CYBER ESSENTIALS

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

ESSENTIAL ELEMENT: YOUR SYSTEMS

THE TASK : Protect Critical Assets and Applications

Protecting your systems requires knowing which devices are connected to your network, which applications are in use, who has access to these, and the security measures in place. A cyber-ready business keeps its systems up-to-date and secure. These actions can support a proactive risk management culture and limit the risk of compromise.

Essential Actions

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

Learn what is on your network. Inventory all hardware and software assets so you know what is in-play and at-risk from attack. Establish a monitoring strategy to identify unusual activity that could indicate an attack.

Resources for Taking Action

NIST Computer Security Resource Center: *NIST's cybersecurity- and information security-related projects, publications, news, and events help supports stakeholders.*

Center for Internet Security (CIS) Controls: *Control 1 and Control 2 provide guidance on managing hardware and software assets on your network.*

Global Cyber Alliance: *a guide and checklist to identify and secure devices and applications.*

National Cyber Security Centre's Cyber Essentials: *a Small Business Guide outlining five steps that can save time, money, and reduce the chances of a cyber-attack on your business.*

NSA Actively Manage Systems and Configurations: *offers network management tips.*

Cyber Readiness Institute's Cloud FAQ: Improving Cybersecurity for Remote Workers: *a guide to help prioritize data to keep on your network and data you can move to the cloud.*

Leverage automatic updates for all operating systems and third-party software. An easy step is to establish and maintain network security/patching procedures to prevent attacks by configuring functions and programs necessary for security. Enable automatic updates whenever possible and be sure to obtain, test, and deploy the latest versions of operating systems and applications.

Resources for Taking Action

NIST Computer Security Resource Center: *NIST's cybersecurity- and information security-related projects, publications, news, and events help supports stakeholders.*

CIS Control 3: *offers tips to help organizations maintain continuous vulnerability management to avoid compromised computer systems.*

National Cyber Security Centre's Cyber Essentials: *a Small Business Guide outlining five steps that can save time, money, and reduce the chances of a cyber-attack on your business.*

Cyber Readiness Institute Cyber Readiness Program: *contains information about reducing cyber risk and training materials for your employees.*

Implement secure configurations for all hardware and software assets so that your physical and virtual assets are protected. Create and maintain policies that identify and prioritize secure configurations. Review and implement secure configuration guidance from your vendors and other sources. Conduct frequent vulnerability scans to identify and resolve weak or unprotected entry points.

Resources for Taking Action

CIS Control 5: *offers tips to manage security configuration of hardware and software assets using a configuration management and change control process.*

NSA top ten cybersecurity mitigation: *NSA's Top Ten Mitigation Strategies counter a broad range of exploitation techniques used by Advanced Persistent Threat (APT) actors.*

Guide for Security Focused Configuration Management of Information Systems

Center for Internet Security Benchmarks: *configuration guidelines for various technology groups to safeguard systems against today's evolving cyber threats.*

Australian Cyber Security Centre: *a prioritized list of mitigation strategies to protect organizations and their systems against a range of adversaries.*

National Cyber Security Alliance Resources Library: *tips and resources to protect devices.*

Remove unsupported or unauthorized hardware and software. Supported hardware and software generally allow you to receive updates and patches for vulnerabilities that otherwise are not available for unauthorized and unsupported assets. Inventory authorized hardware and software throughout your organization. Know the physical location and user of the hardware to keep patching updates current. This also allows for any unauthorized hardware or software to be identified and removed.

Resources for Taking Action

CIS Control 3: *offers tips to help organizations maintain continuous vulnerability management to avoid compromised computer systems.*

CISA Binding Operational Directive 19-02: *ensures effective and timely remediation of critical and high vulnerabilities identified through Cyber Hygiene scanning.*

National Cyber Security Centre's Cyber Essentials: *a Small Business Guide outlining five steps that can save time, money, and reduce the chances of a cyber-attack on your business.*

Australian Cyber Security Centre's Essential Eight Explained: *a prioritized list of mitigation strategies to protect organizations and their systems against a range of adversaries.*

Leverage email and web browser security settings to protect against spoofed or modified emails and unsecured webpages. Content filtering applied to external websites can prevent attackers from delivering malicious code to desktop applications. Firewalls can also deny traffic to potentially harmful sites while allowing access to acceptable applications. Customize your email settings to allow safe mail. Set the content filters to send mail containing certain words and email addresses to the spam folder.

Resources for Taking Action

CIS Control 7: *tips to minimize access to common points of entry such as web browsers and email clients vulnerable to attack.*

Global Cyber Alliance: *tools that ensure your brand's name and email addresses do not get used by others pretending to be you.*

CISA Binding Operational Directive 18-01: *Enhance Email and Web Security*

CISA securing your web browser: *browser configuration guidance for safer Internet surfing.*

National Cyber Security Centre's Cyber Essentials: *a Small Business Guide outlining five steps that can save time, money, and reduce the chances of a cyber-attack on your business.*

NSA Steps to secure web browsing: *identifies three mitigations in commonly-used web browsers that will ward off nearly all publicly known attacks.*

NIST Special Publication 800-177 Rev 1: *Trustworthy Email*

NIST Special Publication 1800-6: *Domain Name System-Based Electronic Mail Security*

Create application integrity and allow list policies so that only approved software can operate on your systems. Ensure your applications perform in a secure and as-intended manner by instituting an Application Integrity and Application allow list policy that allows only approved, authorized software and their libraries to load and execute. Monitor the integrity of allow list applications with periodic checks of file hashes to ensure no unauthorized modifications have been made. As with identity and access management, due to the complexity and effort required, consider a staged, gradually phased-in approach starting with high impact endpoints (e.g. domain controllers, application servers, databases), followed by any remaining support systems, and ending with any remaining user workstations or endpoints.

Resources for Taking Action

Australian Cyber Security Centre Implementing Application Control: *this document provides guidance on what application control is, and how to implement application control.*

NIST Special Publication Guide to Application Whitelisting: *this publication assists organizations in understanding the basics of application whitelisting.*