

Survey: 65% of School Districts use Cloud

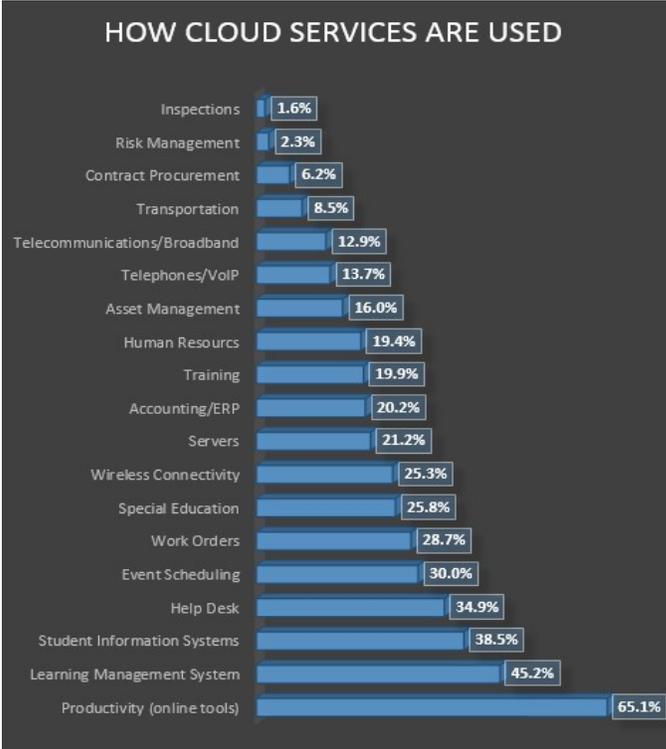
According to the [K-12 IT Leadership Survey](#) by CoSN, more than 65% of IT leaders say their district now uses productivity tools like Google Apps for Education. This is a tremendous increase over last year when only 10% reported using cloud services.

Benefits of Cloud Services:

1. Better enable mobile learning with devices because they don't require students to have to pass through a district firewall to access programs.
2. Less expensive than other software.

Bob Moore, project director for CoSN's Protecting Privacy in Connected Learning stated "when an outside company manages the technical side of the program, technology leaders have more time for working with teachers in classrooms instead of troubleshooting system problems."

For more information on Cloud Services and Data Monitoring for school districts, visit <http://www.Net56.com/Solutions/digital-classroom>



Totals do not equal 100% because responders were asked to "Mark all that apply".

[2015 K-12 IT Leadership Survey Report](#), Demographics used for Report

Q & A with the 2 Minute Tech

Q: We have a Windows 2003 Server. When should we try to replace it? I heard that 2003 was no longer going to be supported. Is that true, and if so, what can we do?

A: The answer is right away. Windows 2003 Server support ends July 14, 2015. One of the main concerns is that hackers are waiting for unknown vulnerabilities once that support ends. Someone also asked if we can upgrade. That answer is no. Windows 2003 Server will need to be reloaded with Windows 2008 R2 Server at the very least in order to take advantage of the latest patches.

Have a question for our 2 Minute Tech? Visit <http://www.Net56.com/2-minute-technology/> and submit your question. All questions are answered within 48 hours.

Dates to Remember

October 18-20 – [LCS Fall Leadership](#)

For an archive of our Newsletters, please visit: <http://www.net56.com/newsletters/>

In this Issue:

- Cloud Services P 1
- 2015 K-12 IT Leadership Survey P 1
- Q & A with the 2 Minute Tech on Windows 2003 Server Support Ends July 14, 2015 P 1
- What's Hiding in YOUR Network? P 2&3



Non-Invasive way to collect data

No business data collected

No conflict with applications

We analyze information and provide comprehensive in-depth audit results

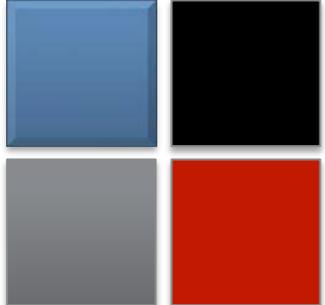
Reports – Easy for business managers to understand

Categorized for easy risk management – Saves you \$

FREE ESTIMATES

Do You Know
What's Hiding
 in YOUR
Network?

CUSTOMIZED NETWORK AND SECURITY AUDITS



- ◆ Detailed Analysis of Active Directory
- ◆ Hardware Inventory
- ◆ Internal & External Vulnerability Scans
- ◆ Network Risk Report & Management Plan
- ◆ Security Risk Report & Management Plan
- ◆ Comprehensive SWOT Analysis

**FAST
 NON INVASIVE
 SAFE
 SAVES YOU \$**

FACT: 9 out of 10 computer networks have potentially serious IT problems sitting undetected.

FACT: Many School Districts don't have the IT staff or skill level to prevent bigger issues from happening because there is no time to handle the daily maintenance that is required.

As a leading provider of managed IT services in the Chicago land area, we would like to meet with you and provide a health audit of your computer network and technology. We will analyze your network to identify vulnerabilities that could leave your school district at risk of a security breach. Depending on what we uncover, we will also make suggestions on ways to prevent unauthorized access, augment security systems, better lock down sensitive data, become more mobile and, in general, get more out of your existing technology infrastructure.

Our Unique Process Has Many Benefits Over Other Audits

- No software installed
- No agents or probes living on your network for days, weeks, or longer
- An average, mid-sized network is scanned and complete reports provided to you.
- You are under no obligation to use our services to resolve issues, but we are available if needed.

Here's What You Get

- Detailed Analysis of your Active Directory
- Hardware Inventory
- Internal & External Vulnerability Scans
- Network Risk Report & Management Plan
- Security Risk Report & Management Plan
- Comprehensive SWOT Analysis

Category	What We Uncover
Hardware:	<ul style="list-style-type: none">✓ Servers, Workstations, Printers, and non-AD devices (like switches/routers/printers)✓ Old computers which are still joined to the domain and have not been removed
Software:	<ul style="list-style-type: none">✓ Systems with missing Patches/Service Packs/Security Updates✓ Local accounts (per-system) with weak/insecure passwords✓ Systems with missing Anti-Virus, Anti-Spyware, or firewall misconfiguration
Configuration:	<ul style="list-style-type: none">✓ Security policy inconsistency across network servers/computers✓ Outbound system access that should be blocked✓ Lack of Content filtering (Social Media, Entertainment, Pornography, Illegal Downloads)
Accessibility:	<ul style="list-style-type: none">✓ Misconfiguration of user access to Network Shares✓ Detailed breakdown of AD Security Group Membership
Security Risks	<ul style="list-style-type: none">✓ Old user accounts which still have access and have not been properly disabled✓ Internal systems with open ports that pose a potential security risk✓ External issues which put your network at risk of business disruption or data loss