Welcome to the CyberSecure My Business Webinar Series

We will begin promptly at 2pm EST

All speakers will be muted until that time

Detecting A Cyber Incident In Your Small Business

Webinar will begin promptly at 2pm Eastern

*Presentation is being recorded

Presented By:

NATIONAL CYBER SECURITY ALLIANCE
Goal of 5-Step Approach

Is Resilience

Know the threats and **Identify** and **Protect** your assets

**Detect** problems and **respond** quickly and appropriately

Know what **recovery** looks like & prepare

---

**Thanks to our National Sponsors**

[TREND MICRO](https://www.trendmicro.com)

[INFOSEC](https://infosec.global)

[StaySafeOnline](https://stay safelineonline.com)

[CYBERSECURE](https://cybersecure.business)
Bradford Willkie, CISSP
Director (Acting), Stakeholder Engagement and Cyber Infrastructure Resilience, Office of Cybersecurity and Communications

https://www.dhs.gov/CISA
CYBER INCIDENT DETECTION

RESOURCES FOR SMALL AND MIDSIZE BUSINESSES
The Importance of (Quick) Detection

Every organization is a potential target, *regardless of size*. Risks include:

- Data compromise or loss
- Weakened trust
- Costly recovery
- Business failure – 60% of SMBs within 6 months.

*U.S. companies take an average of 206 days to detect a data breach.*
Common Types of Attack

Source: Ponemon Institute
Tips & Recommended Practices

The Basics:
• Use threat detection software
  • At a minimum: Antivirus
• Keep system up to date
• Communicate with providers

The Next Level:
• Check your website
• Monitor web analytics & alerts
• Look out for:
  • Suspicious emails
  • Unusual password activity
  • Unusual pop-ups
• Train your staff
  • https://NICCS.us-cert.gov
Information Sharing

Where can you get your “news?”

- Industry associations
- Information Sharing and Analysis Centers (ISACs)
- Information Sharing and Analysis Organizations (ISAOs)
- National Cyber Awareness System (NCAS)

Learn more: https://www.dhs.gov/cisa/information-sharing-and-awareness
40+ cybersecurity tools and resources for public and private sector stakeholders

https://www.us-cert.gov/ccubedvp
Cybersecurity Resources Road Map

Goals:

• Make it easy to identify and access useful resources based on need

• Encourage stakeholders to elevate their efforts toward a more holistic risk management approach

https://www.us-cert.gov/ccubedvp/smb
Cybersecurity Resources Road Map

NCAS Cybersecurity Tip Sheets
https://www.us-cert.gov/ncas/tips
Webinars

Webinars on resources, best practices, and emerging threats, such as:

- Russian Activity Against Critical Infrastructure
- Chinese Cyber Activity Targeting Managed Service Providers
- Combating Ransomware
- Cybersecurity Framework Use Cases among SMBs
- Creating a Culture of Cybersecurity at Work
Events
Please join us for the next C3 Voluntary Program Webinar on August 11!
The C3 Voluntary Program is holding a series of webinars aimed at educating critical infrastructure owners and operators about relevant cyber risk management practices, tools, and resources. The August webinar will focus on five critical infrastructure sectors related to power and defense.
• Date: August 11, 2019
• Time: 1:00 PM-2:30 PM EST
• Dial-In: 1-888-606-9541 PIN: 7134259#
• HSIN Link: https://share.dhs.gov/ccubedvpwebinars/

Updates
The DHS National Cybersecurity and Communications Integration Center (NCCIC) will serve as the Federal lead for asset response activities. Additionally, the Departments of Homeland Security and Justice will maintain and update a fact sheet outlining how private individuals and organizations can contact relevant Federal agencies about a cyber incident.
• Establishing clear principles that will guide the Federal government’s activities in cyber incidents
• Differentiating between significant cyber incidents and steady-state incidents
• Categorizing the government’s activities into specific lines of effort and designating a lead agency for each line of effort in the event of a significant cyber incident;

Featured Resources
Cyber Information Sharing and Collaboration Program (CISCP)
The Department of Homeland Security’s National Cybersecurity and Communications Integration Center (NCCIC) serves as the hub of information sharing activities for the Department to increase awareness of vulnerabilities, incidents, and mitigations. Within the NCCIC, the Cyber Information Sharing and Collaboration Program (CISCP) is DHS’s flagship program for public-private information sharing. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities.
Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners.
Partner Websites

- NIST: https://www.nist.gov/itl/smallbusinesscyber
- SBA: https://www.sba.gov/managing-business/cybersecurity
- FTC: https://www.ftc.gov/tips-advice/business-center/small-business
- NCSA: https://staysafeonline.org/cybersecure-business/detect-incidents/
Resources to Respond: Preview

Report an incident to the Federal government if an incident …

- Results in a significant loss of data, system availability, or control of systems;
- Impacts a large number of victims;
- Indicates unauthorized access to, or malicious software present on, critical information technology systems;
- Affects critical infrastructure or core government functions; or
- Impacts national security, economic security, or public health and safety

Contact: (888) 282-0870 or NCCIC@hq.dhs.gov
For more information: https://www.cisa.gov

Contact the NCCIC:
Email: NCCIC@hq.dhs.gov
Phone: (888) 282-0870
Robin Wetherill, Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission

https://ftc.gov/smallbusiness
Responding to a Cyber Incident in Your Small Business
These views represent the speaker’s and not necessarily the Commission’s or any particular Commissioner’s
FTC Background

• Independent law enforcement agency
• Consumer protection and competition mandate
• Data security and privacy are consumer protection priorities
  • Enforcement
  • Policy initiatives
  • Consumer education and business outreach
What we’ll cover

• What to do before a breach:
  • Develop a breach response plan

• What to immediately following a breach:
  • Secure your operations
  • Notify appropriate parties

• What to do after the breach is resolved:
  • Fix vulnerabilities
  • Reassess your response

• FTC Resources
Time is of the Essence:

Acting quickly can reduce harm to the company and to consumers.
Have a Plan

Before a breach occurs, you should:

• Assemble a Data Breach Response Team
• Understand your legal obligations
• Train your staff
• Know how you will (likely) respond
Building your response team

• Who will be in charge?

• What kinds of expertise will you need?
Understand Legal Obligations

• Data security and/or privacy obligations?

• Notification obligations?
Train Your Staff
Secure Your Operations

As soon as you learn of the breach,
• **Mobilize** your response team

• **Understand** where and how the breach occurred

• **Act** immediately to prevent further data loss

• **Preserve** evidence of the breach

• **Remove** any improperly posted information from the web
Notify Appropriate Parties

- Notify law enforcement
  - Local, state, and federal authorities, depending on your business

- Notify other affected businesses
  - Your service providers or businesses to whom you provide services
  - Depository institutions
  - Credit bureaus
• Notifying affected individuals
  
  • Consider any relevant legal requirements

  • Identify whom you should notify

  • Consult with law enforcement

  • Decide how you should provide notice

  • Decide what information to include
Fix Vulnerabilities

• Understand how various components of your network may have contributed to the breach or resulting harm

• Make any necessary changes to service provider relationships, network segmentation, or user access
Reassess your response
FTC Resources for Consumers

IdentityTheft.Gov/DataBreach

Consumers can submit complaints, learn the warning signs of identity theft, find useful contact information, and develop an identity theft recovery plan

www.bulkorder.ftc.gov

Place free bulk orders for FTC materials that you can distribute to consumers
Publications

Displaying 1 - 3 of 3

All publications and shipping are free.

Cybersecurity and Your Small Business
Topic: Online Safety & Security
Language: English
Format: Booklet

Information on 12 different cybersecurity topics to help small business owners and staff understand common cyber threats and how they can protect their business.

Topic: Online Safety & Security
Language: English
Format: Booklet

What can companies learn from the FTC’s 50+ data security cases? Lesson #1: Start with security.

Data Breach Response: A Guide for Business
Topic: Privacy & identity
Language: English
Format: Booklet

Practical steps for businesses when responding to a data breach.