Marsh & McLennan Companies, Inc.
1166 Avenue of the Americas
New York, NY 10036
212 345 5000

Statement of
Timothy L. Marlin

Senior Vice President
Marsh, LLC

Before the Advisory Council on Employee Welfare and Pension Benefit Plans

September 9, 2022
Washington, DC

Introduction:

Good morning Chairman Butash, Vice Chairwoman Palmer, and Members of the Council, my name is Timothy Marlin and I am the Cyber Product Development Leader for Marsh's North American Cyber Practice and an advisor in the field of cyber risk management. My testimony today will focus on the current marketplace for cyber insurance; how cyber insurance is supporting improved resiliency to defend against cyber threats, including those faced by benefit plans; and specific considerations for benefit plans to consider in connection with cyber insurance. Thank you for the opportunity to share our perspective on this important topic.

Marsh McLennan is the world's leading insurance broker and risk advisor. Through four market leading brands — Marsh, Guy Carpenter, Mercer, and Oliver Wyman — and more than 83,000, employees serving clients in more than 130 countries, we help corporate and public sector clients navigate an increasingly dynamic environment for cyber and other risks. We have a deep understanding of cyber risk and insurance issues, having been engaged with cyber insurance since its inception some 25 years ago. Marsh's role is to work with clients to analyze their risk exposures and, where appropriate, help our clients implement solutions to address and mitigate the financial impact of a cyber incident.

My own background includes 22 years in the insurance industry working in legal, claims, underwriting, product, and insurance brokerage capacities.

Cyber Insurance Market Snapshot

In the Council's final issue statement, one of the identified goals was to gain an understanding of cyber insurers and the current marketplace for cyber insurance. I understand that the Council has already reviewed *The Betterley Report: Cyber/Privacy Insurance Market Survey—2022*, which served as the basis for Mr. Rick Betterley's testimony on July 19. Mr. Betterley's thorough report relies on carrier-provided information, which often has a lag time due to the report's significant collection process and many sources. Rather than restate the information in that report, I will focus on current conditions in the cyber insurance market. For further detail, we have attached to my written testimony a copy of Marsh's recent report, "Signs, Signals, and Significance of a Healthy Cyber Insurance Market."

As noted in prior testimony before this Council, cyber insurance is in the midst of a difficult market marked by rising premium costs, higher self-insured retentions, and some restrictions on capacity and coverage. However, we would note that the sharp rise in cyber insurance pricing of the past two years is giving way to cautious optimism that rate increases soon will stabilize and insurers will reward strong cyber hygiene controls. As underwriters gain more confidence in pricing cyber coverage, competition and interest from new market entrants should increase, raising the likelihood of rate moderation.

For example, for clients with strong cybersecurity controls that experienced a significant increase in their most recent renewal, the rate increases typically have not been as dramatic. In the second quarter of 2022, the average year-over-year increase was about 60%, compared to a high of 133% in December 2021. Still, it is worth noting that even loss-free clients continue to see increases.

Companies that have not made the cybersecurity improvements deemed necessary by underwriters will face challenges in securing coverage. Should they secure coverage, it is likely to be subject to more

restrictive terms and conditions, including co-insurance, restricted ransomware and contingent business interruption coverages, and sub-limited or excluded coverage.

As part of the effort to efficiently manage the total cost of cyber risk, clients increasingly need to make difficult choices regarding limit and retention (deductible) levels. Some organizations are increasing limits, typically driven by the magnitude of their risk or increased awareness by key stakeholders. More, however, are decreasing limits, driven by budget constraints, unfavorable cybersecurity controls that are affecting market capacity, and, for some, a lack of market capacity.

Clients are also using their retention levels as a lever to help offset increasing program costs. The self-insured retention functions like a deductible and represents the amount of loss that the insured will be responsible for paying. A significant percentage of clients continued to increase their retentions in the first quarter of this year, a reflection of the persistently challenging market. While some clients are increasing retentions due to limited coverage availability, others are choosing to do so to manage their premium cost.

There is not one thing that is currently driving the firmness of the current cyber market; rather, there is a confluence of considerations, including:

- Aggregation exposure.
- Potential for systemic losses from common vulnerabilities and common dependencies, such as cloud vendors and software.
- Digital supply chain issues, highlighted by incidents such as SolarWinds, Accellon, Microsoft Exchange, Kaseya, and Log4j.
- Geopolitical tensions.
- Evolving privacy regulations.
- Ransomware.

However, there is cause for optimism. After two years of pricing increases, it appears that rates are starting to moderate. Attritional losses seem to be more under control, with the cyber market's premium growth now exceeding incurred losses. As companies continue to improve their cybersecurity controls, insurers can be expected to calibrate their underwriting and pricing strategies on an account-by-account basis — rather than on a portfolio-basis — and reward policyholders who can demonstrate strong cyber hygiene.

Cyber Insurance and Risk Management for Benefit Plans

As detailed in the Council's issue statement, this hearing intends to explore the insurance coverages that exist to manage the cyber risks faced by employer sponsored benefit plans. The Council has previously been provided with thorough overviews of cyber insurance and the nature of coverage grants, as well as other lines of coverage that could respond to a cyber event.

Large, sophisticated clients, especially those that manage their own plans, are increasingly seeking policy endorsements to add the plan or plans to their cyber insurance program. In these cases, regarding the

coverage afforded to the plan, certain exclusions may need to be amended, such as if the policy contains an exclusion related to violations of ERISA.

Cyber insurers generally have been willing to consider this exposure in connection with larger organizations, which are often taking on a significant self-insured retention/deductible. Smaller, more price sensitive buyers often favor less bespoke, more economical cyber insurance policies that offer less modification. Often, these companies outsource plan administration and rely on their fiduciary insurance and the cyber, professional liability, and other coverages that could potentially respond to a cyber event that impacts the provider.

However, we are seeing an increasing number of clients of all sizes consider standalone cyber insurance for their benefit plans in order to guarantee that coverage is tailored to the plan's needs and to provide separate limits for the fund in the event of a claim.

Generally, benefit plans face many of the same cyber risks as do other entities that provide financial services. The primary risks from a cyber incident affecting a benefit plan include:

- The loss or theft of participant data.
- Cyber extortion.
- Monetary loss/theft of participant assets.
- Third-party and regulatory claims.
- Network and data recovery costs related to malware or hacking.
- Plan system outage due to malware of a common system/computer program.

These exposures can typically be addressed by a robust mix of cyber, fiduciary, fidelity, and third-party crime coverages.

I understand that the focus of these discussions is not to explore the insurance coverage that various service providers, such as asset custodians or record keepers, might have as part of their business with respect to employee plans. However, it is essential that plan sponsors make sure that their service providers have strong cybersecurity practices and a robust insurance program to address losses that could adversely affect the plan and its participants.

The EBSA acknowledged this in their 2021 guidance by including as a best practice to have an insurance requirement for errors and omissions, cyber liability and privacy, and fidelity/crime insurance when contracting with a service provider. I would note that cyber insurance underwriters, when considering pricing and terms for insuring the plan, look favorably upon the existence of third party providers with a strong cyber and professional liability/E&O insurance program in addition to appropriate indemnification requirements that could assume all or some of the costs associated with a cyber/privacy incident.

The Value of Cyber Insurance

The Council advised that it intends to explore the interplay between a plan's existing "cyber hygiene" and the availability and cost of cyber insurance. As noted previously, the cyber insurance market remains challenging in terms of pricing, terms, and conditions. However, the challenges also present an opportunity in that cyber insurance can incentivize good cybersecurity practices via an efficient market that provides materially differentiated terms, conditions, and pricing based on an insured's cybersecurity posture.

The insurance industry has a history of incentivizing and driving the adoption of best practices. One oft-cited example is the requirement from fire insurers that properties have sprinklers and fire suppression systems. This requirement resulted from reviews of fire loss data.

Similarly, cyber insurance can incentivize good cybersecurity practices based on an insured's cybersecurity posture. Similar to the effect of data regarding sprinklers and other measures, cyber insurers can more confidently provide differentiated terms, conditions, and pricing when they have actionable cyber loss data.

Over the past several years, cyberattacks and related cyber insurance claims have increased in frequency. This has allowed cyber insurers to gather more robust data regarding the causes of cyber insurance claims and analyze their relationship to relevant mitigating security controls. Analysis of this data has resulted in a better understanding of the technical steps that organizations can take to build their cyber resiliency. As a result, cyber insurers have adopted certain controls that have become a minimum requirement for insurability.

Working with insurers, Marsh promoted to our clients "12 key controls" that are most necessary for successful cyber insurance renewals. This supports the implementation of effective security, which in turn results in better insurance terms, conditions, and pricing. These controls have been established as best practices for several years, yet some companies still struggle to adopt them — typically due to an inability to justify the cost of implementation, failure to deploy them comprehensively, or a lack of understanding of the need for controls. Still, in response to changing market conditions, many of our clients are now adopting these controls and driving better cyber resiliency.

Of the 12 key controls, insurers have tended to focus on five they indicate as having the greatest positive impact on reducing cyber risk:

1. **Multifactor authentication (MFA):** Requiring at least two pieces of evidence to validate a user's identity helps prevent unauthorized entry into an organization. This control is a top weapon in the arsenal to thwart ransomware attacks, especially in relation to remote access and the management of administrative accounts.

2. **Endpoint detection and response (EDR):** The continuous monitoring and analysis of endpoints can help deflect attacks. In the event of an attack, it can also enable a more efficient response.

3. **Secured, encrypted, and tested backups:** The proliferation of ransomware attacks has placed additional emphasis on a sound organizational backup strategy and implementation. Restoring from backups is one of the ways organizations attempt to recover data, recover from an attack, and avoid dealing with the difficult decision of paying a ransom demand.

4**. Privileged access management (PAM):** This is designed to ensure that employees have only the necessary level of access — and no more — to perform their jobs. This control also helps security teams identify abuse of privilege.

5**. Email filtering and web security:** Email filtering identifies and blocks malicious emails and attachments, whereas web filtering blocks inappropriate sites. These tools primarily are used to help block the spread of malware.

Conclusion

Despite rising premiums and some increased limitations in available coverage for insureds with limited security controls, cyber insurance remains a valuable coverage to respond to the costs associated with cyberattacks. In this way, cyber insurance plays an important role in a larger coordinated risk management strategy for benefit plans that includes both cybersecurity controls and services, as well as an integrated program of cyber, fiduciary, and fidelity/crime insurance. Additionally, given the cyber insurance market's unique insights into the drivers and costs of cyber incidents, their requirements for cyber insurability will serve as an important driver of enhanced cyber resilience.

Attached to my written testimony is a copy of the Marsh's recent "Signs, Signals, and Significance of a Healthy Cyber Insurance Market," which provides a more detailed review of current cyber insurance market conditions.

Thank you for allowing me to present this testimony. I am happy to take your questions.