What SMBs need to understand about cybersecurity

Let's start with a "fun fact": In 1981, the first cybercriminal was convicted of hacking into the AT&T network and altering its internal clock so it charged off-hour rates at peak times. So, it turns out that cybercrime is not all that new. But it stays new in the sense that it is constantly evolving. Cybercriminals now target not only big businesses like AT&T, but also small- and medium-sized businesses. In fact, a recent study pointed out that SMBs are increasingly becoming targets of cybercriminals because their cybersecurity measures aren't as strong, sophisticated, or effective as those of large companies. Often, SMB owners tend to think they are too small to be targeted; in fact, their size and lack of cybersecurity measures make them an easy target for cybercriminals. This whitepaper focuses on what small and medium-sized businesses need to understand about cybersecurity.

One of the first things to understand is–no matter how lucky or careful you are– cybersecurity breaches are bound to happen. You are, at any point in time, just one click away from getting your entire IT network or data compromised. While this truth is the same for both smaller and bigger organizations, as an SMB the impact on your business, revenue, and brand is likely to be far greater when compared to a bigger company.

Second, the landscape of cybercrime is constantly changing. The more security features and components you have in place, the more cybercriminals are changing their tactics. So, you need to be constantly on your guard to keep up with them and fortify your IT infrastructure from a security perspective.

Third, the results of a cyberattack are far-reaching. If you think getting your stolen data back or your system back up and running is the end of a cyberattack episode you are wrong! No matter what industry you operate in, there are certain compliance and regulatory requirements that need to be followed. Apart from the obvious damage to immediate business revenue and reputation

caused by business interruption and downtime, a data breach has far-reaching consequences on the legal front as well. Many firms never recover. Along the same lines, did you know that there are situations wherein you don't even have to be the actual target to be the victim of a cybercrime? Sounds crazy, doesn't it? But it's true. If you have vendors or subcontractors with whom you share business data, a data leak at their end could implicate your business as well.

The fourth and perhaps the most important element here is ensuring that you, as an organization, understand that cybersecurity responsibility has to begin at the C-level executive office. Like all successful corporate priorities, the initiative and drive has to start at the top. But it cannot end there. It has to be a top-down approach, whereby C-level leaders consider cybersecurity to be a priority. But it is not up to the CEO or CTO alone to ensure its success. Like we said before, all it takes is one click and your entire IT infrastructure can come down like a house of cards. And that one click can come from anywhere. It could be Brenda from accounting who thought the link Sam from finance was sharing had cute dog pictures. What's worse, it doesn't even have to happen at work or on one of your computers in the office. With remote work and BYOD becoming the norm, one of your employees using their phone to check or reply to a work email can become an infection source unintendedly. What does this mean? Education at the level of the individual employee is critical to the success of your data hygiene initiatives. Everyone on your team has to have an understanding of the dangers lurking in cyberspace and learning how to identify and avoid cyberthreats such as phishing, clone sites, ransomware, virus and other malware.

Cybersecurity has to be a conscious decision. It is not something to be taken lightly or something that you can engage in passively as though it were yet another random business requirement. In order to stay safe in today's highly vulnerable environment, businesses need to focus on cybersecurity and have clear cybersecurity strategies and action plans in place. This also means budgeting appropriately to support the process. Also, remember, creating a safe cyber space in your organization isn't an idea that starts and ends with IT. Human Resources is a critical component in the design and implementation of any cyber security strategy. Often, SMB owners feel investing so much into IT doesn't offer great returns--which may be true in some cases. Some of the reasons for this include

a) Your in-house IT staff may not have enough work to stay occupied full-time

b) When you have an in-house IT team, there are other costs that come with it, that are generally HR-related, such as training costs, employee benefits, medical insurance, 401(k) etc.,

As a result, sometimes, SMBs tend to resort to the firefighting approach to IT problems, which means, they reach out to an IT service provider when they face an issue.. However, more often than not, it is too little, too late and also, too expensive. Since effective cybersecurity should be a proactive effort, not reactive, this means that SMBs tend to overlook the entire issue as something to push forward into the future

One way to get around this challenge is to have a service level agreement with an MSP. An SLA with a managed service provider offers multiple benefits such as-

a) The obvious one is, you get the benefit of their expertise. An MSP's core job is managing IT infrastructure, so when you bring an MSP onboard to manage your IT infrastructure, you get access to their unparalleled knowledge and expertise, which your internal IT team (even if you have one) may be lacking.

b) Having an SLA ensures that the MSP prioritizes you over other 'Firefighting' customers and situations, meaning they are there when you need them.

c) Your IT infrastructure is consistently monitored and maintained. Depending on the inclusions in your plan, outsourcing your IT to a managed service provider usually takes care of all the mundane, but essential elements of cybersecurity including backups, data recovery, security patches, system upgrades, etc.

d) Overall, it can help you bring down your IT costs as your payroll expenses in terms of IT can be trimmed or eliminated in some cases.

e) Having a managed service provider helps you scale, as they can manage the sudden spike and slumps in your IT infrastructure requirements that may be fuelled by various factors such as the holiday season, staff going on vacation, tax seasons, etc.,

f) A managed service provider can help you draft the right cybersecurity plan for your business and also help you implement it effectively. Further, they can help manage the plan in the long run, ensuring that all the necessary elements are in place and functioning as they are supposed to.

Cybersecurity shouldn't be an afterthought. It is one of the fundamentals of your business structure and should be a part of your core business process. Consult a managed service provider today to learn more about what you can do to keep your business safe and secure from cyber-attacks.