July 1, 2020

CYBER ESSENTIALS

Your success depends on *Cyber Readiness*. Both depend on *YOU*.

ESSENTIAL ELEMENT: YOUR STAFF, THE USERS

THE TASK: Develop Security Awareness and Vigilance

Your staff is often the first line of defense for your organization. Investing in your personnel reduces vulnerabilities and drives a culture of ownership. They must be equipped to recognize cybersecurity risks such as phishing scams, password hacks, and outdated anti-malware, as well as trained to respond and share information appropriately.

Essential Actions

✓ *Actions for Leaders* ✓ *Discuss with IT Staff or Service Providers*

☑ **Leverage basic cybersecurity training.** Your staff needs a basic understanding of the threats they encounter online in order to effectively protect your organization. Regular training helps employees understand their role in cybersecurity, regardless of technical expertise, and the actions they take help keep your organization and customers secure. Training should focus on threats employees encounter, like phishing emails, suspicious events to watch for, and simple best practices individual employees can adopt to reduce risk. Each aware employee strengthens your network against attack, and is another "sensor" to identify an attack.

Resources for Taking Action

National Initiative for Cybersecurity Careers and Studies (NICCS): *the NICCS Training Catalog provides a listing of cybersecurity and cybersecurity-related training courses offered in the United States.*

SANS: Live and virtual computer security training *developed by industry leaders and taught by real-world practitioners.*

FedVTE: The Federal Virtual Training Environment (FedVTE) *provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and U.S. military veterans.*

Federal Trade Commission resources/Cyber basics: *training material on cybersecurity basics and best practices for businesses.*

Cyber Readiness Institute Cyber Readiness Program: *a comprehensive, self-guided tool containing information to reduce cyber risk, training material for employees, and more.*

☑ **Develop a culture of awareness to encourage employees to make good choices online.** Go beyond knowledge; identify the behavior you want to change and develop a cybersecurity strategy that targets cyber expectations. Define what success looks like through guidelines and policies. Continually reinforce cyber hygiene as you would other workplace hygiene (e.g. hand washing, professionalism, etc.). Create incentive structures that promote the formation of good habits (e.g. recognition for good behavior, loss of privileges for persistent reckless behavior). Encourage employees to participate in awareness campaigns like Stop.Think. Connect. and National Cybersecurity Awareness Month.

Resources for Taking Action

National Cybersecurity Awareness Month (NCSAM) toolkit: *comprehensive guide for individuals and organizations, regardless of size or industry, on engaging in and promoting cybersecurity awareness and developing effective practices that foster strong cybersecurity.*

National Institute of Standards and Technology (NIST): *introductory information for small business owners and leaders about cybersecurity, cybersecurity-related risks, and the importance of taking appropriate steps to secure your business*

National Cyber Security Alliance (NCSA): CyberSecure My Business™ *is a national program helping small and medium-sized businesses (SMBs) learn to be more secure online.*

Global Cyber Alliance: *a free toolkit to help small to medium-sized businesses implement basic cyber hygiene which will enable business owners to significantly reduce the cyber risks they face every day.*

FTC's Talking cybersecurity with your employees: *learn the basics for protecting your business from cyber-attacks, developed in partnership with the NIST and Technology, the U.S. Small Business Administration, and the Department of Homeland Security.*

Cyber Readiness Institute Cyber Readiness Program: *a comprehensive, self-guided tool containing information to reduce cyber risk, training material for employees, and more.*

ESSENTIAL ELEMENT: YOUR STAFF, THE USERS

Learn about risks like phishing and business email compromise. Employees should be able to identify the trademark signs of malicious emails. Alert your staff to phishing and scamming tactics and include the latest changes in regular training. Regular updates and reminders keep everyone aware of current threats and how to handle them if encountered. Ensure employees know how and to whom to report suspicious emails or possible phishing attempts.

Resources for Taking Action

Federal Bureau of Investigation resources: *solutions that businesses have employed to safeguard against e-mail compromise scams and criminal groups that engage in the scams.*

FBI Internet Crime Complaint Center: *the Internet Crime Complaint Center (IC3) accepts online Internet crime complaints from victims or from a third party to the complainant.*

CISA Insights: *this CISA Insight provides information on cyber phishing email attacks that non-federal partners can implement.*

Global Cyber Alliance: *DMARC setup guide, free, practical, real-world solutions that improve cybersecurity.*

CISA Security Tips: Avoiding Social Engineering and Phishing Attacks: *security tips for avoiding social engineering and phishing attacks and advice about common security issues for non-technical computer users.*

Cyber Readiness Institute Cyber Readiness Program: *a free compilation of information about what you can do to reduce cyber risk, along with training materials for your employees, and much more.*

Identify and use available training resources. Organizations should know whether they already have training resources that are just being underutilized, or whether they should look outside of the organization to find these. Training your staff and promoting cyber awareness does not mean you have to create training materials from scratch. Many professional organizations, industry associations and academic institutions, as well as private sector and government networks provide ready-to-use cybersecurity training resources at no cost. Encourage your organization's HR department to identify which resources are available to your industry.

Resources for Taking Action

ISACA: *an international professional association focused on information technology governance and provides in-person training on tools and techniques from expert instructors.*

National Initiative for Cybersecurity Education (NICE) framework Workforce Management Guidebook: *key concepts to know and actions to take across your organization.*

National Centers of Academic Excellence: *designed to reduce vulnerability in our national information infrastructure by promoting higher education and expertise in cyber defense.*

Small Business Administration (SBA): *a national program that includes webinars, resources, and access to cybersecurity experts for small and medium-sized businesses.*

National Cyber Security Alliance: *broad-reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online.*

Small Business Guide: Cyber Security: *provides five quick and low-cost methods to improve cyber security in your organization.*

ISC2 Cybersecurity and IT Security Certifications and Training: *webinars, videos, and more offering career advice, resolution to cybersecurity issues, and collaboration with peers.*

Global Cyber Alliance: *free, practical, real-world solutions that improve cybersecurity.*

Maintain awareness of current events related to cybersecurity. Be proactive; alert staff to hazards that the organization may encounter. Maintain vigilance by asking yourself: what types of cyber attack are hitting my peers or others in my industry? What tactics were successful in helping mvy peers limit damage? What does my staff need to know to help protect the organization and each other? On a national-level, are there any urgent cyber threats my staff need to know about?

Resources for Taking Action

CISA National Cyber Awareness System: *offers a variety of information and products for users with varied technical expertise about security topics and threats.*

SANS Security Awareness Newsletter: *The OUCH! Newsletter OUCH! is a free security awareness newsletter designed for everyone.*

Cyber Threat Alliance: *cybersecurity resources including adversary playbooks and information sharing provide the industry with a centralized source of trusted information.*

Cyber Crime Investigations – FBI: *The FBI's Cyber Division provides guidance on awareness and protection from cyber intrusions.*

National Cyber Security Alliance: *broad-reaching education and awareness efforts to empower users with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online.*

Global Cyber Alliance: *conveys trends and issues in the global cybersecurity community by publishing data-driven research and original commentary.*

The tools and resources in this Guide are for informational and educational purposes. DHS/CISA does not guarantee their content nor endorse any specific person, entity, product, service, or enterprise.