Elections Infrastructure ISAC

Essential Guide to Election Security

Incident Response Planning

From power failures to flooding to malicous cyber attacks, incidents occur. While the type of incident and sophistication of the threat actors plays a major role in the outcomes, often the difference between minor and severe consequences have more to do with how you prepare for and respond to the incident.

To get back up and running quickly after an incident, you have to plan well. This means developing written plans – often called incident response plans, disaster recovery plans, or business continuity plans. It also means testing those plans through exercises.

Goals

1. Develop and maintain an incident response plan (Level 1 maturity)
2. Exercise your plans (Level 1 maturity)
3. Conduct after-action reports following and incident (Level 2 maturity)

Actions

For Incident Response Planning, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

1. Create and maintain an incident response plan.
   - Include relevant stakeholders from the various business units that may be impacted.
   - Identify and prioritize critical systems.
   - There are many resources available to help you out, including:
     - The Election Assistance Commission's tips for disaster planning.
     - CISA's Incident Response Support for Election Partners.
     - The Belfer Center's Election Playbook.
2. Exercise your plan regularly. At least once a year; before each election is better.
3. When an incident does occur, execute your plan.
   - The EI-ISAC is here to help during an incident. Contact soc@cisecurity.org.
4. Regularly review the your plan to ensure contacts are up to date and procedures are still effective and relevant

Level 2 and Level 3 Maturity

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. When an incident does occur, conduct an after action reviews to identify what went right, what went wrong, and make improvements to your plan.

Cost-Effective Tools

- CIS's Cyber Incident Checklist: Helps organizations deal with a cyber incident by 1) establishing reliable facts and a way to stay informed, 2) mobilizing a response, and 3) communicating what you know

Learn More

- CISA's Incident and Vulnerability Response Playbooks: Although intended for federal agencies, election offices should review them to benchmark their own vulnerability and incident response practices.
- The incident reponse sections of the Belfer Center's Elections Battle Staff Playbook: Guidance to help you develop incident trackers, train staff, and test your processes.

Mapping to CIS Controls and Safeguards

- 11.1: Establish and Maintain a Data Recovery Process (Level 1 maturity)
- 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents (Level 1 maturity)
- 17.1: Designate Personnel to Manage Incident Handling (Level 1 maturity)
- 17.2: Establish and Maintain Contact Information for Reporting Security Incidents (Level 1 maturity)
- 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents (Level 1 maturity)
- 17.4: Establish and Maintain an Incident Response Process (Level 2 maturity)
- 17.5: Assign Key Roles and Responsibilities (Level 2 maturity)
- 17.6: Define Mechanisms for Communicating During Incident Response (Level 2 maturity)
- 17.7: Conduct Routine Incident Response Exercises (Level 2 maturity)
- 17.8: Conduct Post-Incident Reviews (Level 2 maturity)
- 17.9: Establish and Maintain Security Incident Thresholds (Level 3 maturity)

Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices.

Previous
Backups

Next
Building and Managing Staff

Made with Sphinx and @pradyunsg's Furo
Last updated on Oct 03, 2022