Securing Minnesota

Aaron Verdell Call
State Chief Information Security Officer, Interim Chief Technology Officer

Information Technology for Minnesota Government | mn.gov/mnit
Cybersecurity on the Small Scale
Operating at Enterprise Scale

- More business processes
- More complicated operations
- More severe consequences
- Increased stakeholder diversity
- Broader IT spectrum
- Increased threat exposure
The Threat

**Fraudsters**  
*Financial Gain*  
- Data theft
- Ransomware

**Hacktivists**  
*Civil Disobedience*  
- Denial of service
- Data disclosure

**Nation States**  
*Civil Unrest*  
- Data theft or destruction
- Denial of service
- Persistent infiltration
### Breach Lessons

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>75%</td>
<td>Hacks perpetrated by external actors</td>
</tr>
<tr>
<td>93%</td>
<td>Web application compromises associated with organized crime</td>
</tr>
<tr>
<td>43%</td>
<td>Breaches involved attacks on users</td>
</tr>
<tr>
<td>98%</td>
<td>Systems compromised within minutes</td>
</tr>
<tr>
<td>50%</td>
<td>Victims notified by third party or law enforcement</td>
</tr>
</tbody>
</table>

*2017 Verizon DBIR (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/)*
Enterprise Security Obstacles

**Historical Underinvestment**
- 2% of total IT Spend
- Some agencies with no dedicated budget
- Lack of process maturity

**Decentralized IT Environments**
- Overlapping Technologies
- Extremely costly to secure

**Outdated Business Systems**
- Security Issues no longer fixed by vendors
- Cannot run on secure operating systems
Where to Start
16E.03 Subd. 7. Cyber security systems. 
In consultation with the attorney general and appropriate agency heads, the chief information officer shall develop cyber security policies, guidelines, and standards, and shall install and administer state data security systems on the state's computer facilities consistent with these policies, guidelines, standards, and state law to ensure the integrity of computer-based and other data and to ensure applicable limitations on access to data, consistent with the public's right to know as defined in chapter 13. The chief information officer is responsible for overall security of state agency networks connected to the Internet. Each department or agency head is responsible for the security of the department's or agency's data within the guidelines of established enterprise policy.
Who owns risk?
Cybersecurity Foundation

Service Delivery Model

Policies and Standards

Strategic Plan
Service Delivery Model

Centralized Services
- Information Security Program Management
- Endpoint Defense
- Boundary Defense
- Vulnerability Management
- Incident Response and Forensics
- Monitoring

Local Services
- Secure Engineering
- Risk and Compliance
- Security Awareness
- Disaster Recovery
- Identity and Access Management
- Physical Security Oversight
Talent

- Feeder program
- Career paths
- Training
Policies and Standards

• Derived from existing regulatory and compliance requirements
  • HIPAA
  • CJIS
  • IRS Pub 1075
• Interpreted through industry best practice
• Normalized to provide clear and consistent guidance

https://mn.gov/mnit/
• Click on “Cybersecurity” in nav bar
Strategic Plan

- 5 year aspirational vision
- 18 core strategies
- 1 year milestones
- Extensive vetting
- Annual updates
- Public Version Available
Securing an Enterprise is a Daunting Challenge
Building Toward Secure

- Focus on business risk
- Communicate
- Seek external assistance
- Plan for failure

Priorities

1.
2.
3.
Basic Controls (Top 6 of 20)

✓ Inventory and Control of Hardware
✓ Inventory and Control of Software
✓ Continuous Vulnerability Management
✓ Controlled Administrative Privileges
✓ Secure Configuration for Hardware and Software
✓ Maintenance, Monitoring and Analysis of Audit Logs
Thank you!

aaron.call@state.mn.us