Spring 2021

CYBER ESSENTIALS STARTER KIT

The Basics for Building a *Culture of Cyber Readiness*

Cybersecurity and Infrastructure Security Agency

TABLE OF CONTENTS

CYBER ESSENTIALS

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

THE LEADER'S GUIDE

Reducing your organization's cyber risks requires a holistic approach - similar to the approach you would take to address other operational risks. As with other risks, cyber risks can threaten:

- YOUR ABILITY TO OPERATE / ACCESS INFO
- YOUR REPUTATION / CUSTOMER TRUST
- YOUR BOTTOM LINE
- YOUR ORGANIZATION'S SURVIVAL

Managing cyber risks requires building a culture of cyber readiness.

Essential Elements of a *Culture of Cyber Readiness*:

Yourself - *The Leader*

Drive cybersecurity strategy, investment and culture

Your awareness of the basics drives cybersecurity to be a major part of your operational resilience strategy, and that strategy requires an investment of time and money.

Your investment drives actions and activities that build and sustain a culture of cybersecurity.

Your Staff - *The Users*

Develop security awareness and vigilance

Your staff will often be your first line of defense, one that must have - and continuously grow - the skills to practice and maintain readiness against cybersecurity risks.

Your Systems - *What Makes You Operational*

Protect critical assets and applications

Information is the life-blood of any business; it is often the most valuable of a business' intangible assets.

Know where this information resides, know what applications and networks store and process that information, and build security into and around these.

Your Surroundings - *The Digital Workplace*

Ensure only those who belong on your digital workplace have access

The authority and access you grant employees, managers, and customers into your digital environment needs limits, just as those set in the physical work environment do.

Setting approved access privileges requires knowing who operates on your systems and with what level of authorization and accountability.

Your Data - *What the Business is Built On*

Make backups and avoid the loss of information critical to operations

Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted.

Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.

Your Crisis Response

Limit damage and quicken restoration of normal operations

The strategy for responding to and recovering from compromise: plan, prepare for, and conduct drills for cyberattacks as you would a fire. Make your reaction to cyberattacks and system failures an extension of your other business contingency plans.

This requires having established procedures, trained staff, and knowing how - and to whom - to communicate during a crisis.

BOOTING UP

Things to Do First

Backup Data

Employ a backup solution that automatically and continuously backs up critical data and system configurations.

Multi-Factor Authentication

Require multi-factor authentication (MFA) for accessing your systems whenever possible. MFA should be required of all users, but start with privileged, administrative and remote access users.

Patch & Update Management

Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly.

CYBER ESSENTIALS

THE IT PROFESSIONAL'S GUIDE

✓ *Actions for leaders.*
✓ *Discuss with IT staff or service providers.*

Essential Actions for Building a *Culture of Cyber Readiness*:

Yourself
Drive cybersecurity strategy, investment and culture

- Lead investment in basic cybersecurity.
- Determine how much of your organization's operations are dependent on IT.
- Build a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information.
- Approach cyber as a business risk.
- Lead development of cybersecurity policies.

Your Staff
Develop security awareness and vigilance

- Leverage basic cybersecurity training to improve exposure to cybersecurity concepts, terminology and activities associated with implementing cybersecurity best practices.
- Develop a culture of awareness to encourage employees to make good choices online.
- Learn about risks like phishing and business email compromise.
- Identify available training resources through professional associations, academic institutions, private sector and government sources.
- Maintain awareness of current events related to cybersecurity, using lessons-learned and reported events to remain vigilant against the current threat environment and agile to cybersecurity trends.

Your Systems
Protect critical assets and applications

- Learn what is on your network. Maintain inventories of hardware and software assets to know what is in-play and at-risk from attack.
- Leverage automatic updates for all operating systems and third-party software.
- Implement secure configurations for all hardware and software assets.
- Remove unsupported or unauthorized hardware and software from systems.
- Leverage email and web browser security settings to protect against spoofed or modified emails and unsecured webpages.
- Create application integrity and whitelisting policies so that only approved software is allowed to load and operate on their systems.

Your Surroundings
Ensure only those who belong on your digital workplace have access

- Learn who is on your network. Maintain inventories of network connections (user accounts, vendors, business partners, etc.).
- Leverage multi-factor authentication for all users, starting with privileged, administrative and remote access users.
- Grant access and admin permissions based on need-to-know and least privilege.
- Leverage unique passwords for all user accounts.
- Develop IT policies and procedures addressing changes in user status (transfers, termination, etc.).

Your Data
Make backups and avoid loss of info critical operations

- Learn what information resides on your network. Maintain inventories of critical or sensitive information.
- Learn what is happening on your network. Manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities.
- Domain Name System Protection.
- Learn how your data is protected.
- Leverage malware protection capabilities.
- Establish regular automated backups and redundancies of key systems.
- Leverage protections for backups, including physical security, encryption and offline copies.

Your Crisis Response
Limit damage and quicken restoration of normal operations

- Lead development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often.
- Leverage business impact assessments to prioritize resources and identify which systems must be recovered first.
- Learn who to call for help (outside partners, vendors, government/ industry responders, technical advisors and law enforcement).
- Lead development of an internal reporting structure to detect, communicate and contain attacks.
- Leverage in-house containment measures to limit the impact of cyber incidents when they occur.

Consistent with the NIST Cybersecurity Framework and other standards, these actions are the starting point to Cyber Readiness. To learn more, visit ***CISA.gov/Cyber-Essentials****.*

CYBER ESSENTIALS

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

ESSENTIAL ELEMENT: YOURSELF, THE LEADER

THE TASK : Drive Cybersecurity Strategy, Investment and Culture

Being a cyber leader does not require technical expertise, but rather an ability to change the culture of your organization. Reducing your organization's cyber risks requires awareness of cybersecurity basics. As a leader, you need to drive your organization's approach to cybersecurity as you would any other hazard (e.g. how you identify risk, reduce vulnerabilities, and plan for contingencies). This requires an investment of time and money, as well as the collective buy-in of your management team. Your investment drives actions and activities, and these build and sustain a culture of cybersecurity.

Essential Actions

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

Approach cyber as a business risk. Ask yourself what type of impact would be catastrophic to your operations? What information if compromised or breached would cause damage to employees, customers, or business partners? What is your level of risk appetite and risk tolerance? Raising the level of awareness helps reinforce the culture of making informed decisions and understanding the level of risk to the organization.

Resources for Taking Action

National Association of Corporate Directors: The NACD Director's Handbook on Cyber-Risk Oversight is built around five core principles that are applicable to board members of public companies, private companies, and nonprofit organizations of all sizes and in every industry sector.

National Institute of Standards and Technology (NIST) Cybersecurity Framework: Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, and helps owners and operators of critical infrastructure manage cybersecurity-related risks.

CISA Security Tip – Questions Every CEO Should Ask About Cyber Risks: Provides a primer on basic questions that CEOs of all businesses should ask themselves and their employees to ensure better cybersecurity preparedness and resilience.

U.S. Small Business Administration: Small Business Cybersecurity: A guide to help leaders of small businesses learn about common cyber threats, gain an understanding about where their business might be vulnerable, and steps they can take to improve their level of cybersecurity.

Determine how much of your organization's operations are dependent on IT. Consider how much your organization relies on information technology to conduct business and make it a part of your culture to plan for contingencies in the event of a cyber incident. Identify and prioritize your organization's critical assets and the associated impacts to operations if an incident were to occur. Ask the questions that are necessary to understanding your security planning, operations, and security-related goals. Develop an understanding of how long it would take to restore normal operations. Resist the "it can't happen here" pattern of thinking. Instead, focus cyber risk discussions on "what-if" scenarios and develop an incident response plan to prepare for various cyber events and scenarios.

Resources for Taking Action

Cyber Readiness Institute: The Cyber Readiness Program is a practical, step-by-step guide to help small and medium-sized enterprises become cyber ready. Completing the Program will make your organization safer, more secure, and stronger in the face of cyber threats. The Cyber Readiness Program also provides a template for an incident response plan that your organization can customize.

NIST Small Business Cybersecurity Corner: This platform provides a range of resources chosen based on the needs of the small business community. These resources include planning guides, guides for responding to cyber incidents, and cybersecurity awareness trainings.

CISA CRR Supplemental Resource Guide Risk Management: The principal audience for this guide includes individuals responsible for managing risk management programs for IT operations, including executives who establish policies and priorities for risk management, managers and planners who are responsible for converting executive decisions into action plans, and operations staff who implement those operational risk management plans.

ESSENTIAL ELEMENT: YOURSELF, THE LEADER

Lead investment in basic cybersecurity. Invest in cybersecurity capabilities for your organization and staff. This includes not only investments in technological capabilities, but also a continuous investment in cybersecurity training and awareness capabilities for your organization's personnel. Use the Cyber Essentials to have conversations with your staff, business partners, vendors, managed service providers, and others within your supply chain. Use risk assessments to identify and prioritize allocation of resources and cyber investment.

Resources for Taking Action

NIST Cybersecurity Framework: Created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, and helps owners and operators of critical infrastructure manage cybersecurity-related risk.

Cyber Readiness Institute: The Cyber Readiness Program is a practical, step-by-step guide to help small and medium-sized enterprises become cyber ready. Completing the Program will make your organization safer, more secure, and stronger in the face of cyber threats. The Program also provides guidance on how to select a cyber leader to create a culture of cyber readiness.

Federal Trade Commission: Cybersecurity for Small Business provides resources developed in partnership with CISA, NIST and the U.S. Small Business Administration to help small business owners understand and implement cybersecurity basics.

Global Cyber Alliance: Cybersecurity Toolkit for Small Business: Built for small to medium-sized businesses to address the Center for Internet Security Controls for preventing and/or reducing the most common attacks in today's cyber threat landscape.

National Cyber Security Alliance: CyberSecure My Business™ is a national program helping small and medium-sized businesses (SMBs) learn to be safer and more secure online, with a variety of resources and tools aimed at this stakeholder group.

Build a network of trusted relationships for access to timely cyber threat information. Maintain situational awareness of cybersecurity threats and explore available communities of interest. These may include sector-specific Information Sharing and Analysis Centers, government agencies, law enforcement, associations, vendors, etc.

Resources for Taking Action

CISA: CISA is responsible for protecting the nation's critical infrastructure from physical and cyber threats. CISA.gov has a variety of cyber resources, training opportunities and information available at no cost to stakeholders.

National Council of Information Sharing and Analysis Centers (ISACs): Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.

Multi-State Information Sharing and Analysis Center (MS-ISAC): The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Information Sharing and Analysis Organizations (ISAOs): The ISAOs mission is to improve the nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices. Similar to ISACs, but cross-sector in design.

Global Cyber Alliance: The Global Cyber Alliance is an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world. It aims to achieve this mission by uniting global communities, developing concrete solutions, and measuring the effect.

National Cyber Security Alliance: CyberSecure My Business™ is a national program helping small and medium-sized businesses (SMBs) learn to be safer and more secure online, with a variety of resources and tools aimed at this stakeholder group.

America's Small Business Development Centers: Small business owners and aspiring entrepreneurs can go to their local SBDCs for free face-to-face business consulting and at-cost training. This website includes a number of cybersecurity resources for small businesses.

Lead development of cybersecurity policies. Business leaders and technical staff should collaborate on policy development and ensure policies are well understood by the organization. Perform a review of all current cybersecurity and risk policies to identify gaps or weaknesses by comparing them against recognized cyber risk management frameworks. Develop a policy roadmap, prioritizing policy creation and updates based on the risk to the organization as determined by business leaders and technical staff.

Resources for Taking Action

NIST Cyber Security Resource Center: The Computer Security Resource Center (CSRC) provides access to NIST's cybersecurity and information security-related projects, publications, news and events. CSRC supports stakeholders in government, industry and academia—both in the U.S. and internationally.

SANS Information Security Policy Templates: A library of comprehensive cybersecurity policy templates that business owners can use to inspire and optimize their own cyber policies. These templates cover a wide range of policy areas, including Network Security, Server Security, Application Security and more.

Guide for Developing Security Plans for Federal Information Systems: This guide for developing security plans for Federal information systems has a variety of useful technical data and guidance which can be used by a variety of non-Federal stakeholders as well.

Cyber Readiness Institute: The Cyber Readiness Program is a practical, step-by-step guide to help small and medium-sized enterprises become cyber ready. Completing the Program will make your organization safer, more secure, and stronger in the face of cyber threats. The Program also provides customizable policy templates focused on human behavior that address phishing, patching, passwords/authentication, and USB use.

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.

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 my 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 the world's leading, 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.

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.

ESSENTIAL ELEMENT: YOUR SYSTEMS, WHAT MAKES YOU OPERATIONAL

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.

CYBER ESSENTIALS

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

ESSENTIAL ELEMENT: YOUR SURROUNDINGS

THE TASK : Ensure Access Only to Those Who Belong on Your Digital Space

The access you grant employees, managers, and customers into your digital environment needs limits, just as those set in the physical work environment do (i.e., access to what's "behind the counter" or business records). Setting approved access privileges and establishing your operational procedures requires knowing who operates on your technology and with what level of authorization and accountability. User and Access Management is a complex activity and there is no one size fits all solution. Adopt a strategy appropriate to your organization and leverage a staged approach.

Essential Actions

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

Learn who is on your network. Do you know who is accessing your network? Do they have the proper permissions? How are they accessing your networking, and through which entry points? Create an inventory of connected devices to track who and what is on your network (i.e. Computers, smartphones, printers, and routers). Use network inventory spreadsheets to enhance security by keeping you aware of unauthorized use. Monitor and analyze user activities for anomalous behavior such as access attempts outside of normal operating hours or from unusual locations.

Resources for Taking Action

NSA Actively Manages Systems and Configurations: a guide that offers a range of techniques to minimize mission impact.

NSA Defend Privileges and Accounts: designed to limit exploitation and insider threat.

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

Center for Internet Security Control 4: this guidance focuses on the processes and tools used to control the assignment of administrative privileges.

Center for Internet Security Control 9: this guidance focuses on managing operational use of ports, protocols, and services on networked devices.

Leverage multi-factor authentication for all users. Strong access protection includes two or more factors: knowledge, possession, and inherence. Knowledge factors are something the user and only the user knows and include passwords, or personal identification numbers (PIN). Possession factors are something the user and only the user has, which can be a security badge, SMS text message with a code, and soft or hard token. Inherence factors are something the user and only the user is, such as fingerprints, voice, retina/iris patterns, and palmprints. Start with privileged, administrative, or remote-access users.

Resources for Taking Action

FTC Remote access guidance: identifies tools to secure networks for employees and vendors who need remote access.

NSA Defend Privileges and Accounts: designed to limit exploitation and insider threat.

Two Factor Auth (2FA): lists websites that support multi-factor authentication.

NSA Transition to Multi Factor Authentication: outlines how to use Multi-factor Authentication to defend against an array of authentication attacks.

NIST Digital Identity Guidelines

NIST Special Publication 1800-17: Multifactor Authentication for E- Commerce

Grant access and admin permissions based on need-to-know and least privilege. Restrict user access to only the information, networks, hardware and applications necessary. Are you asking why someone or something needs privileged access? Does the marketing team need access to the company's financial transactions? Does the reservations team need access to social media sites? Does a junior analyst need management-level admin/ configuration privileges? Answering these questions helps you identify and implement need-to-know and least privilege to lower the risks of malware infections, data breaches, and insider threats.

Resources for Taking Action

NIST Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations: this publication explains the principle of least privilege and how to apply least privilege to information systems.

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

NSA Defend Privileges and Accounts: designed to limit exploitation and insider threat.

Develop IT policies/procedures to address changes in user status. Implement policies, processes, and technologies to ensure that only authorized users are granted the minimum privileges needed. Identify and deactivate unused accounts, eliminate shared accounts, remove unnecessary privileges and enforce strong password policies to dissuade cyber criminals from accessing your networks. Termination, separation, or even moves to other departments within the organization with different access requirements require attention to user access abilities.

Resources for Taking Action

NIST Cybersecurity Resource Center: NIST's cybersecurity- and information security-related projects, publications, news, and events help support stakeholders.

NIST Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publications Library: includes guidelines, technical specifications, recommendations, and reference materials comprised of multiple sub-series.

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

NIST Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security: this publication provides security considerations for several remote access solutions.

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

SANS Security Policy Templates

Leverage unique passwords for all user accounts. Many cyber attacks occur due to weak and easy-to-guess passwords, so all passwords should be strong and unique, such as a sentence with numeric and non-numeric digits. Choose a pattern or template for your password that can be applied toward various accounts. This is something that is very individualized and therefore difficult to guess. A personal pattern or template allows for different passwords to be used for every account, while making it easy for the user and only the user to remember. Some hackers are more sophisticated and use algorithms to figure out passwords, so consider mechanisms that are stronger than password authentication such as biometrics, one-time passwords, and tokens for sensitive applications and functions.

Resources for Taking Action

Global Cyber Alliance Small Business Toolkit: provides tips and actions to keep your accounts safer by moving beyond simple passwords.

NIST Special Publication 800-63 Digital Identity Guidelines: covers identity proofing and authentication of users interacting with government IT systems over open networks.

CISA Creating and Managing Strong Passwords: identifies six actions that users can take to create and manage strong passwords.

ESSENTIAL ELEMENT: YOUR DATA

THE TASK : Backup your data and configurations, and keep the backups offline

Learn to protect your information as it is stored, processed, or transmitted. Identify information critical to operations stored on your network. Have plans in place to help recover and restore systems, networks, and data from known good backups.

Essential Actions

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

Learn what information resides on your network. Inventory critical or sensitive information. An inventory of information assets provides an understanding of what you are protecting, where that information resides, and who has access. The inventory can be tracked in a spreadsheet, updated quickly and frequently.

Resources for Taking Action

Global Cybersecurity GCA Toolkit: this toolkit offers free tools, practical tips, and resources and guides to improve your company's cybersecurity readiness and response.

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

Center for Internet Security (CIS) Controls Implementation Groups: helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.

Learn what is happening on your network. Manage network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. Actively maintaining information will give you a baseline for security testing, continuous monitoring, and making security-based decisions.

Resources for Taking Action

CISA Automated Indicator Sharing: enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed.

NIST draft Special Publication Zero Trust Architecture: contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST Special Publication 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations (Final Public Draft)

Domain Name System Protection. Domain Name System (DNS) protection blocks dangerous sites and filters out unwanted content. DNS servers ensure work devices are connecting through a secure portal. This adds a layer of protection against malware, phishing, and other viruses. Filter out connections to unauthorized websites, suspicious domain names, and known malicious domain names associated with malware and phishing. Leverage DNS filtering, also known as DNS Blocking, DNS Firewall, or protective DNS, with integrated threat intelligence. A number of effective commercial solutions are available ranging from free to low cost.

Resources for Taking Action

DNS protection – GCA Quad 9: Quad9 protects users from accessing known malicious websites, leveraging threat intelligence from multiple industry leaders.

NIST Secure Domain Name System Deployment Guide

ESSENTIAL ELEMENT: YOUR DATA, WHAT THE BUSINESS IS BUILT ON

Learn how your data is protected. Data should be handled based on its importance to maintaining critical operations in order to understand what your business needs to operate at a basic level. For example, proprietary research, financial information, or development data need protection from exposure in order to maintain operations. Understand the means by which your data is currently protected; focus on where the protection might be insufficient. Guidance from the Cyber Essentials Toolkits, including authentication, encryption, and data protection help identify methods and resources for how to best secure your business information and devices.

Resources for Taking Action

CIS Controls Implementation Groups: helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.

NIST Small Business Cybersecurity Corner: contains guidance to help protect the security of your business information and devices.

NIST NCCOE Data Security Program: guidance for data integrity and data confidentiality.

Leverage malware protection capabilities. Malware is designed to spread quickly. A lack of defense against it can completely corrupt, destroy or render your data inaccessible.

Resources for Taking Action

Global Cybersecurity GCA Toolkit: helps prevent phishing and viruses.

Cyber Readiness Institute's Ransomware Playbook: helps prioritize the data that is most critical to your organization and instructs how to back it up.

CIS Controls Implementation Groups: helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.

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

Establish regular automated backups and redundancies of key systems. Employ a backup solution that automatically and continuously backs up your business-critical data and system configurations. Regular backups protect against ransomware and malware attacks. Use on-site and remote backup methods to protect vulnerable information. Prioritize backups (based off of the importance of the information) and have a schedule of what to bring back online when so that your business can still function during a cyberattack. Test your backup strategy before you need to use it to make sure you have full read-back verification, a method of preventing errors when information is relayed or repeated in a different form in order to confirm its accuracy.

Resources for Taking Action

CIS Controls Implementation Groups: helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.

NIST Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations

NIST Contingency Planning Guide for Federal Information Systems

Leverage protections for backups, including physical security, encryption and offline copies. Ensure the backed-up data is stored securely offsite or in the cloud and allows for at least seven days of incremental rollback. Backups should be stored in a secure location, especially if you are prone to natural disasters. Periodically test your ability to recover data from backups.. Online and cloud storage backup services can help protect against data loss and provide encryption as an added level of security. Identify key files you need access to if online backups are unavailable to access your files when you do not have an internet connection.

Resources for Taking Action

CIS Controls Implementation Groups: helps organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.

NIST National Cyber Security Center of Excellence: a guide for managed service providers to conduct, maintain and test backup files; protecting data from ransomware and other data loss events.

ESSENTIAL ELEMENT: YOUR CRISIS RESPONSE

THE TASK : Limit Damage and Quicken Restoration of Normal Operations

Plan, prepare, and conduct drills for cyber-attacks and incidents as you would a fire or robbery. Make your reaction to cyber incidents or system outages an extension of your other business contingency plans. This involves having incident response plans and procedures, trained staff, assigned roles and responsibilities, and incident communications plans.

Essential Actions

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

Lead development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often. Incident response plans and disaster recovery plans are crucial to information security, but they are separate plans. Incident response mainly focuses on information asset protection, while disaster recovery plans focus on business continuity. Once you develop a plan, test the plan using realistic simulations (known as "war-gaming"), where roles and responsibilities are assigned to the people who manage cyber incident responses. This ensures that your plan is effective and that you have the appropriate people involved in the plan. Disaster recovery plans minimize recovery time by efficiently recovering critical systems.

Resources for Taking Action

NIST Special Publication SP 800-61 Rev. 2 Computer Security Incident Handling Guide focuses on incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

NIST Special Publication SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems provides guidance to evaluate information systems and to determine contingency planning requirements and priorities.

CISA and MS-ISAC Ransomware Guide provides best practices and recommendations for developing cyber incident response polices and procedures.

CISA Cyber Resilience Review Resource Guide – Incident Management is for organizations establishing an incident management process and improving their existing incident management process.

Center for Internet Security CSC 19 offers actions to develop and implement and incident response infrastructure.

SANS Security Policy Library

Leverage business impact assessments to prioritize resources and identify which systems must be recovered first. Business impact analysis helps identify and prioritize critical systems, information, and assets. This information determines contingency requirements and priorities for critical information and services. It also allows planning for disruption impacts and identifies allowable outage times. This enables personnel to develop and prioritize recovery strategies that can be used.

Resources for Taking Action

NIST Special Publication SP 800-184 Guide for Cybersecurity Event Recovery: this publication provides guidance regarding the planning, playbook developing, testing, and improvement of recovery planning.

NIST Special Publication SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems: this document provides guidance to evaluate information systems and to determine contingency planning requirements and priorities.

Learn who to call for help (e.g., outside partners, vendors, government/industry responders, technical advisors and law enforcement). As part of your incident response, disaster recovery, and business continuity planning efforts, identify and document partners you will call on to help. Consider building these relationships in advance and understand what is required to obtain support. CISA and the Federal Bureau of Investigation (FBI) provide dedicated hubs for helping respond to cyber and critical infrastructure attacks. Both have resources and guidelines on when, how, and to whom an incident is to be reported in order to receive assistance. You should also file a report with local law enforcement, so they have an official record of the incident.

Resources for Taking Action

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities as well as guidelines by which to do so.

Cyber Reporting guidance: this document details different ways SLTT law enforcement partners can report suspected or confirmed cyber incidents to the federal government.

Lead development of internal reporting structure to detect, communicate, and contain attacks. Effective communication plans focus on issues unique to security breaches. A standard reporting procedure will reduce confusion and conflicting information between leadership, the workforce, and stakeholders. Communication should be continuous, since most data breaches occur over a long period of time and not instantly. It should also come from top leadership to show commitment to action and knowledge of the situation.

Resources for Taking Action

NIST Special Publication SP 800-184 Guide for Cybersecurity Event Recovery: this publication provides guidance regarding the planning, playbook developing, testing, and improvement of recovery planning.

NIST Special Publication SP 800-61 Rev. 2 Computer Security Incident Handling Guide: this guidance focuses on incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

Cyber Readiness Institute Cyber Readiness Program provides customizable policy templates focused on human behavior that address phishing, patching, passwords/authentication, and USB use.

Leverage containment measures to limit the impact of cyber incidents when they occur. Communicate and execute your incident response plan, such as isolating a network segment of infected workstations or taking down production servers that were impacted, to rerouting traffic to unaffected infrastructure. Test systems to ensure they are operational and configured securely after the incident is resolved. Communicate the damage done and the improvements applied to recovery planning and action to build trust and a culture of growth and resilience.

Resources for Taking Action

NIST Special Publication SP 800-184 Guide for Cybersecurity Event Recovery: this publication provides guidance regarding the planning, playbook developing, testing, and improvement of recovery planning.

NIST Special Publication SP 800-61 Rev. 2 Computer Security Incident Handling Guide: this guidance focuses on incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

WEBINARS AND TRAININGS

Cyber Essentials FedVTE Course

The CISA Cyber Essentials are available as an engaging one-hour course through FedVTE's public course library. To access the course and get your organization started on the road to cyber readiness, click here.

CISA Cyber Essentials Video

This six-minute flash talk provides an overview of the new Cyber Essentials resources that were initially released in 2020 and available for use by the business community.

CISA Cyber Essentials Chapter 1: Yourself, The Leader Video

This half hour video provides a deep dive into toolkit 1 which focuses on you as a leader and how your investment (e.g., time and money) drives actions and activities, and these build and sustain a culture of cybersecurity within your organization.

Cybersecurity Essentials for the New Year Video

This half hour video provides an in-depth overview of the essential elements of and actions for building a culture of Cyber Readiness.

Cybersecurity Awareness Training Series Webinar: Cyber Essentials

This one and a half hour webinar features a panel of cybersecurity experts who provide training on toolkits 1-3 (Yourself, Your Staff, and Your Systems).

National Initiative for Cyberesecurity Education Online Cybersecurity Learning Content

The National Initiative for Cybersecurity Education (NICE) has compiled a page of numerous online courses for cybersecuirty professionals. To access this free and low-cost online educational content, click here.