Testimony for MN State Legislative Commission on Data Practices

Introduction:  COL Stef Horvath, MNARNG CIO

- CIO responsible for MNARNG Networks (unclassified and classified), Network services and Endpoint management connecting nearly 80 sites in MN supporting thousands of users.
- MNARNG network is an enclave of the DOD Information Network (DODIN)
  - Consolidated network – shared service model
  - Network Accreditation by Federal cybersecurity framework – NIST Risk Management Framework (ref: DOD Instruction 8510.01 Effective May 24, 2016)

Challenges to Defending the Cyber Domain:

1. Defense is never as fun as Offense
   - Information security is not as glamorous as applications or bandwidth speed
   - Adds to the difficulty in securing resources

2. Invisible Avenue of Approach hides this global security challenge
   - Difficult to describe risk, potential impact and ROI
   - Stats are difficult to capture (give meaning)

3. Securing the Cyber Domain is a task unprecedented in scale and velocity
   - “Boil the Ocean” requirement
   - Reliance on the compliance (“checklist”) mentality is false

4. Too much is reliant on too few
   - Numerous internet articles discuss the global shortage of cybersecurity experts
   - Cybersecurity is more than an IT issue
   - Environment favors the adversary – no cyber-deterrence

5. This is only the beginning
   - IOT, Smart Cities, Encryption, AI...

Advantages Gained by Cybersecurity Reform and Modernization Efforts:

1. Modernizing IT affords multiple advantages
   - Software Assurance is an emerging trend – software that is more secure by design
     - OWASP
Intuitive Digital Exchanges Between citizens and Gov or internal Gov processes are accelerated – improves the relationship and trust between citizens and Gov.

1. Example – Jennifer Pahlka – Coding a Better Government
3. DevOps – emerging trend in rapidly developed applications

Improved applications provide traceability, audit readiness, and ability to lock down access

1. Traceability – identify who did what on the transaction
2. Greater granularity in the permissions

(2) Meet Compliance on regulatory guidance – but thankfully much more than that

1. Compliance does not equal security (Numerous Internet articles)
2. Compliance focus is at the low end of emerging cybersecurity maturity models (Ref: https://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/)
3. Compliance as a cybersecurity strategy is today’s “Maginot line” (defensive wall easily circumvented by a determined adversary)

(3) Reducing the elements of Cyber Risk

1. Risk Defined as
2. MN.IT’s Cybersecurity strategy has always encompassed a multi-faceted approach that reduces both probability and Impact
   i. Introduces controls and processes that are preventive, detective, and limiting to reduce chance of successful attack or recover rapidly from an incident
3. Focus on Partnerships and building a cyber workforce is crucial and beneficial

Conclusion

1. Innumerable documents cite the increased risk in the cyber domain – Increase in likelihood (probability of occurrence) and impact of incident
2. Current global competition and conflict in the cyber domain – cyber domain is a global commons without laws and enforcement to protect countries, organizations and citizens
3. Investing in cybersecurity is an unfortunate but absolute necessity

Prepared by: COL Stef Horvath, CISSP, CRISC - MNARNG J6/CIO

Reviewed by: Don Kerr, Executive Director, MNARNG