WHY Cybersecurity Matters To Your Business

You start a business. You grow your company from an idea to a fully functioning and profitable entity. With success comes clients and, as with most companies, you store personal information either to be used in marketing or from a purchase. As a result, you hold the keys to many of the things that your customers value and treasure in their lives and it is now your responsibility to protect their personal information. Additionally, your company has a myriad of confidential and private information internally that needs to be protected.

The premise is simple: Protect your company's data along with your customers' data. But the execution is complex. Over the past several years we have learned this fact as companies -- from the retail giant Target to the credit reporting service Equifax -- have fallen victim to cyberattacks.

While cybersecurity tools, consultants, software and hardware are all handsomely expensive, none of them have the immediate positive impact on bottom lines that other technologically centered additions do. This means that it is just not as fun to invest in cybersecurity products and services as it is to outfit your team with lightning-fast laptops. Still, a sound cybersecurity plan and deft execution can be an amazing selling point for customers and clients as awareness grows across society at large. Here are a few ways to take control.

Understand Cybersecurity Applies To You

The first step to protecting your business is to understand that the threat is real. Many times when news of wide-scale data breaches flood Facebook feeds and media outlets, business owners take solace in the fact that while Target may have been hacked, their company is too small to be at risk. This is a false sense of security. According to Symantec, over 43 percent of cyberattacks in 2015 were targeted toward small businesses — and this number will only rise. Furthermore, only 14 percent of small businesses believe that their current ability to guard against cyberattacks is effective. Thus, cybersecurity is a small- and medium-sized business problem -- one most are not addressing properly.

Seek (Quality) Advice

No matter what type of business your company conducts, even if it is technology-based, your business can benefit from an outside set of eyes. The technology and data surrounding cybersecurity are constantly changing and evolving. This means that while you may have some of the most brilliant tech minds around grinding out your code, their focus is not necessarily security -- and the result is vulnerability.

Accordingly, it is totally acceptable, if not necessary, to work with a cybersecurity professional. A simple Google search for "cybersecurity services" will yield thousands of results. Not only will consulting a professional make your operations more secure, but this contact will go a long way. In the event that a cyberattack happens, the contact will fend off would-be lawsuits by showing that you took adequate measures for security.

Build Your Plan

As part of any consulting relationship or ongoing monitoring facility, all companies must develop a cybersecurity policy and defense plan. This plan must detail what measures the company will undertake to make sure that employees and networks are protected from unnecessary threats. Additionally, the policy must outline what precise steps each employee of the company must take each day to ensure that company and client information is protected.

Finally, every cybersecurity plan should include a process for what to do once a cyberattack occurs. These types of plans include a great deal of detail that is appropriately tailored to a business given what industry it is involved in. A cybersecurity plan for a fintech operation or health data company may be significantly more detailed than one for a regular e-commerce operation, but both plans will have the same underpinnings. This type of a plan can be performed in-house, but generally, cybersecurity consultancies will include this plan in the cost of their audits or as part of ongoing monitoring.

Get Yourself Covered

The final piece of the puzzle regarding cybersecurity is to consider whether or not cybersecurity insurance is a smart option for your company. One of the scariest facts about cyber breaches is that for many small- to medium-sized businesses, once a breach occurs, the business itself ceases to exist within a year. The appeal of cybersecurity insurance is that it can, at least in theory, shift the risk of an attack from your business to the insurance company. After all, insurance companies are very good at managing risk, while most businesses are not.

That said, insurance alone cannot be called a cybersecurity plan, and most policies will include strict provisions dictating what specific measures must be undertaken by the company in order to receive coverage. This means that if there is an attack and a loss and your company files a claim, the insurance carrier will verify to make sure that you were in compliance with the necessary policies and procedures before paying the claim. As such, cybersecurity insurance policies are a great tool for forced compliance with cybersecurity plans.

Finally, while cybersecurity insurance can offset the losses in conjunction with a cyberattack or breach, it does not repair the lost brand equity or reputation that often flows from an attack. Still, it is a valuable asset to consider in the fight against cybercrime.

As you and your company evaluate your risk and exposure to cyberattacks and data theft, remember that there is no avoiding the impact that this new threat has on all businesses of any size. Do not fret, however: There are great resources at your disposal and an army of experienced professionals waiting to lend a hand along the way.

Source: Forbes.com by Ryan Bradley