Local Government Cyber Training

OHIO CYBER PROGRAMS AND RESOURCES

CyberOhio

https://www.oc3.ohio.gov/
https://cyber.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Mark Bell is the Cyber Security Outreach Coordinator for the Adjutant General's Department of Ohio.

Mark coordinates a wide range of cyber partners throughout Ohio, organized into the Ohio Cyber Collaboration Committee (OC3,) to improve the cyber security posture of the state through education and workforce development, the creation of the Ohio Cyber Range, the development of cyber response teams for Ohio, cyber exercises, and the sharing of best cyber practices and policies throughout the state. Mark is also the Chairman of the Ohio Cyber Range Institute's (OCRI) Executive Committee which provides strategic oversight for the Ohio Cyber Range.

Prior to working for the Ohio National Guard, Mark worked for 26 years as a congressional staffer for former congressmen John R. Kasich and Patrick J. Tiberi, serving in a variety of roles from case worker to Chief of Staff.

Mark is also a retired Military Police Command Sergeant Major. During his almost 29 years in the United States Army Reserve, Mark performed many different Military Police functions in both a reserve and deployed capacity and served in a variety of leadership positions at the Company, Battalion, Brigade and Division level. He also served as an adjunct professor of military science at Capital University. His last assignment was serving as the Division Command Sergeant Major of the newly created 87th Training Division located in Birmingham, Alabama.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

The Threat

- Cyber crime is projected to cost the global economy $10.5 trillion by 2025, more than 10 times the cost since 2015. Average per attack is 9.48 million.
- There were over 4,100 recorded data breaches and those breaches exposed 22 billion records in 2023
- The cyber-insurance industry is already estimated to be worth well over $10.33 billion growing to 27.8 billion by 2026.
- Multiple firms project that by 2025, 19 billion devices will be connected to the "Internet of things," a huge growth in the number of devices that connect ever more of daily life to the Web.
- Prevention is cheaper than remediation.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Threat Actors

- Nation State actors
- Criminal enterprises
- Intellectual property theft/industrial espionage
- "Hacktivists"/terrorists
- Personal/political attacks/insiders
- Malicious Acts/Vandalism
- Rogue Malware

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Types of Attacks

- Phishing – emails over 90% of attacks, Vishing, Smishing, Spear Fishing, whaling
  https://www.cisa.gov/sites/default/files/publications/phishing-infographic-508c.pdf
  Block (SPF DKIM DMARC), Educate, Report, Protect (segment, least privilege, updates)
- Ransomware – Every 14 seconds – New threat - Blackmail
- DOS/DDOS Attacks - (distributed denial-of-service) attempts to disrupt normal web traffic and take a site offline by overwhelming a system, server or network with more access requests than it can handle.
- "Man in the middle" – Public wi-fi or weak link on your own network
- Social Engineering
- Insider attacks/physical security/vendor 3rd party corruption
- Password attacks/hacks/brute force
- "Typo squatting" fake login pages, click jacking
- Viruses/other Malware

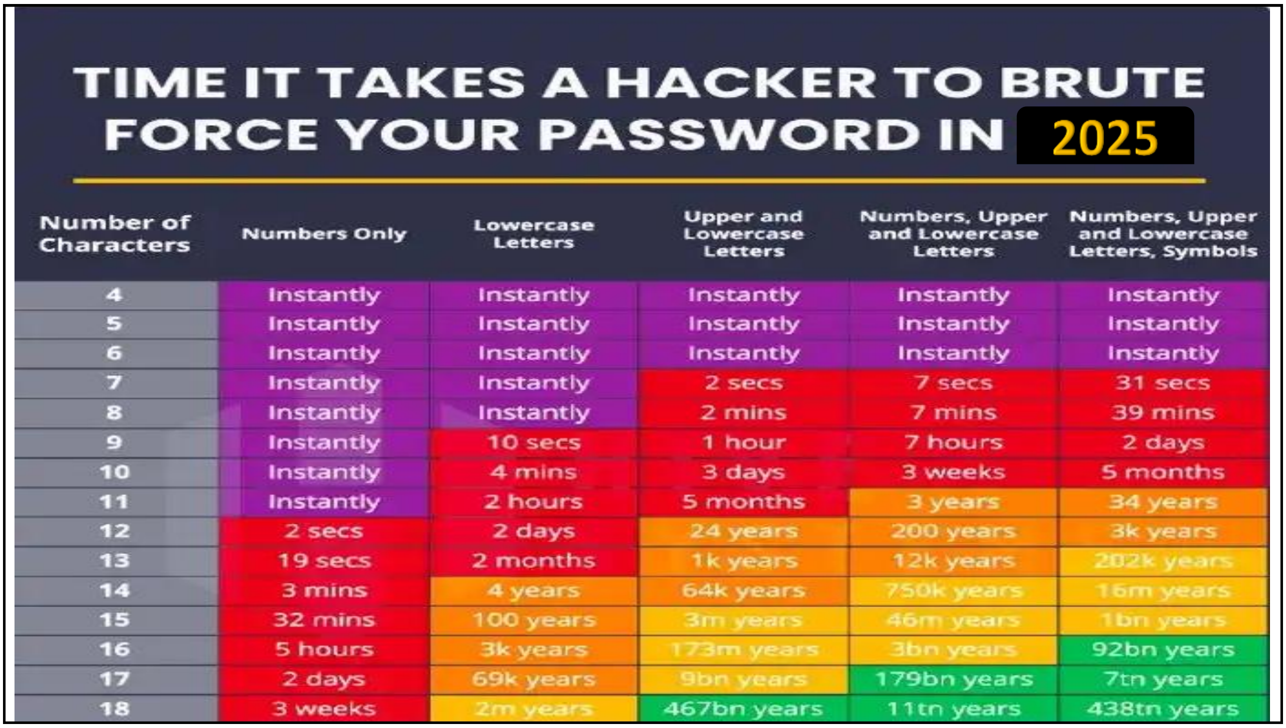
https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Common Vectors of Attack

- Emails and email attachments
- Unpatched vulnerabilities – OS, Apps
- Compromised/weak credentials (username/password)
- Infected downloads (Trojan horse)
- Compromised thumb drives/CDs/DVDs/SD cards
- Malicious links/advertising/QR codes, Domain Shadowing
- Drive by downloads (infected web sites)
- Man in the middle, Open Wi-Fi or weak link on your own network
- Windows Macros
- Deception/social engineering
- Unsecured venders/support programs

https://www.oc3.ohio.gov/



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2025

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HB 96 Requirements

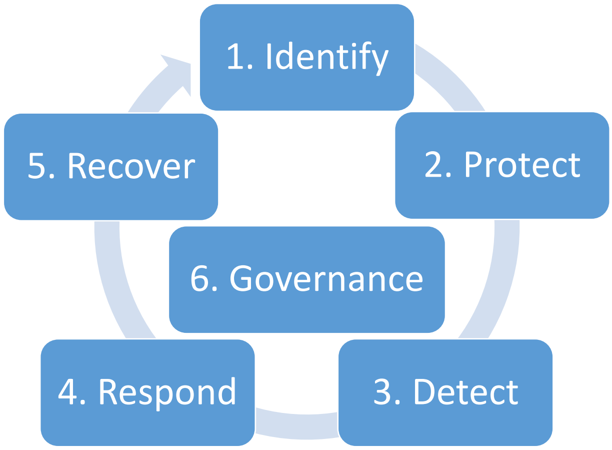
- Passed June 30th, took effect Sept 30, 2025
- Defines a Cyber Incident
- Defines an LGE
- Defines Ransomware
- Restrictions on paying ransomware
- LGEs shall adopt a cyber program, shall be consistent with best practices
- Notification Requirements
- Public Records exceptions for cyber information

CyberOhio

https://www.oc3.ohio.gov/
https://cyber.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework



1. Identify

2. Protect

3. Detect

4. Respond

5. Recover

6. Governance

https://www.oc3.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework

1. Identify (Cyber Inventory)

- Hardware
- Software
- Network Map
- Data
- Governance

https://www.oc3.ohio.gov/

Inventory Your Hardware (Identify)

- All physical items that touch your network, both wired and wireless
- Do both physical inventory and auto scan

- Manufacture, name and model number, date made/purchased, OS/Firmware, Still supported?
- Country of origin
- Status of updates, how done: manual, automatic, central management
- Date item goes out of service (notes from refresh plan)
- Location of device
- Any “shadow” equipment or personal devices

https://www.oc3.ohio.gov/

Inventory Your Software (Identify)

- All apps and programs that exist anywhere on the network
- Do both physical inventory and auto scan

- Manufacture, name and version number, date made/purchased, Still supported?
- Country of origin
- Status of updates, how done: manual, automatic, central management
- Date item goes out of service (notes from refresh plan)
- Location of app or software

https://www.oc3.ohio.gov/

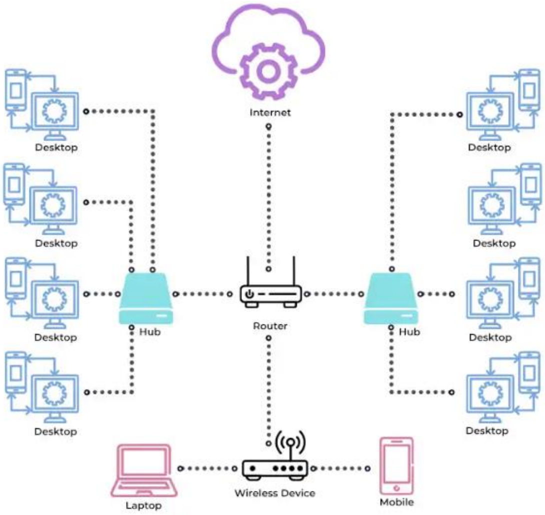
Create Network Map (Identify)

- Show all devices: servers, endpoints, peripherals, firewalls, routers, switches LANS and VLANS

- Do both physical inventory and auto scan
- Show segmentation, LANS, VLANS
- Use notes to detail restricted access points and physical security and location of critical hardware

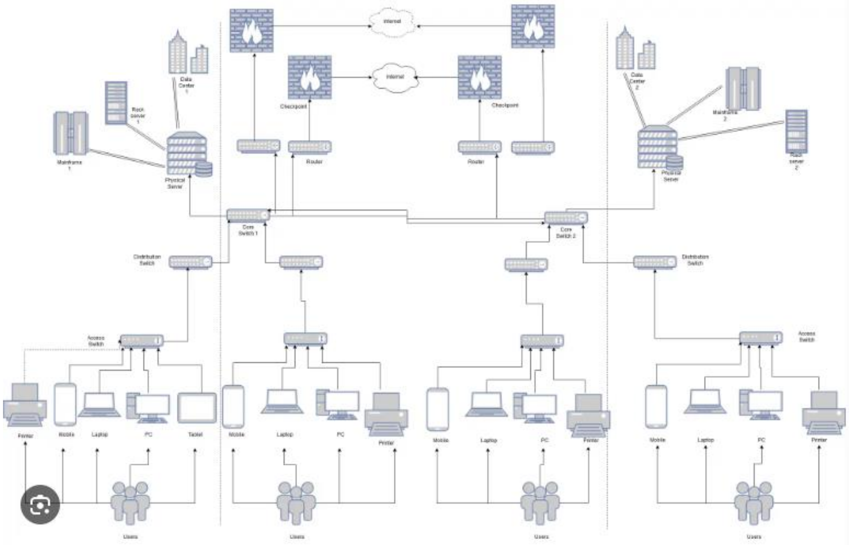
https://www.oc3.ohio.gov/

Network Map (Identify)



https://www.oc3.ohio.gov/

Network Map (Identify)



https://www.oc3.ohio.gov/

Inventory Your Data (Identify)

- What Data do you have?
- Where is it?
- Who can access it?
- How is it protected?

https://www.oc3.ohio.gov/

Inventory Your Data (Identify)

Classifications:

- Public: Data that can be freely shared with the public. Example: Agency press releases.
- Internal: Data intended for internal use only. Example: Staff meeting notes.
- Confidential: Data that requires protection due to its sensitive nature. Example: Employee payroll information.
- Restricted: Data that demands the highest level of security. Example: Criminal investigation records.

Inventory Your Data (Identify)

1. Identify Data and Storage Locations: Begin by cataloging all data within the organization. This includes examining backups, old servers, cloud storage, and databases. Check for rogue downloads on individual devices and unauthorized data storage, as these can pose significant security risks.
2. Encryption and Access Controls: Understand how data is encrypted both at rest and in motion. Review the segmentation and access controls for critical data to ensure they are robust and effective. This step is vital in preventing unauthorized access and ensuring data integrity.
3. Encryption Practices: Ensure that no critical data is stored in plain text. Use strong encryption methods and maintain the security of encryption keys. Regularly review and update your encryption practices to stay ahead of potential threats.
4. Data Retention Policies: Assess your data retention policies. Delete any data that is no longer needed or archive it offline. This practice aligns with the principle that the easiest way to protect data is not to have it. Only retain data that is required by law, regulation, or necessary for operations. Once you have identified the essential data, focus on securing it.

Inventory Your Data (Identify)

Identifying Potential Vulnerabilities

Recognizing and addressing potential vulnerabilities is essential for maintaining data security.

1. Vulnerable Points: Identify vulnerable points based on the type and classification of data. For example, sensitive data stored on devices without encryption is a significant risk.

2. Outdated Devices and Software: Understand the risks associated with outdated devices and software, especially where classified data is stored or accessed. Regular updates and patches are necessary to mitigate these risks

https://www.oc3.ohio.gov/

Inventory Your Data (Identify)

Prioritizing Assets and Data for Protection

Not all data and assets are equally critical. Prioritizing them helps in focusing security efforts where they are most needed.

1. Assess Impact: Assess which assets and types of data would have the most significant impact if compromised. This helps in identifying high-priority data that requires immediate and robust protection measures.

2. Implement Protections: Identify protections to apply immediately, especially for high priority data. This includes encrypting restricted data and limiting access to sensitive information.

https://www.oc3.ohio.gov/

Inventory Your Data (Identify)

Data Encryption and Backup Strategies

Encrypt data at rest and in transit

Data encryption is a fundamental practice for protecting sensitive information. LGEs should ensure that all sensitive data is encrypted both at rest and in transit. This means that data stored on devices and transmitted over networks is protected from unauthorized access.

Backup your data

Regular data backups are essential for data recovery in case of a cyber incident. LGEs should implement a backup strategy that includes regular backups to secure off-site storage locations.

Current better practice is known as the 3-2-1 rule.

- 3 copies of data, 1 golden backup with 2 redundant copies
- 2 different media types such as a local backup server and cloud storage.
- 1 copy off-site for resilience in the event of a catastrophic event (fire, flood, industrial accident).

These backups should be tested periodically to ensure they can be restored successfully

https://www.oc3.ohio.gov/

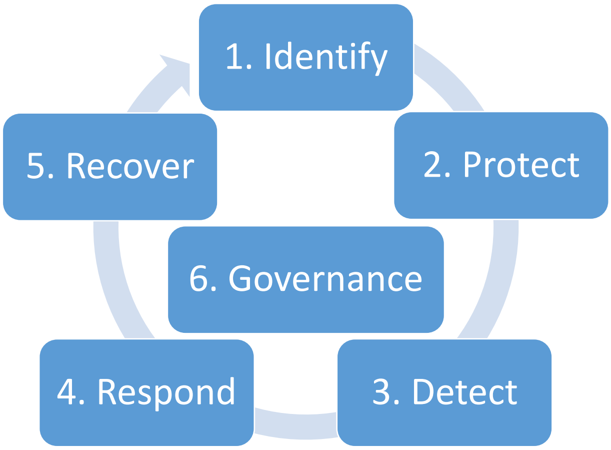
Inventory Your Governance (Identify)

- Identify all cyber plans, policies, agreements and contracts
- Do you have cyber insurance? Review policy and requirements
- Review roles and responsibilities
- Review laws and regulatory guidance as applies to your operation
- Identify any shortcomings in governance

https://www.oc3.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework



CyberOhio

https://www.oc3.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework

2. Protect

NSA how to protect your home network - https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3304674/nsa-releases-best-practices-for-securing-your-home-network/

NSA top 10 - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

CIS top 18 - https://www.cisecurity.org/controls/cis-controls-list

NIST 800-53 - https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

CyberOhio

https://www.oc3.ohio.gov/

Protection Steps (Protect)

- Create strong passwords for your accounts.
- Create unique passwords for each account.
- Consider using a password manager to simplify password management.
- Enable account lockout after 5 failed logon attempts
- Enable Multi Factor Authentication (MFA) on every possible account and device.

o Mandate MFA for administrator access

- Provide home network cybersecurity better practices to your remote/hybrid workforce.
- Separate administrator accounts from routine daily work accounts.
- Change passwords or disable default accounts on network devices and in software applications
- Revoke credentials for departing staff. Disable all accounts when an employee leaves. Collect all key cards, security tokens, door keys.
- Improve physical security. Restrict access to areas where sensitive data is stored.
- Apply software updates as soon as possible.
- Plan migration from Windows 10. Windows 10 end of support date was 10/14/2025.
- Encrypt data at rest and in transit.
- Establish routine backup policy

o Test backups to verify processes

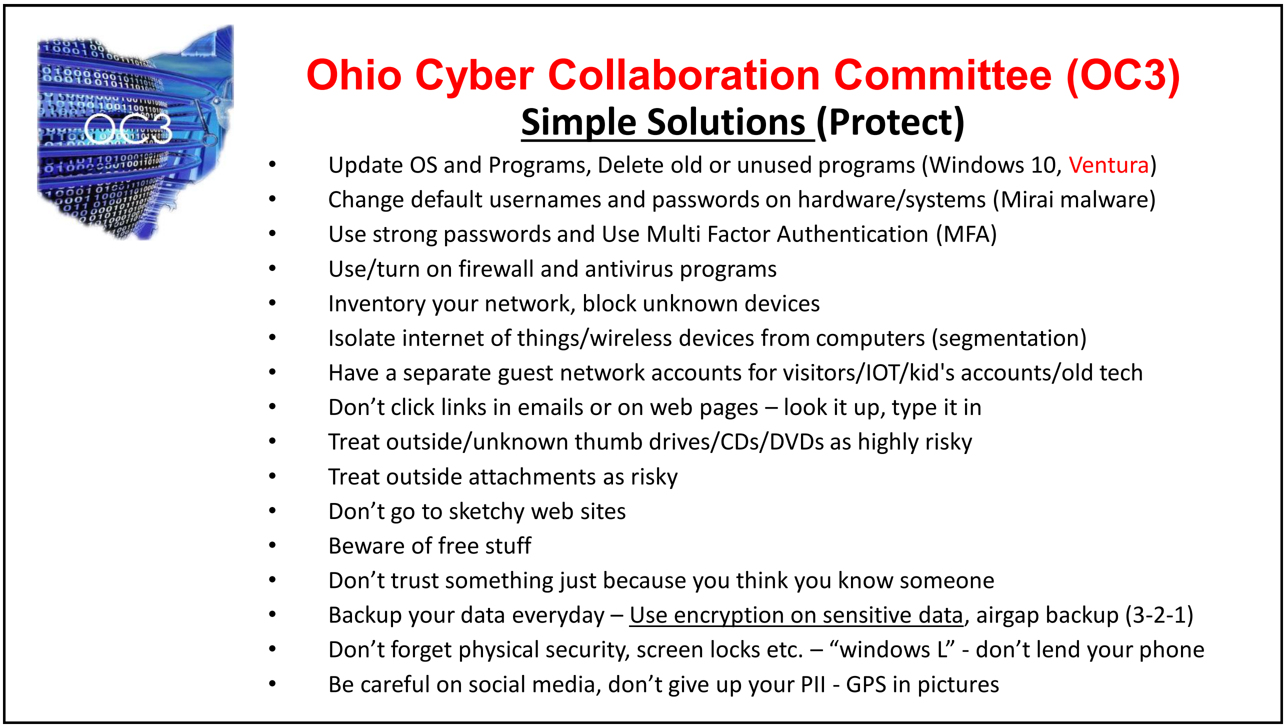
- Explore migration to *.gov domain

Ohio Cyber Collaboration Committee (OC3)

Password Strategies (Protect)

- Never reuse or duplicate passwords
- use long complex passwords – 15 minimum with numbers, upper- and lower-case letters, and symbols - longer is better (74 characters per slot)
- Avoid words in the dictionary, part of your name, where you work, your school, the current year, DOB, anniversaries, pets' names, etc.
- Use embeds
- Use the first letters of phrases i.e. The Beatles The Long and Winding Road – $TlAwRtLtYdWnDiStRb76 21 characters, all 4 options, no dictionary words - (trillions of years to brute force attack!)
- Use a password manager (does have some risks)
- Add multi factor authentication (something you know with something you have) i.e. password plus cell phone and pin number
- Set maximum number of tries, then lock out or freeze account
- Change password any time something bad happens

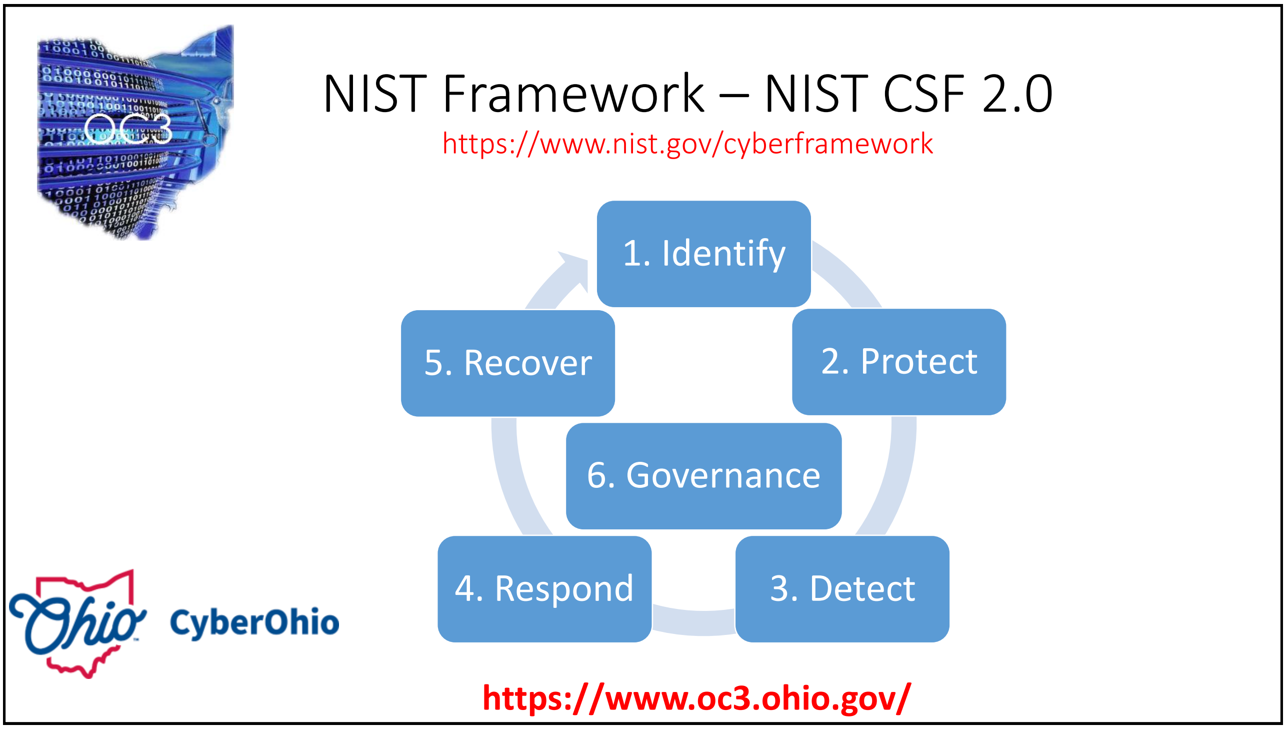
https://www.oc3.ohio.gov/



Ohio Cyber Collaboration Committee (OC3)

Simple Solutions (Protect)

- Update OS and Programs, Delete old or unused programs (Windows 10, Ventura)
- Change default usernames and passwords on hardware/systems (Mirai malware)
- Use strong passwords and Use Multi Factor Authentication (MFA)
- Use/turn on firewall and antivirus programs
- Inventory your network, block unknown devices
- Isolate internet of things/wireless devices from computers (segmentation)
- Have a separate guest network accounts for visitors/IOT/kid's accounts/old tech
- Don’t click links in emails or on web pages – look it up, type it in
- Treat outside/unknown thumb drives/CDs/DVDs as highly risky
- Treat outside attachments as risky
- Don’t go to sketchy web sites
- Beware of free stuff
- Don’t trust something just because you think you know someone
- Backup your data everyday – Use encryption on sensitive data, airgap backup (3-2-1)
- Don’t forget physical security, screen locks etc. – “windows L” - don’t lend your phone
- Be careful on social media, don’t give up your PII - GPS in pictures



NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework

https://www.oc3.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework

3. Detect

Need to monitor your network to see what is happening

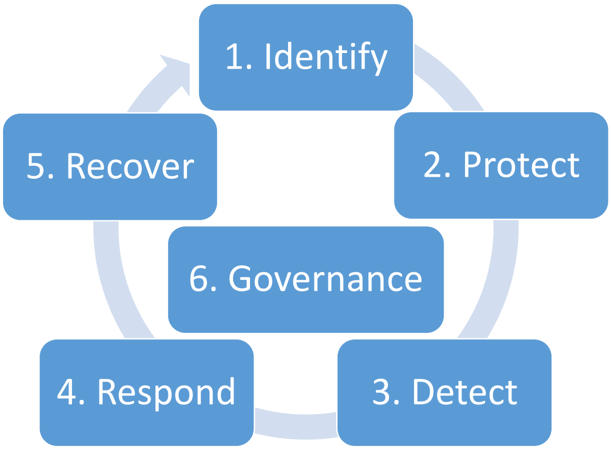
- Antivirus software
- Endpoint detection/Endpoint detection and response software
- SIEM – Security Information and Event Management
- SOAR - Security Orchestration, Automation and Response
- SOC – Security Operations Center
- Review logs and alerts to take action before malware event – forensics will help during response phase

CyberOhio

https://www.oc3.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework



CyberOhio

https://www.oc3.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework

4. Respond

- Develop an Incident Response Plan – Unique to your organization
  - Have hard copy, train all users in what to do/who to call, practice the plan (TTX)
  - Have agreement with venders if needed
  - Cyber Reserve is a resource
- Develop a Continuity of Operations Plan (COOP)

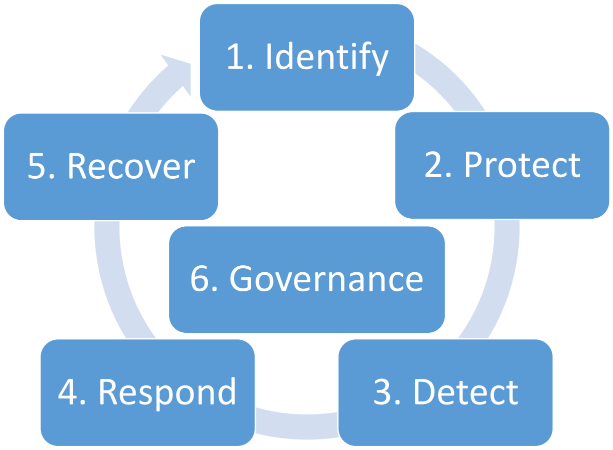
- Identify critical operations, train employees, practice plan

CyberOhio

https://www.oc3.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework



1. Identify

2. Protect

3. Detect

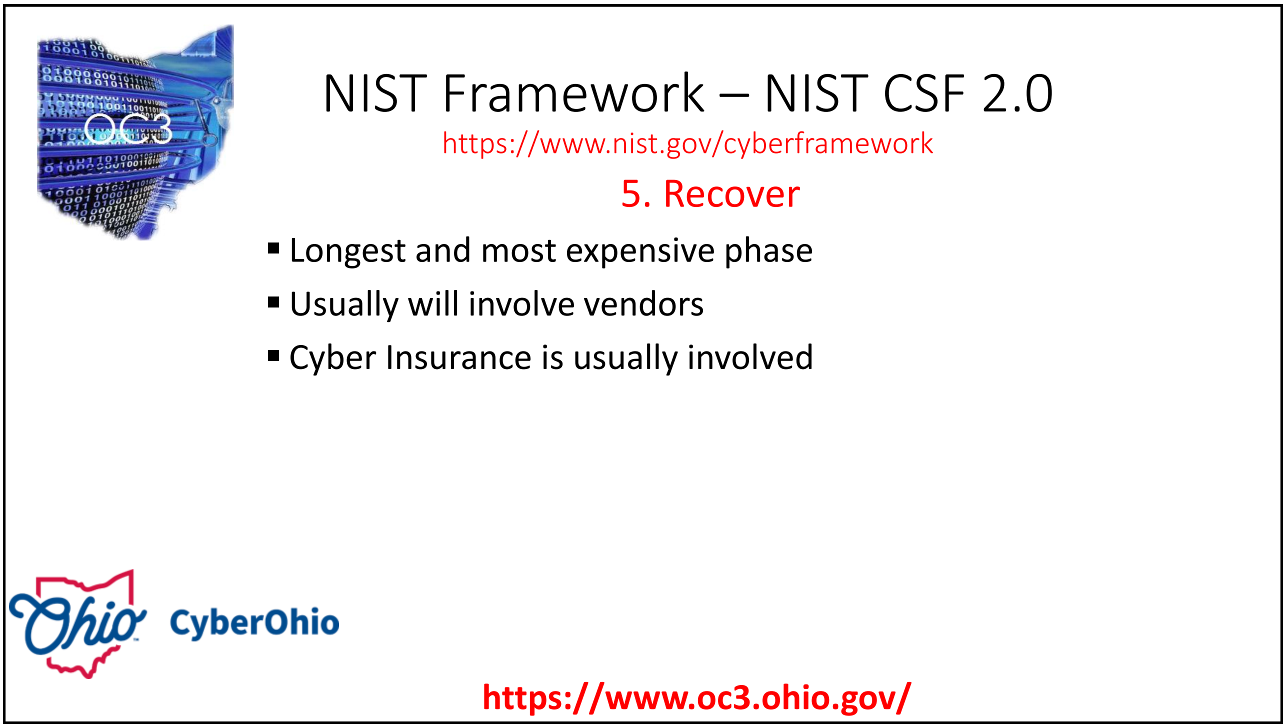
4. Respond

5. Recover

6. Governance

CyberOhio

https://www.oc3.ohio.gov/



NIST Framework – NIST CSF 2.0

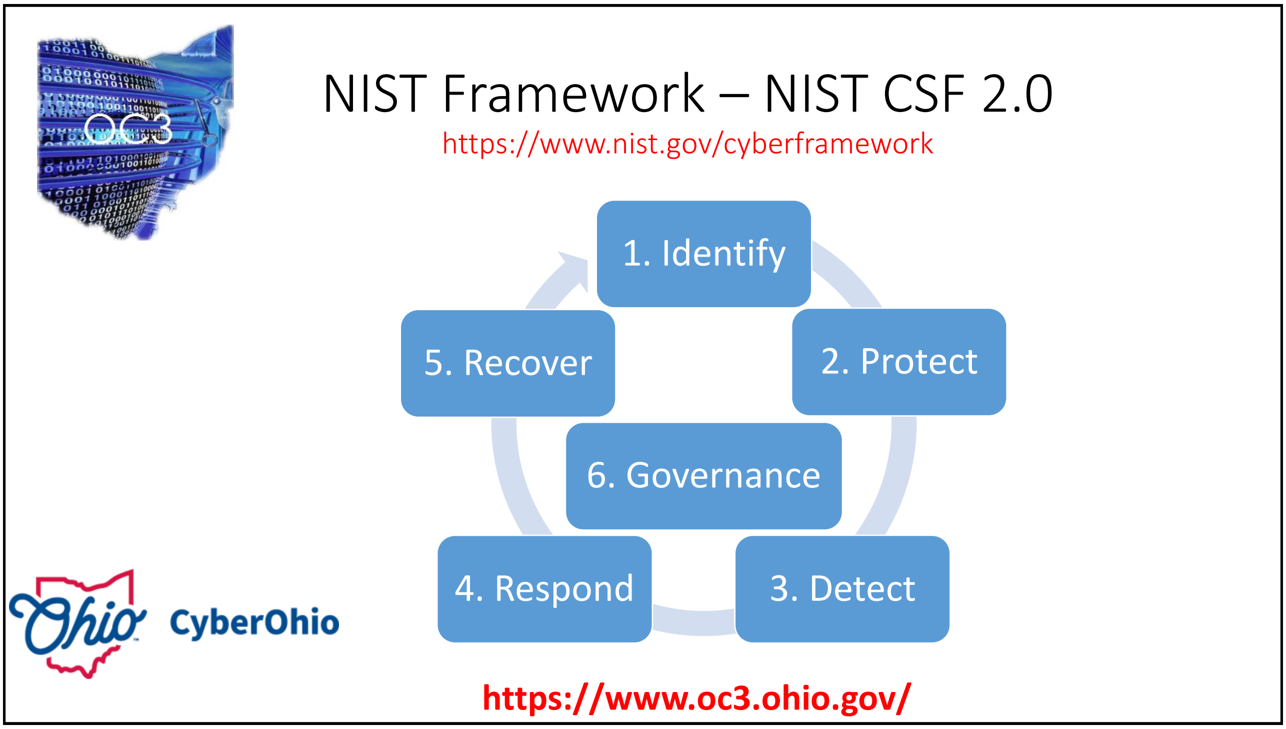
https://www.nist.gov/cyberframework

5. Recover

- Longest and most expensive phase
- Usually will involve vendors
- Cyber Insurance is usually involved

OC3
Ohio
CyberOhio

https://www.oc3.ohio.gov/



NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover
6. Governance

https://www.oc3.ohio.gov/

NIST Framework – NIST CSF 2.0

https://www.nist.gov/cyberframework

6. Governance

- Governance is involved at all times of the process
- Determine framework to follow and draft cyber plan
- Review findings from identify phase, update and correct shortcomings
- Update or draft plans, policies and procedures
- Identify critical processes
- Identify funding requirements

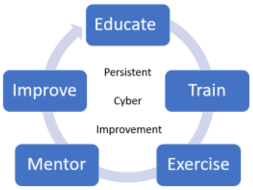
CyberOhio

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Resilience is the Key

- Will never be 100% safe from cyber attack
- Protect as best you can - minimize threat
- Segment network and limit horizontal movement
- Least privilege - limit access to servers and data
- Monitor network in real time/review logs
- Back up data daily / in real time 3/2/1
- Encrypt sensitive data
- Be ready, you will get malware!
- Have a Response and Recovery Plan
- Have a Continuity of Effort Plan
- Practice Plan – TTX
- Goal - Have malware be rare, with limited spread, and fast, full recovery



https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Ohio must posture itself with an enterprise-wide approach that allows for a statewide cyber governance structure. More importantly, Ohio must develop and implement the appropriate authority to provide the capability to respond to and prevent cyber-attacks.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Our Mission: To provide an environment for collaboration between key stakeholders, including education, business and local government to strengthen cyber security for all in the State of Ohio and to develop a stronger cyber security infrastructure.

Our Goals/Committees: OC3 has established three subcommittees to help it achieve its primary goals: Education/Workforce Development, Cyber Range, Cyber Protection and Preparedness. The committees are composed of Ohioans with a wide range of cyber and educational expertise dedicated to making Ohio a leader in how to integrate public-private partnerships into solving the cyber security problem.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Education/Workforce Development Subcommittee:

Grow the workforce and improve the training and education of users and students in cyber security by:

a. Encouraging individuals of all ages to consider cyber security as a career, help individuals to further develop their cyber security skills at the K-12 and higher education level or as adult learning.

b. Identifying critically needed skills and developing training and educational paths to meet the growing need for skilled workers in the cyber security field. Giving students the hands-on experience needed to be ready to work on day one.

c. Training users/students at all levels in good, age appropriate, cyber hygiene and best cyber security practices.

d. Provide educators the skills and tools needed to support this growing workforce.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Ohio Cyber Range/OCRI:

Provide a secure cyber security test and training environment, known as a cyber range, to:

a. Support the education of students at the K-12 and University level.

b. Conduct cyber security exercises and competitions to hone cross organizational incident response capabilities and develop future cyber security professionals.

c. Research and test industry-standard best practices, evaluate and test innovative technologies and processes.

d. Enable a training environment for the current and future cyber security workforce, including National Guard personnel, state and local government personnel, faculty and students in the education community, and private sector entities.

e. Provide a Cyber Portfolio for learners, and support internships.

f. Will be able to connect from any location with OARnet access.

https://www.oc3.ohio.gov/

Ecosystem

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE
POWERED BY UNIVERSITY OF CINCINNATI

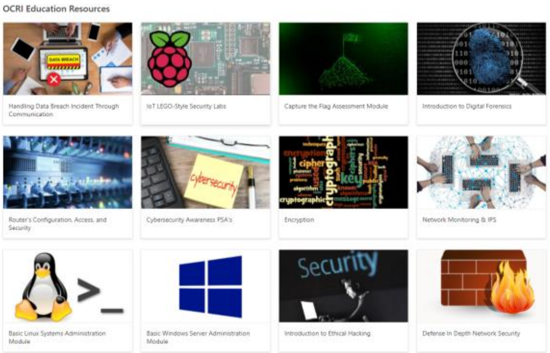
Regional Programming Centers

Bowling Green State University
Cedarville University
Cin-Day Cyber at SOCHE
Cleveland State/Case Western IoT Collaborative
Cuyahoga Community College
Kent State University
Lorain County Community College
Miami University
Ohio State University
Ohio University
Owens Community College
PAST Foundation
Rio Grande Community College
Shawnee State University
Stark State College
Tiffin University & Findlay Partners
University of Akron
University of Cincinnati
University of Dayton

OWENS
BGSU
TU
Lcc
Cuyahoga Community College
KENT STATE UNIVERSITY
Stark State
MIAMI UNIVERSITY
University of Dayton
CEDARVILLE UNIVERSITY
OHIO STATE
OHIO UNIVERSITY
RIO GRANDE
Shawnee State UNIVERSITY
University of CINCINNATI
OHIO CYBER RANGE INSTITUTE

OCRI Education Module Library

- A collection of learning materials
  - Instructional materials
  - Assessment materials
  - Hands-on component
- Geared towards K-12, Higher Ed, and/or Workforce Development
- Developed to be shared
  - Choose parts to develop your own courses
  - Build upon what others have created
  - Contribute and collaborate



OCRI Education Resources

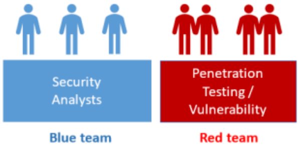
Handling Data Breach Incident Through Communication
IoT LEGO-Style Security Labs
Capture the Flag Assessment Module
Introduction to Digital Forensics
Router's Configuration, Access, and Security
Cybersecurity Awareness PSA's
Encryption
Network Monitoring & IPS
Basic Linux Systems Administration Module
Basic Windows Server Administration Module
Introduction to Ethical Hacking
Defense In Depth Network Security

https://www.ohiocyberrangeinstitute.org/

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

OpFor v Blue Pilot Exercise:

- Capture the Flag (CTF)
- Red Team vs. Blue Team



https://www.ohiocyberrangeinstitute.org/

OC3 Cyber Protection Subcommittee

Deliverables

→ **Ohio Cybersecurity Strategic Plan**

→ **K-12 Cyber Challenge – IN PROGRESS**

→ **OC3 Website Development**

→ **Cyber TTX Exercises – IN PROGRESS**

→ **Cyber Toolkit / User's Guidebook of Best Practices – IN PROGRESS**

→ **Mock Cyber Incident**

→ **Cyber Risk Assessment**

→ **Best practices/public awareness**

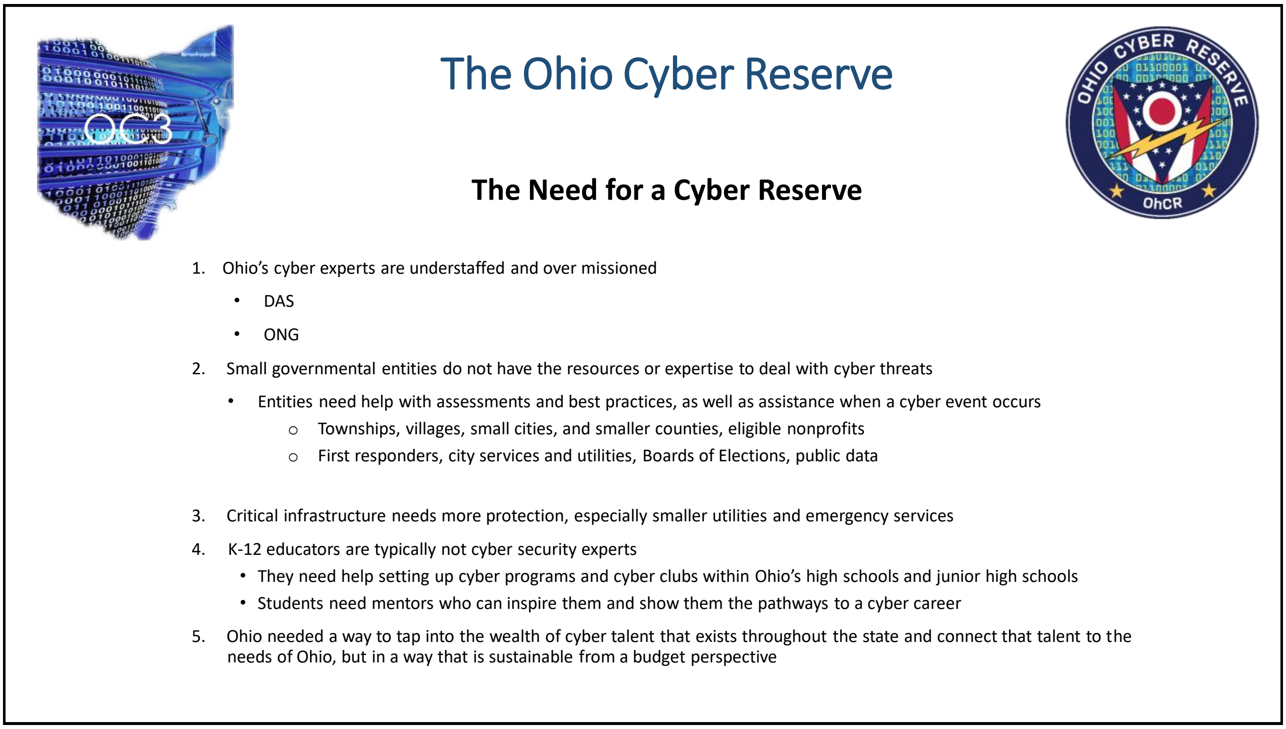
→ **Ransomware Awareness Campaign**

https://www.oc3.ohio.gov/

The Ohio Cyber Reserve

Bringing Cyber Talent to the Fight

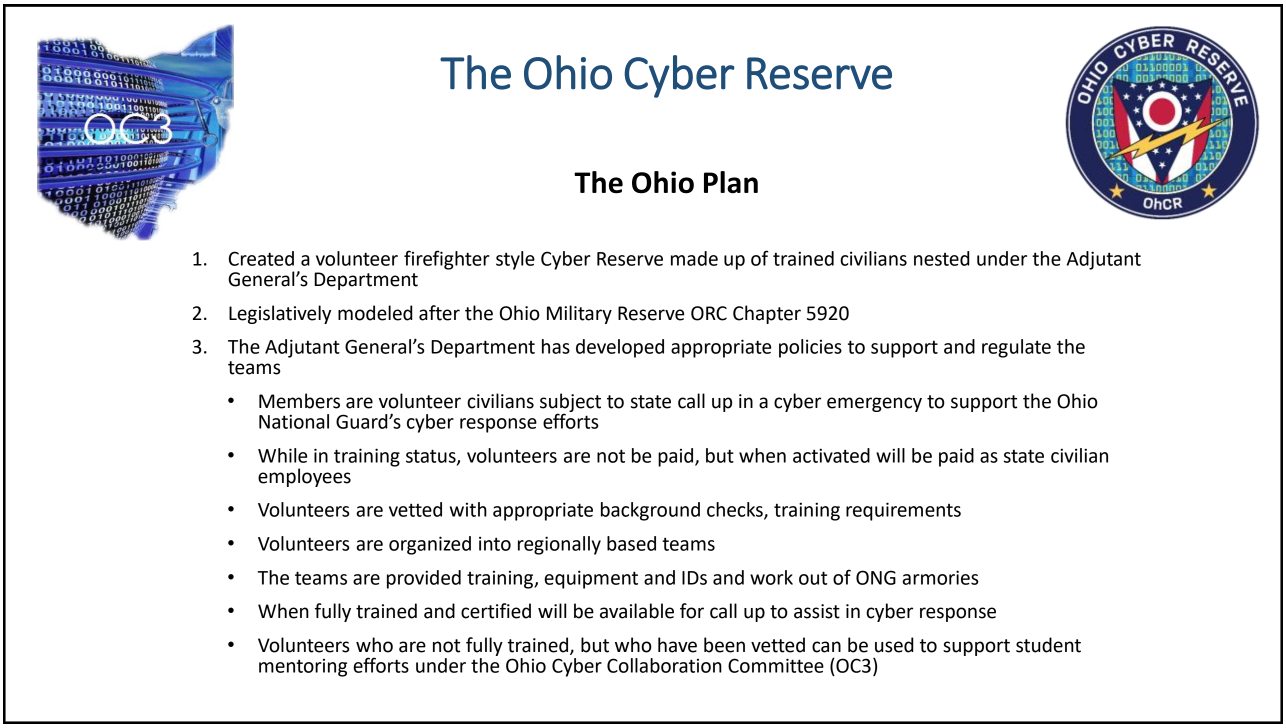
https://ohcr.ohio.gov/



The Ohio Cyber Reserve

The Need for a Cyber Reserve

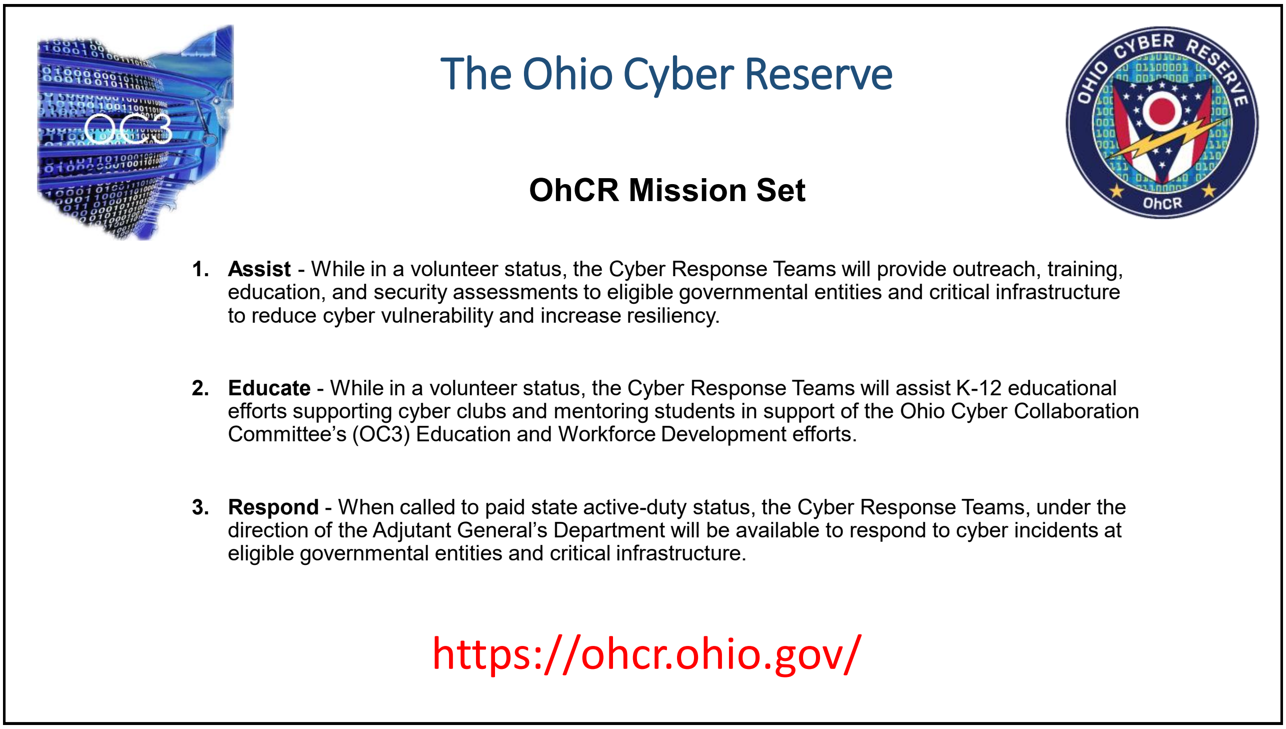
1. Ohio’s cyber experts are understaffed and over missioned
   - DAS
   - ONG
2. Small governmental entities do not have the resources or expertise to deal with cyber threats
   - Entities need help with assessments and best practices, as well as assistance when a cyber event occurs
     - Townships, villages, small cities, and smaller counties, eligible nonprofits
     - First responders, city services and utilities, Boards of Elections, public data
3. Critical infrastructure needs more protection, especially smaller utilities and emergency services
4. K-12 educators are typically not cyber security experts
   - They need help setting up cyber programs and cyber clubs within Ohio’s high schools and junior high schools
   - Students need mentors who can inspire them and show them the pathways to a cyber career
5. Ohio needed a way to tap into the wealth of cyber talent that exists throughout the state and connect that talent to the needs of Ohio, but in a way that is sustainable from a budget perspective



The Ohio Cyber Reserve

The Ohio Plan

1. Created a volunteer firefighter style Cyber Reserve made up of trained civilians nested under the Adjutant General's Department
2. Legislatively modeled after the Ohio Military Reserve ORC Chapter 5920
3. The Adjutant General's Department has developed appropriate policies to support and regulate the teams
   - Members are volunteer civilians subject to state call up in a cyber emergency to support the Ohio National Guard's cyber response efforts
   - While in training status, volunteers are not be paid, but when activated will be paid as state civilian employees
   - Volunteers are vetted with appropriate background checks, training requirements
   - Volunteers are organized into regionally based teams
   - The teams are provided training, equipment and IDs and work out of ONG armories
   - When fully trained and certified will be available for call up to assist in cyber response
   - Volunteers who are not fully trained, but who have been vetted can be used to support student mentoring efforts under the Ohio Cyber Collaboration Committee (OC3)



The Ohio Cyber Reserve

OhCR Mission Set

1. **Assist** - While in a volunteer status, the Cyber Response Teams will provide outreach, training, education, and security assessments to eligible governmental entities and critical infrastructure to reduce cyber vulnerability and increase resiliency.

2. **Educate** - While in a volunteer status, the Cyber Response Teams will assist K-12 educational efforts supporting cyber clubs and mentoring students in support of the Ohio Cyber Collaboration Committee's (OC3) Education and Workforce Development efforts.

3. **Respond** - When called to paid state active-duty status, the Cyber Response Teams, under the direction of the Adjutant General's Department will be available to respond to cyber incidents at eligible governmental entities and critical infrastructure.

https://ohcr.ohio.gov/

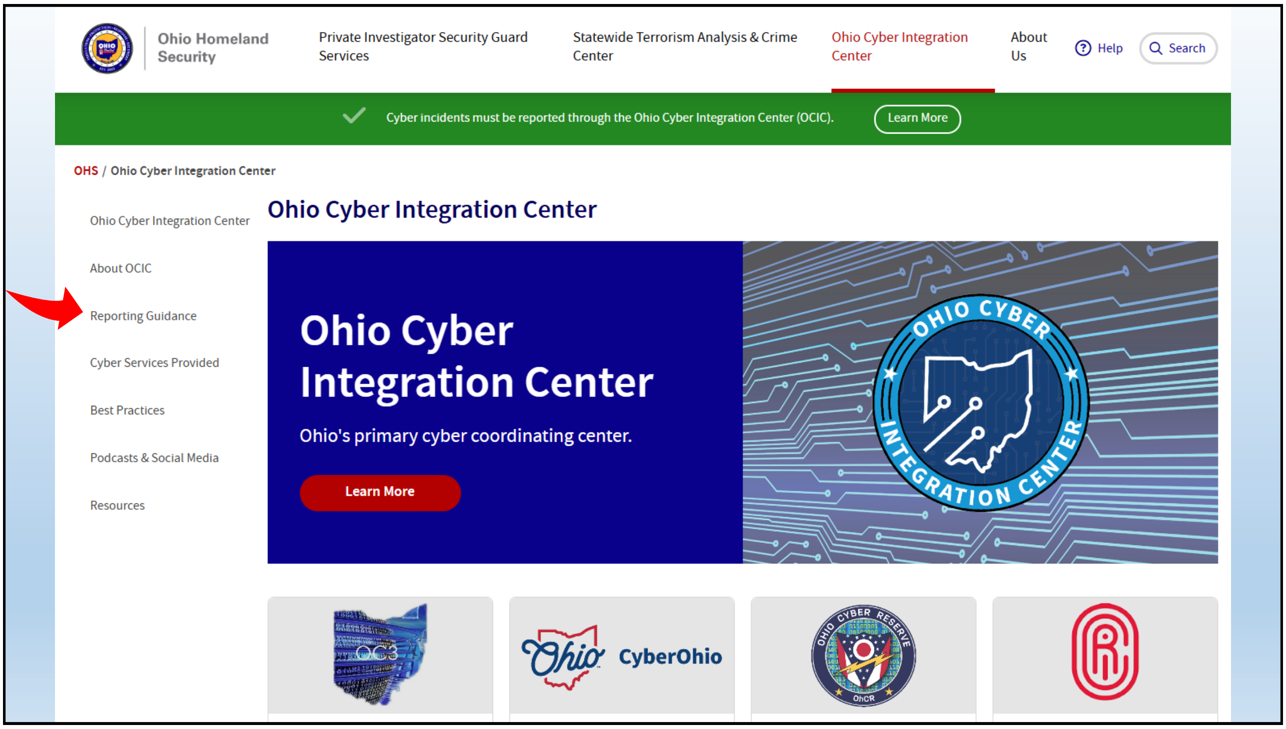
The Ohio Cyber Reserve

Want to be a member?

To join the OhCR or request assistance, go to https://ohcr.ohio.gov/ or email: OhioCyberReserve@ucmail.uc.edu

For more information contact:

Craig Baker
Program Administrator,
Ohio Cyber Reserve (OhCR)
2825 W Dublin Granville Road
Columbus Ohio 43232-2789
O: 614-336-7992
Craig.w.baker2.nfg@army.mil



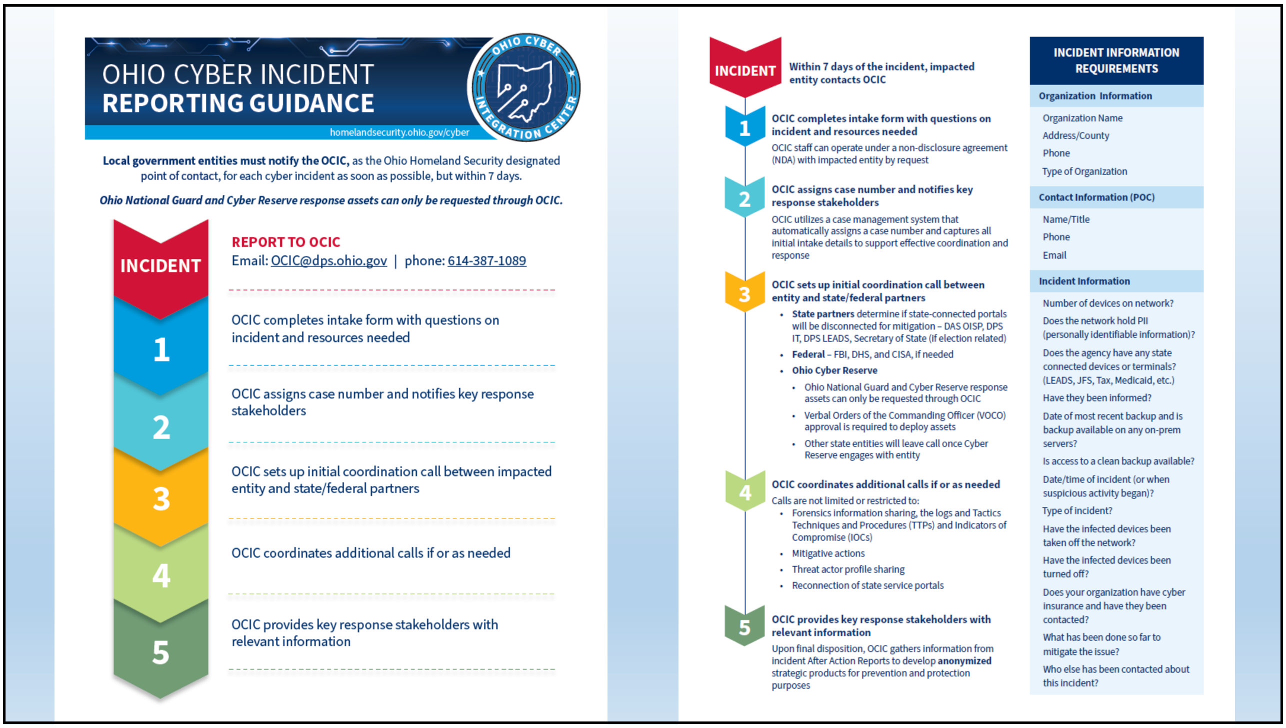
Cyber incidents must be reported through the Ohio Cyber Integration Center (OCIC).

OHS / Ohio Cyber Integration Center

Ohio Cyber Integration Center

Ohio Cyber Integration Center

Ohio's primary cyber coordinating center.



OHIO CYBER INCIDENT REPORTING GUIDANCE

homelandsecurity.ohio.gov/cyber

OHIO CYBER INTEGRATION CENTER

Local government entities must notify the OCIC, as the Ohio Homeland Security designated point of contact, for each cyber incident as soon as possible, but within 7 days.

Ohio National Guard and Cyber Reserve response assets can only be requested through OCIC.

INCIDENT

REPORT TO OCIC
Email: OCIC@dps.ohio.gov | phone: 614-387-1089

1 OCIC completes intake form with questions on incident and resources needed

2 OCIC assigns case number and notifies key response stakeholders

3 OCIC sets up initial coordination call between impacted entity and state/federal partners

4 OCIC coordinates additional calls if or as needed

5 OCIC provides key response stakeholders with relevant information

INCIDENT **Within 7 days of the incident, impacted entity contacts OCIC**

1 **OCIC completes intake form with questions on incident and resources needed**

OCIC staff can operate under a non-disclosure agreement (NDA) with impacted entity by request

2 **OCIC assigns case number and notifies key response stakeholders**

OCIC utilizes a case management system that automatically assigns a case number and captures all initial intake details to support effective coordination and response

3 **OCIC sets up initial coordination call between entity and state/federal partners**

- **State partners** determine if state-connected portals will be disconnected for mitigation – DAS OISP, DPS IT, DPS LEADS, Secretary of State (if election related)
- **Federal** – FBI, DHS, and CISA, if needed
- **Ohio Cyber Reserve**
  - Ohio National Guard and Cyber Reserve response assets can only be requested through OCIC
  - Verbal Orders of the Commanding Officer (VOCO) approval is required to deploy assets
  - Other state entities will leave call once Cyber Reserve engages with entity

4 **OCIC coordinates additional calls if or as needed**

Calls are not limited or restricted to:

- Forensics information sharing, the logs and Tactics Techniques and Procedures (TTPs) and Indicators of Compromise (IOCs)
- Mitigative actions
- Threat actor profile sharing
- Reconnection of state service portals

5 **OCIC provides key response stakeholders with relevant information**

Upon final disposition, OCIC gathers information from incident After Action Reports to develop **anonymized** strategic products for prevention and protection purposes

INCIDENT INFORMATION REQUIREMENTS

Organization Information

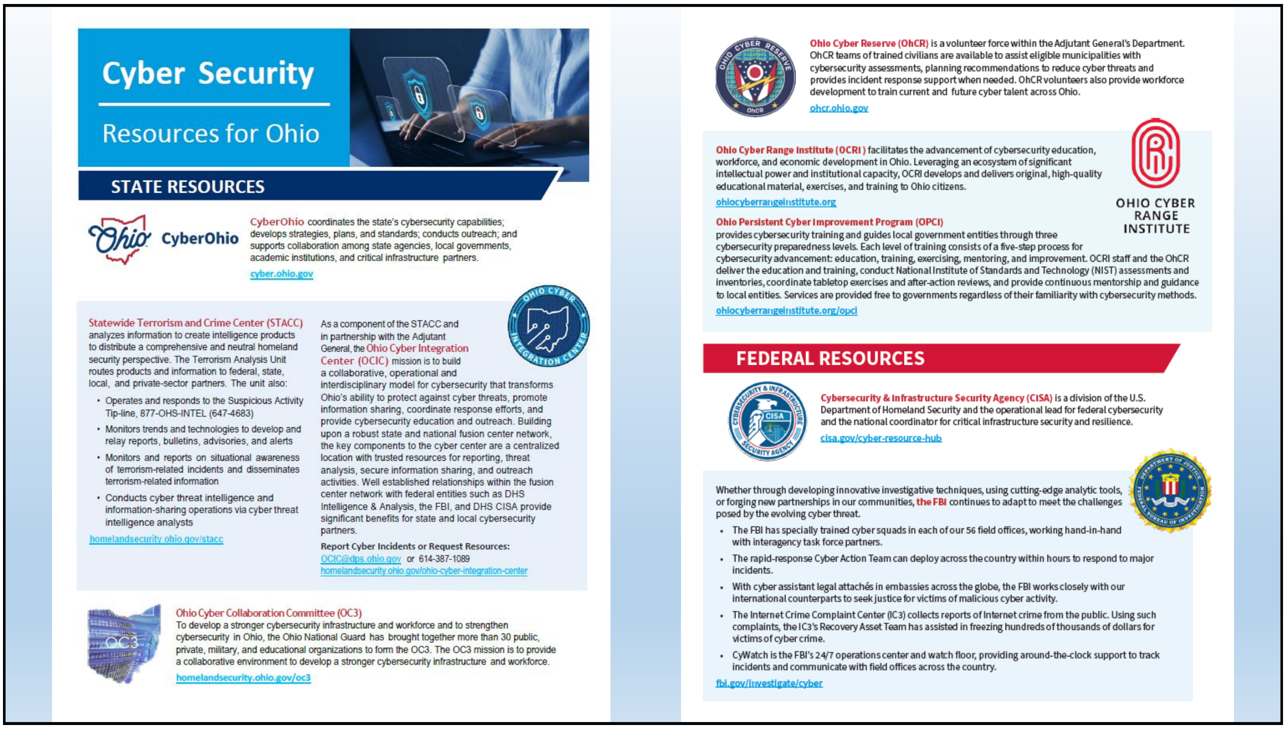
Organization Name
Address/County
Phone
Type of Organization

Contact Information (POC)

Name/Title
Phone
Email

Incident Information

Number of devices on network?
Does the network hold PII (personally identifiable information)?
Does the agency have any state connected devices or terminals? (LEADS, JFS, Tax, Medicaid, etc.)
Have they been informed?
Date of most recent backup and is backup available on any on-prem servers?
Is access to a clean backup available?
Date/time of incident (or when suspicious activity began)?
Type of incident?
Have the infected devices been taken off the network?
Have the infected devices been turned off?
Does your organization have cyber insurance and have they been contacted?
What has been done so far to mitigate the issue?
Who else has been contacted about this incident?



Cyber Security

Resources for Ohio

STATE RESOURCES

CyberOhio coordinates the state's cybersecurity capabilities; develops strategies, plans, and standards; conducts outreach; and supports collaboration among state agencies, local governments, academic institutions, and critical infrastructure partners.

cyber.ohio.gov

Statewide Terrorism and Crime Center (STACC) analyzes information to create intelligence products to distribute a comprehensive and neutral homeland security perspective. The Terrorism Analysis Unit routes products and information to federal, state, local, and private-sector partners. The unit also:

- Operates and responds to the Suspicious Activity Tip-line, 877-OHS-INTEL (647-4683)
- Monitors trends and technologies to develop and relay reports, bulletins, advisories, and alerts
- Monitors and reports on situational awareness of terrorism-related incidents and disseminates terrorism-related information
- Conducts cyber threat intelligence and information-sharing operations via cyber threat intelligence analysts

homelandsecurity.ohio.gov/stacc

As a component of the STACC and in partnership with the Adjutant General, the **Ohio Cyber Integration Center (OCIC)** mission is to build a collaborative, operational and interdisciplinary model for cybersecurity that transforms Ohio's ability to protect against cyber threats, promote information sharing, coordinate response efforts, and provide cybersecurity education and outreach. Building upon a robust state and national fusion center network, the key components to the cyber center are a centralized location with trusted resources for reporting, threat analysis, secure information sharing, and outreach activities. Well established relationships within the fusion center network with federal entities such as DHS Intelligence & Analysis, the FBI, and DHS CISA provide significant benefits for state and local cybersecurity partners.

Report Cyber Incidents or Request Resources:
OCIC@dps.ohio.gov or 614-387-1089
homelandsecurity.ohio.gov/ohio-cyber-integration-center

Ohio Cyber Collaboration Committee (OC3)
To develop a stronger cybersecurity infrastructure and workforce and to strengthen cybersecurity in Ohio, the Ohio National Guard has brought together more than 30 public, private, military, and educational organizations to form the OC3. The OC3 mission is to provide a collaborative environment to develop a stronger cybersecurity infrastructure and workforce.

homelandsecurity.ohio.gov/oc3

Ohio Cyber Reserve (OhCR) is a volunteer force within the Adjutant General's Department. OhCR teams of trained civilians are available to assist eligible municipalities with cybersecurity assessments, planning recommendations to reduce cyber threats and provides incident response support when needed. OhCR volunteers also provide workforce development to train current and future cyber talent across Ohio.

ohcr.ohio.gov

Ohio Cyber Range Institute (OCRI) facilitates the advancement of cybersecurity education, workforce, and economic development in Ohio. Leveraging an ecosystem of significant intellectual power and institutional capacity, OCRI develops and delivers original, high-quality educational material, exercises, and training to Ohio citizens.

ohiocyberrangeinstitute.org

OHIO CYBER RANGE INSTITUTE

Ohio Persistent Cyber Improvement Program (OPCI)
provides cybersecurity training and guides local government entities through three cybersecurity preparedness levels. Each level of training consists of a five-step process for cybersecurity advancement: education, training, exercising, mentoring, and improvement. OCRI staff and the OhCR deliver the education and training, conduct National Institute of Standards and Technology (NIST) assessments and inventories, coordinate tabletop exercises and after-action reviews, and provide continuous mentorship and guidance to local entities. Services are provided free to governments regardless of their familiarity with cybersecurity methods.

ohiocyberrangeinstitute.org/opci

FEDERAL RESOURCES

Cybersecurity & Infrastructure Security Agency (CISA) is a division of the U.S. Department of Homeland Security and the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.

cisa.gov/cyber-resource-hub

Whether through developing innovative investigative techniques, using cutting-edge analytic tools, or forging new partnerships in our communities, **the FBI** continues to adapt to meet the challenges posed by the evolving cyber threat.

- The FBI has specially trained cyber squads in each of our 56 field offices, working hand-in-hand with interagency task force partners.
- The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents.
- With cyber assistant legal attachés in embassies across the globe, the FBI works closely with our international counterparts to seek justice for victims of malicious cyber activity.
- The Internet Crime Complaint Center (IC3) collects reports of Internet crime from the public. Using such complaints, the IC3's Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cyber crime.
- CyWatch is the FBI's 24/7 operations center and watch floor, providing around-the-clock support to track incidents and communicate with field offices across the country.

fbi.gov/investigate/cyber

Other State Programs:

- State aggregate purchasing program
- .GOV migration
- Local Cyber Protection Grants
- TechCred - https://techcred.ohio.gov/

CyberOhio

https://www.oc3.ohio.gov/
https://cyber.ohio.gov/

LOCAL GOVERNMENT CYBER GRANTS

The Infrastructure Investment and Jobs Act (IIJA) included provisions for SLCGP (State and Local Cybersecurity Grant Program) to address cyber risks and threats to the information systems of state, local, or tribal governments. State of Ohio is matching with over $10 million in-kind contributions.

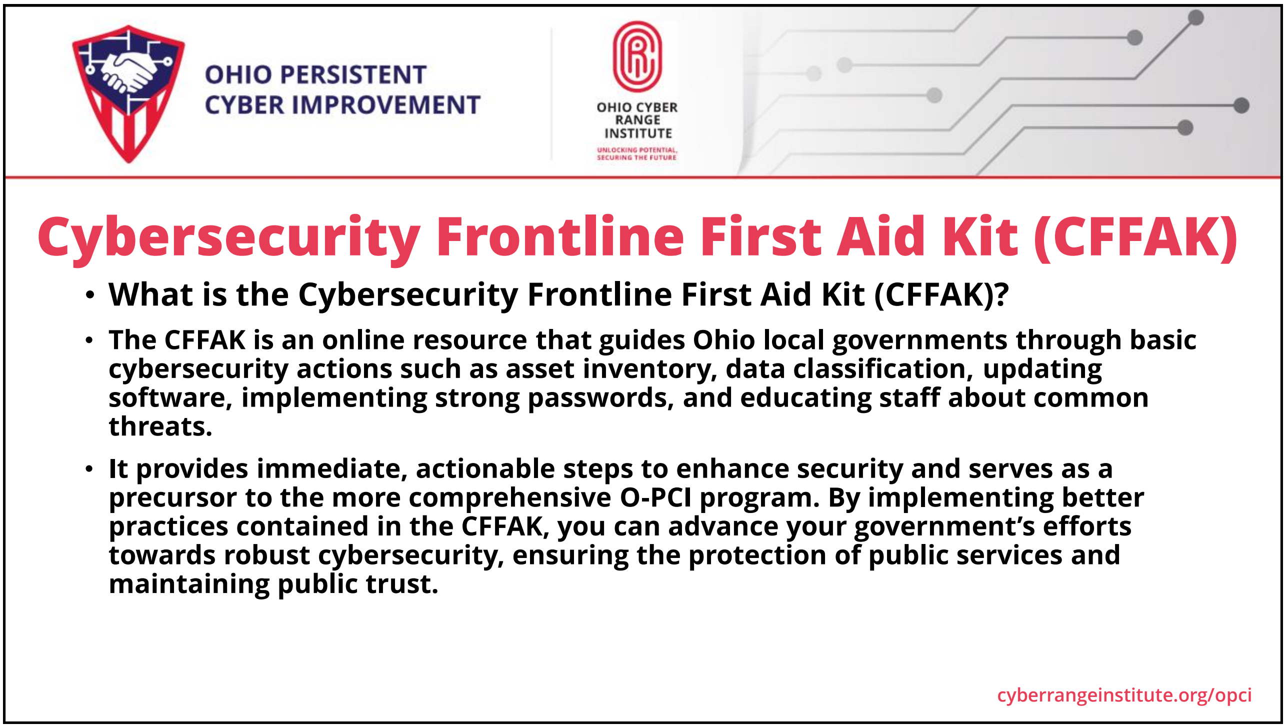
Round 1: $7million – Closed in September

Round 2: Estimated $5 million – Spring 2025
Helping local governments purchase cybersecurity software, transition to a Dot Gov, and targeting collective defense arrangements.

Local government cybersecurity grants (Helps Defend and Recover)

Local government Dot Gov Domain Transition (Protects Websites and Prevents Fraud)

https://cyber.ohio.gov/



OHIO PERSISTENT CYBER IMPROVEMENT

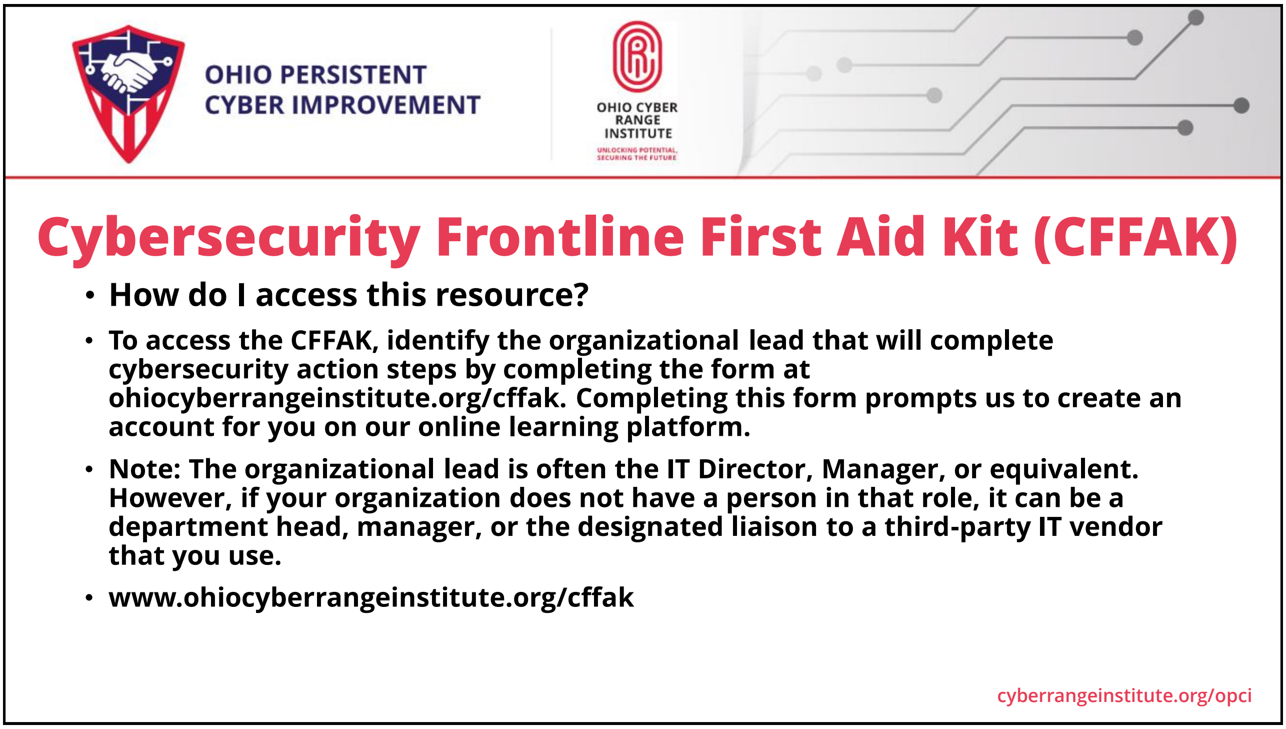
OHIO CYBER RANGE INSTITUTE

UNLOCKING POTENTIAL, SECURING THE FUTURE

Cybersecurity Frontline First Aid Kit (CFFAK)

- **What is the Cybersecurity Frontline First Aid Kit (CFFAK)?**
- **The CFFAK is an online resource that guides Ohio local governments through basic cybersecurity actions such as asset inventory, data classification, updating software, implementing strong passwords, and educating staff about common threats.**
- **It provides immediate, actionable steps to enhance security and serves as a precursor to the more comprehensive O-PCI program. By implementing better practices contained in the CFFAK, you can advance your government's efforts towards robust cybersecurity, ensuring the protection of public services and maintaining public trust.**

cyberrangeinstitute.org/opci



OHIO PERSISTENT CYBER IMPROVEMENT

OHIO CYBER RANGE INSTITUTE

UNLOCKING POTENTIAL, SECURING THE FUTURE

Cybersecurity Frontline First Aid Kit (CFFAK)

- **How do I access this resource?**
- **To access the CFFAK, identify the organizational lead that will complete cybersecurity action steps by completing the form at ohiocyberrangeinstitute.org/cffak. Completing this form prompts us to create an account for you on our online learning platform.**
- **Note: The organizational lead is often the IT Director, Manager, or equivalent. However, if your organization does not have a person in that role, it can be a department head, manager, or the designated liaison to a third-party IT vendor that you use.**
- **www.ohiocyberrangeinstitute.org/cffak**

cyberrangeinstitute.org/opci

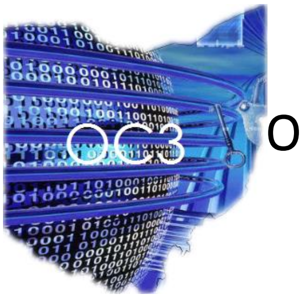
OHIO PERSISTENT CYBER IMPROVEMENT

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

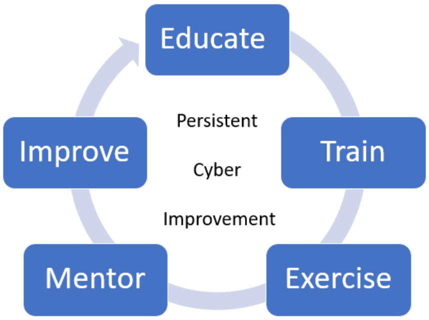
Cybersecurity Frontline First Aid Kit (CFFAK)

- **What happens next?**
- **You'll receive a welcome e-mail from our online learning platform that will grant you access to the Cybersecurity Frontline First Aid Kit. We use this platform to organize the resource so that it is accessible and easy to apply in your work.**
- **The learning platform is located at learn.ohiocyberrangeinstitute.org**
- **As you navigate through this resource, you will often see the Ohio Persistent Cyber Improvement (O-PCI) design. The Cybersecurity Frontline First Aid Kit is a first step towards better cybersecurity, but we encourage all local governments in Ohio to complete the comprehensive O-PCI program that includes training for all the staff in your organization, from frontline workers to executives.**

cyberrangeinstitute.org/opci

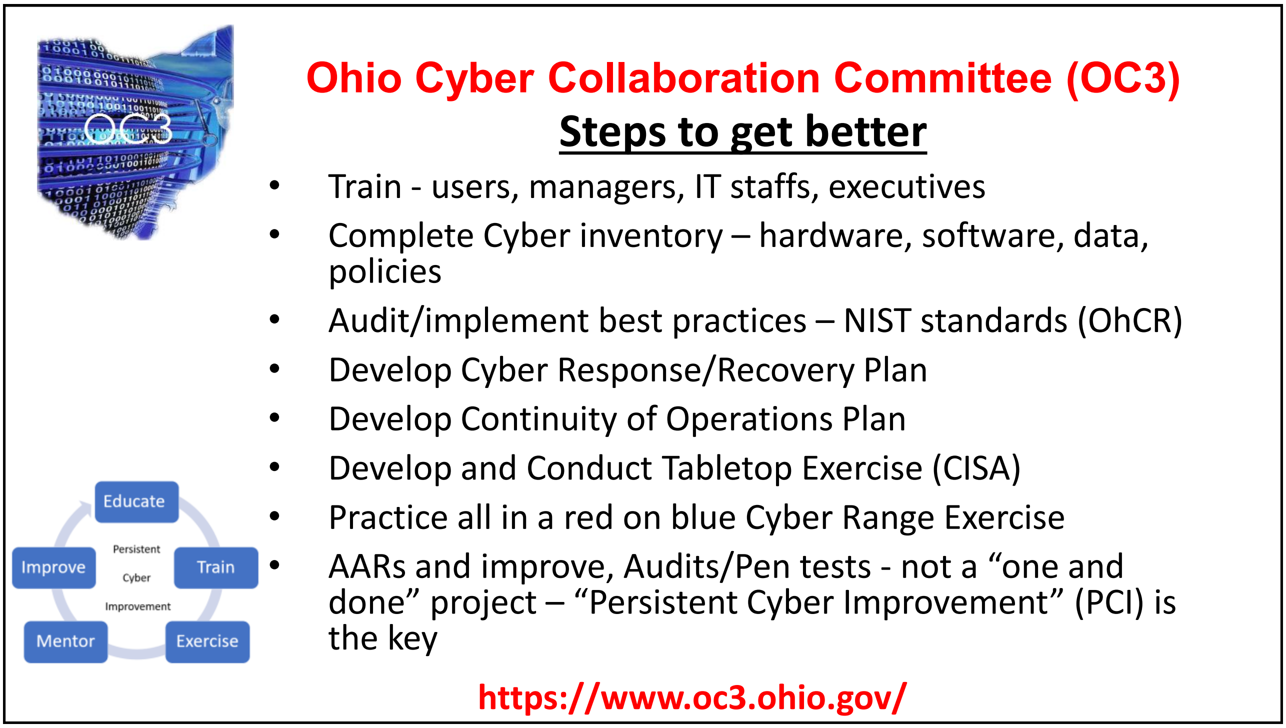


Scalability of OC3 Efforts
Ohio Persistent Cyber Improvement (O-PCI)



OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

OHIO CYBER RESERVE
OhCR

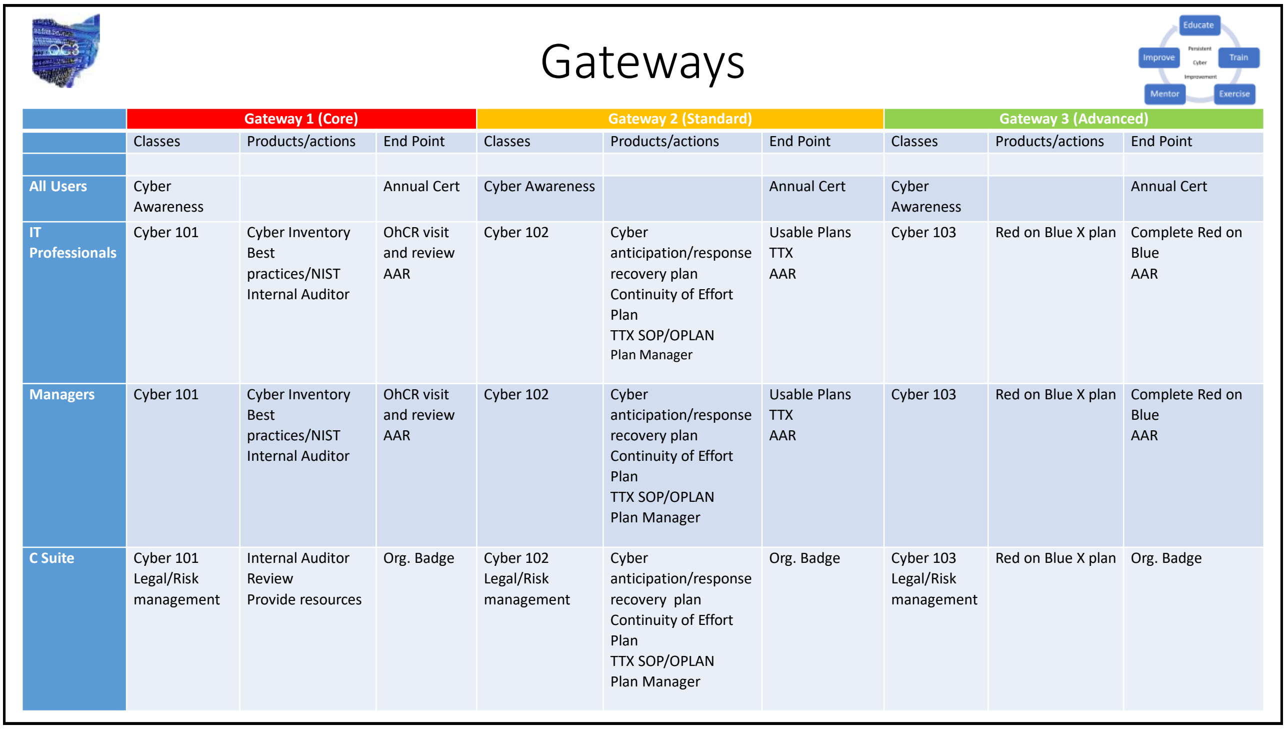


Ohio Cyber Collaboration Committee (OC3)

Steps to get better

- Train - users, managers, IT staffs, executives
- Complete Cyber inventory – hardware, software, data, policies
- Audit/implement best practices – NIST standards (OhCR)
- Develop Cyber Response/Recovery Plan
- Develop Continuity of Operations Plan
- Develop and Conduct Tabletop Exercise (CISA)
- Practice all in a red on blue Cyber Range Exercise
- AARs and improve, Audits/Pen tests - not a “one and done” project – “Persistent Cyber Improvement” (PCI) is the key

https://www.oc3.ohio.gov/



Gateways

OC3
Educate
Train
Exercise
Mentor
Improve
Persistent
Cyber
Improvement

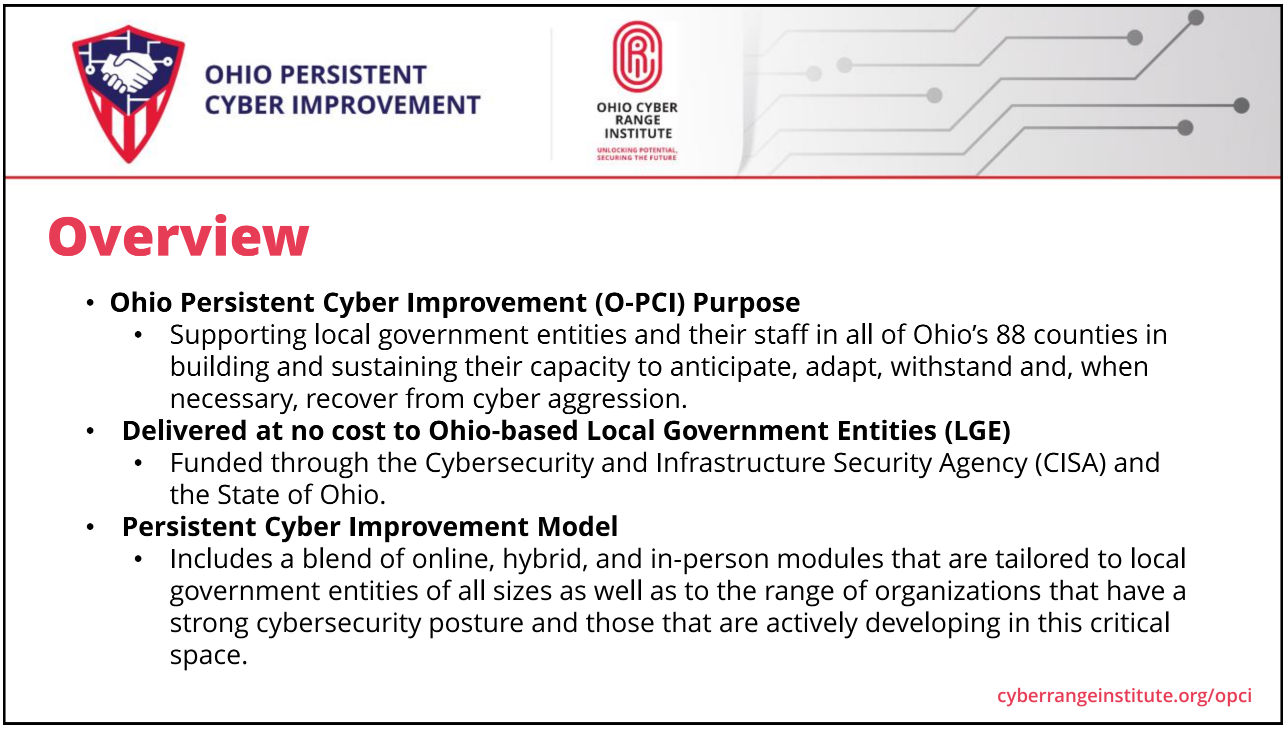
	Gateway 1 (Core)			Gateway 2 (Standard)			Gateway 3 (Advanced)		
	Classes	Products/actions	End Point	Classes	Products/actions	End Point	Classes	Products/actions	End Point
All Users	Cyber Awareness		Annual Cert	Cyber Awareness		Annual Cert	Cyber Awareness		Annual Cert
IT Professionals	Cyber 101	Cyber Inventory Best practices/NIST Internal Auditor	OhCR visit and review AAR	Cyber 102	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Usable Plans TTX AAR	Cyber 103	Red on Blue X plan	Complete Red on Blue AAR
Managers	Cyber 101	Cyber Inventory Best practices/NIST Internal Auditor	OhCR visit and review AAR	Cyber 102	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Usable Plans TTX AAR	Cyber 103	Red on Blue X plan	Complete Red on Blue AAR
C Suite	Cyber 101 Legal/Risk management	Internal Auditor Review Provide resources	Org. Badge	Cyber 102 Legal/Risk management	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Org. Badge	Cyber 103 Legal/Risk management	Red on Blue X plan	Org. Badge

OHIO PERSISTENT CYBER IMPROVEMENT

Serving Ohio's Public Servants

OHIO CYBER RANGE INSTITUTE

UNLOCKING POTENTIAL, SECURING THE FUTURE



OHIO PERSISTENT CYBER IMPROVEMENT

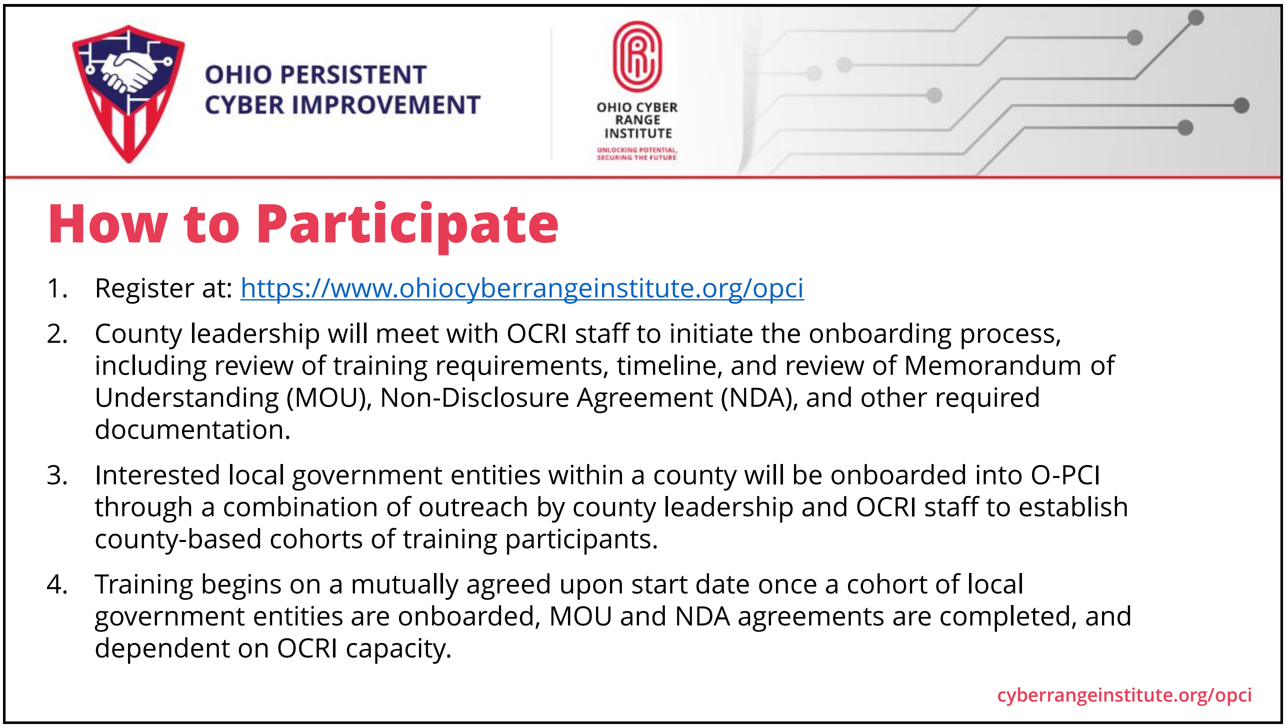
OHIO CYBER RANGE INSTITUTE

UNLOCKING POTENTIAL, SECURING THE FUTURE

Overview

- **Ohio Persistent Cyber Improvement (O-PCI) Purpose**
  - Supporting local government entities and their staff in all of Ohio's 88 counties in building and sustaining their capacity to anticipate, adapt, withstand and, when necessary, recover from cyber aggression.
- **Delivered at no cost to Ohio-based Local Government Entities (LGE)**
  - Funded through the Cybersecurity and Infrastructure Security Agency (CISA) and the State of Ohio.
- **Persistent Cyber Improvement Model**
  - Includes a blend of online, hybrid, and in-person modules that are tailored to local government entities of all sizes as well as to the range of organizations that have a strong cybersecurity posture and those that are actively developing in this critical space.

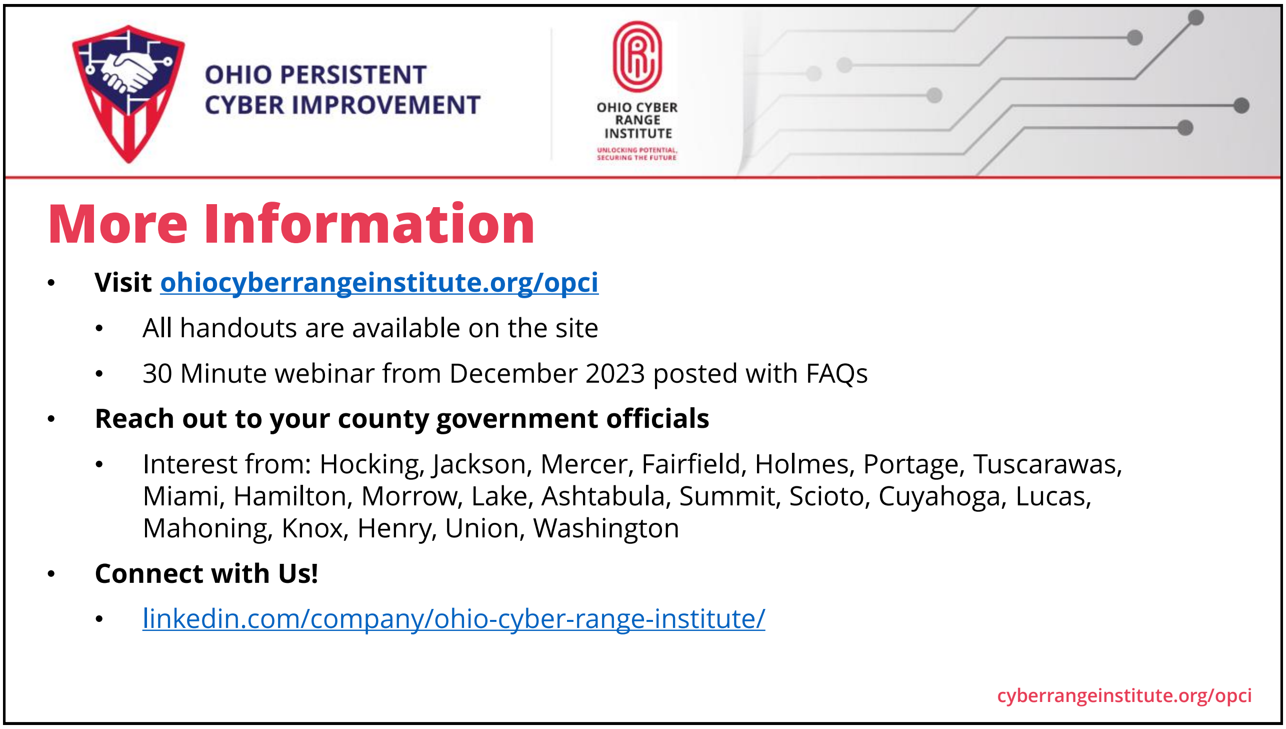
cyberrangeinstitute.org/opci


OHIO PERSISTENT CYBER IMPROVEMENT
OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

How to Participate

1. Register at: https://www.ohiocyberrangeinstitute.org/opci
2. County leadership will meet with OCRI staff to initiate the onboarding process, including review of training requirements, timeline, and review of Memorandum of Understanding (MOU), Non-Disclosure Agreement (NDA), and other required documentation.
3. Interested local government entities within a county will be onboarded into O-PCI through a combination of outreach by county leadership and OCRI staff to establish county-based cohorts of training participants.
4. Training begins on a mutually agreed upon start date once a cohort of local government entities are onboarded, MOU and NDA agreements are completed, and dependent on OCRI capacity.

cyberrangeinstitute.org/opci


OHIO PERSISTENT CYBER IMPROVEMENT
OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

More Information

- **Visit ohiocyberrangeinstitute.org/opci**
  - All handouts are available on the site
  - 30 Minute webinar from December 2023 posted with FAQs
- **Reach out to your county government officials**
  - Interest from: Hocking, Jackson, Mercer, Fairfield, Holmes, Portage, Tuscarawas, Miami, Hamilton, Morrow, Lake, Ashtabula, Summit, Scioto, Cuyahoga, Lucas, Mahoning, Knox, Henry, Union, Washington
- **Connect with Us!**
  - linkedin.com/company/ohio-cyber-range-institute/

cyberrangeinstitute.org/opci

Ohio Cybersecurity for Small Business

Free cybersecurity training for all Ohio small businesses, created by The Ohio State University experts and funded in part by a grant from the U.S. Small Business Administration.

Course Benefits:

- Enhance cybersecurity skills to **prevent, detect and respond to cyber threats**
- Improved ability to **safeguard sensitive data and systems**
- **Reduced risk of financial and reputational damage** from cyberattacks
- **Strengthened resilience and competitiveness** in the digital landscape

CyberOhio

U.S. Small Business Administration

The Ohio State University
Center for Design and Manufacturing Excellence

240+ businesses have signed up and are in the process of certifying their employees.

Sign up here:
https://osucybered.org

Ohio Cybersecurity for Small Business Course Overview

Gateway 1 of the cybersecurity training course provides a comprehensive overview of **essential cybersecurity principles** tailored for small business employees.

It focuses on **best practices**, **risk mitigation** strategies, and **foundational tools** to strengthen a business' cybersecurity posture.

Material covered in **Gateway 2**:

- Ohio **Data Protection Act**
- Regulatory compliance
- **Crown jewel** and risk assessment
- Implementing **controls** and policies
- Additional **in-depth information of Gateway 1 modules**

Both Gateways include **assessments** and **practical resources**, such as **detailed supplements** to help businesses develop **robust cybersecurity plans**. These include tools for creating **incident response plans**, conducting **security audits**, ensuring **continuity of operations**, and **more**.

Successful completion of Gateways 1 and 2 provides companies with artifacts to **reach CMMC** (Cybersecurity Maturity Model Certification) **Level 1 compliance**, positioning businesses to meet **essential cybersecurity standards**.

CyberOhio

U.S. Small Business Administration

The Ohio State University
Center for Design and Manufacturing Excellence

Sign up here:
https://osucybered.org

Resources you can use

- OC3 – https://www.oc3.ohio.gov
- Ohio Cyber Range – https://ohiocyberrangeinstitute.org
- Ohio Persistent Cyber Improvement - https://www.ohiocyberrangeinstitute.org/opci
- Ohio Cyber Reserve – Respond - use ema process (Assist/Educate - OhioCyberReserve@ucmail.uc.edu) Join - https://ohcr.ohio.gov/
- Ohio Homeland Security - https://homelandsecurity.ohio.gov/our-programs/ohio-cyber-program/ohio-cyber-program
- Cyber Ohio - https://cyber.ohio.gov/
- CISA – https://www.cisa.gov
- FBI/NSA/Secret Service
- NIST – https://www.nist.gov
- NICE - https://niccs.cisa.gov/workforce-development/nice-framework
- Trusted vendors
- Secure your home - https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3304674/nsa-releases-best-practices-for-securing-your-home-network

CyberOhio

Ohio Cyber Collaboration Committee (OC3)

OC3 is supported by a “whole of government” approach to ensure its success. Primary sponsors are the Adjutant General’s Department/Ohio National Guard, the Department of Higher Education, The Department of Education, The Department of Administrative Services, The Department of Public Safety, and The Department of Transportation.

OC3 has over 120 organizations who are active members who support the OC3 mission and objectives

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Suggested Next Steps

- Print these slides, review, make notes
- Enroll in and complete Cyber First Aid Kit (CFFAK) Https://ohiocyberrangeinstitute.org/cffak
- Choose Framework (Suggest NIST CSF 2.0) https://www.nist.gov/cyberframework
- Complete Cyber Inventory (Identify) – Slides 10 - 22
- Choose “Protect” Framework - Slides 24 – 27 – complete critical controls
- Schedule Ohio Cyber Reserve Assist Mission - https://ohcr.ohio.gov/ - Slide 48
- Enroll in OPCI whole of government cyber training https://www.ohiocyberrangeinstitute.org/opci
- Complete remainder of NIST CSF 2.0 – Slides 29 – 35
- Continue OPCI Gateways

https://www.oc3.ohio.gov/

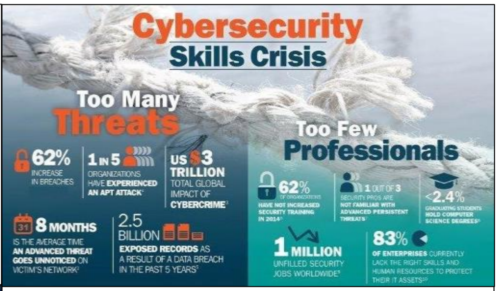
OHIO CYBER COLLABORATION COMMITTEE (OC3)

Ohio’s cyber community working together to help Ohio’s citizens and organizations achieve world class cyber security

Points of Contact

Primary

Mark Bell
Cyber Security Outreach Coordinator
2825 W Dublin Granville Road
Columbus Ohio 43232-2789
Phone 614-336-4903
Mobile 614-256-2391
Mark.a.bell16.nfg@army.mil



Alternate

Craig Baker
Program Administrator,
Ohio Cyber Reserve (OhCR)
2825 W Dublin Granville Road
Columbus Ohio 43232-2789
O: 614-336-7992
Craig.w.baker2.nfg@army.mil