



**Date:** June 20, 2014

**To:** Mayor Willie Charles Shaw, Vice Mayor Susan Chapman, Commissioner Suzanne Atwell, Commissioner Paul Caragiulo, and Commissioner Shannon Snyder

**From:** Pamela M. Nadalini, MBA, CMC, City Auditor and Clerk 

**Subject:** IT Department Risk Assessment Report from Reliaquest, LLC

---

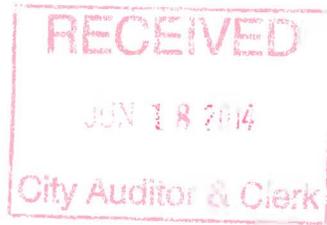
Attached for your information and review is a copy of the above-mentioned report, along with audit responses from the Information Technology Department. The department is continuously making efforts to improve service delivery, preserve the integrity of the City's data and records, and secure the information technology systems from internal and external vulnerabilities. While much work has been done to move the department forward, the most recent audit has identified additional opportunities for growth and improvement and to enhance the capabilities of the professional staff. It is my intent, as well as that of the IT Director and IT staff, to implement the auditor's recommendations to ensure a secure and effective computing environment for the City of Sarasota.

If you have any questions, please do not hesitate to contact me at (941) 954-4169.

Attachment(s):

IT Department Risk Assessment Report from Reliaquest, LLC

c: Philip Hurwitz, Director, Information Technology  
Willie Holland, Manager, Professional Business Services, Information Technology  
Charles Nardone, Database Manager, Information Technology  
File



**City of Sarasota**  
EXECUTIVE SUMMARY  
IT Department Risk Assessment

---

June 15, 2014

ReliaQuest, LLC

## **Table of Contents**

<b>ReliaQuest Overview</b> .....	<b>3</b>
<b>Overview</b> .....	<b>3</b>
<b>Executive Summary</b> .....	<b>5</b>
<b>Methodology and Findings</b> .....	<b>6</b>
<b>Conclusion</b> .....	<b>8</b>

## ReliaQuest Overview

ReliaQuest is a full cycle Information Security Professional Services and Solutions company. Our Information Security Solutions combine technology, services, ongoing support, and training for our customers to manage risk, meet compliance requirements, reduce costs, and other barriers to achieve security effectiveness and operational efficiency.

### Our Approach

We work as an extension of our customer's team. The ReliaQuest certified security engineers bring extensive knowledge and experience from the wide variety of both federal and commercial security environments that they support each month. This broad understanding of security industry best practices and cutting edge solutions is a powerful tool in helping to strengthen each environment and team that we support.

We create and optimize our customer's security posture allowing for continuous monitoring, continuous audit, and complete situational awareness. This is accomplished through advanced correlation, optimizing existing infrastructure and recommending new infrastructure when necessary.

Ultimately, ReliaQuest believes IT Security should not be driven by the fear of what could happen. Instead, we encourage our customers to be forward thinking and help to develop a roadmap that can enhance the organizations ability to operate and deliver products and services effectively while becoming and remaining secure. We promote a strong alignment between IT security and business objectives.

## Overview

---

The purpose of this risk assessment is to assess the IT Operations and Infrastructure for the City of Sarasota's Information Technology Department (ITD) and compile an accurate list of any threats and vulnerabilities, the likelihood of any occurrences, the impact of that occurrence, and factoring in any preexisting conditions and existing controls to determine the known risks and prioritization of remediation.

Compliance regulations are the primary concern for the assessment along with ensuring proactive IT security measures are in place with guidance from NIST, CIS, and other industry best practices and compliance regulations.

The scope of this assessment to determine the risks to the organization encompasses the following components discovered within the 6-week engagement. No actual exploitation of vulnerabilities will be done, but we will address the severity and likelihood of the potential vulnerability happening. The following IT assets will be included in the assessment:

- Physical locations of any IT equipment
- Any public-facing Internet service (see Appendix A for list of included public IP blocks and top level domains in scope).
- All internal networks, 10.20.X.X

- Interviews with staff members from the following IT teams to determine items such as inventory of hardware software used, incident response roles and capabilities, and monitoring/recovery capabilities of all applications and hardware for each team. IT Teams being interviewed include:
  - Server and Applications
  - Network and Infrastructure
  - Telecommunications
  - Software Development
  - Workstations, Helpdesk, and Mobile equipment
  - IT Security

This IT assessment reviewed the administrative and technical controls that have been utilized by the ITD to ensure the integrity, availability, and confidentiality of critical systems and its data. This report is the resulting deliverable and should be used by the ITD to prioritize its current IT security risks. Technical tools that are owned by the ITD were used to perform the technical assessment portion of this engagement.

It should be noted that ReliaQuest did not perform an assessment on the City of Sarasota Police Department's computing system.

## Executive Summary

---

Overall, the City of Sarasota's ITD is mostly reactive and does not seem to be aware and prepared to address the risks identified, in detail, below. The IT team seems to be comprised of individuals that are not working together to solve common IT security problems. This disconnect is evident in the lack of standardization within the department. When referring to the terms leadership, management and staff; this document focuses on personnel at the City of Sarasota ITD Director and below.

After reviewing the risks and vulnerabilities found during the engagement, the top 10 risks to the organization I believe are:

1. Lack of clear understanding of ITD personnel responsibilities.
2. IT Security Manager has never been formally appointed.
3. Minimal cross training on the use and configurations of existing applications.
4. NO alerting and/or correlation of security events.
5. Minimal effective patch management.
6. Limited standardization in department for both technical and administrative procedures.
7. Minimal configuration reviews.
8. Minimal understanding of why things fail or work on the computing system.
9. Lack of change management process.
10. No current and accurate network diagrams.

## Methodology and Findings

Over a period of 6 weeks, ReliaQuest assessed the City of Sarasota's IT Department by observing daily operational tasks, performing personnel interviews and performing technical network scans. The following findings and recommendations were derived by data collected from the assessment.

**Description:** Lack of clear understanding of ITD personnel responsibilities.

**Findings:** ITD staff does not have a clear understanding of their roles and responsibilities boundaries. There is great initiative in the department where staff members take on more tasks than they are supposed to. The desire to do more ultimately leads to them neglecting their base tasks. During interviews it was very clear that certain people take on too many hats; usually without the approval or knowledge of the IT Department leadership.

**Recommendation:** The leadership in ITD needs to re-focus the staff and groom the natural initiative within the department while still making sure their core responsibilities are taken care of. ITD leadership needs to re-enforce "approved and accepted" tasks during personnel reviews.

**Description:** IT Security Manager has never been formally appointed.

**Findings:** The IT Network Manager has assumed the role, but does not have any explicit authorization to perform IT Security Tasks. This causes the individual to be timid in running security scans that may disrupt service.

**Recommendation:** ITD leadership needs to explicitly appoint an IT Security Manager and include the ability to perform intrusive network scans as part of regular tasks.

**Description:** Minimal cross training on the use and configurations of existing applications.

**Findings:** Because there are no written Standard Operating procedures for common applications it is very difficult to provide a consistent level of service to ITD customers. ITD staff has been observed waiting for the resident Subject Matter Expert (SME) to verbally show them how to do something. There seems to be an underlying feeling from staff members that if they share the information in a written format then their "job security" will be diminished in some fashion.

**Recommendation:** Each SME needs to provide an SOP document on how to execute an application that they are responsible for. These documents need to be peer reviewed and stored on an accessed controlled location in MS Sharepoint.

**Description:** No alerting and/or correlation of security events.

**Findings:** It was determined that the ITD has 12 systems that are critical in providing a real-time IT Security posture view to ITD staff. The ITD only has a limited view of its IT Security posture because these 12 systems are not monitored on a daily basis. One example is the fact that ITD staff did not realize that over 250 machines went 48 hours without getting the latest Anti-Virus updates.

**Recommendation:** Implement and configure a Security Incident Event Manager (SIEM). Some examples are McAfee NITRO, HP ArcSight, and SNORT (currently being used by Sarasota County IT).

**Description:** Minimal effective patch management.

**Findings:** IT Security patches mitigate software vulnerabilities from potential exploits. The City of Sarasota has over 2500 missing Microsoft security patches across its workstations and server.

**Recommendation:** Personnel responsible for applying security patches attend vendor training on how to use the Microsoft and third party tools. Commit to a patch schedule.

**Description:** Limited standardization in department for both technical and administrative procedures.

**Findings:** One administrative example is the "30-60-90" planning document. Each member of the ITD used a different format. One technical example is the fact that some users in the ITD utilize MS Windows 8. This handicaps the ability to help the entire customer base that is running MS Windows 7. This non-standardization also causes delay with troubleshooting within the department. During the interviews, it was also determined that there were no written requirements to what makes a "critical or priority 1" help desk ticket. When staff was asked how they determine a "critical or priority 1", they often recited "experience" as the answer.

**Recommendation:** Standardize the department and limit the amount of variables that come out of it.

**Description:** Minimal configuration reviews.

**Findings:** One example is the CISCO ASA Firewall rules. The rules for the City Hall Firewall differ from the ones on the City of Sarasota Police Department. This is an issue because the Police Department CISCO ASA is the backup for City Hall and vice versa.

**Recommendation:** Review system configurations on a regular basis. Track changes if any are made and apply across the board to all related devices.

**Description:** Minimal understanding of why things fail or work on the computing system.

**Findings:** ITD pushed Microsoft configuration changes via Group Policy (GP). These changes went to machines that are part of Microsoft Active Directory (AD). Some machines receive the configuration changes and some did not. ITD staff members cannot explain the discrepancy.

**Recommendation:** Need to share knowledge with all members of the department. There is too many guessing going on that leads to inefficient informal meetings to speculate on what the issue maybe. In the specific case pushing GP via AD, I would recommend ITD engage with Microsoft to perform an AD health check.

**Description:** Minimal change management.

**Findings:** No process in place to review and approve proposed IT changes. Managers have deployed changes without any buy-in from data owners or other IT staff.

**Recommendation:** Define what constitutes a low, medium and major change. Require that all changes go through a change management process. Require that all changes have at least sign-off from the data owner, and two ITD managers. Recommend that ALL major changes have explicit approval of IT Director.

**Description:** No current and accurate network diagrams.

**Findings:** During the engagement, although I asked multiple times for a network diagram of the City of Sarasota's computing systems I never received a one. ITD staff members did not seem to know the status (existence or version) of a network

diagram. This severely handicaps the department's ability to troubleshoot, recover from incident or have a sound plan for upgrading old infrastructure. The lack of a basic network infrastructure diagram supports the first finding on this list. Staff members take on more tasks, but forget about their core deliverables.

**Recommendation:** Create and continuously update a network infrastructure diagram.

## Conclusion

---

The City of Sarasota's IT Department has personnel and technology challenges that it must overcome in order to provide secure IT services to its users. During the engagement it was noted that there has been five (5) different IT Directors within the past nine (9) years. The department needs a period of stable leadership. Furthermore, senior leadership and the IT Director need to evaluate the personnel currently in the department.

The City of Sarasota has purchased state of the art applications and software; however, most of these applications have not been fully implemented. IT Department must make a commitment to finish existing projects and fully deploy purchased software suites.

The City of Sarasota's IT Department needs to adopt procedures that allow its staff to be more knowledgeable and efficient in the existing technologies they have.

#	Subject	Recommendation	Priority	Management Response	Expected Completion Date
<b>2014 03-06 ReliaQuest Risk Assessment</b>					
1	Lack of clear understanding of ITD personnel responsibilities.	The leadership in ITD needs to re-focus the staff and groom the natural initiative within the department while still making sure their core responsibilities are taken care of. ITD leadership needs to re-enforce "approved and accepted" tasks during personnel reviews.	Medium	With the shortage of personnel, particularly with a critical position open, there is definitely an expansion of responsibilities beyond the standard job descriptions. Managers will continue to ensure that critical tasks are prioritized appropriately and roles are understood.	12/31/2014
2	IT Security Manager has never been formally appointed.	ITD leadership needs to explicitly appoint an IT Security Manager and include the ability to perform intrusive network scans as part of regular tasks.	High	The resignation of the Manager ICS leaves a hole in the security management structure. The replacement manager will be tasked with the Security Officer responsibilities. In the interim, the security responsibilities have been distributed to various staff members based on areas of expertise with ultimate responsibility resting with the Director.	12/31/2014
3	Minimal cross training on the use and configurations of existing applications.	Each SME needs to provide an SOP document on how to execute an application that they are responsible for. These documents need to be peer reviewed and stored on an accessed controlled location in MS SharePoint. ReliaQuest has created a "NESSUS SCANNING SOP" document that is on the CD. ITD can use this document as a template for future documents.	Medium	Documentation is critical to day-to-day management as well as continuity of operations. We will review the status of our application documentation (quite a bit of which does exist) and identify holes. Every new project should include documentation as part of the project plan that must be completed before sign off.	12/31/2014
4	NO alerting and/or correlation of security events	Implement and configure a Security Incident Event Manager (SIEM). Some examples are McAfee NITRO, HP ArcSight, and SNORT (currently being used by Sarasota County IT).	Medium	A SIEM would provide an additional and extremely beneficial level of protection. Looking into the possibility of a hosted model because of the significant expertise and personnel requirements to both set it up and monitor it to the level that would make it beneficial.	12/31/2014
5	Minimal effective patch management.	Personnel responsible for applying security patches attend vendor training on how to use the Microsoft and third party tools. Commit to a patch schedule.	High	IT is pushing out patches to all workstations and then validating using Nessus. The procedure has a primary subject matter expert, the process has been shared with two other IT staff, and documentation is in progress. Agreed that additional training is a strong need. We are identifying the appropriate class. A schedule is being developed to match the server patching schedule, based around MS Patch Tuesday dates.	12/31/2014
6	Limited standardization in department for both technical and administrative procedures.	Standardize the department and limit the amount of variables that come out of it.	Medium	Establish written processes and procedures for common tasks. As well, establish a clear definition of what defines a critical priority versus high etc. Utilize templates for documents to create a standard format.	12/31/2014

#	Subject	Recommendation	Priority	Management Response	Expected Completion Date
7	Minimal configuration reviews.	Review system configurations on a regular basis. Track changes if any are made and apply across the board to all related devices	High	All device configurations need to be put under configuration management. As well, we will establish scheduled reviews of configuration security levels.	12/31/2014
8	Minimal understanding of why things fail or work on the computing system.	Need to share knowledge with all members of the department. There is too many guessing going on that leads to inefficient informal meetings to speculate on what the issue maybe. In the specific case pushing GP via AD, I would recommend ITD engage with Microsoft to perform an AD health check.	Medium	There has been a big push to ensure that knowledge is being shared, balanced out by the breadth of knowledge and applications that are dealt with on a daily basis. This, along with other items, points to the need for a centralized documentation management.	12/31/2014
9	Minimal change management.	Define what constitutes a low, medium and major change. Require that all changes go through a change management process. Require that all changes have at least sign-off from the data owner, and two ITD managers. Recommend that ALL major changes have explicit approval of IT Director.	Medium	We need to adopt a change management framework and formalize the workflow.	12/31/2014
10	No current and accurate network diagrams.	Create and continuously update a network infrastructure diagram.	High	We are currently reviewing what documentation exists and creating a schedule to update. Documentation updates are a necessary part of any project.	12/31/2014