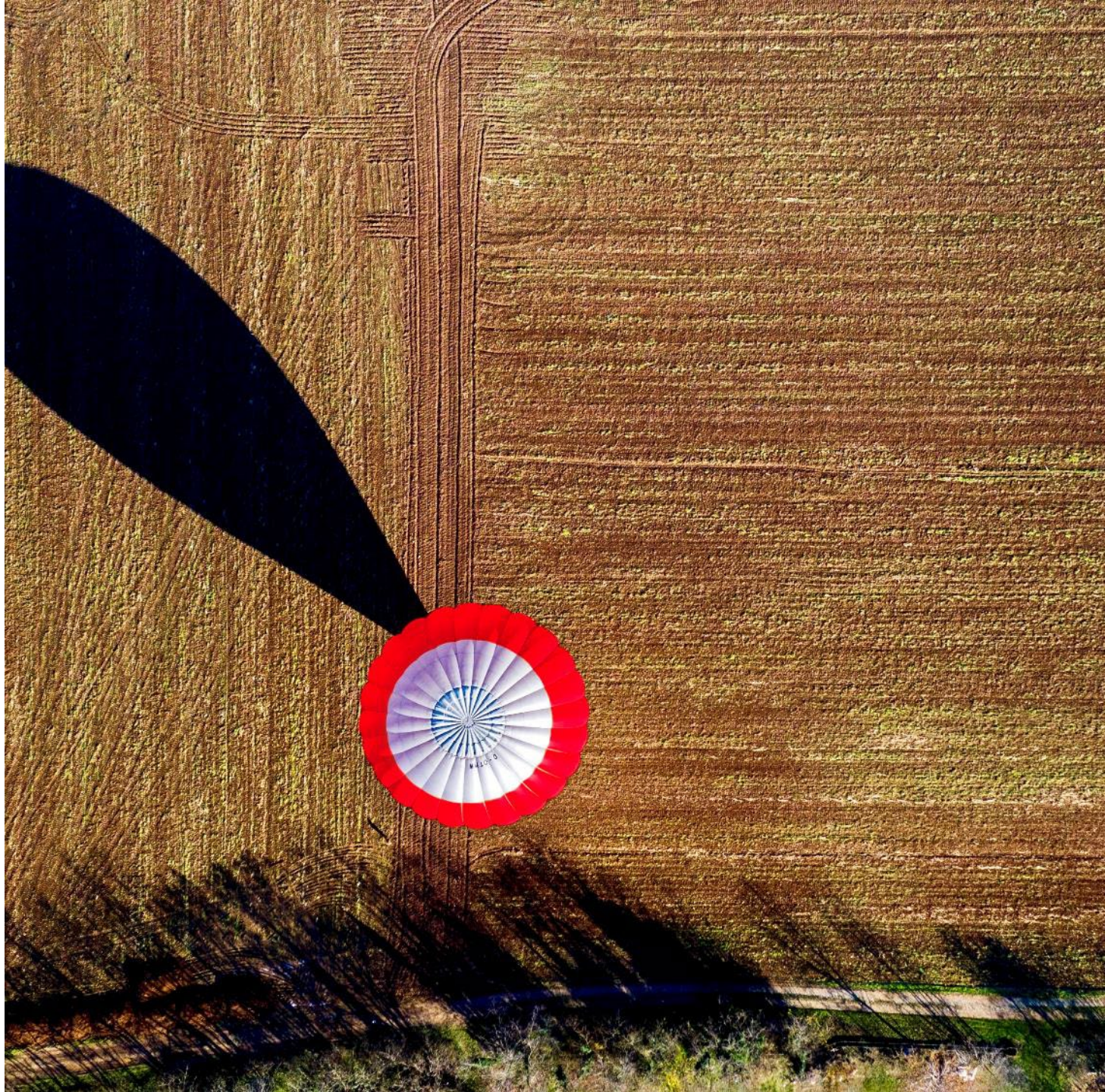
ERISA Advisory Council Meeting

Cybersecurity Insurance and Employee Benefit Plans

Presentation Date: September 8, 2022

AON

This document has been specifically prepared for the ERISA Advisory Council, U.S. Department of Labor. Further distribution and photocopying is permitted for the purposes of the Advisory Council's examination of the role that cybersecurity insurance plays in addressing cybersecurity risks for employee benefit plans.



Role of Brokers and Underwriters

- What is an insurance broker?
- What is an insurance company underwriter?
- How do brokers and underwriters work together?
- Why each role is important?
- How do underwriters evaluate cyber risk, including policy costs, retentions, coverage breadth?

Cyber Key Controls

Marketplace Minimum Expectations

Token Based Multi-factor Authentication (MFA)

Vulnerability Scanning & Patch Management

Endpoint Protection & Response (EDR)

E-mail Filtering & Security (DMARC/DKIM)

Social Engineering Exercises & Awareness Training

Identity, Access, and Privileged Access Management

Network Segmentation: Secure RDP, VPN, OT/IT

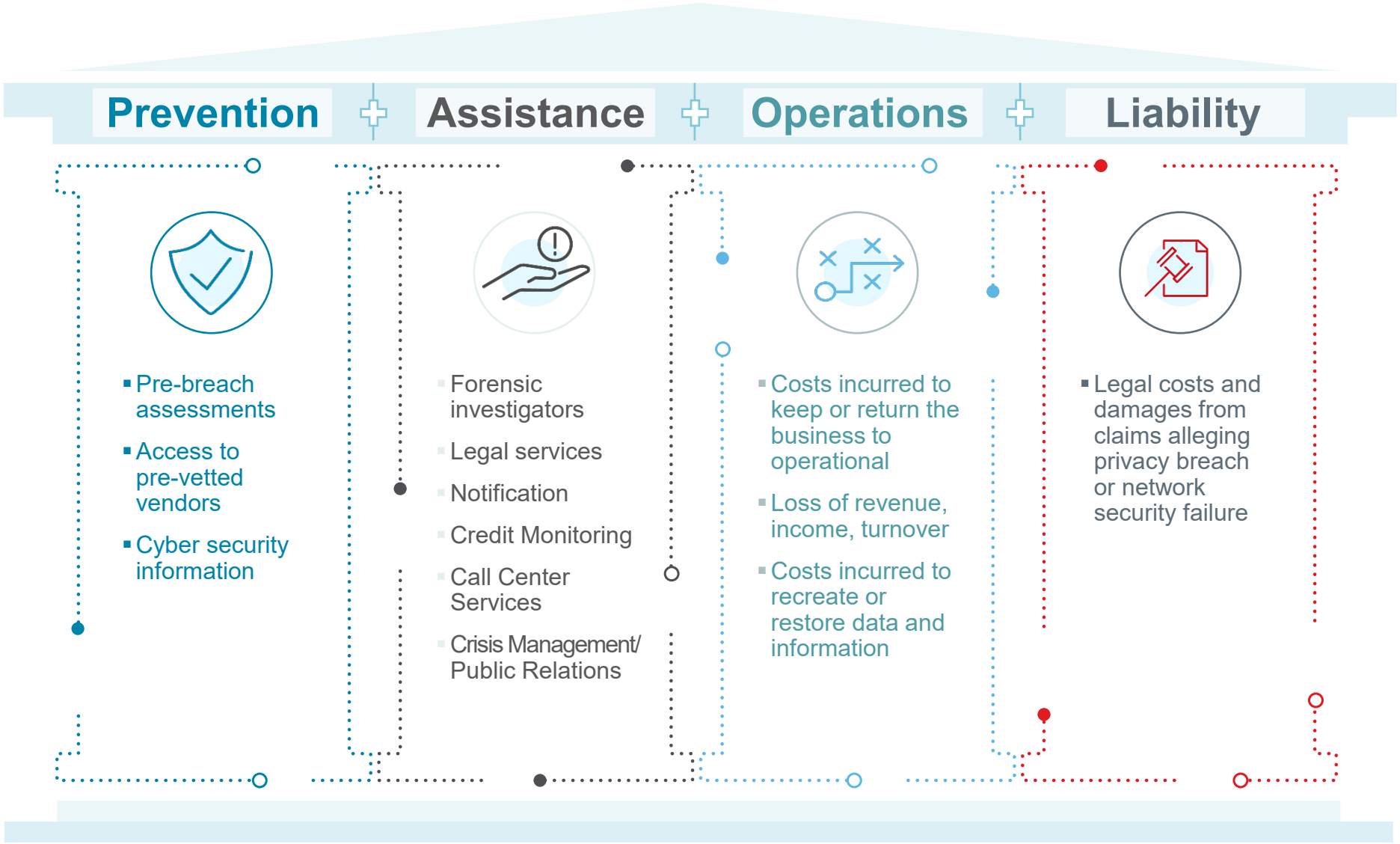
Disaster Recovery Testing, BCP, & Backups

Incident Response Plan (Written & Tested)

Key Underwriting Concerns & Best Practices

Critical Controls aligned with Cyber Insurance:	Key Guidance:
MFA / Controlled Access	**MFA should be required for all privileged and administrative accounts, remote/VPN/Remote Desktop/cloud access, access to backups.**
Endpoint Detection and Response	Effective EDR tools should be installed across all assets and on 7x24x365 basis and monitored by reputable vendors/MSSPs : i.e. Crowdstrike, Carbon Black.
Secured and Tested Backups	Backups of critical systems should be in place and tested regularly. Recovery from backup should be tested often and at least annually. Copy of backup should be stored off network or in immutable storage. Full Physical Recovery should be tested as well to ensure Recovery Time Objectives are achievable.
Patched Systems & Applications	A formalized process and policy for patching all endpoints, servers, systems with the ability to document process compliance and patching levels – especially important for critical patches.
Filtered Emails and Web Content	Spam filtering should be deployed on all email systems (MS-Advanced Threat Detection). Secure web access gateways for web filtering need to implemented.
Protected Privileged Accounts	A Password Asset Management (PAM) solution should be in place in order to manage privileged account passwords and MSLAPs or PAM is used on all endpoints to manage local admin passwords, local admin rights removed.
Logged and Monitored Network	Logging of the entire network, server, cloud and endpoint should be in place with logs managed daily. SOC for monitoring of all log files should be implemented as well.
Encrypted Storage	PCs, server storage and cloud storage are encrypted.
Phishing Aware Workforce	Annual phishing training and phishing simulation campaigns conducted. Reputable companies such as Knowbe4 or Wombat.
Managed Vulnerability and Penetration Testing	At minimum, annual penetration tests and vulnerability scans conducted across the entire network with follow up to close identified issues.
Prepared Incident Response	Formalized IR plan created with identified key internal stakeholders and vendors. Should be coordinated with Cyber Insurance Program.
Other Critical Controls	CISO on staff or on demand, minimize Service Accounts with Domain Privileges.
Business Continuity and Controls of Vendors	Must have in place a reviewed and tested Continuity Plan that includes supply chain vendors and contingencies in place for replacement.
Log4j / Log4Shell	All insurers are releasing their own set of questions to determine exposure and response around this widespread event.

Key Pillars of a Cyber Insurance Policy



Cyber Policies Typically Exclude the Theft of Funds

Example from Zurich Cyber Insurance Policy U-SPR-300-A CW (09/18)

“This Policy does not apply to **Loss**, **Defense Costs**, or **First Party Costs** on account of any **Claim** or **Event**:

based upon, arising out of, or attributable to loss, transfer or theft of monies, securities, or tangible property of others in the care, custody, or control of the **Insured**;”

Cyber Policies Typically Include an ERISA Exclusion With a Carve-back for Breach Costs and Liability Coverage

Example from Zurich Cyber Insurance Policy U-SPR-300-A CW (09/18)

"This Policy does not apply to **Loss**, **Defense Costs**, or **First Party Costs** on account of any **Claim** or **Event**…based upon, arising out of, or attributable to any actual or alleged:

1. violation by an **Insured** of the *Employee Retirement Income Security Act of 1974* (U.S.) (ERISA), the Canadian *Pension Benefits Standards Act*, the Ontario *Pension Benefits Act, 1990*, or any other similar federal, state, provincial, territorial or municipal act…

provided, however, this exclusion shall not apply to:

a. a **Regulatory Proceeding** or a **GDPR Proceeding** that may constitute a violation of Section 5(a) of the *Federal Trade Commission Act (15 U.S.C. 45(a))* (U.S.), as amended, including a **Consumer Redress Fund** established in resolving such a **Regulatory Proceeding** or **GDPR Proceeding**; or

b. an otherwise covered:

(1) **Claim** under Subsection I.A. [Liability Coverages]; or
(2) **Breach Cost** under Subsection I.B.1 [Breach Cost Coverage].

About

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

www.aon.com

AON