Inquiry into

The February 2005 Network Computer Virus

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

Sam M. McCall, CPA, CGFM, CIA, CGAP
City Auditor

Report # 0523 *June 3, 2005*

Summary

The purpose of this report is to provide management with an independent assessment on how the City was infected with the virus and how the virus was removed from the network, the impacts of the virus on City operations, and the lessons learned from this experience. We provided this information by answering five specific questions identified in the scope, objectives, and methodology section below.

On February 14, 2005, the City noted that its computer network was not functioning properly. What was first believed to be a network hardware malfunction, was subsequently determined to be a computer virus that had infected the City network. Once Information Systems Services (ISS) determined that a virus infection had occurred, they began the process of eliminating the virus from all the computers and servers on the City's network by deleting infected files, updating virus signatures, and installing critical security updates.

The infection and subsequent process to eradicate the virus impacted City operations in terms of direct costs and overtime expended and diminished customer service due to inaccessibility of network resources. In addition, we estimated lost employee productivity at a value of $343,000.

Neither ISS nor we were able to determine exactly how or when the network first became infected with the virus, but there is evidence to support that the virus infection occurred prior to February 14, 2005.

While we don't believe that the initial virus infection could have been prevented, we do believe that the spread of this virus across the network would not have occurred if (1) the available operating system updates had been installed and (2) ongoing efforts to segment the City network had been completed.

ISS indicated that they did not have the needed resources (staff or hardware) to adequately test the operating system updates, and therefore chose not to install them to avoid the possibility that the updates would cause software conflicts and disrupt critical City applications. The result was that the City's network was not adequately protected against the virus infection.

After the City's computer network was restored, ISS reviewed events to date and actions taken. They identified the following issues that needed to be addressed as a result of this infection. Those issues include: the number and expertise of ISS staff; communication between ISS and other City departments; network segmentation; operating system updates; automated virus scanning; computer security training for users and ISS staff; and business continuity planning (i.e., plans for alternative means of conducting business when the City network and applications are not available).

Based on our observations, a significant amount of effort and concern was exhibited by all involved City staff to address the issues once identified.

Scope, Objectives, and Methodology

The scope of our work included a review of activities performed by Information System Services (ISS) during the period February 14, 2005, through March 31, 2005, and other City departments during the period February 14-25, 2005, to address the virus infection.

For this Inquiry, our objective was to answer five (5) specific questions.

1. **How was the virus detected, identified, and eradicated?**
2. **What were the impacts of the virus to the City (i.e., financial, customer service, data integrity)?**
3. **How was the City infected with the virus?**
4. **Was the infection preventable?**
5. **What are the lessons learned from this experience?**

While answering these five questions, we will also further explain the virus infection and provide recommendations as applicable.

The methodology we followed to answer these questions included: attended ISS status meetings; interviewed key ISS and user departmental staff; observed ISS virus eradication activities; reviewed related virus and security documentation; examined payroll information; and calculated estimated lost productivity.

Our procedures were conducted in accordance with Generally Accepted Government Auditing Standards and Standards for the Professional Practice of Internal Auditing, as appropriate.

Background

The City's network consists of approximately 2400 computers, 56 servers, other network infrastructure equipment (i.e., switches, routers, and hubs), and mobile computing devices (i.e., laptops, personal digital assistants). The network is maintained by Distributed Network Services, a section within the City's Information Systems Services (ISS) Department. This section consists of 21 employees whose duties include: maintaining network infrastructure, servers, and personal computers (PCs); and operating a user help desk.

Computer viruses, in general terms, are computer programs that: (1) exploit weaknesses in computer software in order to perform malicious activities on computers; and (2) can spread to other computers. Some viruses can only be spread by human actions (e.g., opening an e-mail containing the virus or opening a computer document containing the virus), while other viruses can be spread without human assistance (e.g., the computer coding within the virus directs the virus to replicate and spread automatically).

The City was infected by a type of virus that can replicate without human assistance, referred to as a "worm". Worms can infect entire networks very quickly. The negative impact in this particular instance was that the virus "flooded" the City's network with so much computer activity that users were not able to access the network. In essence, the computer lines were too busy for users to conduct their normal business activities.

The City appeared to have first been infected with the "Win32.Agobot" virus, which is one of hundreds of variants of the "Agobot" virus strain.[1] Internet virus sites note that this virus source code is reported to have been widely distributed to various hacker groups, with each making modifications of its own (hence the hundreds of variants). However, the core functionality of the virus has remained consistent.

The Agobot strain that infected the City copied itself to the network's Microsoft Windows® operating system directory and added commands to run the virus program when users started their computers. Agobot was able to: (1) scan the network looking for other computers to infect; (2) initiate a connection to specific Internet Relay Chat (IRC) web sites; and (3) disable the anti-virus software on computers. It is possible that

[1] Computer Associates International, Inc., Support website (http://www3.ca.com/securityadvisor/)

once connected to an IRC, a hacker could connect to the infected computer and perform multiple functions, including:

- find and change administrative passwords;
- launch “denial of service” attacks;
- retrieve detailed system information;
- download and execute files from Internet sites (including other viruses);
- start and stop processes (including security-related processes);
- execute local files;
- access or manipulate data; and
- modify host files to disable or redirect antivirus software scanning and prevent updating.

Additionally, because the anti-virus software had been disabled, some computers were found to be infected with as many as 200 different viruses as well as numerous other malicious programs (i.e., spy-ware, pop-ups, etc).

The City has a three-part process in place for preventing virus infections. First, firewalls monitor incoming traffic, and block traffic exhibiting characteristics of known viruses. Second, anti-virus software is used to monitor e-mail and block those e-mails that contain known viruses. Third, anti-virus software is installed on individual PCs to scan files as they are opened to identify and remove known viruses. ISS management estimates that there were over 35,000 viruses blocked each week.

Even with those preventative measures in place, infections can and do take place. Infections should be considered a risk of doing business in a networked computing environment that cannot be entirely eliminated. Reasons include:

- new strains of viruses are developed everyday; therefore, antivirus software does not recognize or stop the virus; and
- users make mistakes such as:
  - transferring infected files from one computer to another on floppy disks, compact disks, flash drives, etc.;
  - opening e-mail attachments that contain a virus; and
  - downloading and installing software that contains a virus.

Answers to the Inquiry Questions and Recommendations

Below are the answers to each of the inquiry questions and related recommendations for management’s consideration.

1. How was the virus detected, identified, and eradicated?

On Monday, February 14, 2005, Information Systems Services (ISS) Department noticed a performance problem throughout the City’s network. Initial diagnostics indicated that a key piece of hardware (router) was not working properly. ISS staff focused their efforts toward repairing or replacing the router. The City main application systems and network users experienced intermittent problems. Some users were affected more severely than others.

Early Tuesday morning, February 15, after the router had been replaced, the problems were still present and getting worse. ISS network staff ran additional diagnostics and determined that the problems were due to two types of network activity: (1) excessive Internet requests (called “broadcasts”) to a limited number of suspicious websites; and (2) individual computers scanning the City network for other vulnerabilities that could be exploited. ISS management declared the City network the victim of a virus infection.

ISS staff was busy trying to make preliminary assessments as to the extent of the infiltration and they attempted to identify and clean the computers of the virus. In addition, vendors were contacted to provide assistance. The vendors contacted included the City’s anti-virus software provider, one of the network hardware suppliers, and Microsoft Corporation (Microsoft). ISS staff worked with these vendors over the phone trying to determine the extent of the problem and what corrective actions were needed. Throughout the day, ISS attempted to keep the network functioning properly, however, there were still periods of time when the network was unavailable.

On Wednesday, the network was again partially working. A major obstacle encountered was that computers, which previously appeared to be "cleaned of the virus", were becoming re-infected. ISS was unable to determine exactly which computers on the network were infected and the source of the re-infection of "cleaned computers." ISS determined that to contain the infection, the network needed to be shut down and every computer needed to be cleaned prior to reactivating the network. ISS decided to completely shut down the network on Thursday at 6:00 p.m and begin the process of eradicating the virus from every infected server and computer.

The approach ISS decided to take to re-establish the network was to (1) eliminate the virus from all computers; and (2) install updates to virus software and operating system software to protect those "clean" computers.

On Thursday, technically competent users from other City departments were requested to assist ISS in implementing their plan. ISS management hoped to have the network back in full operations by the following Monday morning. Staff and volunteers began working on 8-hour shifts. For the computers that required cleaning efforts beyond the ability of the volunteers, a notation was made and those computers were bypassed for follow-up by ISS staff. The process to clean each computer and install the patches took much longer than anticipated, anywhere from 2-6 hours per computer.

At the conclusion of the first two shifts, ISS realized there were simply too many computers and not enough people-resources to have all the computers cleaned by Monday morning. On Friday, ISS management realized that the manual process was taking much longer than anticipated and began working with a vendor to find an alternative automated solution. While the automated solution was explored, staff and volunteers continued the manual process.

As of 4:00 p.m., Saturday, with only approximately 25% of the City's computers cleaned and updated, ISS determined that the automated solution was feasible and ISS management shifted all resources to develop an automated solution.

The proposed automated solution included installing an additional software utility that monitors network traffic and automatically disconnects PCs from the network that exhibit abnormal behavior. Such abnormal behavior could include: sending extraordinary large amounts of information over the network; repeatedly scanning the network for unprotected computers; attempting to contact unauthorized websites; and transmitting known virus signatures. With this utility monitoring network traffic, ISS felt confident that the network could be reactivated without allowing the virus to propagate. Once the network was reactivated with the utility monitoring the network traffic, there were approximately 80 computers identified across the City that were exhibiting at least one of the above-mentioned abnormal behaviors and were automatically disconnected. With the network reactivated and the virus unable to spread, ISS was able to automate the manual process that was previously being utilized to clean and update the computers.

On Monday morning, February 21, the City's network was available and major business processes had been re-established; however, the automated process to clean and update the PCs was not completed until Tuesday afternoon. There were, however, functional computers available in each of the City departments even though not all computers had been fully restored. In addition, there were a small number of users dispersed across the City who were unable to use their computers for up to two weeks.

2. What were the impacts of the virus to the City (i.e., financial, customer service, data integrity)?

Business processes have been developed such that departments heavily rely on the City's network for electronic communications, applications, and electronic documents that reside on the network servers to conduct their day-to-day operations. Without these resources, departments were generally unable to conduct business in their normal manner.

City operations were impacted in three main ways:

1) the direct cost of ISS staff work-time and overtime to eradicate the virus;

2) lost employee productivity due to inaccessibility of computer network resources; and

3) diminished customer service to the citizens due to inaccessibility of computer network resources.

Overtime

There is a certain amount of overtime, both paid and unpaid (compensatory time), that occurs every week. Reasons for incurring overtime are not recorded, therefore we were not able to identify the specific hours and estimate the overtime cost relating to the virus infection. To analyze overtime for the period October 1, 2004, through April 29 2005, we calculated the average overtime by pay period for every department and then compared that average to the actual hours incurred during the pay periods in which the infection and recovery occurred. The following table illustrates a summary of our analysis showing only the departments that incurred a material increase in overtime hours related to the virus.

Table 1
Analysis Showing Increase in Overtime Due to the Virus Infection

Department	Average OT Hours (10/1/04 – 4/29/05)	Actual OT Hours (due to virus)	% Increase
Police (Technical Staff)	156	322	107%
Utility Customer Services	205	343	67%
DMA - Supply	15	137	790%
ISS – Application Systems	74	196	163%
ISS - DNS	58	298	416%

OT – overtime
DMA – Department of Management and Administration
DNS – Distributed Network Services

Lost Productivity

Productivity loss proved to be challenging to quantify because often times employees were able to perform other tasks not requiring access to resources within the computer network (i.e., filing, paperwork, and “offline” computer work). These other tasks, however, were generally ones with a lower priority or not part of the employees’ regular business activities.

The impact varied greatly among departments and individuals depending on the employees’ duties and responsibilities and their abilities to perform alternative tasks. For example, many Parks and Recreation employees were not impacted at all because they do not use computers in their duties, while the Planning Department was greatly impacted because practically all their work is conducted on computers using electronic documents stored on the network.

In order to make our estimate as to the financial impact resulting from lost productivity, we interviewed key staff from each department in the City. As part of the interview, we asked a series of questions designed to determine the overall impact of the virus as well as specific questions related to regular and alternative work activities that they were able and/or unable to perform. We also asked for an estimate of percentage of lost productivity for each major classification of employees in the department.

For example, we were told that for the administrative staff in one department there was an 80% loss in productivity (i.e., only producing 20% of normal output). Therefore we used the total payroll for those employees for the week of 2/12 – 2/19 and calculated 80% of that payroll in order to estimate the dollar amount of productivity that was lost for those employees. Overall, we calculated that the virus infection caused a loss in productivity estimated at $343,000 (this amount does not include an estimation of the cost of overtime as previously noted).

Diminished Customer Service

Estimating the non-quantitative impacts to customer services also provided a challenge. However, many department staff identified examples of how their ability to provide customer services to City of Tallahassee citizens and customers was diminished. Examples included:

- Utility customers were not able to obtain information about their accounts because the system that contains that data on the network was unavailable. The customer service agents appeared to have done a commendable job of fielding calls and assisting customers to the fullest extent possible, but information that would normally have been available was not and could not be passed on to the customers.
- The Planning Department was forced to postpone a Planning Commission meeting because materials needed for the meeting were stored on a network server and were unable to be retrieved.
- Growth Management, responsible for issuing building permits, was still able to issue permits because Leon County's connection to the permitting system was used. While the process continued, it was at a slower rate than would have otherwise occurred.

There were examples from almost every City department where services to citizens and customers were negatively impacted.

3. How was the City infected with the virus?

Neither ISS nor our office determined how or when the City was first infected with the virus. ISS management determined that the cost involved to identify the specific cause would far exceed any benefits that may be derived from obtaining that information.

We did note two possible sources of the virus infection. First, there were instances of the Agobot virus being detected and reported "deleted" by the City's antivirus software prior to the week of February 14. Second, ISS discovered a new strain of Agobot when researching some suspicious activities occurring on some City PCs.

ISS decided to focus their resources on restoration rather than investigation for several reasons. These reasons included:

- there are multiple methods of infection possible (as noted in the background section);
- an old version of Agobot was detected earlier than February 14;
- a new strain of Agobot was subsequently discovered; and
- the infection was so widespread across the network.

We concur with ISS's determination that important resources would have been diverted from recovery efforts in order to determine the cause of the infection.

4. Was the infection preventable?

Yes, controls can be put in place to ensure that virus infections never occur. However, those controls would be so restrictive that business processes would be hindered to the point where they are inefficient and unreasonable. Therefore, ISS, like other information system services organizations, balance the risk and cost of virus infections (e.g., overtime, lost productivity, and diminished customer service) with the cost of the controls to prevent those infections (e.g., inconvenience, limiting business operations and communications). Therefore, it is not reasonable to expect every virus infection to be prevented.

Since there is an ongoing risk that infections can occur, controls need to be in place to mitigate the severity of the impact by containing the spread of those infections. An effective control to contain the spread of the virus is to eliminate the vulnerabilities that the virus exploits. Those vulnerabilities are eliminated by installing security updates to operating systems and applications provided by software manufacturers.

Our review showed that ISS management had not been installing the operating system security updates in a timely manner. For example, the particular update that addressed the vulnerability exploited by the Agobot virus had not been installed on the City's systems. That update was issued as a critical update by Microsoft in April 2004.

Our review of the actions taken to clean and protect the City's PCs from the virus infection showed that many updates were installed by ISS in response to the infection. For example, computers using one particular operating system had 32 updates installed which were issued by Microsoft between July 2003 and February 2005.

ISS faces many challenges trying to keep the City's network, applications, and operating systems current. Those challenges include the:

- complexity of the City's network;
- potential impact to critical applications;
- size of the City's computer network; and
- geographical dispersion of the network.

Complexity of the City's Network

The City's computer network is a complex assembly of many different pieces of hardware and software. Parts of the network that appear to be the same may be very different. For example, all computers in the City use a Microsoft Windows® operating system. However, depending on when the computer was purchased, it could be running any one of four different versions (Windows 2000, Windows NT®, Windows® 98, or Windows® 95). Each version has different security weaknesses and must have different procedures performed to maintain and protect them. Microsoft, Inc., provides separate software updates to fix weaknesses for each operating system version as they are identified. For example, an update for Windows NT® cannot be used to fix a Windows 2000 vulnerability.

Potential Impact to Critical Applications

The updates that are provided for each of the operating systems may create conflicts with other applications the City depends upon for business operations. For example, an update to a PC that uses a certain operating system may cause a conflict and prohibit PeopleSoft Human Resources Management System (HRMS) software application from functioning properly. If the PeopleSoft HRMS application is not working properly, then affected departmental timekeepers would not be able to enter payroll information. This potential impact is a major problem not only because of the multiple operating systems that are used but also because of the large number of applications that each update must be thoroughly tested against (such as PeopleSoft Financials, HRMS, and Customer Information System; Growth Management Permit Tracking System; Fleet Management software; and web applications).

ISS management stated that they did not have adequate resources (people and equipment) to thoroughly test each update, and therefore decided that it was not prudent to install the updates since they could not verify that there would not be a negative impact to critical City applications. Had the vulnerability exploited by the Agobot virus been eliminated by installing the applicable update on all PCs, the virus would not have been able to spread across the City's network.

As part of the cleaning and recovery process, ISS installed many untested critical updates to address the immediate problem related to the virus. The City was fortunate that there were no serious negative impacts to critical applications.

Size of the City's Computer Network

As noted earlier, there are approximately 2,400 personal computers (PCs) in the City's network and 21 employees with duties that involve maintaining those PCs. Of those 21 employees, 4 managers and 3 help desk staff are not directly involved in PC maintenance. That leaves 14 employees to maintain the City's approximately 2,400 PCs or a 170:1 ratio.

Geographical Dispersion of the Network

The City's network is spread out to every location from which City business is conducted. Those operations are conducted from diverse locations such as the airport, municipal complex, police department headquarters, City Hall, electric and water plants, and the fire stations. This disperse nature of the City's computer network increases travel time and reduces time available to maintain PCs, servers, and the network infrastructure.

5. What issues did management identify as a result of this virus infection?

After the network operations were restored, ISS management evaluated their previous actions and responses. During that evaluation, they developed a list of areas where improvements were needed, including number and expertise of ISS staff, communication, network segmentation, operating system updates, automated virus scanning, and computer security training for users and ISS staff. Additionally, during our discussions with representatives from City departments, we noted the need for more business continuity planning, i.e., plans for alternative means of conducting business without computers.

ISS Staff

ISS management determined that staffing levels of appropriately trained employees were not adequate to address this emergency. As a result, too much reliance was placed on too few people with the relevant skills and training. It is not practical or cost efficient to maintain staff at levels adequate for emergencies. However, there should be adequate staff with necessary skills to allow "front-line" employees to work in shifts without an undue interruption of work. In our observation of the response to the virus, we noted several ISS employees that worked in excess of 36 hours straight. Working without adequate rest can lead to mistakes.

We recommend that ISS identify employees in other departments with strong computer skills, knowledge, and abilities that can be called upon in emergencies to augment the existing ISS staff. This should allow ISS to reallocate staff resources to better address future emergencies.

Communication

With the growth and prevalence of computers and technology, more and more reliance has been placed on e-mail as the primary means of communication. Without the network, e-mail was unavailable. The phone system was then used as the backup means of communication. This, however was hindered by the large number of departments and sections that needed to be contacted. The time needed to contact all departments would have taken valuable resources from the task of eliminating the virus. To further complicate the use of the phone system as a backup means of disseminating information, the City's phone directory is maintained on the computer network which was unavailable. This affects the ability to efficiently and effectively communicate information to employees dependent on the City's computer network.

We recommend that an alternative means of communication be identified or developed (such as a phone or FAX tree) whereby key individuals in the City's various department can be contacted and then relied upon to disseminate information that would otherwise have been communicated directly by ISS through e-mail.

Network Segmentation

ISS began planning to segment the City's network in fiscal year 2004. To be able to complete the segmentation, many prerequisite improvements to the network infrastructure were needed. ISS has completed many but not all of these improvements. Therefore, at the time of the infection, the City's network could be viewed as one interconnected web of computers. As illustrated in Figure 1, on the next page, when one computer became infected with the virus, there was nothing to prevent the virus from spreading to all computers in the network.

Figure 1
Current Network Configuration

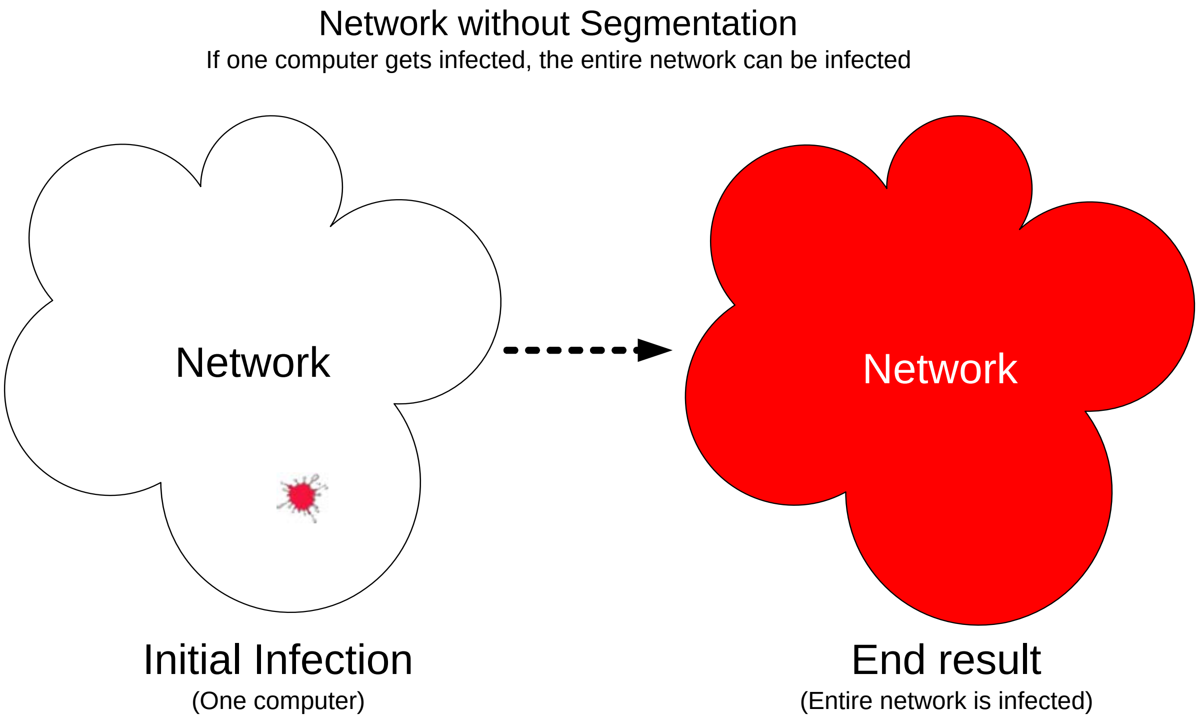
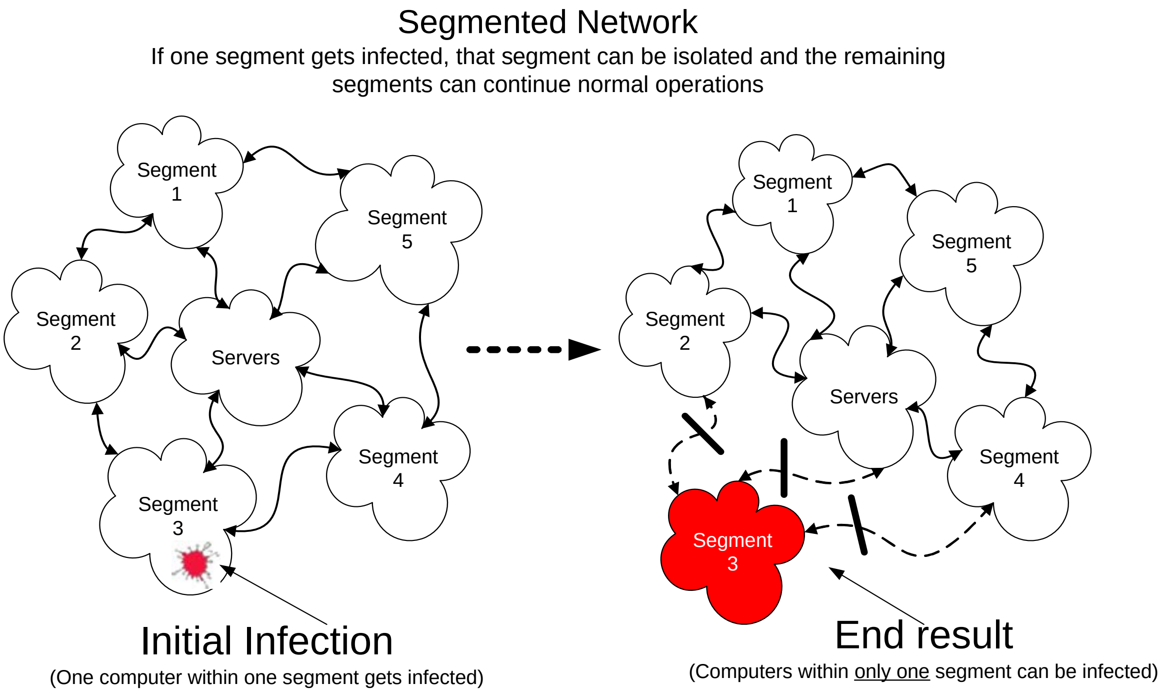

Network without Segmentation
If one computer gets infected, the entire network can be infected
Network
Network
Initial Infection
(One computer)
End result
(Entire network is infected)

Figure 2
Planned Network Configuration


Segmented Network
If one segment gets infected, that segment can be isolated and the remaining segments can continue normal operations
Segment 1
Segment 5
Segment 2
Servers
Segment 4
Segment 3
Segment 1
Segment 5
Segment 2
Servers
Segment 4
Segment 3
Initial Infection
(One computer within one segment gets infected)
End result
(Computers within only one segment can be infected)

Segmentation can provide many advantages to the City's network infrastructure, including the ability to: isolate network problems; improve security; and reduce network congestion. Segmentation issues are described in more detail below.

- Isolate network problems – As shown in Figure 2 (on the previous page), problems such as viruses and hardware failures can be limited to small areas of the network and the impact limited to a much smaller number of users in a segmented network. An analogy would be quarantining someone with an infectious disease.
- Improve security – An unauthorized intrusion into one segment of the network could be limited to that segment thus rendering the remained of the network "invisible" to the intruder.
- Reduce network congestion – Congestion of the network could be reduced when communication within one segment stays within that segment and is not transmitted across the entire network.

We recommend that ISS continue with their plans for network segmentation.

Operating System Updates

ISS acknowledges that updates to operating systems and applications are critical to protecting the City's computing environment. In this particular virus infection, the updates would not have prevented the infection of the first PC; however, it would have prevented the virus from self replicating across the entire network. ISS management stated they are making plans to ensure that updates are regularly and timely installed to all computers on the network through automated processes.

Due to the potential negative impact that updates can have to critical applications we recommend that ISS management also consider implementing testing processes that minimize the loss of critical City applications as a result of updates installed.

Automated Virus Scanning

Prior to the virus infection, the anti-virus software installed on PCs only scanned files and applications when opened or run by users. In response to this virus infection, additional virus detection software was installed on all PCs. That software was configured to monitor what is in the PC's memory, automatically scan the PC's hard drive when initially turned on, and re-scan the hard drive periodically throughout the day. Monitoring and scanning uses a great deal of the applicable computer's processing power and memory. For some of the older computers, this scanning greatly diminished the performance of the PC. To mitigate this impact, ISS has recommended that additional memory be purchased and installed in those older computers so that they can function adequately with the additional scanning. We concur with ISS's recommendation.

Computer Security Training

After this virus infection, ISS management determined that both City users and ISS staff require training that increases staff's expertise and users' awareness of computer security.

This increased user awareness would hopefully reduce or eliminate the most common means of virus infection, including: accessing files on removable media (i.e., floppy disks, CDs, and flash drives); opening infected e-mail attachments; visiting "strange" or suspicious web sites that may automatically run virus scripts; and installing unauthorized or unapproved software that may have viruses embedded. ISS wants all users to be knowledgeable about computer security, so they make reasonable decisions as to what should or should not be done with City computers.

Previously, security at the individual PC level had not been a major point of emphasis with ISS because the City had never encountered a problem of this magnitude. That is not to say that ISS felt security was not important, but that there were other issues that were assigned a higher priority. According to ISS management, there has been a greater focus on training on networking and various software applications than on PC security. In response, ISS is making plans to increase the level of PC security training for all employees. This should also help ISS with the staffing issue that was presented earlier in that existing employees will be trained and will be able to "step up" and assist in similar emergencies in the future.

We recommend that ISS continue with its plans to increase the awareness of the importance of PC level security.

Business Continuity Planning (Alternative Means of Conducting Business)

As noted earlier, the impact to department operations varied from minimal to critical. From this virus infection, many departments learned the importance of continuity planning in order to respond to emergencies.

We noted that some of the departments that were most severely impacted were those that had emergency plans in place for a total loss of resources (i.e., offices are totally destroyed); however, they did not consider how to address a situation where only one part of their operations was interrupted. Other departments had more detailed plans that had provisions for operating without computers; those departments seemed to be impacted less than the others. We recommend that all departments that did not have adequate plans for business continuity in the event of computer related emergencies, develop and/or further refine their disaster plans to encompass the possible loss of any vital resources.

Conclusions

In conclusion, we do not believe the initial virus infection could have been prevented. The risk of virus infections is part of using computers in an interconnected environment. In this particular instance, we do believe the spread of this virus across the network could have been prevented if available operating system updates had been installed.

Unfortunately, virus infections are natural occurrences for everyone that has computers, networks, and Internet connectivity. The key is to minimize the impacts of those infections by implementing preventative measures and having plans developed to re-establish business operations as quickly as possible.

City departments learned many lessons during this virus infection. Some of the actions needed, which are based on the lessons learned, are being funded within the current budget while others are planned for next fiscal year. Areas identified by ISS management that need to be addressed include:

- increasing the number and expertise of ISS staff;
- improving communication;
- implementing network segmentation;
- installing operating system updates in a timely manner;
- implementing automated virus scanning;
- providing computer security training for users and ISS staff; and
- improving business continuity planning throughout all City departments.

Overall, we feel that ISS and the employees that volunteered from other departments should be commended for their response to and elimination of the network's virus infection.

Included as Appendix A is management's action plan to address each of our recommendations except the development or refinement of business continuity plans by all City departments.

Appointed Official's Response

City Manager:

The ability to ensure that the City's information assets are safe and secure from attack is certainly a priority and I appreciate the follow up by Auditing staff. The virus certainly impacted our work processes and plans are in place to complete all of the action items documented in this report. I would like to thank Auditing and DMA/ISS for their work in this effort.

Appendix A - Action Plan

Action Steps	*Responsible Employee*	Target Date
Objective A: *To ensure adequate staffing during times of emergencies.*		
1. Identify employees in departments other than ISS, from across the City, with strong computer skills, knowledge, and abilities that can be called upon to augment ISS staff in times of emergencies.	Don DeLoach	8/1/05
Objective B: *To develop an alternative means of communicating and disseminating information when e-mail is unavailable.*		
1. Identify or develop an alternative means of communicating important information throughout the City for use when e-mail is no longer available.	Don DeLoach	8/1/05
Objective C: *To complete the segmentation of the City's computer network.*		
1. Continue and complete the process of segmenting the City's computer network.	Terry Baker	6/06
Objective D: *To ensure that operating system and application updates are installed and do not impact critical applications.*		
1. Develop and implement a plan to test operating system and application security updates prior to installation.	Terry Baker Tanya O'Neill	10/1/05
2. Install operating and application security updates within a reasonable time frame after completion of testing.	Terry Baker Tanya O"Neill	11/1/05
Objective E: *To improve computer security knowledge and awareness for both ISS staff and other computer users throughout the City.*		
1. Complete development and implementation plans to increase the awareness of the importance of PC level security.	Don DeLoach	11/1/05

Copies of this Inquiry may be obtained at the City Auditor's web site (http://talgov.com/citytlh/auditing/index.html) or via request by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (auditors@talgov.com).

This Inquiry was conducted by:
Dennis Sutton, CPA, CIA, Sr. Auditor
Beth Breier, CPA, CISA, Audit Manager
Sam McCall, CPA, CIA, CGFM, CGAP, City Auditor