Sponsored content from DELL

Defend, Detect and Repel

Part two of a three-part series on cybersecurity for small business

Shields up: Why and how to protect your small business from hackers

43% of small businesses take no internet security precautions at all, and less than half train their employees in cybersecurity. (McAfee, 2012; Better Business Bureau, 2017)

In short, they are playing right into hackers' hands.

Multi-million-dollar attacks on famous companies get the headlines, but most cyberattacks target small business. For good reason: They invest less in cybersvecurity, are less aware of threats and their losses don't get the same attention.

"Small businesses have this idea that they're too small to bother with," says Mario Delapena, a Technology Advisor with Dell Small Business. "Attackers know they can get away with it. If they can get $1,500 from you in a ransomware attack, they'll absolutely take it."

72% of employees admit they'd share confidential info in some circumstances
(Dell, 2017)

A change in perspective for small business

Instead of viewing cybersecurity as an expense, Delapena contends, small businesses should view it as an investment in their business's health.

"In your personal health, you know you need to eat healthy and exercise," he says. "You also need to know what to avoid." People take vitamins, buy exercise equipment, learn to cook healthy meals, cut back on junk food, avoid smoking and get enough sleep.

In cybersecurity terms, "healthy" living means:

- Respecting access security – setting strong passwords and making it a policy to change them regularly.
- Installing security software, firewalls, and securing access to hardware, using laptops featuring TPM 2.0 (Trusted Platform Module) technology, fingerprint readers and facial recognition.
- Practicing safe internet use, knowing not to download suspicious files or click links from strange emails.
- Investing in PCs powered by 8th gen Intel® Core™ i5 vPro™ processors, which deliver hardware-enhanced security features.

Over 90% of successful cyberattacks start as phishing emails
(Better Business Bureau, 2017)

What's at risk in a cyberattack

It's important for small businesses to understand exactly what is at risk so they can accurately assess the value of cybersecurity.

There's the direct financial risk if a hacker is able to extort, steal or scam money from a business or its employees. But for small businesses, the risk can go much deeper.

"I ask small businesses, what would you do if you couldn't access your most important data?" says Delapena. "They have to think about the importance of efficiency and uptime. What if you had to shut down for a day? Or if all the files for a big project just went away?"

The effects tend to ripple outward. Employees might not get paid. Customers may have their own security compromised. And the harm to reputation can have a long-lasting effect.

With that perspective, the value-to-investment ratio for small businesses is often easier to understand.

53% of employees keep confidential work data in personal cloud storage accounts
(Dell, 2017)

An ever-changing threat landscape

The other thing small businesses need to remember is that cybersecurity is an ongoing and evolving practice, not a thing they can set and forget. That's because hackers never stop refining their attacks.

"There's a ton of new stuff coming out," says Delapena. In addition to viruses, malware and other digital threats, hackers increasingly are using social skills, profiling and psychology in their attacks.

Delapena recalled one small business who called Dell for help after being scammed. A hacker used a data breach to learn about a major project, figured out where the small business needed help, and reached out with an offer of assistance that seemed like just what the client needed.

The client paid $10,000 for what it thought was a needed service – and then the hacker took the money and ran.

"The best thing you can do is be very cautious," Delapena concludes. "These people are very inventive and creative and have the wherewithal to try new things."

Top threats to small businesses – and how to defend against them

Phishing: Capturing usernames and passwords by directing victims to fake, but real-looking, login pages.
Defense: Train employees to be suspicious of unexpected emails and look at "from" addresses.

Ransomware: Malicious software that locks the owner out of data and demands payment in exchange for releasing control.
Defense: Don't click suspicious links or download untrusted files. Use security software to inspect files.

Data breaches: Hackers get into company files, where they can steal customer data, client work, intellectual property or financial data.

Defense: Strong passwords, computers with enhanced security features and gap-free network protection – lock down Wi-Fi and don't let employees use private cloud storage to store work files.