CYBERSECURITY INSIDE STATE LEGISLATURES
WEDNESDAY, MAY 22, 2019
2:00 PM ET / 1:00 PM CT / NOON MT / 11:00 AM PT
Cybersecurity Threats in State Legislatures

Jeff Ford
Chief Technology/Security Officer
State of Indiana
Legislative Services Agency
Office of Technology Services

Certified Information Systems Security Professional (CISSP)
Global Information Assurance Certification (GSEC)

NALIT – Vice Chair
NALIT 2018 Cybersecurity Survey

- 25 states responded
- 48% use executive branch cybersecurity services
- 28% have a Chief Information Security Officer
- 26% have at least 1 dedicated Security Analyst
- 6 states use a security framework (NIST, ISO)
- 9 states provide security awareness training to legislators, but only 1 makes it mandatory
- 14 states provide security awareness training to legislative staff, but only 5 make it mandatory
Securing our Infrastructure

Legislative Services Agency
Office of Technology Services
Securing our Devices
Top 6 CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Legislative Services Agency
Office of Technology Services
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises
Cybersecurity Teams

- Blue Team
  - Defensive
- Red Team
  - Offensive
- Purple Team
  - Hybrid
Common Opensource Tools

- SOFELK
- Bro
- Snort
- Kali
- Security Onion
- FireEye Commando VM
- FireEye Flare VM
- REMnux
- Ghidra
Top Threats

- Hacktivists
- Script Kiddies
- Insiders
- Nation State
  - Advanced Persistent Threat (APT)
- Organized Crime
Things to Remember

- We don’t operate inside of castles anymore, protect your endpoints
- If you can’t do 1-6 well you are just checking the boxes
- Pick 5 things to work on and then move on to the next 5
- Our most valuable security assets are our employees
- Security can no longer be just part of someone's job description
Resources

- MSISAC – Multi-State Information Sharing and Analysis Center
- US-CERT – United States Computer Emergency Readiness Team
- www.cisecurity.org
- SANS.org
- http://www.newsnow.co.uk/h/Technology/Security
- Hacker News
- Brian Krebs
- John Strand – Black Hills Information Security
Contact Information

Jeff Ford CISSP|GSEC
Chief Technology/Security Officer
State of Indiana
Legislative Services Agency
Office of Technology Services

jeff.ford@iga.in.gov
Twitter: @jeffridford
Washington State Legislature Cybersecurity

Michael Norris
Cybersecurity Administrator
Legislative Service Center

Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Identifying the Need

- Regulatory Drivers
- Cybersecurity Audits
- Cybersecurity Breaches in the News
- Consulting Advice - Gartner
  “An organization should have one dedicated security person for every 30 IT staff.”
- IT Self-Identifies Security Needs
Filling the Need

• A few things to consider:
  • Temporary CISOs or security admins offer a unique opportunity to create the function and scope of a security program.
  • Utilizing contractors or firms can help provide time to find right person with the right skill.
  • Do not adopt an event-based approach. Waiting for an event is too late. There can be a lot of damage done between an event and a hire.

Note: Contracting firms often provide assessments with the intent to sell additional services. Be very deliberate about the engagement’s scope.
Common Options

- **Insourcing**
  - Hiring New – Can be a long process
  - Promoting from Within – Builds on institutional knowledge but can lack experience

- **Outsourcing**
  - Contract to Hire – Often a good option but candidate wants guarantees
  - Temporary Contract – Can address immediate issues but it is a short-term solution

- **Deputizing**
  - Not recommended for managing the program
  - Useful to expand teams without adding head count
Setting Expectations

• A security person cannot guarantee there will be no security issues but is the best person to respond when a security issue comes up.

Old security saying “You cannot stop a targeted attack – you can just respond to it.”

• Rome was not built in a day – It will take time to implement a program.
Starting Our Security Program
The first priority was to identify the biggest gaps and quick wins.
Our approach was to use the NIST Cybersecurity Framework and generate a Security Profile.

<table>
<thead>
<tr>
<th>Disciplines</th>
<th>Domains</th>
<th>Average Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY (ID)</td>
<td>Gov.</td>
<td>1.3</td>
</tr>
<tr>
<td>PROTECT (PR)</td>
<td>Gov.</td>
<td>1.9</td>
</tr>
<tr>
<td>DETECT (DE)</td>
<td>Gov.</td>
<td>3.5</td>
</tr>
<tr>
<td>RESPOND (RS)</td>
<td>Gov.</td>
<td>1.5</td>
</tr>
<tr>
<td>RECOVER (RC)</td>
<td>Gov.</td>
<td>1.0</td>
</tr>
</tbody>
</table>
Year 1

• Profile focus was on identification, prevention and remediation
  • Key Projects
    • Network Security
    • Data Security
    • Training
    • Multifactor for Email (MS Office)
    • Incident Response
Focus on Incident Response
Incident Response

“By failing to prepare, you are preparing to fail.”

Benjamin Franklin
Standards

Lifecycle

Figure from NIST SP 800-61r2
IR Roles and Responsibilities

- Incident Manager
- Incident Technical Team Lead
- Technical Owners
- Subject Matter Experts
- Leadership
- Third Parties
Don’t Recreate the Wheel

• Use what you have
  • If you have disaster recovery processes that overlap, use them.
  • If you have deployed incident management processes, incorporate them.
  • Use customer communication templates.

• Differences
  • Cybersecurity IR must be contained to a select few.
  • Evidence must be collected in a manner that could hold up in a court case.
  • Users’ privacy and organization data must be maintained and secured.
  • Processes, plans, and tools must be guarded.
Run Books

• Benefits
  • Ensure required activities and steps are followed.
  • Save time and focus efforts.
  • Provide legal counsel or auditors the steps you took or should take in the event of an incident.

• Considerations
  • Start with the common events or threats that cause the most risk.
  • Don’t go into the weeds – stay high level until you have tested your plans.
  • Include any third-party contact information.
  • Make sure you have multiple copies of the plan and team members can access the plans from offsite locations.
IR Exercises

Test your incident response plan at least annually.

- This can be accomplished via table-top exercises.

- Live exercises can be conducted with the following parameters:
  
  1. All exercises must have rules of engagement.
  
  2. No production systems outside the scope of the engagement should be affected.
  
  3. No data should be corrupted or irrecoverable.
  
  4. If the exercise will affect production systems, communicate with customers about what to expect.

- If an incident occurs during the year, it should be documented and can count as an exercise.
Incident Response References

- Best practices from CERT

- NIST standard

- Courses
  - https://digital-forensics.sans.org/training
Contact

Michael Norris, CISSP, CISA
Cybersecurity Administrator
Legislative Service Center
(360) 786-7149 | Michael.Norris@leg.wa.gov | http://leg.wa.gov
Questions?

Contact
pam.greenberg@ncsl.org