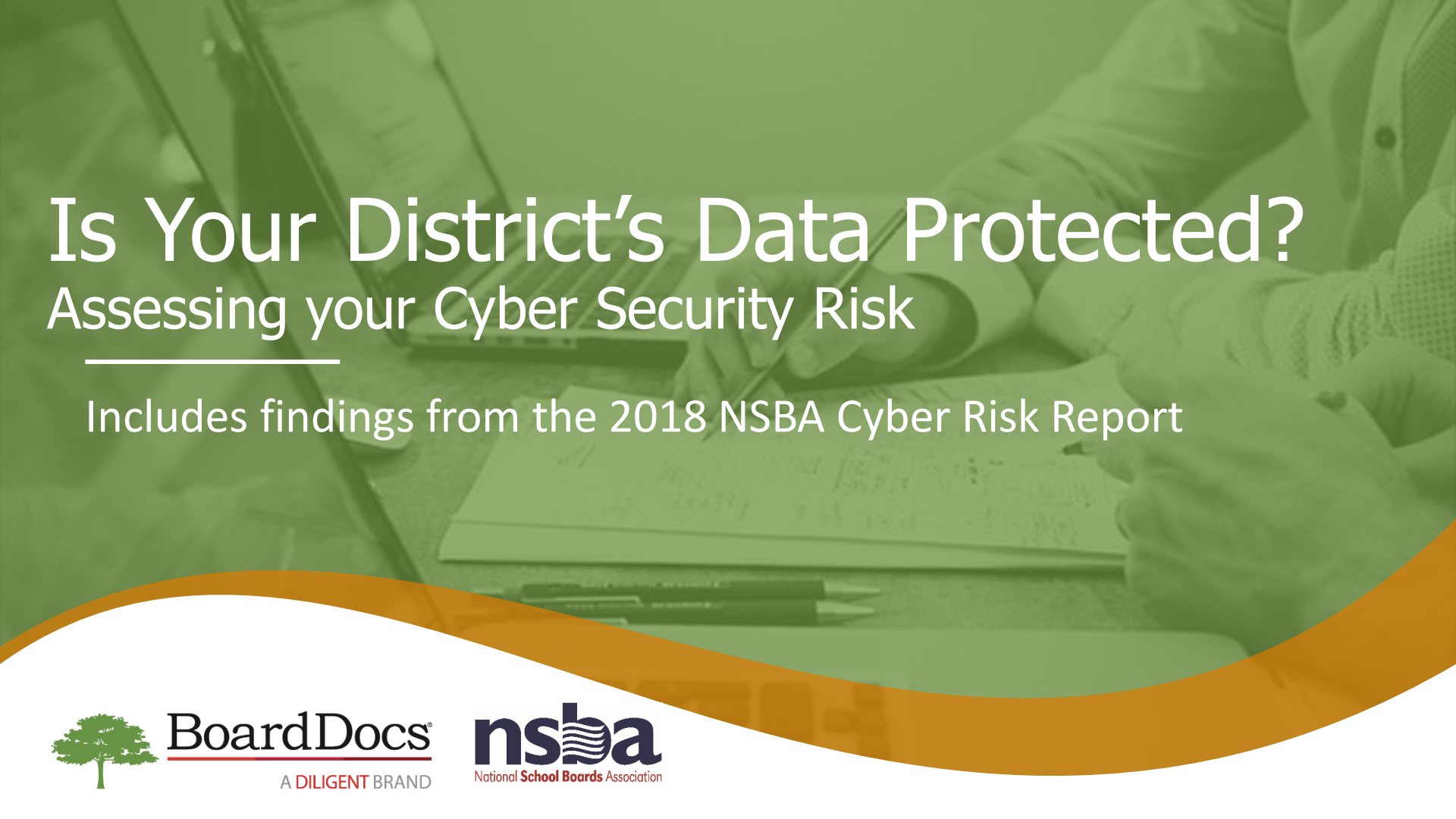


Is Your District's Data Protected?

Assessing your Cyber Security Risk

Includes findings from the 2018 NSBA Cyber Risk Report

BoardDocs® A DILIGENT BRAND

nsba National School Boards Association

Session Overview

01 60 minute session – including Q&A 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

Today's Presenters

Dottie Schindlinger

VP of Thought Leadership BoardDocs

Presenter

Adam Lustig

Director, Center for Safe Schools

Presenter

The Center for Safe Schools was formed to:

- Provide a national forum and platform by which school district leaders/employees, students, parents, and communities can **educate, engage and be empowered** to ensure that schools are a safe place to learn and grow.
- Promote and develop collaborative relationships with and between state school boards associations, communities, educators, law enforcement, emergency responders, and other entities concerned with school safety.
- Keep local school districts informed of relevant and current information in a timely fashion.
- Provide critical resources, information and best practices in four key focus areas:
    - Infrastructure
    - Crisis and Emergency Management
    - Whole Child Health
    - Cyber Security

Infrastructure

The physical aspects of school buildings and facilities designed to safeguard against attacks and potential threats.

Key components of **Infrastructure** include:

- Risk assessments
- Building/Facility design and modification
- Mechanical and electronic systems
- Communications systems
- Safety and Security technology

The Center for Safe Schools provides resources, information and best practices on how the design and modifications of infrastructure elements can ensure that buildings and facilities are properly equipped to prevent, protect and mitigate risk associated with environmental and human threats.

Crisis and Emergency Management

The detection, prevention and management of critical events and emergencies. By working together, schools and community partners can focus on crisis and emergency preparedness including efforts to build a positive, prevention based, school culture.

Key components of **Crisis and Emergency Management** include:

- Risk assessments
- Planning and policy development
- Training, drills and exercises
- Community-based collaborations (law enforcement, emergency responders, etc.)
- Safety and Security technology

The Center for Safe Schools provides resources, information and best practices on how schools can create plans around the intentional prevention of critical incidents and emergencies while also focusing on how to effectively prepare, respond and recover in the event they do occur.

Whole Child Health

A child's physical, mental and social and emotional well-being essential for them to achieve positive outcomes in their academic, professional and personal lives. Everyday life experiences can impact the abilities of all students and these experiences can have lasting effects and present barriers to the well-being of the whole child.

Key components of **Whole Child Health** include:

- School Climate
- Social and Emotional Learning
- Mental Health
- Trauma Informed Practices
- Bully Prevention
- Restorative Justice
- Substance Abuse
- Family/Community Factors

The Center for Safe Schools provides resources, information and best practices on how to accurately identify and support an individual's physical, mental, emotional, and overall wellbeing for success in academics, life and career.

Cyber Security

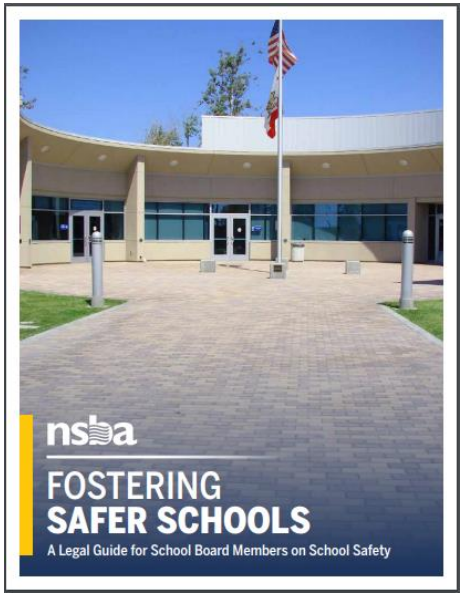
The body of technologies, processes and practices designed to protect personal information and to support students, families and communities in the cyber domain. The rapid pace of technological change is leading to schools facing new challenges in identifying threats, protecting personal information, and promoting the positive and responsible use of technology by staff and students.

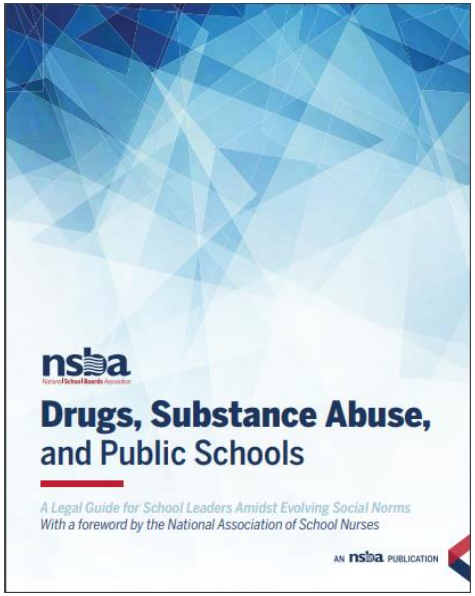
Key components of **Cyber Security** include:

- Risk assessments
- Identification and understanding of new and existing cyber threats
- Safe and secure data storage and sharing
- Responding to threats and security breaches
- Promoting responsible behavior for staff and students in cyber space
- Services and technology

The Center for Safe Schools provides resources, information and best practices on how schools and districts can be aware of potential threats, take preventative measures and be prepared to respond if needed.

NSBA has already created several resources aligned to the issues of school safety that the Center for Safe Schools will continue to build upon





Contact Information

www.nsba4safeschools.org

center4safeschools@nsba.org

Adam Lustig
Director, NSBA Center for Safe Schools
alustig@nsba.org

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

2018 NSBA Cyber Risk Report: School Board Communication at Risk

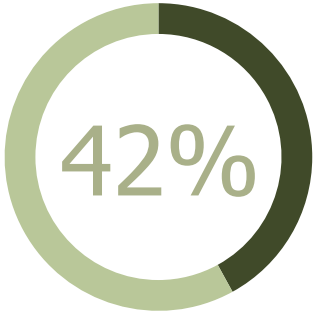
BoardDocs
A DILIGENT BRAND

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"

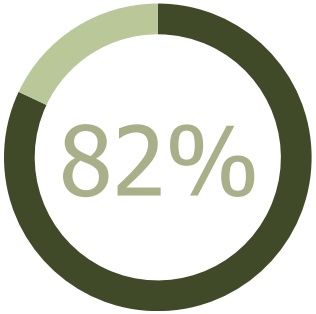
- A gap exists between school boards' concerns for cyber risk and their approach to addressing cyber security



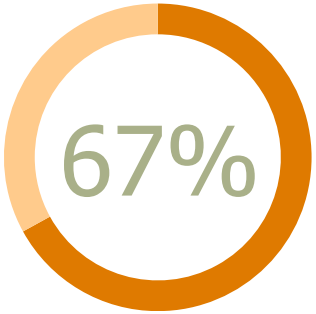
School Board members **believe using digital technology** for board communication **has decreased security**

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

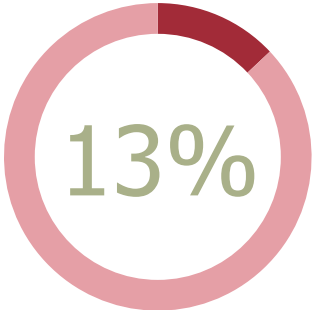
Cyber-Readiness – School Boards Lag Behind



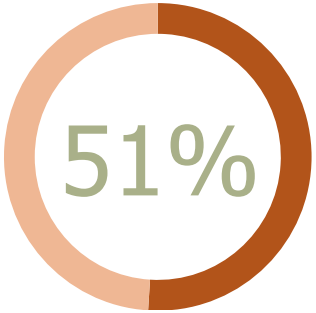
School boards have **never conducted a security audit** of board communication



School boards **don't require cybersecurity training**



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



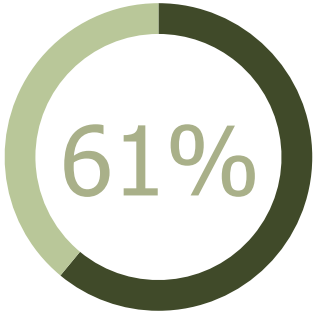
School boards **"don't know"** if there is a cyber crisis plan in place; another **39% know there isn't one.**

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.

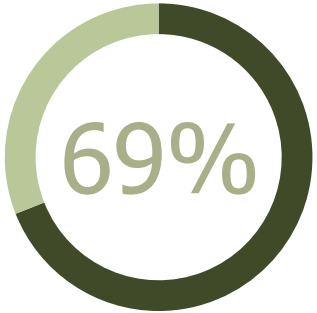


School Board members **use personal email accounts** at least occasionally to discuss board matters

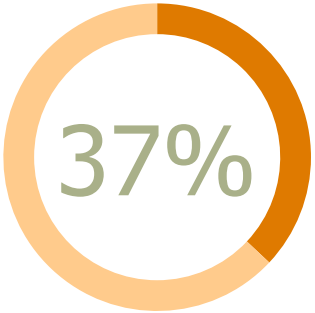
School Board members **use district-supplied email accounts** to discuss board business

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

BoardDocs A DILIGENT BRAND

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

BoardDocs
A DILIGENT BRAND

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

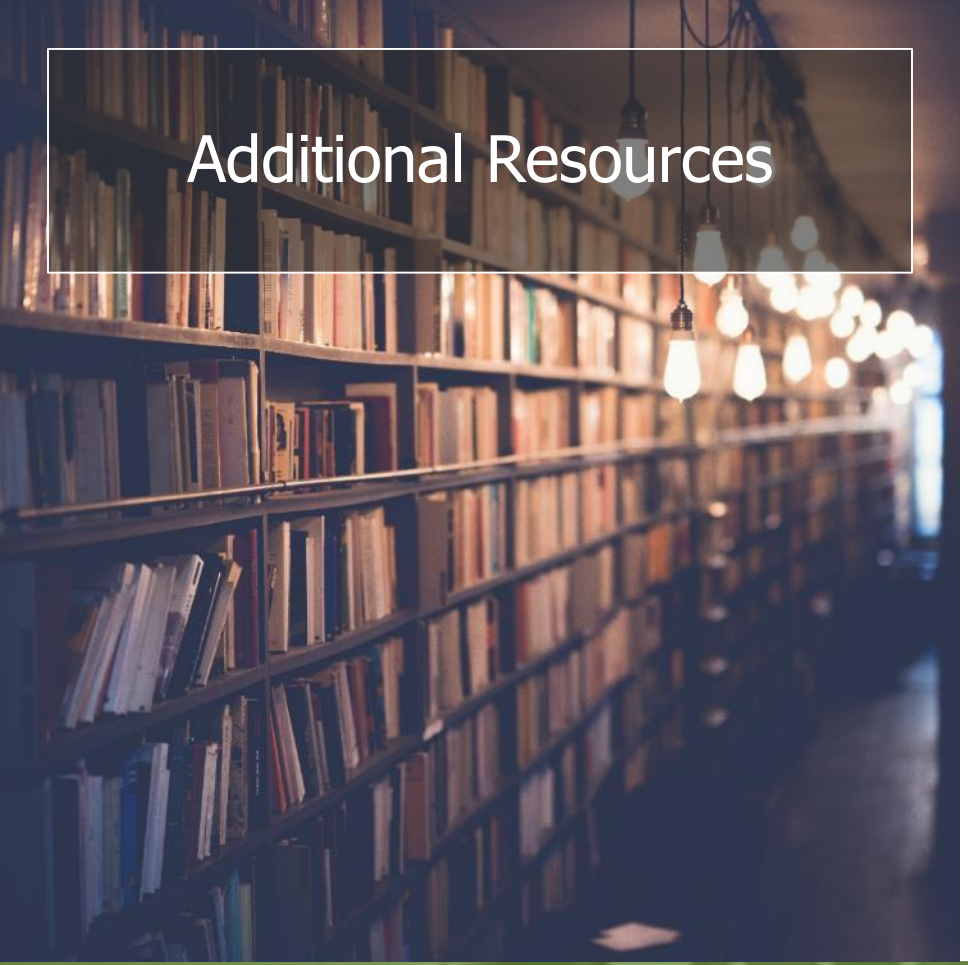
- Superintendent response: 32% oversee and 28% facilitate board communication methods

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

Cyber Risk Q&A

BoardDocs
A DILIGENT BRAND



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

BoardDocs
A DILIGENT BRAND