CYBER ESSENTIALS
Your success depends on *Cyber Readiness*. Both depend on *YOU*.
November 17, 2020

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.