Managing Your Cybersecurity Risk:

Recognizing the Risks and Best Practices

April 19, 2018

Presented by:
Jacob Koering
Lead, Cybersecurity and Data Privacy Practice

What is Cybersecurity?

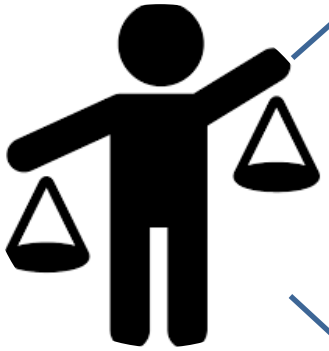
MILLER CANFIELD

Protection of Company and Customer Information

- **Physical Security**
  - Control access to key areas
- **Information Security**
  - Computer and data systems controls and protections
- **Employee Training and Management**
  - 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 data loss

MILLER CANFIELD

Why School Districts Must Care

Districts collect and store desirable PII and PHI of students and employees

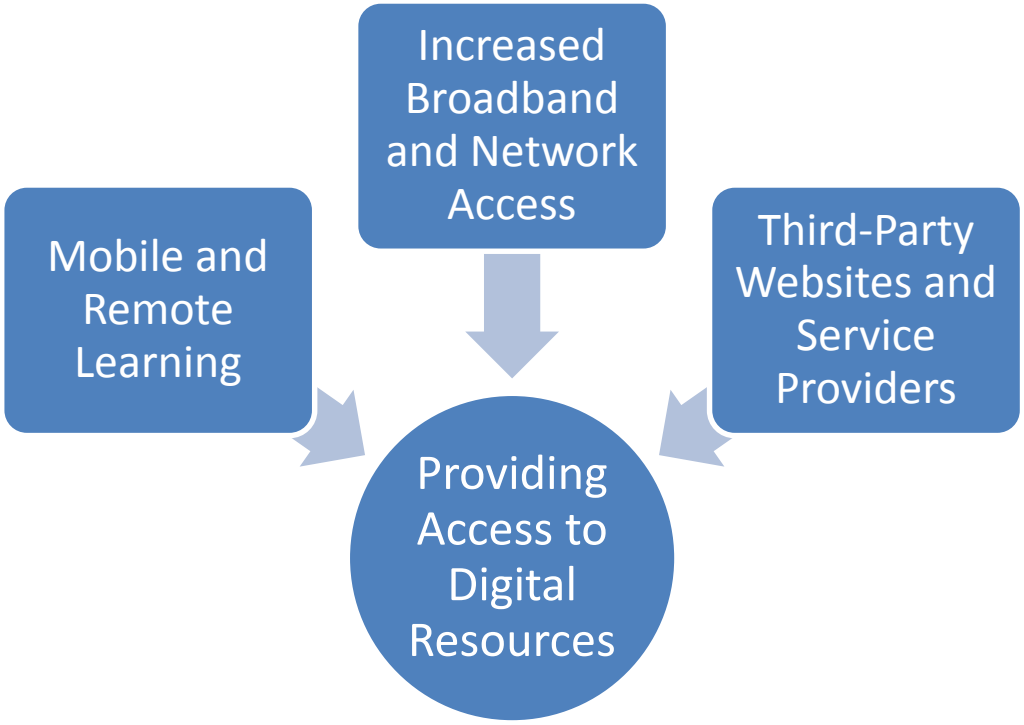
Districts transfer large sums of money to employees, vendors, and are attractive targets

Regulatory framework, standards and enforcement are complex, challenging

MILLER CANFIELD

School Cyber Incidents Since January 2016

The Ongoing Digital Transition



Family Educational Rights and Privacy Act

Regulates:

- Educational institutions that receive Federal funding
- Educational service providers working with those institutions

Requires:

- Protection and limited disclosure of educational records

Enforcement:

- U.S. Department of Education, Secretary of Education
- Enforcement results in fines, loss of Federal Funding

MILLER CANFIELD

Children's Online Privacy Protection Act

Regulates:

- The online collection, use, and disclosure of personal information from children under the age of 13.

Requires:

- Covered website and online service operators to give notice, obtain "verifiable" parental consent, allow access to information

Enforcement:

- Federal Trade Commission (key enforcement priority) – COPPA Rule (15 USC 6501-06)
- Injunctions, enforced compliance, damages are possible

MILLER CANFIELD

Health Insurance Portability and Accountability Act

Regulates:

- Health providers, health plans/insurers, and business associates
- Only applies to schools in limited, specific circumstances

Requires:

- Compliance with standards for handling individually identifiable health information (called the "Privacy Rule")
- Maintaining the security of electronic protected health information (called the "Security Rule")

Enforcement:

- Department of Health and Human Services
- Penalties based on level of negligence, $100-$50K/violation (Max $1.5M/year)

MILLER CANFIELD

Michigan Breach Notice Statute

Regulates:

- Breach notification involving a Michigan resident's "personal information"
- Personal Information: Name + social security number, driver license number or financial account information/access code

Requires:

- Notice of access/acquisition of personal information to the resident and to consumer reporting agencies
- Without unreasonable delay

Enforcement:

- By state attorneys general

MILLER CANFIELD

Who are the Threats?

- Negligent or malicious insiders

- Third-party vendors with system access (i.e. the Target breach)

- Malicious hackers
  - Profiteers and “hacktivists”

Common Attack Methods

- Insider Attacks
- Social Engineering
- Exploitation Malware
- Extortion and Blackmail

Insider Attack Example: The Disgruntled Employee

Insider attack is generally ***intentional***

Hard-to-predict behavior

- Comes from a person with access and authority
- Important to curb access if hostile behavior is determined

May seek to profit, may seek to damage

The Key to Prevention

- System architecture and monitoring
- Prevention = knowledge insider will not "get away with it."

MILLER CANFIELD

Social Engineering Example: Phishing and Spear-phishing Emails

Phishing: general email targeting large numbers

Spear-phishing: relies on specific knowledge and specific targets

Both seek access to secure systems

- Generally looking for usernames/passwords, access to private data
- Also used to reroute funds (vendors, paychecks)

The Key to Prevention

- Employee training
- Sound system architecture

MILLER CANFIELD

Exploitation Malware Example: the Infected Email

Like phishing/spear-phishing, generally relies on people

- Emails with attachments/links are ubiquitous – can contain malware, or link to malware
- People in a hurry click before they think

Exploitation malware needs to be activated to get access

Once activated, malware spreads to connected systems

- Can stay resident, monitor system operation, steal info (Trojan virus)
- More recent malware can try and access secure connected systems (Emotet)

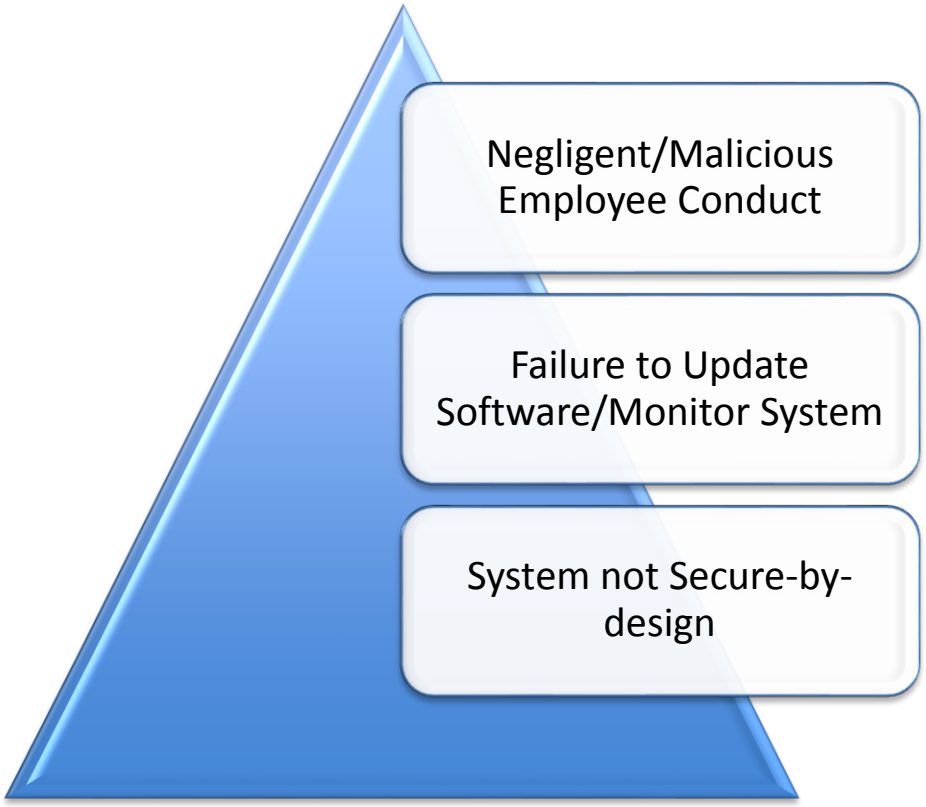
The Key to Prevention

- Employee training and communication
- System architecture, updated virus protection software

Extortion/Blackmail Example: Ransomware

- Can come from social engineering or network intrusion
- Encrypts key systems, data, rendering them unusable
- May require payment to unlock
- The Key to Prevention
  - Employee training and communication
  - System architecture
  - Can potentially avoid payments with frequent, isolated backups

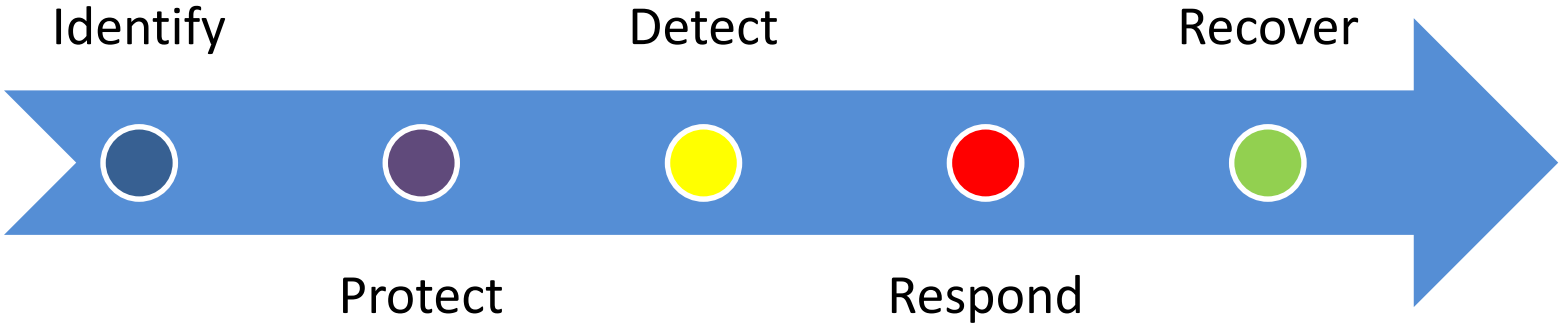
Why Cyber Incidents Happen



Minimizing Liability: Compliance with Regulations and Best Practices

Employee training	Silo information and restrict access	Technical safeguards	Policies and procedures
Maintain and drill incident response plan	Segregation between business and operations	Physical security	Information sharing

The NIST Framework as a Planning Tool



Successful Cybersecurity Outcomes

Reduce risk of successful attack

Increase timely detection and mitigation of attacks

Reduce financial exposure

MILLER CANFIELD

Questions?

Jacob Koering
koering@millercanfield.com
312.460.4272

millercanfield.com