ITS Strategic Roadmap – FY20 Planning

Network Security

Author: *James Zaletel*
Date last updated: *December 27, 2018*

Background

The security of institutional computer networks and information held within them is a front-page topic in the news on a regular basis. Whereas the Information Security Management program established by Mayoral Executive Order is focused on policy, risk, and awareness, the network security program provides operationalized technical services to all Metro departments and agencies and strives to ensure the confidentiality, integrity and availability of Metro's IT resources. This is accomplished through the use of many centralized tools that provide technical solutions for policy controls.

These services include, but are not limited to:

- Maintaining security at the network perimeter
- Protecting Metro assets from malware both on and off-network
- Monitoring the Metro network for any security related issues
- Developing security solutions around mobile devices
- Responding to incidents or events
- Proactively scanning the Metro network for security issues and working with the various stakeholders to correct those issues

Key stakeholders are all of Metro departments and agencies who use Metro's wired and wireless network infrastructure, including external entities that may work with those departments and agencies.

Current Strategic Drivers

1. **Customer Demand: Cloud-based Services** (Game-changing) – Increased customer demand for cloud computing and cloud-based services. Departments' use of SaaS applications from third-party providers requires more scalable security monitoring capability. This demand, coupled with the increasing use of mobile solutions, result in a less "perimeter" focused security posture and a more "data centric" security posture.
2. **Industry Trend: Smart Cities and "The Internet of Things"** 🟦🟨🟩 (Game-changing) – More everyday objects have network connectivity, allowing them to send and receive data. Most smart city initiatives are dependent on IoT. Security is often an afterthought for these devices so their impact is not known.
3. **Customer Demand: Secure Government Systems** (High) – Proliferation of mobile devices, rise of hacktivism, reliance on any time connectivity to Metro network, etc. has increased the need to ensure the security of the Metro network. The complexities of digital business combined with an emerging "hacker industry," significantly increase the threat surface for Metro. Relying on perimeter defense and rule-based security is inadequate, especially as organizations exploit more cloud based services.

4. **Industry Trend: Assume Breach** (High) – "Assuming breach" is a strategic shift from the focus of a one-side purely preventative strategy to include more emphasis on breach detection, incident response, and effective recovery when a breach does occur. In the current threat landscape, a prevention-only focus is not enough to address determined and persistent adversaries. Security programs must be assessed and security controls, such as advanced monitoring and detection, need to be implemented to stop the intruders before they can export any critical data.
5. **Customer Demand: Diverse Communications Technology** (High) – Increased customer requirements to support different communication technologies where the medium is outside of Metro control, such as text messaging (Next-gen 911), wireless (desktop-based and mesh) and cellular (ambulances, PD cars). Many of these technologies are for public safety, which requires it to be robust and secure.
6. **Customer Desire: Mobile Solutions** ▥ (High) – Departments are embracing “mobility” (access to everything, all the time, from any device, from anywhere) as a way to meet their business goals. This demand, coupled with the increasing use of cloud based solutions, result in a less “perimeter” focused security posture and a more “data centric” security posture.
7. **Industry Trend: Continued Integration of Cyber and Physical Systems** (High) – “Smart Cities” solutions promise to deliver many valuable time- and resource-saving conveniences. Every device or sensor that connects to the network broadens the attack surface, creating a potential entry point for cybercriminals to hack to or hack through.
8. **Industry Trend: Deficit of Cyber Security Professionals** (High) – The need for cyber security professionals in both private and public section far outpaces the supply of these professionals. A lack of operational personnel drives the need to automate protections, including the ability to acquire near real-time alerts on anomalous or malicious activity with a high rate of accuracy.
9. **Industry Trend: Increased Targeting of Government** (High) – As Federal, State and Local Governments become more of a target for cybercriminals through an increased use of Ransomware and other attacks such as Crypto mining, as well as more specific threats, such as to election processes, it is important to look beyond internal resources and look to partner with third party security services in an effort to keep Metro secure.
10. **Industry Trend: Increased Use of Hacktivism (social outcry via cybercrime)** (High) – New “hacktivism” movement has set local government as a target. Use of IDS, IPS and better log management needed as additional protections against these external threats. The ability to Identify, Detect, Respond, Protect, and Recover before the proliferation of the attack manifests is critical to the protection of Metro assets.
11. **Regulatory: Compliance Obligations** (High) – Regulations and standards such as HIPAA/HITECH and PCI-DSS have started stating specific information security controls that must be addressed to realize appropriate levels of compliance with applicable laws, standards, and regulations.
12. **Customer Demand: Ease of Use** (Medium) – The increasing dependency on IT based solutions and the desire for faster access drives the need for security solutions that are seamless, easy to use and “invisible” to the customer.

On the Horizon Strategic Drivers

1. **Industry Trend: Artificial Intelligence and Machine Learning** (Game-changing) – Some of the greatest advancements in connected systems that drive business, center on artificial intelligence (AI) and machine learning (ML). The ability of computers to "learn" on their own as well as reason, self-correct and learn through activities such as machine vision and speech recognition will only complicate the way applications and systems are protected.
2. **Industry Trend: "The Device Mesh"** (High) – The device mesh brings together traditional desktop-centered computing, mobile computing, the IoT, smart city technology and cloud computing in a common, connected framework of endpoints and supporting services. This enables it to deliver digital experiences, and support digital and algorithmic business opportunities.

Short Term Goals (0-6 months) 7/1/19 – 12/31/19

#	Goal/Objective	Est. Start	Est. Duration
1	Research, evaluate and test Data Loss Prevention capabilities in our web filtering solution. This will allow the protection and control of Metro data wherever/whenever and be a step towards "data centric" security. Provide report to ELT on findings.	7/19	6 Months
2	Assess security implications of network connected devices ("internet of things") and work to develop standard security guidelines to be met for the use of such devices.	9/19	6 Months
3	Research, evaluate, purchase and deploy security information and event management (SIEM) technology that would: • Aggregate event data produced by security devices, network infrastructures, systems and applications • Combine event data with contextual information about users, assets, threats and vulnerabilities • Normalize data so that events, data and contextual information from disparate sources can be correlated and analyzed • Provide real-time correlation of events for security monitoring query and analytics for historical analysis and other support for incident investigation and compliance reporting. Provide report to ELT on findings. Capital funding will be required.	7/19	12 Months
4	Develop process for conducting workstation assessments using vulnerability management tool.	8/19	6 Months
5	Expand use of Mobile Device Management for all Office 365 connected devices and applications	7/19	12 Months

Medium Term Goals (6-18 months) 1/1/20 – 12/31/20

#	Goal/Objective	Est. Start	Est. Duration
1	Research and conduct an updated external intrusion detection/vulnerability assessment engagement. Provide report to ELT on findings. Capital funding may be required.	2/20	3 Months
2	Address any findings from the external intrusion detection/vulnerability assessment engagement. Capital funding may be required.	5/20	9 Months
3	Investigate additional monitoring and controls around the cloud environment, including Cloud Access Security Brokers (CASBs). Capital funding may be required.	1/20	6 Months

Long Term Goals (18-36 months) 1/1/21 – 6/30/22

#	Goal/Objective	Est. Start	Est. Duration
1	Continue to address any findings from the external intrusion detection/vulnerability assessment engagement. Capital funding may be required.	1/21	12 Months

Related Roadmaps

- Information Security Management
- Identity and Access Management
- System Lifecycle Management
- Field Services
- Wireless Network Infrastructure
- Radio Communications
- Network Infrastructure

Related Resources

- Executive order 034
- Connected Nashville
- Microsoft Cloud Platform Roadmap
- What is a CASB?
- CASB can help address gaps in cyber security