BRINGING THE OHIO CYBER COLLABORATION COMMITTEE (OC3) TO KENTUCKY

Dave Hatter, CISSP, CISA, CISM, CCSP, CSSLP, PMP, ITIL

Cybersecurity Consultant / Mayor of Fort Wright, Kentucky

ABOUT ME

- Technology leader with over 30 years of software development and cybersecurity
- BS in Information Systems from NKU
- Earned industry leading certifications including CISSP, CISA, CISM, CCSP, CSSLP, PMP, PMI-ACP, PMI-PBA and ITIL Foundation V3
- Regular media subject matter expert interviewed more than 2,500 times since 1995
- Educated over 1,000 students as an adjunct at Cincinnati State Technical and Community College, the University of Cincinnati and Gateway Community and Technical College
- Written or contributed to 12 technology books
- Written more than 100 technology articles
- Delivered dozens of technology presentations to community and industry organizations
- Over 25 years of local government service: 8 terms on Fort Wright City Council, 3rd term Mayor of Fort Wright, Kentucky
- Kentucky League of Cities 2020 Elected Official of the Year

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

Microsoft Start

Search the web

CrowdStrike outage reportedly cost over $5.4 billion for top companies alone

Forbes

FORBES › INNOVATION › CYBERSECURITY

Record-Breaking $75 Million Ransom Paid To Dark Angels Gang

TECHSPOT

TRENDING FEATURES REVIEWS THE BEST DOWNLOADS PRODUCT FINDER FORU

SECURITY TECH CULTURE CASH CROWDSTRIKE

Another CrowdStrike-like outage could collapse cashless societies

Microsoft Start

Search the web

Discover Following | News World News Local Science Technology Crime Poli

Hacker group responsible for Columbus cyberattack claims 45% of data is published; ransom deadline extended

POLITICO

CYBERSECURITY

The nation's best hackers found vulnerabilities in voting machines — but no time to fix them

Organizers and participants at the DEF CON Voting Village found cyber vulnerabilities in everything from voting machines to e-poll books, but there is no time before the November elections to fully implement their findings.

INTENT TO KILL | 4:50 PM *by* VICTOR TANGERMANN

Homeland Security Warns of Cyberattacks Intended to Kill People

"The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us."

Ohio Cyber Collaboration Committee (OC3)

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

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

Ohio Cyber Collaboration Committee (OC3)

The Threat

Cyber crime is projected to cost the global economy $9.2 trillion by 2024, 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 2023, 30 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***
- The frequency and impact of threats is rising

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)

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 four subcommittees to help it achieve its primary goals:

- **Education/Workforce Development**
- **Cyber Range**
- **Cyber Protection and Preparedness**
- **Governance and Public Awareness**

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)

Why is Cyber Education/Workforce Development so important?

- Grow the workforce and improve the training and education of users and students in cyber security
- Nearly 11K advertised vacancies in cyber security in Ohio!
- High paying positions well above state average:

a. https://cyberseek.org/heatmap.html
b. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/career-pathways
c. NICE Framework for Cybersecurity
d. https://ohio-k12.help/cyber-security/

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

Cyber Club Toolkit

OHIO CYBER CLUBS
AN OHIO CYBER COLLABORATION COMMITTEE CLUB

1. How to work with your school or organization to create a cyber club
2. Understanding the different cyber club advisor roles
3. Finding a mentor for your cyber club
4. Using membership agreements in your cyber club
5. Marketing your cyber club
   http://education.ohio.gov/Topics/Learning-in-Ohio/Computer-Science/Resources-for-Computer-Science/Cyber-Club-Toolkit

Ohio Cyber Collaboration Committee (OC3)

Ohio Cyber Range/OCRI:

A secure cyber security test and training environment:

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.

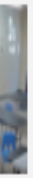
e. Provide a Cyber Portfolio for learners, and support internships.

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

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

OMMENDED


Washing your fruits and veggies isn't enough anymore. Here's how to kill pesticides


Cincinnati day care worker sentenced after pleading guilty to assaulting child

Ohio Cyber Range Institute drills for increasing cyberattacks with help from FEMA

Share

WLWT5

Updated: 6:09 PM EDT Aug 12, 2024

Infinite Scroll Enabled

Brian Hamrick

Reporter

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

OCRI Pilot | 2018 - 2020

OCRI Impact | 2020 - 2024

Economic Development

48 Participating Ohio Counties

Workforce Development

27,888
Cyber Citizen Users

Educational Impact

345
K-12 Classes

727
Higher Ed Classes

232
Instructors

60
Cyber Exercises

57
Bootcamps

60
Camps/Seminars

Ohio Cyber Guardian 2024
July 19-23, 2024

- Incident Response Training Exercise
- Training 4 Ohio Cyber Reserve Teams:
  - Cincinnati, Columbus, Cleveland
  - 100 people
- White Cell/Exercise Orchestration
  - OpFor, Range, ExCon, Assessments, NetO: 55 people
- Emulation of City and Cyber Incident
  - Infrastructure virtualized in the range
  - Grey space and traffic generation
- Distinguished Visitors Day
  - July 22, 2024

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

OCRI Advisory Board - Executive Committee

- Team of leaders with backgrounds and **expertise as diverse as the problems educators, citizens, and companies of Ohio face,** overseeing OCRI policies and ensuring proper governance

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

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
- Cyber Symposium / Annual Conference
- Ransomware Awareness Campaign

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

Ohio Cyber Collaboration Committee (OC3)

Governance and Public Awareness Subcommittee:

Identify and share best practices, policies and technologies for all Ohioans by:

a. Providing a collaborative research and development environment for the development and testing of innovative technologies and processes.

b. Ensuring cyber threats are part of emergency planning at all levels both public and private.

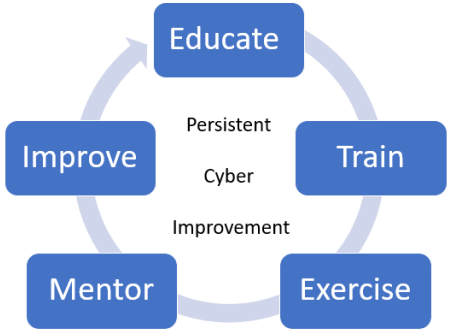
c. Using public awareness tools to educate and inform key decision makers of good cyber security practices and the latest information.

d. Educating the general public on the importance of cyber security for the “Internet of Things.”

e. Sharing threat intelligence between both public and private sector entities, facilitated through the Ohio Homeland Security State Fusion Center.

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

Government Agencies



- Large number of eligible entities in Ohio
  - 88 Counties, 1308 townships, 250 cities, 688 villages, 264 places, 611 school districts, 211 colleges and universities = 3,420 entities
  - Critical infrastructure – number in Ohio 11,440
  - Currently maxed at about 100 events per year. OhCR and CISA spending a lot of time teaching basic concepts.
- Need to scale our efforts to maintain an ongoing and persistent effort to educate/evaluate/test cyber skills and preparedness of Ohio's eligible entities

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.

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.

Ohio Cyber Collaboration Committee (OC3)

Other Pending Programs:

- State aggregate purchasing program
- Cyber Fusion Center
- .GOV migration

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

.GOV Domain Benefits

- Exclusively available to U.S.-based government organizations, ensuring that any website with this domain is an official government site. This exclusivity reduces the risk of cyberattacks and phishing attempts.

- According to CISA, a .gov domain helps the public quickly identify genuine government communications and websites, which is crucial in an era where cyber threats are increasingly sophisticated and pervasive (CISA).

- Eric Goldstein, Executive Assistant Director for CISA's Cybersecurity Division, emphasizes that "people see a .gov website or email address and know they are interacting with an official, U.S.-based government organization."

.GOV Domain Benefits

- **Improved Security:** .gov domains provide enhanced security measures, such as mandatory HTTPS encryption, which protects data in transit from eavesdropping and tampering.
- **DNS Security:** Administrators receive notifications of any Domain Name System (DNS) changes, enabling them to respond quickly to potential threats. This helps mitigate risks before they can impact citizens and city services
- **Phishing Resistance:** With a .gov domain, it becomes more difficult for malicious actors to spoof government emails and websites. This decreases the likelihood of successful phishing attacks, protecting citizens from fraud and identity theft
- **Two-Factor Authentication:** The .gov domain registrar incorporates two-factor authentication, adding an extra layer of security for administrators managing the domain. This reduces the risk of unauthorized access and enhances overall security

Why All Local Governments Should Switch to .GOV

- **Enhanced Public Trust:** A .gov domain signals to citizens that they are engaging with an authentic government entity. This builds trust and encourages more people to use online government services confidently.
- **Reduced Cyber Risk:** Local governments often handle sensitive data, making them prime targets for cyberattacks. The security features inherent in .gov domains provide robust protection against these threats, safeguarding both the government and its citizens.
- **Compliance with Best Practices:** Following CISA’s recommendations and adopting a .gov domain aligns local governments with best practices in cybersecurity. This proactive approach demonstrates a commitment to protecting citizens' data and maintaining the integrity of government services.
- **Simplified Management:** With features like DNS change notifications and two-factor authentication, managing a .gov domain is streamlined and secure, reducing the burden on IT staff and enhancing overall cybersecurity posture.

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
  - Department of Higher Education
  - The Department of Education
  - The Department of Administrative Services
  - The Department of Public Safety
  - 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/


WE ARE NO LONGER
SECURING COMPUTERS
WE ARE SECURING SOCIETY.

We Need a KC3!

- Ohio is running a very successful program that:
  - Provides resources to protect critical infrastructure
  - Bolsters the Ohio work force and the economy
  - Raises awareness about cybersecurity which increasingly impacts us all
  - Gets students interested in these important and lucrative careers
  - Helps stop the “brain drain”
- We can model the good work done by Ohio for Kentucky
- There are people willing to help get this running here
- It will take money
- We should adopt a “whole of government” approach
- What can I do to help make this happen in Kentucky?

Thank You!

Dave Hatter, CISSP, CISA, CISM, CCSP, CSSLP, PMP, ITIL

linkedin.com/in/davehatter

twitter.com/davehatter

dhatter@fortwrightky.gov