OHIO PERSISTENT CYBER IMPROVEMENT

A program of the Ohio Cyber Range Institute

Gateway 1 Courses

Learners complete bite-sized five- to 15-minute-modules for each course. Most courses produce takeaway documents, like plans and procedures, that can be implemented in your organization.

Cyber Mindfulness – 1 hour 50 min

Course designed for all employees

A foundational guide to basic cybersecurity practices that engage all employees throughout the organization. Course offers an overview of cyber mindfulness and how to practice it in daily digital activities such as email, web browsing and social media. Learn to recognize and avoid cyber threats such as phishing, malware, and ransomware.

Learning Outcome

Apply cyber mindfulness techniques to online behavior and habits to identify vulnerabilities and prevent common cyber attacks

Cybersecurity 101 – 1 hour 10 min

Course designed for IT/Cybersecurity Professional

An introduction to the principles and concepts applied to cybersecurity. Gain a deeper technical understanding of the cybersecurity threats and challenges facing local government organizations. This course will explore the fundamental security services, mechanisms, and principles used to establish standards and best practices for cyber persistence.

Learning Outcome

Understand key cybersecurity concepts and principles to apply a persistent cyber strategy in the organization

Cybersecurity Frameworks Introduction – 1 hour 40 min

Course designed for IT/Cybersecurity Manager/Executive

An introduction to core concepts and applied practices of Cybersecurity Frameworks (CSFs), a set of voluntary guidelines and standards for improving cybersecurity and managing cyber risks, tailored to the specific needs and challenges of local governments. This course includes an optional module tailored to understanding and applying the National Institute of Standards and Technology (NIST) Cybersecurity frameworks.

Learning Outcome

Understand the benefits of implementing Cybersecurity Frameworks to implement a persistent cyber defense and mindful workforce

Risk Management – 2 hours

Course designed for Executive and IT Cybersecurity Manager/Executive

Learn essential skills and strategies for protecting data and managing cyber risks. Using various tools and methods, learn to identify, assess, and prioritize cyber risks and vulnerabilities of local government operations and services. Apply the knowledge gained to identify and protect critical systems and processes that support the delivery of essential local government services and functions.

Learning Outcome

Perform risk assessments to measure cyber risk levels; use risk matrices and heat maps to visualize and communicate risk levels

Begin risk management plan for organization

OHIO CYBER RANGE INSTITUTE
POWERED BY UNIVERSITY OF CINCINNATI

Ohio Cyber Range Institute
3080 Exploration Avenue, Suite 320
Cincinnati, OH 45267-0055

Email: opciprogram@uc.edu
Phone: 513-556-8138
Web: ohiocyberrangeinstitute.org

OHIO PERSISTENT
CYBER IMPROVEMENT

A program of the Ohio Cyber Range Institute

Gateway 1 Courses

Vulnerability Management – 5 hours

Course designed for IT/Cybersecurity Professional

IT specialists will take a deeper technical dive into types of vulnerabilities and attack vectors that threat actors can exploit to compromise systems and data. This course provides techniques and tools for conducting automated and manual scans to identify and assess cyber vulnerabilities.

Learning Outcome

Develop and maintain a network system vulnerability management plan

Begin mapping cyber inventory and vulnerability management

Organizational & Third-Party Security – 2 hours

Course designed for IT/Cybersecurity Manager/Executive

Equips local government officials and managers with the knowledge and skills needed to protect their organization's information and infrastructure from cyber threats. Protect the confidentiality, integrity, and availability of personal, private, and sensitive information (PPSI) collected, stored, processed, and shared by the organization.

Learning Outcome

Assess and manage the cybersecurity risks posed by third parties

Begin development of an organizational cybersecurity policy

Network Control Systems – 4 hours

Course designed for IT/Cybersecurity Professional

A deeper dive into the concepts and techniques of network systems controls and security design. Technical implementation of various network security mechanisms will be explored. Learn to analyze and prioritize security controls to design a security architecture that aligns with the critical business systems, policies, and best practices.

Learning Outcome

Design and plan the network systems architecture and topology, security controls and solutions

Begin planning to increase cybersecurity posture

The Anticipation and Resilience Strategy (ARS)

Capstone project for Gateway 1

The ARS project leverages the knowledge gained from completing the Gateway 1 courses, setting the stage for continued improvement of a persistent cybersecurity culture in O-PCI Gateway 2.

Learning Outcome

Align cybersecurity documentation into a format consistent with the National Institue of Standards (NIST) and Cybersecurity Frameworks (CSF)

OHIO CYBER RANGE INSTITUTE
POWERED BY UNIVERSITY OF CINCINNATI

Ohio Cyber Range Institute
3080 Exploration Avenue, Suite 320
Cincinnati, OH 45267-0055

Email: opciprogram@uc.edu
Phone: 513-556-8138
Web: ohiocyberrangeinstitute.org