**1673: Full Cyber Incident Life Cycle**

**Model Content Revised Date: 11/26/2024**

A diagram of a recovery process

Description automatically generated

**Preparation**  
Essential to preventing and responding to a disruptive cyber event. To prepare, implement a series of tools ahead of time. This provides a framework to analyze, isolate, and respond. Developing a cyber incident response plan with key points of contact is important.

**Preparation Mechanisms:**

* Risk Assessments
* Host Security
* Network Security
* Malware Prevention
* User Awareness and Training
* <NCUA ACET (Automated Cybersecurity Evaluation Toolbox): (https://ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources/acet-and-other-assessment-tools)>
* Cyber Self-Assessment: [CSBS Ransomware Self-Assessment Tool](https://www.csbs.org/ransomware-self-assessment-tool)
  + Cyber-Controls Implementation (FFIEC, NIST)
  + Gap Analysis
  + Insurance Coverage
  + Identify Systems/Activities (internal/outsourced)
  + Data Locations
  + Vendor Remote Access
  + Risk Assessments (including Ransomware and Extortion)
  + Risk Mitigation
  + Employee Awareness and Information of Emerging Threats
  + Security Training
  + Cyber Incident Exercises
  + Data Backup Controls
  + MFA
  + Additional Controls
  + Ransomware Scenarios Included in Tabletop Exercises

**Detection and Analysis**  
Detection and analysis involves determining if an incident has occurred, its severity, and its type.

*Incident handling Checklist - Detection and Analysis*

* Determine if an Incident Has Occurred
  + Analyze Precursors and Indicators
  + Look for Correlating Information
  + Perform Research
  + (As soon as it is believed that an Incident has occurred) Begin Documenting and Gathering Evidence
* Prioritize Handling the Incident (based on the relevant factors)
* Report the Incident (to internal personnel and external organizations)

*Prevention Tools*

* DLP
* Executable File Blocking and Alerts
* Privileged Access Rights Change Alerts
* Active Monitoring of Network/Workstations
* Suspicious File Extension Detection
* Mass File Renaming Detection

**Containment, Eradication & Recovery**  
Containment, eradication and recovery focuses on addressing the incident, including preventing the spread and its impact, removing the cause of the incident, and restoring normal operations and recovery any lost or damaged data. Often cycles back to Detection and Analysis to ensure all elements have been identified.

*Incident handling Checklist – Containment, Eradication & Recovery:*

* Acquire, Preserve, Secure, and Document Evidence
* Contain the Incident
* Eradicate the Incident
  + Identify and mitigate all exploited vulnerabilities
  + Remove malware, inappropriate materials, and other components
  + If more hosts are discovered, repeat the Detection and Analysis steps, then Contain and Eradicate them.
* Recover from the Incident
  + Return Affected Systems to an Operational State
  + Confirm Normal Functionality
  + In necessary, Implement additional Monitoring

**Response Components**

* Incident Response Team
  + Roles:
    - Cyber Incident Manager
    - Management
    - Information Security
    - Information Technology
    - Legal (Outside Counsel)
    - Public Affairs (Communications)
    - Human Resources
    - Business Continuity
    - Facilities
* Response Procedures
  + Monitor Social Media/News Sources
  + Prevention/Isolation of Malware
  + Notification of Incident Response Stakeholders
  + Notification to Law Enforcement
  + Authority to Shut Down Third-Party Network Access
  + Implement “Out of Band” Communication Procedures
  + Mitigation of Exploited Vulnerabilities
  + Threat Hunting
  + Notification to Legal Counsel/Cyber-Insurance Carrier
  + Alternate Strategies for Connection to Third-Parties
  + Engagement of Cyber-Response Vendor
  + Escalation Process for BCP/DR
  + Preservation of Logs/Records
  + Data Restoration
  + Notification to NCUA/State Agencies
  + Communication Templates to Staff
  + Determination of Cause
  + Update Key Vendor Contact Information
  + Notify Employees, Credit Unions, Vendors as Warranted
  + Notify and Periodically Brief Stakeholders
* Third-Party Engagement Options

**Post Incident Activity**  
Post incident activity focuses on identifying lessons learned and opportunities for improvement, including best practices and necessary changes to prevent similar incidents, incident response planning, communications, and incident management.

*Incident handling Checklist – Post-Incident Activity:*

* Create a Follow-up Report using collected incident data and evidence
* Hold a Lessons Learned Meeting (mandatory for major incidents, optional otherwise)

*Response Components for Post-Restoration*

* User Testing Post-Restoration
* After Action Review/Lessons Learned
* Update Incident Response Plan with Lessons Learned
* Provide Refresher Training, as needed
* Notifying Stakeholders as Appropriate