Cyber Liability

Presented by: Judith Pearson

Contact information:

jpearson@woodruffsawyer.com

303.917.7766

ITA

INDEPENDENT TRUSTEE ALLIANCE

Agenda

- What is cyber liability and why is it important?
- Exposures
- Insurance policy description
- Recent claim
- Best practices/Risk management techniques
- Training options
- Questions

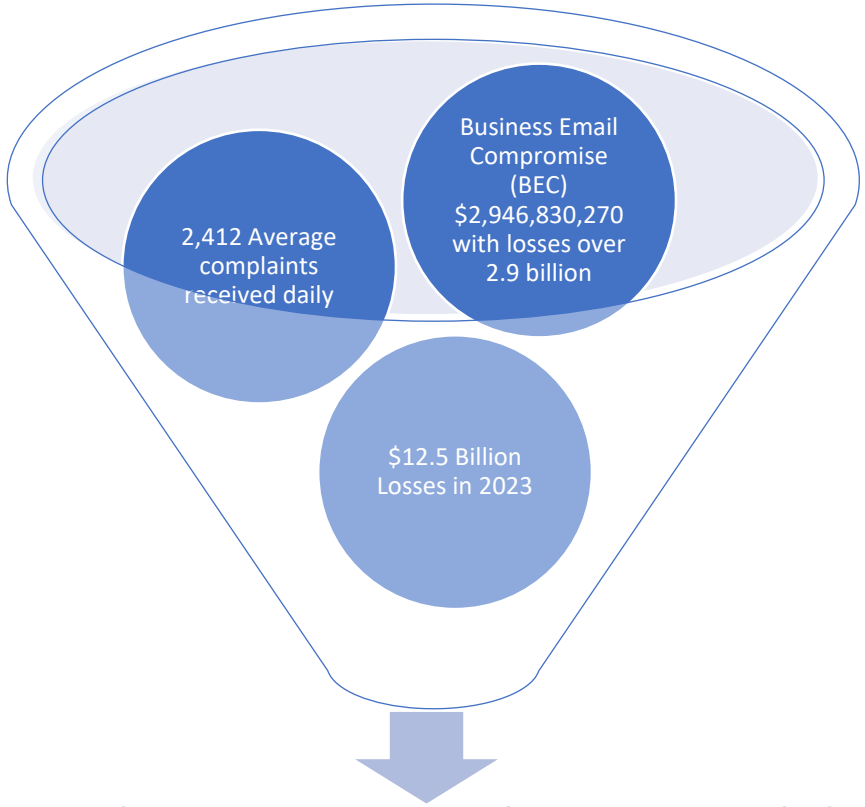
What is cyber liability insurance

Cyber liability insurance helps cover costs associated with data breaches and cyberattacks on your business. Those costs can include such things as lost income due to a cyber event, costs associated with notifying customers affected by a breach, costs for recovering compromised data, costs for repairing damaged computer systems. More importantly it's a service.

- Forensic investigations
- Litigation expenses
- Regulatory defense expenses/fines
- Crisis management expenses
- Business interruption
- System testing
- Cyber extortion
- Cyber crime (social engineering)

2024 FBI Statistics

- Fake invoices, banking account change requests, and demands for immediate payments Business email compromise increased 71% over last year.
- Vendor email compromises (VEC, where a supplier or vendor of the victim organization is impersonated) increased by 137%.
- Smaller organizations (less than 1,000 employees) saw the highest number of BEC attacks.



Fraudsters are increasingly using custodial accounts held at financial institutions for third-party payment processors

Components of a Cyber Policy

NETWORK BUSINESS INTERRUPTION

FIRST-PARTY

Income loss arising from:

- Security Failure
  - DDoS Attack
  - Virus/Malware
- System Failure
  - Failed Upgrade
  - Human Error

NETWORK SECURITY & PRIVACY

FIRST-PARTY	THIRD-PARTY

- Unauthorized Access
- Transmission of Virus or Malicious Code
- Theft/Destruction of Data
- Cyber Extortion
- PII/PHI Data Exposed by
  - Hacker
  - Lost Device
  - Rogue Employee
  - Physical Records

FIRST-PARTY VS. THIRD-PARTY COVERAGE

NETWORK SECURITY & PRIVACY

First-Party	Third-Party
• Forensics • Legal Advice • Notification Cost • Call Center • Credit Monitoring • Public Relations • Data Replacement • Cyber Extortion	• Charges Levied by Credit Card Isuers • Consumer Suits • Customer Suits • Other Third-Party Suits • PCI-DSS Fines • Regulatory - Defense - Fines & Penalties

The number one exposure for trustees is cyber crime- need coverage for care custody and control of funds

Common Cyber Exposure Misconceptions

"WE USE A THIRD PARTY PAYMENT PROCESSOR, SO WE'VE TRANSFERRED THAT EXPOSURE"

- A data breach can occur while data is in transit, not only in the portal or platform used to access it.

"WE DON'T STORE ANY FINANCIAL INFORMATION OR PII ON OUR NETWORK OR DEVIVE"

- In some cases hackers have been able to intercept data in real time, "skimming" passwords, data, and other sensitive information

"WE HAVE UPGRADED OUR SECURITY BY TRANSFERRING OUR DATE TO A CLOUD PROVIDER"

- Cloud providers have the resources to invest in much higher security, but there is inherent vulnerability.
- The data in the could may be an attractive target for high-tech criminals
- Cloud vendors are very successful in limiting their liability

Recent claim example

Email compromise

- Bad actors watching emails between trustee and client
- Consistent monthly distribution

Attack at a busy time (YE close/board meetings)

- After distribution was initiated, there was a request to change wire instructions
- Back-office vender did not verify with a call back
- Bank verifies with trustee not back-office vender

Bank sent wire to new bank account

- Bad actor claimed they didn't receive the distribution
- Second distribution was made
- Trustee tried to reclaim wire (the 1st wire was returned/second wire unknown)
- Bank told trustee they have a 90-day waiting period before they decide the status of the second wire

Lessons learned: insurance perspective

- Trustees do not have custody, but they do have care and control of third-party (customer/beneficiary) funds.
- Fine line between E&O, Wire Transfer Fraud (crime) and cyber liability/social engineering (crime and cyber policy)
- How different insurance policies works
  - Required call back verification
  - Litigation/Subrogation expense
  - Exclusionary language
- Financial institutions liability (how and when decisions are made)
- Who else may have liability (vendors (back office/IT professional/ETC)

What to do in the event of a claim

Notify your cyber insurance carrier and broker.

- Typically, cyber insurance carriers will offer a 24/7 monitored hotline for companies to call and initiate an incident response playbook.

Engage legal counsel.

- Doing this first allows you to protect attorney-client privilege as you work through a cyber incident.
- Insurer has recommended firms

Engage a cyber forensics provider.

- Hired by the legal counsel on your behalf, these specialists can help you investigate the origins of the attack,
- ensure the bad actors are out of your system and identify what systems might have been impacted during the attack.
- They also can negotiate with ransomware attackers and identify the population of consumers potentially impacted by your breach.

If an attack led to funds being transferred out of your accounts, notify the FBI, other law enforcement agencies, and your bank within the first 72 hours will provide the best hope for recovering the funds.

Enhance security

- **Verified Requests**: Always confirm distribution requests and wire instructions through a secondary communication channel, like a phone call, especially if they come via email. Double- and triple-check the instructions, especially if there are urgent requests to change the wire instructions.
- **Secure Communication**: Use secure, encrypted email or platforms for sending sensitive information.
- **Regular Monitoring**: Frequently monitor accounts and transactions for any unusual activity.
- **Strong Authentication Protocols**: Implement strong authentication methods, such as multi-factor authentication, for accessing sensitive systems and information.
- **Update Security Measures**: Regularly update and patch your cybersecurity systems to protect against new vulnerabilities.
- **Incident Response Plan:** Have a robust incident response plan in place. This plan should include immediate steps to take if you suspect a breach or fraud.

Conclusion

Get training

- ITA members had a option for free training through the ITA-Few takers
- Training should include simulated attacks
- Bad actors adapt quickly – Stay up to date