



ALABAMA  
ASSOCIATION OF  
SCHOOL BOARDS

2019 Leadership for Financial Accountability



ALABAMA  
ASSOCIATION OF  
SCHOOL BOARDS

## CyberRisk and Compliance

Dr. W. Greg Price – Troy University  
Pike County Board of Education

# CyberRisk and Compliance

## Agenda

- Cyber Risk – prompting action and review
  - Why are we concerned?
  - What are common examples in education?
- Major Regulatory Concerns?
  - Alphabet soup - who's expecting what?
  - Alabama Data Breach and Notification Law
- Q&A

# CyberRisk and Compliance

## Cyber Risk

▪Any risk of financial loss, disruption or damage to the reputation of an organization from some manner of failure in its information technology systems



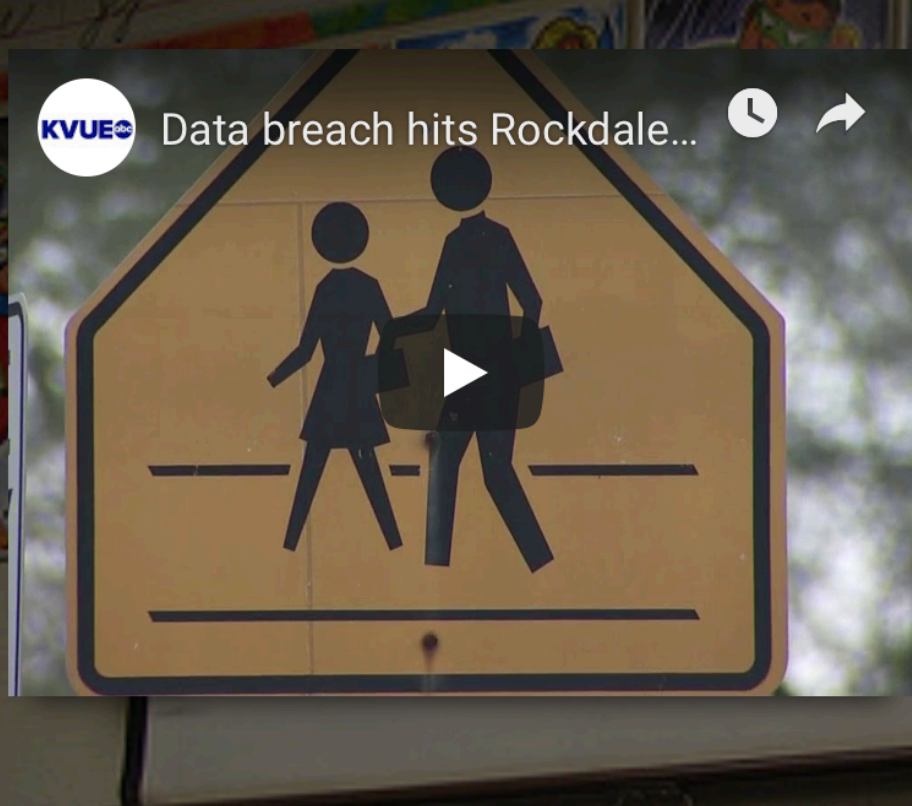
# CyberRisk and Compliance


## Cyber Risk

### ▪ Common Examples

- Identity Theft
- School Official Impersonation
- Damage to reputation, loss of confidence
- Damage to school resources, computers, networks
- Safety concerns
- Lawsuits alleging trademark or copyright infringement
- Misinformation
- Invoice/Accounts payable errors
- Disgruntled employees - access controls
- Regulatory compliance failures

# CyberRisk and Compliance



**KVUE** Data breach hits Rockdale...  

**MARCH 1, 2018**

## TARGETED PHISHING ATTACK LEADS TO IDENTITY THEFT, TAX FRAUD

Texas district officials said an employee responded to a sophisticated phishing email from a scammer pretending to be the superintendent. The criminal actors requested - and received - copies of W-2 tax forms for all

# CyberRisk and Compliance



Data breach at San Diego ...



**LIVE** DEVELOPING STORY

**DATA BREACH AT SAN DIEGO UNIFIED SCHOOL DISTRICT**



5:05

DECEMBER 21, 2018

## ON CUSP OF WINTER BREAK, DISTRICT DISCLOSES MASSIVE DATA BREACH

San Diego Unified schools discovered an unauthorized user was gathering log-in information from staff via an email phishing

# CyberRisk and Compliance



NOVEMBER 1, 2018

## DISGRUNTLED FORMER EMPLOYEE STEALS SENSITIVE DISTRICT DATABASE

A former Chicago Public Schools (CPS) employee left her job with more than just her final paycheck: she allegedly took the personal information of about 70,000 people contained in a CPS database. This incident



# CyberRisk and Compliance



APRIL 14, 2018

## SCHOOL DISTRICT PAYS \$10,000 BITCOIN RANSOM TO RESTORE ACCESS TO CRITICAL SYSTEMS

Affected by ransomware and unable to restore its own technology systems after several weeks had passed, a Massachusetts school

# CyberRisk and Compliance

## Most Common Techniques for Data Theft

- Social Engineering – Phishing, Spear-Phishing
- Ransomware
- Too much access, poor access controls
- Allowing personal devices on school networks
- Lack of proper IT controls, such as patching
- Angry employees
- Allowing students to serve as IT experts

# CyberRisk and Compliance

## Regulatory Concerns - Alphabet Soup

- FERPA
- PCI
- GLBA
- HIPPA
- CIPA/COPPA
- PPRA
- NSLA
- IDEA
- EUGDPR
- AL-DB Act



Mmmm. Mmmm. Good.  
Regulatory Compliance.

# CyberRisk and Compliance

## Alabama Data Breach Notification Act - June 2018

Requires an entity to react formally to a suspected data breach

- What is the nature and scope of the breach?
- What type of PII is involved, and, to whom does it belong?
- Is it believed that the PII has been stolen?
  - If so, is there an expectation of harm to the person(s)?
- What actions have occurred to contain the breach?
- How many Alabama residents were affected?

“Yes” to these questions requires notification.

# CyberRisk and Compliance

## Alabama Data Breach Notification Act - June 2018

Requires an entity to react formally to a suspected data breach

- If the PII was stolen and harm could result, we must notify the a
  - Notice can be sent via email or USPS
  - Notice must contain explanation of event and remedy
- If PII wasn't stolen and no harm is anticipated, no notice
  - But, the entity must document the incident
  - And, retain the documentation for 5 years
  - WHAT's an incident?

# CyberRisk and Compliance

## Alabama Data Breach Notification Act - June 2018

Requires an entity to react formally to a suspected data breach

- If more than 1,000 Alabama residents were affected
  - The Alabama Attorney General must be notified
  - Credit reporting agencies must be notified
  - Fines and additional actions are likely to follow

# CyberRisk and Compliance

## Incidents - common types

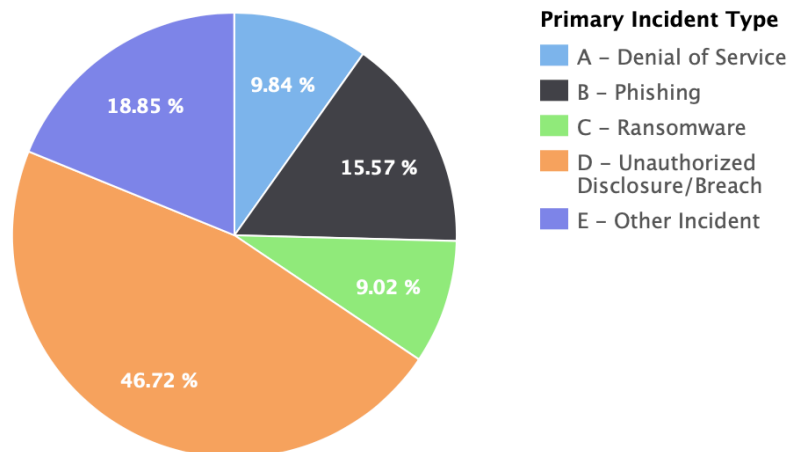
**The most frequently experienced type of K-12 Cyber incident in 2018 were data breaches. The breaches occurred most frequently as the result of:**

- **Unauthorized disclosures of data by employees, mainly due to human error**
- **Unauthorized disclosures of data by vendors and partners**
- **Unauthorized access to data by K-12 students**
- **Unauthorized access to data by external actors**

# CyberRisk and Compliance

## K-12 Cyber Incidents: 2018

Note: Publicly-disclosed incident reports represent a subset of actual incidents experienced by schools and districts. Public reports may also be inaccurate or ambiguous.







ALABAMA  
ASSOCIATION OF  
SCHOOL BOARDS

Q&A

Thank You!