

Understanding Cyberliability Insurance

Michael Ledbetter, CEBS

Partner
Ledbetter Partners LLC
Indianapolis, Indiana

Diane McNally

Senior Vice President
and Principal
Segal
New York City, New York



The opinions expressed in this presentation are those of the speaker. The International Foundation disclaims responsibility for views expressed and statements made by the program speakers.

International Foundation
OF EMPLOYEE BENEFIT PLANS 

Disclaimer

Segal Select Insurance Services, Inc. ("Segal"), a subsidiary of The Segal Group, is a specialty retail broker insurance. Any information and/or opinions herein provided by third parties have been obtained from sources believed to be reliable, but accuracy and completeness cannot be guaranteed. The contents of this presentation and any opinions expressed herein are intended for general education purposes only and not as professional advice specific to any person, entity or circumstance. It is not intended for use as a basis for making insurance-related decisions, including determinations of appropriate types or levels of insurance coverage, nor should it be construed as advice designed to meet the needs of any particular person, entity or circumstance. Please contact Segal or another qualified insurance professional for advice regarding the evaluation of any specific information, opinion, or other content. Of course, on all matters involving legal interpretations and regulatory issues, you should consult legal counsel.

Today's Session

- Overview of data protection landscape
- Cyberliability insurance discussion
 - Can you rely on an "add in" to your fiduciary liability or commercial insurance policy to protect your plan?
 - How much coverage is needed?
 - What is not covered?
 - Are you protected if you aren't performing regular, independent security checks?
 - What is the next trend for fiduciaries to consider?



Data Protection and Employee Benefit Plans

FBI Internet Crime Report 2023— Cyber Crime Continues to Grow



Plan Trustees Not Expected to Be Cybersecurity Experts, But...

- Most ERISA Trustees and Committee Members are not involved in day-to-day operation of plans and delegate “ministerial” duties to administrative staff, **however—**
 - Trustees retain a **duty of oversight**
 - Must remain diligent, involved and monitor plan
 - This includes reviewing the data protection efforts of plan and all vendors

Legal Obligation of Plan Trustees

- **ERISA Standard of Care:** You must exercise the level of care, diligence, and prudence to protect data other directors/coordinators in the same or similar circumstances
 - Ensure confidentiality and integrity of data
 - Protect against reasonably anticipated threats
 - Protect against unauthorized use or disclosure
 - Ensure compliance by workforce

DOL Guidance on Cybersecurity

- Guidance from DOL addressed Cybersecurity
 - Cybersecurity best practices
 - Tips for hiring a service provider
 - Online security tips (for participants/beneficiaries)
- Clarified duties regarding data protection
 - **Extensive vendor due diligence obligations**
 - **Trustees need to take proactive measures**

DOL Guidance on Cybersecurity

“If you’re responsible for plan administration and you’re hiring somebody to run your systems, keep that data, be your recordkeeper, you need to be attentive to whether or not they’re observing good cybersecurity practices.”

– Tim Hauser, Deputy Assistant Secretary for National Office Operations, DOL/EBSA

DOL Guidance— How Are Plans Responding?

- Monitoring data protection programs of all vendors with access to confidential information
 - Review process must be thorough and documented
 - Reports need to be regularly updated and reviewed
 - Some vendors may need to be put out to bid
- Fiduciaries may be found liable for lax oversight
- Contracts need to address cybersecurity obligations of your vendors

Cybersecurity—Advance Preparation Is Key

Programs Should Have:

Documented and Updated Risk Assessments

Written Information Security Policy

Incident Response Plan

Data Backup, Disaster Recovery
and Emergency Operation Plans

Hard Copies of all Policies and Cyber Insurance

Insurance is only part of a comprehensive data defense effort



Cybersecurity Insurance— A Lifeline for Your Organization

Insurance Considerations

- Free piece of legal advice...
 - Work with experienced, knowledgeable insurance professionals who understand your industry and your benefit plans and related organizations
- Cyber liability insurance and enhanced fidelity bonds can be a lifeline if you suffer a security incident



What Is Cyber Liability Insurance?



Incident Response

- Coach Services
- Legal Services
- Forensics
- Notification
- Credit Monitoring
- Public Relations



First-Party

- Extortion/Ransomware
- Data Recovery/
Restoration
- Business Interruption/
Extra Expense
- Crime/Social Engineering



Third-Party

- Privacy Liability
- Regulatory
- Payment Card
- Network Liability
- Media Liability

Cyber Insurance Application Process

Buyer Beware

- How long is the application process?
 - What information is needed?
 - How complex is the application?
 - What are key differences between carrier applications?
- Key application questions
- What happens if required technology has not been implemented?

Cyber Insurance Application Process

Warranty Statements

- In general, warranty statements are very broad attestations that the proposed insureds are not aware of any incident, act, knowledge, error, or omission which might result in a claim under the policy.
- Usually required for the first year of the coverage, but an important factor when applying for renewals and considering changing carriers
- Disputes can arise with the insurance company regarding the knowledge that may lead to insurance claim denials or even policy recession by the carrier



Cyber Insurance Application Process

Third Party Network Scans

- Carriers increased reliance on third party networks scans:
 - Bitsight
 - CyRisk Insight Engine
 - In-house proprietary scans
- Mixed feedback from clients
 - Scanning wrong URLs (e.g., union's site rather than fund's site)
 - Outdated scans
- Scans done periodically throughout the year/mid-term requirements



Problematic Exclusions and Issues

	Professional Services Exclusion		Mechanical/ Electronic Failure
	Criminal or Intentional Acts by Employees		Laptops and Portable Electronic Devices
	Not Following Minimum Required Practices		Property Damage Exclusions
	Systemic Events		War, Terrorism, or State Actors
	Unencrypted Data Exclusion		Not All Data Covered
	Sub-limits and Coinsurance		Limited Coverage Periods

Cyber Insurance and Incident Response Efforts

Typical Incident Response Services

Crisis Hotline

Reporting Urgent Event

- #800 or through a cyber app

Response Coaches

To Triage a Cyber Event

- Maintain client privilege
- Consultation, hours can vary
- Tender a claim to the carrier

Response Specialists

Support Response

- Forensics
- Public relations
- Notification services
- Call center
- Extortion
- Business interruption

What's in Your Incident Response Plan?



Cyber Insurance and Social Engineering Fraud



What Is Social Engineering?

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables
 - These “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems
 - Criminals build trust, convince users to act, exploit systems and disengage

Insurance Coverage and Social Engineering Fraud

- Attacks are generally covered by most carriers when malware is added, data is stolen or held hostage, or money transferred
- The coverage may have exclusions and require certain procedures to be followed to have a covered claim (independent call back provisions, etc.)
- If money is stolen, standard coverage limits are often sublimated to between \$50K and \$250K regardless of the full policy limit
- There may be similar coverage in other policies
- Larger coverage limits are typically available by having excess carriers participate in the insurance program

Social Engineering Application Questions

- Key Application Questions
 - Average volume and frequency of fund transfers over last 12 months, largest and totals? Domestic and foreign
 - Training to detect phishing and social engineering scams?
 - Do you authenticate vendor instructions?
 - Who is authorized to direct accounts payable to pay an invoice and authenticate instructions in place?
 - Authority on wire transfers, verbally, in writing and banking instructions?

Social Engineering and Excess Policy Coverage

- Stand-alone excess policies available for social engineering fraud
 - Typical attachment point of \$250,000
 - Requested limits are typically for \$1-Million to \$5-Million
 - Higher limits may be available depending on market appetite
 - Underwriter appetite can depend on which carrier writes primary coverage



The Evolving Cyber Insurance Marketplace

Changing Cyber Insurance Market

**Many carriers;
many approaches**

**Different risk appetites;
size/complexity**

**Various types of
insurance policies**

**Modular; watch for
gaps in coverage**

**Evolving
coverage and
services**



State of the Cyber Insurance Market



There remains an onus on Insureds for minimum/base controls

Including: Implementation of MFA; Secure RDP's; Robust backup procedures, training and Incident Response Plans



Rate increases have slowed but not for all industry sectors

More stability in premiums, including some decreases



Broader terms/conditions

Reduction/removal of co-insurance; Lower retentions; Increase in sub limits



Increase in cyber liability capacity YOY

Existing markets increase capacity as well as the introduction of additional market capacity

State of the Cyber Insurance Market



Increase in automatic renewals

Automatic renewals can still include changes to premium and terms, but no application requirement usually seen as a positive



Inconsistency with admitted/non-admitted markets still exists

Many carriers continue to use non-admitted paper to allow greater flexibility on rate and coverage changes



Move towards universal applications

Still evolving. Limited flexibility on terms



Interest in additional products/limits

Increased purchasing of Excess Social Engineering Fraud coverage

Future Trends

- Cyber attacks are more prevalent and sophisticated
- Keeping up with security measures is necessary to prevent future attacks
- Cyber insurance market capacity can depend on a carrier's profitability, risk tolerance and an insured's security measures
- Underwriting controls and requirements are increasing
- Cyber insurance pricing remains influx
- Claims continue to rise and could impact future limits and coverage
- Shared losses among other policies could impact future coverage

Key Takeaways



The threat environment has only become increasingly risky in a post-pandemic environment due to an increased number of remote workers and system vulnerabilities



A robust Cyber Liability Insurance policy is a 'must have' in today's perilous environment; ensure you have the appropriate coverage for your organization



Ransomware attacks and Social Engineering attacks are becoming more prevalent, more expensive, and more sophisticated in their ability to trick users



Having knowledgeable professional providers to review your insurance policies

**Your Feedback
Is Important.
Please Scan
This QR Code.**

Session Evaluation

