



AN **nsba** PROGRAM

Copyright © 2019 by the National Schools Boards Association All Rights Reserved.



Understanding Cyber Risks in Our Schools and Homes



Shaun Wiggins
CEO



George Dew
CTO



Samuel Wiggins
COO



Christopher Chambers
General Counsel



PREPARE PROTECT PROMOTE

What is Cyber Risk?



Cyber Risk Defined

Potential physical, financial or reputational damage caused by the unauthorized access to technical infrastructure

Risk = *Threat x Vulnerability x Consequence*

Cyber Risk v. Cyber Threat v. Cyberattack



**Cyber Risk, Cyber Threat & Cyberattack
Are All Interrelated**

Cyber Risk – Threat x Vulnerability x
Consequence

Cyber Threat – possibility a particular
attack may occur

Cyberattack – an offensive action

Six Common Cyber Threat Sources



Six Common Sources of Cyber Threats

1. Nation states
2. Cyber criminals
3. Hacktivists
4. Insiders and service providers
5. Developers of substandard products and services
6. Poor configuration of cloud/network services

Increased Cyber Risk



Elements that Increase Cyber Risk

- Staff/visitors/family accessing your systems from remotely locations
- Staff/students/family using devices remotely
- Staff/student access to administrative privileges on the school/home network or computers
- A *Bring Your Own Device* allowance in schools.
- A relaxed policy related to the regular updating of passwords
- Failure to back-up data
- Neglecting to review your company's cybersecurity policies over the last 12 months OR not having cybersecurity policies at all

Why Understand Cyber Risk?



It's About Security

- Internet provides virtual access to predators and cyber criminals
- Schools and homes seeing increased technology connectivity
- Schools and homes both poorly defended against attacks
- Schools and homes lack comprehensive cyber risk management strategy
- Schools and homes face ever increasing cyber threats
- Cyberattacks are growing fast

Top Five Cyber Risks



1. Phishing

Cyberattack that uses social engineering to trick end users into clicking on what appear to be a legitimate emails. These emails will lure individuals into reveal personal information or clicking on links that install malicious software

Top Five Cyber Risks



2. Distributed Denial-of-Service (DDOS)

Cyberattack that occurs when multiple systems flood the bandwidth or resources of school district servers or home networks

Top Five Cyber Risks



3. Data Breach

An incident in which sensitive, confidential or protected data has been accessed and/or disclosed through unauthorized means

Top Five Cyber Risks



4. Ransomware

Cyberattack that uses a malicious software that encrypts a school's or home's data and requires the payment of a ransom to regain access to the data

Top Five Cyber Risks



5. Internet of Things Vulnerabilities

Cyberattack that infiltrates Internet of Things (IoT) devices installed or used by schools and homes, i.e., smart TVs, security cameras, digital blackboards, locks, etc.

Managing Cyber Risk



What is Cyber Risk Management?

Involves identifying risks and vulnerabilities and applying administrative actions and comprehensive solutions to make sure the organization is adequately protected

Managing Cyber Risk Best Practices



Monitor Risk Environment

Continuously monitor potential risks and explore new trends to determine what will be most likely to impact schools.

Quantify exposures and vulnerabilities on a big-picture scale to create a thorough understanding of the risk environment

Managing Cyber Risk Best Practices



Monitor Assets

Identify the most valuable data assets and monitor regularly. Confidential information is more likely to be the target of a cyber attack and require extra security

Managing Cyber Risk Best Practices



Create a Risk Plan

Develop response and continuity plans for cyber risk scenarios by brainstorming potential situations and determining course of action for each one. Be sure to incorporate multiple departments into the plan

Managing Cyber Risk Best Practices



Prepare Staff and Students

Stress that cyber risk is not solely the responsibility of the IT department. Risk management must not be siloed; all departments, teachers and students should be encouraged to contribute.

Managing Cyber Risk Best Practices



Build Close Ties to External Stakeholders

When something does go wrong, the school needs appropriate relationships with response teams. Public relations, media, and lawyers may be crucial in responding to a cyber attack or data breach.

Managing Cyber Risk Best Practices



Enforce Security Protocols

End-to-end security should be installed on all devices. Create and enforce password policies across the school - suggest for home networks - with a required level of security and change frequency. If staff and students use their own devices, ensure that this data is also password-protected and encrypted.

Managing Cyber Risk Best Practices



Update and Evolve

Technology changes, and systems ***must*** evolve to keep up. Be sure to use industry standards and implement software updates. While impractical to replace costly equipment with every new iteration, they should be updated and maintained. Remember, old, weak systems are ideal targets for hackers.

Tactical Cybersecurity



Bad News

The Online Trust Alliance reported that in 2018, over 2 million cyber incidents led at **LEAST** \$45 billion in losses

Tactical Cybersecurity



Good News

Upwards of 95% of 2018 cyber incidents could have been prevented

Tactical Cybersecurity



Tips & Pointers

What helps?

- Training
- Training
- Training

Tactical Cybersecurity



Tips & Pointers

- Security Audits
- Train staff, students, family in cybersecurity principles
- Install and use antispyware
- Backup Data
- Control physical access to computers and networks

Tactical Cybersecurity



Tips & Pointers

- Download patches and updates as they happen
- Use strong passwords and change regularly
- Use two-factor authentication
- Use firewalls
- Use Virtual Private Networks

Legal Requirements



And Now, A Word From Our Lawyer

Legal issues have fallen and continue to fall in two categories

- Liability
- Regulation

Solving the Most Complex Problems

Soteryx Corp. is a leading provider of business solutions. Our expertise:

Investigations & Intelligence
Crisis Management
Business Resilience
Audience Engagement
Tech Adoption & Innovation

Our solutions help
Prepare Protect & Promote
your organization





Questions?

Contact Information

Adam Lustig
Director, NSBA Center for Safe Schools

alustig@nsba.org
(703) 838-6758

www.nsba4safeschools.org

center4safeschools@nsba.org

