DEPARTMENT OF INFORMATION TECHNOLOGY

CITY AND COUNTY OF HONOLULU

650 SOUTH KING STREET, 5TH FLOOR
HONOLULU, HAWAII 96813
Phone: (808) 768-7684 Fax: (808) 527-6272 Internet: www.honolulu.gov

LATE

PETER B. CARLISLE
MAYOR

GORDON J. BRUCE
DIRECTOR & CIO

FOREST A. FRIZZELL
DEPUTY DIRECTOR

GORDON J. BRUCE, DIRECTOR AND CHIEF INFORMATION OFFICER
Department of Information Technology
City and County of Honolulu
before the
COMMITTEE ON ECONOMIC DEVELOPMENT AND TECHNOLOGY
and the
COMMITTEE ON EDUCATION
on
Tuesday, January 11, 2011
1:15 p.m.
State Capitol, Conference Room 0165

INFORMATIONAL BRIEFING

Chair Fukunaga, Vice Chair Wakai, and Members of the Committee on Economic Development and Technology; and Chair Tokuda, Vice Chair Kidani, and Members of the Committee on Education.

As Director of the Department of Information Technology for the City & County of Honolulu, thank you for the opportunity to discuss this most challenging subject. The protection of public data continues to escalate in complexity and in human and technical resource consumption.

How did we arrive at this?

A.

- 190,000 Rejected E-mails/day
- Malware attacks
- Hostile Network BOTS
- Internally introduced attacks
- Viruses
- Trackware/Adware

City & County of Honolulu policy states that "Information at the City will be processed in a secure information technology environment and all users share the responsibility for the security, integrity and confidentiality of the information."

As custodians of information, we follow the policies set by the data owner agency. We work with them to develop policies as related to information technology based on best practices as well as State and Federal laws regarding personal information. Basic things, which are also in our policy, are:

- Discouraging the storing or information on desktops, laptops, removable drives, CD's, etc., but if the data must be stored on one of those resources, then the data must be encrypted
- Requiring encryption when transmitting
- Not using production data on test/development systems
- Releasing information to only authorized people (need approval from the owner unless subpoenaed)

Some of our prevention methods include:

- Requiring strong passwords on user accounts, refreshed every three months
- Active scanning and patching of resources
- Requiring anti-virus on computers
- Firewalls and Intrusion Prevention Systems (IPS)
- Active monitoring of the network
- Encrypted backup of critical systems such as drivers' license, voter registration, and Enterprise Resource Planning
- Application scanning
- Ongoing audits

B. 2.790 Million Homeland Security (HLS) Grant Critical Infrastructure Protection

1. The goal of this investment was to secure and strengthen the City's computer network, segment network, install and implement network monitoring and detection equipment, and develop an effective cyber incident response team within the city to protect the City's critical network infrastructure and information systems.

2. A consultant was hired to assess the city's network, identify vulnerabilities, and provide recommendations. Equipment was purchased to implement the top priority vulnerabilities and conduct exercises to verify success of the measures.

- Assessment activities – identify and prioritize vulnerabilities, develop policies and procedures for network security and cyber attack responses.
- Implementation activities – purchased equipment to secure the network, monitor network, conduct network scans and assessments, patch management, and application security.

3. A final assessment was conducted in the 2010 grant performance period. Ongoing vigilance and constant monitoring is necessary to detect potential or actual threats and attacks. Early detection and isolation helps to mitigate problems and minimize down time and damage to the City's network and information.

4. Annual Review/Revision of Policies/Standards/Guidelines

5. Access Controls and Management System(ACAMS) – Physical Security - $4+ Million in Grants: Not to be under estimated is a major overhaul of our Physical Security was conducted. In this area alone the City & County of Honolulu has deployed an enterprise wide ACAMS – Physical Security using approximately $4+ Million in Federal Grants. We have issued over 5,000 government employee identification cards that meet Federal Standards and over the next months will be issuing an estimated 1,500 First Responder Credentials that meet Federal DHS PIV-I standards as documented in Homeland Security Presidential Directive 12. This system, can be expanded to include State agencies and other Counties at considerably less cost if they were to do this on their own.

C. Information Security Governance Plan in Development as Identified in Proposed Legislation

- Security Aligned with Agency Business Plans
- Ensure Confidentiality, Availability and Integrity
- COOP Plan Prioritize Critical Systems
- Infrastructure – Internal/External
- Security Requirements
- Policy and Procedures
- Ongoing Monitoring/Administration
- Ongoing Risk Assessment and Management

D. Consultant and Audit Findings Included

- Risk Assessment
- Vulnerability Assessment
- Network Assessment
- Incident Response Plan
- Incident Response Procedures
- Incident Management Matrix
- Incident Response Exercise Scenarios
- Security Hardening
- Network Security Project
- Data Security

E. Information Access

- Logon-ID/Password

    i. Logon-ID

    1. A separate logon-ID shall be issued to each individual who accesses the City's computer networks.

    2. The individual to whom the logon-ID is issued is responsible and accountable for the use of the logon-ID.

    3. Use of a logon-ID by an individual, other than the one to whom the logon-ID is issued, is considered a security violation.

    ii. Password

    1. A password must be kept secret and must not be divulged to another individual.

    2. Passwords should not be written down. If it is deemed that a password must be written down, it must not be placed where it could easily be seen or found and it must not be identified or labeled as a password.

    3. The primary ID password must be set to expire on a scheduled interval.

4. Do not automate the login process with any type of programming (such as script files and macros).

- Data Classification

  i. Data should be classified as it provides guidelines on the processing, storage, and transmission of information.

  ii. Non categorized data will be deemed confidential by default.

- Access to Confidential and Restricted Information

  i. Written authorization from the administrating department's director(s) restricts who and what level of access is granted to confidential and restricted information.

  Access should be granted based on a need to know basis to fulfill their functional responsibilities.

  ii. Production data files shall only be used for production applications and/or systems.

- Information Accessed by the Public

  i. City information accessed by the public must be declared public information.

- Electronic Mail (E-mail)

  i. E-mail shall be used in a lawful manner.

  ii. The City may disclose information to law enforcement or other third parties without the employee's consent. Approval of the DIT Director and Managing Director is required.

  iii. It is a violation for anyone, including system administrators and supervisors, to access, review, monitor, copy, or disclose the e-mail usage of others with no authorized City business purpose.

iv. Users must not use non-City e-mail accounts (such as Hotmail and Yahoo), or other external resources to conduct City business if their e-mail messages contain confidential information.

v. Users must encrypt (the process of converting readable text to unreadable text) messages that contain confidential information if it is sent to someone outside the City's computer networks.

- Anti-Virus Software Protection

i. All workstations, laptops and other portable computer devices, and servers attached to the City's computer networks must use the City's standard anti-virus software or other City-approved anti-virus software to detect and eradicate viruses.

ii. Virus definition files for the anti-virus software should be updated on a weekly basis; or more frequently, in the event of a known threat. Any virus definition automatic update feature should be enabled.

- Encryption (the process of converting readable text to unreadable text)

i. Users should use encryption for confidential information that will be stored in non-secured locations or transmitted over the internet.

ii. Where encryption is used, City approved standard algorithms and standard products must be used.

F. Logging Monitoring and Auditing

G. Incident Handling

CONCLUSION

The intent of the proposed legislation is good. It does not address how to enable the deployment of the necessary resources to pro-actively monitor, and defend against existing and new attacks. I for one do not want to increase the size of government, but if the outcome of this legislation results in the spending of dollars, then I believe that the creation of a single, independent security Administration entity be created perhaps under the Department of Commerce and Consumer Affeairs with representation from the State, University and Counties.

One of the roles would be to provide and administer state-wide programs that include both the State and Counties. In addition processes need be put in place to protect the Citizen further and assist them should their confidential data be compromised.

To be candid, I do not believe that we as government agencies can independently secure our networks, systems and data. This needs “high profile” active oversight with people dedicated and focused in the area of securing citizen data. The challenge is even greater with decentralized systems. This is one of the reasons that the City & County of Honolulu has taken a centralized approach to the management of Information Technology systems and resources.

Respectfully submitted,

Gordon J. Bruce
Director and Chief Information Officer