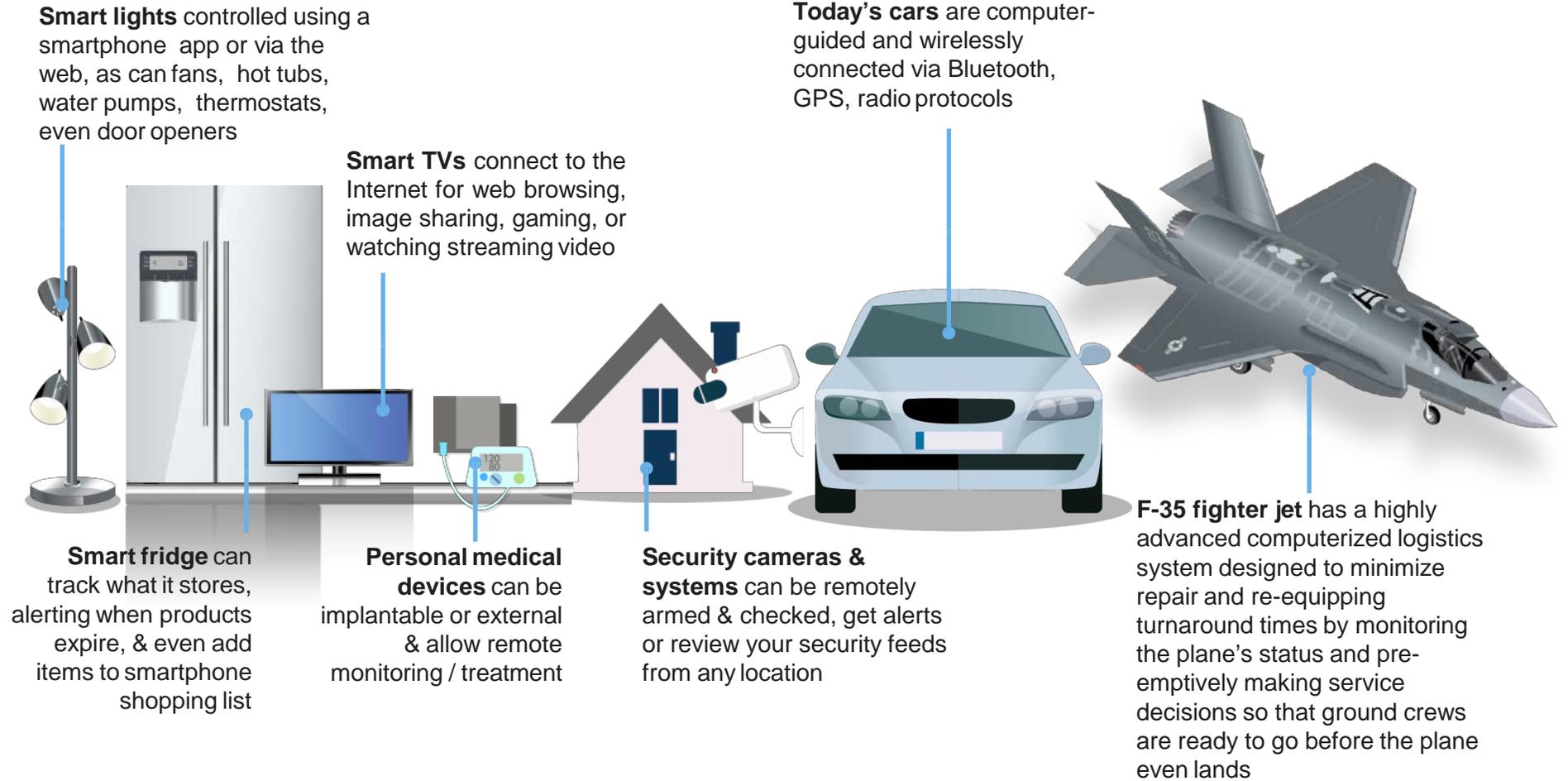# Securing Minnesota: A Plan to Fill the Gaps

Chris Buse | Chief Information Security Officer

The Internet is Way Cool

Over 6.4 Billion Internet Things

Smart lights controlled using a smartphone app or via the web, as can fans, hot tubs, water pumps, thermostats, even door openers

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

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

Smart fridge can track what it stores, alerting when products expire, & even add items to smartphone shopping list

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

F-35 fighter jet has a highly advanced computerized logistics system designed to minimize repair and re-equipping 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

Massive Capacity

Roughly 42,000 times more capacity than it took to put humans on the moon

There is a Dark Side
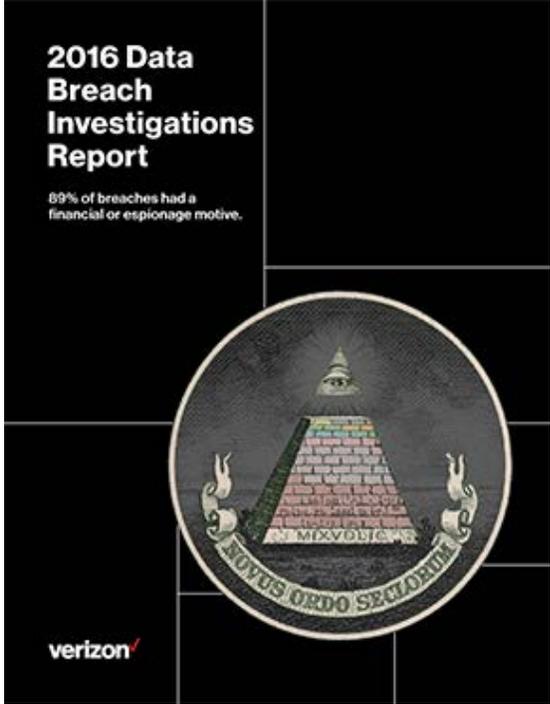
Unprecedented Cyber Threats

*"...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

Fraudsters — THEFT

Hacktivists — DISRUPTION

Nation States — DESTRUCTION

ADDITIVE MOTIVATION PROGRESSION LINE

Threat Landscape

90%	Hacks perpetrated by external actors
60%	Systems compromised within minutes
75%	Initial compromises spread within 24 hours
50%	New vulnerabilities became full exploits in less than 30 days
70 – 90%	Malware samples are unique to an entity

2016 Data Breach Investigations Report
89% of breaches had a financial or espionage motive.
verizon

More Threats
More Targeted
More Sophisticated

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
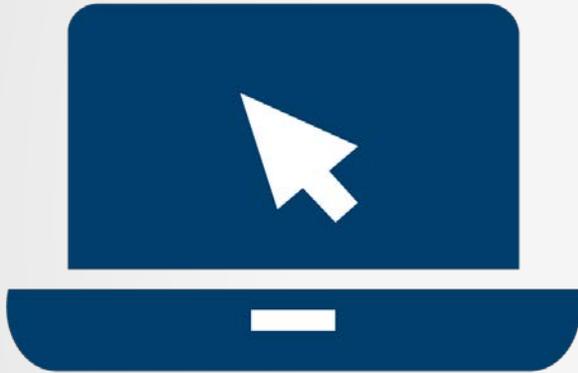
- ✓ 18 core strategies
- ✓ 5 year aspirational goals
- ✓ 1 year milestones
- ✓ Extensive vetting

Theme #1: **Build Secure Systems**

Security Engineering
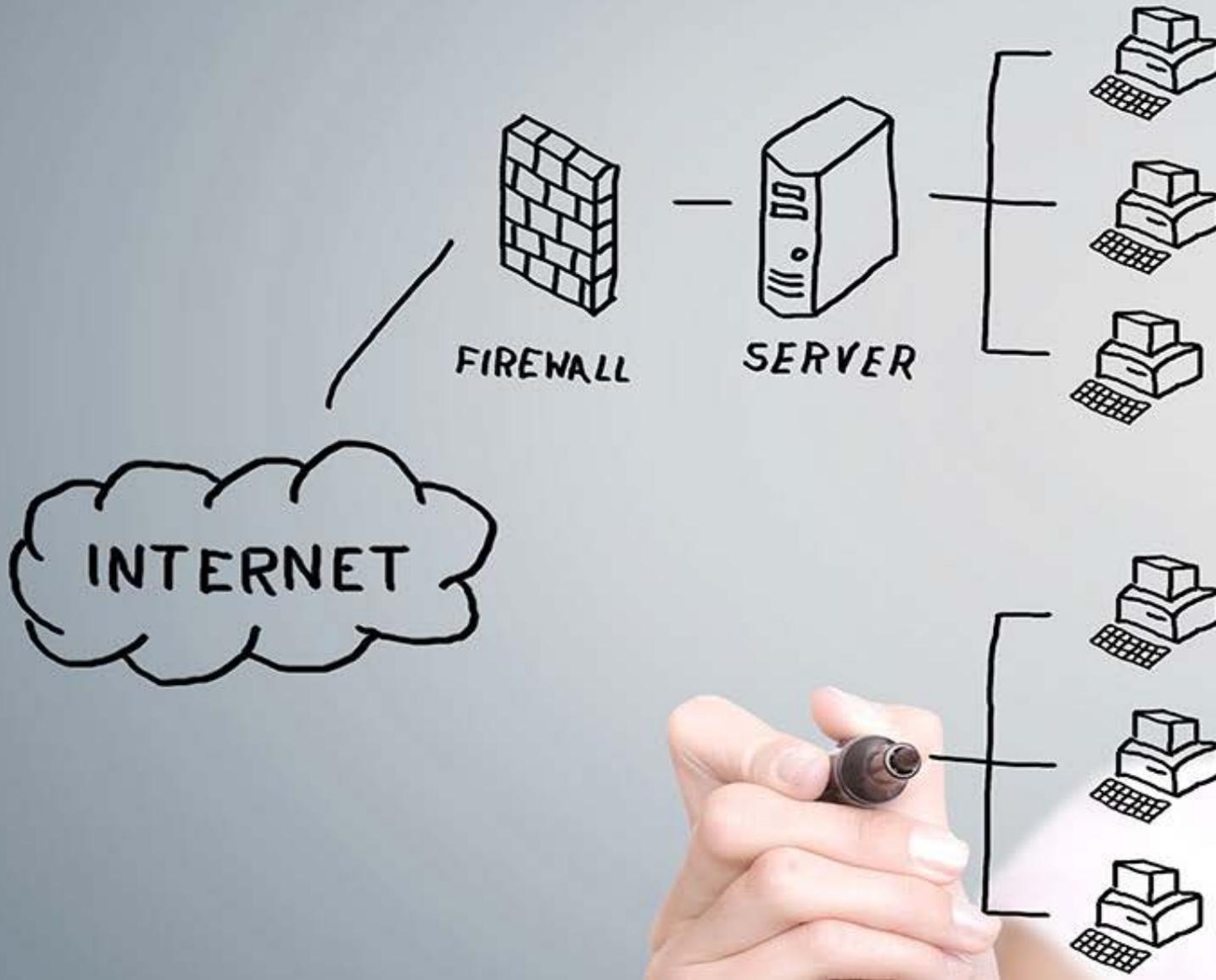
- ✓ Integrated system development
- ✓ Specialized security tools
- ✓ System security plans
- ✓ Risk communication

Secure Datacenters

✓ 24*7*365 staffing

✓ Physical security

✓ Consistent and frequent patching

✓ Enterprise security program tools and processes

- ✓ Advanced monitoring tools
- ✓ Strong perimeter protection
- ✓ Data loss prevention

Theme #2: **Improve Situational Awareness**

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

- ✓ General awareness training
- ✓ Targeted training
- ✓ Executive awareness

Theme #3: **Minimize Operational Risk**

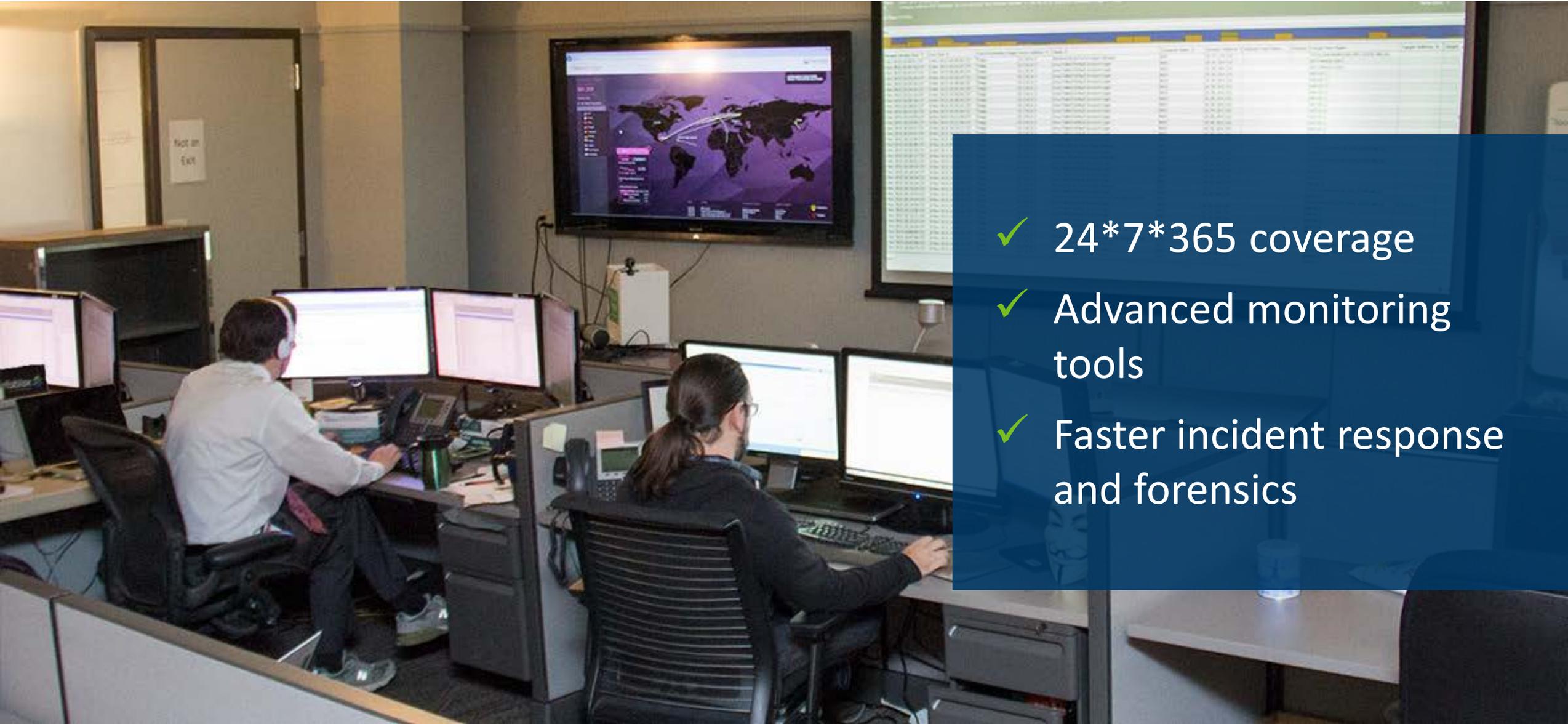- ✓ Streamline mitigation processes
- ✓ Prepare for massive attacks

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?
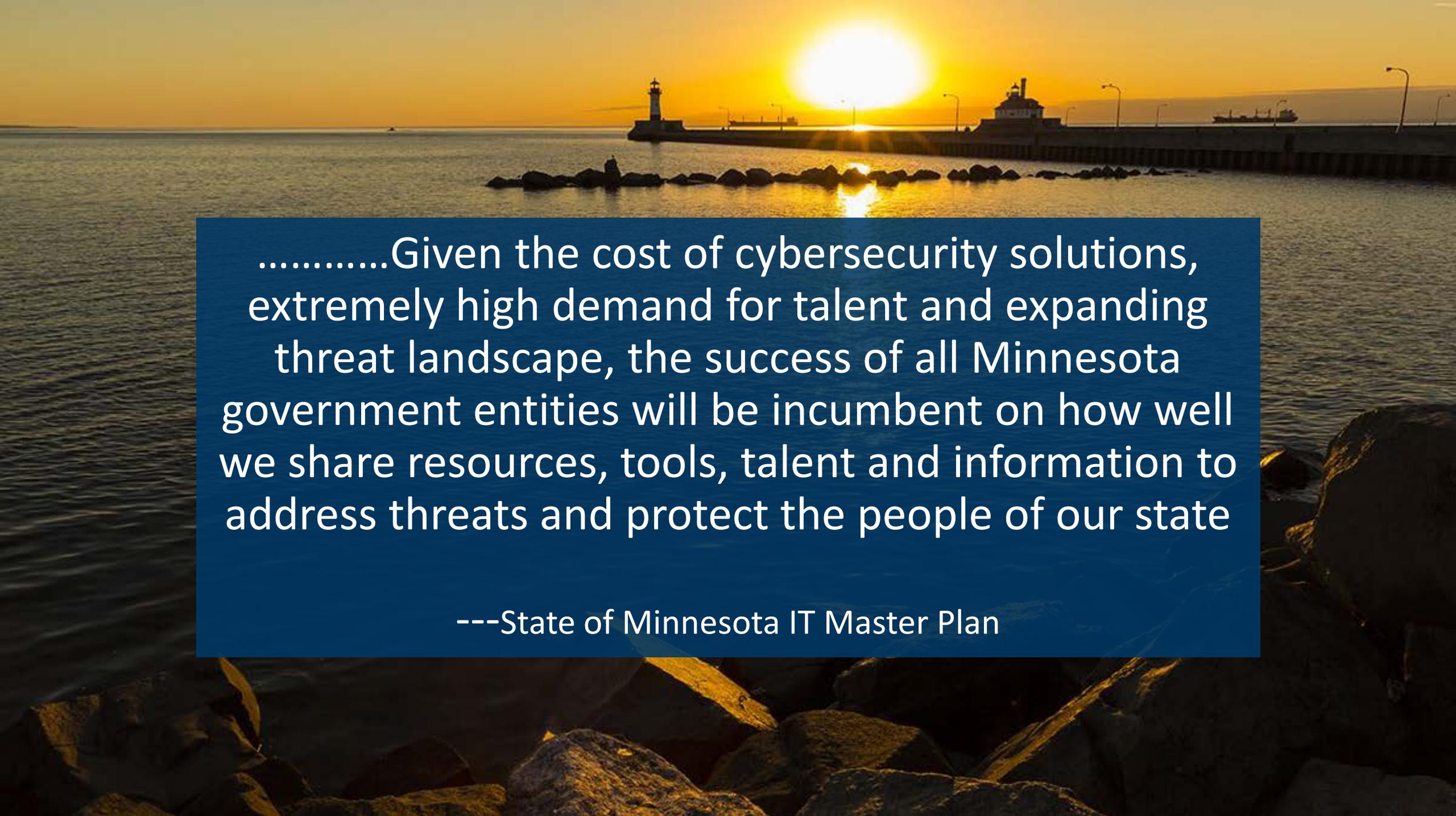
...........Given the cost of cybersecurity solutions, extremely high demand for talent and expanding threat landscape, the success of all Minnesota government entities will be incumbent on how well we share resources, tools, talent and information to address threats and protect the people of our state

---State of Minnesota IT Master Plan

Thank you!

Chris.buse@state.mn.us

@BuseTweet