Securing Minnesota: A Plan to Fill the Gaps

Chris Buse | Chief Information Security Officer
The Internet is Way Cool
Smart fridge can track what it stores, alerting when products expire, & even add items to smartphone shopping list

Smart TV's connect to the Internet for web browsing, image sharing, gaming, or watching streaming video

Personal medical devices can be implantable or external & allow remote monitoring / treatment

Security cameras & systems can be remotely armed & checked, get alerts or review your security feeds from any location

Today's cars are computer-guided and wirelessly connected via Bluetooth, GPS, radio protocols

F-35 fighter jet has a highly advanced computerized logistics system designed to minimize repair and re-equipment turnaround times by monitoring the plane's status and pre-emptively making service decisions so that ground crews are ready to go before the plane even lands

Sources: Gartner, Forbes, Vice, Cisco IBSG, University of Michigan, ABC News, Qmed, Network World

Over 6.4 Billion Internet Things
Roughly 42,000 times more capacity than it took to put humans on the moon
There is a Dark Side
"...the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat."
--- President Barak Obama
<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90%</td>
<td>Hacks perpetrated by external actors</td>
</tr>
<tr>
<td>60%</td>
<td>Systems compromised within minutes</td>
</tr>
<tr>
<td>75%</td>
<td>Initial compromises spread within 24 hours</td>
</tr>
<tr>
<td>50%</td>
<td>New vulnerabilities became full exploits in less than 30 days</td>
</tr>
<tr>
<td>70 – 90%</td>
<td>Malware samples are unique to an entity</td>
</tr>
</tbody>
</table>
2017 Threats Trends

- Internet of Things Exploits
- Cyber crime as a service
- Massive DDoS attacks
- Increase in cyber espionage
- Increase in attacks against elections

- More attacks against control systems
- Increase in attacks against open source software
- Increase in phishing campaigns
- Ransomware
A Foundation for Cyber Risk Management
Strategic Plan

- 18 core strategies
- 5 year aspirational goals
- 1 year milestones
- Extensive vetting
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
✓ College talent feeder program
✓ Scholarship for Service
Is Government on a Path to Succeed?
Given the cost of cybersecurity solutions, extremely high demand for talent and expanding threat landscape, the success of all Minnesota government entities will be incumbent on how well we share resources, tools, talent and information to address threats and protect the people of our state.

--- State of Minnesota IT Master Plan
Thank you!

Chris.buse@state.mn.us
@BuseTweet