TASBO 2021 Engage

LEARN.
CONNECT.
GROW.

CELEBRATING 75 YEARS

ANNUAL CONFERENCE

Remote and Beyond: Cybersecurity Risks for Districts

BRIAN THOMAS AND BRETT NABORS

2/12/2021

Your Presenters:

BRIAN THOMAS, CISA, CISSP, QSA

- **National Practice Leader, Advisory Services – Weaver**

- **Brian Thomas, CISA, CISSP, QSA,** has more than 20 years of experience in management consulting, IT advisory services and leadership of large, complex engagements for many of the firm's largest clients. Before assuming leadership of Weaver's entire Advisory Service line, Brian led Weaver's IT Advisory Services practice, which includes IT Audit, Cybersecurity, IT Governance, Service and Organizational Controls (SOC) reporting and Regulatory Compliance services. Brian has provided these services to clients in a wide variety of industries as well as the public sector.

Your Presenters:

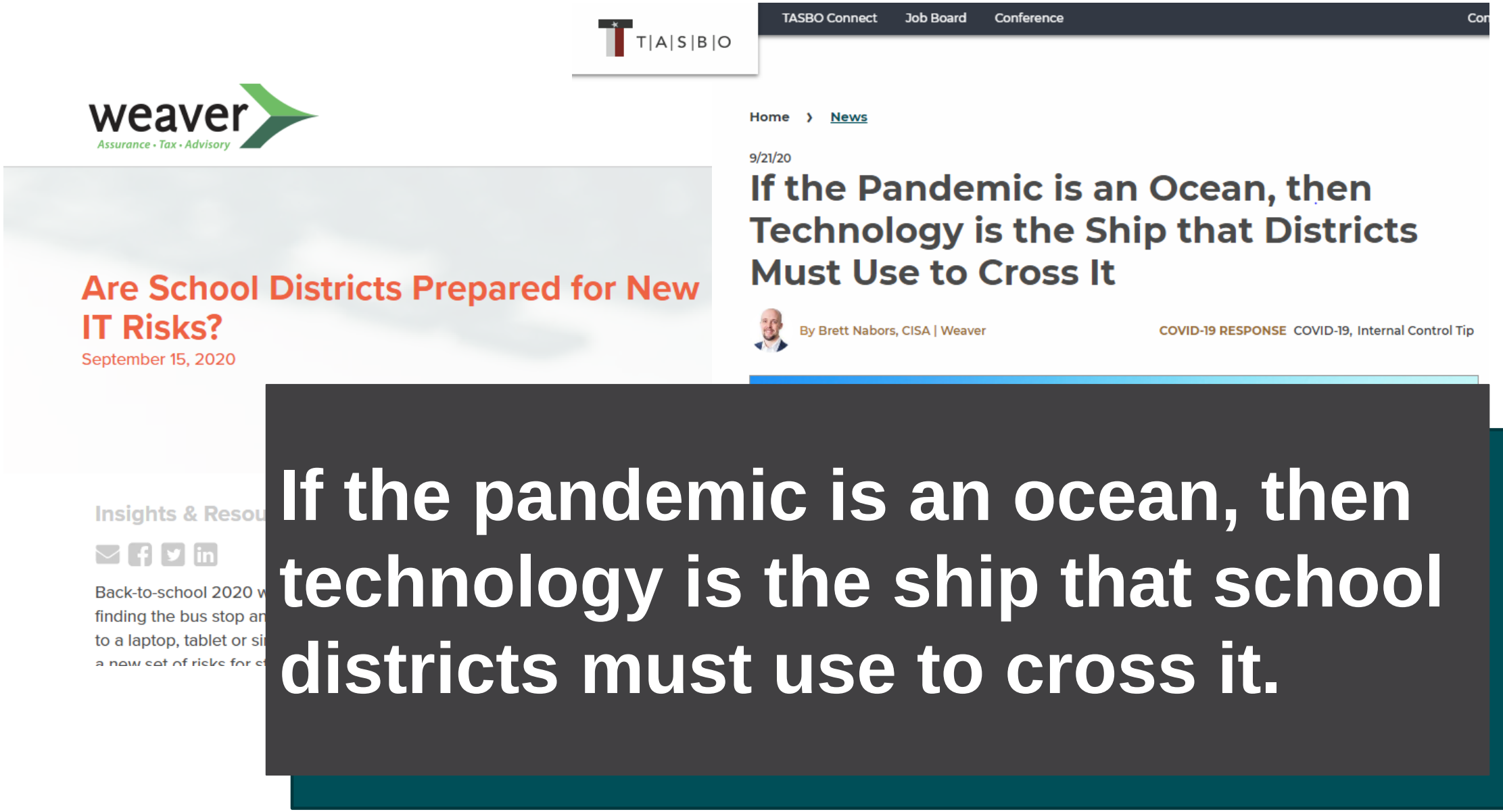
BRETT NABORS, CISA, CDPSE, CCSK

- **Partner, IT Advisory Services – Weaver**

- For more than 15 years, **Brett Nabors, CISA,** has assisted organizations as an internal auditor, external auditor, IT business partner and advisor. He has managed projects, led compliance and regulatory audits, assessed ERP applications and performed IT security assessments. Brett is skilled in system implementations, data analytics, IT control evaluations and other aspects of managing and improving IT performance, effectiveness and security. He helps his clients improve controls and processes, identify and address risks and align IT processes to the overall organizational strategy.

Learning Objectives

- Understand risks that districts should be concern about with remote learning.
- Cybersecurity incidents impact districts across the nation, in the face of slim budgets and increasing IT costs.
- FERPA requirements and considerations for managing through privacy requirements with the expanded use of technology.



Why Talk About This Now…

1. Back-to-school 2020 went *beyond* purchasing supplies, meeting the teachers, finding the bus stop and meeting new friends

2. The 2020/2021 school year involves connecting to a laptop, tablet, or similar computing device – and the school year introduced a new set of risks for students, parents, educators and administrators

3. For **IT departments**, responsibilities have spread beyond just the schools and supporting the teachers, administrators and district staff to now supporting every household for those children engaged in remote learning

Cyber Risks Are Front and Center for Districts!

- Throughout the country, return-to-school efforts introduced not only cybersecurity problems but also a whole new set of technology-related risks for school districts
- As many households with school-aged children engage in remote learning, districts grappled with new and ongoing IT challenges — not just their own, but also students' families who may not have access to technology
- Some issues may be solved with training, while others require structural, organization-wide transformation

Digital Hooky

On the first day of school in Miami-Dade County Public Schools in Florida, students received error messages as they logged in to the district's networks. Administrators later reported that a 16-year-old student had admitted to orchestrating a series of **cyberattacks designed to overwhelm the network**.

(That's how the digital generation plays hooky.)

Cyber Attacks on School Districts

District information hacked through hotel WiFi

Fraudster contacted help desk to change password

Phishing email sent from superintendent requesting file of all W-2s

Phishing email with official looking district survey…must log in to complete…later hack employee portal and change direct deposit information

Identity theft and fraudulent tax returns

Phone calls or emails to change employee banking information (sense of emergency)

Vendor hosting district information compromised

Email or letter from vendor changing address or wiring instructions…millions of construction funds wired

Credit card numbers hacked during Holiday Break

Threat to release student data if do not pay ransom

Malware that encrypted all files on computer system

Fraudulent checks submitted to bank for payment

But There Are More Stories…

- “Delay because there was a miscalculation by a vendor that **caused technology issues**”
- “Students still **can't get reliable Wi-Fi** for school”
- “**School budgets** become casualty of COVID-19”
- “Schools reopen Friday after **hackers request ransom in cyber attack**”
- “**Spiking ransomware attacks** against schools make pandemic education even harder”

K-12 Cybersecurity Incidents on the Rise

* [K-12 Cybersecurity Resource Center]

- Phishing Attacks
- Unauthorized Breaches & Hacks
- Ransomware Attacks
- Denial of Service
- Other Cyber Incidents

K-12 Cybersecurity Incidents Are On The Rise

- Since the K-12 Cyber Incident Map first started tracking incidents in 2016, hundreds of K–12 schools and districts experienced one or more publicly disclosed cyber incident.
- In 2019, 3 times as many incidents were publicly-disclosed as compared to 2018.
  - Most since began tracking in 2016
- Incidents are reported every week.
- Many incidents aren't reported.

Why Be Concerned?

- According to Verizon's 2019 Data Breach Investigations Report, there were 382 reported cybersecurity incidents in the education sector last year.
- The U.S. Department of Education issued a Cyber Advisory Alert on October 16, 2017, stating that K-12 school systems are facing a "new threat where the criminals are seeking to extort money from school districts on the threat of releasing sensitive data from student records."
- The Texas 86th Legislative Session included 2 cybersecurity bills.
- TEA addressed virtual learning and remote work cybersecurity concerns due to COVID-19
- The Internal Revenue Service issued an "urgent alert" about scammers targeting school districts, with the aim of fraudulently obtaining employees' federal W-2 forms, payroll information, or other data that could be used to steal money and file false tax returns. Dozens of districts fell victim to such attacks.
- Fraudsters are getting smarter and smarter.
- Cities, counties and school districts soft targets due to limited budgets and reliance on out-of-date technology.

Why Do Hackers Like School Systems?

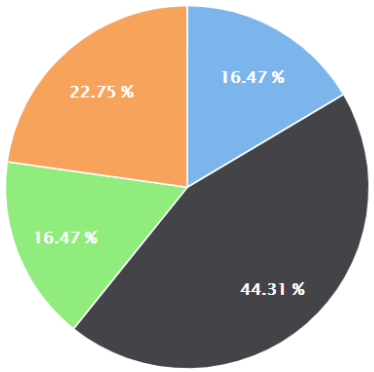
- Virtual Buffet of Valuable Data
  - Personal information like social security numbers, birthdates, home addresses and email addresses
  - Financial Data
  - Medical Data
- Spring 2020 – Virtual Classrooms: 'Zoom-bombing'
  - Inadvertent student name sharing
- Duty to protect employees and students
- Trusting and helpful

Why Are School Districts So Vulnerable?

- Budgets – robust cybersecurity program is expensive
- District salaries must compete with companies for cybersecurity experts
- Outdated IT systems
- School networks are large and have a lot of different types of sensitive data
- Overseeing all potentially weak points is no easy task
- Networks and data need to be accessible by students, staff, parents, government agencies, patrons, 3rd party vendors, etc. (especially new remote learning)

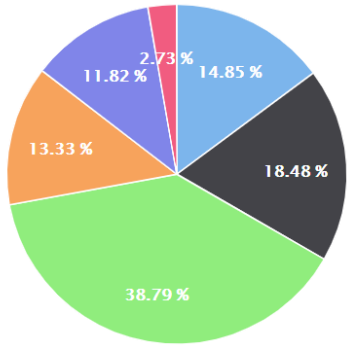
Characteristics of Public School Districts Experiencing Cybersecurity Incidents: 2019

Interacting with the figures will reveal greater details about the characteristics of public school districts and charter schools that have experienced on cyber incidents during calendar year 2019. Note: Limited to regular LEAs and charter schools. Poverty status only includes regular LEAs (data are not for charter schools).



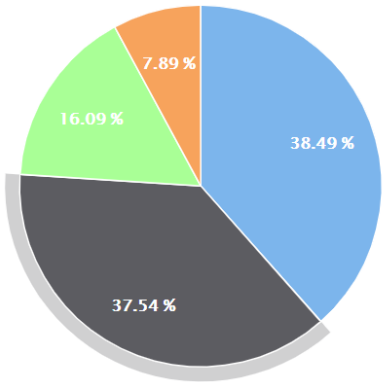
Community Type

- A – City
- B – Suburban
- C – Town
- D – Rural



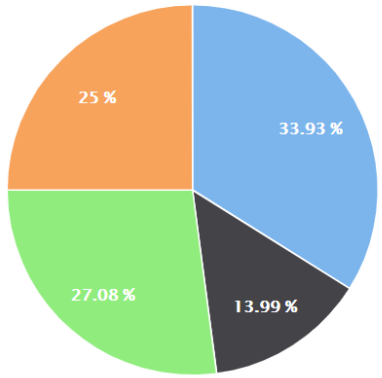
Enrollment Size

- A – Less than 1,000
- B – 1,000 – 2,499
- C – 2,500 – 9,999
- D – 10,000 – 24,999
- E – 25,000 – 99,999
- F – 100,000 or more



Poverty Status

- A – Less than 10 percent
- B – 10 to 19.99 percent
- C – 20 to 29.99 percent
- D – 30 percent or more



Region

- A – Northeast
- B – Southeast
- C – Central
- D – West

- Phishing Attacks – 8%
- Unauthorized Breaches & Hacks – 60%
- Ransomware Attacks – 18%
- Denial of Service – 1%
- Other Cyber Incidents -13%

Source: The K-12 Cybersecurity Resource Center

Types of Cyber Attacks

$$ The Cost is SIGNIFICANT $$

Family Educational Rights and Privacy Act (FERPA)	Loss of federal funding Precluded from providing student data to a vendor for a period of 5 years
Protection of Pupil Rights Amendment	Loss of federal funding
State laws	Repercussions vary by state, but include voiding contracts with vendors, and in the case of one state, incarceration

- Even when these penalties and costs are not imposed, the loss of credibility, embarrassment to the community, and compromising employee and student privacy is detrimental.
- Have requirement to notify affected parties.
- Need some type of cybersecurity insurance!

What Are the Questions…

Let’s review some of the questions school leaders should ask themselves as this unusual school year continues in these trying times.

Access to Services:

Educators depend on tools and systems to work seamlessly, but the end-user experience has to work for all. Not every household includes a computer expert to solve technical or connectivity issues. Districts must consider the capabilities of vendors and software, internet capacity and reliance on ISPs, and the processes required to upgrade, patch or improve upon existing software.

- How can we offer technical support to families so that students have reliable access to teachers and lessons? Can we mobilize additional resources at our internal help desk, or do we need to find vendors to supplement existing resources?
- Do our vendors have the capacity to keep up if everyone must go fully remote? If we begin school online but later transition to in-person learning, will vendors keep extra capacity available in case we have to return to remote instruction?

Access to Services:

Educators depend on tools and systems to work seamlessly, but the end-user experience has to work for all. Not every household includes a computer expert to solve technical or connectivity issues. Districts must consider the capabilities of vendors and software, internet capacity and reliance on ISPs, and the processes required to upgrade, patch or improve upon existing software.

- Do we have change management processes in place to monitor security patches and push out software updates?

Protecting Student Data:

The Family Educational Rights and Privacy Act (FERPA) allows school districts to disclose data to specified parties, but districts must beware of internal or external attacks that could illegally expose sensitive information.

- Are our vendors aware that FERPA requirements may apply to data they are storing or transmitting? Do they have appropriate privacy protections in place?
- Does the district have processes to protect sensitive data from errors in software configuration, updates or issues with inappropriate user access?

Server and Power Capacity:

Some districts have re-opened in a hybrid environment, with some students are attending in person, while others are participating through virtual classroom applications. The load of voice and video traffic on the school's wireless networks and underlying wired network/ISP may cause instability in network connections.

- Do our schools have adequate wired and wireless network capacity for the hybrid environment?
- How can we provide enough electricity for students at their desks, if they are all using devices? Most classrooms aren't designed with that many outlets. How many power strips can we add without overloading circuits?

Third-Party Management:

As districts leverage or repurpose new tools and software, they need to continue to follow policies, procedures, requirements and regulations.

- Do we have processes in place to continuously monitor our software and cloud vendors' compliance with district requirements for security, privacy, availability and other risks?
- Do we require third-party documentation from new vendors, such as a SOC report, to help ensure they are protecting our sensitive information?

Video Conferences:

During the spring 2020, stories of “Zoom-bombing” gave nightmares to school administrators everywhere. Unauthorized access is a risk for every video platform, not just Zoom. There are fairly simply solutions, though.

- Have we provided clear instructions to teachers and families about configuring security options such as waiting rooms, limited screen sharing and requisite passwords?
- Are we regularly pushing out mandatory security patches to protect against emerging threats?

Video Conferences:

During the spring 2020, stories of “Zoom-bombing” gave nightmares to school administrators everywhere. Unauthorized access is a risk for every video platform, not just Zoom. There are fairly simply solutions, though.

- Have we provided clear instructions to teachers and families about configuring security options such as waiting rooms, limited screen sharing and requisite passwords?
- Are we regularly pushing out mandatory security patches to protect against emerging threats?

What Are the Recommended Controls…

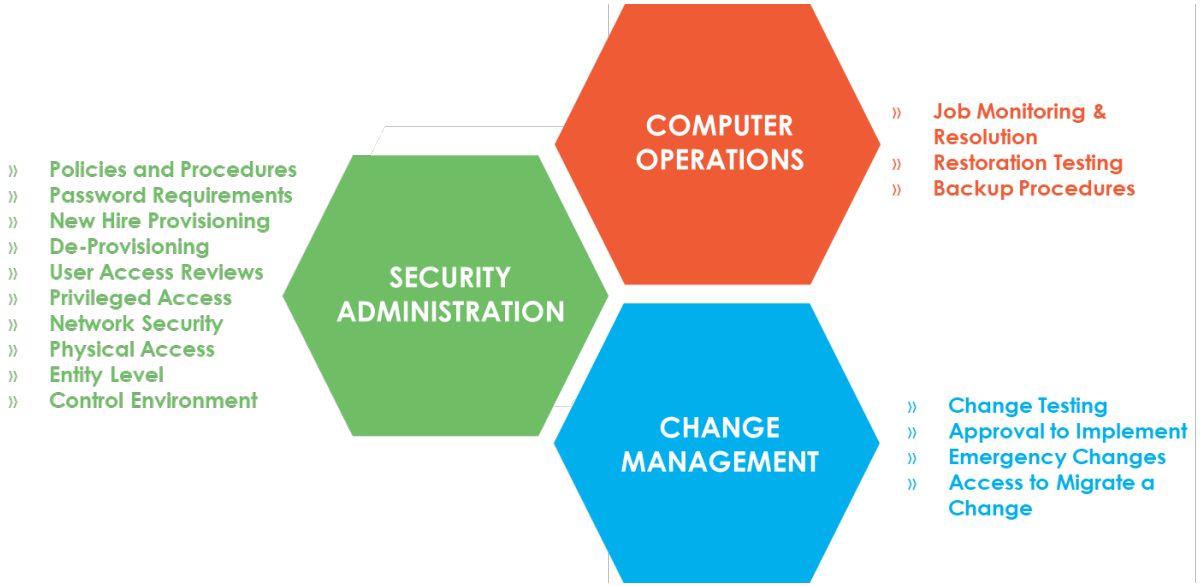
Let’s review some of the controls school leaders should expect are in place to prevent fraud and breaches.

Internal Controls to Prevent Fraud

- Change of address and wiring instructions should be separately verified
  - Replying to an email request is not the appropriate verification method
- Positive pay and debit blocking
- New Vendor and vendor changes separate from Accounts Payable
- Verify vendor name is correct (not a variation)
- Change of direct deposit information done in person with valid district ID and driver's license (or at least verify separately)

Internal Controls to Prevent Breaches

Develop strong IT General Controls across the entire IT environment



- Create stronger password and authorization policies
  - Use two factor authentication methods
- Help desk procedures to verify identity of employee
- Establish policies for emailing sensitive information
  - Data loss prevention tools assist in automatically monitoring and blocking
- Reduce access to information and only allow access to those that need to know and ensure segregation of duties (don't forget shared network drives)
- External tag for outside emails
- Training to increase awareness!!!

Options for Managing Cybersecurity

- Make data privacy a top district priority
- Identify and assess appropriateness of vendor access to data
- Examine information posted on District website…Is it really necessary?
- Enforce password standards
- Triage and Incident Response Plan
- PATCH!
- Use special software or hardware to protect data
- Map data to analyze threats
- Outside risk assessment
- Seek outside help
- Vulnerability Scan
- Penetration Test
- Hire more staff with IT security expertise

Technology Lifeboats

The COVID-19 environment placed and places many demands and extra stress on districts' IT staff, especially when financial crises are forcing staff reductions or hiring freezes. These rising demands and rapid changes in the COVID landscape can also lead to more mistakes and expose vulnerabilities.

Be mindful of what you are asking IT leaders to do, and help them focus resources on the greatest risks and the highest needs.

While this current school year is like no other; at the end of it, we will all come out of it with a new appreciation for the capabilities of our IT networks — and for the people who built our technology lifeboats.

IBM Public Schools Cybersecurity Grant Program

- On 2/4/21, IBM announced a program where public schools could **apply for grants of IBM in-kind services**, to help enhance the school district's cybersecurity posture. A total of **six grants**, valued at $500,000 each ($3 million in total), will be awarded
- School districts can apply between February 4 and March 1, 2021. Grant recipients will be selected based on their **level of cybersecurity needs**, and how they meet the **criteria outlined by IBM**

IBM program announcement:
https://newsroom.ibm.com/2021-02-04-IBM-Introduces-3-Million-in-Cybersecurity-Grants-for-Public-Schools-in-United-States-as-Attacks-on-Education-Grow

Grant application website:
https://www.ibm.org/initiatives/ibm-service-corps/security

Let’s Connect

Brian Thomas

National Strategy Leader, Advisory Services

brian.thomas@weaver.com
713.800.1050

Brett Nabors

Partner, IT Advisory Services

brett.nabors@weaver.com
512.609.1947

Questions?

Resources: Legislative Rulings

IT Frameworks

- Cybersecurity Oriented Frameworks
  - NIST Cybersecurity Framework (CSF)
  - Center for Internet Security (CIS) 20 Critical Security Controls (CSC)
- If you process credit cards, your bank requires PCI Compliance
  - Payment Card Industry Data Security Standard (PCI DSS)
- Student Data Privacy
  - Trusted Learning Environment (TLE) Seal Framework
- Robust Control Frameworks
  - NIST SP 800-53
  - COBIT 2019

Data Privacy Framework

TRUSTED LEARNING ENVIRONMENT

- **Leadership Practice:** manage and collaborate with stakeholders regarding the use and governance of student data to inform instruction
- **Classroom Practice:** implement educational procedures and processes to ensure transparency while advancing curricular goals
- **Data Security Practice:** perform regular audits of data privacy and security practices and publicly detail these measures
- **Business Practice:** establish acquisition vetting processes and contracts that, at minimum, address applicable compliance laws while supporting innovation
- **Professional Development Practice:** requires school staff to conduct privacy and security training and offer the instruction to all stakeholders

Resources: Legislative Rulings

SB 820

(b) Each school district shall **adopt a cybersecurity policy** to:

(1) **Secure district cyberinfrastructure** against cyber-attacks and other cybersecurity incidents

(2) **Determine cybersecurity risk** and implement mitigation planning.

(c) School district's cybersecurity **policy may not conflict** with the information security standards for institutions of higher education adopted by the Department of Information Resources under Chapters 2054 and 2059, Government Code. (Texas Cybersecurity Framework)

Resources: Legislative Rulings

SB 820

(d) The superintendent of each school district shall **designate a cybersecurity coordinator** to serve as a liaison between the district and the agency in cybersecurity matters.

(e) The district ’s cybersecurity coordinator shall **report to the agency** any cyber-attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident.

(f) The district ’s cybersecurity coordinator shall **provide notice to a parent** of or person standing in parental relation to a student enrolled in the district of an attack or incident for which a report is required under Subsection (e) involving the student ’s information.

Resources: Legislative Rulings

HB 3834 - What To Do?

Sec. 2054.5191. CYBERSECURITY TRAINING REQUIRED: CERTAIN EMPLOYEES.

(a-1) **At least once each year**, a local government shall identify local government **employees who have access** to a local government computer system or database and **require** those employees and elected officials of the local government to **complete a cybersecurity training program** certified under Section 2054.519 or offered under Section 2054.519(f).

Resources: Legislative Rulings

HB 3834 - How do we choose the training?

(b) The governing body of a local government may **select the most appropriate cybersecurity training program** certified under Section 2054.519 or offered under Section 2054.519(f) for employees of the local government to complete.

The governing body shall:

(1) **verify and report** on the completion of a cybersecurity training program by employees of the local government **to the department (DIR)**; and

(2) **require periodic audits** to ensure compliance with this section.

Training is to be completed by June 14, 2020