Advisory Council on Employee Welfare and Pension Benefit Plans

Report to the Honorable Martin Walsh, United States Secretary of Labor

Cybersecurity Insurance and Employee Benefit Plans

December 2022

[Page intentionally left blank]

TABLE OF CONTENTS

NOTICE

This report was produced by the Advisory Council on Employee Welfare and Pension Benefit Plans, usually referred to as the ERISA Advisory Council (the "Council"). The Council was established under Section 512 of the Employee Retirement Income Security Act of 1974, as amended ("ERISA") to advise the Secretary of Labor (the "Secretary") on matters related to welfare and pension benefit plans. This report examines the topic of cybersecurity insurance and its relationship to employee benefit plans.

The contents of this report do not represent the position of the Secretary or of the Department of Labor (the "Department").

LIST OF COUNCIL MEMBERS

Peter J. Wiedenbeck, Council Chair

Megan Broderick, Council Vice Chair

Glenn E. Butash, Issue Chair

Alice Palmer, Issue Vice Chair

Beth Halberstadt, Drafting Team Member

John R. Harney, Drafting Team Member

Edward A. Schwartz, Drafting Team Member

Holly Verdeyen, Drafting Team Member

Dave Gray

James G. Haubrock

Marcelle J. Henry

Mercedes D. Ikard

Jeffrey Lewis

Tonya Manning

Shaun C. O'Brien

ABSTRACT OF REPORT

Concerns regarding cyber attacks, cyber theft and the need for strong cybersecurity measures continue to grow in prominence. In 2022, the Council examined the role that cybersecurity insurance plays in addressing cybersecurity risks for employee benefit plans.

The Council conducted research and heard from witnesses, including individuals from insurance companies, insurance brokers, insurance consultants, governmental organizations, and academics studying cybersecurity insurance as well as attorneys litigating cybersecurity insurance coverage issues. The Council also heard from representatives of the plan sponsor community--both multiemployer plans and single-employer plans--and plan service providers.

The Council concluded that the topic of cybersecurity insurance generally and as it relates to employee benefit plans is complex and nuanced. Accordingly, the Council recommends that the Department study this topic further. The Council also found that the issue of insurance coverage for losses relating to cyber incidents might not be well understood by benefit plan fiduciaries and, accordingly, the Council also recommends that the Department, following further study, develop education for plan fiduciaries regarding cyber and other insurance to protect against losses resulting from cyber incidents.

ACKNOWLEDGEMENTS

The Council recognizes the following individuals and organizations who provided testimony or information that assisted the Council in its deliberations and the preparation of its report. Notwithstanding their contributions, any errors in the report rest with the Council alone.

Daniel Aronowitz, Euclid Fiduciary

Kathryn Bakich, Segal

Mariah Becker, National Coordinating Committee for Multiemployer Plans

Richard S. Betterley, Betterley Risk Consultants Inc.

Jon M. Boyens, National Institute of Standards and Technology

Ted Burik, U.S. Government Accountability Office

Marisol Cruz-Cain, U.S. Government Accountability Office

Stefan Dandelles, Esq., Kaufman Dolowich & Voluck

Dan Garcia-Diaz, U.S. Government Accountability Office

Brian Gillin, Aon

Michael L. Hadley, Esq., Davis & Harman LLP (on behalf of the American Benefits Council)

Kara Higginbotham, Zurich North America

Matt Klein, Willis Towers Watson

David Levine, Esq., Groom Law Group, Chartered

Mark Littman, U.S. Government Accountability Office

Timothy Marlin, Marsh McLennan

Kent Mason, Esq., Davis & Harman LLP (on behalf of the American Benefits Council)

Diane McNally, Segal

Mark Miller, Esq. Miller Friel PLLC

Sasha Romanosky, RAND Corporation

Tim Rouse, SPARK Institute, Inc.

Christine Swift, Lincoln Financial Group

Ben Taylor, Callan Associates

Tab Turano, Esq., Miller Friel PLLC

Josephine Wolff, The Fletcher School at Tufts University

I. RECOMMENDATIONS

Recommendation 1

The Department should continue to study the issue of cybersecurity insurance and employee benefit plans. This study should not be limited to "cyber-insurance" *per se* but should include other forms of loss risk-mitigation strategies including but not limited to:

- Cybersecurity insurance
- Fidelity/crime coverage
- Fiduciary liability coverage
- Third-party (service-provider) contractual obligations (including indemnification) and insurance.

Recommendation 2

Following further study, the Department should consider developing education for employee benefit plan fiduciaries, and others, concerning the types of insurance coverages that are available to protect against losses resulting from cyber incidents. Areas of education might include:

- The primary types of cyber-threats faced by employee benefit plans
- The types of losses typically covered by "cyber-insurance" policies vs. other types of policies (such as fidelity/crime policies and fiduciary insurance policies)
- Other aspects of insurance policies--such as exclusions, the identity of the "named insured," deductibles, and coverage limits
- The role that a benefit plan's cybersecurity policies, practices, and controls might play in the application and/or renewal process for cyber-related insurance coverage.

II. BACKGROUND

A. PRIOR COUNCIL REPORTS

The ERISA Advisory Council (the "Council") has twice previously addressed privacy and security issues affecting employee benefit plans. In 2011, the Council examined "Privacy and Security Issues Affecting Employee Benefit Plans."[1] With regard to this topic (which expressly excluded examining health benefit plans), the Council noted "dramatic changes in technology" relating to administering employee benefit plans and examined issues arising from potential security breaches and the misuse of plan data. The Council also took on the question of whether plan fiduciaries had a duty under ERISA to reduce the risk of personal employee information being disclosed to unauthorized persons. As a result of its work, the Council recommended that the Department (1) provide guidance on the obligation of plan fiduciaries to secure and keep private the personal identifiable information of plan participants and beneficiaries; (2) develop educational materials and engage in outreach to plan sponsors, plan participants and beneficiaries on the issues of privacy and the security of such personal information; and (3) include in such outreach and materials information regarding elder abuse related to benefit plans.[2]

In 2016, the Council expanded on its 2011 work, examining "Cybersecurity Considerations for Benefit Plans."[3] In its report, the Council noted that there was no clear guidance or standards for plan sponsors or fiduciaries to follow regarding how to develop and implement an appropriate cybersecurity plan. In this regard, the Council noted that, although the Department had not at that time determined whether cybersecurity was indeed a responsibility of plan fiduciaries, it nonetheless recommended that such standards be established.

---

[1] Report available at: https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2011-privacy-and-security-issues-affecting-employee-benefit-plans.pdf (accessed Nov, 9, 2022).

[2] The topic of elder abuse was later studied (in part) by the Council in 2020. See "Considerations for Recognizing and Addressing Participants With Diminished Capacity," available at: https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2020-considerations-for-recognizing-and-addressing-participants-with-diminished-capacity.pdf (accessed Nov. 9, 2022).

[3] Report available at: https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf (accessed Nov. 9, 2022).

B. GAO REPORTS

The United States Government Accountability Office (GAO) has studied the issue of cybersecurity risks and employee benefit plans in three recent reports to Congress: (1) GAO-21-25, "Defined Contributions Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans" (February 2021)[4]; GAO-21-477, "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market" (May 2021)[5]; and (3) GAO-22-104256, "Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks" (June 2022)[6].

In Report 21-25, the GAO noted:

> In their role administering private sector employer-sponsored defined contribution (DC) retirement plans …, plan sponsors and their service providers--record keepers, third party administrators, custodians, and payroll providers--share a variety of personal identifiable information (PII) and plan asset data among them to assist with carrying out their respective functions …. The PII exchanged for DC plans typically include[s] participant name, Social Security number, date of birth, address, username/password; plan asset data typically includes numbers for both retirement and bank accounts. The sharing and storing of this information can lead to significant cybersecurity risks for plan sponsors and their service providers, as well as plan participants.

The GAO recommended that the Secretary of Labor formally state whether cybersecurity for private sector defined contribution plans is a plan fiduciary responsibility under ERISA. It also recommended that the Secretary develop and issue guidance that identifies minimum expectations for mitigating cybersecurity risks that outline the specific requirements that should be taken by all entities involved in DC plan administration.

In Report 21-477, the GAO, as required by the National Defense Authorization Act for FY2021, studied (without making any specific recommendations) the U.S. cyber

[4] Report available at: https://www.gao.gov/products/gao-21-25 (accessed Dec. 15, 2022).
[5] Report available at: https://www.gao.gov/products/gao-21-477 (accessed Dec. 15, 2022).
[6] Report available at: https://www.gao.gov/products/gao-22-104256 (accessed Dec. 15, 2022).

insurance market. Among the key trends in the current market for cyber insurance, the GAO found:

- *Increasing take-up*. Data from a global insurance broker indicate its clients' take-up rate (proportion of existing clients electing coverage) for cyber insurance rose from 26 percent in 2016 to 47 percent in 2020.
- *Price increases*. Industry sources said higher prices have coincided with increased demand and higher insurer costs from more frequent and severe cyberattacks. In a recent survey of insurance brokers, more than half of respondents' clients saw prices go up 10–30 percent in late 2020.
- *Lower coverage limits*. Industry representatives told GAO that the growing number of cyberattacks has led insurers to reduce coverage limits for some industry sectors, such as healthcare and education.
- *Cyber-specific policies*. Insurers increasingly have offered policies specific to cyber risk, rather than including that risk in packages with other coverage. This shift reflects a desire for more clarity on what is covered and for higher cyber-specific coverage limits.

The report noted that the cyber-insurance industry faces multiple challenges, with industry stakeholders proposing options to help address these challenges, such as:

- *Limited historical data on losses*. Without comprehensive, high-quality, data on cyber losses, it can be difficult to estimate potential losses from cyberattacks and to price policies accordingly. Some industry participants said federal and state governments and industry could collaborate to collect and share incident data to assess risk and develop cyber insurance products.
- *Cyber policies lack common definitions*. Industry stakeholders noted that differing definitions for policy terms, such as "cyberterrorism," can lead to a lack of clarity on what is covered. They suggested that federal and state governments and the insurance industry could work collaboratively to advance common definitions.

In Report 22-104256, the GAO reported that U.S. critical infrastructure (such as utilities, financial services[7], and pipelines) faces increasing cybersecurity risks. Understanding these risks and associated vulnerabilities, threats, and impacts is essential to protecting critical infrastructure. The effects of cyber incidents can spill over from the initial target to economically linked firms--magnifying damage to the economy. For example, the Report noted, in May 2021 the Colonial Pipeline Company learned that it was the victim of a cyberattack that led to short-lived gasoline shortages.

In this report, the GAO noted that cyber insurance and the Terrorism Risk Insurance Program (TRIP)--the government backstop for losses from terrorism--are both limited in their ability to cover potentially catastrophic losses from systemic cyberattacks. Cyber insurance can offset costs from some of the most common cyber risks, such as data breaches and ransomware. However, private insurers have been taking steps to limit their potential losses from systemic cyber events. For example, insurers are excluding coverage for losses from cyber warfare and infrastructure outages. TRIP covers losses from cyberattacks if they are considered terrorism, among other requirements. However, cyberattacks may not meet the program's criteria to be certified as terrorism, even if they resulted in catastrophic losses. For example, attacks must be violent or coercive in nature to be certified.

The report also described how the Department of the Treasury's Federal Insurance Office (FIO) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) both have taken steps to understand the financial implications of growing cybersecurity risks. The report notes, however, that those organizations have not assessed the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response. CISA is the primary risk advisor on critical infrastructure and FIO is the federal monitor of the insurance sector. Accordingly, the GAO views them as well positioned to jointly perform such an assessment. Doing so, and reporting the results to Congress, can inform deliberations on whether a federal insurance response is warranted, according to GAO.

[7] The financial services sector included retirement and pension plans.

In this report, the GAO made the following recommendations to the CISA and FIO:

- The Director of the Cybersecurity and Infrastructure Security Agency should work with the Director of the Federal Insurance Office to produce a joint assessment for Congress on the extent to which the risks to the nation's critical infrastructure from catastrophic cyberattacks, and the potential financial exposures resulting from these risks, warrant a federal insurance response.
- The Director of the Federal Insurance Office should work with the Director of the Cybersecurity and Infrastructure Security Agency to produce a joint assessment for Congress on the extent to which the risks to the nation's critical infrastructure from catastrophic cyberattacks, and the potential financial exposures resulting from these risks, warrant a federal insurance response.

C. EBSA GUIDANCE

In 2021, the Employee Benefits Security Administration (EBSA) published sub-regulatory guidance for plan sponsors, plan fiduciaries, service providers and plan participants regarding cybersecurity.[8] There were three discrete parts to the guidance: (i) tips for plan sponsors/fiduciaries for hiring service providers that have strong cybersecurity practices, (ii) a list of "best practices" for use by recordkeepers and other service providers, and (iii) a description of online security practices for use by plan participants.

The "tips" document for plan sponsors/fiduciaries set out six suggestions to follow in selecting and monitoring plan service providers.[9] These were: (1) to inquire about the provider's "information security standards, practices and policies" and to compare those standards, practices and policies to standards adopted by other financial institutions; (2) to ask providers how they validate their own practices and also to "look for contract provisions" that give the sponsor/fiduciary the right to review audit results that demonstrate compliance with the service providers' security standards; (3) to evaluate the service provider's "track record" with respect to

[8] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity (accessed Nov. 9, 2022).

[9] As noted, *infra*, at 8, this document was specifically addressed to sponsors/fiduciaries of section 401(k) plans and "other types of pension plans."

security incidents, including legal proceedings relating to the vendor's services; (4) to inquire about past security breaches; (5) to ask about cyber insurance, and consider whether it covers losses caused by "internal threats" (from the service provider's own employees or contractors) and losses caused by "external threats" such as hacking; and (6) to require, in any contract with the service provider, that the service provider comply with cybersecurity and information security standards and to apply particular scrutiny with respect to provisions that limit the service provider's responsibility with respect to cyber breaches. With respect to the last item, the tip sheet identified as important provisions addressing the use, sharing, and confidentiality of information; provisions regarding notification of the plan sponsor/fiduciary in the event of a cybersecurity breach (and regarding cooperating in an appropriate investigation of the incident); and provisions referencing compliance with applicable laws relating to records-retention, data privacy, and information security.

The foregoing tips were said to apply to "plan sponsors of all sizes" and were intended to "help business owners and fiduciaries [to] meet their responsibilities under ERISA to prudently select and monitor [plan] service providers."

The "best practices" guidance for plan recordkeepers ("and other service providers") encompassed 12 areas of focus and set forth detailed elements within each area. The areas were: (1) having a formal, and "well documented," cybersecurity program; (2) conducting annual risk assessments; (3) undergoing annual third-party audits; (4) assigning qualified personnel (including senior executives) to oversee and carry out the organization's cybersecurity program; (5) implementing access-control protocols; (6) conducting periodic security reviews and assessments with respect to data stored "in the cloud" or that are managed or maintained by other entities; (7) conducting annual (or more frequent) cybersecurity awareness training for all service-provider personnel; (8) implementing a "system development life cycle program" (which includes "penetration testing," "code review," and "architecture analysis" of the provider's systems); (9) having express business continuity, disaster recovery, and incident response programs; (10) insuring that sensitive data is encrypted--both "at rest" and when "in transit"; (11) implementing other technical controls, including hardware and software updates and routine patch management; and (12) taking appropriate action (list provided) in response to any cyber incident in order to protect the plan and its participants.

Finally, EBSA developed "Online Security Tips" for participants that included such things as: monitoring account activity; using strong and unique passwords (and not sharing passwords); keeping contact information up-to-date; closing or deleting unused accounts; avoiding using "free" wi-fi (public networks such as at airports, hotels, or coffee shops); being vigilant against possible "phishing" attacks; using anti-virus software; and promptly reporting identity theft or cyber incidents.

Although the service-provider "best practices" document and the participant "security tips" document included no express reference to the types of employee benefit plans to which it applied (and, indeed, the participant document clearly has application to areas other than employee benefits), the "tips" document for plan sponsors/fiduciaries expressly identified the audience as sponsors/fiduciaries of "401(k) and other types of pension plans," suggesting a limited reach. Indeed, in its press release announcing the 2021 guidance, the Department underscored this focus, referring expressly to the risks faced by the estimated 34 million defined benefit pension plan participants and 106 million defined contribution plan participants in the United States and the estimated (private) plan assets of $9.3 trillion.[10] Several witnesses testifying before the Council stated that these references (in the "tips" sheet and the press release) to retirement plans have led to some confusion in the regulated community as to whether (or to what extent) this guidance applies with respect to plans other than pension/retirement plans, including, for example, health benefits plans.

III. WITNESS TESTIMONY

A. GOVERNMENTAL ORGANIZATIONS

1. Government Accountability Office

Dan Garcia-Diaz, Nate Gottfried, Ted Burik, and Marisol Cruz Cain appeared on behalf of the U.S. Government Accountability Office (GAO). According to this panel of witnesses, trends in cybersecurity are moving in a dramatic way--the FBI has reported that the number of

[10] See "News Release: US DEPARTMENT OF LABOR ANNOUNCES NEW CYBERSECURITY GUIDANCE FOR PLAN SPONSORS, PLAN FIDUCIARIES, RECORD-KEEPERS, PLAN PARTICIPANTS; Guidance seeks to help protect in estimated $9.3T in assets (April 4, 2021), available at: https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414 (accessed Nov. 9, 2022).

cyber incidents are growing and ransomware demands increasing dramatically. However, there is no readily available market data on the frequency of cyber attacks on qualified retirement plans. In this regard, the witnesses noted that:

- Federal agencies are required to report cyber attacks
- Some private sectors have requirements to report cyber attacks, but this is not universal
- Many private entities are not as willing to report such attacks.

Almost every aspect of cyber insurance is growing:

- The number of policies from 2016 – 2019 increased 60%
- Retentions [the amount for which the policyholder remains responsible] increased about 50%
- The number of insurers offering insurance increased by 26%
- There are increasing demands for insurance in a concentrated market (10 insurance companies represent nearly 70% of cyber insurance premiums)
- Premiums increased 9% to 34% in the past year.

Cyber policies generally cover costs for notifications, remediation, and business interruption. However, as written today, cyber insurance policies might not cover the theft of assets.

The GAO believes that cybersecurity insurance is critical for tax-qualified retirement (defined contribution) plans, a belief that has only grown with time. The following specific concerns were cited:

- Typically, cyber policies are enterprise-wide, do not acknowledge the defined contribution plans specifically (nor the personal identifiable information held by these plans)
- There is no federal insurance coverage for plans; plans are usually covered by private insurance

- There is a belief that an attack on the financial sector could directly trigger losses in the retirement plan sector, suggesting a need for a federal backstop.

The general belief of the GAO is that losses associated with cyber incidents are an insurable risk, but there are still a lot of unanswered questions about the minimum coverages that are needed by fiduciaries.

However, the GAO does not think it is enough simply to issue "best practices" documents and, therefore, recommends that the Department identify minimum required standards. According to the GAO, these standards should include:

- A requirement to use dual-authentication and encryption. In this regard, however, the GAO stated that it recognizes that technology is evolving, so standards would need to be broad (for example, the Department should not require a specific type of encryption, as that technology is still evolving)
- A requirement to comply with minimum requirements on data transfer to decrease risks around information exchanges (data exchanges are typically daily transmissions)
- A requirement to leverage the assessment questionnaires being issued by the fiduciary insurers. Here, the expectation is that this would result in lower premiums and retentions by the insurers as employers get smarter about the risks for retirement plans.

The GAO believes the insurance companies have a role to play. In this regard, the GAO noted that insurers should:

- As part of the policy underwriting process, identify the risks and who is the responsible party for mitigating those risks and how are they covered
- Seek to standardize cybersecurity insurance policies, so cyber attacks are described/categorized more consistently from policy to policy
- Examine the policy limit in comparison to the intended scope of coverage and notify insureds of potentially inadequate insurance coverage issues.

2. National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce and is responsible for developing standards for federal departments and agencies. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. On the issue of cybersecurity insurance, NIST provided the testimony of Jon M. Boyens, Deputy Chief of the Computer Security Division in the Information Technology Laboratory at NIST.

Mr. Boyens provided a general overview of the cyber insurance market, focusing on some of the barriers that employers face getting cyber insurance. He outlined what he viewed as the challenges facing employers: that generally there is a lack of understanding of cyber risks; that data regarding the frequency and type of breach incident are hard to find; that cyber threats are man-made and always changing; and that this is still a relatively new area so there is not a lot of available data. Mr. Boyens also highlighted that standards and practices differ with each insurance firm and that he has observed communications barriers where terms and conditions in policies vary based on industry jargon.

Mr. Boyens identified NIST Special Publication 800-53[11] as a resource that "provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk." While there is no specific resource for employee benefit plans, Mr. Boyens also cited the work of the Financial Services Sector Coordinating Council in addressing the cyber risks facing financial institutions.

[11] Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed Dec. 15, 2022).

Mr. Boyens also described what NIST views as the cybersecurity 5-factor framework:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Mr. Boyens testified that this framework allows organizations to assess their own cybersecurity risks, to plan future assessments and enable companies to communicate their assessment and approach. He noted that while NIST does not have expertise in the employee benefit plan market, it does have applicable financial services sector experience specifically with regard to the cybersecurity framework.

Mr. Boyens closed out his comments by sharing his insights in terms of the "next round of challenges" that face employers with regard to cybersecurity: how can employers/plan sponsors obtain more metrics on cyber incidents, understanding/quantifying how those cyber incidents impact firms/plans, which cyber controls are most effective, and getting employers to share their incident data so more learning can take place.

B. INSURERS, INSURANCE BROKERS, AND CONSULTANTS

1. Aon

Aon plc ("Aon") is a leading global professional services firm providing services in the areas of commercial risk solutions, reinsurance, health-related consulting and broking, and "wealth solutions" (retirement consulting, pension administration, and investments consulting). Brian Gillin, Managing Director and East Region Leader for Aon's Cyber Solutions E&O/Broking team, appeared before the Council and shared his views and professional expertise regarding cybersecurity insurance. At Aon, Mr. Gillin is responsible for managing a team of insurance brokers and for providing clients with "broking expertise" and advice regarding cyber, professional liability, technology, and media-related risks.

Mr. Gillin explained how insurance brokers work on behalf of clients seeking insurance coverage for various risks. Brokers both advise their clients regarding coverage solutions and will often also negotiate with the insurance providers regarding the coverage that the client is trying to secure. As relevant to the issue of cyber insurance, Mr. Gillin explained that brokers typically compile a presentation regarding the client that describes the types of cybersecurity controls that the client has in place and why, therefore, the client can be viewed by the insurance company as a "favorable" risk. At the same time, the broker is educating its client about how they can manage (and transfer to an insurer) their cyber risk.

Mr. Gillin shared that access to the cyber insurance market is available to companies and entities of all sizes, although the "distribution channels" for insurance products might differ, depending on market segment, industry, and complexity of risk. With respect to cost, Mr. Gillin explained that insurers typically use an entity's revenues as a common way to assess risk (and thus to determine pricing). However, insurers also look to the controls that the entity or organization seeking insurance has in place to address cyber risk.[12] Although different insurers might place greater emphasis on certain controls over others, Mr. Gillin stated that insurers universally look to see that the organization has deployed multifactor authentication (MFA) for remote access to systems or accounts before considering whether to underwrite a risk.

Mr. Gillin explained that, in the simplest terms, cyber insurance is focused on insuring against losses relating to data. Where a cyber event occurs that damages, deletes, destroys or otherwise compromises an organization's data (or that prevents the organization from accessing or using that data), cyber insurance reimburses the policy holder for the costs incurred in returning to normal operations. The core of a cyber insurance policy is breach response costs. This can include costs relating to hiring forensic investigators (to determine how the breach occurred and its scope), hiring legal counsel (to advise on how best to respond to the breach, potential liability, and legal obligations with respect to data-breach notification laws and credit-monitoring requirements), and even hiring a public relations firm to assist with mitigating any reputational damage associated with the incident.

[12] See also, *infra*, at 19-20 for a description of the cyber controls that most insurance companies use in connection with underwriting cyber-related risk.

Mr. Gillin added (consistent with the testimony of other witnesses who appeared before the Council) that cyber insurance policies will not address losses relating to the theft of funds.

Mr. Gillin also explained that cyber insurance policies typically exclude from coverage breaches of fiduciary duty under ERISA, although he noted that it is possible to negotiate with an insurer to "carve [such coverage] back" into the policy, such that coverage is available for the loss of data even where that loss emanates from a breach, or alleged breach, of fiduciary duty. He cautioned, therefore, that employee benefit plan fiduciaries seeking cybersecurity insurance coverage should make sure that there is a proper "carve back" to the ERISA exclusion so that such data breaches are covered and not excluded. Ultimately, though, he acknowledged that the interplay between the coverage that is available under a cyber insurance policy and that which is available under a fiduciary liability insurance policy will depend on the wording of those policies.

2. Euclid Fiduciary

Daniel Aronowitz, Managing Principal and owner of Euclid Fiduciary, a leading fiduciary liability insurance underwriting company for employee benefit plans, testified before the Council about the multiemployer plan market. Mr. Aronowitz testified that about 95% of multiemployer plans have stand-alone cyber insurance coverage, with the multiemployer plan being the name insured. Mr. Aronowitz believes the Council should focus on the multiemployer plan market to gain an understanding of how the cyber insurance market for employee benefit plans will evolve, because multiemployer plans are the ones buying cyber insurance for the employee benefit plans, as opposed to single-employer plans, which generally rely on the cyber coverage of the broader corporate entity (and which might or might not include the employee benefit plans as covered entities, depending on the policy terms and the insuring agreements). He believes a "bundle" of fiduciary, cyber and crime insurance is the model that multiemployer benefit plans will increasingly use in the future.

Mr. Aronowitz also testified that many multiemployer plans have put greater cyber controls in place as a direct result of the cyber insurance companies imposing stricter underwriting standards on multiemployer plans to secure cyber insurance coverage. Mr. Aronowitz listed the essential coverage elements that he believes a comprehensive cyber

insurance policy should contain: breach response, cyber extortion/ransomware, business interruption for self and third parties, liability to third parties, and cyber crime. Further, Mr. Aronowitz stated that he believes the Council should recommend to the Department that all single- and multiemployer plans be required to maintain cybersecurity insurance, crime insurance, and fiduciary liability insurance, in addition to the fidelity bond that is required to be maintained today[13].

3. Lincoln Financial Group

Christine Swift testified before the Council on behalf of Lincoln Financial Group. As Vice President of Litigation and Corporate Insurance, Ms. Swift primarily focuses on complex litigation. She communicated the importance of understanding that a portfolio of insurance coverages is needed to cover all the aspects of a cyber attack. She outlined the main cyber risks that employee benefit plans are able to manage by purchasing insurance and the insurance coverages that would be required to respond to each risk. For participant monetary loss or theft of funds, a type of fidelity insurance, called a crime bond, would most likely be needed, which is separate from the mandatory ERISA fidelity bond. For theft of participant confidential data, a cyber insurance policy would likely be needed. For breach of fiduciary duty claims related to a cyber attack, fiduciary liability insurance would be needed. Standing alone, none of these coverages will cover all aspects of a cyber attack on an employee benefit plan.

Ms. Swift also said that it is important to make the distinction between participant monetary loss itself and liability for money loss. These two types of losses require different coverages. For example, the employer or plan sponsor's liability for breach of fiduciary responsibility that results in a participant's monetary loss would generally be covered under a fiduciary liability policy or an errors and omissions (E&O) policy. However, the employer/plan sponsor or other entity holding assets that are taken from its possession in connection with a cyber event could file a claim for reimbursement of the dollars taken under a fidelity policy, specifically a crime insurance policy. This claim could typically be made without a determination that the insured has breached its duty with respect to protecting the assets in its possession, and if the employer/sponsor or custodian is not liable to the participant for the cyber

[13] *See* ERISA § 412 (29 U.S.C. § 1112).

loss then the employer/sponsor or custodian may have no legal obligation to reimburse the participant for such monetary losses.

4. Marsh McLennan

Timothy L. Marlin, Senior Vice President of Marsh McLennan and Cyber Product Development Leader for Marsh's North America Cyber Practice and is an advisor in the field of cyber risk management, appeared before the Council and shared his views and experiences regarding the current marketplace for cyber insurance.

Mr. Marlin has observed that capacity in the cyber market has tightened over the past few years and insurance carriers are more selective with their policy placement. He estimates that there are 50 policy writers today with about $400-$500 billion in capacity. While capacity may be more constrained, he believes the tides are turning as carriers are getting more comfortable with clients "cyber hygiene" programs. There is demonstrated optimism in the market, and rates are starting to moderately reward those that can demonstrate strong cyber hygiene. Specifically, rate increases are slowing down: the Q2-22 year-over-year increase was 60% vs the Q4-21 year-over-year increase, which was 133%.

Mr. Marlin noted that, given these rate increases, his clients have had to make some difficult decisions to manage cyber insurance costs. They have had to consider reducing their limits levels, increasing retentions (deductibles) and/or making an investment in building more robust controls

Mr. Marlin also noted that retirement/benefit plans generally face many of the same risks as other financial service organizations and there are many factors that are driving change in the cyber insurance market for retirement/benefit plans. Insurance coverage for the employer and their plans is a mosaic of coverage for first-party and third-party providers, and he added that he is seeing increasing interest in retirement plans either being named within the corporate cyber policy or placing a separate policy for the plan, or are amending the ERISA exclusions in the corporate policy.

The "mosaic" of coverage typically includes a fiduciary insurance policy, a fidelity bond, and a crime policy. Fiduciary insurance provides coverage in the event a fiduciary did not act

prudently or otherwise committed a breach of fiduciary duties under ERISA. A fidelity bond covers those who access the money and therefore need to be bonded; internal employees are typically covered under this bond. A crime policy is more focused on external parties that can steal money; therefore, it is important to ensure that policy language is updated to reflect the evolving environment regarding cyber impacts like fraudulent access and social engineering coverage. Mr. Marlin has observed some ERISA exclusions in crime policies that warrant additional scrutiny/study.

As cyber attacks have increased, cyber insurers are able to gather more data about how the breaches have occurred and determined that certain controls can minimize attacks. Marsh, in partnership with insurers, developed list of ***12 key controls*** to ensure an employer has strong cyber hygiene in place for their benefit plans. Mr. Marlin identified five key controls as having the greatest positive impact:

1. Multi-factor authentication (MFA)
2. Endpoint detection and response (EDR)
3. Back-ups
4. Privileged access management (PAM)
5. Email filtering/web security.

Council members asked Mr. Marlin if he thought that most plan sponsors/employers were employing this mosaic of coverage and if it was sufficient. He responded that he was not observing obvious gaps but commented that coverage is unique to each client's facts and circumstances. He further commented that all coverages are essential and need to work together and that a good broker can help by reviewing and identifying any gaps.

5. Segal

See Part III.C.3.

6. Willis Towers Watson

Matt Klein testified to the Council on behalf of Willis Towers Watson. Mr. Klein serves as the National Fidelity Product Leader of the FINEX Financial Institutions Practice at Willis

Towers Watson. Mr. Klein began with an explanation of the difference between theft of participant assets, which is often mislabeled as a cyber attack, and an actual cyber attack, for the purposes of insurance coverage. A cyber attack is when personal data is obtained by an unauthorized nefarious third party and is covered under a cyber insurance policy. Theft of participant assets includes the loss of funds or assets from the employee benefit plans due to social engineering or direct theft and is not covered under a cyber insurance policy. Rather, a fidelity/crime bond is the primary coverage to respond to loss of assets--either assets owned directly by the insured or assets owned by third parties for which the insured is responsible, which include the participants in retirement plans for which the covered organization is responsible.

Mr. Klein stated that for non-financial institutions, like the average retirement plan sponsor under ERISA, a fidelity/crime bond only offers "first-party" coverage, meaning a claim could only be filed by the insured party that that was in control of the funds when the theft occurred. For example, if a cyber attack resulted in loss of funds from a custody account, the custodian's fidelity bond would respond to the loss. If a cyber attack occurred on a plan sponsor's system and resulted in the theft of funds from an employee benefit plan under the plan sponsor's control, then the employer's fidelity bond would respond to the loss. Mr. Klein explained that, even though a fidelity bond is a "first-party" insurance policy, it can still provide coverage for loss of assets suffered by third parties (such as retirement plan participants, employees, or customers) because the "first party" (i.e. the insured organization) can make a claim that includes the loss of money from the employee benefit plans that are under its control, as long as the coverage is structured properly. The distinction in this case between first-party coverage and third-party coverage is not necessarily about the covered party itself but rather about which party is able to file claims directly with the insurance carrier. Mr. Klein explained that additional insuring agreements are typically added to a fidelity bond or a crime coverage policy that can provide additional coverages specific to employee retirement plans. Mr. Klein recommended that all non-financial institution crime policies contain two additional insuring agreements covering computer systems fraud resulting in loss of participant funds and social engineering fraud resulting in fraudulent wire transfer of participant funds due to social engineering.

7. Zurich North America

Zurich North America ("Zurich") is a leading underwriter of commercial property and casualty insurance coverage and provider of insurance-related services in the U.S. and Canada. Kara Higginbotham, Vice President, Corporate Accounts Manager for Professional Liability and Cyber at Zurich, testified before the Council regarding her experience leading a team of underwriters responsible for evaluating and pricing cyber-risk coverage for large organizations in the U.S. across various industries.

Ms. Higginbotham explained that, prior to issuing an insurance policy that provides for cybersecurity coverage, underwriters will seek information, typically via an insurance application but also occasionally through in-person meetings with the applicant, relating to the applicant's risk profile. In this regard, underwriters will look at the controls, processes, and procedures that the applicant has in place to mitigate their exposure to losses resulting from cyber incidents. Based on the information gathered, the insurer's underwriters will develop a coverage proposal--or decline to underwrite the risk.

Like other witnesses who appeared before the Council, Ms. Higginbotham stated that cybersecurity insurance does not cover a loss of funds but rather only losses relating to the loss, theft, or misappropriation of data. (Ms. Higginbotham also stated that most cyber-insurance policies exclude from coverage ERISA breach-of-fiduciary duty claims, although she recognized that a breach of fiduciary duty claim might also relate to a loss of data.) Pricing for cyber-insurance coverage is typically a function of (i) the size of the applicant-organization (usually measured with reference to the organization's revenues), and (ii) the volume and type of data that the organization possesses.

As part of the underwriting process, underwriters will also look at specific controls that the applicant has in place to mitigate the risk that there will be a loss, misuse, or theft of data. With respect to cyber controls, Ms. Higginbotham agreed that the market has coalesced around a handful of controls that are viewed as marketplace minimums. Ms. Higginbotham identified the following types of controls as constituting insurance industry "minimum expectations":

1. Multifactor authentication (MFA)--requiring a second form of authentication (beyond user name and password) in order to access a system or an account
2. Vulnerability scanning and "patch" management--scanning a network for potential vulnerabilities (particularly relating to software) and addressing those vulnerabilities in a timely, efficient, and organized manner
3. "Endpoint Detection & Response" (EDR)--in the context of a network, monitoring for suspicious activity at the "endpoints" (e.g., on users' laptop computers)
4. E-mail filtering and e-mail security--using spam-filtering software (to reduce the incidence of "phishing" e-mails getting through to users)
5. Awareness training (including social-engineering exercises)--conducting annual (or more frequent) awareness training regarding cybersecurity risks, including implementation of periodic "mock" phishing exercises
6. Access management--limiting network or systems access to those who need to access such network or system (based on the employee's role), including "privileged" access (restricting access to those parts of a network or system containing highly sensitive or high-value data to only certain individuals possessing "privileged" credentials)
7. Network segmentation--designing a network such that unauthorized access to one part will not enable access to other parts
8. Disaster recovery planning and testing--having the ability to recover quickly from a cyber event, including, with appropriate data backup, the ability to restore missing or stolen data without the need to pay ransom
9. Incident response plan--having written (and tested) business continuity plans and vendor/supply-chain continuity plans; essentially, being prepared, in advance, to respond to a cyber event, where the above controls all fail.

Some controls--such as the use of multifactor authentication for remote access--are universally acknowledged as critical to negating a cyber attack, she said. However, in

underwriting risk, different carriers might place different emphases on different controls and also exhibit some variation in what they are willing to accept in terms of "control adequacy."

Ms. Higginbotham also referenced the issue of re-insurance (the process whereby insurance companies attempt to reduce their exposure to large losses by transferring some of the risk that they have underwritten to other insurers). Ms. Higginbotham explained that most insurance companies do indeed use some type of reinsurance with respect to their cyber insurance risk, although the exact details of that process will differ from carrier to carrier. At Zurich, she explained, reinsurance underwriting is an annual process. The company's reinsurers will look at Zurich's underwriting decisions (from a "portfolio" perspective) and engage in a dialogue with the company about those decisions. The use of reinsurance is increasing, she explained, particularly now with increasing ransomware incidents.

Ms. Higginbotham concluded by stating that cyber insurance coverage, whether provided through standalone policies or as part of a package of coverage, is available to all sizes of organizations--small, medium, and large.

C. PLAN SPONSORS, PLAN FIDUCIARIES, AND PLAN SERVICE PROVIDERS

1. American Benefits Council

Kent Mason and Michael Hadley, partners at the law firm of Davis & Harman LLP, testified on behalf of the American Benefits Council (ABC). ABC is a trade organization that advocates on public policy matters relating to employee benefits. Its advocacy is focused on the employee benefit plans offered by their large employer members. ABC's "more than 440 members are primarily large U.S. employers and also includes organizations that provide services to employers of all sizes regarding benefit programs. Collectively, the ABC's members directly sponsor or provide services to retirement and health plans covering virtually all Americans who receive employer-sponsored benefits."[14]

[14] https://www.americanbenefitscouncil.org/about-the-council/about-us/#whoweare (accessed Oct. 1, 2022).

At the time of their appearance before the Council, ABC was still developing a planned survey of its members regarding the types of insurance that their members have and the types of losses that existing insurance is available to cover. The results (described further below) were shared with the Council after Messrs. Mason's and Hadley's appearance.

Messrs. Mason and Hadley shared that, in putting the survey together, ABC felt that it was fundamental for the Council to consider first whether the law actually requires plan fiduciaries and plan service providers to guarantee against the loss of participant retirement assets, when the plan fiduciary or service provider has done everything that it reasonably could to prevent cyber-related incidents that might harm participants. They went on to say that, for purposes of the Council's investigation, looking at this question through the lens of benefit plans subject to Department oversight and guidance, the ERISA fiduciary standard would apply, adding that this is one of the highest standards of care owed by one party to another. If a fiduciary acts prudently in connection with its efforts to prevent cybersecurity incidents and the plan service provider acted appropriately with respect to its responsibilities and the participant is still harmed, there is generally no legal duty for the plan fiduciary or the service provider to remedy that harm. In such a case, plan insurance coverages would also not be available. In making this point, they highlighted the fact that bad actors can obtain participant data, which they would use to perpetrate a fraud theft, from data breaches that have nothing to do with the plan fiduciaries' exercise of prudence or plan service providers' failures. In this regard, they pointed out that there was recently an IRS data breach that compromised individual taxpayers' personal identifiable information and that other regulators, such as the Department, have requested, via plan examinations, confidential data and that those organizations could be subject to a cybersecurity breach that might enable the theft of participant information or assets through no fault of the fiduciary or service provider.

However, if a plan fiduciary did not act prudently to prevent a cyber incident and that incident were to harm a participant, then the fiduciary would have breached its ERISA fiduciary duty and would be liable for monetary harms caused by the breach. In this regard, fiduciary liability insurance is something that most plan fiduciaries carry and consequently damages resulting from a fiduciary's breach would already be covered under the plan's fiduciary liability insurance policy.

The loss of a participant's retirement savings that can occur when the plan fiduciaries, and their prudently selected service providers, have done nothing wrong is an important and larger social issue in need of a broader policy solution, they said.

Messrs. Mason and Hadley also recommended that, if the Department were to decide to take action to address this larger policy issue, which ABC did not think would be appropriate, the Department should certainly do so via a notice and comment process rather than through the issuance of sub-regulatory guidance. In their view, the notice and comment process introduces more rigor and opportunity for stakeholder input that would naturally lead to more comprehensive and better rulemaking.

Following Messrs. Mason's and Hadley's appearance before the Council, ABC shared the results of its member survey. The results indicated that (of the employers/plan sponsors responding) most were not aware of the potentially useful aspects of cyber insurance and how it could address losses that are not tied to culpability.

2. Callan Associates

See Part III.C.4.

3. National Coordinating Committee for Multiemployer Plans and Segal

The National Coordinating Committee for Multiemployer Plans (NCCMP) is a nonpartisan, nonprofit organization organized to protect the interests of multiemployer pension and welfare plans, the 20 million active and retired Americans who participate in these plans and their labor and employer sponsors. On the issue of cybersecurity insurance, the NCCMP provided the testimony of Diane McNally, Senior Vice President and Insurance Practice Leader with Segal Select Insurance Services, Inc.

Ms. McNally noted that the early forms of cyber insurance emerged in the 1990s as third-party policies designed to protect against media and data processing errors. With rising data events and increasing threat actors, cyber attacks are more frequent, costly to address, and have long-term exposures for plans. She further stated that leading carriers for cyber insurance are managing their risk appetite, addressing profitability results and increasing their focus on clients

with strong cyber hygiene. Accordingly, the cyber insurance market environment remains challenging with high demand for this form of insurance and a cautious approach to the underwriting of coverage.

Ms. McNally also testified that cybersecurity insurance is almost universal in the multiemployer plan space. Ms. McNally noted that cybersecurity insurance most often provided breach incident response, first party coverage and third party coverage for data incidents. Cyber insurance affords valuable assistance to plans that have incurred data breaches by providing forensic and legal services, assistance with breach notification, and credit monitoring. In situations involving ransomware attacks, cyber insurance deals with the extortion demands inherent in the attacks while working to restore the plan's computer capabilities. Ms. McNally also indicated that multiemployer plans may have other forms of insurance such as fiduciary insurance and bonding that may come into play during a cybersecurity event.

The NCCMP also informed the Council that insurance carriers and their underwriting departments are requiring additional information from plans seeking cybersecurity insurance for the first time or with renewals of existing policies. Ms. McNally identified the following areas that cyber underwriters are requiring:

- 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
- 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.

3. SPARK Institute, Inc. and Callan Associates

Tim Rouse, Ben Taylor and David Levine testified before the Council as part of a panel.

Mr. Rouse presented in his capacity as the Executive Director of the SPARK Institute. The SPARK Institute is a trade group representing defined contribution plan recordkeepers, investment providers and other investment related plan service providers. Joining Mr. Rouse on the panel was Ben Taylor, vice president and head of tax-exempt defined contribution research for Callan Associates, an independently owned investment consulting firm in the U.S. Mr. Taylor shared his views based on his work with public sector and non-profit-plan firm clients. David Levine, a principal of the Groom Law Group, Chartered, a boutique employee benefits law firm, testified based on his experience in the benefit plan industry.

SPARK has a Data Security Oversight Board dedicated to helping their constituents mitigate the risk of cybersecurity fraud threats. In furtherance of this aim, SPARK developed a framework for their members to use to describe the organization's cybersecurity fraud/threat capabilities to its plan clients as well as to set forth industry best practice fraud controls that outline a baseline of cybersecurity controls plan vendors should seek to maintain.

This panel also made four additional points for the Council:

1. Cybersecurity insurance does not cover the loss of a participant's assets resulting from a cybersecurity theft incident.
2. Small plans have trouble obtaining cybersecurity insurance.

3. Ransomware attacks can be hugely impactful even if the plan or plan's service provider has backups of data because the attack could corrupt the operating systems making the backups ineffective.
4. Information-sharing about threats or attack strategies is seen as important to a coordinated effort to prevent these attacks.

These witnesses recommended the development of a common understanding of what is meant by the term "cybersecurity insurance." Currently, it seemed to them that this understanding did not broadly exist. Cybersecurity insurance does not cover all harms flowing from a bad actor's use of technology to impact a benefit plan.

Identifying the various threats or means of attack that allow bad actors to harm a plan is important to identifying the most appropriate coverage to protect against that specific harm.

D. REPORTERS, RESEARCHERS, AND ACADEMICS

1. Richard Betterley

Richard S. Betterley is the president of Betterley Risk Consultants, an insurance and risk-management consulting firm that provides advice and counsel on matters relating to the commercial property and casualty insurance industry and its customers. Mr. Betterley created *The Betterley Report* in 1994 to serve as an objective source of information about specialty insurance products such as management liability, cyber risk, privacy, intellectual property, and media insurance products. *The Betterley Report* (today published by the International Risk Management Institute) is an annual survey of insurers and reports information relating to cybersecurity insurance products and coverage.

Mr. Betterley explained that cybersecurity insurance is purchased in the commercial insurance marketplace and is readily available. Like many other witnesses who appeared before the Council, Mr. Betterley emphasized that cybersecurity insurance is largely intended to cover (and is limited to covering) losses arising out of the loss or breach of <u>data</u> (as opposed to tangible property or investment assets).

Mr. Betterley provided the Council with a copy of the most recent issue of *The Betterley Report*.[15] The 2022 report contains detailed information gathered from 22 insurance companies regarding their cybersecurity insurance products.[16] The report includes information regarding such topics as: capacity, deductibles, and coinsurance amounts; "Coverage Triggers"; types of data covered and types of losses covered; and exclusions (including exclusions for war, terrorism, and state-sponsored terrorism).[17]

In a section titled, "Security Assessment Requirements," the report notes that "[i]nsurer-required assessments of the prospective insured's [cyber] security policies are rare now …."[18] In a table reporting the survey results on this topic, the 2022 report reveals that, of the 22 insurers responding, only 3 (i.e., 9%) said that they required completion of cybersecurity questionnaires, with another 4 (18%) reporting that they required them only sometimes (depending on risk). Notably, 16 of the 22 insurers (70%) reported they did not require such assessments at all as part of their underwriting process.[19]

2. Sasha Romanosky

Sasha Romanosky is a Senior Policy Researcher at the RAND Corporation. Mr. Romanosky researches the economics of cybersecurity and has authored or co-authored a number of articles regarding cybersecurity insurance, including a 2019 research paper[20] on the pricing of cybersecurity insurance. His testimony before the Council centered on how risk is priced by the cybersecurity insurance carriers and the types of pricing strategies they use when setting their rate schedules.

Mr. Romanosky's basic conclusion from his research is that insurance carriers do not have explicit information about what security controls work best to mitigate cyber incidents, and their pricing strategies are sub-optimal. As evidence, Mr. Romanosky presented the findings

---

[15] *The Betterley Report, Cyber/Privacy Insurance Market Survey--2022: Rate Increases Sustain this Product but for How Long?* (June 2022) [hereinafter, "Betterley Report"].
[16] Id., at 3.
[17] See id., at 16-118.
[18] Id., at 10 (emphasis added).
[19] Id., at 56 (table).
[20] S. Romanosky, L. Ablon, A. Kuehn, & T. Jones, "Content analysis of cyber insurance policies: how do carriers price cyber risk?," 5 *Journal of Cybersecurity* 1 (2019).

from his research study on how insurance carriers price cybersecurity risk. He and his co-authors created a data set over 180 filing dockets from New York, Pennsylvania, and California filed under the broad category of property and casualty (P&C) insurance--since "cybersecurity insurance" is not covered under a single line of business but instead is distributed across multiple lines of property and casualty insurance. These states were chosen, he explained, because they are three of the largest states by population and therefore would be expected to produce a wide variety of policies. His and his colleagues' research showed that the most common pricing strategies are the following: 1) flat-rate pricing which is the same for every firm, 2) base-rate pricing which is based on a firm's size and type, and 3) information-security pricing which incorporates some information about the firm's security controls. Flat-rate pricing uses data from industry and academic reports and is targeted toward small businesses. Base-rate pricing starts with revenue and increases the base rate and limits based on the characteristics of the company. Information-security pricing includes changes to the base rates depending on a company's response to a security questionnaire about their security practices.

Mr. Romanosky concluded that the insurance industry is currently unable to effectively assess which security controls are most effective, that the connection between risk and metrics is weak, and as a result, firms and policy makers do not know how much to optimally spend on cyber insurance. Finally, his analysis demonstrated that the cost of cybersecurity incidents is not as high as commonly believed, at a median cost of $200,000 for a data breach. Mr. Romanosky believes that when people point to companies not doing enough to mitigate cybersecurity risks today, the companies may be justified in not spending more on cybersecurity today because there is not conclusive research on what "enough" means, and companies must manage a wide variety of risks (financial, supply chain, regulatory), and cybersecurity is just one these risks and perhaps not a priority because the median cost of a breach is relatively low.

3. Josephine Wolff

Josephine Wolff is a professor of cybersecurity policy at the Fletcher School at Tufts University. She is the author of two books regarding cybersecurity: *You'll See this Message When it's Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches* (Cambridge, MA: MIT Press, 2018), and *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware,*

Computer Fraud, Data Breaches, and Cyberattacks (Cambridge, MA: MIT Press, 2022). The latter title reviews the history of cyberinsurance and includes her public policy observations.

Professor Wolff explained to the Council that, initially, all cybersecurity information was based on data breaches. Around 2010, insurance policies focused on big retailers but have since branched out, driven by demand, involving ransomware and business interruption. A trend began toward stand-alone cyber policies. A new market emerged within the insurance industry, with approximately $6-8 billion per year of insurance premiums.

She further explained that there has been a drive by insurance companies in recent years to exclude cyber coverage from general business insurance policies in favor of separate, standalone policies. Most cyber policies now have relatively low limits.

She also stated her belief that insurers are not confident in their ability to properly vet the security measures of potential insureds. The amount and quality of collected cybersecurity/cyber crime data over the last decade have not materialized as anticipated.

Early lawsuits regarding data breach were class action lawsuits. Attorney-client privilege, due to lawyers being engaged, has hurt the ability to gather data via claims activity.

Professor Wolff shared that she finds it "demoralizing" that insurers are not, at present, leading the effort to improve data sharing. Perhaps they do not have the data or they are reluctant to share because of competition with other insurers. Insurers in general are frustrated because they cannot find meaningful trends (or "answers") from the data that they do have, regarding what defensive measures work best. More required reporting from insurers would probably help the situation and would promote better data sharing throughout the overall cyber industry.

She also explained that insurers do not tie the pricing of their policies to actual security measures that a client may have in place, but rather insurers look to minimize their risk exposure via low limits. Current insurance policies are based more on "word of mouth" knowledge versus being grounded in data.

Additional required disclosures from insurers might be helpful in likely prohibiting attorney-client privilege from blocking better data collection. More cyber-related activity, in

general, will probably lead to higher premiums; however, more sophisticated data collection--and improved sharing--will eventually help all involved, especially if best practices are effectively communicated.

Data breach notification requirements already exist in all states, but most types of cyber attacks do not require disclosure. Reporting regarding cyber attacks should be required. More severe penalties are needed regarding noncompliance with minimum required cybersecurity measures for companies. Insurance companies are not seeing the urgency to change their current practices.

E. LITIGATORS

1. Stefan Dandelles

Stefan Dandelles is an attorney with Kaufman Dolowich & Voluck, LLP, and he represents insurers, thus offering a significantly different perspective than Mr. Miller and Mr. Turano (see section III.E.2, *infra*). He agrees with much of what the other two gentlemen shared. However, he emphasized that insurance should be the final backstop, not the first line of defense, regarding cyber breaches and disputes. Solid policies and procedures should be the primary means of addressing cyber issues. Brokers and underwriters should tailor the right policies for a given business. This is a two-way street: policies must be tailored to businesses, but businesses must also tailor themselves to policies.

According to Mr. Dandelles, given the many different types of policies that he and his firm see regarding cybersecurity, it is important to differentiate a data breach, which is a cyber issue, from theft of assets or property, which is a crime/fidelity issue. In the context of an employee benefit plan, risk lies not just at the plan level and the plan sponsor level but also at the individual account level within a given plan--and thus at the plan administration level. Identity theft occurs at relatively high levels when verification procedures are weak. Once bad actors gain access, there is usually no stopping them. Theft occurs at the individual account level, not at the higher plan level. Thus, policies and procedures should focus on addressing administration involving individual account-level activity. Current policies that address cyber issues involve a blend of first and third party indemnity.

Regarding insurance coverage for theft of assets, given the various roles of custodians, Mr. Dandelles believes that the relevant questions involve: who owns the asset, who holds the asset, and who is legally liable for the asset. The question of who is legally liable for a given asset is open to different circumstances and interpretations, which can trigger certain provisions within policies.

Mr. Dandelles believes that underwriters, brokers, and insureds must work together to improve procedures, such as required "call backs" in any even remotely suspicious situation, as an added level of verification before money gets transferred. He also stated that policyholders who make material misrepresentations regarding their cybersecurity controls could risk having their claims denied or their policies even being rescinded. Education and training would help avoid such situations.

Mr. Dandelles added that "stacking" of different insurance coverages, and coordination of appropriate limits within policies, will help navigate future disputes toward better resolutions.

2. Mark Miller and Tab Turano

Mark Miller is an attorney with Miller Friel, PLLC. He represents corporate insurance policy holders that have disputes with insurers. Tab Turano is also an attorney with Miller Friel, PLLC, and he also represents corporate insurance policy holders that have disputes with insurers.

Mr. Miller noted that some insurance-coverage cases involve investment account losses. The caselaw involved is old. This makes it challenging in situations where hackers, who pose as investors, steal, e.g., crypto-related assets. Crime bonds, E&O policies, D&O policies, and general liability policies all have relevance to this topic. He noted too that caselaw varies significantly from state to state.

Mr. Turano noted that computer fraud, funds transfer fraud, and social engineering fraud are all prevalent threats. Mr. Turano noted a case in Indiana[21] where a trial court found no fraud, just theft, in a ransomware situation. This was affirmed by the court of appeals. The Supreme

[21] *G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.*, 165 N.E.3d 82 (Ind. 2021).

Court of Indiana overturned the decision, finding that the applicable hacker committed fraud. This is an example of how computer fraud can and does come into play in cyber related cases.

Mr. Turano also referenced a 2022[22] case where a trial court determined that computer fraud is very limited and only applies in certain situations. However, the relevant appellate court found that such coverage is broader and therefore applicable. In a separate case in Minnesota[23], a court found that a loss due to a cyber attack was not caused by computer fraud but rather by a poor decision by the CEO of the insured company. In a separate 2021 case[24], a court found that no insurance coverage applied because of the varying points in time when custody of applicable funds occurred. Thus, Mr. Turano highlighted the various decisions that have been reached in many different cases, involving complicated sets of circumstances.

Mr. Miller agreed that cybersecurity situations tend to be complex and confusing, and that case law has gone in many different directions. He said that he feels that business owners and managers must question what policies really fit each given business. Finding the most appropriate policy or policies must be evaluated by experienced brokers and attorneys who understand relevant case law.

Mr. Turano noted that cyber policies with third party coverage have very significant limitations.

Regarding whether the failure of maintaining proper controls leads to a decline in insurance coverage, Mr. Miller notes a policy should specify how the insured must adapt as various situations unfold. If not adhered to by the insured, then the policy should state that coverage does not apply. Passionate lawyers argue both sides of disputes on this topic.

Regarding what types of cyber coverage issues might be litigated in the future, Mr. Miller recalls that cyber policies have been a very significant "cash cow" for insurance companies and their investors. Applicable insurance companies have enjoyed very low loss ratios, at least until

[22] *Ernst & Haas Mgmt. Co. v. Hiscox, Inc.*, 23 F.4th 1195 (9th Cir. 2022).
[23] *SJ Computers, LLC v. Travelers Cas. & Sur. Co. of Am.*, 2022 WL 3348330 (D. Minn. 2022).
[24] *RealPage, Inc. v. National Union Fire Ins. Co.*, 21 F.4th 294 (5th Cir. 2021).

recent years. Mr. Miller feels there will be more litigation regarding insurance companies' denial of cyber related claims.

IV. DISCUSSION AND COUNCIL OBSERVATIONS

A. OVERALL IMPRESSIONS

The Council was of the overall impression that the market for insurance relating to losses attributable to cyber incidents is still somewhat new and is also evolving. Additionally, the changing nature of cyber threats (as bad actors discover new ways to exploit vulnerabilities in an increasingly internet-connected world) will necessarily cause the scope, cost, and availability of cyber-related insurance also to continue changing and evolving.

B. "CYBERSECURITY" INSURANCE VS. OTHER TYPES OF INSURANCE

One of the key things that the Council learned during its study regarding cyber insurance is that cyber insurance policies generally do not cover theft of assets. Instead, such policies' primary focus is covering losses arising from the theft of data.

Fidelity/crime policies can cover losses arising from the theft of assets, but there might be limitations on such coverage. For example, some fidelity policies only provide coverage for losses attributable to the wrongful acts of employees of the insured (and not those of a third party or other external "bad actor"). Other policies can provide coverage against losses due to theft by third-parties or strangers (most typically under policies written for the financial services sector as opposed to under a "commercial" lines policy). Like most insurance, there might be a deductible (or retention) amount and also a cap on the overall coverage amount.

Fiduciary liability insurance provides coverage against third-party claims of breach of fiduciary duty. Depending on how a claim arising from a cyber incident is articulated (i.e., as a claim alleging a breach of fiduciary duty under ERISA or as some other type of claim such as

one predicated on state or other federal law), coverage under a fiduciary liability insurance policy might or might not be available.[25]

Based on the foregoing, plan fiduciaries that have "cyber insurance" coverage need to understand the limitations of such coverage. Plan fiduciaries should determine whether the theft of plan assets is covered under other available insurance policies. In this regard, a fiduciary who wishes to have coverage in place for all losses relating to cyber incidents will likely need to construct a "portfolio" of insurance coverage.[26]

C. DISTINCTION BETWEEN "FIRST-PARTY" AND "THIRD-PARTY" LOSSES

Cyber-insurance policies (which, as noted above, generally provide coverage only for losses arising out of the theft of data) provide coverage for what is referred to as "first-party" losses and "third-party" losses. "First-party" losses generally means losses incurred directly by the named insured. "Third-party" losses generally means losses incurred by a person other than the named insured, where the third party is asserting a claim against the named insured for those third party losses.

Examples of first-party losses that are often included as part of a cyber insurance policy are: the cost of notifying affected individuals (e.g., plan participants) of a data breach; the cost of providing credit monitoring services for affected individuals (e.g., plan participants) for a period of time; the cost of ransom (in a ransomware attack); the cost of forensic investigators (to determine the root cause of the cyber attack); the cost of outside legal advice; the cost of hiring a public relations firm to manage publicity relating to the incident; and other costs relating to the disruption of one's business. Obviously, the specific terms of any given policy will control.

Examples of third party losses that can be included as part of a cyber insurance policy are: the cost of any judgment or settlement of a claim brought against a named insured for losses arising out of a cyber incident and the cost of outside counsel to defend against such claims. Here again, the specific terms of any given policy will control. In this regard, some cyber insurance

[25] Another consideration related to fiduciary liability insurance coverage is whether the cost of such insurance can be paid from employee benefit plan assets. Treatment of this consideration is discussed in section IV.G., below.
[26] As also discussed further below, oversight of plan service providers (and determining what insurance, if any, they have) is an important part of managing a plan's cyber risk. See section IV.F, below.

policies have exclusions from coverage for third-party claims, which might include an exclusion for claims predicated on an alleged breach of fiduciary duty under ERISA.

D. INCREASING PREVALENCE OF STANDALONE CYBER INSURANCE POLICIES

The Council heard from witnesses who noted that they are seeing increased interest in cybersecurity insurance from single-employer benefit plan sponsors of all sizes who are considering standalone cyber insurance for their benefit plans. Plan-specific insurance allows sponsors to tailor the coverage to the plans' needs and provides separate limits for the plan/fund in the event of a claim. One witness provided market statistics:

- Five years ago, less than 10% of benefit plans were protected by cyber insurance
- Today, over 95% of multiemployer are protected by cyber insurance coverage
- Estimates are that approximately 60-75% of single-employer plans are protected under the plan sponsor's cyber policy, with greater uptake of coverage for large plans.

As noted above, it is common for cyber policies to contain exclusions related to violations of ERISA. The broker community noted that some larger, more sophisticated, single-employer clients are increasingly seeking policy endorsements to add their benefit plan or plans to their cyber insurance programs. Witnesses noted that this could necessitate an amendment to any ERISA related exclusions in the employer's corporate cyber policy.

More than one witness noted that most multiemployer clients prefer standalone cyber insurance policies. For such multiemployer plans, the policy may be written in the name of the Plan or include related plans and entities depending on how comfortable the board of trustees is with having the shared policy limits and how costly the premiums for separate policies would be.

E. CONNECTION BETWEEN CYBER INSURANCE AND "CYBER HYGIENE"

One of the key issues that the Council hoped to understand better was the link (if any) between obtaining cyber insurance and "cyber hygiene."

The Council heard testimony from witnesses who explained that, currently, it is simply not possible to purchase or renew cybersecurity insurance coverage without demonstrating that the insured has implemented cybersecurity risk controls. Controls that underwriters look for can include:

- Multi-factor authentication (MFA) (protocol for users to access systems)
- Social engineering exercises (mimicking of phishing) and cyber-awareness training
- E-mail filtering and security
- Vulnerability scanning and "patch" management (timely software updates/patches)
- "Endpoint" (e.g., laptop computer) protection and response
- "Privileged" access protocols (limiting access to certain systems to only certain persons)
- Network segmentation (having different processes/data on different networks)
- Disaster recovery preparedness (including practice for regular data backups)
- Incident response plan.

Not all insurers require all of the above, although witnesses frequently identified MFA as a minimum requirement.

The basic premise of requiring insureds (or prospective insureds) to demonstrate their adoption of cyber-related risk controls is that insurance carriers use the data received from past claims to determine which security policies/controls are most effective and then provide incentives to organizations who adopt these security policies/controls.

a. Some witnesses testified that the improving cybersecurity practices of insured organizations is a direct result of cyber insurers requiring certain controls as minimum requirements for insurability. These witnesses noted that, because the threat landscape is evolving and cyber insurance is a relatively new concept, the data continues to evolve as to which controls have the greatest impact on

mitigating cyber risks (and which therefore have the greatest impact on premiums).

b. However, the Council also heard testimony (and received written submissions) suggesting that not all insurers ask about cyber controls when they are underwriting cyber risk. Although some insurers do ask about an insured's (or prospective insured's) cyber practices, for other insurers underwriting decisions were made based on the size of the organization (namely, revenues), its sector (e.g., healthcare), and perhaps the number of devices connected to the network. One witness also suggested that, while various controls are viewed as common or "best practices," it is very hard to tell whether any given set of controls is actually effective at stopping cyber incidents.

As more data are collected, and the pricing models developed by researchers and insurers become more robust, the hope is that not only will cyber insurance lead to better cyber hygiene at organizations, but also that the organizations' cyber hygiene will materially affect their cyber insurance pricing and terms.

In summary, many experts view the insurance industry as having a direct positive impact on the overall cyber hygiene of organizations which will ultimately result in fewer cyber attacks and less damage to consumers, employees, participants, and beneficiaries. There was some disagreement among the experts as to whether insurance carriers and brokers have explicit information about what security controls work best in preventing cybercrime, because, if they did, one would expect to observe greater pricing reduction as a result of having those controls in place than is observed today. Ultimately, the interplay between cyber insurance and cyber hygiene could become an important policy question about whether cyber insurance can serve to reduce cyber risk broadly, beyond just shifting responsibility for the loss to a third party.

F. ROLE OF PLAN SERVICE PROVIDERS

The Council consistently observed that cyber insurance is but one way to protect plans, plan participants and plan beneficiaries. With most plan administration being outsourced to third-party service providers, plan fiduciaries might reasonably look to contractual indemnification from those service providers as a way to protect plans, plan participants and beneficiaries from

losses relating to cyber incidents, regardless of whether those losses are due to identity theft or actual theft of retirement account assets.

Optimal oversight of plan service providers should perhaps include routinely asking about service providers' own insurance coverage(s). Such a measure may be especially important where a cyber attack (such as a malware or ransomware incident) might affect a given service provider's entire client base, and thus raises the issue whether the applicable service provider has adequate resources (absent insurance) to respond to a cyber incident that affects more than a single client.

A number of witnesses appearing before the Council referred to cases involving what might be characterized as "blameless" incidents, i.e. where the plan service provider (and/or plan fiduciary) contends that it is without fault for the incident. For example, a plan participant's identity might be stolen--outside the employer or plan recordkeeping environment--and the "bad actor" (who might even be a trusted friend or relative) then uses that stolen identity (e.g., username and password) to access plan systems and cause a distribution to be made from the plan to a bank account controlled by the bad actor. While the Council reached no particular conclusion regarding this issue, it wished to "flag" this type of incident for the Department's consideration.

G. COST OF CYBER-INSURANCE COVERAGE

The Council heard testimony regarding recent increases in the cost of cyber insurance (due, primarily, to increasing ransomware attacks) and also heard some general testimony about the cost of coverage but did not obtain comprehensive information on this issue. Obviously, the cost of coverage is dependent on many factors.[27]

For fiduciaries purchasing coverage to protect a plan and its participants from losses relating to a cyber incident, the question arises as to whether the cost of such coverage can be paid from plan assets. While the Council did not explore this issue fully through witness testimony, as a general matter, the Council makes the following observations--

[27] See, generally, *supra*, at part III.

- ERISA section 404(a) provides that plan assets may only be used for (in addition to paying plan benefits) "defraying [the] reasonable expenses of administering the plan." Whether the cost of cyber-insurance coverage will be considered reasonable is necessarily a facts-and-circumstances assessment.
- In addition to the foregoing, ERISA section 410(b) allows a plan to purchase insurance for its fiduciaries or itself to cover liability or losses occurring by reason of the act or omission of a fiduciary, provided that the insurance permits recourse against the fiduciary in the case of fiduciary breach.
- Given both the fiduciary duty to protect plan assets and the potential harm to a plan in the event of a cyber incident, it would seem reasonable for plan fiduciaries to consider the purchase of cyber-insurance coverage to be a reasonable and necessary plan expense (or to provide some other form of protection against cyber threats to the plan, its participants and beneficiaries).
- In the context of retirement plans, some Council members flagged the fact that the Department (through the fee-and-expense disclosure under DOL Reg. § 2550.404a-5) and participants (in class action lawsuits) have placed a focus on plan costs and the effect those costs have, over time, on retirement accumulations and noted that plan fiduciaries would need to balance the need for such coverage with concerns about plan costs. Additionally, the Council observed that cyber insurance (and other insurance coverage) can cover many "named insureds," and as a result the plan fiduciary that is using plan assets to pay for the cost of coverage might need to be sensitive to the risk of a benefit plan's inadvertently subsidizing the cost of coverage for insureds other than the plan and its participants.

H. SMALLER EMPLOYER (AND SMALLER MULTIEMPLOYER PLAN) CHALLENGES

The Council learned that it critical that plan sponsors ensure that their third-party service providers have strong cybersecurity practices and a robust insurance program to address losses that could adversely affect the plan and its participants. However, in this regard, there is concern

that smaller employers (and also smaller multiemployer benefit plans), with fewer resources, might have a more challenging time screening their third-party partners and getting them:

- to share details on their own cyber insurance coverage
- to demand minimum cyber coverages, and/or
- otherwise to demonstrate strong cyber controls.

That said, administration of small plans, like large plans, is largely outsourced, and accordingly, the cyber risk resides more significantly at the service provider. With respect to data at the employer, based on the witness testimony, the risk of a cyber incident occurring at a small employer, or a small multiemployer plan, might be lower than the risk of a cyber incident involving a large employer, or large multiemployer plan, if for no other reason than the limited amount of valuable data and assets that could be acquired makes smaller entities relatively less attractive targets.

Additionally, "small employer" insurance products are likely less customizable and may provide less coverage per premium dollar. This potential difference would likely need to be explored further to determine its implications, if any. There might be differences in insurers available to the smaller entities (including smaller multiemployer plans), and those entities might have a more difficult time identifying potential insurance carriers. However, it is the Council's understanding that many carriers cover all market segments while others may specialize in the larger or smaller end of the market.

I. DISTINCTION BETWEEN MULTIEMPLOYER PLANS AND SINGLE-EMPLOYER PLANS IN TERMS OF LIKELIHOOD OF COVERAGE

The Council heard testimony suggesting that most multiemployer plans (or at least the largest such plans) typically maintain cyber insurance whereas the adoption of such policies by single-employer plans is less common. It should be noted that the Council did not receive hard data on this issue, and so this should be understood as simply the Council's impression.

If true, there could be a simple reason for this. For multiemployer plans, the only assets backstopping a potential benefit plan loss (and the only entity who might reasonably be expected to step in to address losses or disruptions caused by a cyber incident) is the plan itself or the plan

sponsor. However, for a multiemployer plan, the plan sponsor is the board of trustees--a group of individuals with likely modest resources (compared to potential cyber-related losses)--and not, as in the context of a single-employer plan, a corporate entity with its own assets and resources. Without the backstop of an entity with resources to address a cyber event, it seems natural that boards of trustees of multiemployer plans would reasonably conclude that purchasing cyber insurance for the plan makes sense, whereas the need for doing so in the context of a single-employer plan might seem less critical.

J. DISCUSSION REGARDING EDUCATION AND GUIDANCE

The Council recognizes the Department's important educational mission with respect to the public (and to the regulated community). Given the importance of this topic—which will only increase—education and publicity makes sense. At the same time, a number of Council members expressed concern regarding the potential for any "sub-regulatory guidance" (tip sheets and best practices) as having the effect of regulations. Other Council members, though, disagreed with this concern.

V. BASIS FOR RECOMMENDATIONS

Recommendation 1

As noted, the Council's first recommendation is that the Department continue to study the issue of cybersecurity insurance and employee benefit plans. This study should not be limited to "cyber insurance" *per se* but should include other forms of loss risk-mitigation strategies including but not limited to:

- Cybersecurity insurance
- Fidelity/crime coverage
- Fiduciary liability coverage
- Third-party (service-provider) contractual obligations (including indemnification) and insurance.

The basis for this recommendation is as follows:

There are many considerations relevant to a better understanding of cybersecurity insurance and its relation to employee benefit plans. Issues to be further explored include, but are not limited to:

- The evolving landscape of responsive insurance coverages
- Whether the plan is a retirement plan or a welfare plan
- Whether the plan would be responsible for financial harm, or some other party
- The probability of a cybersecurity incident based on the size of the organization or plan, and
- The type of claims filed in connection with the cybersecurity incident.

All of the above make it apparent that additional study is needed before any guidance on this topic is issued.

Recommendation 2

The Council's second recommendation is that, following further study, the Department should consider developing education for employee benefit plan fiduciaries, and others, concerning the types of insurance coverages that are available to protect against losses resulting from cyber incidents. Areas of education might include:

- The primary types of cyber-threats faced by employee benefit plans
- The types of losses typically covered by "cyber-insurance" policies vs. other types of policies (such as fidelity/crime policies and fiduciary insurance policies)
- Other aspects of insurance policies--such as exclusions, the identity of the "named insured," deductibles, and coverage limits
- The role that a benefit plan's cybersecurity policies, practices, and controls might play in the application and/or renewal process for cyber-related insurance coverage.

The basis for this recommendation was the Council's perception that:

- Insurance issues might not be well understood by plan fiduciaries
- This is a complex, evolving area

- The Department's current knowledge, coupled with additional learning from the Council, provides an opportunity to share relevant information in a timely manner with a large audience.

\end