OCTOBER 14, 2020

Cybersecurity and Environmental Management

PRESENTED BY

Colman McCarthy | *Partner* | Kansas City/Los Angeles
Dalton Mott | *Associate* | Kansas City

HEALTH / SCIENCE / TECHNOLOGY / SHB.COM /
Critical in a crisis, creative in court.®

SHOOK HARDY & BACON

Speakers

HEALTH / SCIENCE / TECHNOLOGY / SHB.COM /

Colman McCarthy

Parntner/Director of Shook's Privacy Compliance Task Force

cdmccarthy@shb.com

Dalton Mott

Associate, Shook's Environmental and Toxic Tort Group

dmott@shb.com

SHOOK HARDY & BACON

Overview

01 **Threats to the Environmental Sector**

02 **Ransomware and Business Email Compromises**

03 **Data Privacy Concerns**

Overview

- Many industries subject to environmental management are considered critical and subject to increasing cybersecurity threats
- Threats include ransomware and business email compromises
- Developing area of law and guidelines, regulatory oversight is not always clear
- Environmental management is not the biggest data privacy concern but concern does exist

MINIMIZING LEGAL RISKS

Cybersecurity Threats to Environmental Management

Critical Industries

- Industries that the Cybersecurity and Infrastructure Security Agency identify as critical:
  - Chemical
  - Commercial facilities
  - Emergency services
  - Energy
  - Government facilities
  - Water

Type of Consequences

Area	Description
Loss of Confidentiality	Loss of information, critical data, customer information, financial data, etc.
Loss of Integrity	The critical system is in operation, but the company cannot control the system or the process; i.e., someone external to the company/entity is controlling the system
Loss of Availability	Denial of Service type attack, where system becomes inoperative or ineffective
Destruction of System	Destruction of system with inability to restore

Water Systems

- Both water and wastewater systems are at risk
- Maroochy Water System attack
- Regulated by EPA but EPA cannot gather data and has not set guidelines

Chemical/Pollution Controls

- Vulnerable due to computerized operating systems
- Even unconnected systems may be at risk
- Major consequences if there is a release
- Regulated by DHS at least for chemical plants

Remediation Systems

- Computerized remediation systems are becoming more common
- Consequences may initially be less, but liability is unknown
- EPA's Remedial Design/Remedial Action Handbook does not speak to cybersecurity nor does the current model consent decree

2014 German Steel Mill Attack

2015 Ukraine Power Grid Attack

2017 Saudi Petrochemical Attack

MINIMIZING LEGAL RISKS

Ransomware and Business Email Compromises

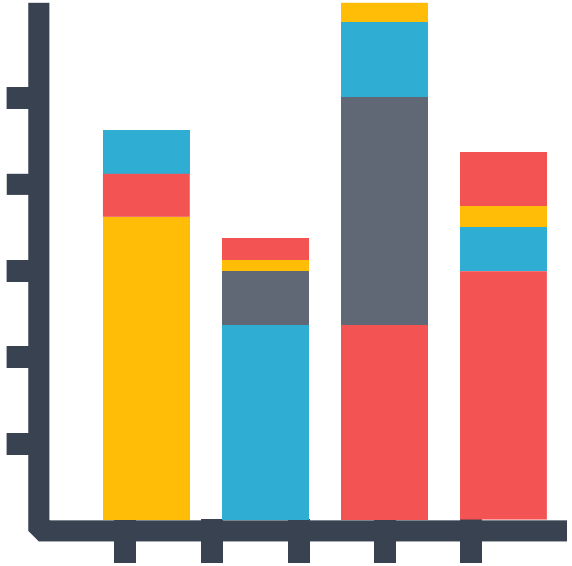
Data-Breach Stats

- 287 days on average to ID and contain a breach
- 2021 Average cost (38% due to lost-business cost)
  - USA - $9.05 million
  - Global - $4.24 million
  - Energy - $4.65 million
- Entities with incident-response measures in place saw an average **48% drop** in the cost of a breach

*IBM/Ponemon Institute, *2021 Cost of a Data Breach*

Ransomware Statistics

- Q3 2021
  - Average payment = $139,739
  - Median payment = $71,674
- Data exfiltration threatened 83.3% of the time
- Top variants
  - Conti
  - Mespinoza
  - Sodinokibi / REvil
- Top attack vectors
  - RDP
  - Email phishing



*Coveware, https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

Ransomware Attacks

- What is ransomware?
  - Encryption / Data exfiltration
  - Ransomware-as-a-service
- To pay or not to pay
  - Backups?
  - Insurance
  - OFAC Sanctions
- Colonial Pipeline
  - Compromised through a single account not in use
  - $4.4 million ransom payment
  - 100 GBs of data stolen

Business Email Compromise

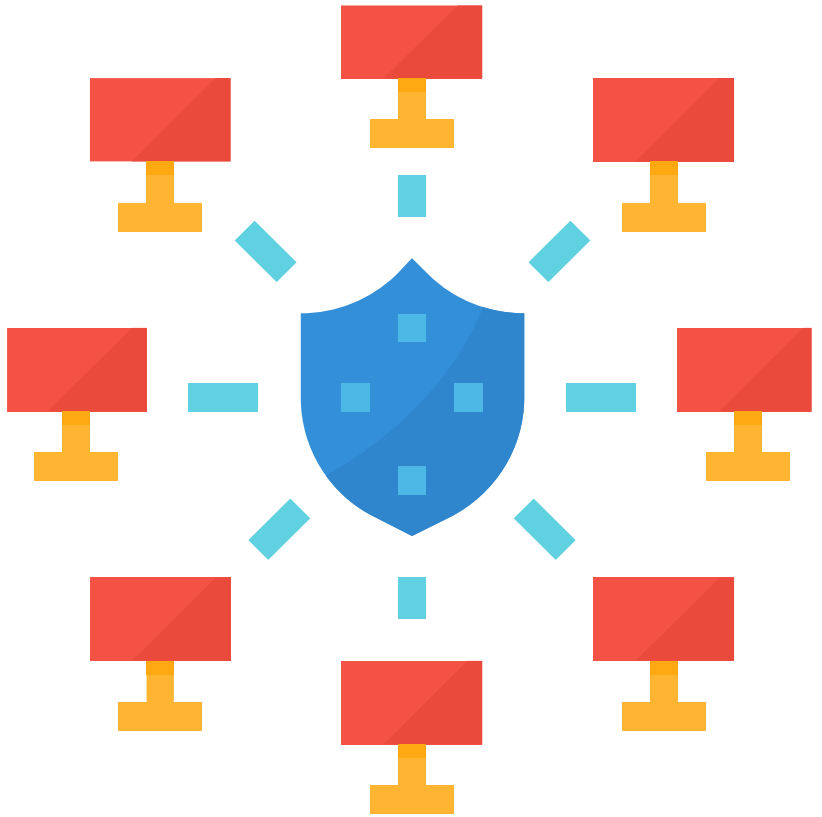
- What is a business email compromise?
- What's the goal?
  - Financial motivation
- How does it originate?
  - Phishing
  - Vendor / customer breach
- Tips to help prevent
  - Multi-factor authentication
  - "[External]"

Legal Issues to Consider

- Notifying insurer
- How to engage a forensic firm to maximize privilege
- Ransomware - whether to pay the ransom
- Whether the incident is a notifiable event, who to notify, and when
- Liability created by statements to employees and public
- Evaluating potential third-party liability / indemnification
- Cyber insurance coverage/exclusions

Risk-Minimization Techniques

- Secure backups
- Multi-factor authentication
- Endpoint detection and response
- Managed network monitoring
- Regular third-party assessments
- Incident response plan
- Tabletop exercise
- Cyber insurance
- Employee training / Phishing campaigns

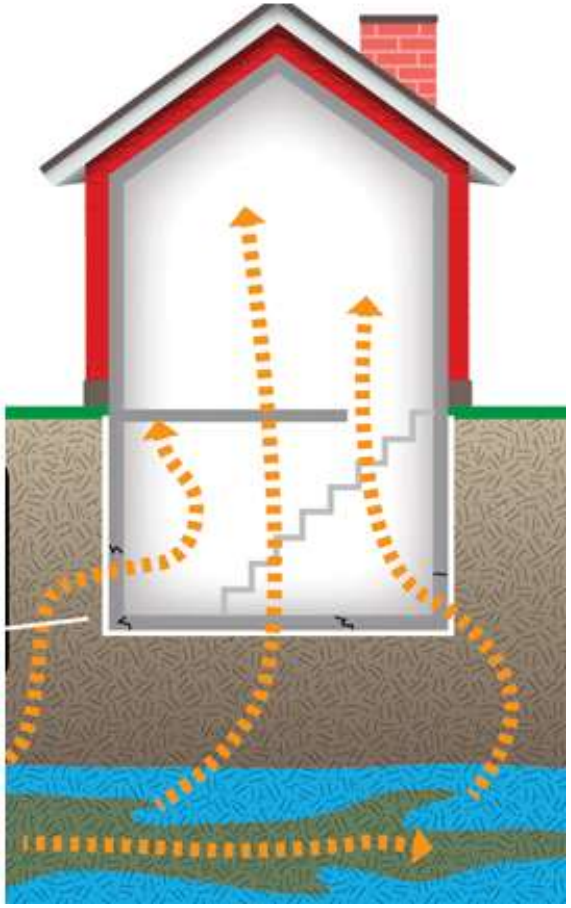


MINIMIZING LEGAL RISKS

Data Privacy Considerations

What Personal Data is Collected?

- Health Assessments – Surveys
- Vapor Intrusion Work
- Employee health and safety programs



Comprehensive privacy laws

- California Consumer Privacy Act
- Virginia Consumer Data Protection Act
- Colorado Privacy Act

Comprehensive privacy bills

(drawing on CCPA or GDPR)

- Alabama HB 216
- Alaska HB 159, SB 116
- Arizona HB 2865
- Connecticut SB 893
- Florida HB 969, SB 1734
- Illinois HB 2404
- Kentucky HB 408
- Massachusetts H 142
- Minnesota HF 36, HF 1492, SF 1408
- New Jersey A 3283, A 3255
- New York A 400, S 567, A 3586
- North Carolina SB 569
- Oklahoma HB 1602
- Utah SB 200
- Washington SB 5062
- West Virginia HB 3159

What About Kansas, Missouri, Nebraska, and Iowa?

- Data-breach-notification laws
  - "Personally identifiable information"
  - Notice to individuals and regulators
- Reasonable-security laws:
  - …implement and maintain **reasonable security procedures and practices** that are appropriate to the nature and sensitivity of the personal information…
  - …**shall require by contract** that the service provider implement and maintain reasonable security procedures and practices…

Practical Tips

- Data minimization = liability minimization
- Data mapping/inventory
- Privacy/security provisions in contracts for vendors/contractors


SHOOK
HARDY & BACON