Securing Minnesota: A Plan to Fill the Gaps

Thomas Baden | Commissioner and Chief Information Officer

Aaron Call | Chief Information Security Officer
We Operate in a Threat Laden World
The Actors

**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/)*
Securing Government is a Daunting Challenge
Pain Points

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Outdated Business Systems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
Building A Foundation for Success
Cybersecurity Foundation

Service Delivery Model

Policies and Standards

Strategic Plan
Strategic Plan

- ✔ 5 year aspirational vision
- ✔ 18 core strategies
- ✔ 1 year milestones
- ✔ Extensive vetting
- ✔ Annual updates
Theme #1: Build Secure Systems
Security Engineering

- Integrated system development
- Specialized security tools
- System security plans
- Risk communication
Secure Datacenters

- 24*7*365 staffing
- Physical security
- Consistent and frequent patching
- Enterprise security program tools and processes
Secure Network

- Advanced monitoring tools
- Strong perimeter protection
- Data loss prevention
Theme #2: Improve Situational Awareness
Risk Management

- Ongoing application risk assessments
- Cybersecurity risk scorecards
- Cybersecurity insurance
Training

- General awareness training
- Targeted training
- Executive awareness
Theme #3: Minimize Operational Risk
Denial of Service

- Streamline mitigation processes
- Prepare for massive attacks
Vulnerability Management

- Find exploitable vulnerabilities faster
- Reduce time to remediate issues
Monitoring

- 24*7*365 coverage
- Advanced monitoring tools
- Faster incident response and forensics
Disaster Recovery

- Testable recovery strategies
- Exercise viability of plans
Theme #4: Foster Strategic Partnerships
Threat Intelligence

✓ More intelligence feeds
✓ Local government coordination
Talent

- College talent feeder program
- Scholarship for Service
Gaps in the Foundation
Strategic Plan

- 104 total outcomes
- 60 cannot be addressed, 12 of which are high risk

<table>
<thead>
<tr>
<th>Previous Initiative</th>
<th>FY18</th>
<th>Ongoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Security Program</td>
<td>$8.04M</td>
<td>$4.78M</td>
</tr>
</tbody>
</table>
Secure Datacenters

- Progress to reduce number of legacy datacenters hampered by lack of seed capital
- Complete transition may take 5 years or longer at current pace

<table>
<thead>
<tr>
<th>Previous Initiative</th>
<th>FY18</th>
<th>Ongoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Consolidation</td>
<td>$14.1M</td>
<td>$0</td>
</tr>
</tbody>
</table>
Outdated Business Systems

- System upgrade Initiatives in all budget bills
- Only a small percentage of initiatives funded
- Legacy technology security issues will continue to get worse

Priorities

1.
2.
3.
We are all part of the cybersecurity risk equation. MNIT needs policymaker support to protect citizens’ data and ensure the continued availability of critical government services.
Thank you!

Thomas.Baden@state.mn.us
Aaron.Call@state.mn.us