NATIONAL COORDINATING COMMITTEE FOR MULTIEMPLOYER PLANS

815 16TH STREET, N.W., WASHINGTON, D.C. 20006 • PHONE 202-737-5315 • FAX 202-737-1308

MARIAH M. BECKER
DIRECTOR OF RESEARCH AND EDUCATION
E-MAIL: MBECKER@NCCMP.ORG

September 7, 2022

ERISA Advisory Council
U.S. Department of Labor

Re: Cybersecurity Issues Affecting Health Benefit Plans
Cybersecurity Insurance and Employee Benefit Plans

Dear Members of the ERISA Advisory Council:

The National Coordinating Committee for Multiemployer Plans ("NCCMP") appreciates the opportunity to appear before the ERISA Advisory Council on these important topics affecting multiemployer pension and health and welfare plans. We are pleased to provide written statement on behalf of our members. I am the Director of Research and Education for the NCCMP. I am also an Enrolled Actuary, and a member of the American Academy of Actuaries Multiemployer Plans Committee.

The NCCMP is the only national organization devoted exclusively to protecting the interests of multiemployer pension and health and welfare plans, their sponsoring labor and employer organizations, as well as the more than 20 million active and retired American workers and their families who rely on these plans for their retirement and health care. The NCCMP's purpose is to assure an environment in which multiemployer plans can continue their vital role in providing retirement, health, training, and other benefits to America's workers and their families.

The NCCMP is a non-partisan, nonprofit, tax-exempt social welfare organization established under Internal Revenue Code ("IRC") Section 501(c)(4), with members, plans and contributing employers in every major segment of the multiemployer universe. These sectors include the airline, agriculture, building and construction, bakery and confectionery, entertainment, health care, hospitality, longshore, manufacturing, mining, office employee, retail food, service, steel, and trucking/transportation sectors. Multiemployer plans are jointly trusteed by employer and employee representatives.

Multiemployer pension and health plans are essentially pools of workers' earnings held in trust under federal law for the exclusive purpose of providing benefits to plan participants and beneficiaries. The trust funds are funded entirely by collectively bargained employer contributions for which covered workers explicitly trade off wages through the bargaining process. In a very direct sense, workers pay for their retirement benefits and health coverage. If a trust fund's costs increase, despite the trustees' best efforts at cost containment, the burden falls directly on the workers, as trustees may be faced with the need to reduce benefits or adjust eligibility rules to address new costs.

NCCMP works closely with a number of professionals to evaluate and advise on policy proposals affecting multiemployer pension and health plans. We are pleased to provide the attached testimony of Kathy Bakich, a Senior Vice President and Health Compliance Practice Leader with Segal in response to your Issue Statement on Cybersecurity Issues Affecting Health Benefit Plans and from Diane McNally, a Senior Vice President, Senior Consultant and Principal and Insurance Practice Leader with Segal in response to your Issue Statement on Cybersecurity Insurance and Employee Benefit Plans.

We are pleased to present to the Advisory Counsel on these important topics on September 9, 2022, and look forward to answering any questions that may arise from our statements or our presentation.

Best regards,

Mariah M. Becker

Mariah Becker
Director of Research and Education
NCCMP

Kathryn Bakich
Senior Vice President
T 202.833.6494
M 917.531.5109
kbakich@segalco.com

1800 M Street NW
Suite 900 S
Washington, DC 20036
segalco.com

Memorandum

To: ERISA Advisory Council

From: Kathryn Bakich

Date: September 6, 2022

Re: Cybersecurity Issues Affecting Health Plans

Thank you for the opportunity to appear before the ERISA Advisory Council on this important topic. I am happy to provide this written statement concerning cybersecurity issues affecting health plans and other employee benefit plans. My testimony is presented as a representative of the National Coordinating Committee for Multiemployer Plans. I am a member of the NCCMP Working Committee and regularly work with them on issues related to health plans.

About the NCCMP

The NCCMP is the only national organization devoted exclusively to protecting the interests of multiemployer plans, as well as the unions and the job-creating employers of America that sponsor them, and the more than 20 million active and retired American workers and their families who rely on multiemployer retirement and welfare plans. The NCCMP's purpose is to assure an environment in which multiemployer plans can continue their vital role in providing retirement, health, training, and other benefits to America's working men and women.

The NCCMP is a non-partisan, nonprofit, tax-exempt social welfare organization established under Internal Revenue Code Section 501(c)(4), with members, plans and contributing employers in every major segment of the multiemployer universe. These include airline, agriculture, building and construction, bakery and confectionery, entertainment, health care, hospitality, longshore, manufacturing, mining, office employee, retail food, service, steel, and trucking/transportation. Multiemployer plans are jointly trusteed by labor and management trustees.

Statement

I have provided privacy and security consulting to group health plans and other employee benefit programs since joining Segal in 1998. With the passage of HIPAA and implementation of the HIPAA privacy and security regulations, I led the Segal team assisting clients to implement the new rules. I am the author of the Employer's Guide to HIPAA Privacy, and a frequent speaker on privacy and security issues.

My team at Segal and I have worked with hundreds of multiemployer health plans to assist them with HIPAA and HITECH compliance. These plans include all types of multiemployer plans, and range from small fully insured arrangements to large self-insured and self-administered plans.

The rules were designed to be scalable to the size and needs of the organization, so each plan has similar but diverse compliance needs.

Multiemployer plans have taken significant steps to address the privacy and security rules, and issues that are presented within the plan's structure. These include but are not limited to:

- Conduct HIPAA Security Risk Assessments periodically (every 2-3 years) and whenever new technology is introduced (e.g., a new benefits system, new mobile devices, or a cloud conversion);
- Require Business Associate Agreements for all entities that use or disclose plan Protected Health Information;
- Maintain a Notice of Privacy Practices;
- Establish and maintain privacy and security policies and procedures;
- Maintain plan documents that are amended in accordance with the privacy rule;
- Utilize secure transmissions for PHI and ePHI between service providers;
- Redact identifiable information from all appeals heard by the Board of Trustees; and
- Train staff and fiduciaries on the HIPAA and HITECH rules and threats to PHI and ePHI.

I have provided a PowerPoint presentation that reviews the regulatory and enforcement structure of the HIPAA privacy and security regulations and the HITECH Act.

HIPAA and HITECH provide a robust statutory and regulatory framework for protection of both Protected Health Information (PHI) and Electronic PHI (e-PHI) used, maintained, and disclosed by multiemployer health plans and their partners (known as "Business Associates.") Congress has recognized this regulatory structure and enhanced it in 2021, when it passed legislation encouraging plans to utilize standards and practices established by the National Institute of Standards and Technology (NIST). HIPAA's privacy and security rules and HITECH's breach rules set forth a mature and complete set of guidelines for protection and enforcement of how ERISA group health plans use and disclose PHI and e-PHI.

HITECH also makes business associates (such as third-party administrators and pharmacy benefit managers) directly liable for compliance with the Security Rule's administrative, physical, and technical safeguards, and documentation requirements.

HIPAA and HITECH are enforced by the Centers for Medicare & Medicaid Services (CMS), which regularly monitors breach reports and complaints. CMS's Office for Civil Rights has a detailed enforcement process, and it frequently publishes enforcement data including case examples and resolution agreements.[1] Guidance is frequently issued on special topics such as cloud storage, ransomware, and the use of remote devices. Thus, based on current regulatory guidance (in particular, HIPAA) there is already sufficient protection and oversight of ERISA group health plans. There exists sufficient guidance on what group health plans need to do to protect the valuable data and information with which they are entrusted.

[1] https://www.hhs.gov/hipaa/for-professionals/index.html

The sub-regulatory guidance published by the Department of Labor (DOL) in 2021[2] is almost identical to existing HIPAA and HITECH guidance, so its principles were already being used by group health plans to enhance their cybersecurity stance. More so, significant internal risk mitigation concerns coupled with external commercial pressures have also resulted in most group health plan sponsors reviewing and enhancing their cyber risk management practices (via NIST, ISO or other cybersecurity risk frameworks).

Conclusion

I am available to answer any questions the Advisory Council has and happy to supplement this statement with any issues that arise at the hearings on September 8-9, 2022.

cc: Mariah Becker, NCCMP

[2] https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414

Diane McNally
Senior Vice President
T 212.251.5146
M 929.240.1433
drmcnally@segalco.com

333 West 34th Street
New York, NY 10001-2402
segalco.com
CA License No. 0I06323

Memorandum

To: 2022 Advisory Council on Employee Welfare and Pension Benefit Plans

From: Diane McNally

Date: September 6, 2022

Re: Cybersecurity Insurance and Employee Benefit Plans

I have been asked to address the topic of "Cybersecurity Insurance and Employee Benefit Plans" as a representative of the National Coordinating Committee for Multiemployer Plans (NCCMP). Specifically, I will provide an overview of cyber liability insurance and provide an understanding of the cybersecurity market for employee benefit plans.

I am a Segal Senior Vice President and the National Practice Leader of Segal Select Insurance Services, Inc. Segal Select is a wholly owned subsidiary of The Segal Group and operates as a national retail insurance brokerage firm. Segal Select specializes in financial and commercial insurance products including cyber liability insurance.

Segal is an over 80-year-old full-service employee benefit and human resources consulting firm. Our clients include multiemployer funds, corporations, higher education institutions, health systems, nonprofits and public sector entities, among many others.

My goal is to respond to questions by the Council regarding the types of insurers writing cybersecurity insurance, underwriting standards and requirements for placing the insurance policy, including who an insured is, typical policy terms and cost of insurance.

Introduction

In the 1990s, the first early forms of cyber insurance emerged as third-party policies were designed to protect against media and data processing errors, subject to certain covered perils. In today's environment, with rising data events and increasing threat actors, cyber attacks are more frequent, costly to address and can have increased long-term exposures for businesses.

Leading carriers today are managing their risk appetite, addressing profitability results and increasing their focus on clients with strong cyber hygiene. It remains a challenging market environment with high demand for cyber insurance and a cautious approach to the underwriting of the business.

Underwriting standards

In today's cyber insurance environment, insurers are leading the charge with cyber hygiene requirements to offer cyber insurance and/or maintain existing insurance programs. With data breach events rising since before COVID (2022 Verizon Data Breach Investigation report https://www.verizon.com/business/resources/reports/dbir/) and increasing breaches involving "Human Element, including Social Attacks, Errors and Misuse," insurers are responding with additional underwriting questionnaires, client meetings and utilizing third-party vendor assessments as tools to determine their underwriting appetite. Third party assessments can provide useful information for insurers and insureds in evaluating exposure to external threats and often come with remediation suggestions and insights to findings that could affect a client's risk score.

As supplemental applications become outdated, new underwriting questions are often required and focused on responses from insureds or first-time buyers. Here are a handful of more recent focus areas by cyber underwriters.

- **Multifactor authentication** – Confirming what dual entry controls exist for access to networks, systems, web-based emails and administrator accounts
- **Data backup procedures and encryption** – Where and how backups are stored, encrypted if MFA is required and how tested for malware
- **Patching procedures and vulnerability scanning and maintenance programs** – To better understand the cadence of vulnerability scans, evaluating computer systems and addressing critical patch work timeframes
- **Email security and security training** – Confirming what type of email scanning is needed to prevent malware attacks and how often insureds are conducting simulated phishing tests with employees or staff is requested
- **Privileged accounts and credentialing processes** – Focusing on gaining an understanding of protecting the most vulnerable information and estimates on number of records; PCI (Payment Card Industry) transactions provides a sense of the scope and exposure to an insured's system.

  Endpoint Detection and Response (EDR) - EDR solutions combine real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. Simply stated, if a single workstation or server should become infected by a successful ransomware attack, the EDR solution would be able to automatically quarantine the infected system from the rest of the network, limiting the possibility of the ransomware to spread to other systems.

Who are Name Insureds? How should cyber liability policies be structured?

For multiemployer plans, a cyber liability policy may be written in the name of the Plan or include related plans and entities. It largely depends on the Board of Trustees' appetite to have the cyber policy share limits, and the premiums for separate policies can be costly. In addition, underwriters may weigh in depending on a policyholder's systems structure for potential systemic risks along with overall security controls and loss history.

In our experience, most multiemployer clients prefer cyber insurance policies as standalone policies, not combined with other insurance policies. There are limited insurance products that combine cyber type coverages that would provide the full breath of coverage, which a monoline cyber lability policy can provide an insured. In addition, policy limits could potentially be diluted with a cyber claim when packaging coverage with other lines of business. There are several ways to address package policies, but it does vary by carrier appetite, and policies need to be carefully vetted.

What is cyber insurance?

The policy is designed to protect policyholders in time of a data event for first- and third-party coverage including costs related to a covered event. Most policies come with customized, vetted breach response firms, some at no cost, to assist policyholders in navigating a data event. Engaging these providers prior to an event can help strengthen and improve an Insured's response planning and risk management in time of an attack.

Here one can visualize the basics of a Cyber Insurance policy; however, these policies are not uniform and can vary widely by carrier including limit structures and retentions.

Cyber Liability Insurance provides:

What are limits of liability and deductibles?

Carriers may provide cyber liability programs with various limit and retention structures as a method to respond to changes in cyber risk. However, in an advancing cyber threat environment, some policyholders may face limitations in coverage and lower limits for specific type of loss costs and, in some cases, experience Coinsurance, a term found in other insurance policies designed to require policyholders to share in the claim based on a specific percentage attached to a type of loss, such as seen with ransomware events.

Circumstances for loss of coverage

Market conditions continue to dictate changes to policy terms, conditions, premiums and especially to coverage limitations. Several carriers have tied changing policy terms to growing ransomware and social engineering events. Lowering limits, eliminating the coverages and addressing larger timeframes for policies to respond to business interruption costs make policies difficult to navigate.

Traditional policies such as fidelity and commercial crime bonds typically exclude losses of data that theoretically could be covered under a cyber policy. Many insurance carriers provide carve backs to these bond exclusions to cover losses where the data itself can be a covered loss with carriers already offering narrow coverage for these types of losses.

Since ERISA requires the purchase of a fidelity bond, plan assets have traditionally been used to pay for such policies. While cyber policies are not required to be purchased, the breach response services they provide – forensics, privacy counsel, data restoration, notification services, etc. – would, without a policy in place, presumably be incurred and paid for by the plan, so the purchase of a cyber policy using plan assets would appear to mitigate such expenses to the plan. These type of coverages and services are not traditionally provided under other insurance policies and are often provided with narrow coverages.

Disclaimer

Segal Select Insurance Services, Inc. (“Segal”), a subsidiary of The Segal Group, Inc., 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.

In Closing

Thank you for the opportunity to participate in this process.

cc: Mariah Becker, NCCMP