Advisory Council on Employee Welfare and Pension Benefit Plans

Report to the Honorable Thomas E. Perez,
United States Secretary of Labor

Cybersecurity Considerations for Benefit Plans

November 2016

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 ERISA to advise the Secretary of Labor on matters related to welfare and pension benefit plans. This report examines Cybersecurity Considerations for Benefit Plans.

The contents of this report do not represent the position of the Department of Labor.

LIST OF COUNCIL MEMBERS

Mark E. Schmidtke, Council Chair

Jennifer K. Tretheway, Council Vice Chair

Deborah A. Tully, Issue Chair

Deborah L. Smith, Issue Vice Chair

Jeffrey G. Stein, Issue Vice Chair

Stacy R. Scapino, Drafting Team Member

Christine S. Hwang, Drafting Team Member

Tazewell V. Hurst III, Drafting Team Member

Elizabeth Y. Leight, Drafting Team Member

Rennie Worsfold

Kevin T. Hanney

Dennis F. Mahoney

Beth A. Almeida

Patricia Haverland

Cynthia J. Levering

ABSTRACT

The 2016 ERISA Advisory Council examined cybersecurity considerations as they relate to pension and welfare benefit plans. The 2016 Council focused on information that would be useful to plan sponsors, fiduciaries and their service providers in evaluating and developing a cybersecurity program for their benefit plans. The work of the 2016 Council expanded on the findings of the 2011 Council, which examined privacy and security issues effecting employee benefit plans. The 2016 Council has focused on outlining cyber risk management strategies that can be scaled based on sponsor and plan size, type and resources. The 2016 Council has also created materials for plan sponsors and fiduciaries to utilize when developing a cybersecurity strategy and program.

Based upon testimony received during two days of hearings supplemented by submissions of written material from interested stakeholders, the 2016 ERISA Advisory Council formulated and drafted a document – "Employee Benefit Plans: Considerations for Navigating Cybersecurity Risks" and this report. The 2016 Council's objective in producing these documents is to provide relevant information to, and raise awareness with, plan sponsors, fiduciaries and service providers regarding the development of cybersecurity risk management programs for benefit plans.

ACKNOWLEDGEMENTS

The Council recognizes the following individuals and organizations who contributed greatly to the Council's deliberations and final report. Notwithstanding their contributions, any errors in the report rest with the Council alone.

Allen Brill	Kroll Cyber Security
Hervia Ingram	Xtreme Solutions, Inc.
Scott Esposito	PricewaterhouseCoopers
James Fox	PricewaterhouseCoopers
Kevin Schlotman	Benovation
Matthew McCabe	Marsh
Kathy Bakich	Segal Consulting
Mercedes Tunstall	Pillsbury Winthrop Shaw Pittman
Jonathan Falk	Siemens
Tim Rouse	SPARK
Tim Oxborough-Powell	Tata Consultancy Services
Becky McQuilling	Google
Kevin Stadmeyer	Google
Dan Nutkis	HITRUST
Ben Taylor	Callan Associates, on behalf of SPARK
Eric Nordman	NAIC
Doug Peterson	Empower Retirement, on behalf of SPARK
Brian Finch	Pillsbury Winthrop Shaw Pittman
Brian Smith	Segal Select Insurance Services, Inc.
Eugene Eychis	Beazley Group
Matt Prevost	Chubb
Larry Good	Employee Benefits Security Administration
Thomas Norris	Employee Benefits Security Administration

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY…….. 1

II. RECOMMENDATIONS…….. 2

III. BACKGROUND…….. 3
- A. 2011 Council Report
- B. Benefit plan cyber risk environment

IV. EXISTING CYBERSECURITY FRAMEWORKS……. 8
- A. NIST
- B. SAFETY Act
- C. Industry based initiatives and developments

V. EMPLOYEE BENEFIT PLANS: CONSIDERATIONS FOR NAVIGATING CYBERSECURITY RISKS……. 15
- A. Objectives
- B. Establishing a strategy
- C. Contracting with service providers
- D. Insurance considerations

VI. COMMON CYBERSECURITY TERMINOLOGY AND USEFUL LINKS.. 22

VII. CONCLUDING OBSERVATIONS……. 23

VIII. APPENDIX……... 24

I. EXECUTIVE SUMMARY

The 2016 ERISA Advisory Council ("2016 Council") examined cybersecurity considerations as they relate to pension and welfare benefit plans. The 2016 Council focused on providing useful information to plan sponsors, fiduciaries and service providers in evaluating and developing a cybersecurity risk management program for benefit plans. The 2016 Council's work built upon the 2011 ERISA Advisory Council's ("2011 Council") prior work, which examined privacy and security issues affecting employee benefit plans. The 2011 Council report included, among other things, recommendations with respect to guidance and educational materials for plan sponsors, plan participants and vendors. In addition, the 2015 ERISA Advisory Council ("the 2015 Council") devoted some time to the topic of cybersecurity. Leveraging the previous Councils' work, the 2016 Council focused specifically on outlining elements of cyber risk management strategies that can be scaled, or adjusted, based on sponsor and plan size, type, resources and operational complexity.

The 2016 Council observed that while cybersecurity is a focus area for organizations with regard to ongoing business activities, benefit plans often fall outside the scope of cybersecurity planning. Benefit plans often maintain and share sensitive employee data and asset information across multiple unrelated entities as a part of the benefit plan administration process. This data and asset information should be specifically considered when implementing cybersecurity risk management measures. Because benefit plans are regulated by the Employee Retirement Income Security Act of 1974 ("ERISA"), anyone who interacts with the plan should be particularly aware of the impact that breaches have on participants and beneficiaries and the associated rights and duties of plan fiduciaries and service providers arising under ERISA.

Plan sponsors and fiduciaries should consider cybersecurity in safeguarding benefit plan data and assets, as well as when making decisions to select or retain a service provider. The 2016 Council believes that the Department of Labor ("Department") should raise awareness about cybersecurity risks and the key elements for developing a cybersecurity strategy specifically focused on benefit plans. The 2016 Council is providing suggested materials for plan sponsors, fiduciaries and service providers to utilize when developing a cybersecurity strategy and program in the form of the document included in the appendix of this report titled "Employee Benefit Plans: Considerations for Navigating Cybersecurity Risks."

II. RECOMMENDATIONS

Based upon witness testimony and Council research, the 2016 Council recommends that the Department:

1. Make this report and its appendices available via the Department's website as soon as administratively feasible to provide plan sponsors, fiduciaries and service providers with information on developing and maintaining a robust cyber risk management program for benefit plans.

2. Provide information to the employee benefit plan community of plan sponsors, fiduciaries and service providers to educate them on cybersecurity risks and potential approaches for managing these risks. The 2016 Council has drafted a sample document titled "Employee Benefit Plans: Considerations for Managing Cybersecurity Risks" ("the Cybersecurity Considerations Document") for the Department as an illustration.

III. BACKGROUND

A. 2011 COUNCIL REPORT

The 2011 Council studied "Privacy and Security Issues Affecting Employee Benefit Plans." The 2011 Council focused on the privacy and security of benefit data and personal information in light of the dramatic changes in technology and its use in employee benefit plan management. The 2011 Council examined issues and concerns about potential breaches of the technological systems used in the employee benefit industry, the misuse of benefit data and personal information, and the impact on plan sponsors, service providers, and participants and beneficiaries.

The 2016 Council's analysis builds on this prior work. Although cybersecurity and threats have continued to evolve, the 2011 Council noted several points that remain relevant for the current Council.

1. Administrative service providers are essential in any efforts to protect personally identifiable information ("PII").
2. Everyone who comes in contact with PII has a role to play in protecting data.
3. Many organizations, such as financial services organizations, are subject to extensive regulation or other legal requirements that result in multi-faceted efforts to protect their customers' PII.
4. Because there are many different users and service providers in the benefit administration area, the regulatory system and data security approaches might have weak, and possibly, unprotected areas.
5. Large employers and organizations are more likely to have the resources to obtain guidance on the management of PII in benefit plans and to increase their due diligence efforts in this area.
6. Small and mid-sized employers and organizations are less likely to have the resources to obtain this level of support and guidance.

Many of the environmental challenges noted in the 2011 Council report still exist. For example, the 2011 Council noted that Third Party Administrators ("TPAs") and other service providers did not have a comprehensive and consistent regulatory framework to guide their data security programs. This deficiency continues to exist. Additionally, the legal environment around data security continues to focus on protecting consumer information held at financial institutions and does not directly address benefit plans, outside of the Health Insurance Portability and Accountability Act ("HIPAA"). Federal regulations and state privacy laws remain inconsistent and, in some cases, conflict.

The 2011 Council identified four major areas for effective practices and policies:

1. Data management.
2. Technology management.
3. Service provider management.
4. People issues / Training.

These areas continue to represent the primary focal points for plan sponsors and various providers involved in managing and administering benefit plans and their data.

The 2011 Council recommended that the Department: (i) provide guidance on the obligation of plan fiduciaries to secure and keep private participants' and beneficiaries' PII; and (ii) develop educational materials and outreach efforts for plan sponsors, participants and beneficiaries to address PII privacy and security issues.

The 2015 Council devoted some time to cybersecurity issues. After an initial review and witness testimony in May 2015 hearings, the 2015 Council determined that the topic deserved more attention and should be a future topic for more in-depth review.

The 2016 Council has focused on developing educational materials for plan sponsors, fiduciaries and their vendors; highlighting the need to focus on benefit plan cybersecurity in addition to enterprise cybersecurity. The 2016 Council is aware that ambiguities and potential issues remain with regard to whether cybersecurity is a fiduciary responsibility as well as whether state cyber laws are preempted by ERISA; however, the 2016 Council has determined that providing guidance on these topics is beyond the scope of the 2016 Council's study.

B. BENEFIT PLAN CYBER RISK ENVIRONMENT

1. Challenges

In the five years since the 2011 Council report, cybersecurity has become increasingly important to a wide range of daily operations and service delivery, including benefit plans. Cybersecurity events have demonstrated that risks can emerge from peripheral functions and work their way to sensitive data and/or mission critical functions. Consequently, non-core technologies and functions should be considered as part of a holistic cybersecurity strategy and program.

Alan Brill of Kroll provided testimony to the 2016 Council (Mr. Brill also testified before the 2011 Council), indicating:

> [C]yber risks faced by both employers and services organizations are more severe and significant than in the past, and certainly more important than when I last had the opportunity to brief this Council [in 2011].

Mr. Brill further stated:

> Cybersecurity has become a matter of central importance to every organization that is part of the eco-structure of organizations that create, use and store personal and financial information for participants….

Benefit plan management and administration largely depends on outside service providers, such as plan administrators, actuaries, auditors, trustees, insurers and consultants. These providers collect and maintain sensitive employee data to meet their responsibilities and deliver services. This data may include social security numbers, addresses, dates of birth, account balance information, beneficiary information and bank account details. In addition, plan administrators

and other service providers may maintain systems that allow employees to initiate transactions online, such as obtaining loans and/or account withdrawals. Consequently, a cybersecurity breach within a benefit plan could result in employees' identities, personal information or plan assets being compromised.

Most employee benefit plans rely on a network model to manage daily activities and support their participants. Smaller plans and sponsors have significant dependence on third parties. This approach means that employee benefit plans typically use and share data with several independent third parties. Often with benefit plans, the exchange of data involves sensitive employee, beneficiary and employer information. The most significant cybersecurity breaches are increasingly coming from third party vendors and even vendors not directly related to the services being provided (e.g. Goodwill, Home Depot, Lowe's, and Target). For example, in the Target breach, an outside vendor was hacked and its credentials were used to enter Target's internal systems and retrieve customer data. Third parties can be the weakest cybersecurity link.

The 2016 Council heard testimony from James Fox of PricewaterhouseCoopers, who recommended that plan sponsors:

> [F]ocus on the data. Focus on what could be done with this information, and then decide who has it, what's the minimum amount they have to have to get the job done. And for the ones [service providers] that absolutely have to have lots of different information, I recommend you put a second level of evaluation on them because you are giving them more trust. And if you do those things, you have a set of objectives you can measure yourself against…

The 2016 Council also heard witnesses report on the substantial threats in the environment in which benefit plans operate. Examples of cyber threats that are common today include:

- *Ransomware* where criminals encrypt and seize an entire hard drive and will only release it for a high ransom.
- *Phishing* where fraudulent emails are sent with the objective of enticing the user to interact and inadvertently provide an avenue for a cyber-criminal to infiltrate a computer network.
- *Wire transfer email fraud* where cyber criminals pretend to be senior executives asking employees to transfer funds.
- *Malware via external devices* where intrusive and harmful software is stored on an external drive that is inserted into and executed on a network computer.

Individual data and information, as well as the potential to access assets, are valuable, so cybersecurity threats will continue to exist and evolve. Consequently, any cybersecurity discussion is not only about what and how data is held, but also different ways to access the data, how the data is transferred, where the data is transferred and whether unrelated parties can disrupt the data flow. In particular, the use of mobile devices to access accounts and initiate transactions has grown significantly. Cloud facilities have changed how companies receive, hold and store data, as well as run systems. Many companies rely solely on cloud-based services for their technology operations. Consequently, encryption has become an essential component of an

organization's cybersecurity strategy, particularly where data is transferred among multiple parties or companies move data to and from the cloud. According to Kevin Stadmeyer from Google:

> The important thing to keep in mind…is how does your data get to that offsite center, what does it look like once it's in that offsite center, and how do you get it out of there? …There's no security issue inherent with storing the data in one location or another location. It's a question of physical access of that location and how the data moves around as it goes between those locations.

Rebecca McQuilling, also from Google, stated:

> When we talk about encryption we're really talking about multiple levels… the means by which it [data] moves, is encrypted…. Then you also have that second layer where the data itself is …encrypted so that even if someone should be able to see your data, they couldn't read the true form of the data… when you have those remote sites and you're moving data back and forth it's important…to use both forms of encryption. There's no such thing as a private link. People refer to … a private link between …data centers. That's a fallacy that doesn't exist.

Overall, encryption allows financial institutions to route transactions, health care providers to share medical information, and consumers to transact online for goods and services. The benefits of encryption are clear but there are many standards for data encryption and often organizations fail to incorporate encryption into their cybersecurity strategy. Access, facilities and functionality have changed significantly since the 2011 Council report and represent a significant challenge in managing cybersecurity around benefit plans.

Plan sponsors and fiduciaries may be challenged by limited resources, technical expertise and the lack of clear standards. The 2016 Council heard from several witnesses who noted the complexity and technical specificity that surrounds the topic of cybersecurity and stressed the value of seeking expert advice when navigating the area. Individuals responsible for benefit plan management rarely have expertise in cybersecurity, yet benefit plans contain significant sensitive individual data that could be prone to a cyber breach. Consequently, plan sponsors and fiduciaries may want to carefully consider whether to consult with a cybersecurity expert when developing a cybersecurity strategy for their plans. Many witnesses stated that firms that are small or do not have the resources or capacity to develop a customized, robust cybersecurity risk management strategy may opt to use cloud-based resources to offload cybersecurity burdens onto the cloud provider. Alternatively, cyber insurance or other tools may be useful in designing a cost effective program.

Several witnesses commented that there is no such thing as a cyber risk elimination strategy. The 2016 Council believes that plan sponsors and providers should approach cyber risk management strategies with the understanding that a good program will not eliminate risks. Hervia Ingram of Xtreme Solutions, Inc. noted in his written comments that:

> Many will venture into developing and implementing a cyber risk strategy with the goal of risk mitigation. Instead, the focus should be on risk management, instead of risk mitigation; no matter what type of organization.

Given the cyber threat environment, many benefit plan service providers have developed significant cybersecurity programs to protect themselves and their clients; however, many plan sponsors and fiduciaries remain challenged in obtaining this information or developing a sufficient understanding of their providers' programs. According to the Society of Professional Asset-Managers and Recordkeepers ("SPARK"),[1] plan administrators spend significant time and resources responding to cybersecurity queries from their clients and prospects. Additionally, many vendors believe that revealing sensitive information about their cybersecurity programs puts them further at risk of a cyber breach by revealing potentially confidential risk management strategies and tactics. Consequently, SPARK is studying ways to provide plan sponsors and fiduciaries with sufficient assurances about cybersecurity while also preserving time and resources for all parties. (See Industry Initiatives in Section IV(C) below for greater detail.)

2. Legal environment

As noted in the 2011 Council report, there continues to be no comprehensive federal law governing cybersecurity for benefit plan service providers. There are laws that govern the financial industry's use of financial information, such as the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and the Fair and Accurate Credit Transactions Act. These laws, however, do not apply directly to benefit plans or the sensitive individual data held in conjunction with those plans.

Benefit plans typically maintain data elements that can make up PII and Protected Health Information ("PHI").

The Office of Management and Budget ("OMB") defines PII as:

> [I]nformation which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[2]

PHI is akin to Individually Identifiable Health Information, defined under HIPAA[3] as:

> [I]nformation that is a subset of health information, including demographic information collected from an individual, and:

---

[1] SPARK is a member driven, non-profit organization for the defined contribution retirement industry.

[2] Office of Management and Budget Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."

[3] Section 1171 of Part C of Subtitle F of Public Law 104-191 (August 21, 1996: Health Insurance Portability and Accountability Act of 1996: Administrative Simplification and 45 CFR (Code of Federal Regulations) 160.103.

> (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Most states have laws that address the protection of PII and PHI in some form but, like federal laws, these laws generally apply to health plans, and not to other welfare benefit plans or to pension plans.

Existing legislation provides some guidance for how sponsors might approach the problem. Under HIPAA, health plan sponsors already manage their plans in accordance with data privacy and security rules. Health plan sponsors enter into business associate agreements with TPAs and other service providers. Business associate agreements establish each party's obligations under HIPAA in connection with the plan's HIPAA-protected information.

In addition to HIPAA, health plan sponsors might also reference state data breach notification laws and cyber liability insurance in business associate agreements. Several witnesses referenced these business associate agreements as examples of a potential approach that could be used in the broader benefit plan universe. Business associate agreements, HIPAA and the myriad of state laws provide a starting framework for guiding other types of benefit plans, their sponsors and fiduciaries in considering how to approach cybersecurity issues and handling PII.[4]

IV. EXISTING CYBERSECURITY FRAMEWORKS

As a result of the continually evolving and expanding cybersecurity threat environment, governmental and private cybersecurity frameworks have been, and continue to be, developed to help organizations evaluate and navigate cyber risk. Several witnesses referenced existing cybersecurity frameworks that could provide the foundation for cybersecurity strategies for benefit plans.

A. NIST

President Obama issued Executive Order 13636 on February 12, 2013, "Improving Critical Infrastructure Cybersecurity," which established U.S. policy to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." The Cybersecurity Framework was developed and published one year later on February 12, 2014 through collaboration of the government via the National Institute of Standards and Technology ("NIST") and private sector

[4] Christensen, Lisa; "Cybersecurity and Employee Benefit Plan Fiduciary Duties: Going Beyond HIPAA" April 26, 2016 posted in Cybersecurity, Employee Benefits published by The Labor & Employment Attorneys of Bond, Schoeneck and King.

industry stakeholders, to set voluntary standards and best practices for managing cybersecurity risks to critical infrastructure services. "Critical infrastructure" is defined in the Executive Order as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, nation public health or safety, or any combination of those matters."

The Framework is a voluntary guideline, targeting organizations that own or operate critical infrastructure; however, the standards, guidelines and practices set out in the Framework are not meant to be a one-size fits all, nor are they industry or even country specific. The Framework is intended to complement and not replace an organization's existing risk management processes and for organizations that do not have cybersecurity programs, the Framework is to be used as a reference. It provides a mechanism for organizations to assess and determine their cybersecurity capacity, and assists them in planning for and improving cybersecurity programs.

The Framework has three parts. The first part is the "core," which outlines five concurrent and continuous functions that should occur to form an effective cybersecurity risk management program. The functions are:

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

Together, these functions provide a strategic view of an organization's cybersecurity risk management lifecycle. For each function, the Framework then provides categories into which a function can be organized and subcategories of specific actions. For each level, the Framework also provides references to resources to support designing a risk management framework. *The 2016 Council utilized the concepts contained in this first part of the NIST framework to develop its document in Appendix A.*

The second part of the Framework focuses on implementation of a risk management program and assists organizations in understanding where they are with regard to implementation. The Framework defines four implementation categories:

1. Partial
2. Risk informed
3. Repeatable
4. Adaptive

Users of the NIST framework should evaluate where they are on the spectrum of implementation and determine whether and how to move along that spectrum. For example, organizations that are partially prepared are encouraged to be at least risk informed; however, entities should use the level of threat and cost effectiveness of implementing a risk management program to determine whether to move beyond being risk informed.

The third part of the Framework focuses on developing an organizational profile using the functions, categories and subcategories outlined in the Framework core along with business drivers and a risk assessment to determine which are most important. A firm can build a current profile, which can then be used to prioritize and measure progress toward a target profile. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

The Framework promotes the following basic process for establishing a cybersecurity risk management program. This process is substantially the same for most risk management programs; however, along with the subject matter guidance detailed in the Framework an entity should be able to establish a suitable program.

1. Prioritize and scope.
2. Orient the scope within the entity.
3. Develop a current profile.
4. Conduct a risk assessment.
5. Identify a target profile.
6. Analyze gaps.
7. Implement an action plan.

The Executive Order that established a cybersecurity task force specifically required the resulting Framework to address data privacy and civil liberty implications. The Framework advocates that organizations consider circumstances in which specific measures are appropriate, such as: minimizing data collection, disclosing and retaining material personal information, the need for individual consent, and redress for adverse impacts. The Framework has specific suggestions and management programs for protecting data privacy and civil liberties.

The 2016 Council encourages plan sponsors, fiduciaries and service providers using the NIST framework to reference NIST's website for further detail and useful materials to help them navigate the multiple components of the framework. Appendix C of this report includes useful links including the NIST website for reference.

B. SAFETY ACT

Congress enacted the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 ("SAFETY Act") to encourage the use of anti-terrorism products, services and technologies in civilian settings. The SAFETY Act specifically provides risk management protections to firms that develop, sell or deploy these technologies, as well as contractors, subcontractors and consumers downstream. The SAFETY Act protections include liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where Qualified Anti-Terrorism Technologies ("QATTs") have been deployed.

The Act gives the Secretary of the Department of Homeland Security ("DHS") broad discretion to designate a technology as a QATT and may consider, as well as give relative weight to, some or all of the following non-exclusive list of factors:

1. Prior U.S. Government use or demonstrated substantial utility and effectiveness;
2. Availability of the technology for immediate deployment;
3. The potential liability of the Seller;
4. The likelihood that the technology will not be deployed unless the SAFETY Act protections are conferred;
5. The risk to the public if the technology is not deployed;
6. Evaluation of scientific studies; and
7. The effectiveness of the technology in defending against acts of terrorism.

The range of SAFETY Act protections conferred when a technology receives a Designation as a QATT, include: capping liability at an approved level of insurance, exclusive federal court jurisdiction for claims against sellers arising from an act of terrorism, limits on non-economic liability and exemption from punitive damages.

Technologies that the Secretary of the DHS deems as Certified give even greater protections. Sellers of QATTs with a Certification have additional immunity conferred by a rebuttable presumption of the government contractor defense. This defense can only be rebutted by a showing of fraud or willful misconduct by the seller in submitting information to DHS.

While the definition of an "act of terrorism" – which triggers SAFETY Act protections – may not have originally contemplated financial harm arising from a cybersecurity attack within a benefit plan, an argument can be made that where a certain technology (product or service) is intended to protect critical infrastructure, and that technology has received a SAFETY Act "Designation" or "Certification," these protections may be applicable in the benefit plan context. Brian E. Finch of Pillsbury, Winthrop, Shaw, Pittman, LLP testified regarding the potential ways that SAFETY Act awards can be useful for plan sponsors. To date, DHS has awarded over eight hundred Designations and Certifications and while most have been related to products and services, DHS has increasingly been vetting processes and procedures in the cybersecurity arena.

Benefit plan sponsors, fiduciaries and third party service providers may want to consider whether SAFETY Act certifications could fit into their overall cybersecurity risk management strategy. Mr. Finch suggested that plan sponsors can take advantage of the Act's liability protections by retaining vendors that have or use SAFETY Act approved processes or procedures. Doing so may help protect plans from third-party liability for losses resulting from cyber-attacks and can potentially provide further assurance around a third party's cybersecurity processes and controls.

The 2016 Council also received testimony from other witnesses indicating the SAFETY Act may not necessarily be the right option for all plan sponsors. Brian Smith of Segal Select Services, Inc. noted that the cost of compliance with the SAFETY Act standards may outweigh the coverage that the SAFETY Act provides relative to the cost of cyber insurance coverage and therefore may not be the best use of plan assets. The 2016 Council concludes that each plan sponsor should carefully evaluate what resources and tools to utilize in developing a cybersecurity risk management strategy in a way that fits its specific needs. While compliance with the SAFETY Act may be the right fit for one plan sponsor, utilizing plan assets to purchase insurance may be a better alternative for another plan sponsor.

C. INDUSTRY BASED INITIATIVES AND DEVELOPMENTS

1. SPARK

Concurrent with the 2016 Council's work, several industry organizations also are focusing on cybersecurity in an attempt to help plan sponsors and service providers navigate the continually evolving cybersecurity environment. These groups aim to develop consistent guidelines to which vendors can refer as standards for developing cyber risk management programs and communicating those programs to their clients.

The 2016 Council heard testimony from Tim Rouse, Ben Taylor and Doug Peterson on behalf of the SPARK Institute. SPARK is in the process of establishing uniform data management standards for the defined contribution retirement plan market. This initiative has been driven by the fact that defined contribution providers are getting an increasing number of inquiries from clients and intermediaries, each with numerous and varying questions regarding cybersecurity arrangements, which in turn is increasingly taking time and resources away from day-to-day operations. In addition, defined contribution providers expressed concern that complete transparency to outside parties regarding cybersecurity practices could put security arrangements in jeopardy and increase the likelihood of becoming cyber threat targets. As an industry group, the membership recommended that SPARK develop an industry standard against which the members could be compared to give their clients reassurance and communicate that the administrators have met a specific benchmark.

SPARK has established a Data Security Oversight Board ("DSOB") to oversee program development and implementation. The DSOB includes representatives from plan administrators, consultants, SPARK staff and DHS. SPARK will be reaching out to cybersecurity experts and providers as it moves the project forward.

SPARK has identified four core principles for designing a certification framework:

1. The assurance certification is not a guarantee against a breach.
2. The assessment must be dynamic with at least an annual validation.
3. The certification should incorporate available independent attestations and audits to prevent parties from redoing something that has already been done.
4. The certification should help providers in obtaining cyber insurance and ultimately reduce the premiums.

SPARK proposed six steps to developing the certification framework:

1. Establish the DSOB (complete).
2. Expand DSOB membership (complete).
3. Write a mission statement (complete).
4. Draft RFP questions for the providers to complete regarding cybersecurity programs (in process).

5. Consult with experts on the efficacy of the questions and adequacy of responses, as well as the overall approach to certification. (Not started).
6. Define standard certification criteria and assurance standards (Not started).

As of this report, SPARK's cybersecurity certification initiatives are still a work in progress; however, its efforts may be useful for plan sponsors and service providers in the future. We encourage the Department, plan sponsors, fiduciaries and service providers to continue to monitor SPARK's efforts.

2. Health Information Trust Alliance ("HITRUST")

HITRUST was founded in 2007 as a not-for-profit consortium to represent various providers in the healthcare industry, such as pharmacies, pharmacy benefit managers and various manufacturers with regard to cybersecurity and raise the level of security within the industry. HITRUST developed a Common Security Framework ("CSF"), tools and cyber Risk Management Framework ("RMF"), all of which ultimately formed a foundation for the HITRUST certification program.

The NIST framework outlines best practice procedures and steps for developing a cybersecurity framework with the objective of developing cyber resilience. Consistent with NIST, HITRUST takes a cyber resilience approach. The HITRUST CSF integrates and harmonizes various standards, incorporating different state and federal requirements and best practices. This standardization is not industry specific, so organizations of all sizes across a variety of industries can use the framework as a standard in developing a customized risk management program. HITRUST updates the CSF every year to remain relevant.

The CSF in combination with the HITRUST Assurance program comprises the RMF. The HITRUST Assurance program provides a mechanism for accurate and consistent cybersecurity program evaluation and reporting. The CSF and Assurance program focus on data security, integrity and privacy. HITRUST RMF enables organizations to identify and measure their risks and establish appropriate controls aligned to the type and size of the risks. From a reporting perspective, the HITRUST framework creates a common language for communicating what controls should be in place and are applicable to a particular organization.

The American Institute of Certified Public Accountants ("AICPA") recognizes the HITRUST CSF as acceptable criteria and established guidance for SOC 2 reporting, which is discussed in more detail below, because the guidance provides clarity around the risks and appropriate controls. Because HITRUST has worked in partnership with the AICPA, SOC 2s using the HITRUST framework result in greater consistency in audit standards across providers/firms and auditors. Consequently, either the HITRUST Certification or a SOC 2 using the HITRUST framework can be used in vendor management programs to verify that the firm has appropriate controls to preserve the core principles of security, integrity and privacy.

HITRUST CSF and RMF are free. HITRUST has other tools that can be used by third party auditors to authenticate and certify that a firm meets the requirements. Many of the tools can be used in industries other than health care. For example, printing companies, banks and insurers

use the tools. The users can select the relevant regulations that are applicable to them and build a custom framework to evaluate the risk management approach.

Adopting a cybersecurity framework and obtaining certification are very different activities. The HITRUST CSF is prescriptive and scalable. Many firms that adopt a CSF then do a self or third-party assessment to understand whether they could get a certification. The assessment generally results in a strategic plan that gets them to a point where they can get certified. Certification can take a year or much longer (e.g., 5 years). During the process, firms can consider their assessment scores category by category. If they fail certification in a particular category, the firm can remediate and reapply for certification. Because the process is thorough and adapts over time, certification may require resources and time to acquire, but stakeholders can place reliance on the credentials.

3. AICPA Initiatives and SOC Reporting

The AICPA has developed, or is in the process of developing, useful tools and resources that can be helpful to plan sponsors when developing a cybersecurity risk management strategy.

When a plan sponsor outsources to service providers[5] many tasks or functions, the plan sponsor is still responsible for establishing effective controls over those outsourced tasks and functions. As such, the AICPA Service Organization Control ("SOC") reports may provide user management with helpful information about the service organization's controls to help them in assessing and addressing the risks associated with an outsourced service. A SOC 1 report is prepared in accordance with the Statement on Standards for Attestation Engagements ("SSAE 16") for reporting on controls relevant to internal control over financial reporting. The SOC 2 report is designed to meet user entity requirements beyond that of a SSAE SOC 1 report. A SOC 2 report addresses risk of IT-enabled systems and privacy programs beyond the controls necessary for financial reporting.

> SOC 1 - Report On Controls At A Service Organization Relevant To User Entities' Internal Control Over Financial Reporting - Specifically intended to meet the needs of the management of user entities and the user entities' auditors, as they evaluate the effect of the controls at the service organization on the user entities' financial statement assertions. There are two types of reports for these engagements: Type 2 - report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period; and Type 1 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

[5] "Service providers" are referred to as "service organizations" in this portion of the Council report to coincide with terminology used by the AICPA.

SOC 2 - Report On Controls At A Service Organization Relevant To Security, Availability, Processing Integrity, Confidentiality Or Privacy - These reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. Similar to SOC 1 engagements there are two types of SOC 2 reports: Type 2, report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and Type 1, report on management's description of a service organization's system and the suitability of the design of controls.

The AICPA Assurance Services Executive Committee has formed the Cybersecurity Working Group ("Working Group") to work in collaboration with the Auditing Standards Board ("ASB") to develop a consistent, profession-wide approach to performing and reporting on attestation engagements related to cybersecurity. The Working Group is designing an examination-level attestation engagement (referred to as a cybersecurity examination) that is intended to meet the needs of a broad range of potential users; developing suitable criteria for the engagement; and developing a cybersecurity attestation guide (referred to as the cybersecurity guide) to provide practitioners with guidance on how to perform and report in the cybersecurity examination engagement. The purpose of a cybersecurity examination engagement is to provide potential users with the cybersecurity information discussed in the preceding paragraph and a CPA's opinion on whether the information is fairly presented, in all material respects, in accordance with suitable criteria. The CPA's opinion enhances the degree of confidence that intended users can place in the information.

V. EMPLOYEE BENEFIT PLANS: CONSIDERATIONS FOR NAVIGATING CYBERSECURITY RISKS

A. OBJECTIVES

Because benefit plans face significant cybersecurity threats and the consequences can be significant, the 2016 Council has developed the attached educational document - the Cybersecurity Considerations Document.

The purpose of the Cybersecurity Considerations Document is to enhance and broaden awareness of cybersecurity issues and risks as they apply to employee benefit plans, and help plan sponsors and fiduciaries better navigate complex cybersecurity issues. Cybersecurity threat prevention is impossible, but an effort must be made to limit the threat, which requires implementing security protocols. Every plan is different and cybersecurity risk management is a process, not a product. One cybersecurity strategy will not meet everyone's needs. Plans sponsors, administrators, fiduciaries and other service providers must determine what is reasonable from a commercial perspective and an ERISA perspective for each plan. The 2016 Council's goal is to be helpful in this process.

The Cybersecurity Considerations Document is not intended to be prescriptive. Rather, the goal is to educate and inform plan sponsors, fiduciaries and their service providers about the

cybersecurity risks that they may face, existing frameworks that can form the foundation of a cybersecurity strategy, questions to ask and processes to consider establishing a cybersecurity strategy. By proposing the Cybersecurity Considerations Document, the 2016 Council is not opining on whether cybersecurity is a fiduciary or settlor function or what should be acceptable fiduciary conduct with respect to cybersecurity for benefit plans. This issue was not within the scope of the 2016 Council's work and we did not hear testimony or receive commentary on the issue sufficient to reach any conclusions or recommendations.

Witnesses emphasized that implementing a cybersecurity risk management strategy cannot be a checklist. Instead the program should be dynamic with attention and commitment at the highest levels, including regular reporting, frequent reviews and process updates. Equally importantly, the 2016 Council was told that protection is not enough, because everyone is likely to be a cyber-attack victim at some point in time.

As a part of the Cybersecurity Considerations Document, the 2016 Council identified important considerations for contracting with service providers. Plan sponsors that rely on service providers and vendors should know whether these business partners have proper procedures in place and monitor the cyber protocols and practices of these providers.

Another area highlighted in witness testimony was cyber insurance and the role cyber insurance can play in benefit plan cybersecurity risk management. As a part of developing a cybersecurity strategy, plan sponsors should evaluate insurance coverage to gain an understanding of what aspects of cyber risks may be covered under existing insurance arrangements, such as fiduciary insurance, and determine whether additional insurance coverage would provide valuable protection to the plan sponsor and participants. The 2016 Council included some considerations that should be addressed in evaluating cyber insurance policies.

B. ESTABLISHING A STRATEGY

1. Understanding the plan's data

To establish a cybersecurity strategy for a benefit plan, one must obtain a thorough understanding of the data and assets being utilized and shared as a part of the plan's administration. Plan sponsors and their service providers should maintain an inventory of data collected. Examples of data elements that may be collected include social security numbers, names, birth dates, hire dates, retirement dates, compensation information, medical record information and asset balances. Many data elements can, in combination, comprise PII and PHI. Plan sponsors and service providers should also understand how data and information related to plan assets or individual balances / transactions are being used.

Given the sensitivity around handling PII and PHI, plan sponsors and their service providers should maintain and share only the data and asset information that is necessary to meet the needs of the plan and no more. Multiple experts who testified before the 2016 Council recommended that plan sponsors go on a "data diet." In his testimony, Mr. Brill of Kroll noted:

> It's time for companies to go on a data diet. Don't collect information unless there is either a documentable legal requirement for the data, or a demonstrable business process in which it is actually used. Similarly, once information is no longer needed (assuming there is no legal or regulatory requirement to keep it) it should be deleted.

Once plan sponsors have identified data and asset information that they must keep and share, plan sponsors should work with internal staff and service providers to understand how and where this data is stored and for how long.

2. Frameworks

All plan sponsors and their service providers should consider a framework upon which to base a cybersecurity risk management strategy. Several experts testifying before the 2016 Council noted the NIST framework, as previously outlined in this report, as a basis for evaluating and developing a robust cybersecurity risk management strategy; however, there are other certifications and audit approaches that can be used in conjunction with or independent from the NIST framework. The 2016 Council utilized the concepts contained in this first part of the NIST framework to develop its document in Appendix A and commends the NIST framework as a potential starting point that plan sponsors, fiduciaries and their service providers look to as they establish their own cybersecurity strategies.

In addition, witnesses referenced the SAFETY Act as a potential tool for the benefit plan community (as discussed earlier in this report), which the 2016 Council also mentions in the Cybersecurity Considerations Document.

3. Process considerations

The 2016 Council heard from multiple witnesses that a cybersecurity risk management strategy must be more than a checklist. The risk management strategy should be dynamic and adaptive to the particular situation of the plan, plan sponsor and its service providers, as well as the continually changing cybersecurity landscape. The 2016 Council does not intend the Cybersecurity Considerations Document to be an all-inclusive guide or checklist for strategy or process development. As a part of the document, the 2016 Council has included items to consider when establishing processes as a part of a cybersecurity strategy. These considerations include:

> *Implementation and Monitoring*
> For a strategy to be successful, someone should have responsibilities for strategy implementation within the plan sponsor organization, the fiduciary body and at third party service providers. Identifying and documenting ownership is critical to success. In addition, a benefit plan cybersecurity strategy and the corresponding processes should reflect changes in the cybersecurity risk environment. Once ownership is identified, the frequency at which the strategy will be reviewed and potentially updated should be established.

Testing and Updating
All entities involved in benefit plan cybersecurity should agree to the frequency and type of testing procedures to be conducted and by whom. Consideration may also be given as to whether outside certifications, such as the HITRUST model or SOC2 reporting for vendors, may help streamline testing procedures. Plan sponsors and service providers also might want to consider consulting a cybersecurity expert to determine the best testing approaches for the plan. A variety of tests can be conducted, including penetration testing where a cyber-attack is simulated with the objective of evaluating the effectiveness of an organization's existing cybersecurity controls.

Reporting
When developing a benefit plan strategy and processes, plan sponsors and fiduciaries should consider the level and frequency of reporting including, if applicable, any established benefits committees, the investment committee or other named fiduciaries as identified within the plan's delegation structure.

Training
A common theme among witnesses was that cybersecurity is a people issue and training is critical. A key component of any cybersecurity strategy should include training staff involved with benefit plans or with direct or indirect access to benefit plan data. This training should occur within the plan sponsor entity and across any service providers who maintain, collect or transmit benefit plan data.

Controlling Access
Given the importance of people in a cybersecurity strategy, plan sponsors and fiduciaries should understand exactly who has direct or indirect access to sensitive data and they should endeavor to limit access to data as much as possible. Several witnesses noted that data access should be granted only to those users who absolutely need the information to perform their jobs. Limiting data access is one of the best ways to reduce cybersecurity risk.

Data Retention and Destruction
In addition to limiting who can access data, plan sponsors and fiduciaries should consider limitations on data sharing, data storage and data retention periods. Many experts recommend limiting data sharing and storage to the minimum necessary to execute a function and satisfy responsibilities to reduce the impact of breaches.

Third Party Risk Management
Plan sponsors should understand service providers' security programs regarding data shared and stored. A first step is to inventory all service providers who have involvement with the plan's participant and/or asset data. The second step is to understand whether those service providers outsource activities to other providers. Once a comprehensive list has been developed, plan sponsors should consider requesting information on each provider's security procedures and how they impact their benefit plans or an industry recognized certification / audit.

4. Customizing a strategy

While cybersecurity is something that every plan sponsor, fiduciary and service provider should consider important, the strategy should be customized to fit each plan's particular needs and circumstances. There is no "one size fits all strategy" and the 2016 Council does not prescribe a particular approach. In addition, the cybersecurity landscape is continually evolving with new and changing threats. Benefit plan cyber risk management strategies need to be customized and must be dynamic. Within the Cybersecurity Considerations Document, the 2016 Council suggests items that plan sponsors may wish to consider as they form a customized strategy, including:

- Resources;
- Strategy integrations within a larger organization (e.g. corporate entity, multi-employer/union environment, etc.);
- Cost;
- Insurance coverage; and
- Industry or governmental certifications (e.g. HITRUST, SPARK, SOC2, SAFETY Act).

Balancing the scope of a cyber risk management strategy against the size and sophistication of the plan sponsor and the plan is important, but smaller entities are as likely to be a target of cyber-crime as larger organizations; so everyone should be prepared.

5. Striking the right balance

ERISA requires that assets be held for the exclusive purpose of providing benefits to participants and their beneficiaries and defraying reasonable expenses of administering the plan. To the extent an ERISA plan bears all or part of the cost of developing and implementing a cybersecurity risk management strategy, the parties involved should approach the strategy within the context of ERISA requirements, which may be different than the approach taken for non-ERISA entities. The 2016 Council believes this is an area that is particularly plan specific and should be evaluated based on size, complexity and overall risk exposure. Plan sponsors may wish to seek the guidance of ERISA legal counsel along with cybersecurity experts when making this evaluation.

6. State law considerations

The 2016 Council heard testimony from witnesses pointing out that the state and federal cyber laws are not comprehensive or consistent. Witnesses noted that, in addition to well-recognized federal laws, such as HIPAA, a myriad of state laws may impact employee benefit plans in the event of a breach. Tina Fletcher of Ullico Casualty Group, in a letter to the 2016 Council, wrote:

> [E]ach state has different laws governing cyber concerns. Unfortunately, many benefit plans cover multiple states or at the least include retirees who moved out of state. . . these state laws may require participant notification, a press release, website disclosure, a toll-free number for affected individuals, credit monitoring services, and fines and penalties.

The question of whether ERISA preempts these state laws is beyond the 2016 Council's study scope. The 2016 Council notes that anyone dealing with employee benefit plan data should have legal counsel advise them on the applicability of such laws in the event of a breach. Tina Fletcher pointed out that cyber insurance may provide such expertise as part of its first party coverage.

C. CONTRACTING WITH SERVICE PROVIDERS

The 2016 Council received testimony and materials from witnesses emphasizing the importance for plan sponsors to vet service providers regarding cyber-risk and to negotiate contractual provisions to mitigate risk to the plan. Recognizing that smaller plans will have less power to negotiate specific contractual provisions, several witnesses provided thoughts on how a plan sponsor or fiduciary can establish a contract that achieves some minimum protections without having to create a fully customized agreement.

Brian Finch of Pillsbury Winthrop Shaw Pittman testified that cybersecurity considerations are critical when plan sponsors negotiate and implement contracts with service providers who have access to plan information or otherwise can impact plan operations. He suggests at least three ways plan sponsors or fiduciaries can ensure higher service provider security levels:

1. Use service providers whose cybersecurity policies and procedures have been vetted and awarded a SAFETY Act Designation or Certification.

2. Clearly define security obligations, setting forth which party is responsible for which security measures and of what exactly those measures will consist. If the service provider has a cybersecurity program, the service provider should identify the officer responsible for oversight and specify how the service provider will share threat information with the plan sponsor and fiduciaries.

3. Include automatic notification and audit obligations. These requirements should be included in contracts with service providers and are "absolutely essential."

In addition, Mr. Finch recommends that plans conduct periodic risk assessments of their service providers' cybersecurity programs and systems.

Mr. Ingram of Xtreme Solutions testified that although many service providers are required to comply with extensive regulations regarding privacy and data security in the ordinary course of their business, plan sponsors should verify that service providers comply with the relevant regulations. He testified further that a solid service provider risk management strategy should include:

1. A contract outlining the business relationship between the plan sponsor and the service provider.

2. Consistent monitoring and audit of service provider performance to ensure that contract stipulations are being met.

3. Guidelines regarding who will have access to what information as part of the service provider agreement.

4. Stipulations to ensure that service providers meet regulatory compliance guidelines for your industry and a method to monitor this compliance.

Mercedes Tunstall of Pillsbury Winthrop Shaw Pittman, LLP recommended that plan sponsors establish due diligence standards for vetting and tiering service providers based on the sensitivity of data being shared. For more sensitive relationships, plan sponsors should consider regularly auditing the vendor or requiring results of a SOC 2 audit or other industry recognized certification. In vetting providers, plan sponsors should make a formal request for information about the service provider's cybersecurity plan; who oversees it; what breaches have occurred; and responses to breaches.

Contractual provisions to consider include identifying sensitive data, how that sensitive data needs to be protected, whether the use is being limited, where the data is located (e.g., in the cloud), the manner by which breaches will be handled, including allocation of liability and risk, and that the service provider must comply with the plan's standards and policies.

Based on the witness testimony, the 2016 Council included in the Considerations Document a list of potential questions to address when plan sponsors are negotiating contracts with service providers.

D. INSURANCE CONSIDERATIONS

Benefit plan sponsors, administrators and service providers likely carry insurance, including fiduciary, commercial, errors and omissions, officers and directors, and other coverage. Anyone dealing with employee benefit plan data and assets should understand whether the insurance covers the consequences of a cyber breach. In response to perceived gaps in coverage, cyber insurance has become a growing part of insurance coverage for plans. The issuance of cyber insurance in the United States is believed to have evolved from the mid to late 1990s, and is still considered to be a developing segment of the insurance industry.

Although considered to be still in its infancy, more than 60 carriers offer stand-alone cyber insurance policies in a market worth over $2 billion in gross written premiums. The market is projected to grow to $75 billion by 2020.

Ms. Fletcher of Ullico explained that traditional liability insurance policies wait for a lawsuit to trigger coverage, which is then considered "third party" coverage. In contrast, the insured may trigger coverage under a cyber liability policy at the first sign of a breach, which is referred to as "first party" insurance. Cyber policies cover both third party liability for losses, lawsuits, and other damages, as well as first party packages that may provide data breach response experts, credit monitoring, public relations and technical assistance for response and recovery.

The 2016 Council heard testimony from several witnesses on the applicability of cyber insurance in the context of benefit plans. As the cyber threat environment has grown and become more complex, the cyber insurance market has also developed as a tool that can be used within a cyber risk management strategy. To that point, Matt McCabe of Marsh testified that:

> [C]yber insurance should not be viewed as a stand-alone solution; it is instead a key component of cyber risk management and which can provide strong market incentives to pursue greater security.

Plan sponsors and fiduciaries should understand what cyber insurance does and does not provide and how it coordinates with other types of insurance coverage, so that they can appropriately consider whether to incorporate cyber insurance into their cyber risk management strategy.

Some components of cyber insurance include:

- Reimbursement of company costs in responding to a cyber threat;
- Payment of fees and damages that a company may pay in response to litigation from a cyber incident; and
- Reimbursement for revenues lost or expenses incurred due to a disruption related to a cyber incident.

In addition, organizations that secure cyber insurance have more tools at their disposal to respond to data breaches through the insurance provider's services because the insurer is also motivated to help the customer avoid or mitigate a cyber breach.

Brian Smith of Segal Select Insurance Services, Inc. testified that small plans that may not have the resources to develop and implement a cybersecurity risk management plan on their own may find it more cost effective to obtain cyber insurance to assess risks, implement a strategy, provide services in the event of a breach and provide liability coverage to third parties.

Similar to other insurance types, one cyber insurance benefit is that the underwriting process forces those who seek insurance to maintain a certain level of cyber risk management process to be eligible. Mr. McCabe noted in his testimony that the Department of Commerce Internet Policy Task Force recently commented that cybersecurity insurance is potentially an "effective market-driven way" of increasing cybersecurity in the private sector.

VI. COMMON CYBERSECURITY TERMINOLOGY AND USEFUL LINKS

Professionals who specialize in benefit plan and ERISA matters do not often overlap into the world of cybersecurity expertise. However, those professionals are likely to be on the front lines of developing a benefit plan cybersecurity strategy. With the help of the witness testimony and additional assistance from Becky McQuilling and Kevin Stadmeyer of Google, the 2016 Council developed the list of common terminology in Appendix B. In addition, the 2016 Council is also including a list of useful websites in Appendix C to assist the Department and the benefit plan community as they navigate the cybersecurity environment.

VII. CONCLUDING OBSERVATIONS

Given the amount of sensitive individual participant data and asset information that is maintained and shared across various parties in the process of administering ERISA plans, the 2016 Council believes it is important to raise awareness about cybersecurity risks and the benefits of developing a prudent cybersecurity risk management strategy specific to benefit plans. The 2016 Council believes that many organizations are already focusing on cybersecurity as it relates to their core businesses. In many cases, this focus has not broadened to the benefit programs offered by these same organizations.

The 2016 Council has prepared this report and sample materials in order to help plan sponsors, fiduciaries and service providers better understand cybersecurity issues and develop a risk management strategy for their plans. The 2016 Council recommends that the Department make these materials available as soon as administratively feasible, given the immediacy of the issue and the evolving nature of cybersecurity risks. While the 2016 Council recognizes that these materials are merely a starting point for developing a cybersecurity risk management strategy for benefit plans, we believe it is critical to take this first step in raising awareness. By making these materials available, the Department can play a role in encouraging plan sponsors, fiduciaries and service providers to prioritize this area as a part of their responsibilities in administering employee pension and welfare benefit plans.

VIII. APPENDIX

A. EMPLOYEE BENEFIT PLANS: CONSIDERATIONS FOR NAVIGATING CYBERSECURITY RISKS

EMPLOYEE BENEFIT PLANS: CONSIDERATIONS FOR MANAGING CYBERSECURITY RISKS

(A RESOURCE FOR PLAN SPONSORS AND SERVICE PROVIDERS)

Cyber threats, including losses due to compromised data and assets, are a daily headline. No individual, organization or industry is immune from cyber threats, including benefit plans and service providers. Common cyber risks to benefit plan participants include identity theft, privacy breaches and theft of assets. The cost of a breach, which includes detecting the extent of the breach, recovering the data and restoring the system, can be substantial.

Cyber threats cannot be eliminated but they can be managed. Cyber experts say that it is not a question of *if* you will have a cyber-attack, rather it is a question of *when*. The next question is *what* you are going to do about it. In addition to taking action to minimize cybersecurity risk, all parties involved in the administration of benefit plans and their data should be prepared to **RESPOND** and **RECOVER** in the case of a cyber event. Cybersecurity is everyone's responsibility. Critical actions and decisions can be anticipated, so they should be considered before an incident occurs, not while it is occurring or after it has occurred. You should be **PREPARED IN ADVANCE**.

Because benefit plans are regulated by the Employee Retirement Income Security Act of 1974 ("ERISA"), anyone who interacts with the plan should be particularly aware of the impact that breaches have on participants and beneficiaries and the associated duties of plan sponsors and service providers arising under ERISA. The operations and administration of benefit plans requires data sharing and asset movements among multiple parties, including third party administrators, custodians, actuaries, auditors, trustees, funds and financial accounts. It is critical for plan sponsors, administrators and service providers to have a strategy to: (1) manage data and assets with the objective of minimizing exposure to the cyber threats that exist now and that will develop in the future, and (2) respond and recover should a breach occur.

CYBERSECURITY RISK MANAGEMENT STRATEGY

Plan sponsors commonly have policies and procedures related to plan investments, conflicts and plan expenses, but may not have a strategy for protecting the data or assets of a benefit plan. They may even have a cybersecurity strategy for their business needs, but not a separate strategy for their benefit plans. Cybersecurity concerns for ERISA plans are unique and differ from business enterprise issues, so they should be specifically considered.

Designing and implementing a cybersecurity risk management strategy may seem overwhelming, but it does not have to be. There is no "one size fits all" answer to cybersecurity. A strategy should align with the plan's complexity and service provider arrangements. This strategy can integrate with other cybersecurity plans and the broader business, or remain entirely separate.

The information that follows is intended to help plan sponsors, administrators, fiduciaries and service providers focus on cybersecurity risks as they apply to benefit plans and formulate a cybersecurity risk management strategy that fits the needs and resources of the benefit plan environment.

ESTABLISHING A STRATEGY

When developing a cybersecurity risk management strategy, plan sponsors should understand the potential risk sources and exposure size. Plan sponsors can start by identifying and prioritizing what data are most critical to protect and the foreseeable threats to that data. Based on those priorities, a strategy to minimize threats and respond to any breaches can be developed.

UNDERSTANDING PLAN DATA

Although there are certainly important cybersecurity considerations relative to managing plan assets, the primary focus of this document is considerations for managing cybersecurity risks associated with plan data.

The availability and use of participant data is critical to benefit plan operations. Understanding how plan data is handled and who is handling it is fundamental to a cybersecurity risk management strategy. To facilitate this understanding, plan sponsors and/or fiduciaries may ask:

What should be protected? Participant data can contain confidential and sensitive personally identifiable information. This data may include social security numbers, names, dates of birth, dates of hire, compensation, medical claims data, personal bank account information and individual asset balance information.

What is the plan type? Plan type affects the kinds of data at risk. For example, defined contribution retirement plans have individual asset balance information, whereas health and welfare plans track healthcare data. Plans may also have personal bank account details.

How is the data classified? Benefit plan data sometimes have special classifications. Specific standards of care apply to different types of data. Examples include Personally Identifiable Information ("PII") and Protected Health Information ("PHI").

Where is the data stored? Multiple parties handle and retain benefit plan data, so understanding where the data is held, how the data is being stored, and the retention period are important security elements for evaluating the total risk exposure.

Who is accessing the data? Benefit plan data is shared across multiple parties and systems as a part of the plan administration process. Involved parties will want to state any security requirements, so data is not shared unless the requirements are met.

How is data accessed? Systems used to administer the plan may be linked to unrelated systems that give hackers unintended access. How benefit plan data is shared, accessed, transmitted and secured across systems provides insight into overall vulnerabilities and total exposure.

Is access properly controlled? Human errors (accidental exposure, lost devices and other non-malicious forms of data loss) represent a significant percentage of data breaches. Therefore, it is important to understand how access is controlled and what manual and automated procedures are in place to manage that access. Encryption is essential and experts agree that data should be encrypted both at rest and as it moves through systems. Automated procedures can be more controlled than manual procedures.

What data is needed? Transmitting and receiving data that is not needed to execute a task or support the plan puts more data at risk than is necessary, increasing risk.

What data needs to be retained? Holding on to data that is not needed increases the potential for the data to be unnecessarily compromised.

What are the threats? Threats are changing all the time, so it is important to have a dynamic system. Hackers steal data and sell it. A ransomware criminal can freeze your system until you pay a ransom fee. Threats can come through email, social media, Internet exposure, or even through unrelated applications.

CYBER SECURITY FRAMEWORKS

Responding to an Executive Order from the President of the United States, the National Institute of Standards and Technology ("NIST") of the U.S. Department of Commerce developed a standard framework for reducing cyber risks to critical infrastructure. Based on the NIST framework, experts agree that some components of a cybersecurity strategy include:

IDENTIFY- Describing a process to identify risks. Once you "understand" your data (see above), you can identify the risks, which might include high probability/low impact or even low probability/high impact risks. It is often said that the weakest links can cause the greatest risk. Experience so far indicates that one of the weakest links is people who are careless or poorly trained or even criminal.

PROTECT- Developing a program to protect data that could be at risk. Based on the particular risks and data, protection might involve technological applications, such as encryption, or human resource practices, such as frequent training and background checks. Fostering a culture of awareness is critical for safeguarding data. It is also important to make certain that as software is updated, security is updated as well.

DETECT- Stating how breaches will be detected. Experts say that breaches will occur, so it is important to note what is being done to detect a breach quickly. Testing, including penetration testing, can be helpful in determining vulnerability.

RESPOND- Showing how your plan can respond. Once a breach occurs, the strategy might state what the response will be to minimize the damage.

RECOVER- Detailing how your plan will recover. Recovery can be the most difficult and expensive part of the program, so recovery should be a critical component of the strategy.

PROCESS CONSIDERATIONS

A cybersecurity risk management strategy is more than a checklist or a technology application- it should be a dynamic and fundamental component of benefit plan administration, including protocols and/or policies for the following elements:

- **Implementation and Monitoring**- Establish who is responsible for designing, documenting, implementing and maintaining the strategy.

- **Testing and Updating**- Determine how often cybersecurity procedures will be tested (including penetration testing), modified, updated and enhanced.
- **Reporting**- Establish the manner in which regular reports will be made to fiduciaries and memorialized in official records.
- **Training**- Provide a plan for regular cyber risk awareness training and reviews.
- **Hiring Practices**- Require background checks and screening of new personnel.
- **Controlling Access** – Identify procedures for determining users who need access to data and restricting data access on an as needed basis.
- **Data Retention and Destruction** - Establish strategy for getting rid of unnecessary data to reduce cyber risks.
- **Third Party Risk Management** - Evaluate service provider security programs, including identifying service providers that access data and stating the conditions under which access is given.

CUSTOMIZING A STRATEGY

Just as all plans are not alike, all cybersecurity risk management strategies are not alike. A commitment of resources and effort is needed to implement a strategy. Even if a plan is small and the plan sponsor has limited resources to develop and maintain a cybersecurity risk management program, the plan may nonetheless be at risk of becoming a target. In addition to leadership commitment, many other functions may be involved with developing a cybersecurity risk management strategy for plans, such as IT, human resources, finance, audit, supply chain/procurement and legal. A first important step may be marshalling those resources.

Here are a few items to consider when customizing a strategy to fit the needs of a benefit plan:

- **Resources**- What resources are internally available to (1) evaluate cyber-risks, (2) to implement a cybersecurity risk management program, and (3) respond and recover should a breach occur? If expertise is not available internally, should external resources be considered? Are there other commercially available resources or tools that can be used?
- **Integration**- When plans are part of a larger organization (for example, corporate entity, controlled group or a multiemployer/union environment), can cybersecurity risk management be integrated with the rest of the administration (if so, are there valid cost-sharing protocols)?
- **Cost**- If the costs of implementing a cybersecurity risk management strategy seem too costly, has the cost of dealing with a breach been considered?
- **Cyber insurance**- Can cyber insurance (see insurance considerations below) provide cost effective access to expertise and resources?
- **Certifications**- Are there industry certifications that you and/or your service providers can explore that can enhance your cybersecurity risk management strategy?
- **New Developments**- Cybersecurity is changing rapidly, so are you keeping current on new tools and resources as they become available?

STRIKING THE RIGHT BALANCE

ERISA requires that assets be held for the exclusive purpose of providing benefits to participants and beneficiaries and defraying reasonable expenses of administering the plan. Based on the type of plan and its resources and to the extent that the plan is bearing some or all of the costs of developing and implementing a cybersecurity risk management program, plan fiduciaries will need to determine the balance of preventive measures relative to the probability of the threat, the loss exposure, and the cost of protective action. This challenge suggests that a scalable, individualized cyber risk assessment strategy is the prudent starting point.

COMPLIANCE WITH STATE LAW

Many states have laws concerning cyber breaches that may include such things as notification rules, reporting requirements or fines and penalties. It may be prudent to consult with benefit plan counsel regarding such compliance requirements and their applicability to ERISA plans.

For more background and information on cybersecurity frameworks, strategies and processes, please see the Advisory Council on Employee Welfare and Pension Benefit Plan's 2016 report *"Cybersecurity Considerations for Benefit Plans."*

CONTRACTING WITH SERVICE PROVIDERS

When contracting with service providers for plan administration (for example, Third Party Administrators, Pharmacy Benefits Managers and Recordkeepers, to name just a few), the service providers will have access to plan data and can be a potential source of a breach. The following questions regarding the protection of data may be helpful when contracting with and evaluating service providers:

1. Does the service provider have a comprehensive and understandable cybersecurity program?
2. What are the elements of the service provider's cybersecurity program?
3. How will the plan(s) data be maintained and protected?
4. Will the data be encrypted at rest, in transit and on devices, and is the encryption automated (rather than manual)?
5. Will the service provider assume liability for breaches?
6. Will the service provider stipulate to permitted uses and restrictions on data use?
7. What are the service provider's protocols for notifying plan management in the case of a breach and are the protocols satisfactory?
8. Will the service provider agree to regular reports and monitoring and what will they include?
9. Does the service provider regularly submit to voluntary external reviews of their controls (such as SOC reports or a similar report or certification)?

Service Organization Control Reports® are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service.
SOC 1® Report – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting These reports, prepared in accordance with *Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization*, are specifically intended to meet the needs of the of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user auditors), in evaluating the effect of the controls at the service organization on the user entities' financial statements. Use of these reports is restricted to the management of the service organization, user entities, and user auditors.

SOC 2® Report— Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy These reports are intended to meet the needs of a broad range of users that need information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

10. What is the level and type of insurance coverage that is available?
11. What is the level of financial and fraud coverage that protects participants from financial damage?
12. If the service provider subcontracts to others, will the service provider insist on protections (as noted above) in its agreement with the subcontractor?
13. What controls does the service provider have in place over physical assets that store sensitive data, including when such assets are retired or replaced (servers, hard drives, mobile devices, etc.)?
14. What are the service provider's hiring and training practices (for example, background checks and screening practices and cyber training of personnel)?

INSURANCE CONSIDERATIONS

Various types of insurance, including fiduciary liability, errors and omissions, commercial, and crime and fraud protection insurance are commonly offered. Many insurance carriers now offer cyber insurance policies to augment existing insurance protection. In addition to third party damage and defense costs, cyber insurance policies may include "first party coverage," which means that an insured does not have to wait for a third party to sue the plan; rather the plan can trigger coverage upon a breach in order to obtain direct risk management and services such as disaster recovery and response assistance. Third party coverage is triggered by a lawsuit and may include such things as forensic investigations, the cost of legal advice or specialists and the settlement of lawsuits, and the cost of remediation, credit monitoring, and credit freezes.

When considering the role that insurance will play in a cybersecurity risk management strategy, determine what is included and excluded from insurance policies already in place should there be a cyber breach, and how the coverage compares to the cyber risk assessment. Be careful when reviewing policy terms related to a cyber breach. Consider if the coverage limits are acceptable and whether policy terms and conditions of coverage can be complied with. Finally, consider the types of protection needed (for example, protection for participants against financial damage in the case of a breach, first party coverage to offer material assistance to respond to and recover from a breach, and coverage of the costs related to required breach notification and the penalties for failure to comply with breach notification laws).

B. COMMON CYBERSECURITY TERMINOLOGY

Clouds/The Cloud: An Internet environment meant to provide expandable resources on demand. By default, Clouds/The Cloud should be assumed to be multi-tenant.

Cyber Gap: The number of information security vulnerabilities in a given system, expressed as the difference between the attacks known to defenders and the attacks known to malicious actors.

Cyber Insurance: Insurance protecting against threats and risks resulting from cyber-attacks. Some insurance may cover first-party losses to organizations for example, data fraud, theft or business interruption. Another type of cyber insurance may cover third-party liability losses, for example, privacy, network security or media liability.

Denial of Service ("DoS") Attack: An attack on a computer/information system where the goal is to prevent access to that service either by permanently or temporarily disabling the system or the access to the system.

Digital Signature: An encrypted string which can only be written by the person who controls the key used to encrypt the string and is tied to a specific document. Most digital signatures allow anyone to verify the validity of the signature and provide for assurance of the integrity of the document.

Distributed Denial of Service ("DDoS") attack. A denial of service attack undertaken by multiple locations, systems or entities where the combined activity generated by the attackers overwhelms the target system via (usually) brute force.

Dark Net / Dark Web: Content on the Internet that is neither indexed by traditional search engines nor accessible to those not running specific software, and with authorization to access that content. It is often encrypted and usually uses anonymization to hide the identity of site operators. This content is often associated with criminal activities, although the dark web can be used for any purpose.

Encryption: Encryption is the process of converting data to an unrecognizable form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.

Least Privilege: The principle of least privilege is a foundation of information security and states that a secure system should permit access to the least number of people needed to function. Access should be granted on a "need to know" basis.

Malware: Software meant to perform a malicious action such as encrypting a hard drive and providing the password for a ransom, deleting files, or stealing information for financial gain.

National Institutes of Standards and Technologies ("NIST"): A U.S. governmental organization that has published a cybersecurity framework to set voluntary standards and best practices for managing cybersecurity risks to critical infrastructure services.

Network Scan: A security audit which is limited to the network level, very commonly performed against external networks, network scans should be considered a baseline level of security but is not sufficient to guarantee the security of an environment.

Penetration Test: A security testing activity where the goal is to compromise a given network or asset and produce proof of that compromise.

Personally Identifiable Information ("PII"): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Phishing: An attack relying on deception in an attempt to induce the target to voluntarily provide security sensitive information such as financial information or credentials. This attack often relies on exploiting a similar look (both in appearance of the page and the pages URL) to an authentic resource.

Private Clouds: Similar to the Cloud but assumes only one tenant, who is also responsible for the upkeep and maintenance of the cloud environment.

Protected Health Information ("PHI"): Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Ransomware: Malware which restricts access to information or computing resources, usually via encryption, until a ransom is paid.

Risk Assessment: An activity that is meant to enumerate the chances of a specific adverse event to a given resource. For example, if organized criminals have created malware targeting 18 of the top 20 financial institutions, there is a high risk that the remaining 2 will be targeted in the future.

Risk Management Framework ("RMF"): A process and documentation created by NIST to help companies understand and manage risk as it pertains to information systems.

SAFETY Act: Support Antiterrorism by Fostering Effective Technologies Act of 2002. A law that provides critical incentives for the development and deployment of anti-terrorism technologies by providing liability protections for qualified anti-terrorism technology providers. It is enforced and administered by the Department of Homeland Security.

Security Audit: Similar to a penetration test, a security audit differs in that it seeks to catalog all security issues present in a given environment and typically is completed when all areas have been thoroughly reviewed, regardless of the ability to compromise a specific piece of information or area of the environment.

SOC 1 - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting: These reports, prepared in accordance with *Statement on Standards for Attestation Engagements ("SSAE") No. 16, Reporting on Controls at a Service*

Organization, are specifically intended to meet the needs of user entities and the user entities' auditors, as they evaluate the effect of the controls at the service organization on the user entities' financial statement assertions.

SOC 2 - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy: These reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. These reports are performed using the AICPA Guide: *Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* and are intended for use by the service organization's stakeholders so that they have a thorough understanding of the service organization and its internal controls.

Spear Phishing: A targeted phishing attack/campaign limited in scope and typically using customized messages and attacks to increases the chances of success against a limited number of targets.

Static/Dynamic Source Code Analysis: A tool or program which attempts to identify security vulnerabilities via direct analysis of the source code itself, or the execution environment in which it is run.

Threat Assessment: An activity which is meant to enumerate the specific threats to a given resource. For example, organized criminals may create malware targeting a specific financial institution and any protections implemented by that financial institution must consider the threat that this activity poses.

Threat Actor / Malicious Actor: An individual or organization looking to attack a given resource to create an adverse effect (e.g. stealing data, denying access to the service, attack the users of the service, etc.)**.**

Threat Modeling: An activity which is meant to consider the threats and risk of those threats to a given resource and construct a model which details the various risks posed by credible threats to that resource and presents a plan to mitigate the identified risks.

Universal Resource Locator ("URL"): The address of an Internet resource, i.e., http://www.example.com or ftp://ftp.example.com

The Gramm-Leach-Bliley Act ("GLBA"): A federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.

Transport Layer Security ("TLS"): The "s" in "https," an algorithm that is used to encrypt communications, a replacement for SSL.

C. Cybersecurity Risk Management – Useful links

NIST Cybersecurity Framework:
https://www.nist.gov/cyberframework

SAFETY Act:
https://www.safetyact.gov/pages/homepages/Home.do

Open Web Application Program Security Organization (not for profit entity focused on improving the security of software):
https://www.owasp.org

Federal Financial Institutions Examinations Council - cybersecurity assessment tool:
https://www.ffiec.gov/cyberassessmenttool.htm

Vendor Security Assessment Questionnaire (VSAQ):
https://vsaq-demo.withgoogle.com

Health Information Trust Alliance (HITRUST):
https://hitrustalliance.net/

National Conference of State Legislatures listing of state data breach and notification laws:
http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws

SIFMA Small Firm Cyber Guidance & Checklist:
http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms

United States Computer Emergency Readiness Team (US-CERT) at:
www.us-cert.gov

Federal Trade Commission's Business Center – Privacy and Security:
https://www.ftc.gov/tips-advice/business-center/privacy-and-security

Health and Human Services Guidance on Ransomware:
http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Cybersecurity in the Golden State:
https://oag.ca.gov/cybersecurity

National Association of Insurance Commissioners:
http://www.naic.org