

Management Advisory 2003 – 2

To: Pat Blaney Internal Audit Director
From: Ilonka E. Washburn Senior Internal Auditor
CC: Dwight E. Brock Clerk of the Circuit Court
Audit File
Date: June 4, 2003
Re: Software licensing

Software Licensing

BACKGROUND

Information Technology's (IT) mission is: to operate, maintain and safeguard the County's telecommunications, 800MHz Public Safety radio, data networks and core network services; to plan, acquire, operate and maintain software applications and their server platforms on behalf of County departments; to plan, operate, support and maintain the desktop workstations and core productivity software for the County staff; to plan, support and safeguard the utilization and maintenance of County data.

The IT department provides for test equipment and software systems to monitor server operating parameters and utilization as well as software for central deployment. The desktop support program provides for the installation, support, and maintenance of desktop workstation users. This program provides for "field" staff who work with users at their locations, as well as tools, spares and software systems.

It is against County policy to install personal software on public property. One area of weakness noted during an initial interview was the stand-alone computer. They may not always be quarantined from the network, and consequently, IT's network management software cannot detect what programs may be on those machines' hard drives.

AUDIT OBJECTIVES & SCOPE

The specific objectives of this review were to determine whether the computer software installed complied with applicable licensing requirements. The scope of this advisory was limited to confirmation of software programs with corresponding licenses available for three sample departments.

FINDINGS

1. Facilities Management

All twenty-one computers in the Facilities building were inspected for unauthorized software installations and/or programs downloaded from the Internet. Eight computers, or 38% of all inspected, were found to be in non-compliance with County policies. Seven computers had programs downloaded from the Internet, with some having as many as five Internet programs. One computer had nine programs installed by its user, who claimed to have licenses for each at his home. The user claimed these programs were directly job related, however, one of the nine programs was a computer game.

The matter of personal license possession was not researched further as it is beyond the scope of this review to determine if the unauthorized software found on the County's computer is also loaded on the user's personal home computer. However, it is against County policy to install personal software on public property because this could seriously damage the County's computer network, and it could expose the County to liability for software piracy.

2. Code Enforcement

Forty-one computers in the Code Enforcement Department were examined for unauthorized software, and thirty-two computers were found in compliance with County policy. The 20% (8) of computers with unauthorized software had programs downloaded from the Internet with two of the non-compliant computers having more than one downloaded program. Not one of the forty-one computers examined had personal programs installed on it.

While downloaded programs from the Internet may not be as potentially costly as actually installed personal programs (due to license requirements and possible fines) they could disrupt the operating system by changing the network settings to accommodate their specific needs.

3. Transportation Design Operations

Forty-one computers in Transportation Design Operations were examined for unauthorized software. Eighteen (18) computers, or 44% of all computers inspected, had unauthorized software downloaded from the Internet, with one computer having five downloaded programs, while most others had one Internet program. Another one of the computers contained a program that IT had not installed, but was later approved by IT. During the detection phase a license for this program was presented to this auditor, and IT verified it to be a program used in the daily accomplishments of this user's work.

However, as mentioned previously, the IT department should pre-test and install all programs to ensure compatibility with the operating system. It should also be emphasized again that downloaded programs could pose a threat to the network and are against Collier County policy.

RECOMMENDATIONS:

1. Facilities Management; 2. Code Enforcement; 3. Transportation Design Operations

Whereas it may be difficult to prevent downloading from the Internet, it should be noted that installation of personal software poses a threat to the operating system as it could result in the potential loss of data and/or the breakdown of the entire network to all County departments. If it is necessary to install personal software on County owned property, the IT department should perform the prerequisite testing and installation, as well as keeping the corresponding software license readily available. As far as downloading from the Internet is concerned, periodic spot checks could prevent or limit this misuse of county property. IT could accomplish said spot checks while responding to a help call.

Individual departments may perceive installation of personal software on public computers as a cost savings, however, this practice is not only illegal – if also loaded on the user's personal computer, it is also against Collier County policy. To disrupt the Collier County Information Network through the installation of unauthorized and untested software could not only be financially detrimental but could bring the County network to a screeching halt if the system became non-functional.

Information Technology's Response (Exhibit A)

I concur with the "Conclusion" section of the audit.

The item having to do with compliance with legal licensing was very much contained and has been dealt with.

IT is in the process of implementing process improvements, which will go a long way to improve our capabilities to proactively enforce county policies.

1. Only a very few users will have administrative rights to their workstations. This will greatly curtail installation of Internet downloads, except for plug-ins - which will intend to allow.
2. We are implementing much better software for "discovery" and software inventory. We will be able to search out unauthorized software much better with this improved automation.
3. We are establishing standard workstation disk images and we will not repair malfunctioning machines. We will re-image them. This effectively puts the workstation back into a known state - which is supportable and totally in compliance with county policy.
4. We will continue to educate our management staff and users regarding county policy.

Operating a computer network is not risk free. We must strike a balance between the controls we need to ensure the availability of network services and safeguard county data and the flexibility required to provide improved productivity services to our users. We will continue to work with you to ensure we strike the correct balance.

CONCLUSION

While Information Technology (IT) is continuously striving to prevent the illicit installation of unauthorized software or the downloading of Internet programs, distant monitoring of software actually loaded on each computer needs to improve. IT should not only monitor but also remove unauthorized software/programs without causing disruption to the system as a whole or the individual server.

While IT is responsible for the monitoring and maintenance of the information system, it is the responsibility of each department to ensure that any software intentionally installed on their computers should be for a public purpose and with the appropriate software license for each program.

-----Original Message-----

From: Axelrod, Barry
Sent: Tuesday, June 03, 2003 3:17 PM
To: Ilonka E. Washburn
Cc: Dwight E. Brock; Pat Blaney; ochs_l
Subject: Software Licensing Audit

I concur with the "Conclusion" section of the audit.

The item having to do with compliance with legal licensing was very much contained and has been dealt with.

IT is in the process of implementing process improvements which will go a long way improve our capabilities to proactively enforce county policies.

1. Only a very few users will have administrative rights to their workstations. This will greatly curtail installation of Internet downloads, except for plugins - which will intend to allow.
2. We are implementing much better software for "discovery" and software inventory. We will be able to search out unauthorized software much better with this improved automation.
3. We are establishing standard workstation disk images and we will not repair malfunctioning machines. We will reimage them. This effectively puts the workstation back into a known state - which is supportable and totally in compliance with county policy.
4. We will continue to educate our management staff and users regarding county policy.

Operating a computer network is not risk free. We must strike a balance between the controls we need to ensure the availability of network services and safeguard county data and the flexibility required to provide improved productivity services to our users. We will continue to work with you to ensure we strike the correct balance.

If you require actions beyond those described above, please contact me directly.

Barry Axelrod
Director, Information Technology
Collier County Board of County Commissioners
239-774-8854