DOW JONES, A NEWS CORP COMPANY

JOURNAL REPORTS: SMALL BUSINESS

The Cybersecurity Mistakes Startups Make When They Get Big

Very often, small companies don't scale their security to match their new size

Small companies often keep protecting devices individually, even as they add more and more of them. **PHOTO:** GETTY IMAGES/ISTOCKPHOTO

By Dennis Nishi

Nov. 25, 2018 10:02 p.m. ET

When small businesses start to boom, they often rush to add employees, ramp up production and get bigger offices. But something usually gets left off the to-do list: upgrading their cybersecurity.

A growing business means more computers—and that means more weak points in a network that hackers can attack. It also means more employees who aren't up to speed on security, and who click on suspicious links or fall for online scams.

Here's a look at some of the biggest security mistakes small businesses make as they grow, and what they can do to prevent them.

1. Sticking with piecemeal protection

When most small businesses start out, they don't have a lot of hardware to protect, so they install antivirus software and other safety measures on each device individually.

The trouble is that, as companies grow, they add many more computers but often keep protecting them on a device-by-device basis. And hackers have a variety of attacks in their arsenal that can bypass the protective software used for individual computers. If they can compromise one machine, the whole network is open to them.

JOURNAL REPORT

- Insights from The Experts
- Read more at WSJ.com/SmallBusinessReport

MORE IN SMALL BUSINESS

- Life Lessons We Can Learn From Entrepreneurs
- 9 Movies That Can Teach Children About Business
- These Franchises Were Huge. Why Did They Collapse?
- Adventurous Tactics for Winning Over Investors
- Asking Friends and Family for Cash Over Social Media

"You need a variety of different protections to deal with a variety of different threats. It's like dressing for unpredictable weather," says Jason McNew, chief executive officer of Stronghold Cyber Security in Gettysburg, Pa., which tests clients' security systems to look for potential vulnerabilities.

He recommends a security strategy that protects the entire network and not just individual devices. One solution: unified threat-management platforms, or UTMs, which take the place of the routers that most individuals and businesses use to manage their network traffic.

The devices integrate a firewall, antivirus protection and content filtering in one box and have a single set of controls, so they're easy to set up and maintain.

2. Not training employees

In an office with just a handful of people, it is relatively easy to get all employees on the same page about best practices regarding cybersecurity. Don't open suspicious emails. Don't click on dubious links.

But when new workers come on board during a big expansion, many businesses are so busy attending to other matters that they get lax about training. Or they forget that they can't trust everybody in the office the way they could in the old days.

That is when things get dangerous. Cybercriminals like to target new employees with scams involving sophisticated faked emails—which look like correspondence that people *should* trust—because the newcomers aren't yet familiar with company protocols.

And it is very easy to spot those new hires, since most companies announce staffing changes on their website, says Joshua Peskay, vice president of technology strategy for Round Table Technology, a contract IT firm in Portland, Maine.

One small nonprofit fell prey to this kind of scam and reached out to Mr. Peskay for help. The chief financial officer received a faked email request for a wire transfer that looked like it came from the executive director. Cybercriminals had purchased a web domain that was very similar to the nonprofit's and forged the executive director's email signature.

"The CFO is a very intelligent and responsible person but was new to the organization, as was the executive director," says Mr. Peskay.

The CFO transferred the money, and the nonprofit ended up losing $3,000. Afterward, it asked Mr. Peskay to strengthen its security and boost employee awareness.

There are many resources available that offer online guidance to small companies, Mr. Peskay says. The Small Business Administration's Office of Entrepreneurship Education has a free course on cybersecurity, he says, and third-party companies offer training. The Federal Trade Commission has also been adding to its online cybersecurity guide at FTC.gov/StartwithSecurity.

3. Grouping all data together

Small companies—like individuals—typically have networks that pool all of their users and data in the same place. This allows everybody who uses the network to easily communicate and share information.

But as networks grow and more people need access—whether they are new employees or vendors—there is more chance of the wrong people getting their hands on sensitive information. To contain risk, growing businesses should divide their networks so that different information is blocked off in different zones, and only certain people should have access to each.

Segmenting can be done with software or hardware such as switches, routers and UTMs, says Douglas Concepcion, director of security solutions engineering for Micro Strategies Inc., a technology services and solutions provider in Parsippany, N.J. "Each zone can be given its own role and level of security," he says. "An attack on one zone won't affect the others as quickly, since communication between zones is limited."

Once different zones are set up, companies should routinely review and update permissions that determine who has access to each—something that can get overlooked if new people get added or change jobs.

4. Not dealing with personal gadgets

In a small office, letting employees do business on their own smartphone or laptop doesn't seem like a big deal. But when many new employees come on board, it can get tough to keep track of who's using what device to do what. That means more chances for a security breach.

So, it's critical to spell out and enforce a clear bring-your-own-device policy about what personal devices are allowed and aren't allowed onto the network, say experts.

As part of that, companies should insist that their employees enable safety features such as two-factor authentication on all apps, and have employees use virtual-private-network software, which shields their internet traffic from spying, when they're on a public Wi-Fi network. It's also a good idea to install mobile-device-management software, which gives companies the ability to remotely secure data on devices that are lost or stolen.

Overall, even the simplest preventive steps help, such as doing online searches about potential threats and the best protection against them, says John Iannarelli, a former FBI special agent who is now a consultant specializing in cybersecurity, espionage and terrorism. "Just taking a few moments on the front end can save you a lot of time and heartache and finances on the back end."

Mr. Nishi is a writer in Los Angeles. Email reports@wsj.com.

Appeared in the November 26, 2018, print edition as 'Security Goofs Small Firms Make As They Grow.'

- **College Rankings**
- **College Rankings Highlights**
- **Energy**
- **Funds/ETFs**
- **Health Care**
- **Leadership**
- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**