ENJOY SAFER TECHNOLOGY®

4 STATS THAT WILL MAKE YOU RETHINK CYBERSECURITY FOR YOUR SMALL BUSINESS

4 stats that will make you rethink cybersecurity for your small business

By Stephen Cobb, ESET Senior Security Researcher

For many small businesses, cybersecurity may not seem like a priority. Often small businesses don't have the big-budget IT security that enterprise organizations do, so allocating funds to cyber is often pushed down to the bottom of (or off) the list. Small business owners often believe they don't hold valuable enough information to make them a hacking target, but the reality is, small businesses are often a target for this exact reason. It's the "small business cybercrime sweet spot," as ESET Sr. Security Researcher Stephen Cobb calls it.

In light of National Small Business Week's focus on cybersecurity this year, we conducted a survey to understand the small business mindset when it comes to protecting systems and information. The data gathered from the 500 respondents are enlightening—and suggest steps small businesses can take to improve their security posture now.

1. Twenty percent of respondents said they had no IT security in place at all. This despite the fact that 60 percent of small businesses that

suffer a breach go out of business within six months. Additionally, 35 percent of small businesses say the company "owner" manages IT security for the company. This is not surprising, since small business owners often wear many hats. This just happens to be a big hat, considering that IT security even at the basic level can help thwart an attack and can be a relatively low investment. To start, some basics include employee education and making sure you have a security suite—like *ESET Multi-Device Security*—on all company-issued devices. Also consider you might be required to have certain security policies in place if you are obligated by compliance mandates. Take a look at this "*Small Business Cybersecurity Survival Guide*" for a deep dive.

2. The #1 cybersecurity concern for small business owners/managers is customer data being stolen and exposed. Forty-four percent of respondents marked it their greatest concern. This is not surprising given that a data breach can scare off customers—not to mention larger organizations you may be doing business with. An internet or system failure was the #2 concern. This is important to note because we continue to see ransomware attacks rise—and these attacks not only hold data hostage but also shut down critical systems until you pay.

3. More than 40 percent of small businesses said they don't provide any cybersecurity training or education for employees. The first line of defense against cybercriminals is your own employees. Since many attacks target employees through phishing scams (like trying to get them to download a file or click on a link) and social engineering, make sure team members are aware of what the threats are, can identify them and know the action to take if they suspect foul play.

4. Almost 50 percent of small businesses said they don't have a cyber crisis response plan in place. While we all hope to never have an issue that forces us to open up that crisis response manual, the reality is that both how and when you respond is critical. At a minimum, you should have a basic plan in place (with hard copies accessible should you have a system failure). Make sure to keep a list of critical people within the organization (with contact information) whom you will need to reach in case of a breach or system failure. This might include local law enforcement, an attorney, and any outside IT support or forensics you will need to call upon. Also, make sure you know what type of client data/personal information you have and where it is stored. More tips can be found in our post on *steps to take if your company is infected*.

In line with National Small Business Week's "Dream Big, Start Small" theme this year, we urge small businesses to take action to protect themselves from cybercriminals. After all, one small step today can bring you closer to a safer and more secure business tomorrow.

Stephen Cobb has been researching information assurance and data privacy for more than 20 years, advising government agencies and some of the world's largest companies on information security strategy. Cobb also co-founded two successful IT security firms that were acquired by publicly traded companies and is the author of several books and hundreds of articles on information assurance. He has been a Certified Information System Security Professional since 1996 and is based in San Diego as part of the ESET global research team.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit ***www.eset.com****.*

ENJOY SAFER TECHNOLOGY®