



Memorandum

TO: PUBLIC SAFETY, FINANCE AND
STRATEGIC SUPPORT COMMITTEE

FROM: Stephen R. Ferguson
Chief Information Officer

SUBJECT: SEE BELOW

DATE: November 6, 2008

Approved

Deane Jutra

Date

11/7/08

SUBJECT: 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, 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. Due to the potential for security breach by the release of possible system vulnerabilities, periodic updates to Council have been provided at Closed Sessions.

This memorandum will provide the Public Safety, Finance and Strategic Support Committee with an overview of the information security audit, as well some of the immediate and long-term actions in progress or planned. Attached to this memorandum is a recent high-level "report card" from VeriSign for the Committee's review.

ANALYSIS

In addition to identifying real and potential information security risks for the City, 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.

San José is involved in a wide variety of security activities with both common and unique considerations. At the time of the audit, it was noted by VeriSign that these activities have no single authority to govern security best practices. In addition, once the programs or systems are implemented, oversight and attention to ongoing security is limited or non-existent. VeriSign recommends the following key criteria as part of a sustainable Information Security Program:

Staffing

According to the recommendations of VeriSign, surveys from the Information Security Forum (ISF) and the 2006 Computer Economics Staffing study, the number of information security staff worldwide averages approximately 0.5 FTE per 1000 of the total enterprise-wide staff. Using this benchmark against the City's enterprise staffing numbers (as of June, 2008) of 6,992, the number of full time information security staff at the City of San José should be 3.5. 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). With last month's departure of the interim Chief Information Security Officer (CISO) appointed by the City Manager in July 2008, there is no dedicated information security staff and the department is working with the City Manager's Office on an interim staffing plan.

Funding

A discussion of staffing levels cannot be taken seriously without taking into consideration the funding of an Information Security Program. Recent studies published by PriceWaterHouseCoopers and the Information Security Forum (ISF) indicate that most businesses worldwide spend an average of 3 to 5 percent of their IT budget on Information Security. Differences in cultures, how IT security is defined, overall threat levels and variances in implemented technologies argue for prudent interpretation of these average percentages. The case has been made for up to 12 percent of the IT budget to fund Information Security programs in IT services-based companies. Using the average benchmarks and the City's annual IT budget of \$24.5M (as of June, 2008), the City should be expected to spend an average of \$1.22 to \$2.93 million per year on information security in efforts to safeguard its data and related technologies. Considering the City's current lack of information security investment and deployment, VeriSign recommends that the annual budget be at the top end of this range and reviewed each year to evaluate the adequacy of investment.

Information Security Governance

Development of an information security policy, 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 finds 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

The Information Technology Department has developed the following work plan to assist in the remediation of vulnerabilities and improve the baseline security posture of the City. The workplan was divided into three phases, with some of the highest priority items indicated below:

Short Term Actions (July 1 – September 30):

- City Manager - Appoint a CISO to direct remediation efforts (Randall Murphy)
- CISO - Develop a work plan for vulnerabilities identified through the audit
- ITD - Contract with VeriSign for remediation guidance
- ITD - Contract with VeriSign for guidance in Security policy development
- CISO, ITD, Finance, CAO - Review 3rd Party contracts for security compliancy

Mid Term Actions (October 1 – June 30):

- CISO - Direct ITD to reduce the organizational risk profile by reducing duplicative services
- SAA -Develop a Citywide standards-based computing environment
- Sr. Analyst - Direct ITD to identify opportunities to host commodity type applications within the cloud (SaaS) provided security concerns could be addressed more adequately in a hosted environment
- CISO - Develop a Citywide patch/change management methodology
- SAA and Sr. Analyst - Design security monitoring policies, procedures and practices

Long Term Actions (July 1 - ongoing):

- Sr. Analyst - Develop and implement a security awareness training program for Citywide staff
- Sr. Analyst - Develop a Council-adopted City Security Policy, with consideration of the City's current Information Security Policies
- CISO - Develop a sustainable model for ongoing information security risk mitigation, including internal and external audits

A report from VeriSign addressing the City's response to the audit and further recommendations is attached for the Committee's review.

CONCLUSION

VeriSign has confirmed that the City finds itself at risk by the lack of an ongoing, dedicated Information Security Program. As recommended by VeriSign, the program should maintain an independent operating budget from those of the departments, so as to not create a conflict of interest between running essential operations and that of information security. While the City of San José is off to a good start with the short term actions and identifying efficiencies through the

consolidation of technology services, it is at best a reaction to the initial audit results and unsustainable in the mid and long term.

In order to achieve immediate required actions, existing staff has reprioritized current projects and delayed the implementation of several new technologies. Since the time of the audit, the IT Department has seen five vacancies (representing an approximately 12% reduction in staffing), stretching those resources even further. ITD is discussing Security governance and funding strategies with the City Manager's Office.

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 Vijay Sammeta, Deputy Director of Technical Infrastructure, at x53566.



Stephen R. Ferguson
Chief Information Officer



ATTACHMENT A

1. CITY OF SAN JOSE INFORMATION SECURITY – STATUS REPORT

1.1 Overall Status

	Program Development	Remediation Efforts
Percent Complete	<5%	<1%

1.2 Reporting Timeframe

Project Name: Security Program Development and Remediation

Project Date: JUL 01, 2008 through JUL 01, 2009

Reporting Period: NOV 06, 2008

1.3 Overview

VeriSign concluded a comprehensive security audit of citywide infrastructure, policies and operating procedures in the second quarter of 2008. VeriSign met with the CIO and Deputy Director of IT during the week of OCT 20 and NOV 06, 2008, to review project efforts and provide trusted advisor guidance for next steps. A strategic plan has been created by the interim CISO to address recommendations from the security audit.

Although the City has made some progress towards short term actions, a 12% reduction of IT operational staff has occurred since the audit was performed. Sufficient IT administrators are needed to make progress towards goals outlined by the CISO. The lack of a permanent CISO with adequate authority combined with a reduction of ITD staffing levels and permanent security personnel put some of the short term and all mid term and long term action items at risk of failure.

1.4 Short Term Action Review

- The city appointed an interim CISO in July to create a strategic plan and to address immediate security risks identified in the audit. The position is currently vacant and has not been made permanent. In addition, it does not have the authority required to oversee a citywide security program. VeriSign recommends immediate action be taken to appoint a permanent CISO with the authority to act on behalf of City Manager's office eliminating departmental boundaries in the area of information security.
- The city is working to develop a work plan for vulnerabilities identified through the audit. The city has made some progress with remediation of known and potential vulnerabilities. The vulnerability scans performed in the second quarter of this year provided a snapshot of issues at that time but do not provide for on-going risk mitigation. Regulatory bodies require these scans and remediation efforts to be performed on a quarterly basis. ITD does not have the resources required to implement an on-going vulnerability management program.





ATTACHMENT A

- The city has contracted with VeriSign to provide remediation and “trusted advisor” guidance as it relates to the audit findings. VeriSign has begun to meet with city staff and vendors to review security design, proposed solutions and provide recommendations for best practices moving forward.
- The city has contracted with VeriSign to provide security policy development, the foundation for a sustainable security program to be implemented citywide. Since dedicated security personnel including the Sr. Analyst position have not been appointed, no action has been taken on this critical first step.
- The city has made significant progress identifying contracts for services and support of critical systems and now requires certain contracts to be reviewed and approved by ITD and finance before purchase or renewal. Duplicative services and providers will be consolidated through this centralized control. For example, 4 individual departments previously contracted with a provider for the same service, combining these relationships into a single contract will reduce cost and infrastructure requirements..
- The city has begun a review of 3rd party contracts to validate compliancy to various regulatory requirements.

1.5 Mid Term and Long Term Actions

These actions are at risk of failure as key fundamentals, such funding and staffing, are not in place to create or maintain a comprehensive citywide security program.

- A permanent CISO has not been appointed resulting in limited efforts to reduce organizational risk and duplicative services across city departments.
- As outlined in the audit, VeriSign recommends creating a security group headed by the CISO to include a Sr. Analyst and Supervising Applications Analyst. As stated previously, these positions must have the authority to create and implement security across departmental boundaries. Public sector organizations of similar size would require at a minimum, 3.5 security personnel to meet requirements and achieve objectives.
- Implementing a formal citywide change management process will be a priority for the new CISO. A formal change management does not exist and is necessary to gain control of city resources and improve security citywide.
- Implementing a security monitoring program is at risk without adequate IT resources and security personnel and is dependent on future ITD and security projects still to be identified and mandated by some regulatory bodies.

1.6 Conclusion

The City of San Jose should be spending an average of \$1.22 to \$2.93 Million dollars a year on Information Security based on organizations of similar size. Considering the current level of information security investment and deployment within the City of San Jose, VeriSign recommends that the annual budget be at the top end of this range and reviewed each year to ensure that the level of investment is adequate. The numbers represent an approximate budget necessary to maintain an adequate security program, VeriSign is concerned these numbers do not take into account effort and funding required to bring existing operations to a secure level.

