COPY EXCERPT

How a Cybersecurity Breach Could Impact Your SMB

Call or write CopyEngineer to receive a PDF of the complete blog post. Or view it online at:
https://blog.lastpass.com/2017/09/cybersecurity-breach-impact-smb.html/

The threat of cybercrime to small and midsize businesses continues to rise, presenting significant risk to these organizations in particular. For those of you in IT or running your own small business, this isn't news to you, but you might be having a hard time conveying the gravity of the cybersecurity problem to your peers, your CEO, or your employees. To help paint that picture, we've done some digging to get the alarming facts on the real state of security breaches and attacks that present real risks to your business, and why you need to be implementing a cybersecurity strategy.

In a recent study by Kaspersky Lab, 90% of firms surveyed admitted a security incident, and 46% lost sensitive data due to either an internal or external security threat. Verizon, in its latest Data Breach Investigation Report, found "81% of hacking-related breaches leveraged either stolen and/or weak passwords." And Symantec, which tracks cyberthreats through a global network of 98+ million sensors, reported this year that cybercriminals had spawned more than 375 million new, unique malware variants in 2016, and that there are now more than 98 million malware bots lurking in cyberspace.

Meanwhile, the National Cyber Security Alliance reports that more than 70 percent of cyberattacks target small businesses. They also found 60% of hacked SMBs go out of business *within 6 months!*

In other words, it's not a question of IF your business will be attacked. It's a question of WHEN, how severely and… will you survive?

The total cost of a cyberattack on an SMB

A cyberattack can have a massive impact on an SMB, paralyzing operations, damaging its reputation, threatening its existence. Even for those who survive, the repercussions may be felt for years.

Kaspersky estimates that costs incurred by small or midsize businesses to recover from a cybersecurity breach average $46,000. Of that total, $38,000 are spent on direct costs (money paid for professional services to cover lost contracts and downtime), while about $8000 goes toward indirect costs (additional staff hiring and training, infrastructure upgrades etc.). The Ponemon Institute, calculated an average cost per stolen record of $141. Ponemon also estimates that the per capita cost of a cybersecurity breach to SMBs is more than three times that experienced by large enterprises ($1388 vs $431).

copyengineer   B2B Copywriter specializing in technology and software