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.
- Lead for the MNARNG Cyber Response Strategy (2010-2017)
- 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
    i. OWASP
    ii. Software Engineering – Security as a Process in the SDLC (Ref: https://www.sans.org/reading-room/whitepapers/securecode/software-engineering-security-process-sdlc-1846)

- o Intuitive Digital Exchanges Between citizens and Gov or internal Gov processes are accelerated – improves the relationship and trust between citizens and Gov.
  - i. Example – Jennifer Pahlka – Coding a Better Government
  - ii. Security and functionality do not have to be mutually exclusive - http://www.govtech.com/dc/Digital-Cities-Survey-2017.html
  - iii. DevOps – emerging trend in rapidly developed applications

- o Improved applications provide traceability, audit readiness, and ability to lock down access
  - i. Traceability – identify who did what on the transaction
  - ii. Greater granularity in the permissions
  - iii. Tamper proof – "The Next Wave of Cyberattacks Won't Steal Data – They'll Change It (Ref: http://www.defenseone.com/threats/2015/09/next-wave-cyberattacks-wont-steal-data-theyll-change-it/120701/)

(2) Meet Compliance on regulatory guidance – but thankfully much more than that
- o Compliance does not equal security (Numerous Internet articles)
- o Compliance focus is at the low end of emerging cybersecurity maturity models (Ref: https://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/)
- o 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
- o Risk Defined as
- o 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
- o 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