

Lessons Learned From Data Breaches

South Carolina Association
of School Business Officials

2020 Spring Conference

March 4, 2020

Jim Denning

Burr Forman McNair

Session Overview

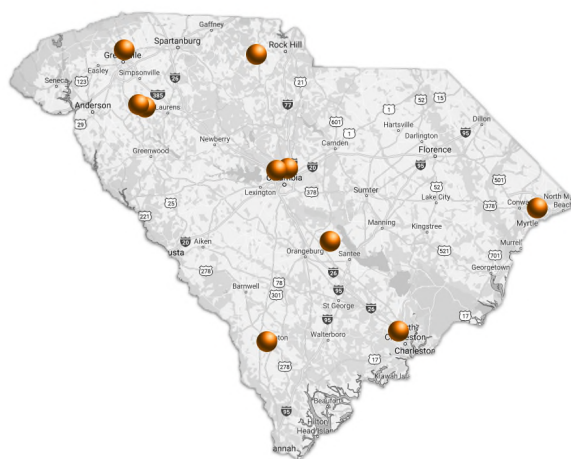
This presentation will provide an understanding of

1. Why cybersecurity is important to your district;
 2. Methods used by criminals and insiders to access and steal your district's data and money;
 3. Some ways to avoid or mitigate data loss and the related costs, including vendor relations; and
- › As we discuss these issues, we'll consider how school districts and others have been compromised, and what can be learned from their experiences to help prevent and mitigate the damage.

The Bottom Line of Data Breaches

- › For any organization, there is a **cost in real dollars** required to **identify, stop, and remedy** a data breach
- › There is **also a reputational and political cost** to the district, its board and leadership
- › State and federal laws require notification and assistance to affected individuals and companies
- › **Stakeholders** may **lose** financially and otherwise, through the resulting identity theft or disclosure of **personal and financial information, lose access** to services or information, **suffer anxiety** about possible harm, and **feel a loss of confidence** in their elected and appointed leaders and support staff

School District Breaches (2016 -2019)



Understanding the Risks; Preparing a Strategy

It is critical that you understand:

- › The threats – who the bad actors are and the tools they use
- › How your district and schools can be exposed, and
- › How to prepare for and respond to a data compromise

Common cybersecurity threats and attacks

- › Malware (viruses, ransomware, spyware, etc.)
- › Hacking (via zero-day exploit, malware, etc.)
- › Network intrusions
- › Denial-of-service and distributed denial-of-service (DDoS) attacks
- › Data theft (exfiltration)
 - › Confidential Information
 - › Personally identifiable information
 - › Intellectual property & proprietary information

Common cybersecurity threats and attacks

- Social Engineering Scams
 - › **Phishing** – uses email to trick recipient into taking action requested by cybercrook; often use bank/credit card company or other vendor impersonation to create impression of urgency
 - › **Spear phishing** – phishing that targets a specific individual or small group by disguising cybercrook as trustworthy friend or co-worker/boss; uses details about recipient to provide added authenticity
 - › **Vishing** – phishing-like activities using video chat
 - › **Smishing** – phishing-like activities using texting
 - › **Whaling** – high-level executives are targeted

Common cybersecurity threats and attacks

- › Insider threats
 - › Disgruntled employees
 - › Nonresponders
 - › Insider collusion
 - › Insider profiteers
- › Systems misuse
- › Fraud/embezzlement
- › Sabotage
- › User mistake or error
- › Vendor Breaches

Ransomware Attacks Continue to Grow

- 23 Texas cities were targeted in August 2019 in what authorities are calling a “coordinated ransomware attack”.
- According to IT security firm Barracuda Networks in a late-2019 report, “from 2018 to 2019, there was a 235% increase in ransomware attacks on K-12 and higher education.”
- Even if target organization doesn’t pay the ransom, the press coverage of the attack may encourage other crooks to take aim at similar organizations to obtain notoriety or due to perceived wealth

Ransomware – The Basics

- › Ransomware based on the principal of extortion.
- › Either prevents you from accessing / using your data OR copies your data and threatens to make it public
- › Most frequently seen model is encryption (locking out)
- › A growing pattern of encryption followed by threat of release (double-dipping)
- › Recently no encryption (Maze), crooks just exfiltrate the data and extort with threat of public release
- › Encryption key / return of data traded for \$\$ in bitcoin
- › Growing in frequency as pre-built toolsets are sold
- › Since ransomware attacks are generally initiated via email attachments or links, the incidence of spear phishing is also on the rise. (but vishing & smishing)

Ransomware (cont.) – p. 2

- Cybersecurity firm Armor tracks school district ransomware incidents. Armor reported in December 2019 that from January through November, ransomware infections hit at least 72 US school districts, potentially impacting 1,039 US schools. 11 districts were hit in November 2019.
- A report issued on December 31, 2019 by antivirus software maker Emsisoft says 89 ransomware incidents occurred during 2019 at US school districts and other educational establishments, impacting the operations of 1,233 schools and colleges.

Ransomware (cont.) – p. 3

- In October 2019 alone at least 15 school districts across the US were hit, affecting over 100 K-12 schools.
- While it is true that ransomware operators and affiliates have not typically followed through with their threats to release data, this may be changing....
- On November 21, the operators of the Maze Ransomware publicly released 10% of the data that was stolen from a security staffing firm after they did not pay the ransom demanded. The criminals state that they will release the rest of the data if an increased ransom payment is not made.

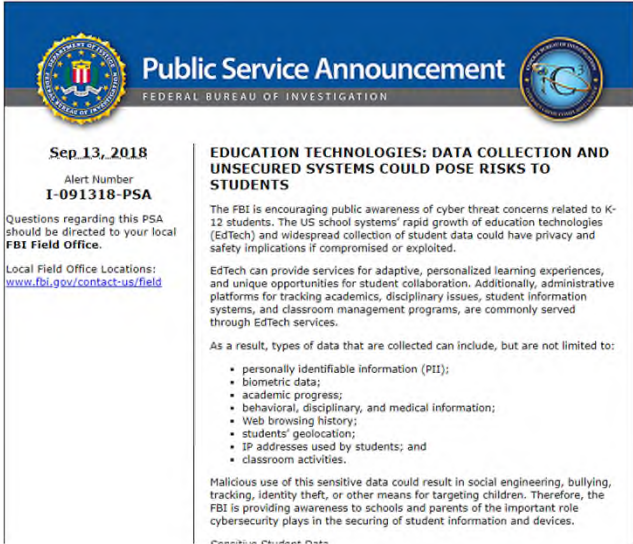
Third Parties Create Additional Risks

- In an interconnected world, you have to worry about more than your own internal security – You need to be concerned about the security policies, technology and practices of your vendors and service providers.
- Some of the largest retailers in the US (e.g., Target, Best Buy, etc.) have been hit by data breaches that began with hacking of service providers and contractors.

Ed / EdTech Vendor-Related Risks

- Vendor errors and vulnerabilities are just as prevalent in the education sector as the retail industry.
- The K12 Cybersecure Resource Center reported in its recently released 2019 Year-in-Review that “51% of student and educator data breach incidents during 2019 were due to the actions (or inaction) of school vendors” (or in some cases other third parties).
- Takeaway: Shore up internal policies and practices, and require the same from vendors

Ed / EdTech Vendor-Related Risks



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Sep 13, 2018
Alert Number
I-091318-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

EDUCATION TECHNOLOGIES: DATA COLLECTION AND UNSECURED SYSTEMS COULD POSE RISKS TO STUDENTS

The FBI is encouraging public awareness of cyber threat concerns related to K-12 students. The US school systems' rapid growth of education technologies (EdTech) and widespread collection of student data could have privacy and safety implications if compromised or exploited.

EdTech can provide services for adaptive, personalized learning experiences, and unique opportunities for student collaboration. Additionally, administrative platforms for tracking academics, disciplinary issues, student information systems, and classroom management programs, are commonly served through EdTech services.

As a result, types of data that are collected can include, but are not limited to:

- personally identifiable information (PII);
- biometric data;
- academic progress;
- behavioral, disciplinary, and medical information;
- Web browsing history;
- students' geolocation;
- IP addresses used by students; and
- classroom activities.

Malicious use of this sensitive data could result in social engineering, bullying, tracking, identity theft, or other means for targeting children. Therefore, the FBI is providing awareness to schools and parents of the important role cybersecurity plays in the securing of student information and devices.

Protecting Student Data

360 Attorneys. 19 Offices. 1 Firm. **Southeastern** Strong. 15 **BURR FORMAN MCNAIR**

© 2020. Burr & Forman LLP

Ed / EdTech Vendor-related Risks

- In 2017, two large EdTech breaches made national news...
 - › **Schoolzilla**, a K-12 data storage and management platform, exposed personal information, including social security numbers, of up to 1.3 million students and staff by backing up data to a public-facing server.

Takeaway: Require encryption at rest & in transit
 - › **Edmodo**, a K-12 social learning platform, was hacked, and usernames, email addresses and hashed passwords of 77 million user accounts were stolen and posted for sale on the Dark Web.

Takeaway: Hashed passwords helped limit harm

Ed / EdTech Vendor-related Risks

- **Pearson Education** - In July 2019 the public learned that Pearson's AimsWeb 1.0 student assessment and progress monitoring platform has been hacked in a massive data breach involving 13,000 enterprise customers (mostly school districts and universities).
- Pearson has refused to go on record with the number of students and educator records compromised, but estimates range from tens to hundreds of millions of individuals.
- Information included one or more of: first, middle, and last name, date of birth, home address, SSN, school and district of attendance.
- Several districts in South Carolina were impacted.

Ed / EdTech Vendor-related Risks

- **How can you improve your district's vendor-related data security during procurement?**
 - › Submit written questions as a part of RFP for EdTech services
 - › Interview finalists using multidiscipline team (e.g., IT, purchasing, finance and legal) keying off responses to written questions
 - › Negotiate vendor services contract with vigor and require transparency, application of appropriate security measures, and immediate notification of incidents and breaches

Suggested Questions for EdTech Vendors

- **Seven questions suggested by Powerschool**
[\(https://www.powerschool.com/resources/blog/do-your-edtech-vendors-take-student-data-privacy-seriously-here-are-7-key-questions-to-ask/\)](https://www.powerschool.com/resources/blog/do-your-edtech-vendors-take-student-data-privacy-seriously-here-are-7-key-questions-to-ask/)
 1. What student data does your software collect—and for what purpose?
 2. Do you share student data with any third party? If so, why?
 3. How is student data stored and protected?
 4. Are your systems independently tested for security vulnerabilities?

Suggested Questions for EdTech Vendors

5. Are you fully compliant with FERPA, HIPAA, COPPA, and other laws?
6. Have you taken the Student Privacy Pledge?
 › <https://studentprivacypledge.org/privacy-pledge/>
7. In the event of a data security breach, how quickly will you notify us—and what steps will you take?
 › See USDoEd Checklist at:
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf

Further Questions for EdTech Vendors

- Has your company appointed a chief privacy officer?
- Does your company monitor federal privacy laws and policy for changes that may affect your privacy policy/program?
- Describe your company's privacy plan for implementing applicable privacy controls, policies, and procedures?
- Describe how your company provides resources to accomplish this implementation?

Some Legal Clauses of Interest

- Acknowledgement of Protected Information
- Obligation to Protect and Limit Use of PI
- Prohibition on Unauthorized Use of PI
- Ownership & Return of PI Upon Termination
- Responsibilities & Liabilities Upon Breach of PI
- Right to Inspect and Audit Vendor Records
- Specific Clauses re FERPA/COPPA/HIPAA
- Insurance Requirements
- Indemnification Requirements
- Service Level Agreement (Service Availability)

Tips for Negotiating EdTech Contracts

- Remember that contracts are negotiable.
- Pay attention to details and specifically include performance expectations and privacy/security responsibilities and liability.
- Evaluate the initial price; seek price / service concessions. Cap increases.
- Pilot test at a couple of schools to seek better pricing on district-wide purchases.
- Be sure the district owns all student data and that it will be returned or destroyed at termination.
- Confer with legal counsel.

What's Ahead in 2020?

- Continued escalation of spear phishing and ransomware attacks with increasing sophistication as ransom demands increase and increasingly succeed
 - › “Double” Ransom to remove encryption PLUS additional ransom to prevent public disclosure or sale of information
 - › Disclosure Ransom to prevent (maybe) publication of data
- Introduction of Deepfake attacks into the mainstream:
 - › Deepfake is artificial intelligence technology that is used to create audio and video that appear credible but are not
 - › One threat: convincing fakes of voices of executives to trick workers into transferring money into criminal's account
 - › Likely to further advance into convincing fake video of an executive asking for emergency transfer of funds
- 5G network (5th generation cellular wireless) will introduce new vulnerabilities as the technology matures and expands

Fundamental Rules of Data Security

- Know what (software/hardware/data) you have.
- Know what (software/hardware/data) you need.
- Get rid of what (software/hardware/data) you have but don't need.
- Maintain and protect what (software/hardware/data) you keep.
- Only keep it (software/hardware/data) for so long as you need it; weigh the risk of keeping it.
- When you get rid of it (software/hardware/data), do so in a responsible, safe, and secure way.
- Know who needs what you have and control their access.
- Continually re-evaluate each step.

Cyber Insurance – Key Elements

- Cyber insurance generally contain some combination of these policies:
 - › Network Security
 - › Privacy Liability
 - › Network Business Interruption
 - › Media Liability
 - › Error and Omissions (E&O)
- Be mindful of coverage overlaps or gaps with your existing policies, and sublimits on important / expensive / common claims

Cyber Insurance -- Coverage

- First Party Coverage – covers your network
 - › Cyber extortion payments
 - › Cyber forensic services
 - › Legal counsel assistance in evaluating regulatory and legal requirements
 - › Notification of affected individuals (victims)
 - › Effects of and extra resources required due to business interruption
 - › Regulatory fines and penalties
 - › Public Relations services
 - › *Credit monitoring / ID theft repair services

Cyber Insurance -- Coverage

- Third Party Coverage – defense of claims made against your organization by others
 - › Attorneys' fees and other legal defense costs
 - › Settlements
 - › Expert witnesses
 - › Court costs
 - › Judgments
 - › *Credit monitoring / ID theft repair services

Cyber Insurance – Cost of Coverage

- The premium cost to your organization reflects, among other things:
 - › The amount of sensitive information handled by your organization
 - › The type of industry
 - › The number of employees in the organization
 - › Vendor contracts with cybersecurity and indemnification of your organization
 - › Types of coverage sought & exclusions
 - › Coverage limits and sublimits
 - › Existence and amount of deductible / self-insured retention

Cyber Insurance – What is Covered?

- Be attentive to What is Covered – and Not.
- Watch coverage gaps with other policies & sublimits
- Does the policy cover
 - › Employee negligence?
 - › Social engineering (e.g., spear phishing) and network attacks (DDOS, intrusions, hacks)?
 - › Any attack your organization falls victim to OR ONLY those targeted specifically against your organization? (e.g., phishing vs spear phishing)
 - › Breaches that begin with a vendor and infiltrate your network via vendor credentials, etc.?
 - › Outages of cloud and remote network systems?

Questions?

Jim Denning
(864) 271-4940
jdenning@burr.com

© 2020. Burr & Forman LLP

Jim Denning



Practice Areas

Data Privacy and Cybersecurity
Data Breach Response
Advertising and Promotions
International Trade Law and Import Issues
Licensing and Intellectual Property
Corporate

Practice Description

Jim counsels domestic and foreign businesses, local governments and school districts, universities, and individuals, helping with cybersecurity and data privacy issues, advertising clearance, import, tariff, and customs matters, and operational and strategic relationships and transactions. He also assists clients with protection and monetization of intellectual property and technology services and products, using licenses and other commercialization and development agreements. He addresses software, web and mobile app opportunities and issues.

360 Attorneys. 19 Offices. 1 Firm. Southeastern Strong. 39

© 2020. Burr & Forman LLP

360 Attorneys.
19 Offices
1 Firm.
Southeastern Strong.

33 **BURR FORMAN MCNAIR**

© 2020. Burr & Forman LLP

Get Connected

[linkedin.com/company/burrforman](https://www.linkedin.com/company/burrforman)
 @burrforman
 www.burr.com

Thank you
for your
participation

© 2020. Burr & Forman LLP