National Cyber Security Alliance
How do you define Cybersecurity?
Define Cybersecurity

“The ability to protect or defend the use of cyberspace from cyber attack.”
National Institute of Science and Technology (NIST)

“Enabling people and businesses to do more online with trust and confidence.” NCSA
Today’s Discussion

• What are the threats
• NIST 5-Step Approach to Cybersecurity
• 5-Step Scenario
• Federal Trade Commission “Start with Security”
• Resources
Physical Office Security

Physical Security vs. Cybersecurity

Keypad Door Lock = Authentication
Interior Camera = Intrusion Detection System
Electronic Strike Door Lock = Firewall
Exterior Camera = Anti-Virus Protection
THREATS
What are the threats?

Only Nine Categories
The threats facing businesses fall into these categories

- Physical Theft and Loss
- Payment Card Skimmers
- Point-of-Sale Intrusions
- Crimeware (Malware/Ransomware)
- Web Apps
- Denial of Service
- Cyber-espionage
- Insider and Privilege Misuse
- Miscellaneous Errors
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America (Article 1, Section 8, Clause B; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.) Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content; elements of violence and child pornography. Spam messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your MoneyPak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address: fine@FBI.gov.
Business Email Compromise

June 14, 2016

Alert Number
I-061416-PSA

Questions regarding this PSA should be directed to your local FBI Field Office.

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE: THE 3.1 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to the Business E-mail Compromise (BEC) information provided in Public Service Announcements (PSA) 1-012215-PSA and 1-082715a-PSA. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data.

DEFINITION

BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail
5-Step Solution
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
5-Step Approach for Fire Prevention

<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Assets And Staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CyberSecure MY BUSINESS
5-Step Approach for Fire Prevention

**Identify**
- Building Assets
- And
- Staff

**Protect**
- Fire Exits
- Smoke Alarms
- Label Inventory

**Detect**
- Alarm Goes Off

**Respond**
- Meet at Mailbox
- Call 9-1-1
- Call Insurance

**Recover**
- Purchase New Items
- Notify Customers
- Clean up Smoke and Water Damage

---

*CyberSecure - My Business*
Let’s Try It!
A Real-Life Scenario – County Treasurer
Step 1: Identify
Exercise: Page 3
What are the most important data and technology assets the Treasurer’s Office needs to protect from cyber attacks?
<table>
<thead>
<tr>
<th><strong>STEP 1 - IDENTIFY</strong></th>
<th><strong>Identify</strong></th>
<th><strong>Protect</strong></th>
<th><strong>Detect</strong></th>
<th><strong>Respond</strong></th>
<th><strong>Recover</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Staff accesses</strong></td>
<td><strong>financial</strong></td>
<td><strong>accounts,</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Staff accesses</strong></td>
<td><strong>State</strong></td>
<td><strong>and</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Staff accesses</strong></td>
<td><strong>Federal</strong></td>
<td><strong>Data</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Inventory List Sample

<table>
<thead>
<tr>
<th>Physical Devices</th>
<th>Data</th>
<th>Location/Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers</td>
<td>Social security numbers</td>
<td>Administrators</td>
</tr>
<tr>
<td>Phones</td>
<td>Health data</td>
<td>Room</td>
</tr>
<tr>
<td>Servers</td>
<td>Payment data</td>
<td>IP addresses</td>
</tr>
<tr>
<td>Tablets</td>
<td>Personal information</td>
<td></td>
</tr>
<tr>
<td>Hard drives</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 1: Identify

Exercise: Page 4

What are the most important data and technology assets YOU need to protect from cyber attacks?
THE BREACH HAPPENS
Business Email Compromise – Where did the money go?

Barton County Treasurer's Office recovers portion of money lost in email scam

GREAT BEND, Kan. (KWCH) UPDATE: The Barton County Sheriff's Office says some of the money lost during an email scam to the Barton County Treasurer's Office has been recovered.
How did this happen?

**Social Engineering/Phishing**

How much are you/your staff sharing online?

Do you scrutinize email requests?

Are there protocols set up to address suspicious requests?
Step 2: Protect

Exercise: Page 5

What could the Treasurer’s Office be doing to protect his data and devices?
# STEP 2 - PROTECT

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
</table>
| Email    | Add strong authentication to email | Train staff often | Limit what is shared online | Establish protocols with clients early | **Email**

- Contains dates, times, accounts for wire transactions
<table>
<thead>
<tr>
<th>Let’s Talk About Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passwords don’t work</strong></td>
</tr>
<tr>
<td>Most popular is still “123456” or “password”</td>
</tr>
<tr>
<td>We don’t store them safely</td>
</tr>
<tr>
<td><strong>Make a Passphrase</strong></td>
</tr>
<tr>
<td>Example: I like to eat ice cream on Sundays</td>
</tr>
<tr>
<td>Passphrase: ILikeToEatIceCreamOnSunday$</td>
</tr>
<tr>
<td>Add one letter at the end of phrase that matches the URL</td>
</tr>
<tr>
<td><strong>Authentication Required</strong></td>
</tr>
<tr>
<td>Passwords/passphrases can be stolen</td>
</tr>
<tr>
<td>Authentication is critical to add to email, social media etc.</td>
</tr>
</tbody>
</table>
Step 3: Detect

Exercise: Page 5

What could the Treasurer’s Office have done to detect that something was wrong before the breach?
## STEP 3 - DETECT

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
</table>
| Email **Contains dates, times, accounts for wire transactions** | **Add strong authentication to email**  
Train staff often  
Limit what is shared online  
Establish protocols with clients early | **Use intrusion detection system to flag bad emails**  
Regular non-electronic comms  
Scrutinize email requests | | |

---

**CyberSecure**

**MY BUSINESS**
Step 4: Respond

Exercise: Page 6

How could the Treasurer’s Office respond once they learn of the breach?

Two areas – fix the issue and business continuity
### STEP 4 - RESPOND

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email</strong></td>
<td><strong>Add strong authentication to email</strong></td>
<td><strong>Use intrusion detection system to flag bad emails</strong></td>
<td><strong>Call financial institution immediately</strong></td>
<td></td>
</tr>
<tr>
<td>Contains dates, times, accounts for wire transactions</td>
<td>Train staff often</td>
<td>Scrutinize email requests</td>
<td><strong>Contact local FBI</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limit what is shared online</td>
<td>Regular non-electronic comms</td>
<td><strong>File complaint with IC3.GOV</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Establish protocols with clients early</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 5: Recover

Exercise: Page 6

What does recovery look like?
### STEP 5 - RECOVER

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email</strong></td>
<td>Add strong authentication to email</td>
<td>Use intrusion detection system to flag bad emails</td>
<td>Call financial institution immediately</td>
<td>Who is responsible for the lost money?</td>
</tr>
<tr>
<td>Contains dates, times, accounts for wire transactions</td>
<td>Train staff often</td>
<td>Regular non-electronic comms</td>
<td><strong>FBI</strong></td>
<td>Depends on state laws</td>
</tr>
<tr>
<td></td>
<td>Limit what is shared online</td>
<td>Scrutinize email requests</td>
<td>Contact local</td>
<td><strong>Reputation management</strong></td>
</tr>
<tr>
<td></td>
<td>Establish protocols with clients early</td>
<td></td>
<td>File complaint with IC3.GOV</td>
<td></td>
</tr>
</tbody>
</table>
ADD STRONG AUTHENTICATION!

- Train employees in security principles
- Protect information, computers, and networks from viruses, spyware etc.
- Delete or block spam
- Verify email sources: Digital signatures, check addresses, verify by phone
- Forward vs. reply: Ensure typing the correct address
- Keep a Clean Machine: Update software regularly
- Have IT support you can trust and interact with regularly
3-2-1 Back-Up Rule

- 3 back-up copies
- 2 different media
- 1 offline and in a separate location

Exercise: What is your back-up plan? Take a few minutes to write a plan or confirm the plan you already have.
Cloud Services

Make a list of cloud services you use. Ask about how they handle:

- Maintenance
- Patching
- Firewall
- Encryption
- Backup/Restore

FEDRAMP.GOV
5-Steps with Cloud Providers

- Identify
- Protect
- Detect
- Respond
- Recover

Vendor Support
Vendor Support
Vendor Support
Vendor Support
Vendor Support
Make a list of contact you need when a breach happens.

- Train employees to identify and report breaches
- Establish financial institutions you need to notify
- Reporting obligations differ depending on state law
  - 49 states have reporting laws
  - National Conference of State Legislators
  - [www.ncsl.org](http://www.ncsl.org)

Consult your counsel BEFORE a breach!
Policy Examples

What policies do you already have in place?

**Acceptable use (of information technology)**
All device/network users will read and sign an access and use agreement.

**Training and awareness**
All staff will participate in cybersecurity education program.

**Physical security**
Devices must be secured when leaving your desk or traveling.

**Password and authentication**
Passphrases must (be strong and unique for work) and authentication enabled on all email accounts.

**Personnel security**
All personnel data will be protected from viewing or changing by unauthorized persons.

**Email Usage**
Personal or sensitive data may not be sent in email.
PUBLIC WIFI SECURITY

VPN

Hotspot
FCC Response Plan

- Privacy and Data Security
- Scams and Fraud
- Network Security
- Website Security
- Email
- Mobile Devices
- Employees
- Etc.
Don’t be overwhelmed
...Resources are available
Federal Trade Commission (FTC)“Start with Security”

1. Start with Security

Factor security into all decision making
• What kinds of information do you collect?
• How long do you keep it?
• Who do you share it with?
• Who has access?

Lead by example to create a culture of security at work

2. Control Access to Data Sensibly

**BEST PRACTICES**

- Restrict access to sensitive data to **those who need it for job duties**
- Minimize administrative privileges on your network

**FTC CASE: TWITTER**

Granting administrative access to most employees increased risk of eventual breach.

3. Require Secure “Passphrases” and Authentication

**BEST PRACTICES**

- Store passphrases securely and add strong authentication
- Guard against brute force attacks

**FTC CASE: GUIDANCE SOFTWARE**

Network credentials stored in cleartext helped hacker access credit card information.

4. Store Sensitive Information Securely and Protect During Transmission

BEST PRACTICES

• Ensure staff handling sensitive data understand how to protect it
• Encrypt sensitive information stored on network and during transmission

FTC CASE: SUPERIOR MORTGAGE

Sensitive customer data encrypted on collection at website was decrypted and emailed to branch offices.

5. Segment your network and monitor who’s trying to get in and out

**BEST PRACTICES**

- Not all computers need to communicate
- Monitor network activity

**FTC CASE: DSW**

Computers were not prevented from connecting across in-store and corporate networks.

**BEST PRACTICES**

Before enabling remote access:

- Assess client/vendor security
- Ensure staff computers/devices are secure
- Restrict access to known IP addresses; grant temporary access as needed

**FTC CASE: LIFELOCK**

No antivirus programs installed on staff computers used to remotely access network.

7. Apply Sound Security Practices When Developing New Products

**BEST PRACTICES**

- Train your engineers in secure coding
- Verify that privacy and security features work
- Test for common vulnerabilities

**FTC CASE: SNAPCHAT**

The company advertised that messages would “disappear forever,” but they failed to ensure the accuracy of that claim.
8. Make Sure Service Providers Implement Reasonable Security Measures

**BEST PRACTICES**

- Include reasonable security requirements in service provider contracts
- Verify compliance during contracts period

**FTC CASE: GMR TRANSCRIPTION**

Hired service providers to transcribe sensitive audio files but failed to require reasonable security measures. For example: Encryption

9. Put Procedures in Place to Keep Security Current and Address Vulnerabilities

BEST PRACTICES

• Update and patch 3rd party software when urgent need and on regular schedule
• Act quickly on credible warnings and ensure risks are addressed

FTC CASE: FANDANGO

Security warning wrongly categorized as customer service request was ignored.

10. Secure Paper, Physical Media and Devices

**BEST PRACTICES**

- Protect mobile and storage devices on the move when traveling or commuting
- Secure paper records - lock up sensitive items
- Dispose of sensitive personal data securely - disk drives, printers etc.

**FTC CASE: GOAL FINANCIAL**

Employee sold surplus hard drives with unencrypted sensitive information of 34,000 customers.
Federal Trade Commission – Even More

Ftc.gov/smallbusiness

Protecting Small Businesses

As a small business owner, you have a lot on your mind. You can’t afford to lose time or money to scammers or a compromised network. We can help you avoid scams, protect your computers and networks, keep your customers’ data safe – and protect your bottom line. You can also find out what the FTC is doing to protect small businesses. Thinking about starting a new business? See our advice about buying a franchise or business opportunity.

Business Center

ADVERTISING & MARKETING
CREDIT & FINANCE
PRIVACY & SECURITY
PROTECTING SMALL BUSINESSES

SELECTED INDUSTRIES

LEGAL RESOURCES
BUSINESS BLOG

Protect Your Business from Scams
Scammers target small businesses. Learn to recognize those scams by reading these tips or watching these videos.

Cybersecurity
Running a company with a few employees? Check out these computer security basics for small businesses. And learn how to protect computers and networks against threats, develop a plan to protect customers’ personal information, and what to do if there is a data breach.
Committed to helping small businesses leverage technology as a core driver of growth and differentiation. That means increasing digital education and training to Launch, Grow, Manage, and Win their business.
Critical Infrastructure Cyber Community (C³) Voluntary Program

- Over 40 no-cost resources currently featured, including the Cyber Resilience Review and the SMB Toolkit
- Pages are organized by stakeholder group, including Small and Midsize Business
- Resources are aligned by Framework Core Function: Identify, Protect, Detect, Respond, and Recover
6 Steps to Better Security

- Protect accounts with strong authentication
- Keep software updated
- Avoid phishing attempts
- Use unique passwords
- Protect mobile devices
- Use trusted security tools
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 and prepare
Thank You