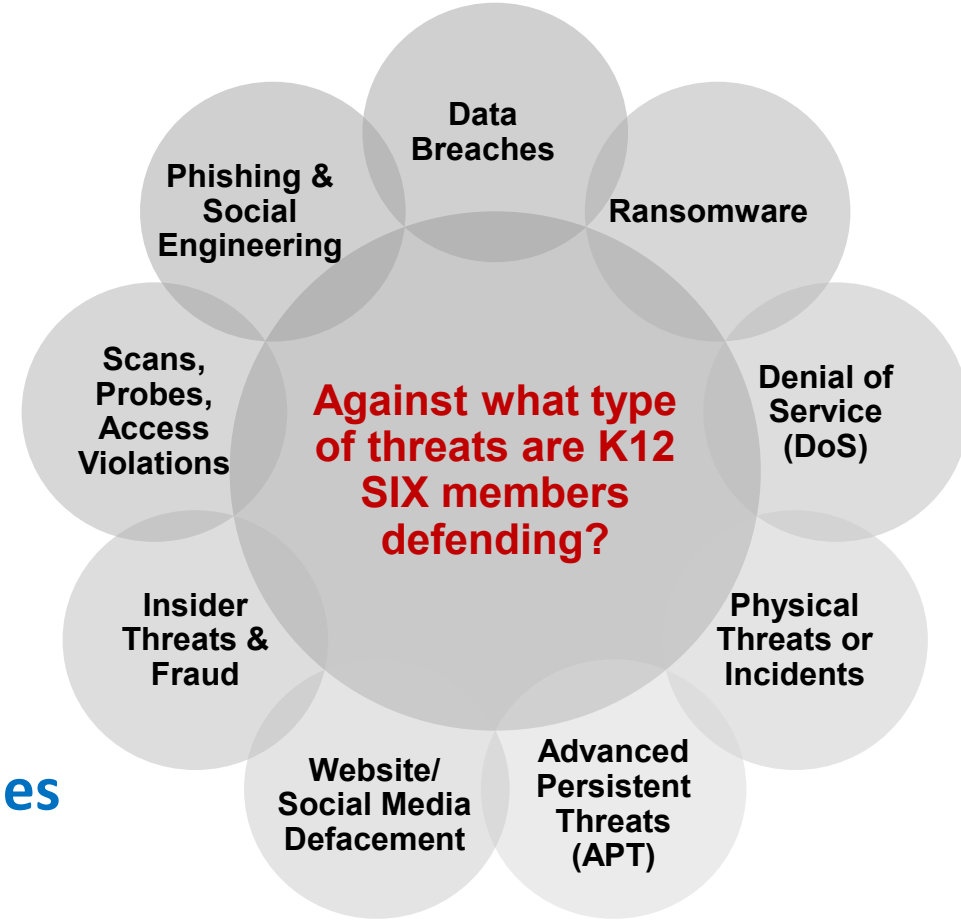
Beyond IT: Building Cabinet Buy-in for a ‘Zero Trust’ Cybersecurity Program

K12 SECURITY INFORMATION EXCHANGE (K12 SIX)

MAY 3, 2023

K12 Security Information eXchange (K12 SIX)

- A Global Resilience Federation (GRF) member community, K12 SIX is a real-time cyber threat intelligence sharing hub ***exclusively for schools***, to aid in preventing and mitigating cyber threats.
- This non-profit member community provides cost-effective collective defense by crowdsourcing security information among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis from the K12 SIX security team.



Collective defense | Best practices | Model policies
Professional development | Advocacy

https://www.k12six.org/member-benefits

Today's Sponsor

Learn more at: https://www.iboss.com/education/

Today's Speakers

Paul Martini
CEO/CTO & Co-founder
iboss

Lenny Schad
Chief Information and Innovation Officer
District Administration

Richard Quinones
Senior Vice President, Public Sector
iboss

Julie A. Evans, Ed.D.
Chief Executive Officer
Project Tomorrow

Beyond IT:

Building Cabinet Buy-in for a

“Zero Trust” Cybersecurity Program

Beyond IT: Building Cabinet Buy-in for a "Zero Trust" Cybersecurity Program

Why is cabinet buy-in important today?

It is time to think beyond just the technology and to understand the critical role of people and process in effective cybersecurity planning and preparation.

Beyond IT: Building Cabinet Buy-in for a "Zero Trust" Cybersecurity Program

Setting the context for our discussion:

Examining evidence from the **iboss – Project Tomorrow** annual research on the views of district leaders about K-12 cybersecurity awareness and preparation

iboss-Project Tomorrow Research on Cybersecurity

Spring 2022 National Findings

1,290 K-12 leaders completed a Project Tomorrow Speak Up survey to provide input and feedback on cybersecurity in spring 2022

Diversified set of stakeholders:

- **69% were K-12 Technology Leaders**
  - 33% identified as being a CIO, CTO or CISO within their district
- **20% were District Administrator Leaders who did not have technology titles**
  - 43% identified as being a Superintendent or Assistant/Deputy Superintendent
- **11% were District PR/Communications Leaders**

iboss-Project Tomorrow Research on Cybersecurity

Cyber and ransomware attacks in K-12 schools and districts are happening with greater regularity now.

Anytime, anywhere learning – impact on cybersecurity

Technology leaders report on top ed tech initiatives:

- 1:1 device assignment to students – to use in school and to take home (55% say this now district policy)
- Use of Google for Education apps in the classoom (48%)
- Cloud applications that are primarily student and teacher facing apps (47%)

Anytime, anywhere learning – impact on cybersecurity

What types of cloud applications for instructional uses?

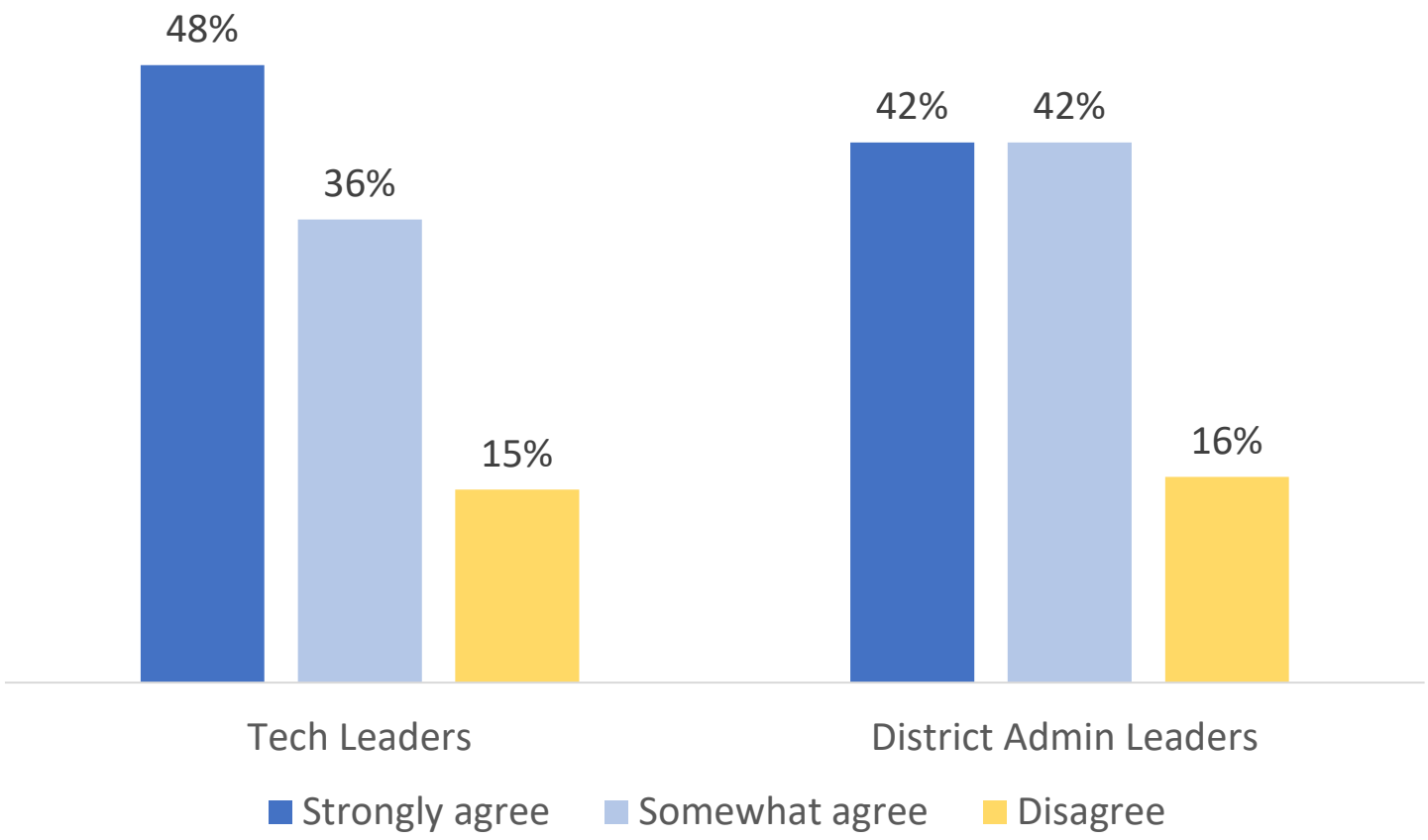
- ✓ Online courses (61%)
- ✓ Learning management system (59%)
- ✓ Online curriculum portal (56%)
- ✓ Student information system (56%)
- ✓ School portal for parent and student usage (56%)
- ✓ Digital content repository (54%)
- ✓ Gradebook (53%)
- ✓ Collaboration and productivity tools (44%)

Anytime, anywhere learning – impact on cybersecurity

What types of cloud applications for instructional uses?

- ✓ **Online courses (61%) – 32% growth since 2018**
- ✓ Learning management system (59%)
- ✓ **Online curriculum portal (56%) – 30% growth since 2018**
- ✓ Student information system (56%)
- ✓ School portal for parent and student usage (56%)
- ✓ Digital content repository (54%)
- ✓ Gradebook (53%)
- ✓ Collaboration and productivity tools (44%)

iboss-Project Tomorrow Research on Cybersecurity



Agree or disagree:

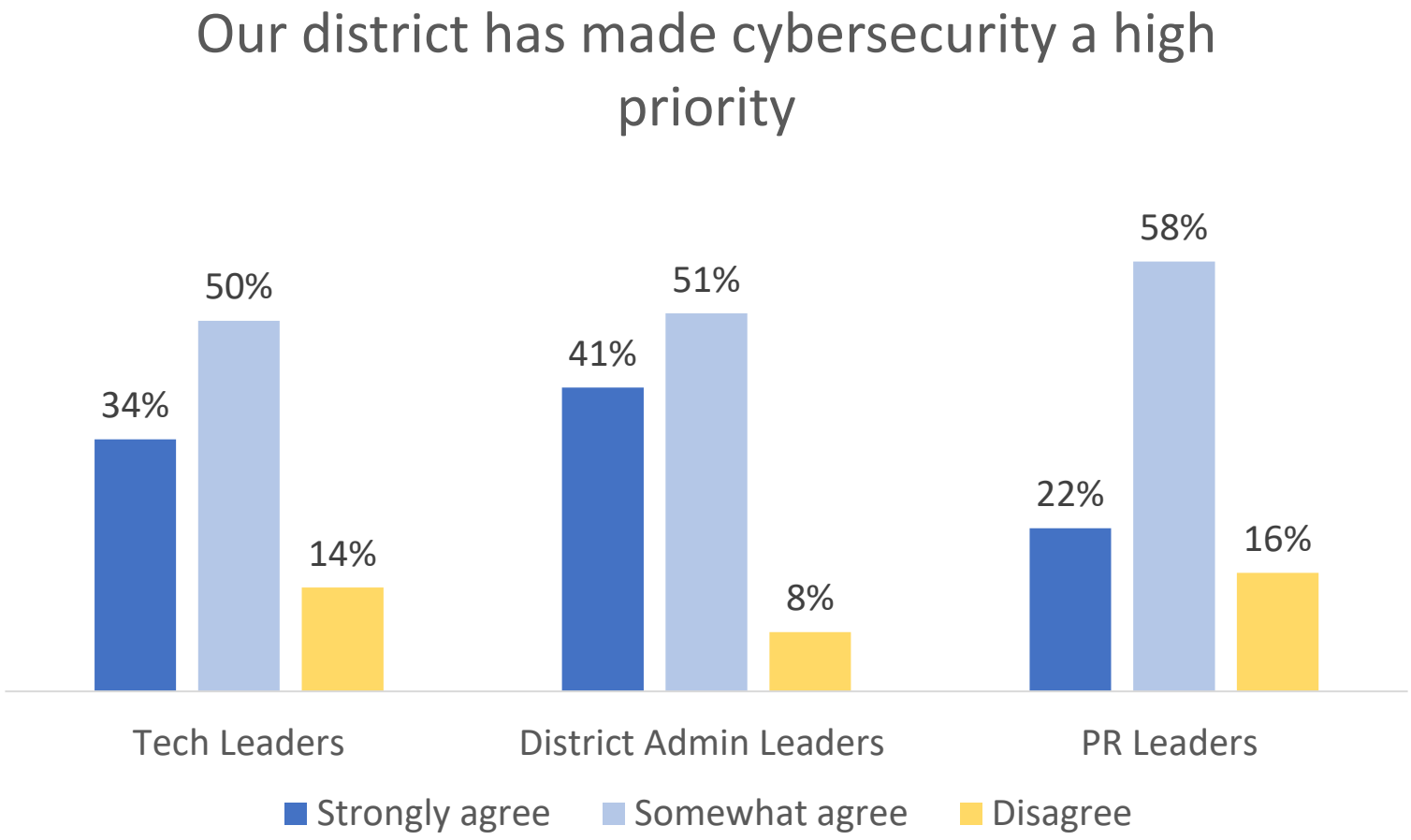
"Our nation's K-12 schools and districts are at a higher risk now for a cyber attack than ever before."

Do you personally know of a school district that has had a cyberattack within the past 12 months?

- **Yes - 85% of Technology Leaders**
  - *30% say it has happened in their district.*
- **Yes - 73% of District Administrators**
  - *30% say it has happened in their district.*
- **Yes - 78% of District Communication Leaders**
  - *20% say it has happened in their district.*

Talking the talk, but not yet walking the talk.

Technology Leaders say cybersecurity is a top concern . . .but their districts are not making cybersecurity policies and procedures a high priority yet.



iboss-Project Tomorrow Research on Cybersecurity

Findings: Is meaningful action taking place?

What are you doing to reduce your vulnerability?

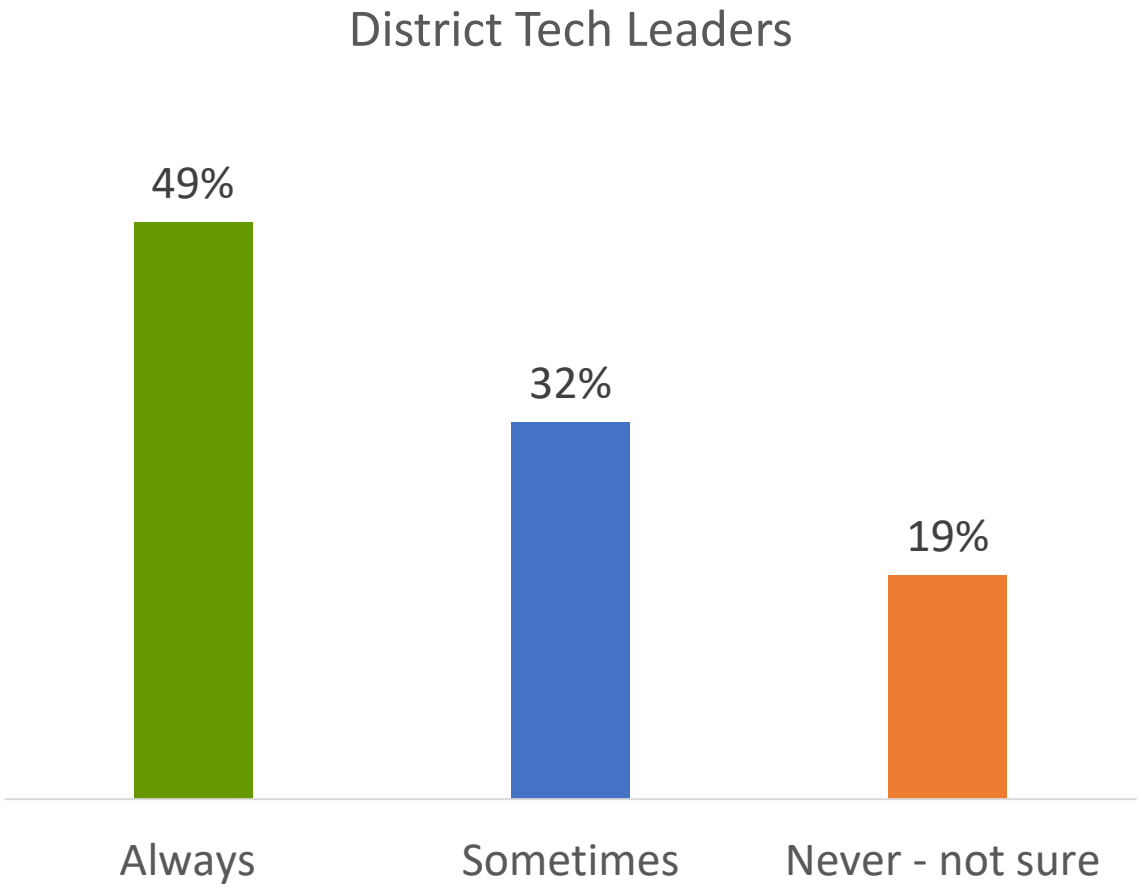
- **Conduct a security audit (50%)**
- Create and review audit logs for suspicious activity (47%)
- Ensure network security platform is appropriate for district needs (44%)
- Maintain rigorous anti-virus tools (38%)
- Research content filtering providers (38%)
- Develop a contingency operations plan in case of an attack (38%)
- Limit access to sensitive data by tightening admin privileges (34%)
- Train staff and students on data security best practices (32%)
- Monitor national trends and policies (31%)
- Implement a password change schedule districtwide (31%)

Why is increased awareness ≠ increased actions?

Anytime, anywhere learning – impact on cybersecurity

Does your district ensure that vendors provide evidence of third-party validation and cloud compliance certificates?

Anytime, anywhere learning – impact on cybersecurity



Does your district ensure that vendors provide evidence of third-party validation and cloud compliance certificates?

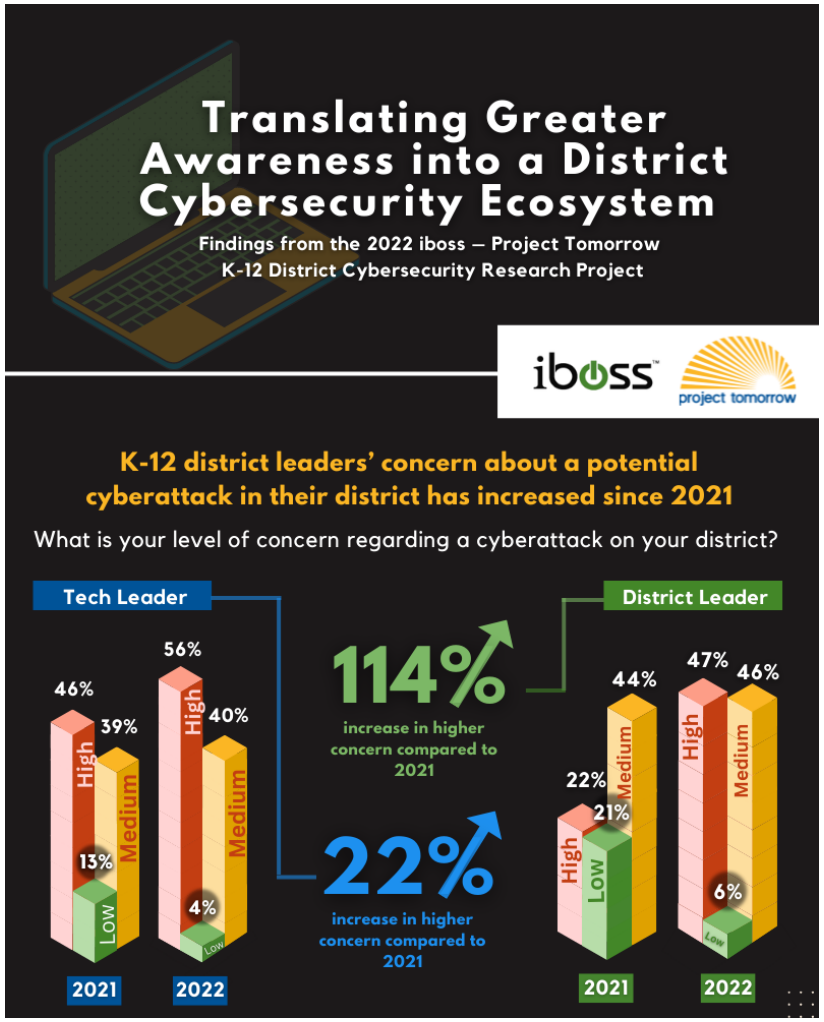
What do you need to be better prepared for a cyberattack?

- **Education on best practices – 49%**
- **Assessments we can use to evaluate our own readiness and preparation – 42%**
- **Leadership buy-in on the importance of cybersecurity – 42%**
- Increased funding for cybersecurity – 39%
- Experts to call on for advice – 38%
- Communication plan in case of an attack – 35%
- More highly trained and experienced staff – 33%

Indication of the need for more information

- Only 22% of District Technology Leaders say they are using the NIST framework to design, guide or support their local cybersecurity plans and approaches

iboss – Project Tomorrow Research results:



New report and infographic

It's Time to Think Differently: Why a District Cybersecurity Ecosystem in Critical Today

Beyond IT:
Building Cabinet Buy-in for a "Zero Trust" Cybersecurity Program

Paul Martini
CEO, iboss

Questions?

K12 SIX Public Resources

- **The K-12 Cyber Incident Map:** https://www.k12six.org/map **and "State of K-12 Cybersecurity: Year in Review" report series** https://www.k12six.org/the-report
- **K12 SIX 'Essentials' Series:** https://www.k12six.org/essentials-series
  - Cybersecurity Frameworks: What K-12 Leaders Need to Know
  - K-12 Essential Cybersecurity Protections Series
  - K-12 Cyber Incident Response Runbook
- **K12 SIX Annual Conference and Webinar Series**

  5/18: "Kickstarting Your K-12 Cybersecurity Program: Where and How to Start" https://www.k12six.org/webinars

- **Membership and partnership inquiries: info@k12six.org**