Sponsored content from DELL

Defend, Detect and Repel

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

98.2% of all enterprises in the U.S. are small with fewer than 100 employees (U.S. Census Bureau, 2015). They are thriving thanks to a new generation of networked devices, smart workspaces and new ways to innovate, collaborate and engage with customers.

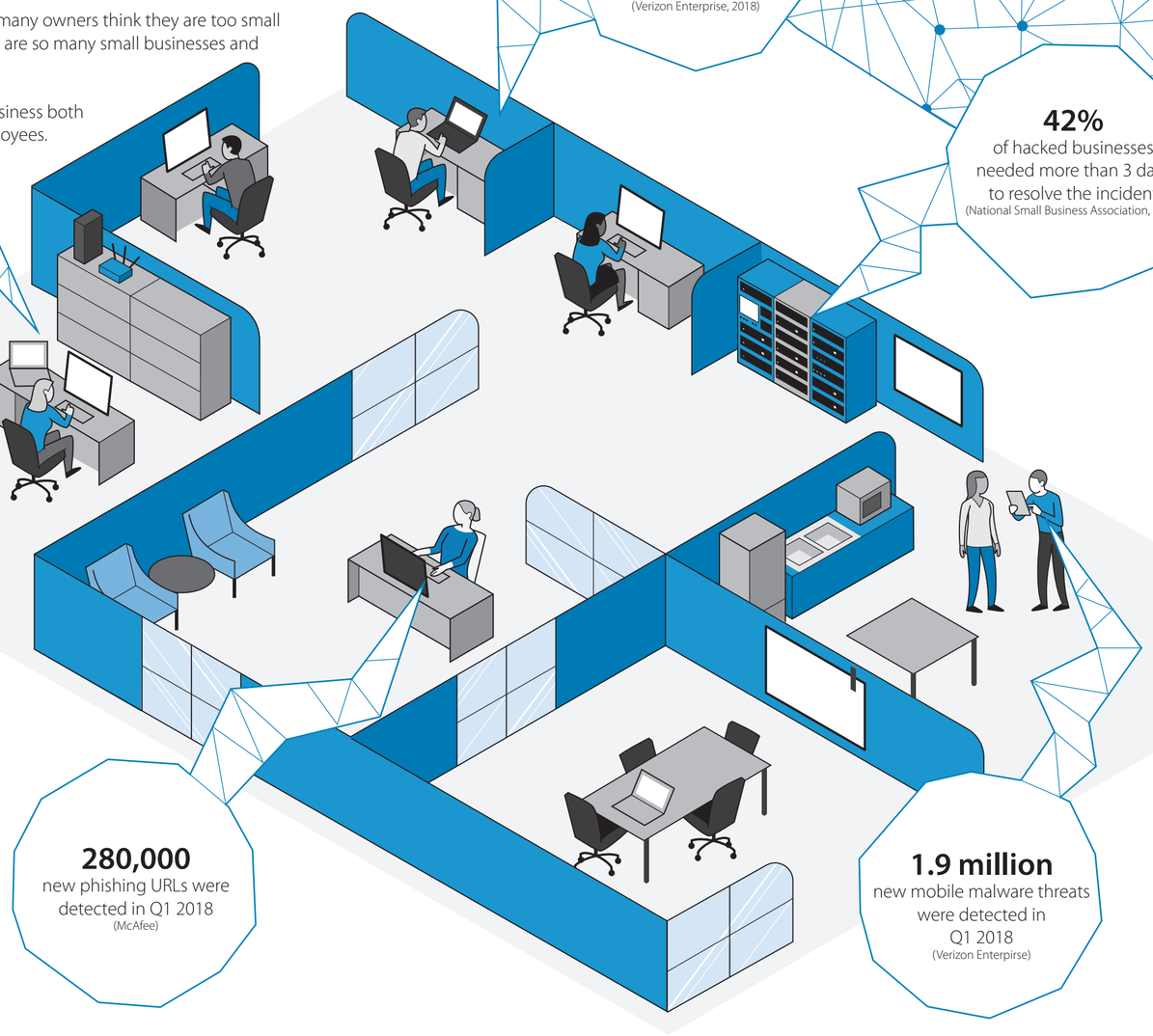
However, those tools have exposed small businesses to new threats. While many owners think they are too small to be targeted by cybercriminals, they are in fact a top target because there are so many small businesses and their security measures tend to be less robust than large organizations.

Don't become a cybercrime statistic. Learn how you can protect your business both proactively and reactively, through a mix of technology and educated employees.

58%
of confirmed breaches in 2017 were at small businesses
(Verizon Enterprise, 2018)

42%
of hacked businesses needed more than 3 days to resolve the incident
(National Small Business Association, 2016)

95%
of data breaches occur at endpoints or through employees
(Dell, 2016)



280,000
new phishing URLs were detected in Q1 2018
(McAfee)

1.9 million
new mobile malware threats were detected in Q1 2018
(Verizon Enterpirse)

Secure access to shield your business from hackers

A good defense is layered and involves both robust technology and smart people. Building that shield starts with knowing the threats you face and ensuring the defenses you have in place are oriented towards those threats.

Just as important as having the right defenses is ensuring they are actually used correctly – a lock only works on a door that is closed. Here are four common defenses you can deploy cost-effectively to help seal security gaps.

SECURITY MEASURE: Train your employees.
Help them learn to spot fraudulent emails, not click on suspicious links or attachments, use secure passwords and change them frequently.
WHY IT'S IMPORTANT: Fraudulent emails are a common first step in stealing passwords or scamming an employee into sending money. Many viruses and trojans (legitimate-looking software that does something bad in the background) come through email or unsafe web browsing. Weak passwords can be guessed in mere hours. All these can be prevented if employees stop, think and make smart choices.

SECURITY MEASURE: Use email encryption. Install software to encode emails so that they can't be read if they are intercepted by a hacker.
WHY IT'S IMPORTANT: A great deal of sensitive business information is sent via email, making it a common target of attacks. Most end users aren't familiar with the encryption options built into their email system, so setting it up to encrypt automatically is critical.

SECURITY MEASURE: Protect network access and devices.
Require logins on your Wi-Fi, network, computers and mobile devices. Use the latest laptops equipped with security-enhancing 8th gen Intel® Core™ i5 vPro™ processors and hardware login security like TPM 2.0 (Trusted Platform Module), fingerprint readers and facial recognition.
WHY IT'S IMPORTANT:
Unprotected networks and devices offer many opportunities for hackers to get into your system – once logged in, they may be able to log onto computers on the network or get into your shared files, where they can do enormous damage.

SECURITY MEASURE: Use robust anti-virus and firewall solutions.
High-quality security software solutions are affordable and effective at sniffing out attacks and helping repel them.
WHY IT'S IMPORTANT: Attackers are clever and aggressive. They change tactics often and develop new tools. No security is perfect, but network security systems are best able to keep on top of the latest threats and give you time to react if an attack does get past first-line defenses.

Detect, repel and recover from attacks

Hackers are not passive; they are creative, tenacious and persistent. The sheer scale and variety of cyber attacks shows convincingly why small businesses need to be vigilant and active in their own defense – cybersecurity isn't a one-and-done installation, it's a mindset and a way of life.

Some attacks will get through, despite your best defenses, but you can still take action as long as you have planned and prepared. Here are four ways to minimize the harm from cyberattacks.

PREPARE: Establish a cybersecurity incident plan.
By having clearly laid out steps to follow, you eliminate panic and ensure a rapid response to attacks, with everyone working together.
WHAT'S INVOLVED: Make sure your employees are trained on what to do if an attack gets through – most importantly, notifying an established (or pre-identified) security lead on your team, evaluating the system and quarantining potentially compromised hardware and files. Ensure the right people know where backups are kept and how to deploy them. Time is of the essence – every hour you can't serve customers compounds losses.

BACK EVERYTHING UP: Automatic backups can avert disaster.
A reasonable investment in backup technology can ensure business continuity.
WHAT'S INVOLVED: Backups often involve software that automatically copies files on protected computers and copies it either to a separate data storage drive at your business or a cloud storage, where it is kept in an off-site data facility. Your best option? Both.

DETECT: Make network monitoring someone's job.
On average, malicious software lives in a network for months before being detected, often because no one is looking for it.
WHAT'S INVOLVED: Setting up and using anti-virus and firewall software. Businesses must also establish policies for reviewing reports, tracking down threats and removing them.

REPORT: Call in reinforcements and alert stakeholders. An attack isn't a time to improvise. Report anything suspicious to an IT expert. Don't be afraid to ask for help fixing things and make sure customers or other stakeholders know.
WHAT'S INVOLVED: Transparency about attacks serves many purposes. One, it gets the right people involved to set things straight. Two, you can educate employees to watch for similar attacks, and your experience may help inform other businesses. Being honest with customers lets them take steps to protect themselves and is better in the long run for your reputation than hiding an incident.

Part Two

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

From phishing to ransomware to viruses, the threats facing businesses are growing every day, both in number and sophistication.

Learn more about the serious risks of insecure endpoints, and the best ways to improve security using technology and smart employee policies.

Coming Tuesday, October 2

Part Three

Fighting back: How small businesses can detect, respond and recover from a cyberattack

When a cyberattack happens, the effects on a small business can be catastrophic. Taking proactive steps so that you're ready to react quickly and correctly is a crucial part of any cyberattack response plan.

Learn what it takes to get your business back up and running fast.

Coming Wednesday, October 3