Sponsored content from DELL

Defend, Detect and Repel

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

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

Even though 78% of cyberattacks are aimed at small businesses, only 15% of small businesses have a plan to deal with an attack. (Verizon Enterprise, 2018; Better Business Bureau, 2017)

This explains why small business cyberattacks can be so devastating. Losing money and data is just the tip of the iceberg. Loss of reputation, customers and intellectual property can compound the effects of an attack.

"Attackers are getting very savvy," says Megan Wright, a Technology Advisor with Dell Small Business. They can be brutal as well. "The attacks are just more pain after more pain. They might pay in a ransomware attack and still not get their data back. Small businesses can just get wiped out."

With so much on the line, it's vital that small businesses know what to do in the event of a cyberattack.

Only 17% of small businesses have someone responsible for information security

(Better Business Bureau, 2017)

Before an attack: Back up data and keep the network secure

Many cyberattacks are aimed squarely at your data. In ransomware attacks, data is held hostage for a cash payment. In other cases, hackers may be after intellectual property, customer data, or account numbers.

Wright encourages all small businesses to back up all critical data. A strong backup plan involves:

- **Automation:** Make sure critical data is identified and backed up regularly
- **Redundancy:** Ideally you will have local and cloud backups
- **Isolation:** Backups should be sequestered from the main network and kept secure
- **Accessibility:** Someone should know how to access the backup in case of an attack

Businesses need to practice good basic security as well: strong passwords, 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, and installing anti-virus and firewall solutions.

380 days: Average time threats remained undetected in networks

(Secureworks, 2018)

Small businesses should assign someone to be responsible for information security. Often attacks go undetected because no one checked the firewall or anti-virus log, or ran needed updates.

Remember that networks evolve, and cracks can appear. Wright recalls one small business who said they'd been too busy to review how new hardware fit into the existing network. The resulting, preventable security gap allowed an attack that took the system down.

During an attack: Detect, report and react

The first rule is don't panic. The second is to act fast. The employee tasked with security should immediately track down, isolate and remove the infection, or bring in someone who can.

But since many attacks come through email and the web, all employees should be trained to spot and report them. If they get a suspicious email, they should report it to leaders and IT immediately.

"I tell small businesses, security doesn't just come from me as a technology advisor," says Wright. "It has to be a priority for the entire business."

Employees also need to be on the lookout for financial scams, like urgent orders to transfer money supposedly from business leaders. "Make it a policy to be over-cautious," Wright says. "If it's important, the sender will follow up."

$32,000 average loss for small businesses whose bank accounts were compromised

(National Small Business Association, 2015)

After an attack: Getting back on your feet

After an attack, a business with a solid incident response plan will be able to recover much faster than one that needs to rebuild. Data can be restored from backups, financial losses made whole through cyberattack insurance, and customers reassured.

Security specialists have detailed knowledge of the latest threats and planning for recovery. "You might need to find corrupted devices and files and pull them off the network," Wright says. "Depending on the level of the attack, you might also bring it to the authorities."

At the end of the day, small businesses need to make sure they secure the trust of their customers. "Your customers are why you exist," says Wright. "They trust you with their data. That is worth all the protection you can give it."

Five steps to take before, during and after a cyberattack

Back up everything ahead of time: Maybe back it up twice. A safe, uninfected data backup is critical to recovery.

Don't panic: Plan ahead and train your team. Response will be faster and surer.

Check on your backup and keep it secure: When an attack happens, make sure the backup is secure and ready.

Make your network secure: Remove affected devices and files, figure out where the breach came from and close the gap.

Get back on your feet: When appropriate, alert customers so they can see to their own security. Swap in your backup data once gaps are plugged.