LEGAL ADVISOR

A PilieroMazza Update for Federal Contractors and Commercial Businesses

Hackers Are No Match for Employee Missteps

By Nichole Atallah and Tony Batt

Do your employees understand how they might be exposing the company to risk simply by working remotely, losing documents, or failing to properly discard information? Imagine John Doe has access to company files and emails on both his laptop and cell phone. One day, John stops by a local coffee shop and logs into its free, public wi-fi on both his work phone and his laptop. Just as John starts sipping his coffee and checking his work email, he unknowingly becomes a victim of a hacker. Because of John's carelessness, this hacker now has access to all of the company's proprietary data and sensitive client information that John could access.

In an age where large companies, such as Target Stores, Sony, Marriott, and Yahoo!, have all scrambled to address data breaches, the external forces and highly technical defenses that are at issue often garner the most attention. However, poor data security culture and policy breakdowns can lead to data security vulnerabilities that are equally, if not more, damaging. In a 2018 survey of business owners by Shred-It, an information security company, 47 percent of business owners reported that employee negligence relating to documents or internet use had caused a data breach within their organizations.

Whether you are just turning toward cultivating a work environment that emphasizes data security or have been focused on this issue for years, below are five recommendations any company should consider implementing as front line defenses against a data breach.

TIP 1 Create a Culture That Values Protecting Information

The value employees place on protecting company information starts at the top. It is important to evaluate how your organization can emphasize the critical role employees play in protecting information and how seriously the company takes violations of company data security policies. Creating this culture necessitates a review of internal policies, but efforts cannot stop there. Management teams need to ensure that those policies and best practices are communicated clearly and frequently.

TIP 2 Evaluate Internal Data Protection Controls

In light of evolving requirements for government contractors and new laws that govern data protections at the state level, it is important to ensure that your internal data security protections are up to current standards. For example, your company should have a process for regularly updating anti-virus and malware protections and ensuring proper password protection. Passwords should be sufficiently complex and not duplicative of any passwords an employee has previously used for any other website or application. In addition to information technology controls, there are often documents with sensitive information in print that need to be protected. It is important to have processes for locking up sensitive data, properly discarding of documents no longer in use, and taking print data out of the office.

TIP 3 Consider Additional Protections for Remote Work

Although the best protection against data vulnerability due to using untrusted networks is to completely abstain from using them, this option is not practical for many

Continued on page 2

PILIERO MAZZA

businesses. Employers can reduce the risk of a security incident by requiring employees to use a mobile hot spot or a cellular tether to access information in remote, unsecure locations, or providing employees with a Virtual Private Network (VPN) to encrypt traffic over the internet. Also, for employers that allow employees to use their own cell phones and/or laptops to access work material, it is essential to have a clearly established Bring Your Own Device (BYOD) policy that includes a requirement for employees to maintain passwords on those devices as well as pre-approved anti-virus and malware protection.

TIP 4 Do Not Get Overwhelmed

Data security compliance and risk can be overwhelming to companies that already have a lot on their plates and are concerned about managing the process and related costs. Rest assured, there are ways to manage cost and resources, while also taking into consideration reasonable, business conscious measures. Additionally, there are increasingly more federal and state programs that provide financial assistance to help companies minimize data security risks.

TIP 5 Ask for Outside Help

There are a number of consultants that provide services to companies of all sizes to assess system vulnerabilities. Moreover, legal counsel can assist in ensuring your policies and practices meet the applicable legal standards. In the event of a data breach, it is important to seek assistance to understand the scope of potential legal liability and to mitigate these risks as quickly as possible.

About the Authors: Nichole Atallah is a partner and heads the Labor & Employment Law Group. She may be reached at natallah@pilieromazza.com. Tony Batt is an associate in the Litigation, Labor and Employment Law, and Business and Corporate Groups. He may be reached at abatt@pilieromazza.com.