

CDW-G School Safety Index 2008

May 19, 2008



Study Focus and Objectives

- Now in its second year, the CDW-G School Safety Index provides a nationwide, first-hand view of school safety issues from the perspective of district IT and security directors. Additionally, the index enables schools to measure themselves against a national benchmark with current questions and data
- Working with Quality Education Data, CDW-G surveyed more than 400 K-12 district IT and security directors to:
 - Evaluate districts' cyber and physical security
 - Assess current cyber and physical security measures
 - Understand the impact of cyber and physical security education and communication
 - Understand the proliferation of security breaches



Contents

Crash Course: Executive Summary	Page 4
Understanding the Index	Page 5
The School Safety Index	Page 9
Pop Quiz: Education Security	Page 10
Hall Monitoring: Network Access	Page 11
Taking Attendance: Network Authentication	Page 13
School Rules: Cyber Education	Page 14
Breaking the Rules: IT Breaches	Page 15
Test Taking: IT Barriers	Page 16
Hall Monitoring: Campus Access	Page 17
Hall Monitoring: Mass Notification	Page 19
Breaking the Rules: Physical Breaches	Page 21
Test Taking: Physical Barriers	Page 22
Homework: Calls to Action	Page 23
Methodology and Demographics	Page 24



Crash Course: Executive Summary

- **New Tools Lock Down the Network**

- Districts are actively engaged in using new tools and techniques to improve cyber safety, including network access control (NAC), which ensures that only authorized users and applications access the network

- **Barriers Still Loom Large**

- Despite the availability of tools to improve cyber safety, IT security breaches are up, and *one-third* of districts report that their networks are vulnerable to attack. Districts continue to struggle with budget constraints and with how to best utilize limited staff resources to improve cyber and physical security

- **Physical Safety Pushes Ahead of Cyber Safety**

- Implementation of mass notification systems, coupled with increased use of security cameras, gives physical safety an edge. While availability of advanced technology tools is enabling schools to do more with the same or fewer security staff, districts have not yet registered a decline in incidents

- **“Eye in the Sky” Access Improves Police Response**

- More districts should consider utilizing the “Internet” in IP security cameras to give local police and fire departments real-time access to footage during an emergency. “Eye in the sky” access puts police on the front lines by providing instant information during time-critical situations



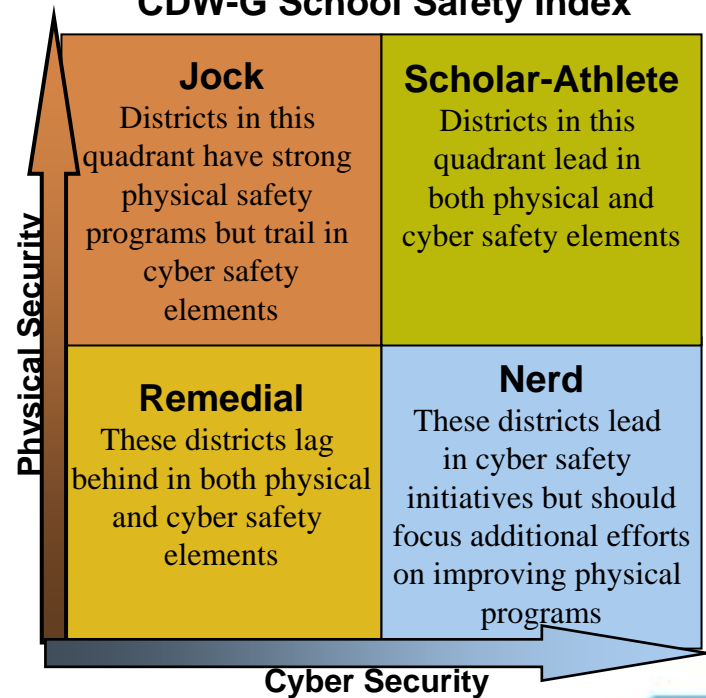
Understanding the Index

Based on research from Quality Education Data, national safety organizations and CDW-G's market expertise, the CDW-G School Safety Index's 8 positive indicators and 4 contraindicators represent the elements of an overall security program. The CDW-G School Safety Index sets a national benchmark to gauge the current status of school safety and outlines steps for improvement. Additionally, the Index aims to focus attention on the convergence of IT and physical security in public school districts.

CDW-G School Safety Index Elements

Cyber Security Indicators	Physical Security Indicators
District Cooperation	Security Tools
Data Monitoring	Local Authority Communication
Network Access	Emergency Communications
User Authentication	
Education	
Contraindicators	Contraindicators
IT Breaches	Physical Breaches
IT Barriers	Physical Barriers

CDW-G School Safety Index

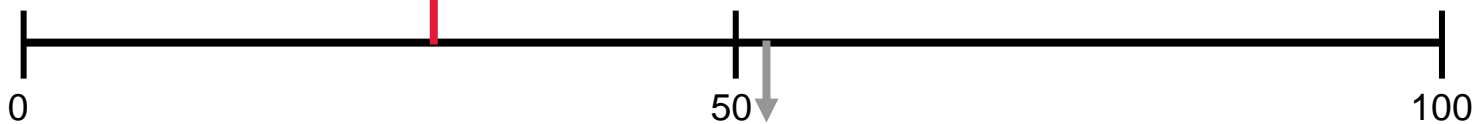


2008 Cyber Safety Index

Element	Question	Yes
District Cooperation	Regarding plans or purchases that affect cyber security and physical security, do your district IT and physical security department share or collaborate on plans and/or purchases?	65%
Data Monitoring	Does your district monitor access to student records?	85%
Data Monitoring	Does your district monitor access to student email?	40%
Data Monitoring	Does your district monitor access to teacher/staff records?	74%
Data Monitoring	Does your district monitor access to teacher/staff email?	69%
Network Access	Does your district restrict access from outside devices on the network, such as students' or teachers' personal computers, MP3 players, etc.?	66%
Network Access	Does your district use network access control (NAC)?	57%

Element	Question	Yes
User Authentication	Does your district authenticate users as they access the network?	89%
User Authentication	Do you authenticate users to the network using unique user names and passwords?	94%
Education	Does your district update the Acceptable Use Policy at least once a year?	64%
IT Breaches	Has your district had an IT breach in the last 12 months?	14%
Cyber Security Barriers	What are your district's main barriers to improving IT security: Budget?	79%
Cyber Security Barriers	Too few human resources?	61%
Cyber Security Barriers	Lack of defined policies?	22%
Cyber Security Barriers	Hardware/Software barriers?	47%
Cyber Security Barriers	Lack of user participation?	29%

2008 National Cyber Safety Average = 38.6



2007 National Cyber Safety Average* = 51.3

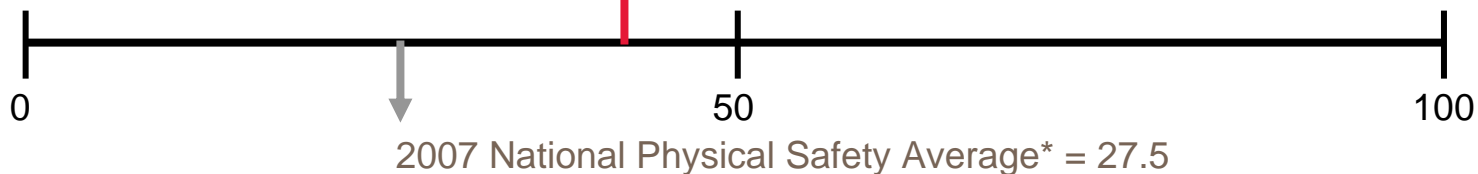
* Weighted average for comparison



2008 Physical Safety Index

Element	Question	Yes
Security Tools	Does your district currently use any of the following tools to limit or monitor access to the facilities: ID Cards?	32%
Security Tools	Security cameras?	67%
Security Tools	Security team?	26%
Security Tools	Metal detectors?	4%
Security Tools	Real-time access to sex offender database?	28%
Security Tools	Does your district currently use security cameras in and around school buildings?	70%
Local Authority Communication	Do your local police have the capability to access your security camera footage in real time?	33%
Emergency Communications	Does your district use a mass notification system?	45%
Emergency Communications	Do you use your mass notification system (MNS) to alert the community to any of the following: School closures?	84%
Emergency Communications	Weather-related emergencies?	81%
Emergency Communications	School lockdown?	59%
Emergency Communications	Physical threat to the school?	60%

2008 National Physical Safety Average = 44.7



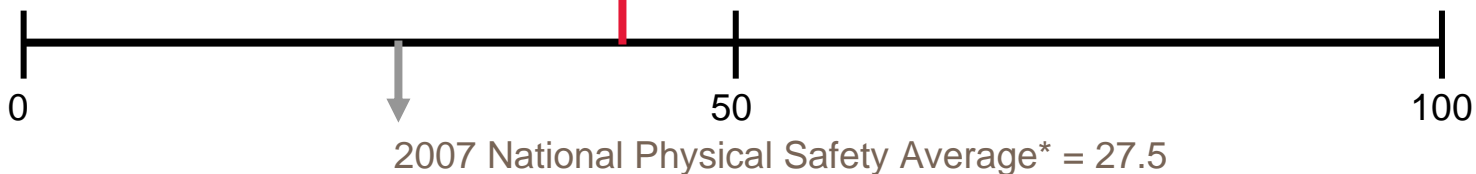
* Weighted average for comparison



2008 Physical Safety Index (cont.)

Element	Question	Yes
Emergency Communications	Who receives messages from the MNS: Faculty/staff?	91%
Emergency Communications	Administration?	84%
Emergency Communications	Students?	39%
Emergency Communications	Parents/guardians?	82%
Emergency Communications	What capabilities does the MNS have: Email alerts?	61%
Emergency Communications	Automated phone messages?	70%
Emergency Communications	Text message alerts?	32%
Emergency Communications	Sirens or loud speakers?	28%
Physical Breaches	Has your district experienced any breaches in physical security in the last 12 months?	31%
Physical Barriers	What are your district's main barriers to improving physical security: Budget?	69%
Physical Barriers	Too few staff resources?	29%
Physical Barriers	Lack of defined policies?	10%
Physical Barriers	Need for more tools?	32%
Physical Barriers	Lack of user participation?	12%

2008 National Physical Safety Average = 44.7

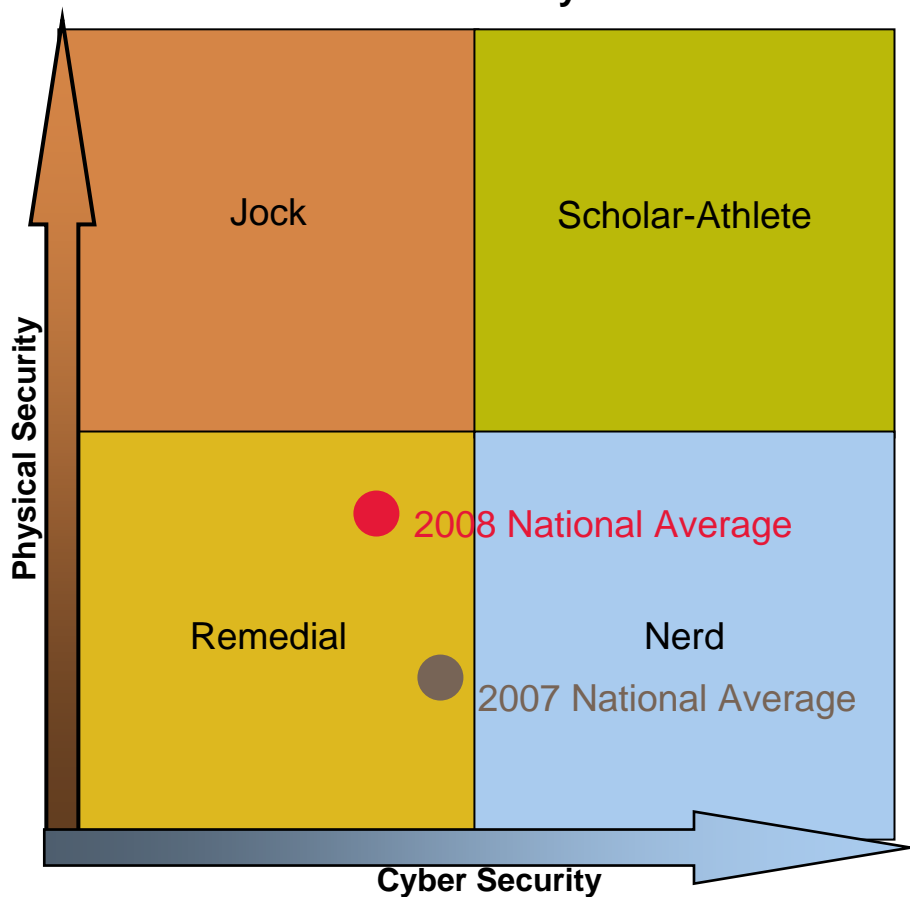


* Weighted average for comparison



The School Safety Index

CDW-G School Safety Index



Taken together, the Cyber Safety Index and the Physical Safety Index comprise the School Safety Index. In 2008, K-12 districts nationally are more athletically inclined in their approach to physical security but could use a refresher course in IT to improve cyber security performance

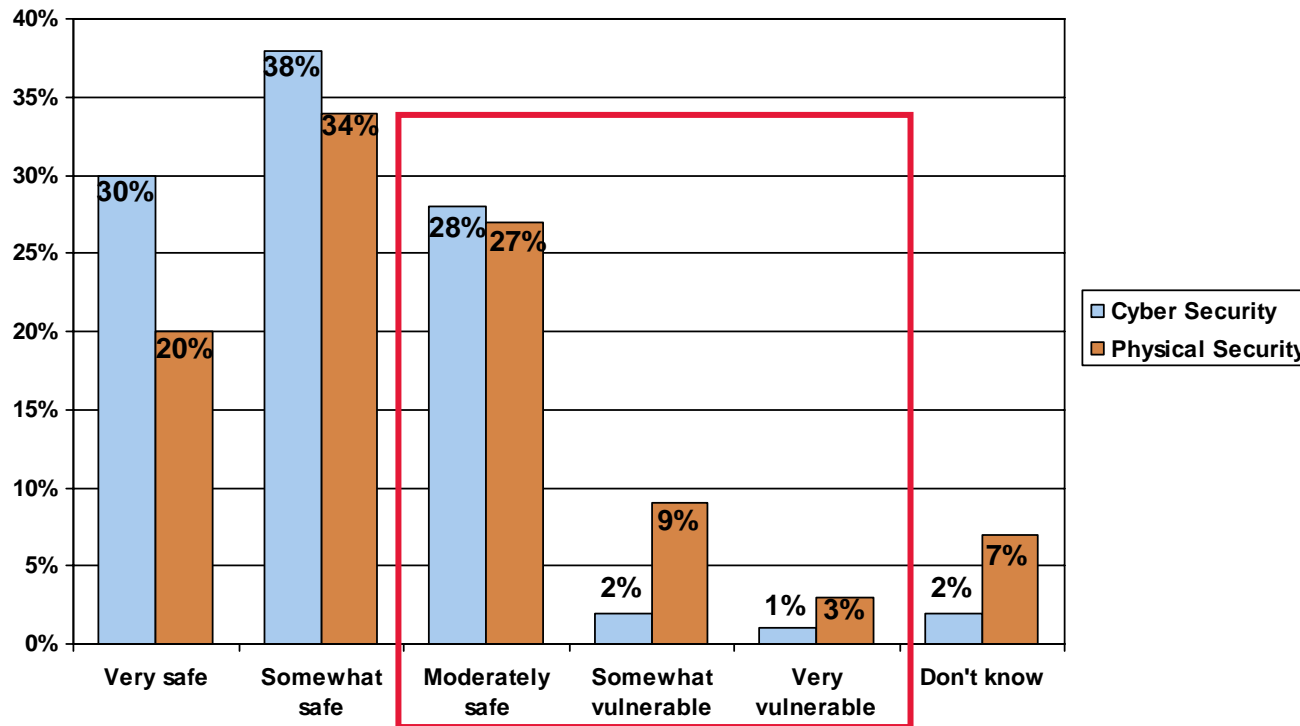


Pop Quiz: Education Security

Asked to evaluate their own district's security:

- **31%** of respondents indicated that their cyber security needs improvement
- **39%** of respondents indicated that their physical security needs improvement
- When it comes to plans or purchases that affect *both* cyber and physical security, **32%** of respondents don't collaborate with their IT/physical security counterpart

Grade Your Own Work: Rate Your District's Cyber and Physical Security

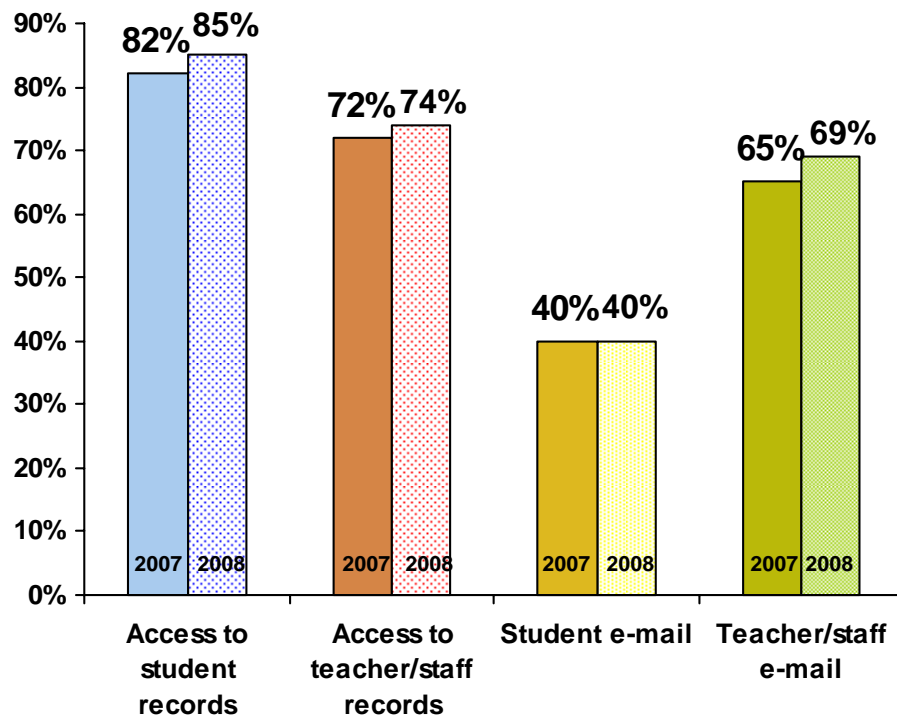


Hall Monitoring: Network Access

Monitoring access to district records and email helps prevent data breaches and deters unauthorized access to the network.

- Compared to 2007, the percentage of districts monitoring access to student/faculty records and emails remains virtually unchanged
- **66%** of districts are protecting their networks from unauthorized software and viruses by preventing outside devices from accessing the network

Do you monitor access to the following?



Do you allow outside devices to access the network?

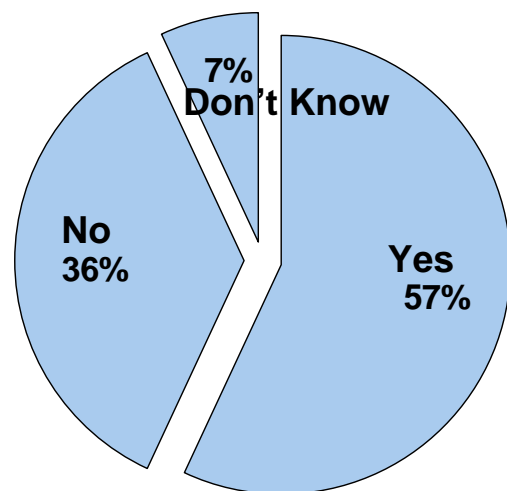
Yes, faculty/staff only	18%
Yes, students/faculty/staff	14%
No	66%
Don't Know	2%

Hall Monitoring: Network Access

Network access control (NAC) ensures that every computer on a district's network is secure by providing updates to each user's applications and applying security patches. Additionally, NAC enables IT staff to view and control who and what is on the network.

- **36%** of districts are not using NAC

Are you using network access control?



Districts using NAC	
Rural	60%
Suburban	54%
Urban	45%

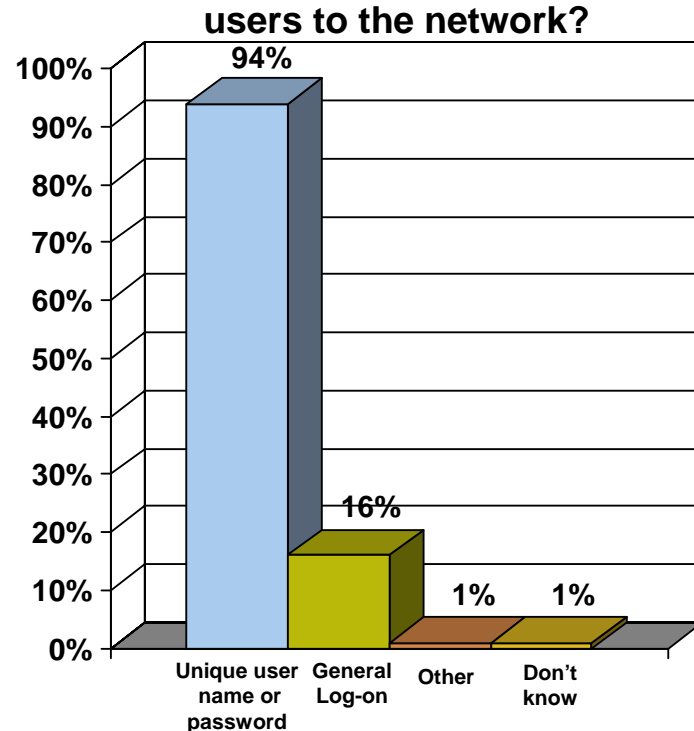
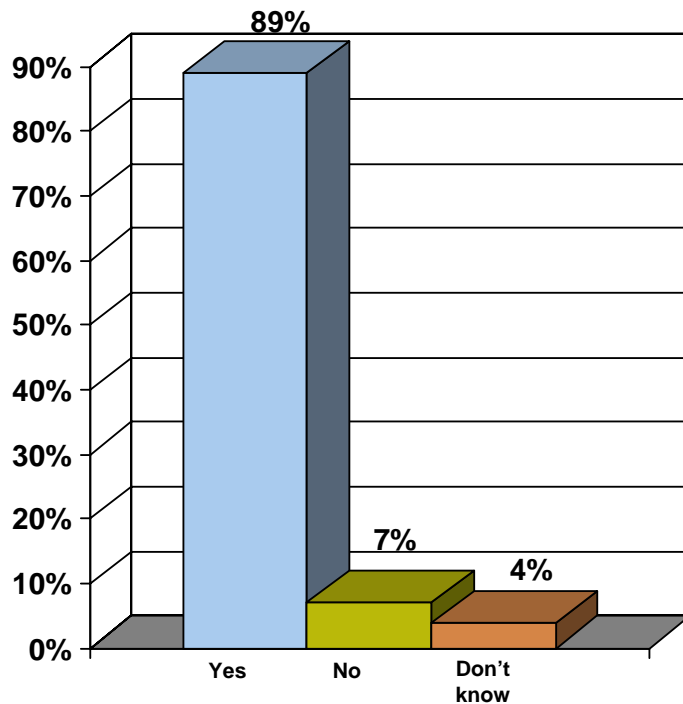
Consider utilizing NAC to:

- Separate student and teacher access on the LAN
- Monitor and control how network resources are used
- Enable identity-based control of applications, users and threats in a single platform

Taking Attendance: Network Authentication

The majority of districts – **89%** – are doing a good job of protecting the network by authenticating users. But between 2007 and 2008, there has been no change in *how* districts ensure that only authorized users access their networks, with **16%** of districts still using general log-ons rather than unique user names and passwords, exposing themselves to a security breach.

Do you authenticate users to the network? How does your district authenticate users to the network?



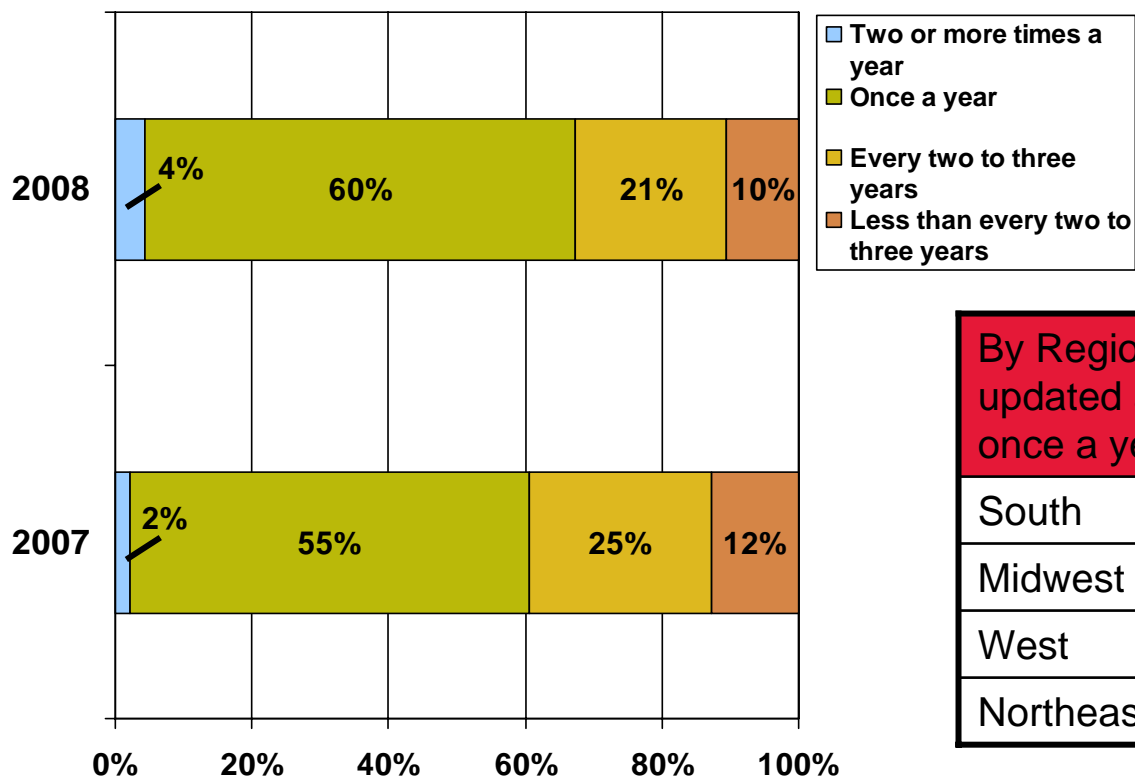
Other Authentication Methods
Novell Network
Voice Recognition
WEP Encryption for Wireless

School Rules: Cyber Education

Acceptable use policies (AUP) enable school districts to ensure that network users follow the policies and procedures that protect students and the network.

- This year's results show a 7% improvement in districts that update their acceptable use policies at least once a year

How often is your district AUP updated?



By Region: AUPs updated at least once a year

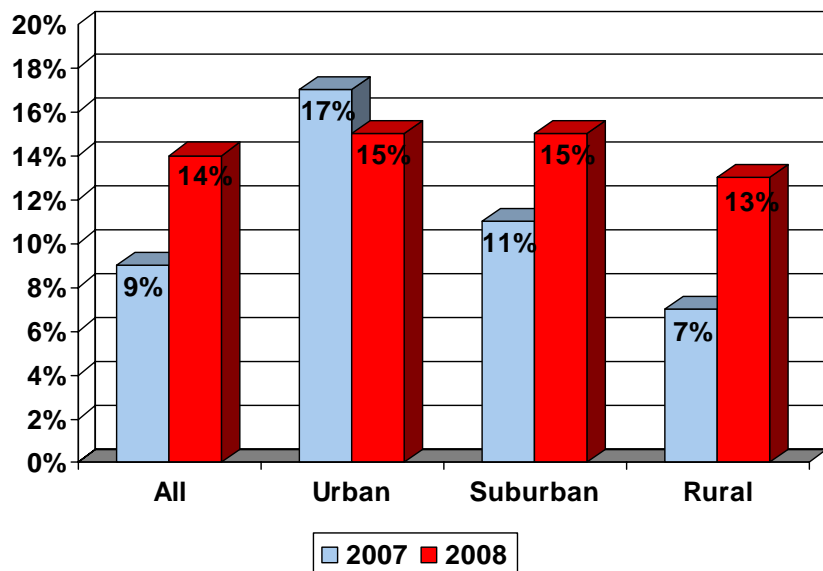
South	75%
Midwest	68%
West	64%
Northeast	43%

Breaking the Rules: IT Breaches

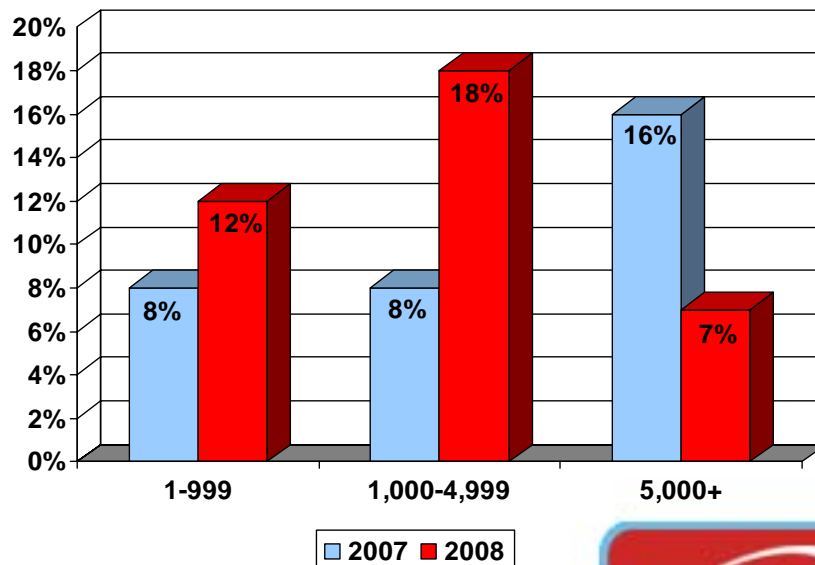
IT security breaches are up in every segment but urban. Overall, **14%** of districts report at least one IT security breach in the last 12 months, up from **9%** in 2007.

- Urban and mid-size districts report the most breaches
- **31%** of districts report that their networks are “in need of improvement,” “somewhat vulnerable” or “very vulnerable” to attack

Breaches by Metropolitan Area



Breaches by Enrollment

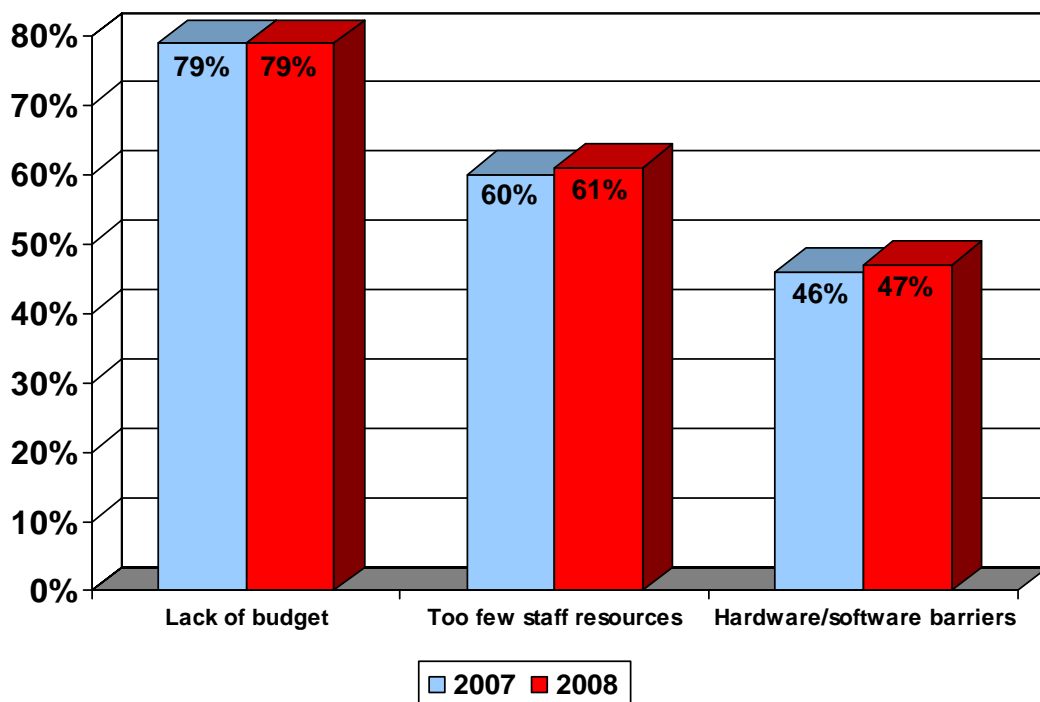


Q) Have you experienced any breaches in IT security in the last 12 months?

Test Taking: IT Barriers

Budget challenges remain the biggest barrier to IT security improvements. Respondents also cite a lack of sufficient staff resources and hardware/software barriers.

What are your district's biggest barriers to improving security?



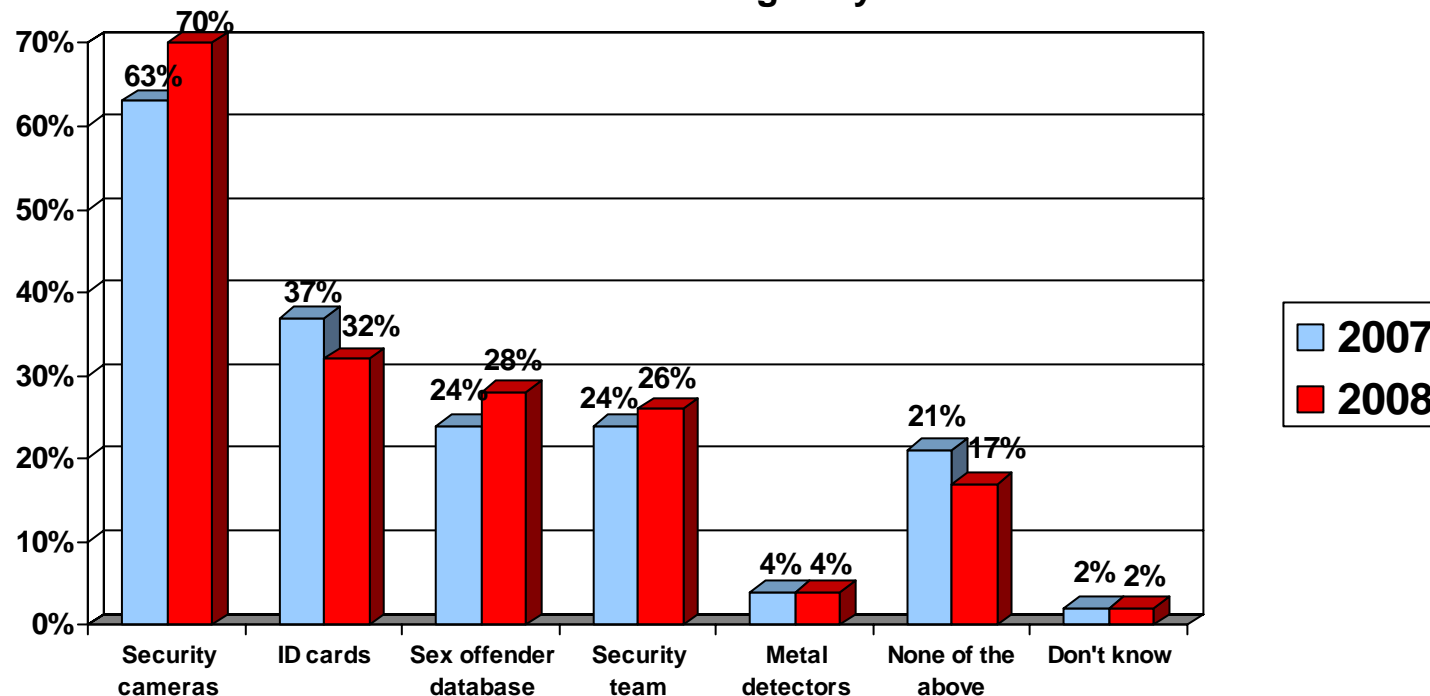
Other Barriers to Improving IT Security

- Lack of user participation
- Lack of defined policies
- Lack of leadership or support from Board of Education or administration
- Lack of time, training or resources

Hall Monitoring: Campus Access

Districts have myriad tools available to secure their buildings and monitor access: **70%** use security cameras, the leading method for monitoring buildings; **32%** use ID cards; **28%** have real-time access to sex offender databases; and **26%** use security teams.

Does your district currently use any of the following methods to monitor or control access to the buildings in your district?



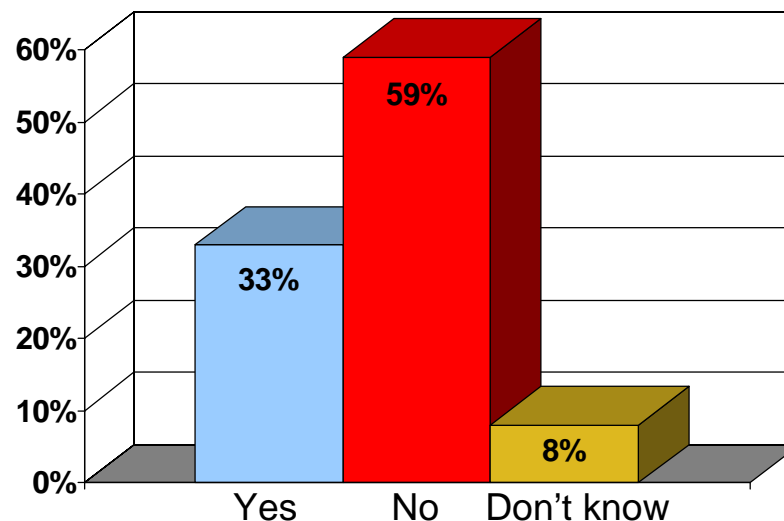
Hall Monitoring: Campus Access

In an emergency, local authorities need as much information about the situation as quickly as possible.

- **33%** of districts take advantage of a key feature of IP cameras by providing local police the ability to access footage during an emergency
- **Extra Credit:** **29%** of districts report that security cameras have made a positive impact on security, and **24%** are considering adding security cameras in their district

Does your district currently use security cameras in or around school buildings?	
Yes	70%
No	29%
Don't know	1%

Can local police access your security camera footage in real time?

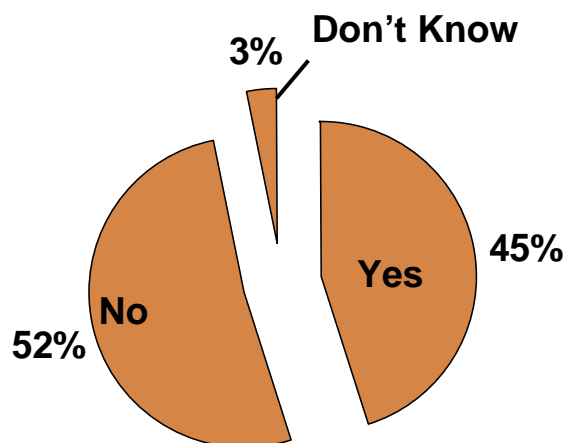


Hall Monitoring: Mass Notification

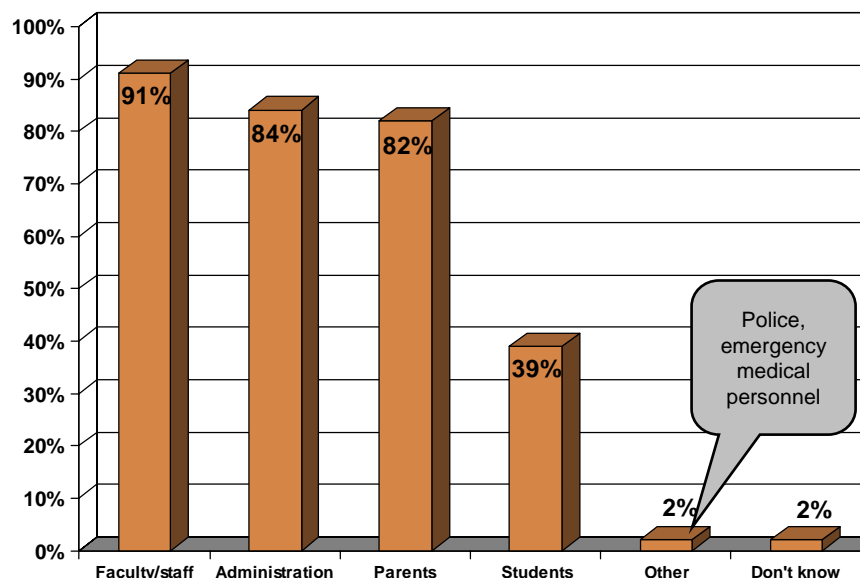
Just as important as working closely with local authorities is alerting faculty, staff, parents, and even students during an emergency. A modern mass notification system (MNS), also known as an emergency alert system, notifies the community about an on-campus emergency or disruption via email, text messages *and* broadcast alerts.

- Despite efforts to improve emergency communications, fewer than half the districts (45%) said they use a MNS
- Most districts' MNS systems target faculty and administrators, but often do not reach all community members

Does your district use a MNS?



Who can receive messages from your district's MNS?



Hall Monitoring: Mass Notification

Mass notification systems have the ability to reach staff, parents and students quickly and wherever they are, but districts are not taking full advantage of their capabilities.

- More respondents said they use their emergency alert systems to relay school closures and weather-related emergencies than for physical threats at the school or lock downs
- Districts push out messages primarily via automated phone systems (**70%**) and email (**61%**), with ***less than 1/3 of districts utilizing newer technologies such as text messages***

Do you use your MNS to alert the community to any of the following?	
School closures	84%
Weather-related emergencies	81%
Physical threat to the school	60%
School lock down	59%
None of the above	7%
Don't know	1%

What are the capabilities of your MNS?	
Automated phone messages	70%
Email alerts	61%
Text message alerts	32%
Sirens/loud speakers	28%
Other*	3%
Don't know	4%

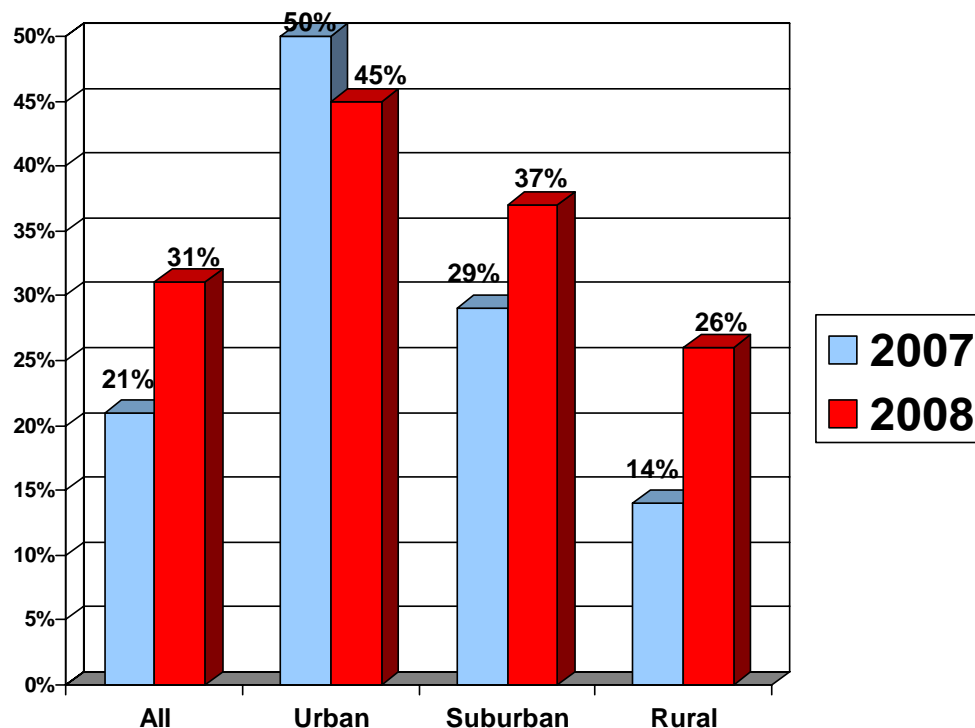
*Other: Phone tree, Instant message and Television



Breaking the Rules: Physical Breaches

Physical security breaches are up **10%** since 2007. Suburban and rural schools saw the greatest increases in incidents over the last 12 months. With shrinking district and state budgets, schools will need to be more vigilant and consider using technology tools in new ways to reduce incidents.

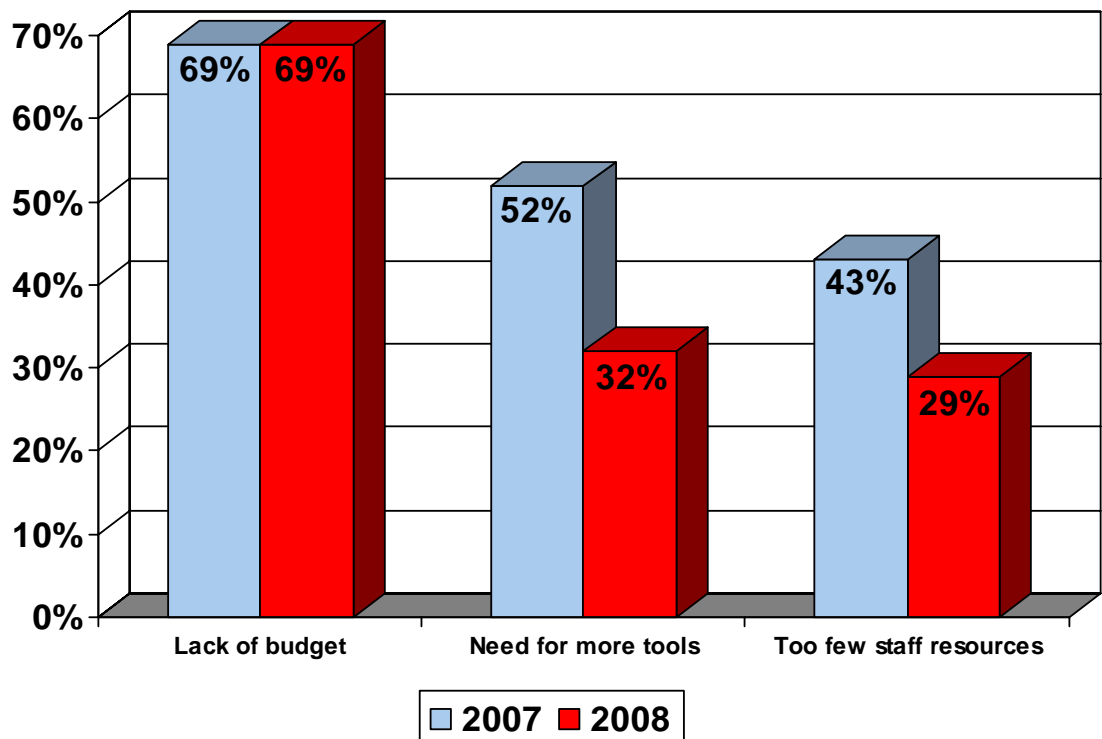
Has your district experienced any breaches in physical security in the last 12 months?



Test Taking: Physical Barriers

As with cyber security, budget remains the biggest barrier to physical security improvements. But availability of advanced technology tools is enabling schools to do more with the same or fewer security staff.

What are the biggest barriers to physical security?



Other Barriers to Improving Physical Security

- Lack of user participation
- Lack of defined policies
- Lack of knowledge about available tools
- Lack of interest

Homework: Calls to Action

- IT and physical security silos are becoming less apparent, yet districts are not making the most of technology advancements. Given the pace of technology change and limited budgets, K-12 school districts need to take advantage of convergence to improve IT and physical security simultaneously by adopting tools like IP cameras, network access control and mass notification systems
- Network access control means that only approved and secured software and hardware make contact with the network. Districts should explore this capability in order to free valuable staff resources to work on more pressing issues and projects
- Districts are using multiple emergency communication channels but need to ensure that information not only is *delivered*, but is *received* as quickly as possible. Comprehensive mass notification systems that use multiple communication methods to reach the community with pre-selected messages enable administrators to focus on the situation at hand, rather than lose valuable time with older, less effective, communication models. Districts should aim to be prepared, so that messages are clear, calm, concise – and timely



Methodology

- QED conducted a phone survey of district IT and security personnel in April 2008
- A total of 403 IT and security personnel from a variety of K-12 public school districts – from urban to rural – completed the survey
- The sample size equates to a +/- 5% margin of error at a 95% confidence level
- Calculating the CDW-G School Safety Index:
 - Each positive indicator question is based on a value of 10
 - Each contraindicator question is based on a value of -10
 - Using the data from the national survey, the percentages were divided by 10, resulting in a numeric value



Respondent Demographics

- Job function:
 - 47% IT director/coordinator
 - 14% Network systems administrator
 - 11% Superintendent
 - 4% Assistant superintendent for network security or emergency planning
 - 7% Chief Information/Technology/Security Officer
 - 4% Director of emergency planning or security
 - 13% Other IT or security title
- Job responsibilities include:
 - 85% IT or network security
 - 52% Emergency communications
 - 46% Emergency planning
 - 39% Building security



Respondent Demographics

- Metropolitan Statistical Area:
 - 5% Urban
 - 39% Suburban
 - 56% Rural
- District Enrollment:
 - 46% 1-999 students
 - 40% 1,000-4,999 students
 - 14% 5,000+ students
- Region:
 - 19% Northeast
 - 24% South
 - 37% Midwest
 - 20% West



Thank You

For all media questions and inquiries, please contact:

*Ryan Kurtz
CDW-G Public Relations
847-968-0211
ryankur@cdw.com*

*Meredith Braselman
O'Keeffe & Company
703-883-9000 ext. 107
mbraselman@okco.com*

www.cdwg.com/schoolsafetyindex

