CDW-G K-12

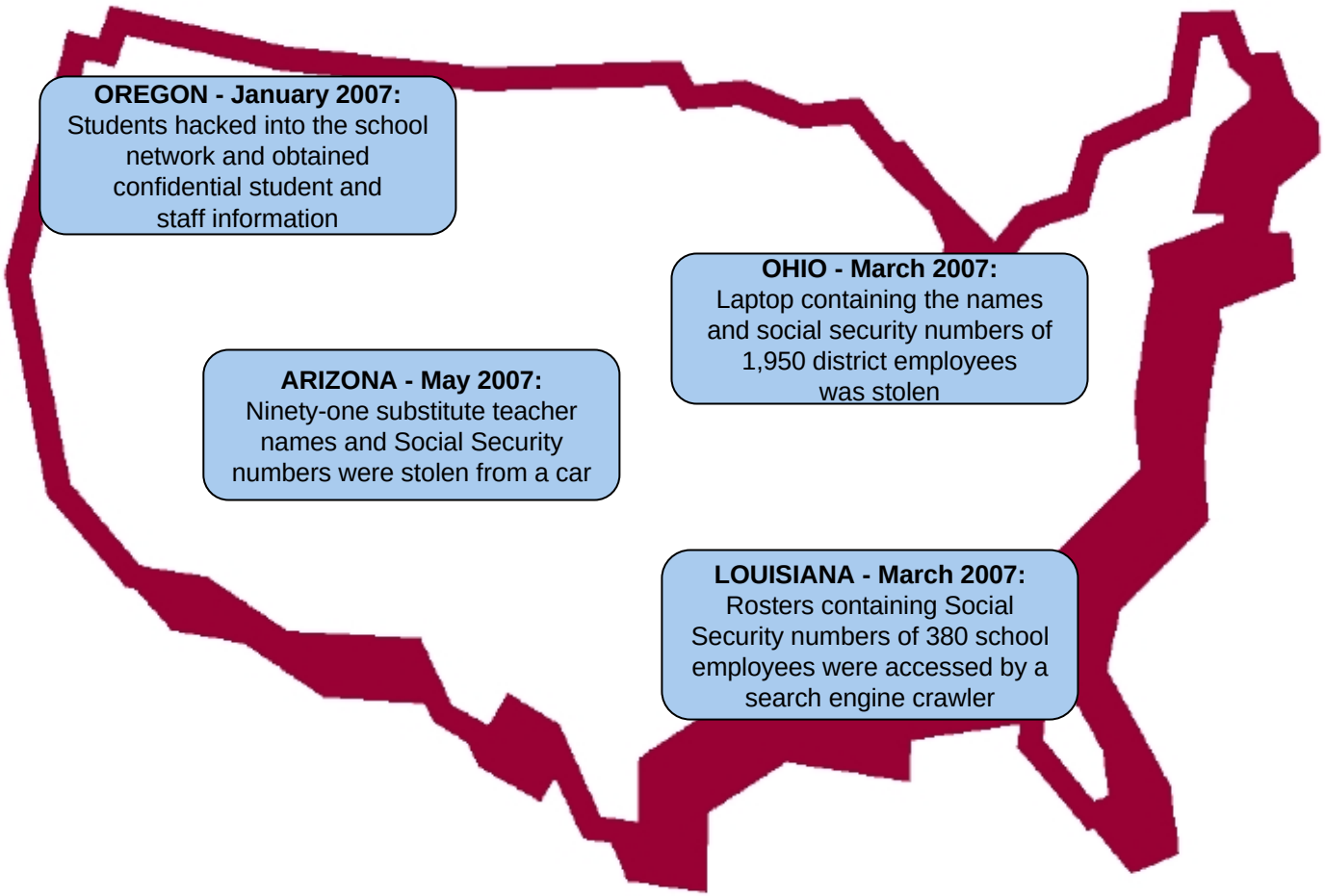
School Safety Index 2007

June 25, 2007

Study Focus and Objectives

- CDW Government, Inc. (CDW-G), the public sector subsidiary of CDW Corporation, worked with Quality Education Data to conduct a survey of K-12 public school district information technology (IT) directors 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

Security Incidents – 2007 Alone



According to the Privacy Rights Clearinghouse, www.privacyrights.org, more than 155 million records* have been stolen since 2005

***Includes Social Security numbers, account numbers, and driver's license numbers**

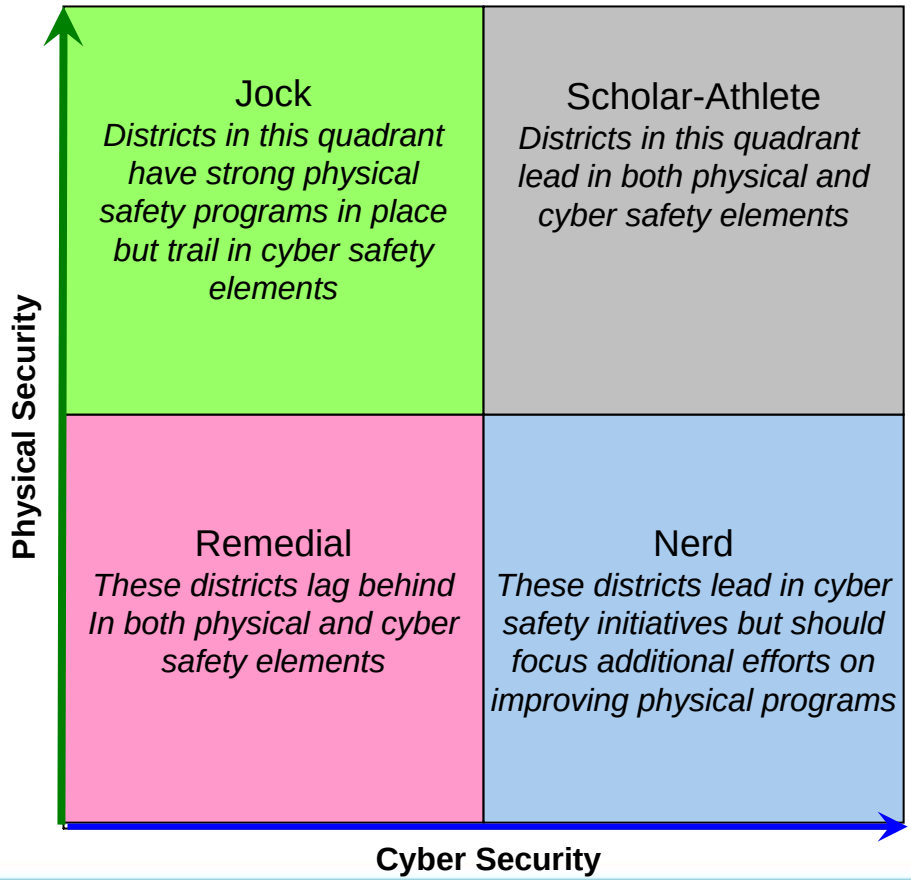
Understanding the Index

Based on research from Quality Education Data, national safety organizations, and CDW-G's market expertise, the CDW-G School Safety Index's 10 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

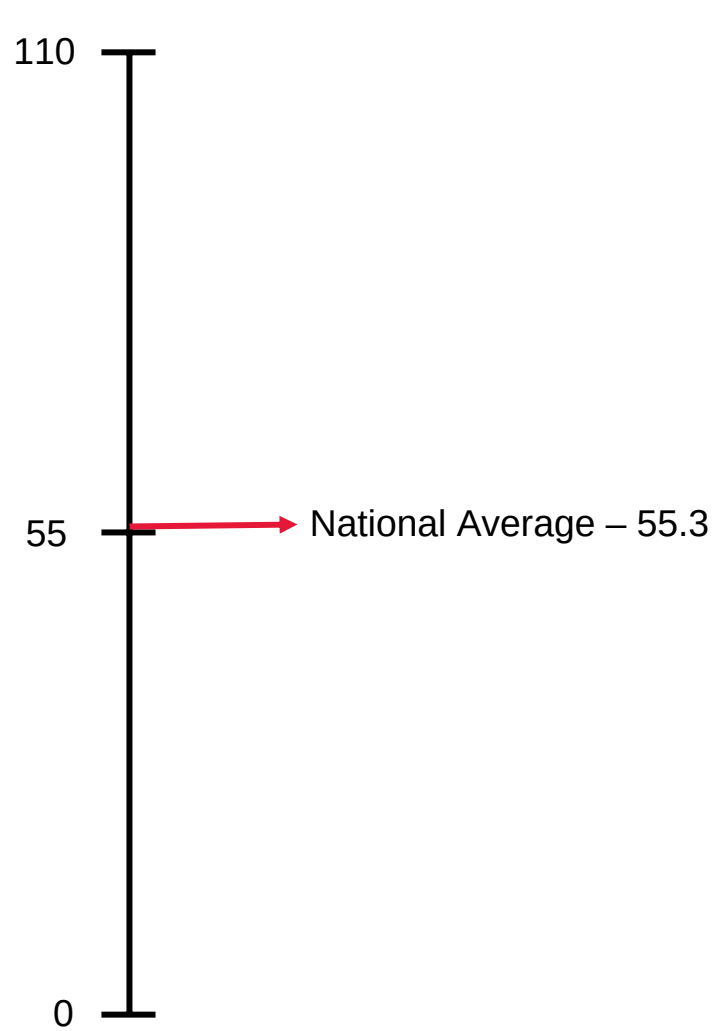
Cyber Security Indicators	Physical Security Indicators
Data Monitoring	Building Access
Network Access	Local Authority Communication
User Authentication	Education
Education	Faculty Communication
Student Protection	Parental Communication
Contraindicators	**Contraindicators**
IT Breaches	Physical Breaches
IT Barriers	Physical Barriers

CDW-G School Safety Index



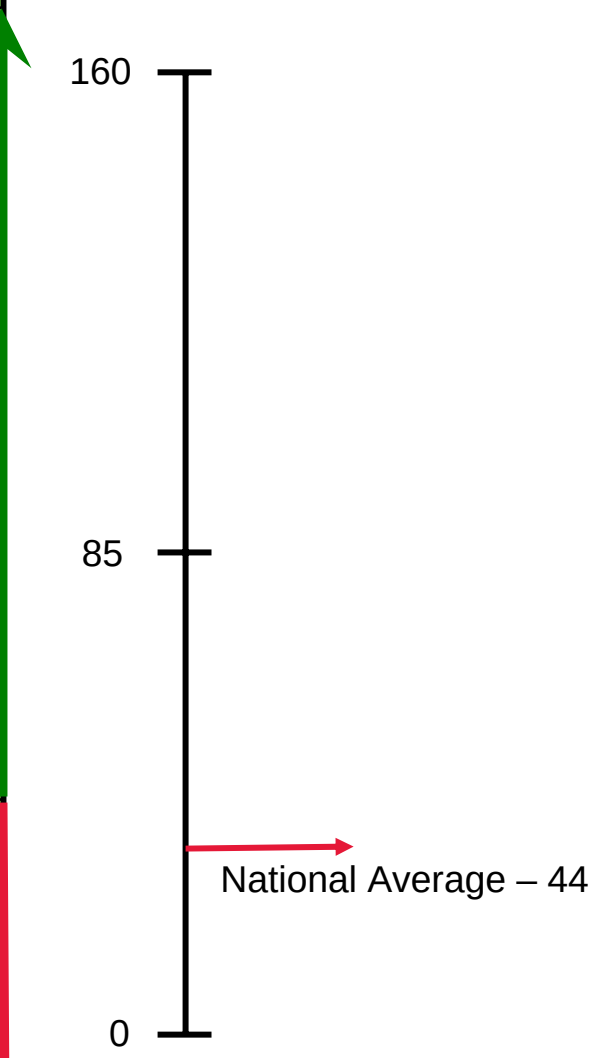
2007 Cyber Safety Index

Element	Question	Yes
Data Monitoring	Does your district monitor access to student records?	82%
Data Monitoring	Does your district monitor access to student e-mail?	40%
Network Access	Does your district restrict access to devices outside its network?	39%
User Authentication	Does your district authenticate users as they access the network?	88%
Education	Does your district update the Acceptable Use Policy at least once a year?	57%
Education	Does your district provide cyber security training?	8%
Student Online Protection	Does your district do any of the following to protect students while they are online: Operate a closed network?	38%
Student Online Protection	Monitor student Internet activity?	81%
Student Online Protection	Place computers within the full view of adult supervisors?	89%
Student Online Protection	Block or limit Web sites?	95%
Student Online Protection	Use filtering software?	33%
IT Breaches	Has your district had an IT breach in the last 12 months?	9%
Cyber Security Barriers	What are your district's main barriers to improving IT security: Budget?	55%
Cyber Security Barriers	Too few human resources?	18%
Cyber Security Barriers	Lack of defined policies?	2%
Cyber Security Barriers	Hardware/Software barriers?	7%
Cyber Security Barriers	Lack of user participation?	6%

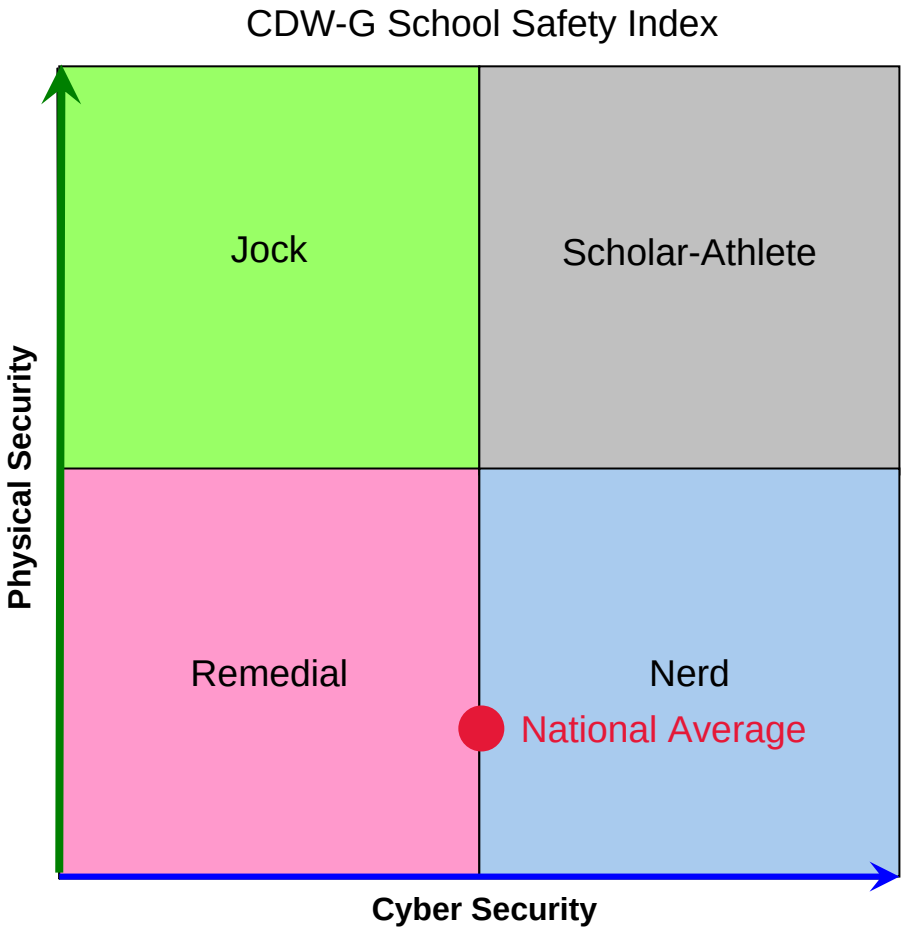


2007 Physical Safety Index

Element	Question	Yes
Building Access	Does your district currently do any of the following to limit access to the facilities? ID Cards?	37%
Building Access	Security cameras?	63%
Building Access	Security team?	24%
Building Access	Metal detectors?	4%
Building Access	Real-time access to sex offender database?	24%
Local Authority Communication	Are the schools in your district connected via the Internet to local response authorities?	35%
Education	Do you have written physical security policies?	44%
Education	Do you review physical security policies with students?	43%
Faculty Communication	How do you communicate with faculty/staff during emergencies: E-mail alert?	31%
Faculty Communication	Phone call?	37%
Faculty Communication	PA/Intercom?	48%
Faculty Communication	Shortwave radio?	19%
Parental Communication	How do you communicate with parents during emergencies: E-mail?	31%
Parental Communication	Phone call?	54%
Parental Communication	Web site?	3%
Parental Communication	Broadcast radio/TV?	12%
Physical Breaches	Has your district experienced any breaches in physical security in the last 12 months?	21%
Physical Barriers	What are your district's main barriers to improving physical security: Budget?	50%
Physical Barriers	Too few human resources?	4%
Physical Barriers	Lack of defined policies?	5%
Physical Barriers	Need for more tools?	13%
Physical Barriers	Lack of user participation?	2%



Key Findings



- **Physical Safety Trails Cyber Safety:**
  - Districts score higher on cyber safety, lacking some of the crucial elements to improve physical safety programs
- **Over-reliance on Technical Solutions:**
  - Districts rely too much on software to protect students, faculty and their networks from threats. Safety education is not a priority
- **Students Challenge IT Staff Technology Skills:**
  - Students know all too well how to side-step security measures. Student-designed proxy servers continue to frustrate IT departments
- **Communication Lags:**
  - The majority of districts still prefer the phone over other methods when communicating emergency information to the community. Many districts cite outdated campus infrastructure as a barrier to using new technology
- **Small Budgets Loom Large:**
  - Districts say that lack of budget, staff resources and proper tools hinder their ability to properly protect themselves

From the Field

In order to gather more insight on the challenges and successes in K-12 security, CDW-G and QED conducted in-depth interviews with district technology directors. Their comments are included throughout the survey.

Roger Geiger
Director of Technology
Forney Independent
School District
Texas

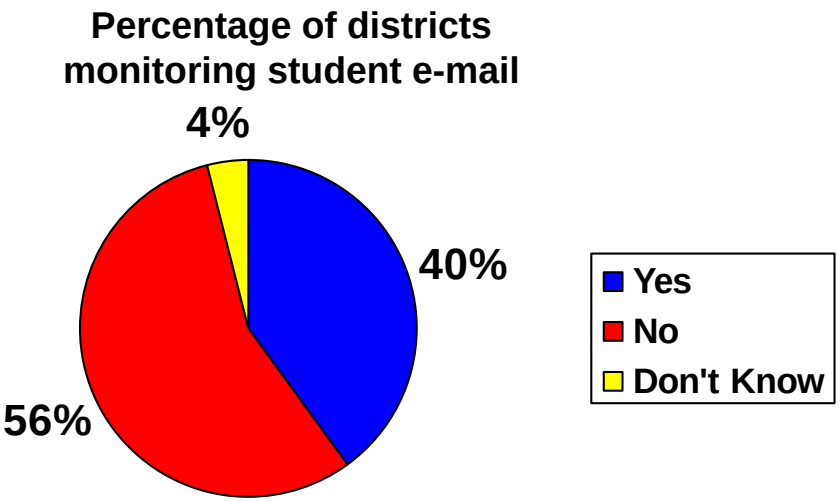
Justin Schaef
Director of Data and Technology
Washingtonville Central
School District
New York

Steve Stewart
Technology Services Director
Boerne Independent
School District
Texas

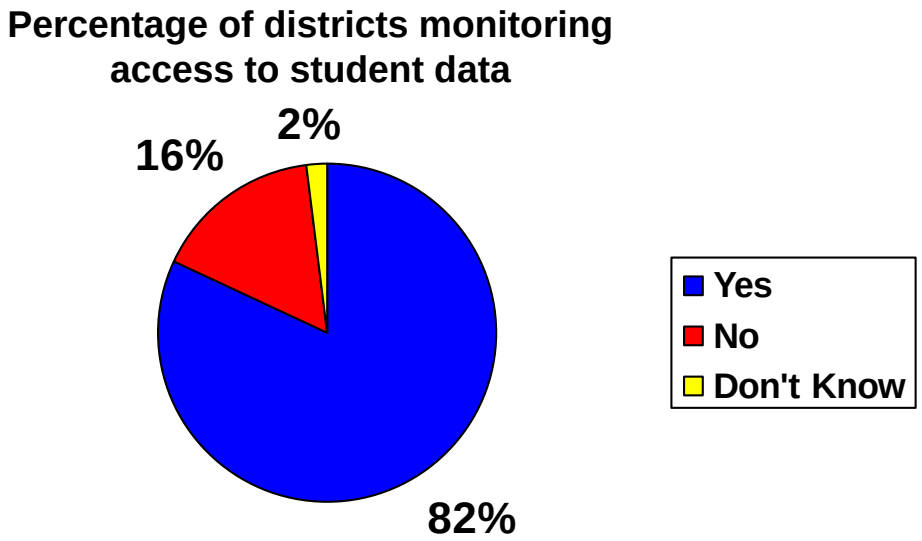
Data Monitoring

Monitoring student e-mail, as well as who is accessing that data, is a first line of defense in keeping networks and students safe, yet:

- **56** percent of districts do not monitor student e-mail
- **16** percent do not keep track of who is accessing student information



Q2c) Does your district monitor student e-mail? N=381

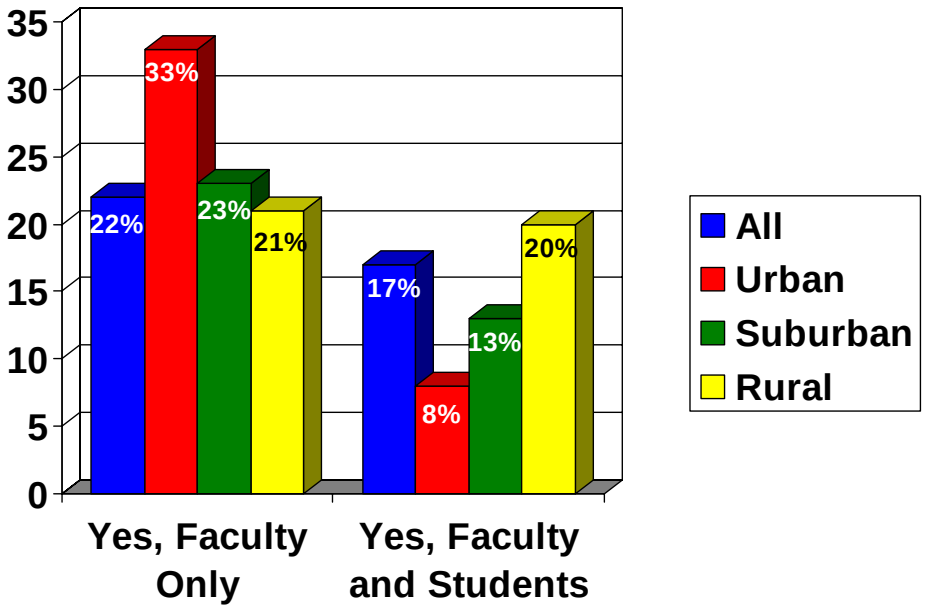


Q2a) Does your district monitor access to student records? N=381

Network Access

Access

39 percent of districts allow outside devices on the network, increasing the chance of introducing viruses and other malware to the network.



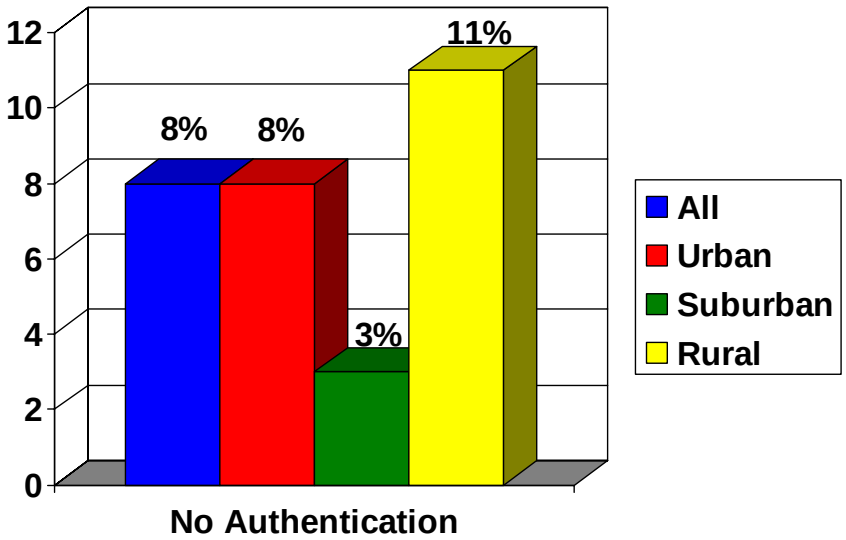
"In the last year, we've prevented faculty and students from installing software. We now remotely push out software because it can be very dangerous when they do this on their own."

Q3) Does your district allow non-district owned devices to access the district's network? N=381

User Authentication

Authentication

- Without proper authentication, districts may not become aware of holes or intrusions until it's too late
- **11** percent of rural districts and **19** percent of western districts do not authenticate users

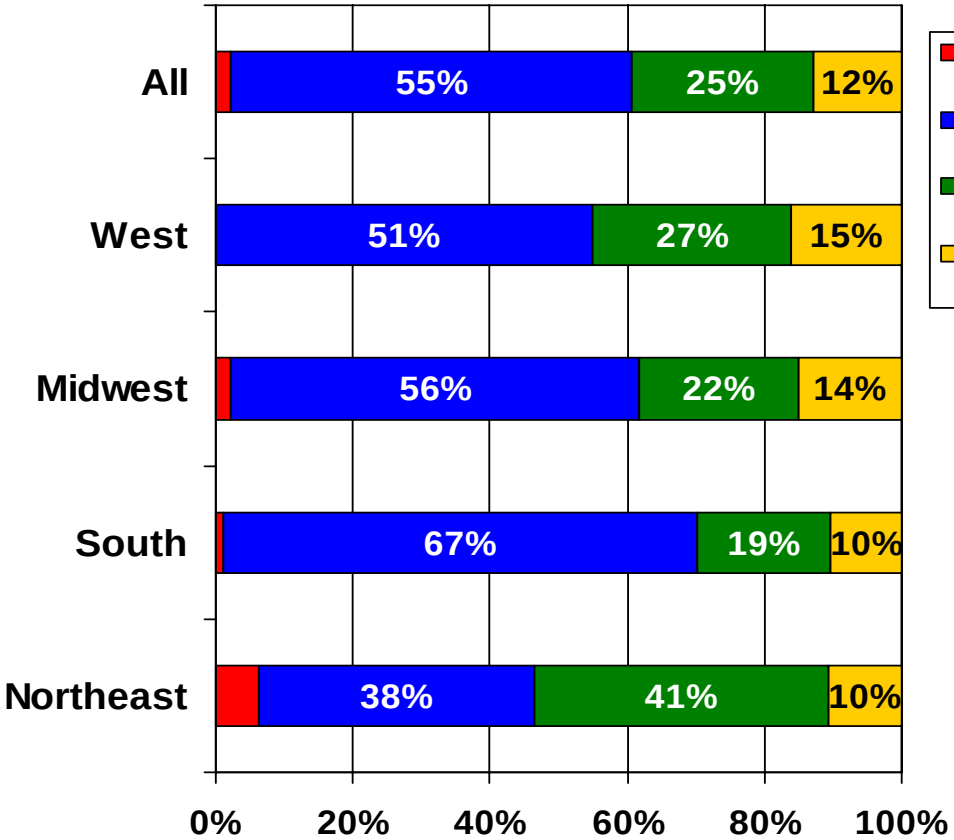


Tactic: Authentication limits the threat of malicious activity on the network. Consider dual-factor authentication with password and revolving key for access to sensitive data

Q3) Does your district authenticate users to the network? N=381

Education

While acceptable use policies (AUP) are nearly universal (**99** percent of districts report having one), **55** percent of districts update AUPs no more than once a year.



Q5b) How often is the AUP updated? N=381

Tactics: AUPs should be treated as living documents, posted on district Web sites, and updated as often as necessary.

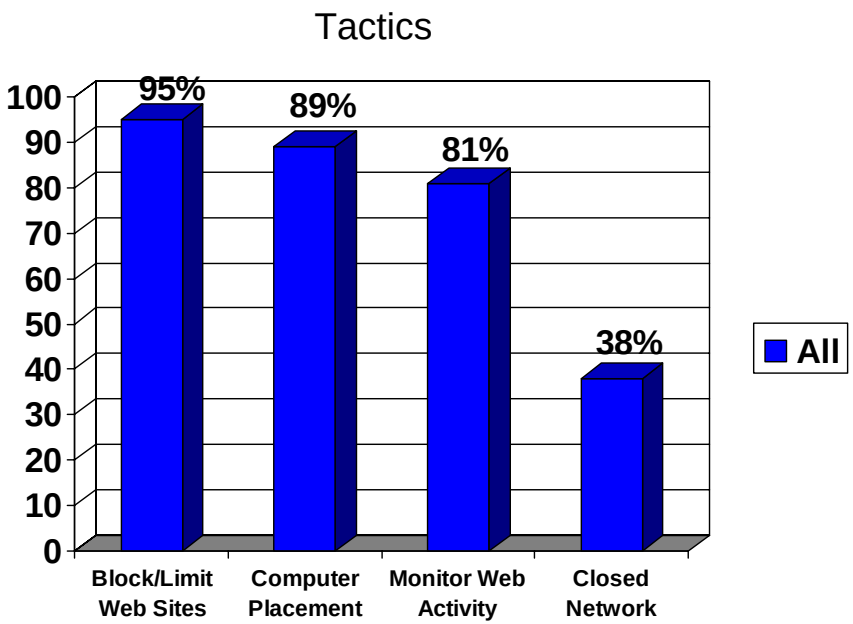
All users should sign an AUP before receiving access to district computers and networks.

Educate students and teachers throughout the year about online safety.

Network Protection

Top district IT safety programs

- 95 percent block or limit Web sites
- 89 percent place computers in view of adults
- 81 percent monitor student Web activity
- 38 percent maintain a closed district network



Tactic: Many districts are turning to closed networks to limit access to only filtered content and to monitor e-mail communication.

Districts can also evaluate Web sites on a regular basis to block them or make sites available, protecting First Amendment rights.

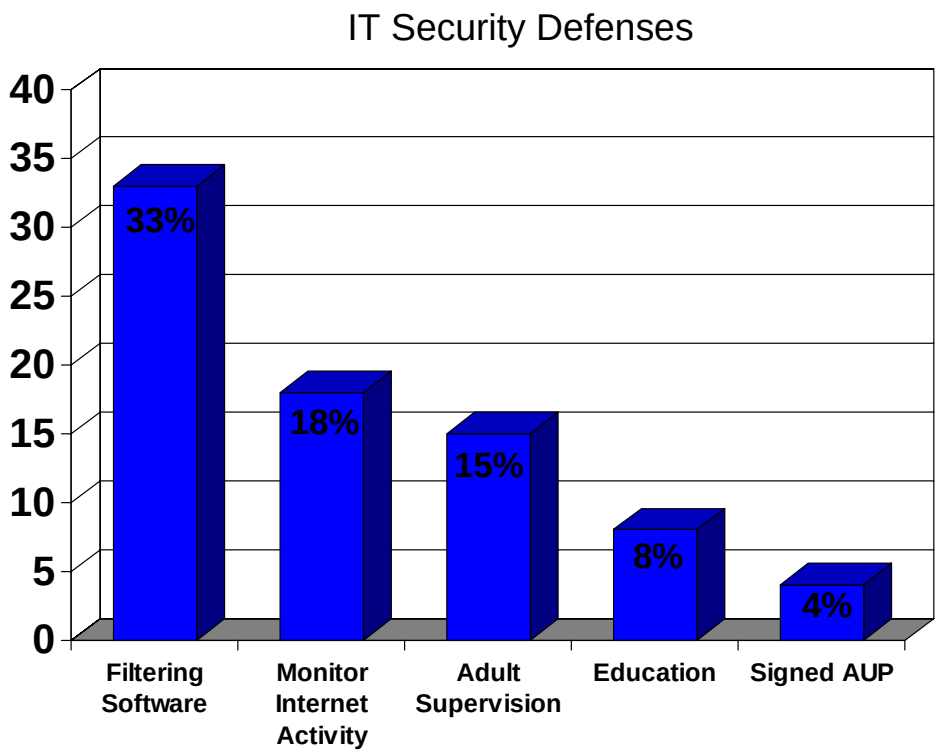
Q9b) Does your district do any of the following to protect students while they are online at school? N=381

Network Protection

Districts rely on filtering software as a primary defense method. More districts could benefit from using safety education as a tool to improve security.

Tactic: Filtering software is not a substitute for educating students, parents and staff about the dangers of the Internet. Districts need to engage the entire community in the IT security process.

"I would say that we're constantly looking for ways to improve. At a minimum, [these new technologies] take a lot of management. What we're looking for as technology evolves are new ways to defend."



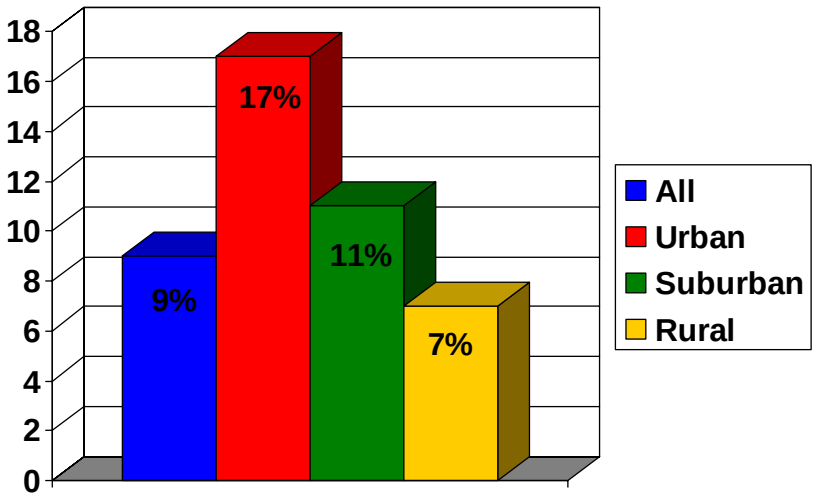
Q10) What are some additional ways your district protects students while they are online? N=375

IT Breaches

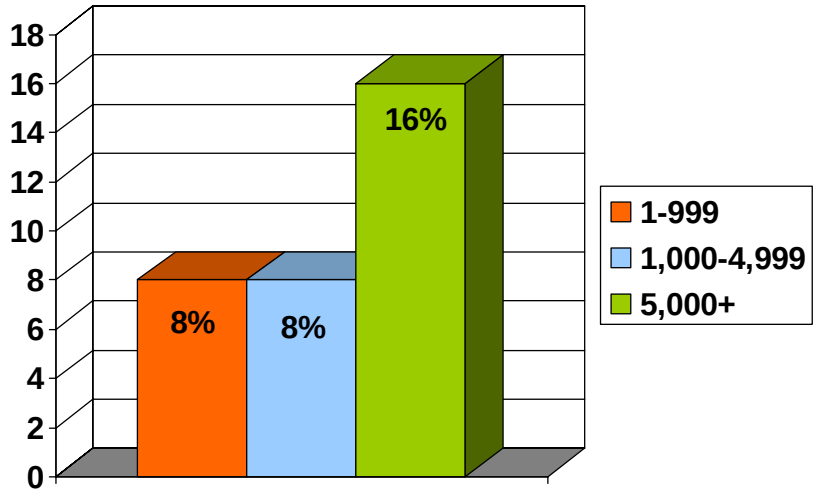
9 percent of districts report at least one IT security breach in the last 12 months.

- Urban and large districts are at greater risk
- **6** percent of districts say their networks are somewhat or very vulnerable to attack

Breaches by Metropolitan Area



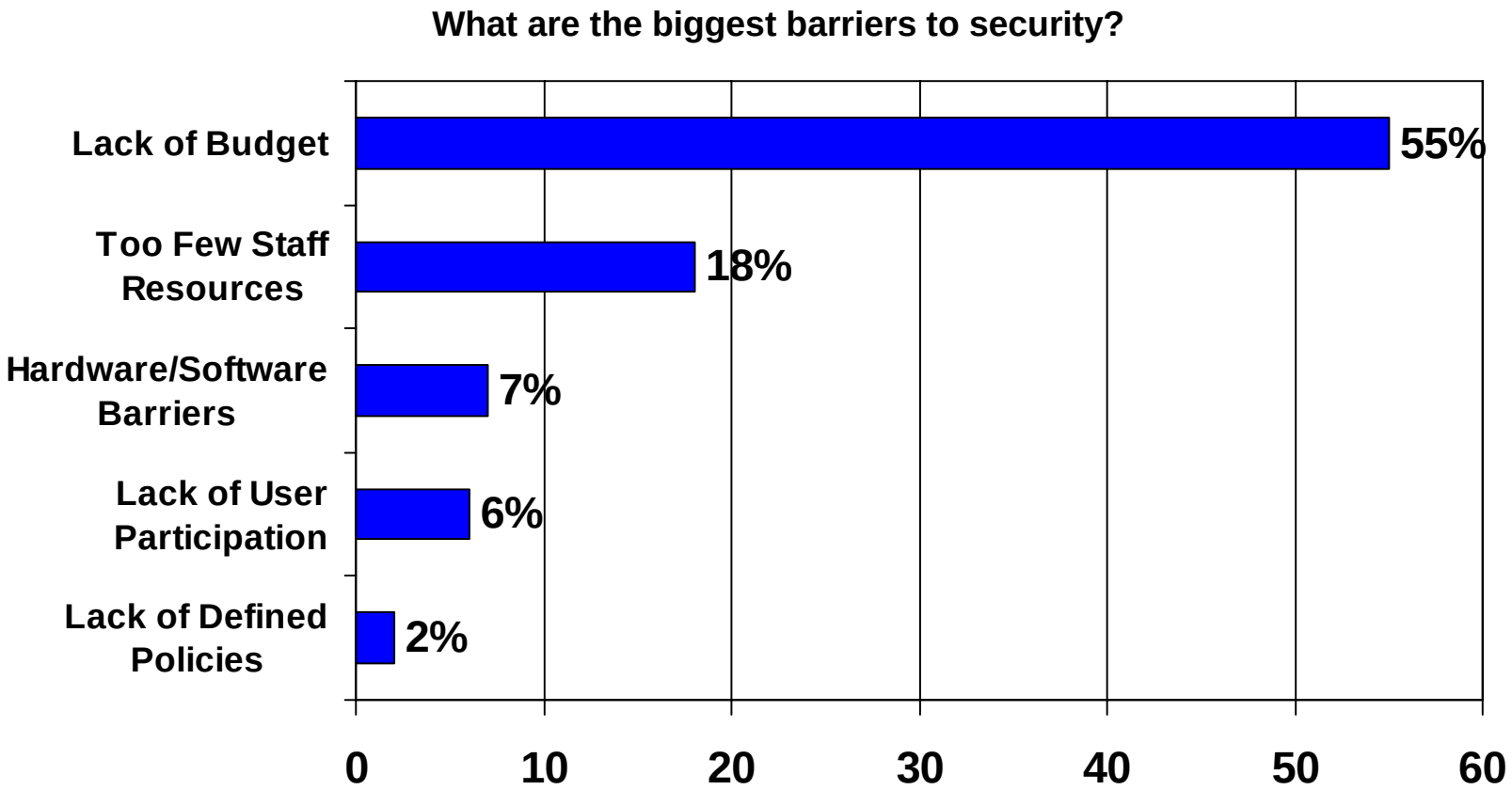
Breaches by Enrollment



Q7) Have you experienced any breaches in IT security in the last 12 months?

IT Barriers

Respondents say that a lack of funding and sufficient staff resources are the biggest barriers to improving district security.

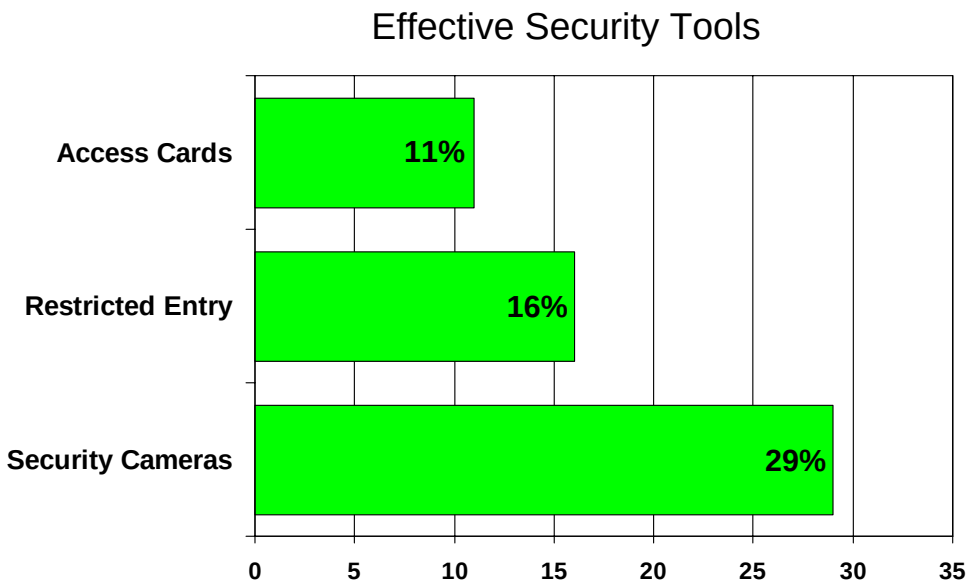


Q11a) What are your district's main barriers to Improving IT security?

Campus Access

At **63** percent, security cameras are the preferred access control method among districts.

- Cameras, restricted entry and access cards are cited as having the most effective impact on physical security
- Retrofitting older buildings can be costly, hampering improvement efforts, forcing many schools to still use traditional locks and keys



Tactic: Most districts do not have real-time access to sex offender registries. Districts can add another level of security by cross-checking visitors with the registry before granting visitors access to campuses.

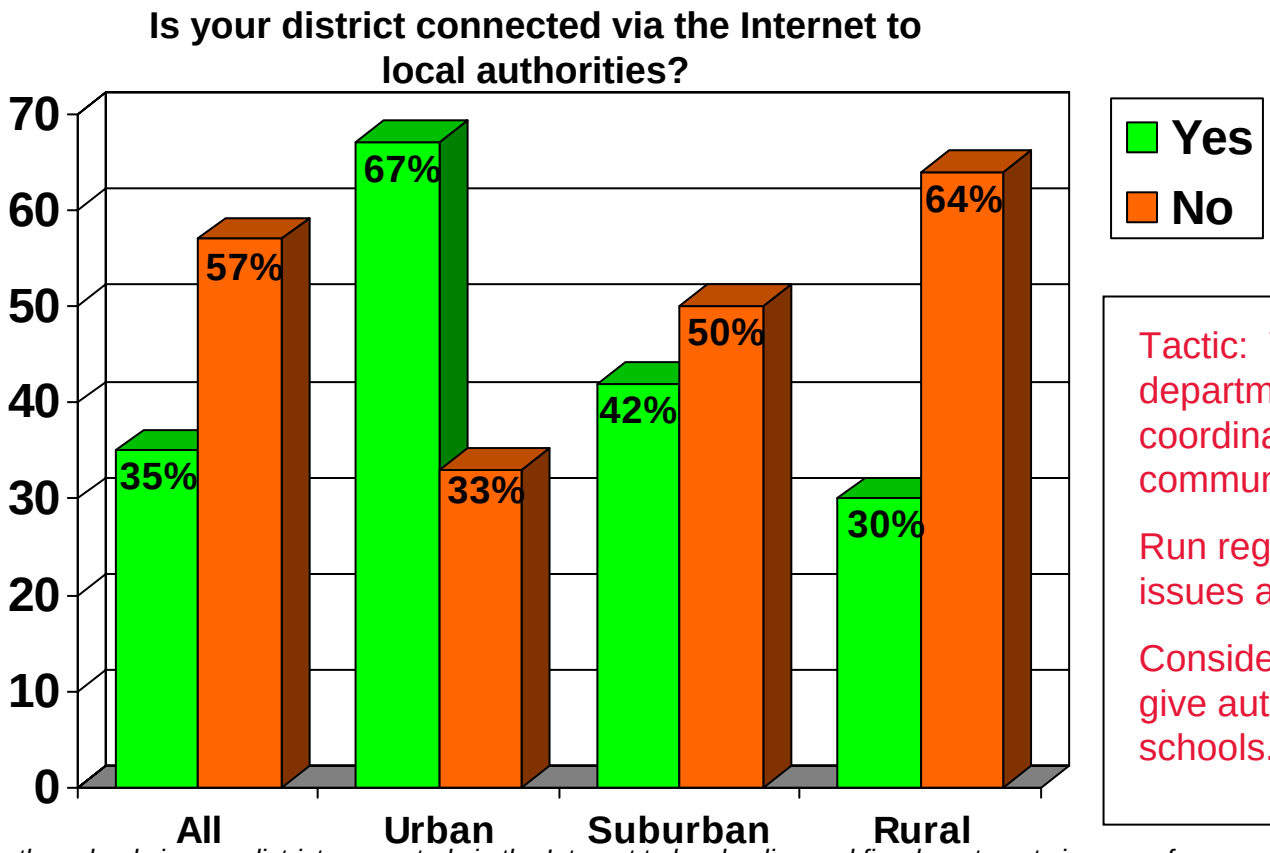
Q19) Does your district currently use any of the following methods to monitor or control access to the buildings in your district? N=381

Q22) What changes implemented by your district have made a positive impact in physical security? N=381

Local Authorities

During an emergency, real-time access and instant communication with local authorities improves response time and the ability to quickly address situations.

- Only **35** percent of districts are connected to authorities



Tactic: Work with local fire departments and police to coordinate emergency plans and communication.

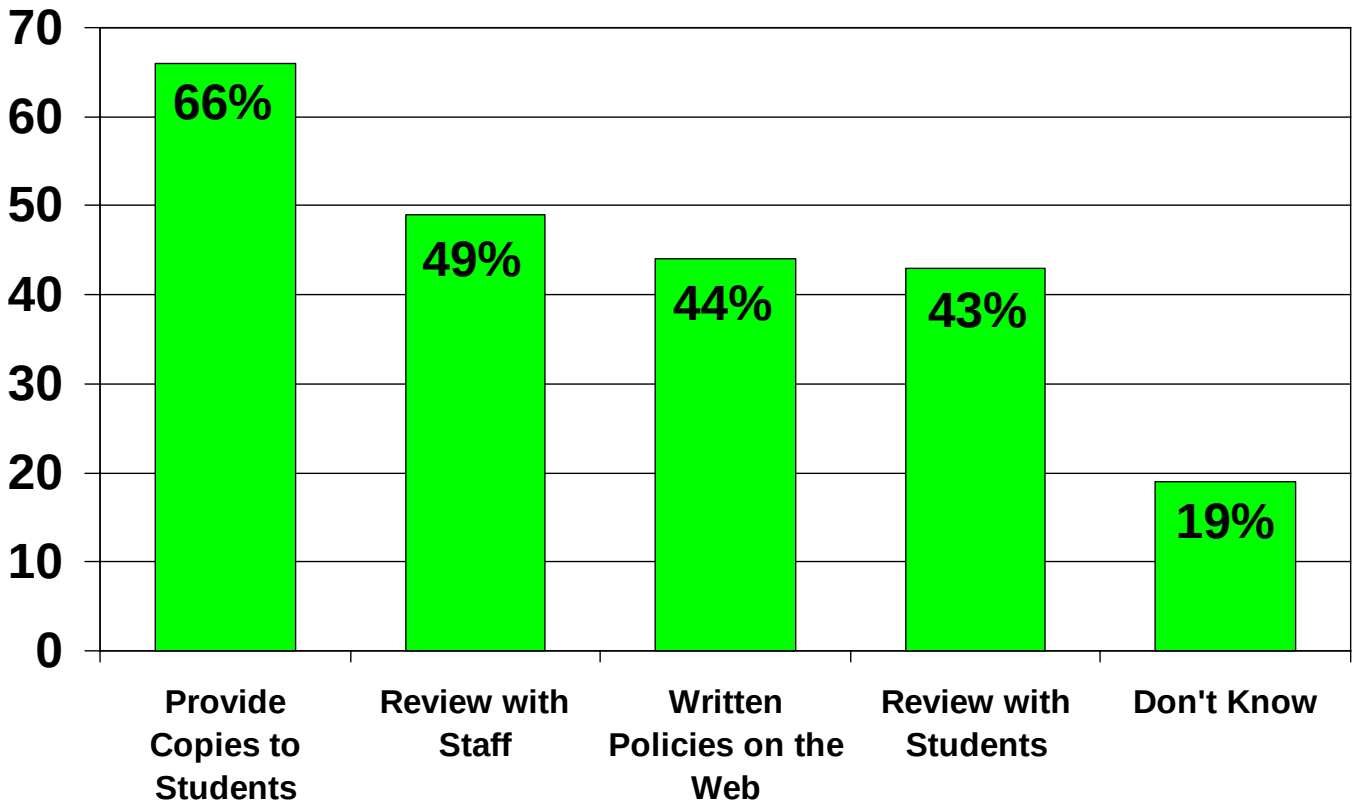
Run regular mock drills to work out issues ahead of time.

Consider IP security cameras to give authorities an "inside view" of schools.

Q24) Are the schools in your district connected via the Internet to local police and fire departments in case of emergencies? N=381

Education

How do districts educate and communicate with students, parents, staff and the public about physical security policies?



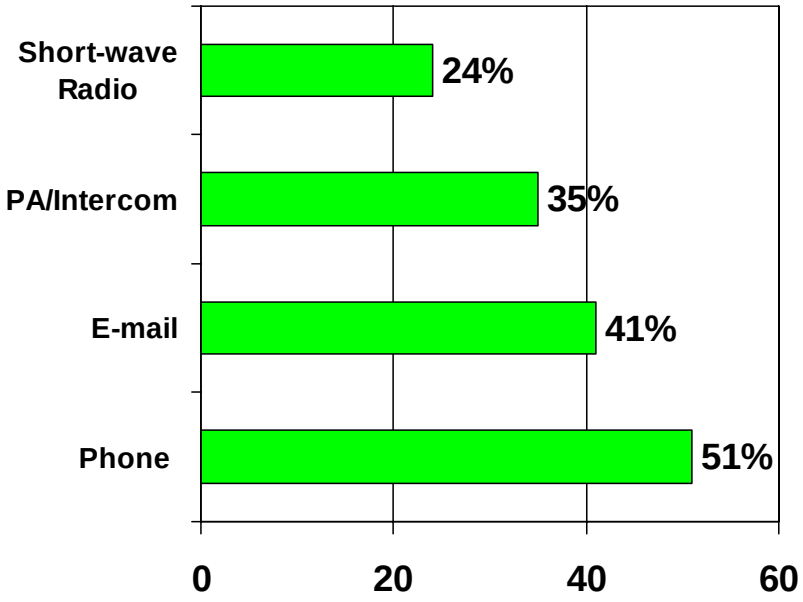
Q18) In what ways does your district education parents, students, teachers or the public about physical security policies? N=381

Faculty Communication

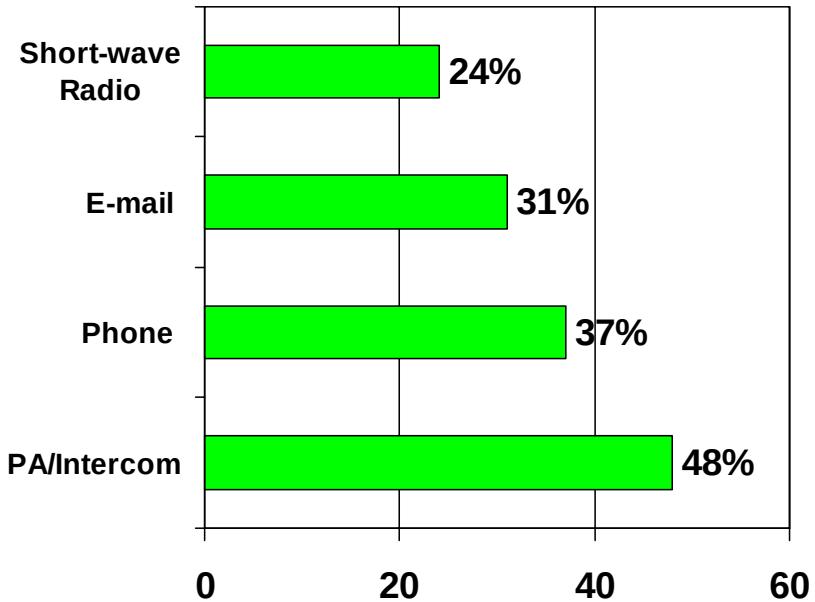
Districts rely heavily on traditional communication methods, like the phone and intercom, to reach faculty during emergencies.

- Less than **3** percent of districts use cell phones as a tool

Weather-related Faculty Communication



Emergency-related Faculty Communication



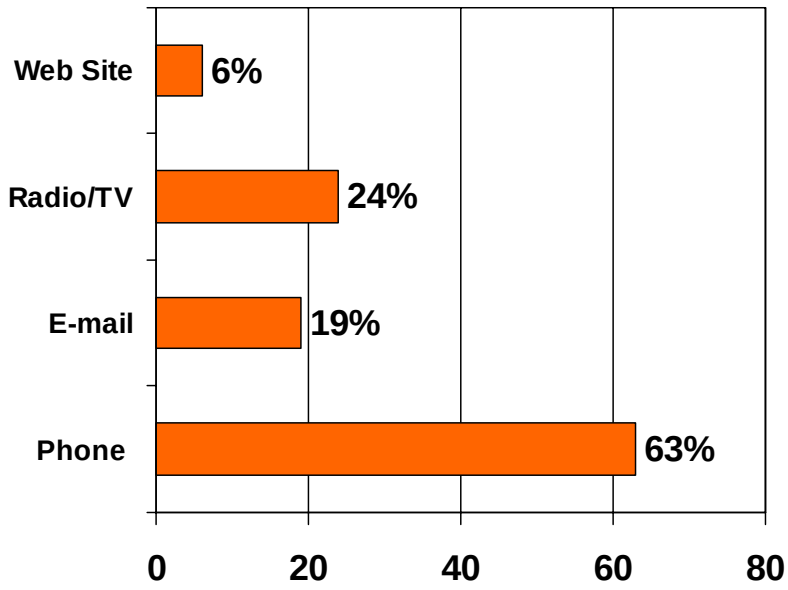
Q25) In a weather emergency, during school hours, how does your district communicate with faculty? N=381

Parent Communication

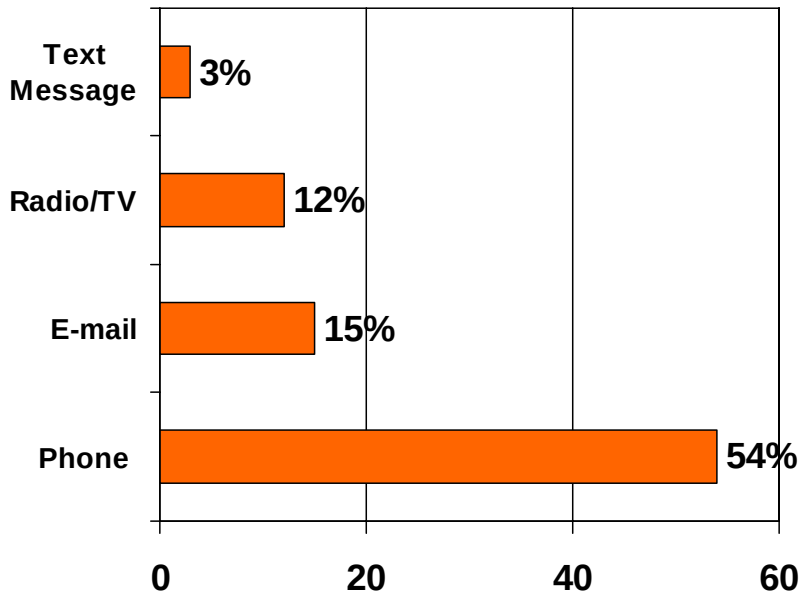
To reach parents during emergencies, districts use the phone far more than any other communication tool.

- Only **1** percent of districts report that they are considering emergency alert/notification systems that send e-mail and text messages to pre-selected groups

Weather-related Parent Communication



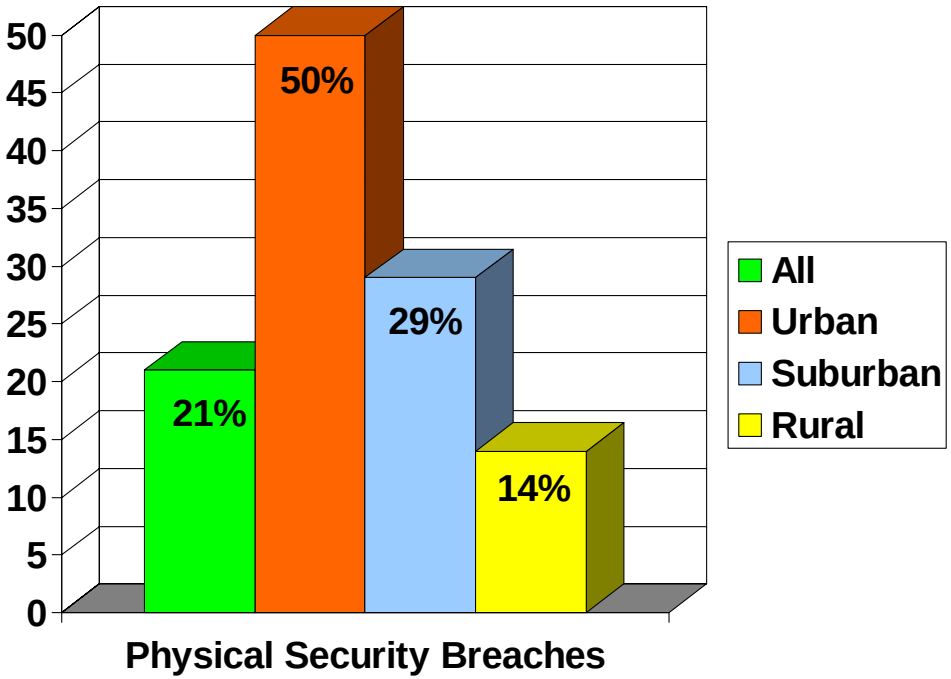
Emergency-related Parent Communication



Q26) In a weather emergency, during school hours, how does your district communicate with parents? N=381

Physical Breaches

21 percent of districts report experiencing a physical security breach in the last 12 months; **50** percent of urban districts have had a breach.



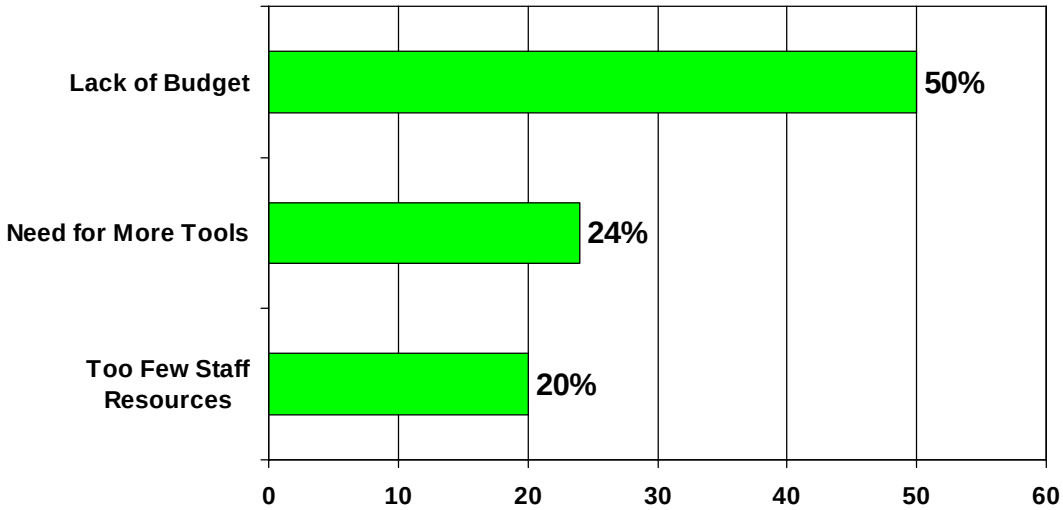
"Physical security has definitely been on our radar screen for a while. Columbine was, I think, the catalyst that has really increased security awareness."

Q23) Has your district experienced any breaches in physical security in the last 12 months? N=381

Physical Barriers

Respondents say a lack of budget, tools and staff are the biggest barriers to improving physical security.

What are the biggest barriers to physical security?



"We've done a lot of planning and thinking and some practicing, and what led to all that was our growth. We're growing so fast that we've had to sit down and really think about the issues we will have to face in the future."

Q11a) What are your district's main barriers to Improving physical security? N=381

Call to Action

- Whether it's physical or cyber security, threats will continue to become more sophisticated. Districts must recognize that, while they may not be able to stop everything, a solid framework, the right tools and proper planning will head off many threats and keep districts ahead of the game

- Understanding the total financial impact of a major security breach – costs associated with technology, downtime, staff time spent on recovery, communications and public relations, legal action, etc. – can help leaders make the business case for additional funding for the tools and resources that may prevent or mitigate security breaches

- Utilizing peers and the vendor community is an effective way to understand new methods and best practices to secure districts. Often, new programs will yield greater return on investment and can enhance the long-term safety of a district

- Take action to help students, faculty and parents understand the benefits and dangers of the online world. Educate students about the potential long-term negative impact that inappropriate content and behavior can have on their collegiate and career plans. Additionally, help faculty see cyberspace as a tool for greater student engagement and safety

Methodology

- QED conducted the online study of district IT and security personnel between May 9 - 29, 2007
- A total of 381 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

How Does Your District Rate?

Cyber Security	Score
Does your district monitor access to student records?	
Does your district monitor access to student e-mail?	
Does your district restrict access to devices outside its network?	
Does your district authenticate users as they access the network?	
Does your district update the Acceptable Use Policy at least once a year?	
Does your district provide cyber security training?	
Does your district do any of the following to protect students while they are online: Operate a closed network?	
Monitor student Internet activity?	
Place computers within the full view of adult supervisors?	
Block or limit Web sites?	
Use filtering software?	
Has your district had an IT breach in the last 12 months?	
What are your district's main barriers to improving IT security: Budget?	
Too few human resources?	
Lack of defined policies?	
Hardware/Software barriers?	
Lack of user participation?	
TOTAL SCORE out of 110	

Answer the following questions to see where your school or district falls on the cyber portion of the CDW-G School Security Index.

A yes answer for each blue question earns 10 points.
A no answer earns 0 points.

A yes answer for each red question earns -10 points.
A no answer earns 0 points.

National Cyber Average – 55.3

How Does Your District Rate?

Physical Security	Score
Does your district currently do any of the following to limit access to the facilities? ID Cards?	
Security cameras?	
Security team?	
Metal detectors?	
Real-time access to sex offender database?	
Are the schools in your district connected via the Internet to local response authorities?	
Do you have written physical security policies?	
Do you review physical security policies with students?	
How do you communicate with faculty/staff during emergencies: E-mail alert?	
Phone call?	
PA/Intercom?	
Shortwave radio?	
How do you communicate with parents during emergencies: E-mail?	
Phone call?	
Web site?	
Broadcast radio/TV?	
Has your district experienced any breaches in physical security in the last 12 months?	
What are your district's main barriers to improving physical security: Budget?	
Too few human resources?	
Lack of defined policies?	
Need for more tools?	
Lack of user participation?	
TOTAL SCORE out of 160	

Answer the following questions to see where your school or district falls on the physical portion of the CDW-G School Security Index.

A yes answer for each green question earns 10 points. A no answer earns 0 points.

A yes answer for each red question earns -10 points. A no answer earns 0 points.

National Physical Average – 44

Respondent Demographics

- Job function:
  - 54% IT director/coordinator
  - 14% Network systems administrator
  - 7% Assistant superintendent for network security or emergency planning
  - 5% Chief Information/Technology/Security Officer
  - 2% Director of emergency planning or security
  - 18% Other IT or security title

- Job responsibilities include:
  - 88% IT or network security
  - 45% Emergency communications
  - 41% Emergency planning
  - 39% Building security

Respondent Demographics

- Metropolitan Statistical Area:
  - 4% Urban
  - 39% Suburban
  - 57% Rural
- District Enrollment:
  - 21% 1-999 students
  - 48% 1,000-4,999 students
  - 41% 5,000+ students
- Region:
  - 17% Northeast
  - 24% South
  - 38% Midwest
  - 21% West

Thank You

For all questions and inquires, please contact:

Barbara Crystal
CDW Public Relations
847-968-0710
bcrystal@cdw.com

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