedule the training sessions throughout the year, and to make a plan to ensure that all of your technology systems are consistently and properly updated over the course of the year.

Do Some Housekeeping. Many homeowners "clean house" periodically and throw away or give away unwanted items. A business also should take inventory and reduce the amount of information it is collecting and storing. You can reduce the harm from a breach by minimizing the amount and types of information you collect to only that which is necessary. As part of the periodic housekeeping process, you and your employees should also change your passwords and confirm that you do not use the same password for multiple accounts.

If you need help reviewing existing policies or creating new ones, or you would like to discuss ways to help prevent becoming the victim of a cyberattack or scam, please contact Colin Coleman, John Ottaviani, or Brian Reilly at Partridge Snow & Hahn LLP.

Date Created
January 10, 2019