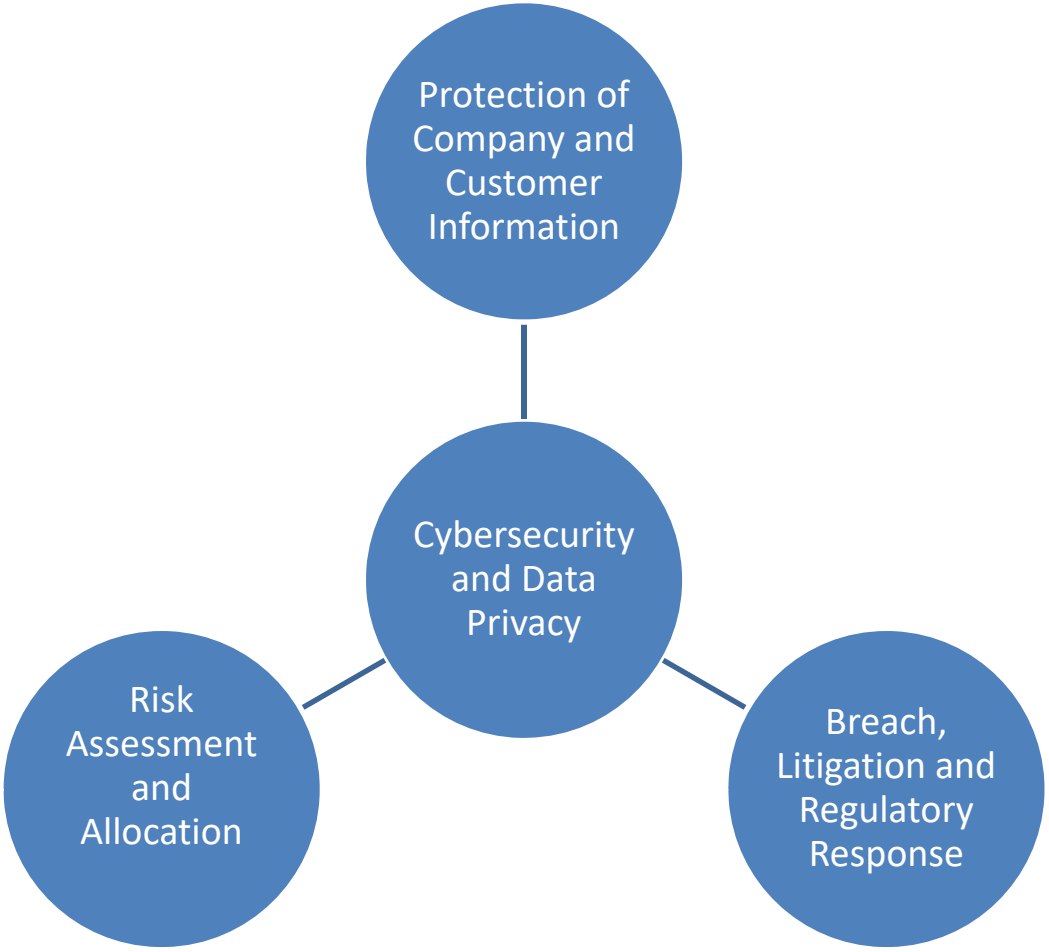
Data Privacy and Cybersecurity for School Districts

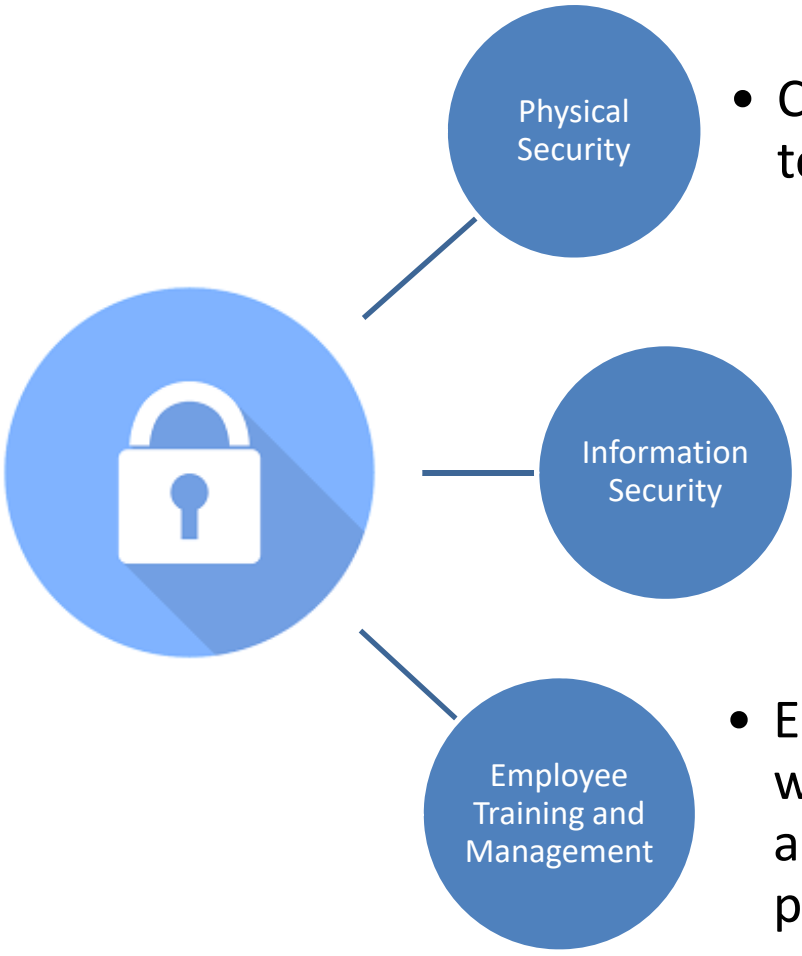
Jacob Koering

March 9, 2018

What are Cybersecurity and Data Privacy?



Protection of Company and Customer Information



- Control access to key areas
- Computer and data systems controls and protections
- Ensure those with proper access use it properly

MILLER CANFIELD

Risk Assessment and Allocation

Understand Company Risk

- Know what information you have where it is

Allocate in Contracts and Relationships

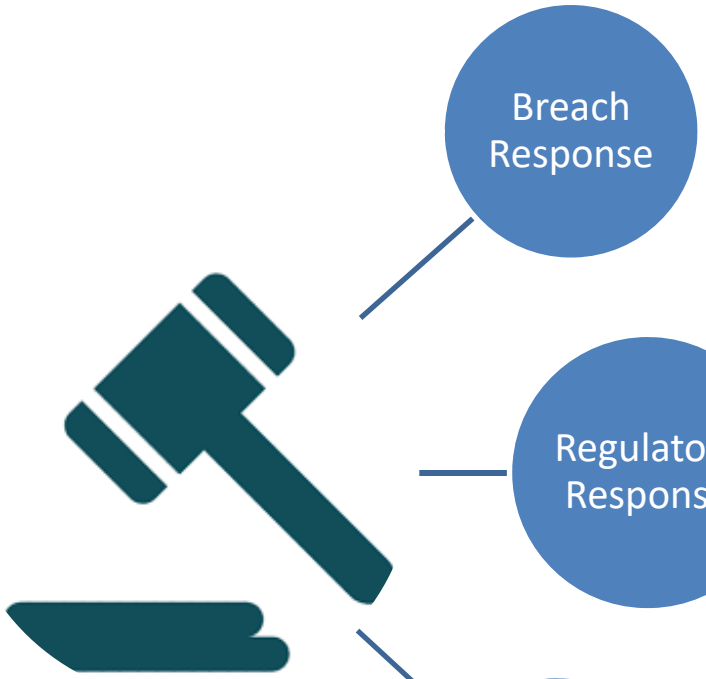
- Know what you share with customers, partners, clients, and vendors

Appropriately Insure

- Fill gaps in cyber risk profile with insurance

MILLER CANFIELD

Breach, Litigation and Regulatory Response



Breach Response

- Detection and response to intrusion or loss of data

Regulatory Response

- When state or Federal agencies come calling, what do you do?

Litigation

- The almost inevitable result of customer data loss

MILLER CANFIELD

School Districts are Attractive Targets

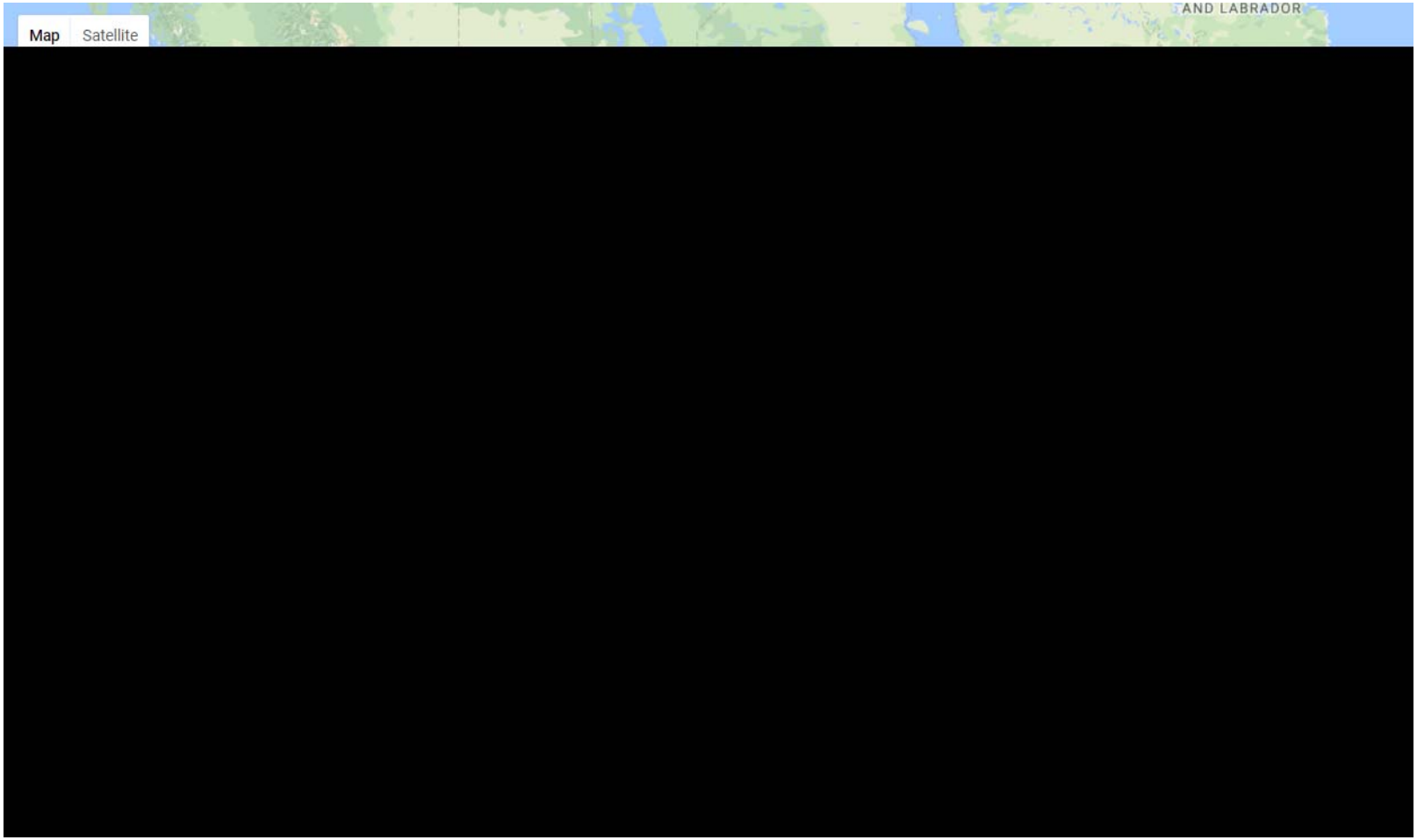
Education sector ranked 6th for cyber incidents in 2016 per Verizon's Data Breach Investigations Report

Districts have PII and in some cases PHI of students and employees that can be used for identity theft

Cybersecurity Programs at school districts are frequently weak, making intrusion easier

- Budgets are already stretched thin
- Networks can be sprawling and have many entry points, i.e. staff at different schools, parents, vendors, etc.

School Cyber Incidents Since January, 2016



MILLER CANFIELD

Data Privacy Regulation

Family Educational Rights and Privacy Act

- Applies to all educational institutions that receive federal funding and education service providers
- Limits disclosure of education records
- Federal funding can be terminated for violations, though it has not happened yet

Common Threats

Ransomware

- Hacker introduces malware that encrypts data or compromises system function and only provides key to unlock upon payment of ransom

Phishing and Spear Phishing

- In phishing emails, hacker drafts generic message and casts wide net, hoping someone will bite
  - E.g. Nigerian prince wants to deposit $5 million in your bank account
- In spear phishing emails, recipient is specifically targeted
  - E.g. Hacker spoofs CFO and emails HR to send all district employee W-2s

Consequences of Cyber-Attack

Loss of access to data and functionality of system

- School districts throughout country have had to pay ransom to unlock systems
  - E.g. Ransomware prevented New Jersey school district from administering online statewide tests as scheduled

Theft of PII and PHI

- Hackers obtain personal information regarding students and employees
  - In 2014, 10,000 Maryland school district employees had data compromised in cyber-attack
  - In 2014, a New Jersey charter school obtained the personal information of New Jersey public school students to mail them registration forms
  - In 2013, students in a Long Island school district had their personal information accessed and posted online, including whether they received free or reduced lunches
- Identity theft or other issues ensue

Prevention and Mitigation

Districts must devote resources to developing and implementing Cybersecurity Plan

Employee training is a must

- Human error is a leading cause of initial intrusions

Technology and policy-based safeguards:

- Firewalls, network monitoring, encryption, and multi-factor authentication
- Develop and maintain information security plans and data breach incident response plans
- Consider security of and vulnerabilities in systems of vendors who have access to district systems and information

Jacob Koering
koering@millercanfield.com
312.460.4272