Metropolitan Washington Council of Governments

NCR EPC CYBER PANEL DISCUSSION QUESTIONS

September 14, 2016

1. How many of you truly know the risks of:
    a. Forwarding government email to a personal email account?
    b. Never changing a password, or changing one very infrequently (say, once a year)?
    c. Underfunding, or under-supporting, your IT security teams' ability to have security assessments conducted, to have exercises and training completed, to be able to partner with law enforcement and outside organizations for the purpose of sharing threats, best practices, and plans.

2. When was the last time a report on your agency's security risks came across your desk – for awareness or reporting? For instance, do you know your current security posture as it relates to industry best practices, such as the NIST Cybersecurity Framework or the Critical Security Controls?

3. Does your jurisdiction have a full-time employee whose tasking is Information Technology (IT) Chief Information Security Officers (CISO)?

4. What is the cost/spend basis of your current IT security program? For instance, do you account for:
    a. Percentage of IT annual budget dedicated to security (personnel, equipment, procedurals, and training)?
    b. Costs per constituent versus security value of a breach prevention (i.e., cost of breach per record lost)?
    c. Costs to train staff versus potential cost per 'click-hack' incident?

5. Is your jurisdiction or IT department funded for an annual Third Party IT Security risk assessment?

6. Does your agency have cyber insurance? Does it cover:
    a. Breach investigation, response, and mitigation (i.e., coverage for you and identity protection for citizens)?
    b. Disruption expenses – due to network denial-of-service, equipment compromise causing interruptions, ransom-events, etc.?
    c. Engineering and operational technologies, such as SCADA, process control, building automation (hacks)?

7. If you went to file a claim for "theft of information" with your cyber insurance provider, how exactly would you prove that the information has been stolen (i.e., copied) when

in-fact, since it's digital information, it likely still resides in your enterprise as 100% authentic information?

8. What is the number one security asset your agency uses to prevent, detect, or mitigation cyber attacks:
    a. Two-factor authentication and role-based access provisioning?
    b. A firewall with IDS/IPS?
    c. Anti-virus with a SEIM system?
    d. A big "P" security plan and set of operations procedures, that includes external partnerships for threat intelligence/identification, information sharing, and incident coordination?

9. Does your jurisdiction Procurement Office and/or IT security team utilize contract language that requires vendors and contractors to confirm the use of Cyber Security Best Practices with regard to storing or handling government sensitive data? Secondarily:
    a. Does this apply to Cloud service providers?
    b. Does this apply to security management notifications, such as sharing vulnerability and threat information, breaches that affect their operations/support to your agency?

10. Has your government or organization eliminated the use of Social Security Numbers as employee tracking numbers?

11. Do all employees receive annual IT Security training (online or classroom training)?

12. Does your (new and continuing) employee awareness training program not only account for IT Security topics, but how you measure success of your training efforts (i.e., rates of occurrence and measures of success)?

13. Regardless of your IT security program(s) centralization or de-centralization of activities, personnel, and authority… how do you put together a common operating picture of cyber threats, attacks, and events? How have you built or asked your cyber security leaders to build this, to include:
    a. Law enforcement agencies and operations
    b. School districts
    c. Operational technology

14. Does your government or organization maintain an internal web presence where employees can go to learn about Cyber Security Best Practices, Threats, Risk, etc.?

15. Is your jurisdiction's IT department also responsible for School Systems or are they separate entities?