The State of Small Business Cybersecurity in 2021

https://securityintelligence.com/articles/state-small-business-cybersecurity-2021/

May 20, 2021 | By David Bisson

Most business owners are overconfident about their small business cybersecurity postures. Two-thirds of senior-level decision-makers who participated in a 2019 survey said they didn't believe the small- to mid-sized businesses (SMBs) for which they're responsible would fall victim to a digital attack. Within this prevailing view, many respondents didn't view small business cybersecurity as important. Therefore, **they didn't have a plan to protect their employer against digital attacks**.

- 9% of survey respondents cited digital security as the most important factor facing their SMB
- 18% ranked digital defense as least important.
- 60% of business leaders revealed that they didn't have a cyberattack prevention plan.
- 25% of respondents stating that they wouldn't know where to even start with SMB cybersecurity.

What's Behind This Bravado?

There's a tendency for SMBs to underestimate their digital security risks by thinking that digital attackers are inclined to go after enterprises only. But don't let this swagger fool you. It doesn't reflect the reality of small business cybersecurity.

The truth is **threat actors behind today's most common cybersecurity risks go after SMBs in nearly half (43%) of digital attacks**, reported CNBC at the end of 2019. It's thus not surprising that two-thirds of SMBs globally had actually reported a digital attack in the preceding year. (It was even higher for U.S. businesses at 76%, noted the Ponemon Institute and Keeper Security.) Those attacks ended up causing data loss in 63% of cases.

The problem is that SMBs lack cyber insurance and other means that could help them absorb the estimated $200,000 price tag of a data breach. In response, **60% of SMBs that have fallen victim to a data breach end up closing six months later**, reported Inc.

Don't Forget About the Influx of New Tech

The issue is that **SMBs are downplaying the importance of small business cybersecurity** while still expanding their attack surfaces.

Sometimes, they know what's up, while other times, they don't. Take mobile use as an example. Close to half (48%) of respondents said they used mobile devices to access more than 50% of business critical apps, reported the Ponemon Institute and Keeper. That's one percentage point less than the respondents who realize how this practice undermines their small business cybersecurity posture.

It's a different story with Internet of things (IoT) devices, though. Four-fifths of respondents to that same study said that their SMB had suffered a security incident as a result of an unsecured smart product. Even so, just 21% of respondents revealed that they actively monitor their business' IoT devices for security risks.

The Door's Wide Open

The findings discussed above provide a snapshot into how employers think of small business cybersecurity. In the case of mobile, they have employees who are knowingly going against security best practices. With IoT, they have yet to act upon risks that have helped to produce incidents in the past.

Together, **these forces leave the door open for all kinds of threats to ravage SMBs' networks**. Chief among them is ransomware. Information Security Buzz pointed out that more than half (55%) of ransomware attacks now involve companies with fewer than 100 employees. Part of the reason why this is so is because SMBs lack proper data backup solutions. Ransomware attackers figure that small businesses will be more inclined to pay the ransom.

The Way Forward for Small Business Cybersecurity

Small business cybersecurity won't change unless someone at the top supports it. For many, this support is lacking. **Close to a third (32%) of SMB respondents to a 2020 study named a lack of budget as the greatest barrier to digital security.**

Therefore, someone in IT or security might need to try to gain C-suite buy-in for an overhaul. People trying to change this can begin by trying to orchestrate their asks around areas where the business already expects to see growth. That could make it easier for executives to approve funding in those areas.

But first, they need to understand what's being said. Hence why it's crucial for people arguing for better protection to speak the language of risk. Use metrics that illustrate how certain **small business cybersecurity threats undermine the employer's business goals**. This could include creating a proof-of-concept for a proposed solution or process. It should show how it can save the business time and money.

With that buy-in from higher up, they can focus on small business cybersecurity basics. Consider using asset discovery tools to build an inventory of all mobile devices, IoT products and other hardware connected to the network. They can then use network segregation, security configuration management and other controls to monitor those devices within their own network zones. It could also involve pairing those with data backup tools to limit the potential scope of a successful ransomware infection.

Keeping Employees in the Loop

At the same time, they'll want to make sure their employees know what's expected of them. They can **create a small business cybersecurity awareness training program** towards that end. Regular trainings will not only keep employees familiar with their employer's policies, but also keep them informed about some of the new types of attacks in the wild.

Not all SMBs will know how to do those types of things on their own, of course. That doesn't mean that they need to give up, though. It just means they might be better off working with a managed security service provider that has a history of helping SMBs to secure their networks while driving the growth of their business.

No One's Too Small for Small Business Cybersecurity

SMBs make an alluring target for digital threat actors. Like large enterprises, they contain personal data, IP and other sensitive information. However, they might not think need to protect it despite possibly having suffered an attack in the past.

In the end, there's no room for overconfidence when it comes to small business cybersecurity. No business is too small to be targeted. That's why it's essential for SMBs to make some changes and to take their security seriously in 2021