This webinar is being recorded

NIST Small Business Cybersecurity Webinar

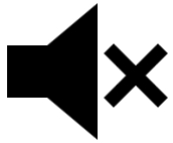
Back to Basics: Foundational Cybersecurity Practices for Small Businesses

August 20, 2026
2:00 PM–3:00 PM EDT

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Notes and Reminders

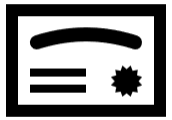
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.

Webinar recording: This webinar will be recorded and posted here: nist.gov/itl/smallbusinesscyber/events Registrants will be notified via email when the recording is available.

Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.

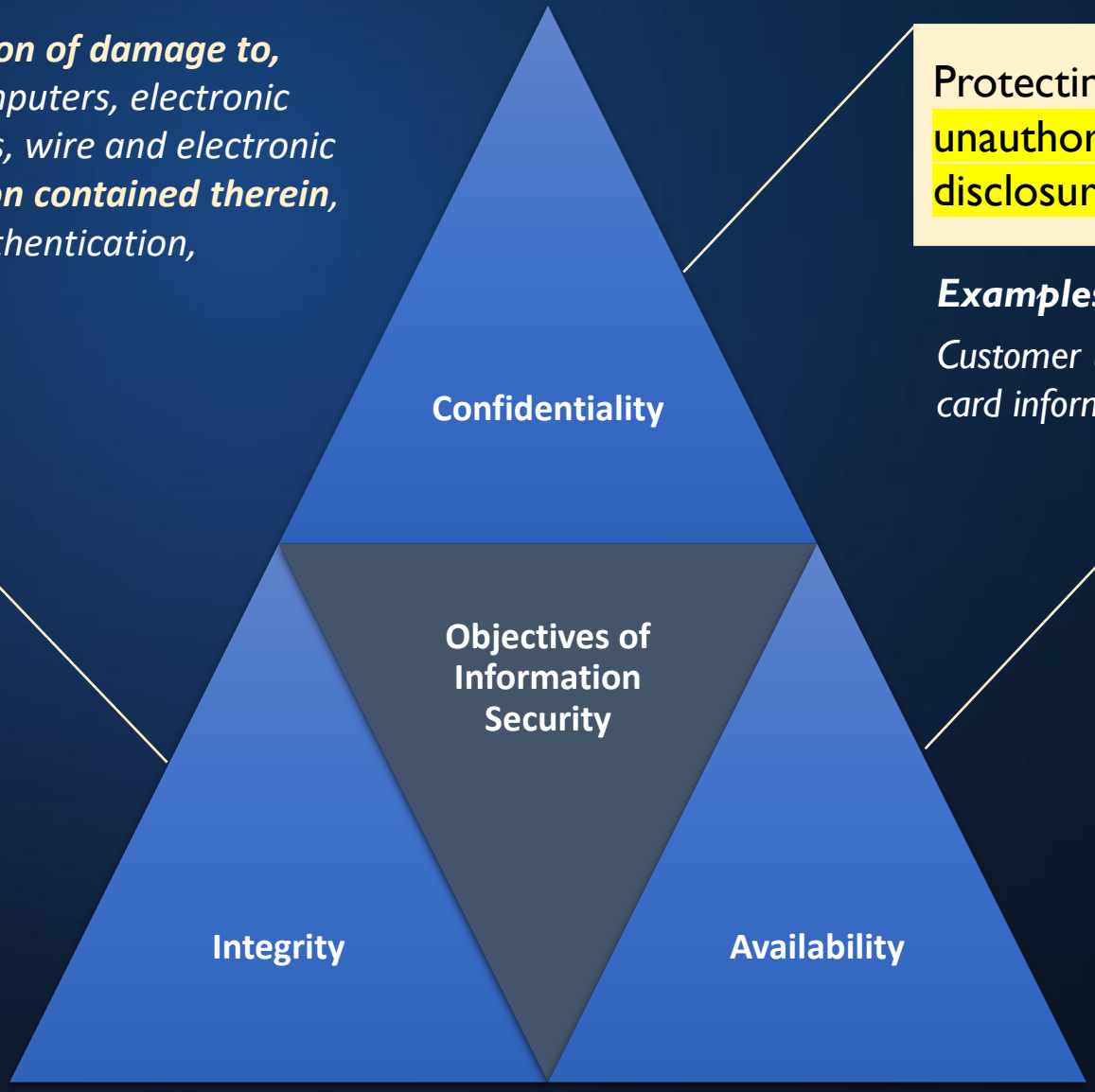


CEU/CPE credits: NIST does not provide specific information regarding CE/CPE credits. Attendees are welcome to use their registration confirmation email to self-report to their certification bodies.

CIA Triad

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Definition of cybersecurity: ***Prevention of damage to, protection of, and restoration of*** *computers, electronic communications systems and services, wire and electronic communication,* ***including information contained therein,*** *to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*
https://csrc.nist.gov/glossary/term/cybersecurity



Protecting information from unauthorized access and disclosure

Examples:

Customer usernames, passwords, or credit card information are stolen

Protecting information from unauthorized modification

Examples:

Payroll information, customer routing numbers, or product designs are altered

Preventing disruption in how information is accessed

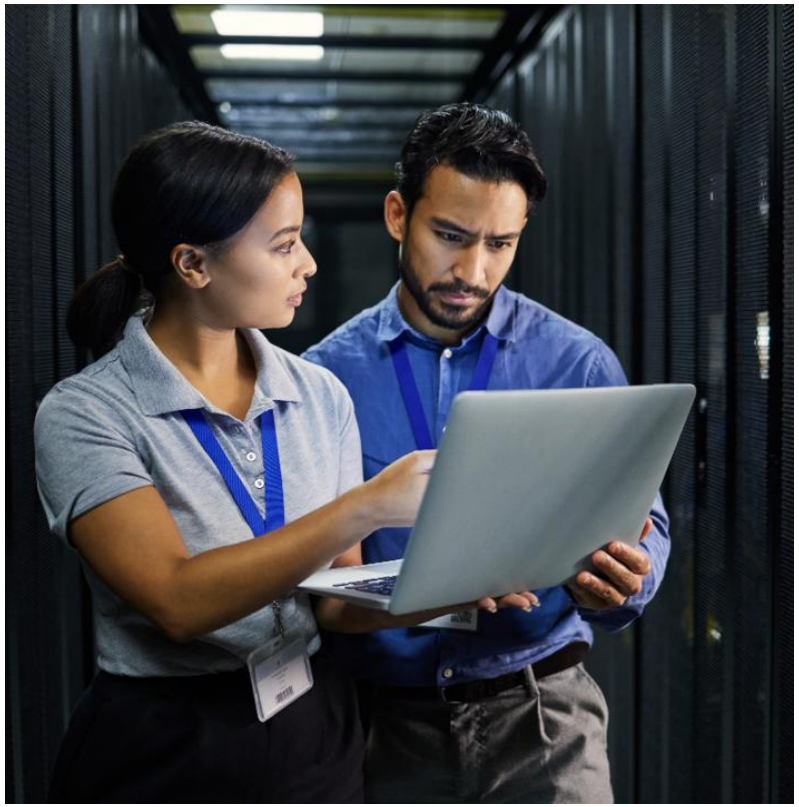
Examples:

Customers are unable to access your online services, or you can't access critical business systems

BACK TO BASICS: FOUNDATIONAL CYBERSECURITY PRACTICES FOR SMALL BUSINESSES

Christine Serrano Glassner
August 20, 2026

Why Cybersecurity Matters



- Many organizations are directly or indirectly connected to critical infrastructure.
- If an organization's systems are compromised, it could disrupt essential services and impact public safety.

CI FORTIFY

STRENGTHENING RESILIENCE ACROSS
CRITICAL INFRASTRUCTURE

Four Cybersecurity Essentials

The following four practices are the foundation of organizational cybersecurity and should be as automatic as buckling a seatbelt:

Teach employees to avoid phishing

Recognizing and reporting suspicious emails and links may prevent cyber attacks.

Require strong passwords

Long, random, unique passwords make accounts harder to breach.

Require multifactor authentication

Adds an extra layer of protection if a password is compromised.

Update software

Keeps systems protected against known vulnerabilities.

CISA LIVE!

UNDERSTANDING BOD 26-04: PRIORITIZING SECURITY UPDATES BASED ON RISK

August 27, 2026 | 11:30 am – 12:00 pm ET

HOST:

Christine Serrano Glassner
Chief
Office of the Chief External Affairs Officer

SPEAKER:

Jay Gazlay
Acting Associate Director for Vulnerability Management
Cybersecurity Division

Level Up Our Defenses

Once the core protections are in place, we can strengthen our defenses with additional practices:

Use logging and monitoring

Helps detect suspicious activity early to prevent or limit damage.

Back up data

Ensures you can recover quickly from ransomware or data loss.

Encrypt data

Makes stolen data unreadable without the proper key.

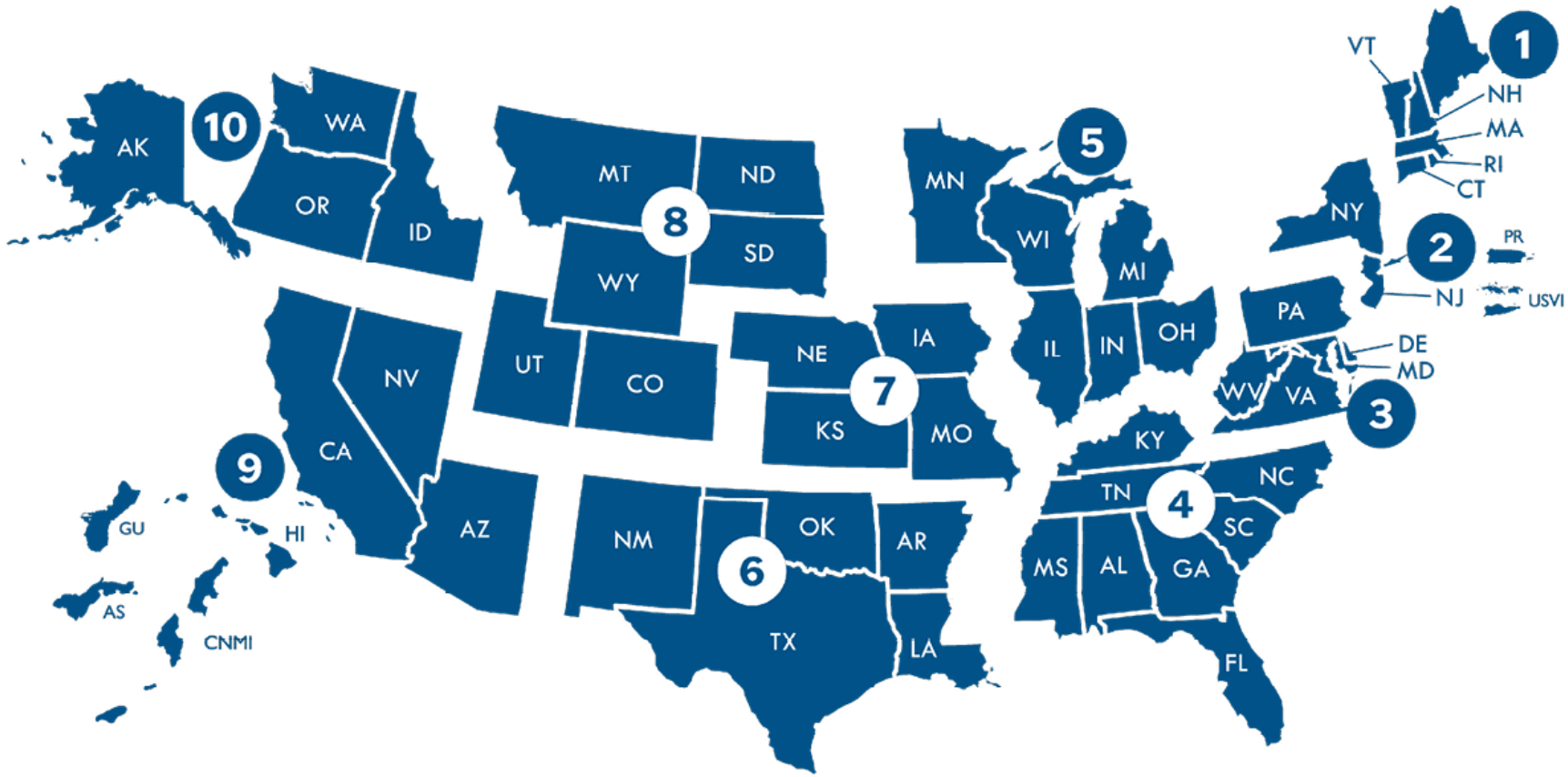
Create A Culture of Cybersecurity

Cybersecurity is a culture, not just a checklist.

A strong cybersecurity culture includes clear policies, regular employee training, and engagement from IT and leadership. It also means ensuring that partners and vendors follow strong security practices.

CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



CISA.GOV/REGIONS

For more information on CISA resources and programs please visit CISA.gov.


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Small Business Cybersecurity Fundamentals

C.P. Ferranti
CyD Assistant Section Chief
Cyber Engagement Section

Cyber Threat Landscape

Today's cyber landscape is threatened by a multitude of malicious actors who have the tools to conduct large-scale fraud schemes, hold our money and data for ransom, and endanger our national security. Profit-driven cybercriminals and nation-state adversaries alike have the capability to paralyze entire school systems, police departments, healthcare facilities, and individual private sector entities. The FBI continues to combat this evolving cyber threat. Our strategy focuses on building strong partnerships with the private sector; removing threats from US networks; pulling back the cloak of anonymity many of these actors hide behind; and hitting cybercriminals where it hurts: their wallets, including their virtual wallets.

(U) The FBI is also aware and tracking malicious actors' ability to leverage artificial intelligence to conduct cyberattacks. AI-based attacks harness the power of algorithms and machine learning to automate and optimize different phases of the attack lifecycle. These phases include reconnaissance, exploitation development, and lateral movement. We've also seen actors harness AI in social engineering and distributed denial of service (DDoS) attacks.

(U) Our strategy for countering cybercriminal actors is focused on disrupting:

- (U) **The actors: Identifying key criminals and working with partners to arrest them abroad.**
  - (U) That means administrators and affiliates of ransomware groups, and operators of services facilitating cybercrime like crypto tumblers, bulletproof hosting providers, and others.
- **(U) Their infrastructure: That we can seize or disable to disrupt attacks and glean intelligence.**
  - (U) Like the international operations we led against the Qakbot and 911 S5 botnets in 2023 and 2024, taking down key facilitators of ransomware, fraud, and other crimes.
- (U) **Their money: Making crime less profitable and taking away the funds used to run new illicit operations.**
  - (U) Within the past year, the FBI has seized cryptocurrency directly from ransomware actors as well as from cryptocurrency infrastructure that was facilitating cyber crime, including ransomware. Dismantling cryptocurrency infrastructure providers such as illicit exchanges and mixing services, in combination with cryptocurrency seizures, stunts ransomware groups' abilities to effectively conduct attacks, pay associates, and launder proceeds.

Key Points Today

- Know What You Need to Protect
- Lock Down Accounts
- Patch and Maintain Everything
- Protect Email
- Back Up Critical Data (Keep Backups in Separate System)
- Secure Devices and Networks
- Limit Administrative Access
- Have a Response Plan
- Train Employees - Train, Train and Train again…
- Avoid Security by Complexity

Know What You Need to Protect

The business question is not "Can we be hacked?"

But rather…

"If we are compromised tomorrow, what happens to our business?"

- Cyber incidents can affect:
- Revenue and cash flow
- Customer trust
- Business operations
- Sensitive information
- Regulatory or contractual obligations
- Reputation
- Management attention and productivity

Lock Down Accounts

Identity Is the New Perimeter

- A stolen password can provide an attacker with access without ever touching the company's physical network.

Common pitfalls

- Reused passwords
- Shared accounts
- No Multi-factor Authentication (MFA)
- Former employees still active
- Excessive privileges
- Administrators using their privileged accounts for everyday work
- Service accounts nobody owns or monitors

Patch and Maintain Everything

Vulnerabilities Become Business Risks When They Remain Unaddressed

- Software and hardware inevitably develop vulnerabilities. The risk increases when organizations leave known weaknesses unpatched.

Common pitfalls

- “We'll update it later”
- Unsupported operating systems
- Old network equipment
- Critical applications with unclear ownership
- Updates performed inconsistently
- Fear that updates will interrupt operations

Protect Email

Email Remains One of the Most Valuable Targets

Common pitfalls

- Employees trust familiar names and logos
- Payment requests aren't independently verified
- MFA prompts are approved reflexively
- Suspicious attachments are opened
- Attackers compromise an account and impersonate an employee

Back Up Critical Data

Recovery Is the Measure of Resilience

- Prevention will eventually fail somewhere. The ability to recover determines how severely an incident affects the business.

Common pitfalls

- Backups are incomplete
- Backups are connected to production systems
- Nobody knows how to restore them
- Restoration has never been tested
- Critical SaaS data is assumed to be automatically recoverable
- Backups are encrypted by ransomware along with production data

Secure Devices and Networks

Every Connected Device Is Part of the Business Attack Surface

- Laptops, phones, printers, routers, Wi-Fi systems, servers, and cloud-connected devices can all create avenues for compromise.

Common pitfalls

- Default passwords
- Unsupported hardware
- Poorly configured Wi-Fi
- Unmanaged employee devices
- Unencrypted laptops
- Flat networks where everything can communicate with everything
- Remote access exposed unnecessarily

Limit Administrative Access

Privilege Determines Blast Radius

- An attacker with access to an ordinary workstation is dangerous.
- An attacker with unrestricted administrative access can potentially control the environment.

Have a Response Plan

Organizations often discover during an incident that nobody knows who has authority to make decisions.

Common pitfalls

- No incident-response plan
- Employees don't know whom to call
- IT immediately wipes compromised machines
- Leadership learns about incidents too late
- No communication plan
- Backups aren't readily accessible
- Legal, insurance, or regulatory considerations are discovered after the fact

Train, Train, Train…

Employees Are Both a Risk and a Critical Security Control

- People make mistakes. Good cybersecurity programs assume this rather than treating mistakes as personal failures.

Common pitfalls

- Annual training nobody remembers
- “Don't click phishing emails” as the entire program
- Employees afraid to report mistakes
- Training disconnected from actual business activities
- Security teams treating users as adversaries

Avoid Security by Complexity

More Technology Does Not Automatically Mean More Security

- Small businesses can waste significant resources purchasing security products without establishing basic controls.

Common pitfalls

- Too many overlapping tools
- Security products nobody monitors
- Complex solutions employees work around
- Technology purchased without ownership
- No measurement of whether controls actually work
- Assuming compliance equals security

The Thought Process…

Every security controller should answer three questions:

- **What risk does it address?**
- **Who owns it?**
- **How do we know it works?**

Bottom Line

- Invest in **effective security**, not simply more security technology.

Takeaway - What Good Looks Like

A mature small-business cybersecurity program does **not** necessarily look like a large enterprise security operation.

- It looks like an organization where:
- Leadership knows its most important assets.
- Critical accounts use MFA.
- Employees understand how to report suspicious activity.
- Software and hardware are maintained.
- Administrative access is controlled.
- Backups are protected and tested.
- Email and financial processes include fraud controls.
- Incidents have defined owners and procedures.
- Security investments are tied to business risk.
- The organization can demonstrate that its controls actually work.

The most important shift for a small business is moving from:

“We need cybersecurity.”

To

“We need to protect the business, maintain operations, and recover quickly when something goes wrong.”

The fundamentals are straightforward.

The challenge is **consistent execution**.

Know what matters. Protect it. Limit access. Detect problems. Respond quickly. Recover confidently.

NIST Small Business Cybersecurity Resources

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Small Business Cybersecurity Corner

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

nist.gov/itl/smallbusinesscyber

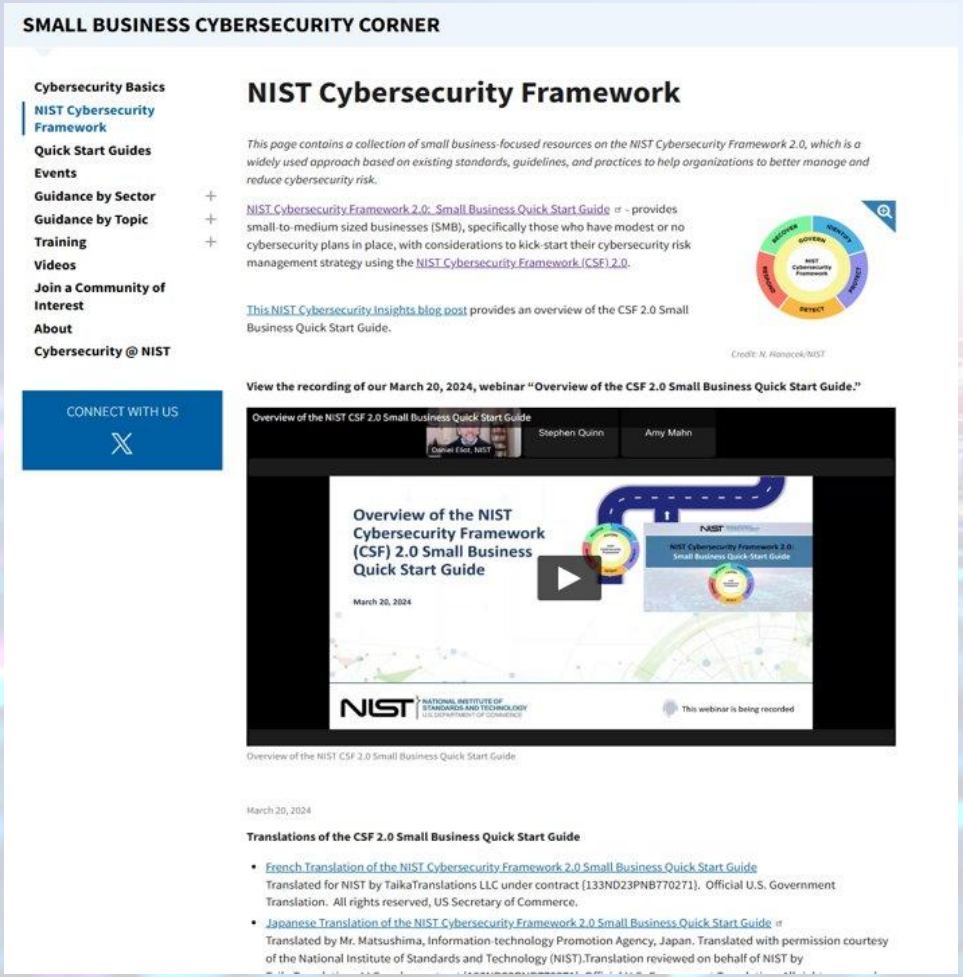
- Cybersecurity Basics
- NIST Cybersecurity Framework
- Quick Start Guides
- Events
- Guidance by Sector +
- Guidance by Topic +
- Training +
- Videos
- Join a Community of Interest
- About
- Cybersecurity @ NIST

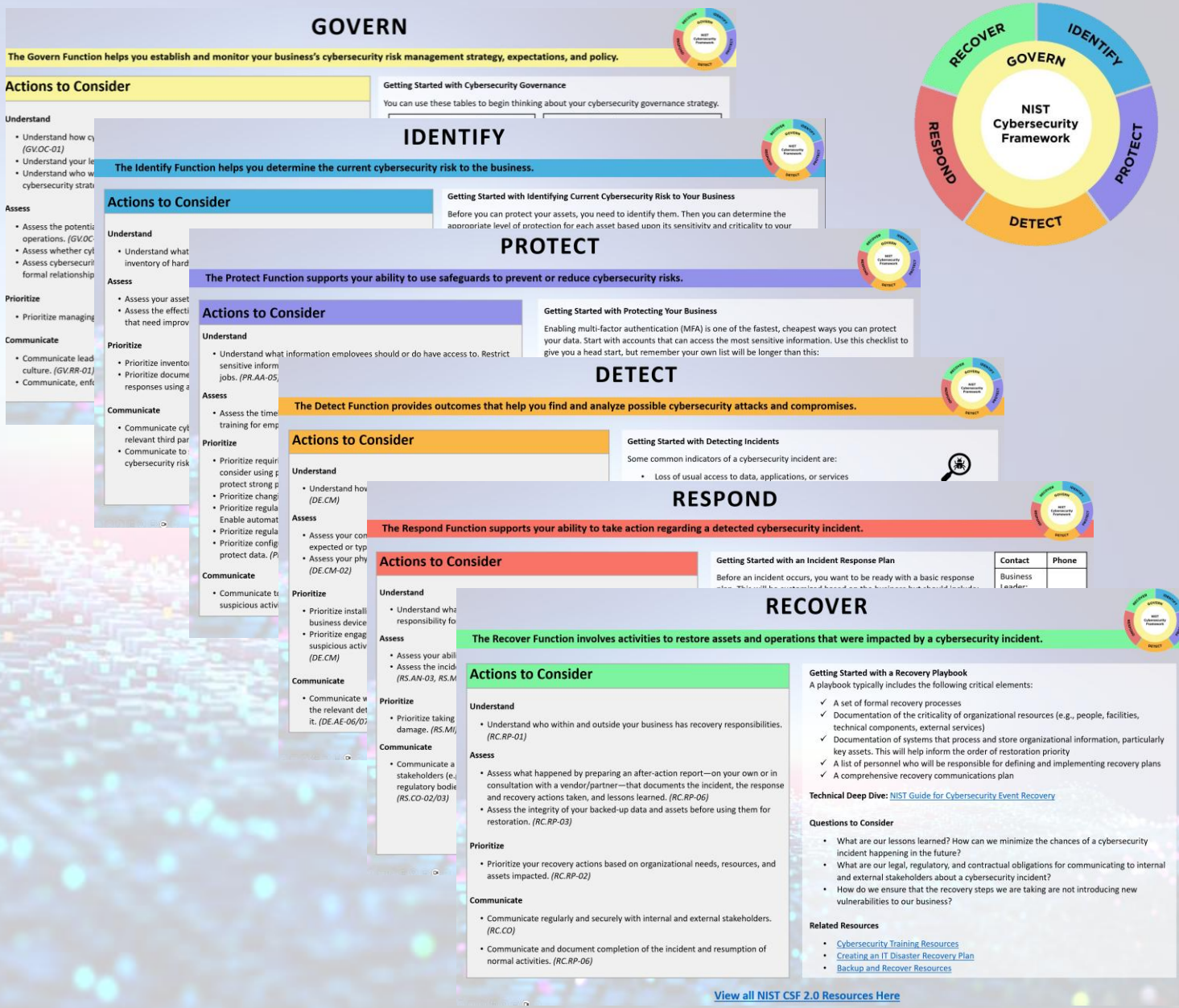
CONNECT WITH US

SPOTLIGHT

- ✓ All-Purpose Guides
- ✓ Choosing A Service Provider
- ✓ Cloud Security
- ✓ Cybersecurity Insurance
- ✓ Government Contractor Requirements
- ✓ Developing Secure Products
- ✓ Employee Awareness
- ✓ Multi-Factor Authentication
- ✓ Building Your Small Business Cybersecurity Team
- ✓ Phishing
- ✓ Privacy
- ✓ Protecting Against Scams
- ✓ Ransomware
- ✓ Responding to a Cyber Incident
- ✓ Securing Data and Devices
- ✓ Securing Network Connections
- ✓ Telework
- ✓ Supply Chain Cybersecurity

NIST Cybersecurity Framework 2.0 Small Business Quick-Start Guide





nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

NIST SMB Cybersecurity COI

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Convening companies, trade associations, and others who can share business insights, expertise, challenges, and perspectives to guide our work and assist NIST ***to better meet the cybersecurity needs of small businesses****.*

Over 21,000
individuals have already joined the full COI since March 6, 2023.

Quarterly Meetings
to share resources, updates, host guest speakers, and have robust discussion.

Next Meeting
- **September 16**

nist.gov/itl/smallbusinesscyber/join-community-interest

Cybersecurity Career Week

https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week

Cybersecurity as a Competitive Advantage

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- Protecting intellectual property;
- Enhancing the business' ability to comply with legal, regulatory, and contractual requirements;
- Positioning the business as a reliable participant in a larger supply chain;
- Gaining the confidence of customers, business partners, and employees;
- Making the business more resilient in the face of perpetual cybersecurity risks.

Questions?

Upcoming Events

- **September 16, 2026 (webinar) – Quarterly NIST Small Business Cybersecurity Community of Interest Call:** www.nist.gov/itl/smallbusinesscyber/events
- **October 19-24, 2026 – Cybersecurity Career Week:** https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week
- **October – Cybersecurity Awareness Month:** https://www.cisa.gov/cybersecurity-awareness-month

Follow @NISTcyber on

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

https://www.nist.gov

https://www.nist.gov/itl/smallbusinesscyber

@NISTcyber