April 2025 | CSN – Q2 - 2025

Security is *Everyone's* Responsibility

Who's Minding the Store Endpoints?

Summary

Regardless of the size of your business, you have endpoints. As your business grows, so does the number of your endpoints. And the more endpoints, the more vulnerable your business is to attack.

Average Number of Business Endpoints*

< 50 Employees = 22 Endpoints

< 100 Employees = 114 Endpoints

> 1,000+ Employees = 1,920 Endpoints

*e.g., computers, laptops, mobile phones, tablets, and servers

What in the World is an Endpoint and Why Should I Care?

An endpoint is a point of access, or a "door," where your employees or devices interact with a network or system, like a computer, smartphone, or server.

A cybercriminal can walk through any of these “doors” and steal money or data, install malicious software, or commit some other crime tricking employees to click on links or attachments that allow for malicious software to be installed – perhaps even ransomware!

A small business, typically defined as one with fewer than 100 employees, has an average number of 114 endpoints. This includes computers, laptops, mobile phones, tablet devices, and servers. However, this number can vary according to the size of the business and the types of devices it needs to operate.

Endpoints should be protected with security protocols and monitored, but you can only protect the endpoints you own. The endpoints belonging to employees and third-party service providers are outside your scope of direct control, though they may provide access to employee information, customer accounts, financial records, intellectual property, and other critical components you require additional security. To learn about the fundamentals of cybersecurity, download a free paper that provides 15 basic leading practices.

Do You Have Recourse?

Recourse can come in many different forms. In the event of burglary, vandalism, and theft, your recourse may be adequate insurance combined with resilience mechanisms, like data backups.

You may have recourse in the form of the legal right to demand compensation or payment in the event of financial loss.

What's Your Risk?

Endpoints put you at some risk. To determine how much, do a risk assessment to identify your business's critical assets and vulnerabilities. That information will help you implement additional controls to protect each endpoint. Risk management advisors, insurance agencies, and consultants can help you.

Helpful Resources

Your financial institution can also talk to you about increasing your endpoint security. Additionally, the Federal Trade Commission assists small businesses' cybersecurity on the following topics:

- Cybersecurity for Small Business
  - Business Email Imposters
  - Cyber Insurance
  - Cybersecurity Basics
  - Email Authentication
  - Hiring a Web Host
  - Secure Remote Access
- Ransomware
- Phishing
- Tech Support Scams
- Physical Security
- Vendor Security

Videos and Quizzes

- Cybersecurity Videos
- Cybersecurity Quizzes

What to Do if You Are Scammed

- Contact your financial institution immediately so they can act and provide recommendations.
- If you are the victim of burglary, vandalism, or theft, contact your local law enforcement agency.
- If your Social Security or individual tax identification number was stolen, immediately report it to IdentityTheft.gov.
- Report suspicious activity to the Internet Crime Center, www.ic3.gov, and/or your local law enforcement agency.

12120 Sunset Hills Rd, Reston
VA 20190