CISA to the RESCUE!

With JD Henry
Supervisory Cybersecurity Advisor – Region 5

10 October 2023

#16 IN THE BLUE CYBER EDUCATION SERIES

The Slides are Located at:

J.D. Henry
Supervisory Cybersecurity Advisor – Region 5
Cybersecurity and Infrastructure Security Agency
We are the Nation’s Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure
Cybersecurity and Infrastructure Security Agency (CISA)

VISION
Secure and resilient infrastructure for the American people.

MISSION
CISA partners with industry and government to understand and manage risk to our Nation’s critical infrastructure.
Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.
Serving Critical Infrastructure

KEY ACTIVITIES

- Identify and Verify Suspicious Cyber Activity
- Understand Incidents and Vulnerabilities
- Build and Maintain Partnerships
- Share Timely and Actionable Information
- Collaborate with Partners to Mitigate Risk

16 CRITICAL INFRASTRUCTURE SECTORS

Brian Yoshino
October 9, 2023
TODAY’S CYBER THREAT LANDSCAPE
Cyber Threats of Today*

**Ransomware**
- Double/Multi-extortion (Lockbit Conti, Hive, Vice Society, etc.)

**Malware**
- IT and OT specific malware

**Denial of Service**
- Cyber criminals, Hacktivists (KillNet / Aviation Sector)

**Threats to External Dependencies**
- 3rd party vendors, service providers, infrastructure providers
- Supply chain compromise

**Advanced Persistent Threats (APTs)**
- Highly sophisticated with substantial financial backing
- Various motivations (political, economic, etc.)

* Not an exhaustive list!
Cyber Threats of Today

SOBERING CYBER STATS

1 IN 3 HOMES with computers are infected with MALICIOUS SOFTWARE

65% OF AMERICANS who went online received at least one online scam offer.

Worldwide, consumers LOST $358 + 21 HOURS on average per year dealing with online crime.

47% OF AMERICAN ADULTS have had their personal information exposed by cyber criminals.

600,000 Facebook ACCOUNTS HACKED every single day.

THE #1 CRIME is the IMPOSTER SCAM with 1 in 5 people reporting a financial loss.

https://www.cisa.gov/be-cyber-smart/facts
The Threat to Critical Infrastructure
Why target Critical Infrastructure?

The ROI of Cybercrime

Where there is profit, there is opportunity.

The economic impact of cybercrime has tripled in the past decade. No longer the hacker in a hoodie, today’s threat actor is a professional. Structured and top line focused, organized cybercriminals act as an enterprise—following the same rules of finance as their targets.

Infographic source: The ROI of Cybercrime (www.sans.org)
October is Cybersecurity Awareness Month

- Launched in 2004
- Co-managed by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA)
- Collaborative effort between government and industry to raise cybersecurity awareness
- Ensures that everyone has the resources they need to be safe and secure online.
Implementing cybersecurity best practices is important for individuals as well as organizations of all sizes to protect personal, financial and sensitive information.

For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to protecting and maintaining business operations.

Cybersecurity is a Team Sport!
4 Easy Ways to Stay Safe Online

Turn on Multifactor Authentication
Use Strong Passwords and a Password Manager
Recognize and Report Phishing Attacks
Update Your Software
6 Easy Ways to Stay Safe Online

- Turn on Multifactor Authentication
- Use Strong Passwords and a Password Manager
- Recognize and Report Phishing Attacks
- Update Your Software
- Use Social Media Responsibly
- Backup your important data
Enable Multi-factor Authentication

WHAT IS IT?

• A code sent to your phone or email
• An authenticator app
• A security key
• Biometrics
  Fingerprint
  Facial recognition

https://www.cisa.gov/MFA
review, to evaluate the security performance of various MFA methods in a largedataset of Microsoft Azure Active Directory users exhibiting suspicious activity. Our findings reveal that MFA implementation offers outstanding protection, with over 99.99% of MFA-enabled accounts remaining secure during the investigation period. Moreover, MFA reduces the risk of compromise by 99.22% across the entire population and by 98.56% in cases of leaked credentials. We further demonstrate that dedicated MFA applications, such as Microsoft Authenticator, perform significantly better than SMS-based authentication, offering enhanced security.

J.D. Henry
October 6, 2023

How effective is multifactor authentication at deterring cyberattacks?

- Lucas Augusto Meyer
  - AI for Good Lab
- Sergio Romero
  - Identity Security
- Tom Burt
  - Customer Security & Trust
- Alex Weilert
  - Identity Security
- Gabriele Bertoli
  - Identity Security
- Juan Lavista Ferres
  - AI for Good Lab

This study investigates the effectiveness of multifactor authentication (MFA) in protecting commercial accounts from unauthorized access, with additional focus on accounts with known credential leaks. We employ the benchmark-multiplier method, coupled with manual account review to evaluate the security performance of various MFA methods in a largedataset of Microsoft Azure Active Directory users exhibiting suspicious activity. Our findings reveal that MFA implementation offers outstanding protection, with over 99.99% of MFA-enabled accounts remaining secure during the investigation period. Moreover, MFA reduces the risk of compromise by 99.22% across the entire population and by 98.56% in cases of leaked credentials. We further demonstrate that dedicated MFA applications, such as Microsoft Authenticator, outperform SMS-based authentication, although both methods provide significantly enhanced security compared to not using MFA. Based on these results, we strongly advocate for the default implementation of MFA in commercial accounts to increase security and mitigate unauthorized access risks.
Use Strong Passwords

CREATE STRONG PASSWORDS:

• Long
  • At least 16 characters

• Unique
  • NEVER reuse passwords

• Complex
  • Upper- and lower-case letters
  • Numbers
  • Special characters
  • Spaces
Why Use Strong Passwords

How an 8-Character Password Could be Cracked in Just a Few Minutes

Advances in graphics processing technology and AI have slashed the time needed to crack a password using brute force techniques, says Hive Systems.

Use a Password Manager

WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks.
Recognize and Report Phishing

- A tone that’s urgent or makes you scared
  "Click this link immediately or your account will be closed"

- Bad spellings, bad grammar

- Requests to send personal info

- Sender email address doesn’t match the company it’s coming from
  Ex: Amazon.com vs. Amaz0n.com

- An email you weren’t expecting

Recognize and Report Phishing

WHAT TO DO

Do NOT

• Don't click any links
• Don't click any attachments
• Don't send personal info

Do

• Verify
• Contact that person directly if it's someone you know
• Report it to your IT department or email/phone provider
• DELETE IT
Updates ensure devices and apps are protected from the latest threats

Don’t click “remind me later,” it could leave you vulnerable to cyber threats

Automatic updates are the easiest way to stay secure
If you are not paying for it, you’re not the customer; you're the product being sold.

First job title: STOP
Favorite food: GIVING
Favorite color: PEOPLE
First pet’s name: YOUR
First child’s name: PERSONAL
Favorite restaurant: INFO
Where are you from: TO
Favorite singer/band: GUESS
Street you grew up on: YOUR
First type of car you had: PASSWORDS
Favorite teacher’s name: AND
Your mother’s maiden name: SECURITY
One unpopular opinion you have: QUESTIONS
Backup your important data

- Hard drives are cheap!!!
- Keep copies of your most important data in “cold storage”
  - Offline, disconnected, stored in a safe place
- Update / rotate regularly
  - Quarterly, every 6 months, etc.

CISA RESOURCES
Cybersecurity Services

CISA Cybersecurity Services & Assessments
- Vulnerability Scanning
- Cybersecurity Performance Goals (CPG)
- Cybersecurity Assessments
- Tabletop Exercises (TTX)
- Training
- & more

For more information on these services and more, please visit

https://www.cisa.gov/topics/cyber-threats-and-advisories
or
https://www.cisa.gov/resources-tools/resources/cisa-services-catalog
GOAL:
Reduce exposure to threats by taking a proactive approach to identifying and mitigating attack vectors

- Hosts with no vulnerabilities detected are rescanned every 7 days
- Hosts with low-severity vulnerabilities are rescanned every 6 days
- Hosts with medium-severity vulnerabilities are rescanned every 4 days
- Hosts with high-severity vulnerabilities are rescanned every 24 hours
- Hosts with critical-severity vulnerabilities are rescanned every 12 hours

Email us at vulnerability@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services” to get started.
What are the CPGs?
- A set of high-impact security actions for critical infrastructure organizations that address both IT and OT/ICS considerations.
- Mapped to the relevant NIST Cybersecurity Framework subcategories, as well as other frameworks (e.g., IEC 62443).

How should organizations use the CPGs?
- Inform strategy decisions and resource investment.

The most current version of the CPGs is located at: https://www.cisa.gov/cpg

The CPG’s Address:
- Account Security
- Device Security
- Data Security
- Governance and Training
- Vulnerability Management
- Supply Chain/Third Party
- Response and Recovery
- Other (network segmentation, email, etc,)
Where to Find Them

- The most current version of the CPGs is located at: https://www.cisa.gov/cpg
- Here you can find:
  - The core list of CPGs
  - CPG Checklist
  - Spreadsheet of all text content
  - Link to our GitHub discussion page
Cybersecurity Performance Goals

### 8.1 Network Segmentation

<table>
<thead>
<tr>
<th>TTP OR RISK ADDRESSED:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Service Discovery (T1046)</td>
</tr>
<tr>
<td>Trusted Relationship (T1193)</td>
</tr>
<tr>
<td>Network Connection Enumeration (OS T0840)</td>
</tr>
<tr>
<td>Network Sniffing (T1040, ICS T0642)</td>
</tr>
</tbody>
</table>

**RECOMMENDED ACTION:** All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, “jump box,” or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets.

### Approximate Cost/Impact/Complexity ratings to inform investment planning.

- **COST:** $$$
- **IMPACT:** HIGH
- **COMPLEXITY:** HIGH

### Mapping to NIST CSF Subcategory

<table>
<thead>
<tr>
<th>CURRENT ASSESSMENT</th>
<th>YEAR 1 ASSESSMENT</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE:</td>
<td>DATE:</td>
<td></td>
</tr>
<tr>
<td>IMPLEMENTED</td>
<td>IMPLEMENTED</td>
<td></td>
</tr>
<tr>
<td>IN PROGRESS</td>
<td>IN PROGRESS</td>
<td></td>
</tr>
<tr>
<td>SCOPED</td>
<td>SCOPED</td>
<td></td>
</tr>
<tr>
<td>NOT STARTED</td>
<td>NOT STARTED</td>
<td></td>
</tr>
</tbody>
</table>

How organizations can demonstrate the effective implementation the security practice, based on input from CISA’s collaborative stakeholder process. These Actions will be updated regularly as new threats and defenses arise.

MITRE ATT&CK TTPs addressed by the Goal
When to Report:
If there is a suspected or confirmed cyber attack or incident that:
• Affects core government or critical infrastructure functions;
• Results in the loss of data, system availability; or control of systems;
• Indicates malicious software is present on critical systems

REPORTING CYBER ATTACKS
• Indiana Office of Technology (IOT) at https://www.in.gov/cybersecurity/report-a-cyber-crime/
• Contact CISA at central@cisa.gov or 888-282-0870
• FBI Field Office: http://www.fbi.gov/contact-us/field or the FBI’s 24-7 Cyber Watch at 855-292-3937 or by e-mail at cywatch@fbi.gov
Information sharing is the key to preventing a wide-spread cyber-attack. CISA develops partnerships to rapidly share critical information about cyber incidents.

Cybersecurity Alerts & Advisories

- Offers the latest cybersecurity news, advisories, alerts, tools, and resources.
- Found at:
  
  https://www.cisa.gov/news-events/cybersecurity-advisories

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Release Date: May 24, 2023
Alert Code: AA23-144A
Reducing Risk of Known Exploited Vulnerabilities

CISA's Known Exploited Vulnerabilities Catalog

The following sections detail the criteria behind each of the three thresholds for KEV catalog updates, which are:

- The vulnerability has an assigned Common Vulnerabilities and Exposures (CVE) ID.
- There is reliable evidence that the vulnerability has been actively exploited in the wild.
- There is a clear remediation action for the vulnerability, such as a vendor-provided update.

https://www.cisa.gov/known-exploited-vulnerabilities-catalog
PUT YOUR ONLINE SAFETY ON LOCK.
Secure your network by keeping things fresh.

Cyber Lessons
Arm yourself with knowledge to stay ahead of the game. Get started.

MULTI-FACTOR AUTHENTICATION
Double up on your login protection.

WI-FI SAFETY
Stay protected while connected.

OVERSHARING & GEOTAGGING
Never click and sell.

APP SECURITY
Keep tabs on your apps.

https://www.cisa.gov/be-cyber-smart
ONLINE SAFETY + PRIVACY BASICS

- Reporting Cybercrime
  September 13, 2023  9 min read

- How to Tell If Your Computer Has a Virus and What to Do About It
  February 13, 2023  10 min read

- Hacked Accounts: What to Do Right Now
  April 27, 2023  8 min read

- Share with Care: Staying Safe on Social Media
  April 27, 2023  8 min read

- Manage Your Privacy Settings
  May 26, 2022  2 min read

- Phishing
  March 10, 2023  5 min read

View all Online Safety + Privacy Basics Resources

https://staysafeonline.org/

J.D. Henry
October 6, 2023
"If You See Something, Say Something®" is a national campaign that raises public awareness of the signs of terrorism and terrorism-related crime, and how to report suspicious activity to state and local law enforcement.

To become a partner, send an email to: seesay@hq.dhs.gov

For more information visit: www.dhs.gov/see-something-say-something
All CISA services and resources can be found by visiting www.CISA.gov
Questions?

Central@CISA.GOV
888-282-0870

Joseph “JD” Henry
Cybersecurity Advisor
Joseph.Henry@cisa.dhs.gov
Kelley Kiernan
DON SBIR/STTR Program Office

**STATEMENT OF LIMITATION OF AUTHORITY:** You are hereby notified that I do not have the authority to direct you in any way to alter your contractual obligations. Further, if the Department of the Navy, as the result of the information obtained from discussions or emails, does desire to alter your contract requirements, changes will be issued in writing and signed by the contracting officer. You should take no action on any change unless and until you receive such a contract modification.
Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DON CISO Blue Cyber Educational Series and be found [here](#)!
- Please provide questions, feedback or if you just want to talk about your cybersecurity/data protection questions to Kelley.Kiernan@us.af.mil

➤ **Daily** Office Hours for answering/researching your questions about DON Small Business cybersecurity and data protection!

**Every Tuesday**, 1pm Eastern, dial in for the DON CISO’s Small Business Cybersecurity Ask-Me-Anything. Register at [www.sbir.gov/events](http://www.sbir.gov/events)