NSBA Cyber Secure Schools

2018 NSBA Cyber Risk Report

July 18, 2018, 11:30 AM – 12:30 PM Eastern

Presenters: Dottie Schindlinger, Kevin Ciak & James Page

BoardDocs®

Session Overview

01 60 minute session – “talk-show” format with questions posed from the audience

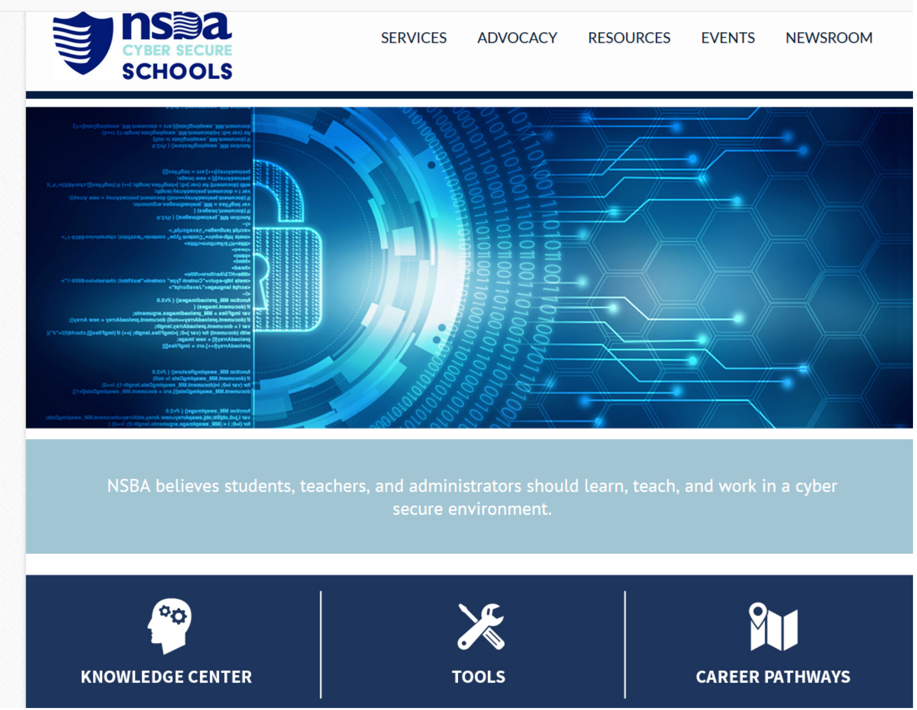
02 Send your questions to the Q&A box on the GoToWebinar control panel

03 Session is being recorded, phone lines will remain muted

04 Download the full 2018 NSBA Cyber Risk Report – available on NSBA’s website

05 Slides and recording will be made available after the session

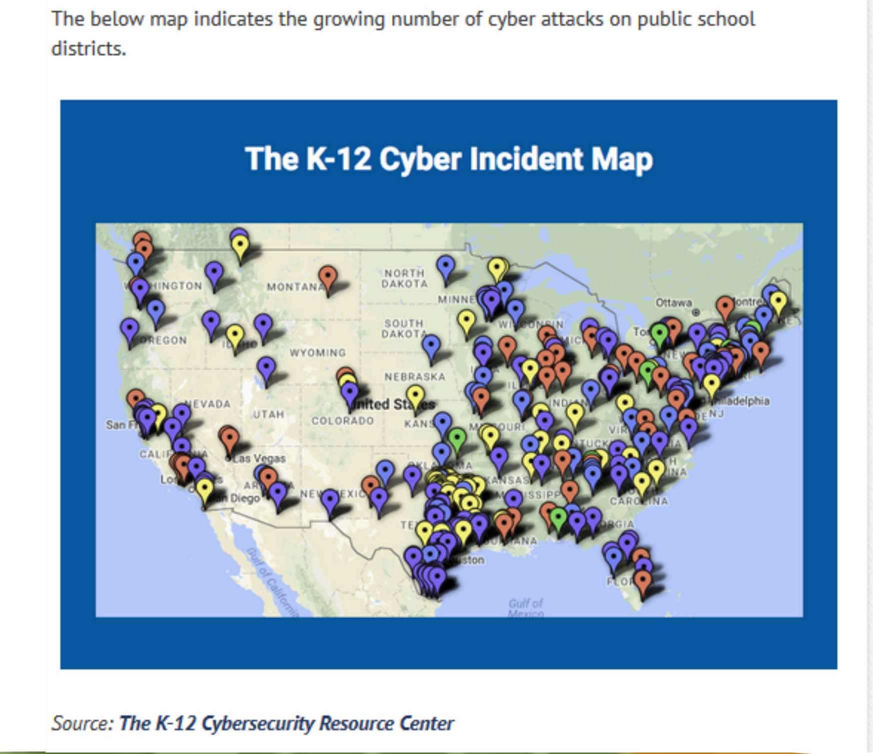
NSBA's Cyber Secure Schools Site



NSBA believes students, teachers, and administrators should learn, teach, and work in a cyber secure environment.

https://www.nsba.org/cyber

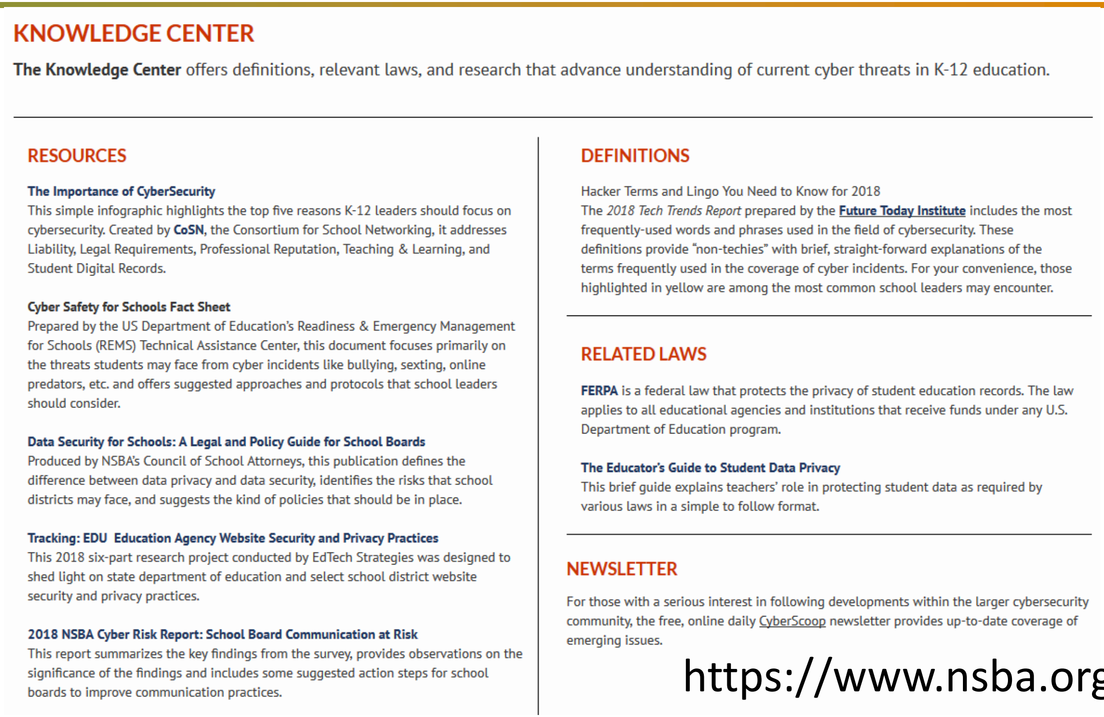
Stay Informed….



The below map indicates the growing number of cyber attacks on public school districts.

Source: ***The K-12 Cybersecurity Resource Center***

In the Knowledge Center…..



KNOWLEDGE CENTER

The Knowledge Center offers definitions, relevant laws, and research that advance understanding of current cyber threats in K-12 education.

RESOURCES

The Importance of CyberSecurity
This simple infographic highlights the top five reasons K-12 leaders should focus on cybersecurity. Created by **CoSN**, the Consortium for School Networking, it addresses Liability, Legal Requirements, Professional Reputation, Teaching & Learning, and Student Digital Records.

Cyber Safety for Schools Fact Sheet
Prepared by the US Department of Education's Readiness & Emergency Management for Schools (REMS) Technical Assistance Center, this document focuses primarily on the threats students may face from cyber incidents like bullying, sexting, online predators, etc. and offers suggested approaches and protocols that school leaders should consider.

Data Security for Schools: A Legal and Policy Guide for School Boards
Produced by NSBA's Council of School Attorneys, this publication defines the difference between data privacy and data security, identifies the risks that school districts may face, and suggests the kind of policies that should be in place.

Tracking: EDU Education Agency Website Security and Privacy Practices
This 2018 six-part research project conducted by EdTech Strategies was designed to shed light on state department of education and select school district website security and privacy practices.

2018 NSBA Cyber Risk Report: School Board Communication at Risk
This report summarizes the key findings from the survey, provides observations on the significance of the findings and includes some suggested action steps for school boards to improve communication practices.

DEFINITIONS

Hacker Terms and Lingo You Need to Know for 2018
The *2018 Tech Trends Report* prepared by the **Future Today Institute** includes the most frequently-used words and phrases used in the field of cybersecurity. These definitions provide "non-techies" with brief, straight-forward explanations of the terms frequently used in the coverage of cyber incidents. For your convenience, those highlighted in yellow are among the most common school leaders may encounter.

RELATED LAWS

FERPA is a federal law that protects the privacy of student education records. The law applies to all educational agencies and institutions that receive funds under any U.S. Department of Education program.

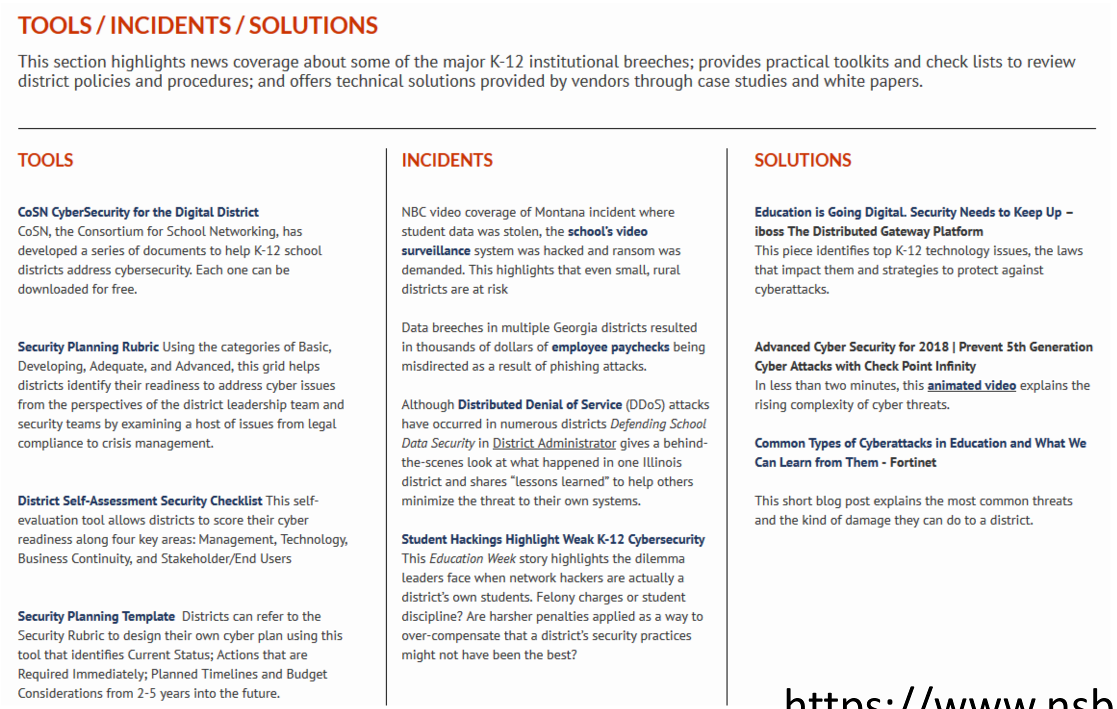
The Educator's Guide to Student Data Privacy
This brief guide explains teachers' role in protecting student data as required by various laws in a simple to follow format.

NEWSLETTER

For those with a serious interest in following developments within the larger cybersecurity community, the free, online daily CyberScoop newsletter provides up-to-date coverage of emerging issues.

https://www.nsba.org/cyber/knowledge

Under the Tools Section….



TOOLS / INCIDENTS / SOLUTIONS

This section highlights news coverage about some of the major K-12 institutional breeches; provides practical toolkits and check lists to review district policies and procedures; and offers technical solutions provided by vendors through case studies and white papers.

TOOLS

CoSN CyberSecurity for the Digital District
CoSN, the Consortium for School Networking, has developed a series of documents to help K-12 school districts address cybersecurity. Each one can be downloaded for free.

Security Planning Rubric Using the categories of Basic, Developing, Adequate, and Advanced, this grid helps districts identify their readiness to address cyber issues from the perspectives of the district leadership team and security teams by examining a host of issues from legal compliance to crisis management.

District Self-Assessment Security Checklist This self-evaluation tool allows districts to score their cyber readiness along four key areas: Management, Technology, Business Continuity, and Stakeholder/End Users

Security Planning Template Districts can refer to the Security Rubric to design their own cyber plan using this tool that identifies Current Status; Actions that are Required Immediately; Planned Timelines and Budget Considerations from 2-5 years into the future.

INCIDENTS

NBC video coverage of Montana incident where student data was stolen, the **school's video surveillance** system was hacked and ransom was demanded. This highlights that even small, rural districts are at risk

Data breeches in multiple Georgia districts resulted in thousands of dollars of **employee paychecks** being misdirected as a result of phishing attacks.

Although **Distributed Denial of Service** (DDoS) attacks have occurred in numerous districts *Defending School Data Security* in District Administrator gives a behind-the-scenes look at what happened in one Illinois district and shares "lessons learned" to help others minimize the threat to their own systems.

Student Hackings Highlight Weak K-12 Cybersecurity
This *Education Week* story highlights the dilemma leaders face when network hackers are actually a district's own students. Felony charges or student discipline? Are harsher penalties applied as a way to over-compensate that a district's security practices might not have been the best?

SOLUTIONS

Education is Going Digital. Security Needs to Keep Up – iboss The Distributed Gateway Platform
This piece identifies top K-12 technology issues, the laws that impact them and strategies to protect against cyberattacks.

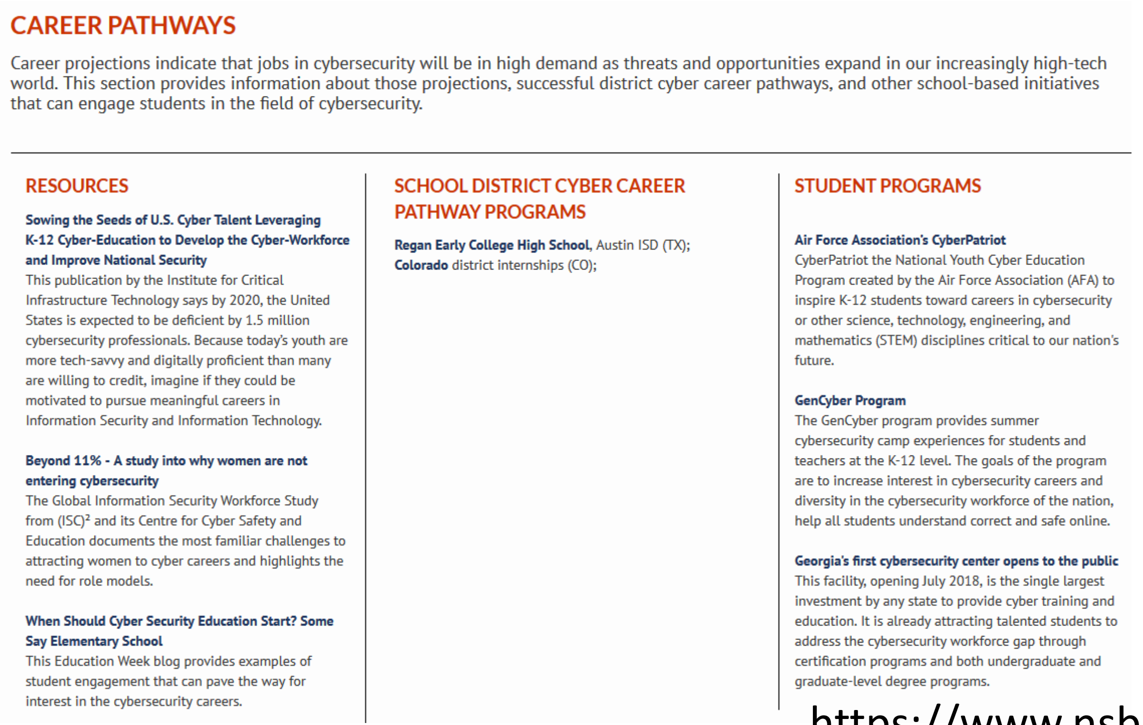
Advanced Cyber Security for 2018 | Prevent 5th Generation Cyber Attacks with Check Point Infinity
In less than two minutes, this **animated video** explains the rising complexity of cyber threats.

Common Types of Cyberattacks in Education and What We Can Learn from Them - Fortinet

This short blog post explains the most common threats and the kind of damage they can do to a district.

https://www.nsba.org/cyber/tools

In Career Pathways…



CAREER PATHWAYS

Career projections indicate that jobs in cybersecurity will be in high demand as threats and opportunities expand in our increasingly high-tech world. This section provides information about those projections, successful district cyber career pathways, and other school-based initiatives that can engage students in the field of cybersecurity.

RESOURCES

Sowing the Seeds of U.S. Cyber Talent Leveraging K-12 Cyber-Education to Develop the Cyber-Workforce and Improve National Security
This publication by the Institute for Critical Infrastructure Technology says by 2020, the United States is expected to be deficient by 1.5 million cybersecurity professionals. Because today's youth are more tech-savvy and digitally proficient than many are willing to credit, imagine if they could be motivated to pursue meaningful careers in Information Security and Information Technology.

Beyond 11% - A study into why women are not entering cybersecurity
The Global Information Security Workforce Study from (ISC)² and its Centre for Cyber Safety and Education documents the most familiar challenges to attracting women to cyber careers and highlights the need for role models.

When Should Cyber Security Education Start? Some Say Elementary School
This Education Week blog provides examples of student engagement that can pave the way for interest in the cybersecurity careers.

SCHOOL DISTRICT CYBER CAREER PATHWAY PROGRAMS

Regan Early College High School, Austin ISD (TX);
Colorado district internships (CO);

STUDENT PROGRAMS

Air Force Association's CyberPatriot
CyberPatriot the National Youth Cyber Education Program created by the Air Force Association (AFA) to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future.

GenCyber Program
The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the K-12 level. The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, help all students understand correct and safe online.

Georgia's first cybersecurity center opens to the public
This facility, opening July 2018, is the single largest investment by any state to provide cyber training and education. It is already attracting talented students to address the cybersecurity workforce gap through certification programs and both undergraduate and graduate-level degree programs.

https://www.nsba.org/cyber/career

Ways to Get Involved

- If your district or organization has developed a tool or strategy for addressing cyber issues in the K-12 community and would like to share it, please contact us at aflynn@nsba.org

- Consider participating in an informal NSBA Cyber Advisory Council that will be a launched later this summer to help our staff stay abreast of the most relevant issues and to ensure our resources are meeting your needs.

- Join the NSBA cyber mailing list to keep up-to-date when new resources are added to the site or when there are other cyber events planned.

https://www.nsba.org/cyber

Today’s Presenters

Dottie Schindlinger

Vice President & Governance Technology Evangelist, BoardDocs

Moderator

Kevin Ciak

Immediate Past NSBA President and Board Member, Sayreville Public Schools

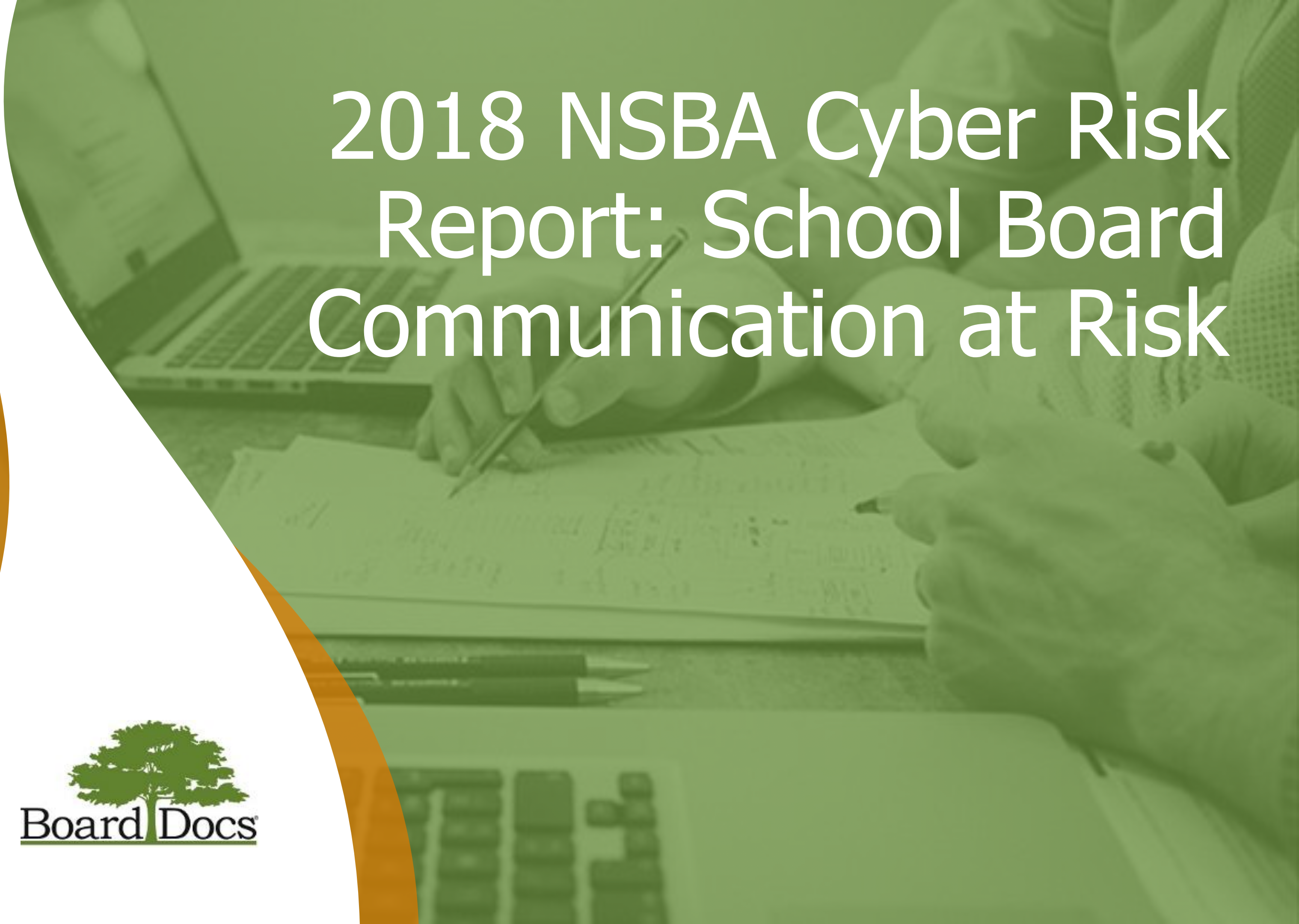
Panelist

James Page

Director of Information Technology and Project Planning, NYSSBA

Panelist

2018 NSBA Cyber Risk Report: School Board Communication at Risk

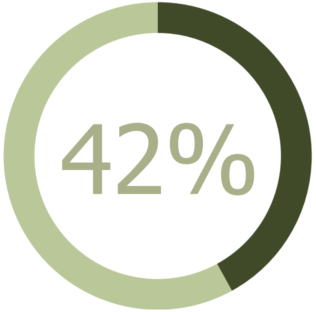


Cyber Risk Trends

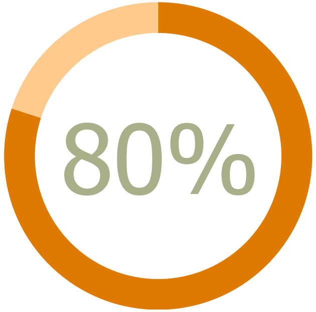
- “As a target for security threats, the public sector is unique, experiencing more cyber incidents than any other industry.” (2017 Accenture, Confidence & Capability: Rebooting Public Sector Cybersecurity)
- US Dept of Ed warns of impending breaches for schools – 800 school websites hacked by terrorist group
- 2018 cost of data breaches is predicted to top $6 billion USD
- 1 in every 131 emails is malicious

Cyber Concern "Gap"

- A gap exists between school boards' concerns for cyber risk and their approach to addressing cyber security

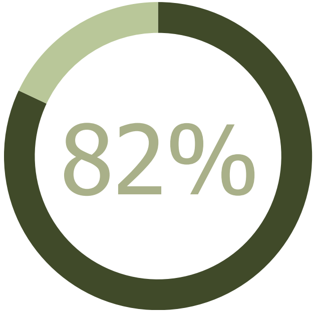


School Board members **believe using digital technology** for board communication **has decreased security**

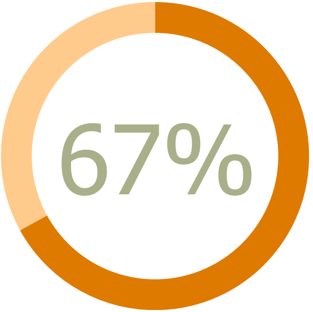


School Board members **regularly use digital technology** to discuss board business

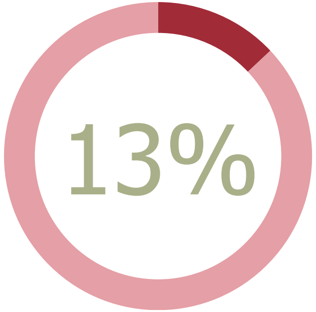
Cyber-Readiness – School Boards Lag Behind



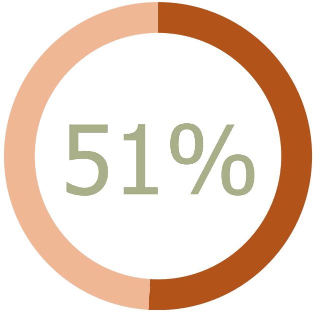
School boards have never conducted a security audit of board communication



School boards don't require cybersecurity training



IT/Data security teams that oversee the security of board communications



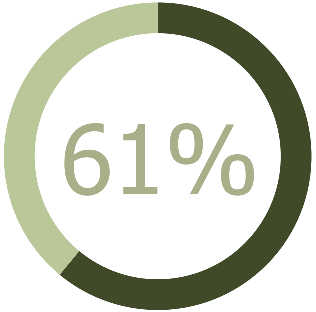
School boards "don't know" if there is a cyber crisis plan in place; another **39% know there isn't one.**

Board Document Security Is Mixed

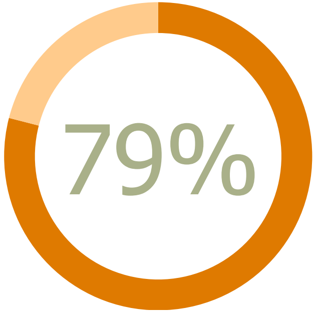
- 13% keep board documents on ***public file-hosting sites***
- 20% store them on ***personal or external drives***
- 39% keep them on ***school website***
- Only 42% store board materials on a secured board portal

School Board Communications Are Largely Unsecured

- School Boards discuss board matters using a variety of unsecured or minimally-secured communication channels.



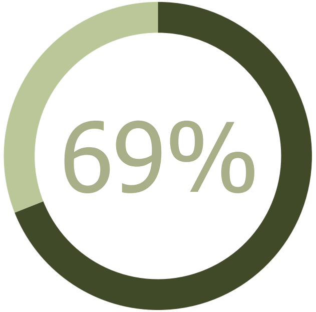
School Board members **use personal email accounts** at least occasionally to discuss board matters



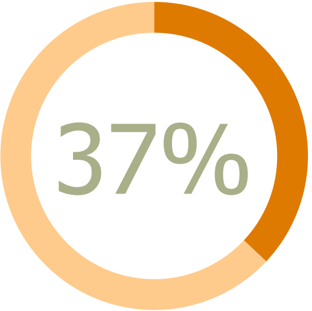
School Board members **use district-supplied email accounts** to discuss board business

School Board Documents Don’t Receive Security Oversight

- School Board Members are downloading, storing and transmitting board documents on a wide variety of systems, with little or no oversight from IT/security teams



School boards members regularly download board documents onto personal devices



Reported downloading at least half of the time

Create a Secure Board Communications Policy and give oversight authority to the district's data security team

Board's Role in Overseeing Cyber Risk

- School Boards are largely unaware of their role in overseeing cybersecurity, nor do they receive adequate training and support to oversee cyber risk management.
- When asked whether a security audit of the school board's communication practices had ever been conducted.
  - 51% - more than half responded "I don't know"
  - 31% responded "no"

Oversight of Board Communication Practices

- Superintendent response: 32% oversee and 28% facilitate board communication methods

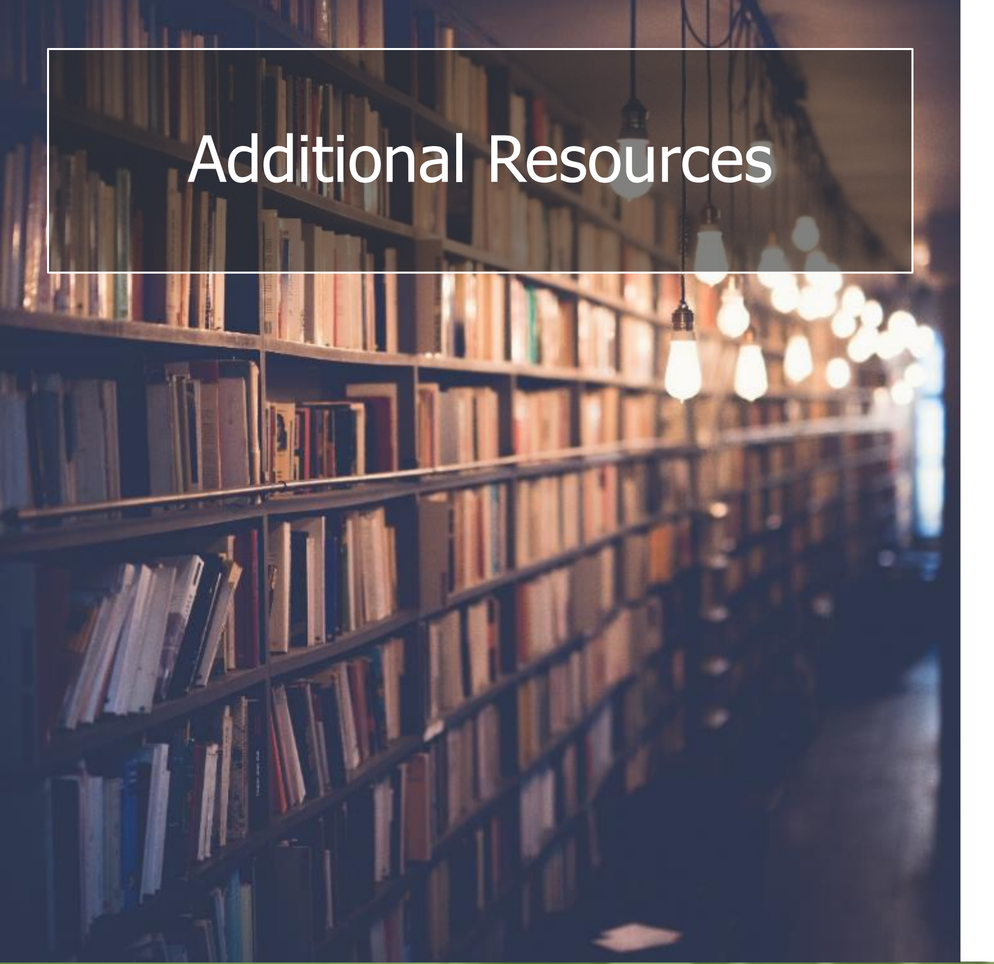
Few schools grant oversight of board communication methods to district personnel most normally associated with managing risk:

- Less than 13% of IT/IS Data Security Team
- 11% General Counsel/School Attorney
- Audit/Risk Committee
- 19% ask Board Chair to provide this oversight – regardless of Chair's cyber knowledge

Panel Discussion & Q&A

Board Docs

Additional Resources



01 Good Governance Blog

02 Best Practice Webinars

03 Whitepapers & Research

Contact Us

(800) 407-0141

info@boarddocs.com

www.BoardDocs.com

1515 Courthouse Road, Suite 210, Arlington, VA 22201