Will You Be Next?

Protecting Your Business Against Cyber Attacks

By Matthew D. Berkowitz, Esq. and Brian O'Shea, Esq.

Cyber hacks and data breaches have become an everyday occurrence and have catastrophic effects on businesses. In 2018 alone, there were almost 1.3 million reported data breaches in the United States with almost 446.5 million records exposed.[1] According to the White House Counsel of Economic Advisors, malicious cyber-activity costs the United States economy between $57 billion and $109 billion.[2] The average cost for a business to recover from a single data breach is $3.86 million.[3] And it is not just large national or multi-national corporations that are affected. Small and medium-sized businesses are even most at risk. More and more, hackers are targeting small "mom and pop" retailers, hotels and hospitality businesses, law firms, accounting firms, medical providers, or any other business that maintains sensitive and confidential information about its customers or clients.

As the number of data breaches has increased, so has the number of data breach class action lawsuits. These class actions are often expensive and difficult to defend. There are a number of legal defenses available to the business owner. These defenses include "standing," meaning that the plaintiffs must suffer an actual injury-in-fact (not just hypothetical or speculative) for the court to have "jurisdiction" and consider their case; "ascertainability," – in simplest terms, that the potential class of plaintiffs be identified through objective criteria; and "predominance," which means that issues common to class members, such as damages, are common to the class as a whole, so the court can avoid a series of mini-trials. Despite these defenses, courts often allow data breach class actions to move forward. Therefore, it is imperative for businesses who have suffered a data breach to retain skilled and experienced class action attorneys, even before a suit is filed. The right attorney can employ strategies to defend against potential liability and limit economic damages and reputational harm.

But the best defense to limit liability and exposure is for businesses to take affirmative steps to prevent a cyber-attack or a data breach in the first place. There are a number of actions that even the smallest of businesses can take to save themselves from potential financial ruin. First, businesses should hire an IT consultant or an in-house expert to assist in managing and protecting the company's network and the sensitive information they maintain. From there, and with the help of the IT professional, businesses should inventory the sensitive data. Questions to consider include: What sensitive data is maintained? Where is it stored? Who has Access? And How is it protected?

To further protect data, and again with the help of an IT professional, businesses should use encryption and firewalls, and consider storing their servers with third-party vendors. Businesses should also limit the number of employees who have access to the sensitive data to only those with a need to access it.

Furthermore, businesses should implement robust policies and procedures and give comprehensive training to their employees regarding the storage and protection of sensitive data. The importance of protecting information should be reinforced. Employees should use the same efforts to protect information in cyber-space that they use to protect confidential information locked in an office file cabinet. Employees should also be required to use sufficiently complicated passwords and two-factor authentication to access the network. Employees should also be trained about "phishing" and malware. Finally, businesses can further protect themselves by purchasing cyber-insurance policies.

Cyber-attacks and data breach class action lawsuits are not going away. They will only continue to increase and will become more expensive and difficult to defend. By taking the simple protective measures outlined above you can improve your chances of not being hacked. If your company does experience a data breach be sure to retain an experienced class action attorney, to minimize the risk and avoid the fate of so many, potential extinction of your business.

---

[1] The Statistics Portal, Annual Number of Data Breaches and Exposed Records in the United States from 2005-2018 (in millions) (2018), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[2] The Council of Economic Advisors, The Cost of Malicious Cyber Activity to the U.S. Economy (Feb. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[3] IBM, Cost of a Data Breach Study (2018), https://www.ibm.com/security/data-breach.