Ohio Cyber Collaboration Committee (OC3)

Cybersecurity Best Practice Website Guide

1. Overview

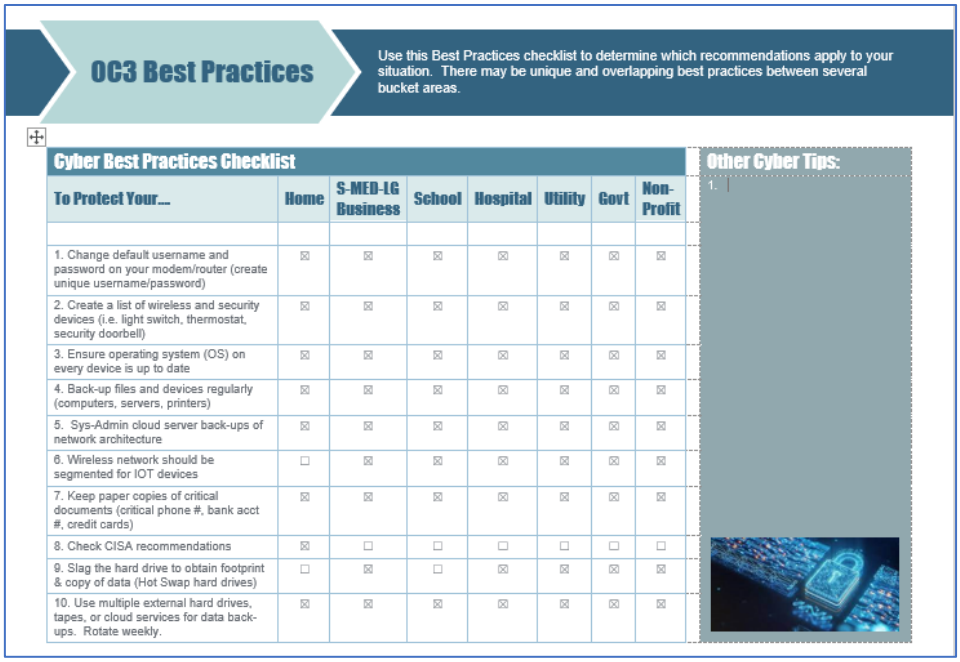
Cyberattacks are prevalent in Ohio, a State with a population of 12 million people and approximately 1 million businesses and organizations. Of all the threats to the daily operation of small businesses and organizations in communities, malware and insider threats are the most common. As we progress into the decade, the number of cyberattacks in Ohio will continue to increase. In response to the cyber threats, the Ohio Cyber Collaboration Committee (OC3) has taken a leadership role in defense of the data most important to Ohioans through the various OC3 subcommittees (S.C.) and partnering agencies, including the Governance S.C., the Cyber Protection and Preparedness S.C., the Education & Workforce Development S.C., the Ohio Cyber Range at the University of Akron, the Ohio Cyber Range Institute (OCRI) at the University of Cincinnati, and the 15 OCRI Regional Programming Centers (RPC's) across the state.

2. Purpose

OC3 professionals are always approached to answer questions about the best practices in cybersecurity. The State of Ohio adopted the NIST Cybersecurity Framework in August 2018 for all of its agencies and supply chain. The Ohio Cyber Reserve (OhCR) is working in their Assist, Educate and Respond missions to answer the same questions on how to meet the NIST Identify, Protect, Detect, Respond and Recover paradigm controls. The OC3 Education & Workforce Development S.C. and the Ohio Cyber Range Institute also answer many of the same frequently asked questions (FAQ's). To unify our efforts, we have designed the Ohio OC3 website with a catalog of best practices and resource documents that will help Ohioans to get started on their cybersecurity defense journey, which is the most efficient use of our time and precious resources to deliver consistent messaging and knowledge to the people.

Scope

This guide will allow Cybersecurity Subject Matter Experts (SMEs) to share ideas and knowledge in a cost-effective manner. The OC3 Cybersecurity Best Practices Website being developed by Ohio Homeland Security supports individual Households, Small – Medium – Large Businesses, Schools, Healthcare Facilities, Utilities, Government, and Non-Profit Organizations.



OC3 Best Practices

Use this Best Practices checklist to determine which recommendations apply to your situation. There may be unique and overlapping best practices between several bucket areas.

Cyber Best Practices Checklist

To Protect Your....	Home	S-MED-LG Business	School	Hospital	Utility	Govt	Non-Profit
1. Change default username and password on your modem/router (create unique username/password)	☒	☒	☒	☒	☒	☒	☒
2. Create a list of wireless and security devices (i.e. light switch, thermostat, security doorbell)	☒	☒	☒	☒	☒	☒	☒
3. Ensure operating system (OS) on every device is up to date	☒	☒	☒	☒	☒	☒	☒
4. Back-up files and devices regularly (computers, servers, printers)	☒	☒	☒	☒	☒	☒	☒
5. Sys-Admin cloud server back-ups of network architecture	☒	☒	☒	☒	☒	☒	☒
6. Wireless network should be segmented for IOT devices	☐	☒	☒	☒	☒	☒	☒
7. Keep paper copies of critical documents (critical phone #, bank acct #, credit cards)	☒	☒	☒	☒	☒	☒	☒
8. Check CISA recommendations	☒	☐	☐	☐	☐	☐	☐
9. Slag the hard drive to obtain footprint & copy of data (Hot Swap hard drives)	☐	☒	☐	☒	☒	☒	☒
10. Use multiple external hard drives, tapes, or cloud services for data back-ups. Rotate weekly.	☒	☒	☒	☒	☒	☒	☒

Other Cyber Tips:

1.

Figure 1 – Cyber Best Practice Checklist

Who Can Assist in Building the OC3 Cybersecurity Best Practices Website?

Ohio Cyber Reserve members can build Best Practices to support the OhCR Assist and Educate missions.

Ohio schools, colleges and university Cyber Clubs can participate in developing Best Practices.

3. Best Practices Process

The NIST 800-53 R5 Cybersecurity Framework lists 1007 separate controls in 20 control families. These cyber hygiene statements just published in 2020 will be constant for many years. A best practice tells a user how a control should be successfully implemented and should facilitate the control's timely and effective implementation in the user's current application.

For example, every student and every employee should take a basic cybersecurity awareness training class annually to meet the NIST control requirement. The problem is that less than 50% of Ohioans have ever taken a comprehensive cybersecurity awareness training class. So this Best Practice should be on the website.

Select a Best Practice topic and build it using the Best Practice template. Verify the training, process, or application with your team. Whatever the practice, the team should do every step, watch all the video, or use the application before the recommendation. Your team leader should verify the Best Practice.

In the Word document file title, it should say **Best Practices OC3 Template REV [#]** with the current revision number. Then add a dash and the title of the Best Practice such as **Cybersecurity Awareness Course.** Put the initial of the group and the verifier such as **OhCR – CWR.**

Example Filename

Best Practices OC3 Template REV1 – Cybersecurity Awareness Course – OhCR - CWR

Have your Organization Best Practice team leader send the finished Best Practice to:

Cheryl Engle
Cyber Program Manager
Ohio Homeland Security

4. Best Practice Template

The Best Practice template recognizes the ongoing work of the OC3 and its many partners, so the OC3 Logo and Title are on the heading.

The Best Practice title, short description, and hyperlink to the Government, Education, or Non-Profit resource is below the heading.

An image showing the homepage, start page of the application, or video is next. If a step-by-step procedure is needed, it appears below the image.

Best Practice and page number is in the footer.

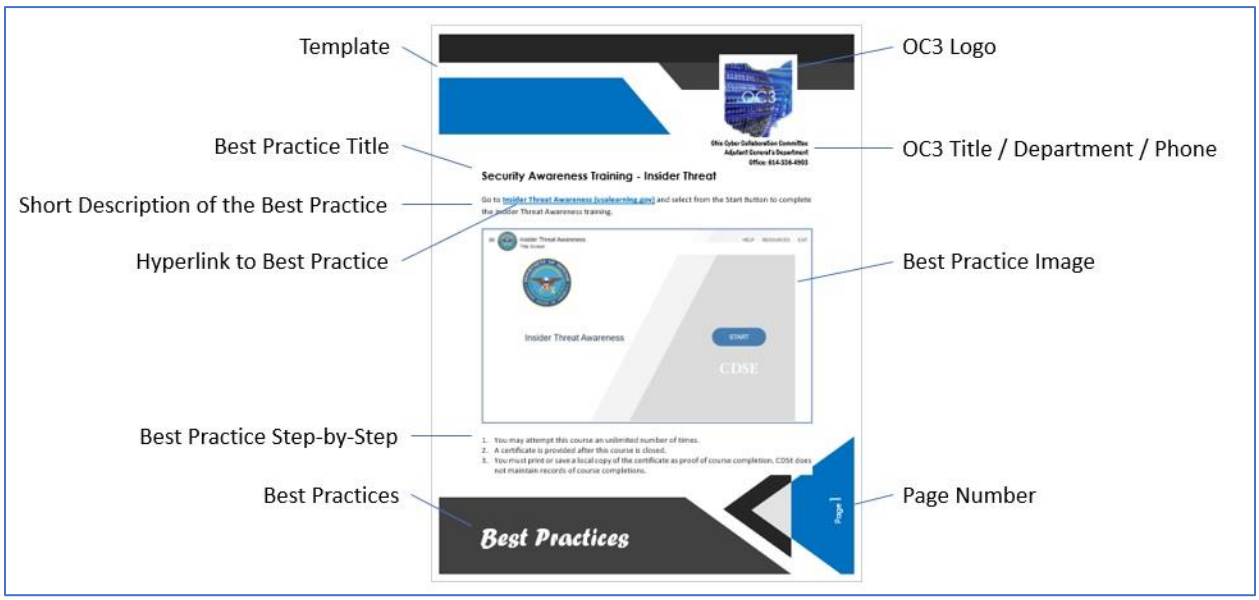


Figure 2 – The Best Practice Template

5 Guide Compliance

This guide complies with NIST Cybersecurity Framework as defined in Ohio ITS-SEC-02 Enterprise Security Controls Framework.

6 Related Standards, Policies and Processes

ITS-SEC-02	Enterprise Security Controls Framework
NIST SP 800-53 R5	Security and Privacy Controls for Information Systems and Organizations

7 Definitions and Terms

NIST	The National Institute of Standards and Technology, a unit of the U.S. Commerce Department. NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

8 Revision History

Date of Change	Responsible	Summary of Change
January 29, 2022	Ohio Cyber Reserve	Created initial draft