techradar pro

Cyberattacks: where can small businesses turn to for help?

Sharp offers solutions for SMBs to overcome cyberattacks

By Newt Higman
September 8, 2020

(Image credit: Altalex)

Small and medium-sized businesses (SMBs) have always been more susceptible to cybersecurity threats. This is because they often lack the resources of larger enterprises to invest in better solutions that will protect them from the various dangers present in an increasingly mobile and digital world. COVID-19 has only made it worse, leading to a sharp spike in global cyberattacks since the start of the pandemic.

In a recent op-ed*, Senator Jim Risch (R-ID), who serves as chairman of the Senate Foreign Relations Committee and is a member and former chairman of the Senate Committee on Small Business and Entrepreneurship, noted that a strong cybersecurity strategy is no longer a luxury for small businesses – it is a necessity. With organizations shifting to a digital economy and distributing applications to the public cloud, IT infrastructure has become even more complex, which in turn has exacerbated the cybersecurity risks for these businesses.

The changing IT landscape

In addition to building up their cybersecurity protocols, SMBs must deal with growing amounts of data to manage and an increase in the number and types of devices to support. In many cases, this increase is the result of bring-your-own-device (BYOD) initiatives, where employees may be using a wide range of technological solutions. This, of course, brings its own security issues, including potential for data theft and malware infiltration. These organizations are distributing applications to the cloud, and as such, must ensure they are managing and supporting these additional intricacies with both on-premises IT equipment and potentially multiple public cloud environments.

It will be critical for organizations to better protect themselves from these security incidents to ensure continued operations. This is especially true considering the severe impact these events can have on businesses of all sizes, which includes lost productivity, business disruption, time spent solving the issue and loss of data. However, the biggest concern and justifiable fear for SMB owners is that these threats can ultimately put them out of business. As organizations digitally transform to become more agile and responsive to their

**Hyperlinks were added after the original article was published.*

customers, it is important that businesses ensure any new IT initiatives are fully vetted and approved by those overseeing cybersecurity.

Dealing with cyberattacks

In a recent study* by Enterprise Strategy Group (ESG), commissioned by Sharp Electronics Corporation, nearly half of North American SMBs surveyed indicated they had multiple security incidents (an average of three) over the last year. The factors contributing to these incidents can vary, including end-user human error and a lack of cybersecurity training and organizational understanding of cybersecurity risk. However, having a smaller IT team that is unable to keep up with workloads was found to be a major issue. Among SMBs surveyed, 85% said they have, at most, one dedicated security professional on their team, while a third said they have no employees on staff at all focused on cybersecurity. It is clear that SMBs need to find other ways to afford themselves greater protection from cyber threats.

The ESG/Sharp study also found that more than three-quarters of respondents are planning to increase their cybersecurity spend in the next 12 months in order to mitigate these risks. Facing such clear challenges with limited options to hire additional dedicated resources, the vast majority of these companies are turning to managed service providers (MSPs) to improve their security posture and navigate new technology deployments. In fact, 95% of SMBs surveyed said they were using, planning to use or interested in using MSPs. This is especially true for newer, digital-native companies (those in operation for less than 10 years).

With no end in sight to cybersecurity threats, many of these organizations are increasingly looking for MSPs to be strategic partners to help them navigate these issues and provide end-to-end solutions over the long run. Those SMBs that have already started working with MSPs have reported seeing many benefits from these long-term relationships. The study found that eight out of ten respondents pointed to reduced organizational risk from their MSP engagement. Other benefits SMBs identified were time savings (80%), staff freed up to focus on other projects (78%), better service-level agreements (77%), reduced complexity (72%) and cost savings (70%).

The reality is that all companies that rely on IT are facing a complex and ever-changing cybersecurity threat landscape, but few are sufficiently equipped to deal with it. The lack of dedicated resources, IT budgets and skills to deploy and operate cybersecurity initiatives poses serious risks. With so many organizations dealing with multiple security incidents each year, finding the right solutions to these problems must be a top priority. MSPs with the appropriate security skills are beginning to play a bigger role in this equation, providing services for SMBs that often go beyond the capabilities of their limited in-house staff. These organizations should consider MSPs and work with them to reevaluate their cybersecurity strategies. Doing so will help ensure they are protected from cyberattacks

**Hyperlinks were added after the original article was published.*

that could threaten the survival of their business.

- *Newt Higman, National Director, Managed IT Services for Sharp Electronics Corporation.*

SHARP®

**Hyperlinks were added after the original article was published.*