NATIONAL CYBER SECURITY ALLIANCE
Put a Response Plan in Place

Moderated by
Daniel Eliot, Director
Small Business Programs
NCSA

Jeff Marron, IT Specialist
Security
National Institute of Standards and Technology (NIST)

Tammy Smith, CISSP
Cyber Security Advisor
FedEx

Eric Jones, Director
Technology and Innovation
U.S. Small Business Administration

Reggie McKinney, Program Director
C3 Voluntary Program
U.S. Department of Homeland Security

Elisa Jillson, Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
NATIONAL CYBER SECURITY ALLIANCE
Put a Response Plan in Place

Moderated by
Daniel Eliot, Director
Small Business Programs
NCSA

Jeff Marron, IT Specialist
Security
National Institute of Standards and Technology (NIST)

Tammy Smith, CISSP
Cyber Security Advisor
FedEx

Eric Jones, Director
Technology and Innovation
U. S. Small Business Administration

Reggie McKinney, Program Director
C3 Voluntary Program
U.S. Department of Homeland Security

Elisa Jillson, Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
Put a Response Plan in Place

Jeff Marron, IT Specialist
Security
National Institute of Standards and Technology
The NIST Cybersecurity Framework Covers 5 Major Functions

This internationally recognized framework gives businesses a way to think about cybersecurity and was created by public and private sector working together.

1. IDENTIFY assets you need to protect
2. PROTECT assets and limit impact
3. DETECT security problems
4. RESPOND to an incident
5. RECOVER from an incident
NATIONAL CYBER SECURITY ALLIANCE
Put a Response Plan in Place

Tammy Smith, CISSP
Cyber Security Advisor
FedEx
WHAT WE KNOW

WHAT WE DON'T KNOW
Failing to prepare = preparing to fail
REACT VS. RESPOND

Fear-based
Impulsive
Blame
Assume

Fact-based
Deliberate
Cooperate
Assess
KEEP CALM AND REMEDIATE
NATIONAL CYBER SECURITY ALLIANCE
Put a Response Plan in Place

Eric Jones, Director
Technology and Innovation
U.S. Small Business Administration
How to Respond to a Breach

Eric Jones
Instagram/Twitter: @ericreecejones

The views expressed are those of the speaker and not necessarily those of the SBA
“Reputation, you know – a lifetime to build, seconds to destroy”
~ Robert De Niro
About the SBA

- Capital
- Counseling
- Contracting
- Disaster Assistance

Source: License - Flaticon Basic License with Vectors Market, Freepik, Roundicons
How to Connect with the SBA

68 District Offices + Satellite Branches

Resource Partners

https://www.sba.gov/managing-business/cybersecurity
SBA’s Top 10 Cybersecurity Tips

1. Protect against viruses, spyware, and other malicious code
2. Secure your networks
3. Establish security practices and policies to protect sensitive information
4. Educate employees about cyberthreats and hold them accountable
5. Require employees to use strong passwords and to change them often
6. Employ best practices on payment cards
7. Make backup copies of important business data and information
8. Control physical access to computers and network components
9. Create a mobile device action plan
10. Protect all pages on your public-facing websites, not just the checkout and sign-up pages
Thank You

https://www.sba.gov/managing-business/cybersecurity
NATIONAL CYBER SECURITY ALLIANCE
Put a Response Plan in Place

Reggie McKinney, Program Director
C3 Voluntary Program
U.S. Department of Homeland Security
CRITICAL INFRASTRUCTURE CYBER COMMUNITY

C³ VOLUNTARY PROGRAM

DHS RESOURCES FOR CYBER INCIDENT RESPONSE

Office of Cybersecurity & Communications (CS&C)
Department of Homeland Security (DHS)
REPORTING AN INCIDENT

Be prepared to provide information about:

• Your organization, operations, and information systems
• Nature of the incident
• How and when the incident was detected
• Response actions taken so far
• Organizations that have been notified
National Cybersecurity Communications and Integration Center (NCCIC) – 24/7 cyber situational awareness, incident response, and management center

Incident Reporting System
888-282-0870
https://www.us-cert.gov/forms/report
CYBER SECURITY ADVISORS (CSAs)

- Serve owners and operators of critical infrastructure, including small and midsize businesses, and governments agencies
- Provide range of cybersecurity services, including incident response

cyberadvisor@hq.dhs.gov
STAYING IN TOUCH

C³VP Website: us-cert.gov/ccubedvp

(scroll to Subscribe To Alerts to obtain our monthly bulletin)

C³VP Email: ccubedvp@hq.dhs.gov

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, 2016
• Time: 1:00 PM - 2:30 PM EST
• Dial-In: 1-888-606-9541 PIN: 7134259#
• HSN 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;

Resource of the Month
Cyber Information Sharing and Collaboration Program (CISP)
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 (CISP) is DHS’s flagship program for public-private information sharing. In CISP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities. Information shared via CISP allows all participants to better secure their own networks and helps support the shared security of CISP partners.
THANK YOU

US-CERT.GOV/CCUBEDVP

CCUBEDVP@HQ.DHS.GOV
Elisa Jillson, Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
HOW TO RESPOND TO A BREACH: FTC GUIDANCE

Elisa Jillson
Federal Trade Commission
ejillson@ftc.gov

The views expressed are those of the speaker and not necessarily those of the FTC or any one of its Commissioners.
FTC Background

• Independent law enforcement agency
• Consumer protection and competition
• Primary data security authority for most business
  • Enforcement
  • Policy initiatives
  • Consumer and business education
Breach Response Resources

https://www.ftc.gov/data-breach-resources
Data Breach Response: A Guide for Business
FTC Video Guidance
Take Action Immediately
Breach Response Steps

- Secure your operations
- Fix vulnerabilities
- Send notification
Breach Response Steps

• Secure Your Operations
  • Mobilize response team to prevent more loss

• Fix Vulnerabilities
  • Take steps so doesn’t happen again

• Send Notification
  • Law enforcement
  • Businesses
  • Individuals
Secure Operations & Fix Vulnerabilities

1. Assemble a team of experts
   Consider hiring data forensics team
   Talk to your legal counsel
2. Secure physical areas
3. Stop additional data loss
Secure Operations & Fix Vulnerabilities

4. Remove improperly posted info from web
   Your website + Other websites

5. Interview people who discovered the breach

6. Do not destroy evidence
Fix Vulnerabilities: Next Steps

• Think about service providers
• Check your network segmentation
• Work with your forensic experts
• Have a communications plan
Send Notification

- Determine your legal requirements
- Notify law enforcement
- Did the breach involve electronic health info?
- Notify affected businesses
- Notify individuals
Notifying Individuals

- Consult law enforcement
- Designate a point person for releasing info
- Considering offering free credit monitoring
Notifying Individuals: What to Say

• What you know about the compromise
• What steps to take (with relevant contact info)
• Current info about how to recover from ID theft
• Law enforcement info
• Complain to FTC about ID theft
• Method of future contact
Model Letter

NOTICE OF DATA BREACH

Dear [Insert Name],

We are writing to inform you about a data breach that has occurred at [Insert Company Name].

What Happened?
[Describe how the data breach happened, the date of the breach, and how the stolen information has been misused if you know].

What Information Was Involved?
[Describe the type of personal information that may have been exposed due to the breach].

What We Are Doing
[Describe how you are responding to the data breach, including what actions you’ve taken to remedy the situation; what steps you are taking to protect individuals whose information has been breached; and what services you are offering (like credit monitoring or identity theft restoration services)].

What You Can Do
We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

Equifax: equifax.com or 1-800-525-6285
Experian: experian.com or 1-888-397-3742
TransUnion: transunion.com or 1-800-680-7289

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and call [Insert contact information (law enforcement if authorized to do so)]. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC’s site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC’s Consumer Sentinel Network, where it will be accessible to law enforcement for their investigations.

More Guidance

- Call 1-877-ID-THEFT
  - Seek guidance anonymously
  - Prepare FTC Consumer Response Center for calls
- Visit business.ftc.gov
National Cyber Security Alliance
Put a Response Plan in Place

Moderated by Daniel Eliot, Director
Small Business Programs
NCSA

Jeff Marron, IT Specialist
Security
National Institute of Standards and Technology (NIST)

Tammy Smith, CISSP
Cyber Security Advisor
FedEx

Eric Jones, Director
Technology and Innovation
U. S. Small Business Administration

Reggie McKinney, Program Director
C3 Voluntary Program
U.S. Department of Homeland Security

Elisa Jillson, Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
Webinar Series
Second Tuesdays
2:00 p.m. EST

March – Recover

More Topics Coming Soon…

To Register: www.staysafeonline.org