Washington Metropolitan Area Transit Authority

Board Action/Information Summary

○ Action ◉ Information	MEAD Number: 201237	Resolution: ○ Yes ◉ No

TITLE:

WMATA Cybersecurity Briefing

PRESENTATION SUMMARY:

Staff will provide a general overview of WMATA's Cybersecurity program. PowerPoint presentation attached.

PURPOSE:

- Provide an overview of Metro's information technology security program
- Discuss certain WMATA information technology security imperatives
- Explain how those imperatives are being addressed by Metro Office of Information Technology

DESCRIPTION:

Metro's Office of Information Technology is chartered with the responsibility of protecting the confidentiality, integrity and availability of the Authority's electronic information. While certain details of the security program will not be included in the public presentation, this summary provides a general overview of the program.

Key Highlights:

- Metro uses a range of strategies to ensure that electronic information within it's custody is protected, including risk management, employee training, documentation protocols and various technologies.
- Metro complies with a range of regulation and industry best practices in governing it's Information Technology security program.
- The security program is designed to protect the confidentiality, integrity and availability of electronic information for internal and external customers, with special emphasis on safety sensitive systems, credit/debit transaction and customer information.

Background and History:

<u>Introduction:</u>
WMATA's Office of Information Technology (OIT) is chartered with the responsibility of protecting the electronic information managed within Metro's IT systems. Within OIT, there is an established Metro Information Technology Security (MITS) organization that conducts the majority of activities associated with this responsibility, including the

development and maintenance of electronic security policy and process. MITS performs routine electronic security operational tasks and manages established electronic security systems on an ongoing basis. From a security perspective, the MITS organization is also is actively engaged in the development and deployment of new electronic systems and applications that are needed by the WMATA community. Information Technology security is an evolving responsibility and WMATA OIT routinely evaluates the security landscape and adapts it's electronic security practices to accommodate changes in the environment.

Discussion:

IT Security Landscape

Metro's Office of Information Technology has an established Cybersecurity program to address electronic information security challenges. The challenges are typical of those faced by corporations and large public sector agencies that perform financial transactions; collect, store and manage personally identifiable information / intellectual property and have a large employee/customer base that is increasingly more dependent upon evolving technology.

Historically, for many years, businesses like WMATA operated with closed computing and network models, with clearly defined boundaries between what was within or outside the corporate domain. This is no longer the case, driven by beneficial technological advances that put more information into the hands of employees and consumers, reducing costs and improving organizational efficiency. However, this continually evolving computing model also puts strain on the traditional definition of the enterprise and data security, with corresponding evolving security challenges.

IT Security Governance

There are many evolving regulations that govern how electronic information is managed at WMATA and other private/public sector entities. Within the realm of electronic information management, personal data has become a huge area of concern, with strict new laws regarding the sharing and dissemination of medical history (HIPAA), misinformation in credit reports (Fair Credit Reporting Act), and many others.

The rules vary by state and there is a need to balance privacy with the need to gather / retain information that can help improve business efficiency, address security breaches or fraud, all while complying with associated legislation.

WMATA is also a Level 1 Credit/Debit service provider, processing over 6M transactions per year, which requires an independent third party audit for Payment Card Industry Compliance (PCI-DSS). This is a requirement of the Payment Card industry for merchants to process credit cards and reduce fraudulent charges. The Payment Card Industry standard is evolving with the threats, both with respect to technology and institutional process.

What Do We Protect?

WMATA's cybersecurity program generally covers three basic areas of responsibility with respect to electronic information management:

- **Confidentiality** – Confidential information must only be accessed, used, copied or disclosed by users who have been giving authorization.
- **Integrity** – For data to retain its integrity, it cannot be created, changed or deleted without proper authorization.
- **Availability** – Requires that the data or systems that provide the data are operational at all times and can provide the correct information when requested.

WMATA uses various techniques to protect the integrity of the electronic information and underlying IT systems within the Authority, centered on the management of people, process and technology.

People:

Business Management and Risk Mitigation

WMATA makes business management decisions about how to provision an IT service with Information Security in mind. There are typically many ways to deploy a particular service, with varying risk models. The most conservative techniques generally offer the least flexibility with respect to information sharing across organizational boundaries, with the most conservative being physical and virtual isolation. For safety sensitive systems and fare management systems, conservative models are typically employed. However, cybersecurity risk needs to be actively managed within the context of being secure without excessively reducing access to services that are valuable to internal and external customers.

Training and Awareness

WMATA trains employees in how to properly manage information. The Security Awareness and Learning Program is initiated at New Employee Orientation before new employees are provided with access to their computers and employees recertify every 12 months.

Policies and Procedures:

Policies:

IT continually reviews and updates the WMATA Information Technology policies to accommodate the evolving IT security landscape. In addition to an annual review of security policies, IT has embarked on an Enterprise Quality Management program to more closely harmonize security policy with other IT policies and procedures.

Procedures

An annual review and update to security processes and procedures is performed by OIT. Additionally, an annual Payment Card Industry Data Security Standard (PCI-DSS) audit is conducted by a third party Auditor. Many best practices are embedded in the PCI requirements, so there are benefits to this audit beyond credit/debit transaction. There are also routine IT conformance audits performed by the Inspector General, FTA, and financial auditors. IT has established an internal quality group, which also plans on performing routine process audits in conjunction with the Quality Management Plan.

Technology:

Defense in Depth

In addition to People, Process and Procedure, WMATA has and will continue to invest significantly in technology to protect Metro's electronic information assets. These industry standard technologies provide multiple rings of defensive layers, including Firewalls, Intrusion Detection Systems, Logging and Monitoring systems, Network Access Control and Identity Management.

- Firewalls, - Next Generation Palo Alto Firewalls
- Intrusion Detection Systems – Active devices to monitor network traffic and alert security personnel to suspicious activity
- Logging and Monitoring – Customizing the logging activities to better correlate events to give a better view of what is happening amongst the systems and devices collectively
- NAC – Implementing Network Access Control to prevent non-authorized devices from connecting to the WMATA networks
- Identity Management – Continuing the phases of Identity Management to better accommodate employee on and off boarding of their access to WMATA systems and applications

FUNDING IMPACT:

There is no impact on funding - informational item only	
Project Manager:	Kevin Borek
Project Department/Office:	OIT

TIMELINE:

Previous Actions	Not Applicable
Anticipated actions after presentation	

RECOMMENDATION:

Information Item.

WMATA Cybersecurity

Safety & Security Committee

January 22, 2014

IT Security Challenges

- Securing financial transaction management
- Protecting business systems and data
- An ever-increasing Corporate dependence upon evolving technology

Evolving Principles, Regulations and Best Practices

- HIPAA - Health Insurance Portability and Accountability Act
- PII - Personal Identifiable Information
- PCI-DSS – Payment Card Industry Data Security Standard

What Do We Protect?

Confidentiality

- ✓ Protecting Information in our custody

Integrity

- ✓ Assuring that Information is both Authoritative and Accurate

Availability

- ✓ Ensuring that the systems are capable of delivering information on-demand to internal and external customers

How Do We Protect Information?

People

✓Business Management and Risk Mitigation

✓Training and Awareness

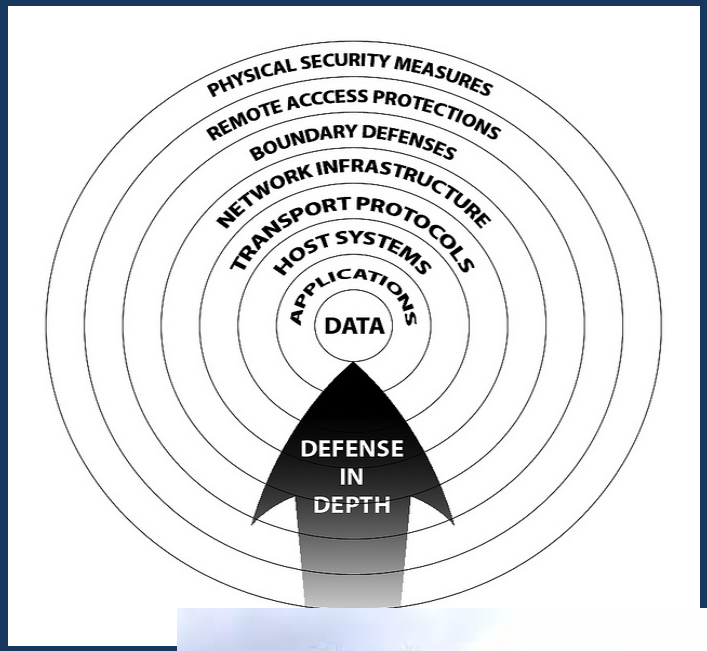
Processes

✓Policies and Procedures – Continuous Improvement of Security Policies, Processes and Procedures

✓Audits and Compliance

Technology

✓Defense in Depth – Multiple rings of defensive layers



Questions?