2023 Fall Conference–

Managing Cyber and Other Threats for Bond Issuers

Technology, Privacy and Cyber Risk Practice

- Cybersecurity
- Incident Response
- Privacy Program Management
- Compliance
- Tech Transactions
- Vendor Management

IceMiller®
LEGAL COUNSEL

icemiller.com

Current State of Laws and Regulation

Business vector created by stories

Start here….

- Has target identified its most critical functions and systems?
- Does target know what types of data it manages?
- What are target's baseline security controls?
- Are there data backup processes (backups) in place for the most important business systems?
- Do staff have an understanding of threats (e.g ransomware, phishing, etc.), how to defend against email fraud, and how to protect themselves online?
- Are critical system and access to the data well documented?
- Does target rely on vendors?

The Vendor Threat

The Vendor Threat

Insurance

First-Party Coverages	
Funds Transfer and Computer Fraud	Traditional Coverage
	Social Engineering
Network Interruption	Security Failure
	System Failure
	Contingent BI
Data Restoration	Security Failure
	System Failure
Cyber Extortion	
Breach Response	Notification
	Investigation
	Remediation
	Public Relations

Created by D3images - Freepik.com

Third-Party Coverages	
Privacy Liability	Privacy Claims
	Business Records Claims
	Regulatory Claims
Network Security Liability	
Media Liability	
Technology Errors & Omissions	


IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

Artificial Intelligence

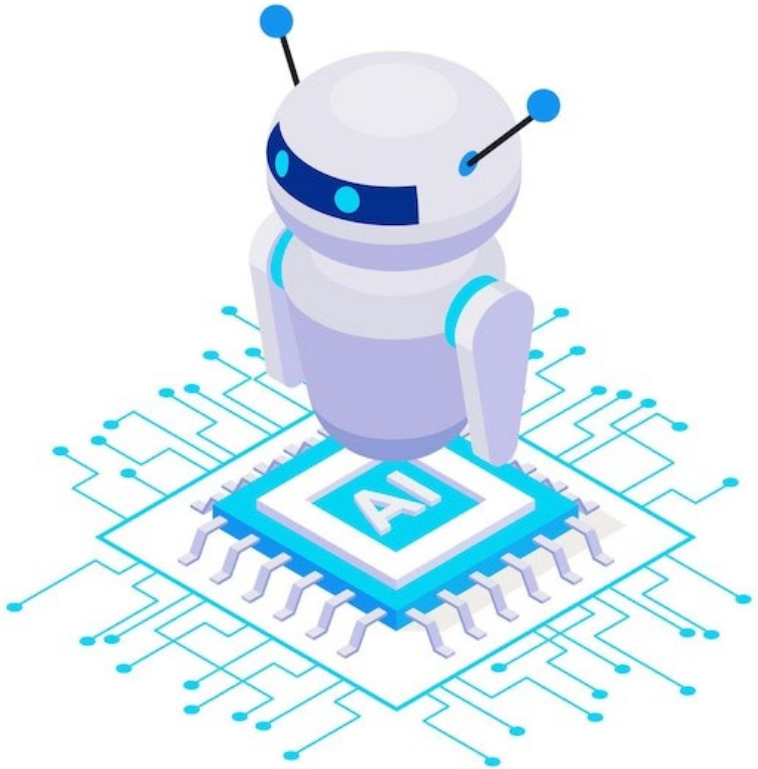


Image by macrovector on Freepik

Privacy Trends

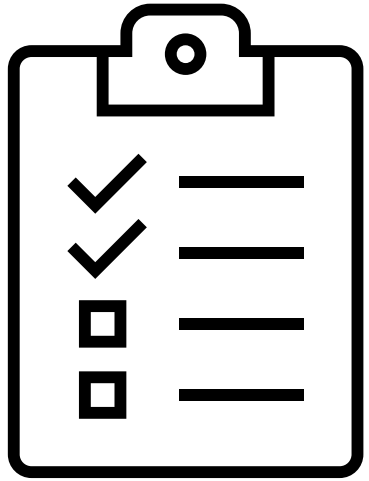
Privacy

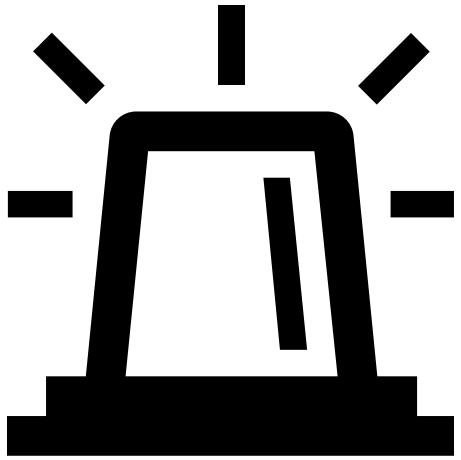
- Who can unlock the folder?
- Who has the keys to the lock?

VS

- What they do with the contents of the folder?
  - What do they do with the information?
  - Why? How? When?

Physical Security and Kinetic Threats





SOPs

Develop policies & procedures to guide incident response plans and employee expectations.

Examples: Active Threats, Bomb Threats, Trespass, Emergency Notifications, Lockdowns, & more.

Tabletop Exercises

Test employee readiness and ensures that efficacy of the SOPs.

Provide hands-on exposure to real-life scenarios while providing a judgment-free test environment.

Investigations

Review and analyze internal compliance with existing policies and procedures.

Suggest improvements on employees training, existing policies, & other proactive measures.

IceMiller
LEGAL COUNSEL

Active Threat SOPs and TTXs

Bomb Threat SOPs and TTXs

Lockdown SOPs and TTXs

Trespass SOPs and Counseling

Emergency Notification SOPs

E-Alert Simulations and SOPs

Implementation of Police / Security Officer Personnel

Regulatory Compliance

Investigations of Safety Missteps

Law Enforcement Relationship Building

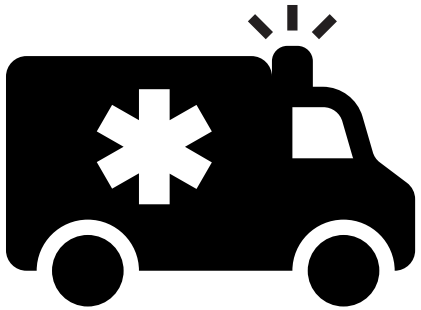
Crisis Management & Response

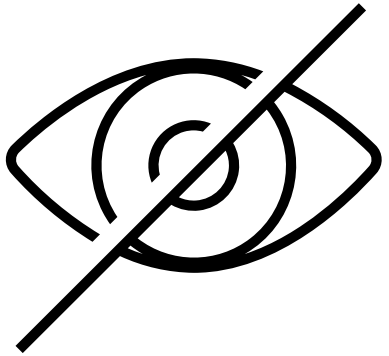
Safety and Cybersecurity Vendor Analysis

Mini-Table Top Exercise (TTX)

Meeting illustration vector created by pch.vector - www.freepik.com

Hot Item – AD Tracking and Healthcare





Mini-Table Top Exercise (TTX)

Red screens appear on computers throughout your organization. All appear to have been infected with the same ransomware. A message is displayed demanding payment of Bitcoin, valued at approximately $100,000, for the decryption key and warning the key will expire unless payment is received within 48 hours. The message also provides instructions to contact the threat actor(s) (TA).

- What actions would be taken at this point? By whom?
- What are your priorities here?
- Should the TA be engaged?
  - Who should engage the TA?
- What communications or notifications (if any) would be made?

Mini-Table Top Exercise (TTX)

36 hours has elapsed.

Several media outlets begin reporting that your organization is experiencing a ransomware attack. You have received multiple media inquiries asking you to comment on the ransomware incident. The media stories are gaining wide attention online and within social media platforms.

- Do you pay the ransom?
- Who would you contact if you need additional assistance?

Mini-Table Top Exercise (TTX)

40 hours has elapsed

A security researcher uncovers a series of posts on the Dark Web and contacts your organization. The researcher believes that the posts purporting to be from a well-known hacker group are genuine and the threat actors have gained access to personally identifiable information (PII). The hacker group has provided a small number of data records to verify their claims and are willing to sell the information for “the right price.”

- Do you pay the ransom?
- What are your public affairs concerns?

Lessons Learned and Preparedness

Q1: Your favorite phishing email?

Q2: What is the “right” level of funding?

Q3: Where is the “right” place the Chief Information Security Officer (CISO) in your org?

Q4: How many have encountered cybersecurity questionnaires in audits, bonds, and/or insurance services?

Q5: Who has strong standard contract terms for technology, data, privacy, and security?

Q6: A suspicious event occurs such as ___. What do you do?

Thank you!