SLTT Cybersecurity Maturity – A Snapshot of 2019

Eugene Kipniss
Member Programs Manager, EI-ISAC and MS-ISAC
Nationwide Cybersecurity Review

- Annual Self-Assessment
  - No Cost
  - Anonymous
- NIST Framework
- Required for some FEMA HSGP grant recipients
  - Align use of these funds to gaps measured by the NCSR year to year
- Cybersecurity Roadmap
  - Identify Areas for Improvement
  - Justify Investments

<table>
<thead>
<tr>
<th>Score</th>
<th>Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Optimized: Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.</td>
</tr>
<tr>
<td>6</td>
<td>Tested and Verified: Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.</td>
</tr>
<tr>
<td>5</td>
<td>Implementation in Process: Your organization has formally documented policies, standards, and procedures and is in the process of implementation.</td>
</tr>
<tr>
<td>5</td>
<td>Risk Formally Accepted: Your organization has chosen not to implement based on a risk assessment.</td>
</tr>
<tr>
<td>4</td>
<td>Partially Documented Standards and/or Procedures: Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.</td>
</tr>
<tr>
<td>3</td>
<td>Documented Policy: Your organization has a formal policy in place.</td>
</tr>
<tr>
<td>2</td>
<td>Informally Performed: Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.</td>
</tr>
<tr>
<td>1</td>
<td>Not Performed: Activities, processes and technologies are not in place to achieve the referenced objective.</td>
</tr>
</tbody>
</table>
Nationwide Cybersecurity Review

2019 Participants

• 3,135 Total Participant Organizations
  • 50 State Governments
  • 16 State Level Elections Offices
  • 2,523 Local Governments
  • 19 Tribal Governments
  • 6 Territorial Participants

https://www.cisecurity.org/ms-isac/services/ncsr
2019 NCSR Results for State, Local, Tribal, and Territorial Governments

<table>
<thead>
<tr>
<th></th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>4.78</td>
</tr>
<tr>
<td>Local</td>
<td>3.61</td>
</tr>
<tr>
<td>Tribal</td>
<td>3.54</td>
</tr>
<tr>
<td>Territory</td>
<td>2.98</td>
</tr>
</tbody>
</table>
2019 NCSR Results for State and Local Elections

State: Elections
- 4.20

Local: Elections
- 3.20
2019 NCSR Key Findings

• All peer groups of SLTT organizations continued to score below the overall minimum recommended maturity level of five (Implementation in Process).

• Adoption of a security framework has a significant impact on organizational cyber maturity.

• Continuous engagement is a key factor in the cybersecurity maturity of SLTTs.

• The lowest scoring categories measured in the NCSR are related to risk management and supply chain risk management.
Highlighted Results by NIST CSF Category

• **Identify - Supply Chain Risk Management** was the area of lowest maturity for State Elections, Local Elections, and State, Local, Tribal, and Territorial Governments

• **Identify - Risk Management Strategy** was the area of second lowest maturity for State Elections, Local Elections, and State, Local, and Tribal Governments

• **Respond – Improvements and Recover – Improvements** were the lowest scoring categories within their functions for the State, Local, Tribal, and Territorial Governments
Improving Maturity Moving Forward
Some Key Recommendations for the SLTT Community and Partners

• **General Recommendation**: Use the [NIST CSF Policy Template Guide](#) to locate template policies for customization and adoption.

• **General Recommendation**: Services and resources for SLTT organizations should be delivered at no or low-cost with low impact on staffing.

• **Identify - Supply Chain Risk Management**: Leverage the [CIS Election Technology Procurement Guide](#). The MS-ISAC Metrics Working Group’s new Supply Chain Subcommittee is collecting policy/procedure templates.

• **Respond – Improvements and Recover – Improvements**: Utilize the MS-ISAC Business Resiliency Working Group’s guide on reviewing lessons learned and turning after-action reporting into improvements to processes.
## 2019 Top Reported Security Concerns

<table>
<thead>
<tr>
<th></th>
<th>Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lack of sufficient funding</td>
</tr>
<tr>
<td>2</td>
<td>Increasing sophistication of threats</td>
</tr>
<tr>
<td>3</td>
<td>Lack of documented processes</td>
</tr>
<tr>
<td>4</td>
<td>Emerging technologies</td>
</tr>
<tr>
<td>5</td>
<td>Inadequate availability of cybersecurity professionals</td>
</tr>
<tr>
<td>6</td>
<td>Lack of a cybersecurity strategy (i.e., shifting priorities)</td>
</tr>
</tbody>
</table>
Nationwide Cybersecurity Review
Tell all the SLTT about it!

• 2019 NCSR Summary Report is coming in Fall 2020
  • Learn more about our findings and data set regarding SLTT maturity

• 2020 NCSR
  • Currently Open for Registration
  • Officially open October 1 through December 31
  • More participation leads to better data and recommendations

• Registration & Resources
  • Located on NCSR Webpage
  • End-User Guidance
  • Results & Reporting Templates

Resources
  ✓ NCSR-FAQ
  ✓ NCSR One Page Overview
  ✓ NCSR-General User Guide

Confidential & Proprietary
Thank You

Multi-State Information Sharing & Analysis Center (MS-ISAC)

Email: NCSR@cisecurity.org
Website: https://www.cisecurity.org/ms-isac/services/ncsr