Risk-based Approach to Election Cybersecurity

NCSL Elections Cybersecurity: States Teaming Up
Jackson, Mississippi

November 30, 2018
About CDT

At the Center of Democracy and Technology, we believe in the power of the internet. Whether it's facilitating entrepreneurial endeavors, providing access to new markets and opportunities, or creating a platform for free speech, the internet empowers, emboldens, and equalizes people around the world.

About Maurice

Roles
Senior Technologist
Technology Fellow (US Senate)
Local Government Manager
Election Volunteer

Education
Public Administration
Political Science
Cybersecurity Strategy
Overview

What is a Risk Management Framework?
Identifying High-value Assets
Protecting Against Cyber Threats
Maintaining Voter Confidence
Fortifying Local Defenses
Thinking Outside of the Box
What is a Risk Management Framework?

**Risk** = Probability x Impact

The objective is to **mitigate** not eliminate risk (zero risk impossible & impractical)
- Reduce impact (backups)
- Shift risk (insurance, partnerships)
- Accept risk (improbable acts)

Identify & **prioritize** all assets (what does the organization care about, what's the worst that can happen?)

**Continuous** monitoring & reassessment (what has changed about the threat & the organization’s priorities?)
Identifying High-value Assets

**Impact**
(security categorization*)
- Low (limited)
- Moderate (serious)
- High (catastrophic)

**CIA**
(security objectives*)
- Confidentiality (disclosure of private, proprietary information)
- Integrity (modification of destruction of information)
- Availability (*disruption of access to information*)

*FIPS 199 (Federal Information Processing Standard)*

Account for **intangible** assets
(voter confidence)
Attackers try to change the registration, votes, & reporting (data or communication)
  • Phishing
  • Ransomware
  • Theft
  • Confusion

Fixating on one attacker is itself a vulnerability (there are plenty of domestic & foreign threats)
  • Nation-state
  • Terrorists
  • Activists
  • Criminal organizations
  • Lucky hacker
Maintaining Voter Confidence

**Acknowledge** the threats & **communicate** preparedness (internally & externally)
- Elections should be included in disaster recovery, business continuity planning
- Post-election risk-limiting audits are cost-effective assurance
- Vocabulary matters (scan, breach, denial of service)

Leverage **social media** to counter fake news (“fake news” is nuanced)
- *Dis*information (false and deliberately created to harm)
- *Mis*information (false, but not created with to cause harm)
- *Mal*information (based on reality, used to inflict harm)
Fortifying Local Defenses

Top 20 **most effective** data security steps*
(start with the **Top 5** to build an organizational culture of security)

- Contact Homeland Security
- 2-factor authentication
- Test backups

<table>
<thead>
<tr>
<th>No.</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Inventory and Control of Hardware Assets</td>
</tr>
<tr>
<td>2.</td>
<td>Inventory and Control of Software Assets</td>
</tr>
<tr>
<td>3.</td>
<td>Continuous Vulnerability Management</td>
</tr>
<tr>
<td>4.</td>
<td>Controlled Use of Administrative Privileges</td>
</tr>
<tr>
<td>5.</td>
<td>Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
</tr>
<tr>
<td>6.</td>
<td>Maintenance, Monitoring and Analysis of Audit Logs</td>
</tr>
<tr>
<td>7.</td>
<td>Email and Web Browser Protections</td>
</tr>
<tr>
<td>8.</td>
<td>Malware Defenses</td>
</tr>
<tr>
<td>9.</td>
<td>Limitation and Control of Network Ports, Protocols, and Services</td>
</tr>
<tr>
<td>10.</td>
<td>Data Recovery Capabilities</td>
</tr>
<tr>
<td>11.</td>
<td>Secure Configuration for Network Devices, such as Firewalls, Routers and Switches</td>
</tr>
<tr>
<td>12.</td>
<td>Boundary Defense</td>
</tr>
<tr>
<td>13.</td>
<td>Data Protection</td>
</tr>
<tr>
<td>14.</td>
<td>Controlled Access Based on the Need to Know</td>
</tr>
<tr>
<td>15.</td>
<td>Wireless Access Control</td>
</tr>
<tr>
<td>16.</td>
<td>Account Monitoring and Control</td>
</tr>
<tr>
<td>17.</td>
<td>Implement a Security Awareness and Training Program</td>
</tr>
<tr>
<td>18.</td>
<td>Application Software Security</td>
</tr>
<tr>
<td>19.</td>
<td>Incident Response and Management</td>
</tr>
<tr>
<td>20.</td>
<td>Penetration Tests and Red Team Exercises</td>
</tr>
</tbody>
</table>

*CIS Controls (Center for Internet Security)
Get out of the security culture **Danger Zone ASAP**
(accountability without capability)
Cultivate **technical** volunteers
(community members with technical skills or an IT support background)
- Schools
- Trade associations
- Businesses

**Larger** federal role in security
(security requires more consistency)
- Voting machine software development, hardware specification
- Procurement & manufacturing (including supply chain vetting)
- States partner with systems integrators to meet local needs
- Full deployment of DHS Continuous Diagnostics and Mitigation (CDM)
- Long-term budgeting (10-year lifecycle)
Resources available from CDT:

Election Cybersecurity 101 Field Guides are a series of short, simple, usable guides intended to help election administrators and staff better understand key concepts in cybersecurity.

- Passwords, Two-factor Authentication, DDoS Attack Mitigation, Audits (coming soon)

Online series of cybersecurity courses with the Center for Technology and Civic Life that will empower your election office to manage cyber threats and communicate with the public about cybersecurity.
THANK YOU | CDT.ORG

maurice@cdt.org
@TypeMRT

Risk-based Approach to Election Cybersecurity