Cybersecurity Tricks and Tips for Growing Businesses

03.18.20

It's been recognized for some time now that small businesses shoulder some of the biggest cybersecurity risk burdens. Yet many of them are still unprepared. If you think your small business's cybersecurity efforts could use a boost, then read on to discover what cyber security tricks and tips BPM's InfoSec team has to help you put together a cybersecurity plan.

Small business are not insulated from the growing amount of cyber-attacks today. In fact, small businesses are increasingly the targets of hackers and scammers, with 43% of online attacks now aimed at them by cyber criminals. That's because it's easier to exploit popular attacks like phishing or spreading viruses against organizations without a robust cybersecurity function, as is the case most growing businesses.

All that makes the mentality of "what could I possibly have that scammers would want?" particularly dangerous. Everybody has something to lose from a cyber-security incident, and small businesses especially, given that 60% of them go out of business within six months of suffering an attack.

If your business needs a cyber-security plan, or needs to bolster the current one, consider this the motivation you need to change that. But to completely overhaul how your organization treats cybersecurity, what you'll need is a plan.

Cyber-security Plan Should Start With Awareness

Everybody knows the importance of cyber-security. But most employees, whether the business is small or large, may not take it as serious as business leaders. Often, that's not because employees are lazy or lackadaisical; it's because management doesn't typically drive home the seriousness of the issue.

What's required for a company to stay vigilant against the multitude of online threats aimed at their way is a culture of cyber-security awareness — a culture in which cyber-security is a key consideration in every decision, from deciding whether to open shady links or how to customize enterprise applications. And that kind of culture can only be implemented top-down.

That's to say, the first cyber-security tip is beginning your plan with Management training. Management needs to make it clear through policy and actions that cyber-security is a priority. There's a number of ways they can do that, whether it's through participation in cyber-security awareness days or months, or discussing effective cyber-security tips in monthly or quarterly letters to employees. The point is, you can't just leave it up to employees to guard against cyber-security risks — you have to demonstrate you're just as invested as you want them to be.

Develop a Cyber-security Plan by Using the Resources Available to You

The National Institute of Standards and Technology, or NIST, is government agency overseen by the Department of Commerce that primarily develops references materials for businesses in the tech and science industries. The company's cybersecurity framework, aimed at helping companies reduce the cyber risk to their critical infrastructure, codifies existing standards, guidelines and practices into a single, digestible document. The NIST framework's prioritized, flexible, repeatable and cost-effective approach makes it an excellent approach for companies trying to reduce their cyber-security risk.

For that reason, we recommend business leaders start here for a comprehensive understanding of what business treats exist, and how to guard against them. It's written in easy-to-understand, accessible language, so you can gain a workable understanding of the various elements of a cybersecurity plan in a relatively short amount of time. Moreover, NIST has already done a lot of the work of putting together a plan for you, including categorizing the distinct functions of a cyber-security program, providing recommendations and examples of implementation, and defining different tiers of cybersecurity rigor so you can build a roadmap for your small business. It's no wonder, then, that more than 30% of all U.S. organizations already use the NIST framework to manage their cyber-security of risk.

Cyber-security Tricks for Creating Secure Passwords

One of the easiest projects with the highest impact a small business can undertake is making regular password training for all individuals mandatory — executives especially. The reason? C-level leaders present the greatest business risk if their personal information or online account is hijacked. At a small or medium business, these leaders might have admin access to items like company credit cards, to payroll with SSNs and other data, to company IT — you name it.

That's why it's so important that everyone at your company practice good password management. That includes practices like not reusing passwords across multiple accounts, using long, secure passwords that can't be easily guessed and securely storing passwords on the backend. To achieve good password management, you'll want to host quarterly or semi-annual password trainings so you're constantly reinforcing the importance of strong cybersecurity practices. Returning to the statistic that 6 in 10

companies go out of business within six months of a major cybersecurity incident, organizing regular security awareness trainings could quite literally save your company.

As you start to plan your regular password trainings, encourage your staff to avoid biometric passwords, because if that data is stolen – well, changing your face is much harder than changing a typed password. Watch BPM's password management webinar to find out more about this topic and other tips to convey at these trainings.

Proactive Cyber-security Measures

We understand leaders of a budding business have limited time to focus their attention on anything else outside of reaching their goals and growing their company. If cyber-security is one of those tasks you know is important, but you don't think you have the bandwidth to take on, an outside security operations center may be the answer to this problem.

By hiring a managed security service provider, you can worry less about inevitable cyber-attacks since you know there's a dedicated team of security professionals on your side. Managed security providers work with you to create a plan based on existing IT systems, identify where your potential threats exist and recommend policies and technical rules to protect your business. These providers will "continuously monitor", prioritize, and test your infrastructure to ensure threats are identified and avoided immediately. They often integrate with your ticketing and call workflow systems to provide the fastest services possible, while staffing 24X7 for you.

BPM's Security Operations team has the experience and skills to be your managed security service provider, so your internal team can focus on upcoming and future goals without worrying about inevitable cyber-security threats. With more than 15 years of experience, we make it quick, painless and cost-effective to implement a security operations center that fits the needs of your business and industry.

For other cyber-security testing requests, BPM's Information Assessment Security Services group understands how to balance information security and business needs. Our team performs a variety of tests and reviews, including the Comprehensive Penetration Test and Information Security Program Review, to identify vulnerabilities in a client's IT infrastructure, allowing companies to make well-educated decisions on where to best allocate resources.