



Memorandum

TO: PUBLIC SAFETY, FINANCE AND
STRATEGIC SUPPORT COMMITTEE

FROM: Stephen R. Ferguson
Chief Information Officer

SUBJECT: CITYWIDE INFORMATION
SECURITY

DATE: November 4, 2009

Approved

Date

11/5/09

RECOMMENDATION

It is recommended that the Public Safety, Finance and Strategic Support Committee accept this report on Citywide Information Security.

BACKGROUND

On April 3, 2008, the City entered into an agreement with VeriSign for the purpose of performing an independent, 3rd party information security audit. The Information Technology Department (ITD), City Manager, City Attorney and individual departments worked very closely with VeriSign during the assessment period to address recognized and potential immediate risks to the security of City-managed systems and data, including personal and public safety information.

The Public Safety, Finance and Strategic Support Committee has been presented with regular status updates on immediate and long term actions as a result of the audit. The most recent report was approved by the Committee on May 21, 2009. This memorandum provides an update on Citywide Information Security and the current status of remediation efforts.

ANALYSIS

As noted in prior reports to Council, VeriSign made several recommendations for remediation and risk avoidance. Of paramount importance is the City's development of a sustainable and dedicated security program. Information security, when addressed at the City, is currently done so at the department, work group, or even the program level or in some cases not at all.

At the time of the audit, it was noted by VeriSign that the City's security activities had no single authority to govern security best practices. In addition, once programs or systems are implemented, oversight and attention to ongoing security is limited or non-existent. VeriSign recommended that the City add 3.5 FTE's dedicated to a sustainable Information Security Program. The number of dedicated (full time) information security staff is a major factor in, and can be traced directly to, the success or failure of an information security program. Included in

this recommendation is the identification of an executive level management position with a working title of Chief Information Security Officer (Program Strategist), a Senior Analyst to develop Citywide policy and security awareness training programs (Policy and Practice), and a Supervising Applications Analyst to conduct vulnerability assessments and address technical remediation and mitigation efforts (Risk Assessment and Compliancy).

To date, the City has assigned Chief Information Security Officer (CISO) duties to the Chief Information Officer and at the beginning of FY 2009-2010 hired a Supervising Applications Analyst to oversee the development of an on-going security governance model and audit program. The Supervising Applications Analyst has reviewed the audit findings in detail, and is currently working with the IT teams to heighten security awareness, as well as develop policy and practices for use in daily operations. As a part of this process, the Supervising Applications Analyst developed a gap analysis between the state of current operations and the recommendation made by VeriSign. The Supervising Applications Analyst is currently working with IT Management to prioritize, in some cases re-prioritize, workload of IT technical staff to address the gap and move the City's security posture to a more sustainable model wherever feasible given the current staffing levels.

VeriSign also noted in their recommendation that an organization the size of the City of San José should make an average annual investment of \$1.22 to \$2.93 million on information security. There currently exists no ongoing budget dedicated to information security; however, \$139,000 was rebudgeted from the 2008-09 IT non-personal base for use in 2009-10 to address the most immediate information security concerns. ITD is planning to use these funds to validate the gap analysis and perform further auditing.

Development of an information security policy (a draft framework is nearing completion), related employee training and compliancy tracking are some of the most crucial aspects of the Information Security Program. A Citywide security policy will apply to every employee and contractor of San José, and the City continues to find itself at risk without a comprehensive Citywide information security policy. Current City policies are generally geared solely toward acceptable use, rather than how to accomplish business objectives while considering information security.

Actions to Date

As previously reported to the committee, ITD initially developed the following work plan to assist in the remediation of immediate vulnerabilities and improve the baseline security posture of the City. The work plan was divided into three phases. A status update of the most important elements is provided below. Budget constraints and reducing staff have slowed down progress considerably and targeted completion dates have not been met in many instances.

Short Term Actions (July 1, 2008 – September 30, 2008)

Action	Status
City Manager – Appoint a CISO to direct remediation efforts	Appointed Steve Ferguson, CIO, as the new CISO.
CISO – Develop a work plan for vulnerabilities identified through the audit	Short term work plan for the most immediate threats at the time of the audit were completed by previous CISO.
ITD – Contract with VeriSign for remediation guidance	VeriSign has provided remediation guidance or implementation guidance on a number of City initiatives including the Airport shared use system and several in place and under development IT systems.
ITD – Contract with VeriSign for guidance in security policy development	The Security Framework Draft document is now complete and has been distributed to key stakeholders (i.e. City Attorney’s Office, Office of Employee Relations, Police Dept.) for final comment
CISO, ITD, Finance, CAO – Review 3 rd party contracts for security compliancy	New contracts are being reviewed for security compliance prior to execution.

Mid Term Actions (October 1, 2008 – June 30, 2009):

Action	Status
CISO – Direct ITD to reduce the organizational risk profile by reducing duplicative services	Limited resources prevent efforts toward consolidation. ITD is working with the City Manager’s Office on Citywide IT study to address duplicative technology functions and resources throughout the organization.
SAA – Develop a Citywide standards-based computing environment	This SAA position has been hired and a gap analysis is complete. Currently IT operations are under review to move the City’s security posture to a sustainable model.
Sr. Analyst – Identify opportunities to host commodity type applications within the cloud (SaaS) provided security concerns could be addressed more adequately in a hosted environment	There is currently no Sr. Analyst dedicated to a security program.
CISO – Develop a Citywide patch/change management methodology	The SAA is currently working with the IT technical teams to present a series of options to present to the CISO.
SAA and Sr. Analyst – Design security monitoring policies, procedures and practices	The framework for an information security policy has been released but little progress has been made since due to the erosion of staffing resources and the ramp up time required by the SAA to address the full scope of the audit.

Long Term Actions (July 1, 2009 - ongoing):

Action	Status
Sr. Analyst – Develop and implement a security awareness training program for Citywide staff	It is unlikely a training program will be developed without additional resources.
Sr. Analyst – Develop a Council-adopted security policy, with consideration of the City’s current information security policies	Current staff will make efforts toward developing a City security policy among competing operational priorities.
CISO – Develop a sustainable model for ongoing information security risk mitigation, including internal and external audits	This deliverable has been shifted to the Supervising Applications Analyst and operational teams with VeriSign acting in a trusted advisor role. It is anticipated the recommendations be made to the CISO in Q3 of the FY2009-2010 with implementation beginning in Q4.

CONCLUSION

Although efforts were made to address the most immediate information security risks at the time the audit was performed, the City’s exposure continues by not maintaining a proactive security program and ongoing budget to address remediation efforts. Remaining ITD staff have reprioritized projects and delayed the implementation of several new technologies in attempts to address the most critical issues. Since the time of the audit, the department has eliminated 12.5 FTEs, further reducing the staffing level to 75% of the number of IT FTEs in place prior to 2001-02. Despite reductions in staff, the growing demands for technology and requirements to ensure safety of financial and personally identifiable information of customers, as well as increased regulatory compliancy (e.g. PCI for credit card processing) continue to grow.

The department has made some progress by hiring a Supervising Applications Analyst, but this position alone will not be able to change the security posture of the City with implementation and operational staff continually eroding through position eliminations, demotions and position bumping as a result of the seniority system. While the SAA will assist the CISO in developing, maintaining and managing the technical aspects of a security governance program, this position represents less than 1/3 of the recommended minimum staffing and does not address the budgetary or policy/procedural aspects of the program. The City continues to see demands for a security program as new service delivery mechanisms such as SaaS and e-commerce (e.g. Happy Hollow Park and Zoo retail and ticketing) are on the forefront of many departments’ business models.

Recently, the integrated utility billing system (IBS) experienced an incident in which a limited amount of account information from one user became available to another user with a similar user name due to an interface problem with a 3rd party payment processor. Although VeriSign confirmed that no personally identifiable information had been exposed, the amount of time

involved implementing an incident response action plan, analysis of the issue(s) and subsequent remediation efforts were lengthened due to lack of staff resources and a governance model that moved items of such nature to resolution quickly and efficiently.

As noted in prior memos, information security cannot be addressed in a single point in time. Rather, it is an ongoing effort due to the dynamic nature of technology and sophistication of threats.

COORDINATION

This memorandum was coordinated with the City Attorney's Office.

Should you have any questions regarding this memo or any information security issues, please contact me at 535-3560.


OBC Stephen R. Ferguson
Chief Information Officer