SAEED & LITTLE
ATTORNEYS AT LAW

Is It Time To Rethink Your Company's Cybersecurity?

As a small business owner, you may not consider cybersecurity one of your top priorities. Especially if you have a limited online presence. However, that kind of thinking can leave your company seriously vulnerable to hackers and a rapidly increasing number of online threats.

The threat against small businesses is at an all-time high. In fact, more than half of all small businesses suffered a breach of client data, according to a recent study by Hiscox insurance. The pandemic has only added to the risk. With more and more employees working remotely, where they often use unsecure public networks, shared personal computers, and mobile devices, businesses are more vulnerable than ever.

As a result, the FBI reports a 400 percent increase in cyber attacks since the pandemic began. The cost to resolve a single data breach averages roughly $200,000, and some 60% of small businesses that suffer a cyber attack go out of business within six months. If you haven't taken your company's cybersecurity seriously, you most definitely need to start. https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html

While you should consult with a cybersecurity specialist and your business lawyer to implement a comprehensive digital protection plan, taking the following five actions can help protect your business from cyber threats and minimize the damage should you experience a breach.

1. Install Multiple Levels Of Security
Protect your company's network, servers, and computers with a comprehensive array of cybersecurity systems, such as anti-virus software, firewalls, intrusion-prevention systems, and anti-subversion software. The key is to add as many layers of security as possible, since hackers are likely to move on to an easier target if your network and devices are well defended.

Remember to regularly install updates to your security software so you'll be protected against all of the latest threats. Regularly check your software vendors' websites and the U.S. Computer Emergency Readiness Team's website to stay up-to-date on the latest viruses, vulnerabilities, and patches.

If you don't have one already, consider hiring a dedicated IT specialist whose job is to prioritize your company's cybersecurity, keep your systems updated, and provide cybersecurity training to the rest of your team. If you can't afford your own IT specialist, you can outsource the job to an outside firm that specializes in small business cybersecurity.

2. Educate Your Team
Oftentimes, your own employees are your biggest security risk. It's essential that you train your team how to recognize and defend against email phishing, social engineering attacks, ransomware, and other cyber threats. You should also train them in cybersecurity best practices, and ensure they are aware of the potential cost a data breach can have on your business—and their livelihoods.

Some 63% of data breaches occur due to weak, default, or stolen passwords. Given this, implementing and enforcing team-wide password protocols, limiting who has access to sensitive data, and requiring frequent password resets is one of the easiest and most effective ways to beef up your cyber defenses. https://www.fundera.com/resources/small-business-cyber-security-statistics

For best results, document your password protocols and other cybersecurity policies in a standalone resource that your team can easily reference if they have any questions or issues with cybersecurity. Make cybersecurity education a part of your onboarding, and require training updates in response to new threats and implement enhanced security measures.

3. Partner With The Most Secure Web Hosting Service
Web hosts house your website, online applications, and other data on off-site servers. There are numerous web hosting services available, and they come with varying levels of server-side protection, including security cameras, anti-virus and anti-spyware systems, and hard-wired firewalls.

Choose a web host that offers a high level of security, especially against cross-side server attacks, which involve hackers who open a fake account with the web host to access other websites on the same server. For enhanced protection, use a virtual private server (VPS), which partitions your website from other sites that share the same server.

For maximum protection, open a private server account in which your website and data are maintained on your own separate server. This option can be pricey, but it's still a lot cheaper than getting fined or sued for a data breach.

3. Invest In Cyber Insurance
As with other forms of liability your business faces, having the proper insurance in place is a key component of your company's cybersecurity plan. Cyber insurance offers protection against damages resulting from data breaches, hacking, network failures, and other events. If your business' network is breached, the cost to recover and restore this information can be

extensive. You can also be held liable for damages to third parties such as customers and vendors, whose data was lost or stolen from your system.

Depending on the coverage, cyber insurance can pay for a wide array of services needed to repair your network and retrieve your data, including investigative analysis, business interruption, and data recovery. It can also cover the cost of notifying clients of the breach, paying regulatory fines, as well paying for lawyer fees, judgments, and settlement costs resulting from a lawsuit.

Not all businesses need cyber insurance, and the ones that do can require varying levels of coverage. Before you buy a cyber policy, consult with us, your business lawyer, to assess the risk your particular business faces and determine the kind of policy best suited for your operation.

4. Hire Cybersecurity Professionals

If you are in an industry that's at high risk for cybercrime, such as finance, banking, healthcare, or logistics, consider hiring an outside cyber security firm to monitor your company's network and computer activity. These experts are specifically trained in the latest trends in hacking and other cyber threats, and they can add an extra layer of protection when combined with your own in-house IT specialist.

That said, such security firms are often quite expensive, and not all businesses will need to partner with one. As your business lawyer, we can help you better assess the risk and reward of hiring these specialists and advise you on whether your company requires such an investment or not.

A Strong Digital Defense

Regardless of the size of your digital footprint, you should stay apprised of the latest cyber threats to ensure your sensitive business and client data has the maximum level of protection. As your business lawyer, we can advise you on the different safeguards you should have in place and keep you updated on the ever-changing legal landscape surrounding data privacy. In addition, if you're ever hacked, we can defend you in court against any lawsuits or other liabilities that might result. Contact us today to learn more.

This article is a service of Saeed & Little, LLP. We offer a complete spectrum of legal services for businesses and can help you make the wisest choices on how to deal with your business throughout life and in the event of your death.