March 2017 Report on Cybersecurity

SCSI AGENDA: 03/02/2017
ITEM: d (3)

CITY OF
SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: SMART CITIES AND SERVICE IMPROVEMENTS COMMITTEE

FROM: Rob Lloyd

SUBJECT: REPORT ON CYBERSECURITY

DATE: February 21, 2017

Approved

Date 23 FEBRUARY 2017

RECOMMENDATION

Review and accept the report on Cybersecurity, including current progress, the Work Plan described, and immediate focus areas.

BACKGROUND

The use of technology permeates every level of the modern organization. For the City of San José, technology-based tools shape how individuals communicate and how departments process almost every transaction the City conducts with community members. These facts color the realization that software, networks, and computing devices have become intrinsic to the flow of local government. In many ways, every organization is now a technology organization and every employee is some level of technology worker. And the security of information and business processes connected to that environment impacts every San Jose resident, business, and visitor.

Cybersecurity has emerged as a dominant technology issue for the reasons described above. Past industry practices emphasized time-to-market and customer convenience over the security of products. This triggered the era of rampant data breaches, network-based attacks, intellectual property theft, and easily-hacked computers and software we see today. It will take years for most vendors to rebuild their products to attain a level of true security and resilience. Meanwhile, the exponential growth in the number of devices and amount of data organizations manage magnifies these vulnerabilities.

Residents, businesses, and governments face the repercussions every day. Media stories give regular accounts of today's pervasive cybersecurity problem: Credit and debit card data for over 90 million customers hacked at Target and Home Depot lost the retailers hundreds of millions of dollars in revenues and stock value. In late 2016, cybercriminals hacked a local municipal transit agency's fare system[1], costing it over $2 million per day. Weeks later, a police department lost

[1] Transit Hack: http://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked

eight years of electronic files and evidence[2] due to ransomware accidentally launched by an employee. A month after that, a county government's phones, computer systems, and part of its 9-1-1 go down due to a similar attack[3]. And in an egregious example, a community college system incurred over $26 million in costs after its records were breached[4], it failed to respond effectively, and the FBI notified it that its students' data were for sale on the dark web.

Due to severe resource constraints faced by the City of San José over the past decade, the organization has not managed to invest in the staffing, tools, and services matching its risk profile. The City is one of the largest municipalities in the nation, carries a $3.2 billion total budget, has prominence for its location at the heart of Silicon Valley, is home to critical infrastructure and companies that support the entire Internet economy, and has been the target of cyberattacks by political hacktivists.

Beginning in August 2016, the Information Technology Department (ITD) began the process of assessing the current state of the City's technology environment to respond to the organization's risk profile. Recent audit and compliance reviews validated the need for fast, concerted action in a number of areas. ITD completed a summary assessment using the National Institute of Standards and Technology (NIST) Cybersecurity Framework[5], identified gaps and compliance needs, and generated a work plan to address both near-term actions to resolve critical risks, as well as long-term requirements for protection, detection, response, and recovery. This report provides an organizational view into those activities to designate Cybersecurity as a top priority for the City of San José.

ANALYSIS

Cybersecurity encompasses every facet of an organization's operations— its communications, management of information and systems, adherence to laws and regulations, internal policies, contract terms, technical management of networks and business systems, and controls affecting all financial and information assets. Externally, the City's risks come from disparate groups of malicious actors ranging from hacktivists and individual cybercriminals, to criminal syndicates, to nation states. This combination of assets, vulnerabilities, and threats is exceptionally difficult to manage. Adding to the challenge, there is an exceptional shortage of qualified cybersecurity professionals able to build the types of risk management programs that effectively control risks we see in today's environments. Traditional audit-centric approaches are too slow. Network security and anti-malware tactics have proven ineffective.

This Information Technology Department built the City of San José's 2017 Cybersecurity Work Plan around the NIST Cybersecurity Framework for the reasons detailed, above. At a high level, we focus on five core "Functions":

[2] Police Ransomware: https://www.theregister.co.uk/2017/01/27/texas_cops_lose_evidence
[3] County Outage: http://www.portclintonnewsherald.com/story/news/local/2017/02/06/hackers-seizing-ohio
[4] College Breach: http://www.azcentral.com/story/news/local/phoenix/2014/12/17/costs-repair-massive
[5] NIST CF: https://www.nist.gov/document-3766

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

NIST Cybersecurity Framework outcomes are defined along 22 "Categories" that the organization must reach to achieve secure operations. In a summary assessment, the City has substantial work to achieve necessary rigor and capability in 21 of the 22 Categories. Work is not serial and significant efforts are required to meet and maintain capability levels. Most important, the framework lays a foundation that enables the City to take a comprehensive approach to both its current risk profile, as well as new risks as they evolve.

In response, to the assessment conducted, as well as known compliance needs, the Information Technology Department (ITD) set the following Cybersecurity Work Plan priorities with current statuses noted:

- **Cyberthreat Response Alliance** –
  - Join and support cybersecurity cooperatives for advanced security intel and feeds across public, private, non-profit, utilities, and academic sectors. Incorporate intel into the City's daily cybersecurity operations. (**Complete**)
  - Develop relationship with FBI, Homeland Security, emergency management, and state/local government partners to support joint response in the event of cyberdisasters. (**In-Progress**)
- **Compliance** –
  - Resolve findings and recommendations from external auditors and the City Auditor. (**In-Progress**)
  - Coordinate across all departments to complete Payment Card Industry Data Security Standard (PCI DSS) documentation, training, audit, and remediation work to adhere to all Control Objectives. (**In-Progress**)
  - Catalog and build action plans for adherence to Criminal Justice Information System, Health Insurance Portability and Accountability Act, Federal Information Security Management Act, Federal Information Security Management Act, and or other standards as required by City operations. (**Future**)

- **Capacity Building** –
  - Create a City Information Security Officer executive position with delegated authority to administer the City's span of security and compliance requirements. (**In-Progress**)
  - Create the ITD Cybersecurity Office with dedicated staff to execute this workplan and sustain continued security operations. (**In-Progress**)
  - Identify resources to invest in continuous citywide security training to reduce risks; advanced training for cybersecurity staff to augment protect, detect, and response capacities; security event management; and automation tools. (**In-Progress**)
  - Pursue cybersecurity insurance to administer financial risks associated with cybercrime against the City. (**In-Progress**)
  - Lead a Cybersecurity Assessment and Advanced Services RFP to create contractual access to an array of vendors providing required products and services before needs arise. Include Audits as a bi-annual required process. (**In-Progress**)
  - Incorporate information and systems security provisions into City contracts. Review and refresh these terms at least annually. (**In-Progress**)
- Identification, Protection, Detection, and Response –
  - Modernize the City's Information and Technology Policy, Cybersecurity Policy, and Mobile Devices Policy. Build standards separate from policies and require annual review to ensure policies and standards remain current. (**In-Progress**)
  - Automate block lists and alerts. Implement and maintain Data Loss Prevention in coordination with the City Attorney's Office and City Clerk's Office. (**In-Progress**)
  - Complete a full cybersecurity assessment. Resolve findings and recommendations. Achieve a letter of attestation affirming the City's secure technology environment from the security auditor. (**Future**)
  - Complete an Incident Response Plan for critical systems affecting life/safety, financials, and essential compliance systems. (**Future**)
  - Complete an identity management cleanup. Implement and routinize at least semi-annual department review of access permissions the City's network, enterprise applications, and departmental business systems. (**In-Progress**)
  - Pursue pattern-based cybersecurity solutions to replace limited IP address, malware signature, and simple password solutions. (**Future**)
  - Conduct an educational program for Cybersecurity Awareness Month each October. (**In-Progress**)
  - Implement cloud-based disaster recovery/business resumption with ITD Infrastructure and Operations Division staff. (**Future**)
  - Execute a cyberdisaster exercise with the Office of Emergency Services. (**Future**)
  - Update and maintain all security solutions to current version. Eliminate unused and/or ineffective tools. (**Future**)

EVALUATION AND FOLLOW-UP

Complete PCI Compliance documentation, training, audit, and remediation work to adhere to all Control Objectives with the Finance Department. Confirm with the City's bank and credit card processor in April 2017.

PUBLIC OUTREACH

This item will be posted on the City's website for the March 2, 2017, Smart Cities and Service Improvement Committee agenda.

COORDINATION

The memorandum has been coordinated with the City Manager's Budget Office, City Auditor's Office, Finance Department, Office of Emergency Services, and the Office of Civic Innovation and Digital Strategy.

COMMISSION RECOMMENDATION/INPUT

The memorandum does not require input from a board or commission.

FISCAL/POLICY ALIGNMENT

This action is consistent with the City's Fiscal Year 2016-2017 Operating Budget City Service Areas Delivery Framework for Performance Driven Government for Operational Services: 1) front line service delivery, 2) make improvements, and 3) Strategic Support's Effective Use of Technology.

COST SUMMARY/IMPLICATIONS

The City of San José's compliance needs and cybersecurity risk profile require significant catch-up investments. Specific investments and their costs will be detailed in the 2017-2018 Budget Process to ensure cybersecurity priorities are decided within the context of all City needs.

BUDGET REFERENCE

N/A

CEQA

Not a Project, File No. PP10-066 (a) Agreements and Contracts.

ROB LLOYD
Chief Information Officer

For questions, please contact Rob Lloyd, CIO at (408) 535-3500.