CYBER ESSENTIALS

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

May 29, 2020

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.*

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.