Brian E. Finch, Esq.

Partner, Pillsbury Winthrop Shaw Pittman LLP

August 24, 2016

Written Statement For The Record Delivered To The U.S. Department of Labor's Advisory Council on Employee Welfare and Pension Benefit Plans (a/k/a "ERISA Advisory Council") On Cybersecurity Considerations for Benefits Plans

Issue Chair Tully, Vice Chairs Stein and Smith, Executive Secretary Good, distinguished Members of the ERISA Advisory Council ("Council"), thank you for allowing me to appear before you today to discuss various cyber-threats facing employee benefit plans and certain measures that can be taken to mitigate the associated risks.

My name is Brian Finch and I am a partner at the law firm of Pillsbury Winthrop Shaw Pittman LLP. I am also a Senior Fellow at The George Washington University Center for Cyber and Homeland Security - where I serve as a member of the Center's Cybersecurity Task Force, a Senior Advisor to The Homeland Security and Defense Business Council, and a member of The National Center for Spectator Sport Safety and Security's Advisory Board.

Please allow me to begin by setting forth what I believe to be a fundamental principle: when it comes to cyber-threats, there is no such thing as risk elimination, only risk mitigation. This simple but undeniable fact is ignored or misunderstood by many, and because of that there often are unrealistic expectations imposed on information security experts as well as those with managerial and fiduciary obligations as to the cybersecurity results they can obtain.

I would counsel the members of the ERISA Advisory Council, as well as those that heed its guidance, to learn that fact quickly. The sooner people

understand that cyber-risks can only truly be managed and not eliminated, the sooner this community will begin developing a practical framework for limiting the threats associated with cyber-attacks.

More generally, I am in agreement with the members of the Council and previous witnesses that cybersecurity best practices and risk management processes are critical to our nation's economic security and physical safety. Members of this Council know all too well that our cyber enemies are numerous, growing, and increasingly sophisticated. If we have learned anything over the past few years with respect to the threat posed by our cyber enemies, it is that even our most advanced cyber defenses cannot keep up with the sophistication and innovation of cyber-attack methodologies. The result is a steady, if not increasing, "cyber gap" between defense and offense.

Important to remember here is that part of the reason why the "cyber gap" is growing is because the cost of conducting cyber-attacks remains stubbornly low, and, if anything, it decreases with each passing day. Consider the following figures:

- The age of computer forensic experts being able to proactively identify viruses and develop defenses against them is over. Why? Because now on average nearly 600,000 new computer viruses and other pieces of malicious software are being developed daily.
- For only $30, persons who have developed their own malware/viruses can submit their malicious program to a black market testing lab in order to determine if the newly developed virus will penetrate commonly used software and hardware defenses.
- For an average of $2/hour (four hours minimum), a freelance hacker can be hired to conduct a "distributed denial of service" or DDoS attack. For those who are unfamiliar with that term, a DDoS attack is one where a website is overwhelmed with internet traffic to the point where it is no longer accessible.
- Previously unknown software exploits for which there exist no defenses are readily available for purchase on underground cyber-arms bazaars. The cost for these so-called "zero-day" exploits vary greatly, ranging from $5,000 to over $250,000.
- Perhaps most worrisome is that many malicious tool kits are available to would-be hackers for free. Examples of free hacking tools include: systems to generate fake e-mail addresses, translation services to assist in the dissemination of spam/fraudulent e-mails, and so-called "ransomware,"

which encrypts the information on a computer and can only be decrypted upon payment of a ransom.

This represents but a small portion of the threats facing businesses, including the operators and administrators of employee benefits plans. The question thus becomes, what can be done to fight back against these threats?

One relatively popular solution has been the development and marketing of cyber-insurance tools. As a general matter, the development of the cyber-insurance market is a positive step. Providing mechanisms for reimbursement of losses following a cyber incident is a positive one, too. However, I believe this market needs greater maturity and a different line of thinking before it can become truly beneficial to operators and administrators of employee benefits plans.

What I would like to bring to the attention of the Council is that today's cyber-insurance products would be of greater benefit if they attacked the cyber problem from a different angle.

Cyber insurers, like many others, have correctly assessed that cyber-attacks will successfully strike a company at some point. However, these cyber-insurance models suffer a fundamental disconnect in that they operate under the assumption that cyber-attacks will be sporadic and will rarely succeed.

The reality is that cyber-attacks are a constant threat, seeking to penetrate information systems and technologies from every direction and through every possible entry. I would argue therefore that the cyber-insurance market has been using incorrect models and assumptions when developing policies for use in cyber risk management.

Rather than viewing cyber-attacks as infrequent events like a fire or natural disaster, I believe cyber risk management would be best served if insurers looked towards policies that use a personal health model. That means cyber insurers should look to establish an infrastructure that supports *constant* care and promotes wellness, not merely reimbursement for periodic losses. In my mind, what follows then is that cyber insurers should develop cyber policies using a health maintenance organization or "HMO" model.

Under that model, the insurer's goal will be to promote the "right" kinds of claims – ones that encourage healthy behavior. This model addresses the reality that inevitably some sort of cyber disease will work its way into the blood stream

by supporting interventional care that prevents minor scratches from developing into a serious infection.

Companies would gain access to the cyber HMO by paying monthly premiums along with associated "co-pays," "deductibles," and similar expenses typically associated with a health insurance plan.

That cyber HMO plan would give the insured access to a vast network of cybersecurity vendors and professionals at discounted rates that could be called upon in the event of a problem (the "co-pays" and "co-insurance" equivalents).

The cyber HMO plans would also provide low cost or even free access to basic "cyber hygiene" care, such as routine diagnostic examination of information technology systems, perimeter defense systems, and other basic defense systems (the annual physical and low cost or free vaccine equivalents).

More "advanced" defense systems could be subject to a higher co-pay and deductible, and companies could even choose to go "out of network," but only by shouldering more of the cost.

I firmly believe that this Council should look for ways to support the concept of a "cyber HMO," as a model that actively promotes and rewards healthy cyber behavior – a Gordian knot that no carrier has yet been able to untie using traditional insurance models. That is a critical piece of the cybersecurity puzzle, as the challenge has been how to get companies to engage in *effective* cybersecurity rather than the most easily accessible form of it.

Best of all, using the cyber HMO model addresses a presumed obstacle to cyber insurance: a lack of actuarial data. Through its mere existence, the cyber HMO will gather the data needed to assess and underwrite costs. This enables cyber benefits to be more finely tuned, benefitting its members and society writ large.

At the very least, this approach has the benefit of trying to *solve* the problem at hand, not simply forcing a square peg into a round hole. If nothing else, maybe this idea will generate more discussion around trying to take proactive security measures.

One other model I would like to present to the Council is the notion of creating cyber "pools" of insurance. Through risk pooling, companies can work

together to purchase more insurance than might otherwise be available to them while also establishing hard liability limits and sharing cyber defense resources.

Risk pooling mechanisms come in a number of forms, including "risk purchasing" and "risk retention" groups. Those groups allow collections of companies (usually similarly situated in terms of industry sector) to jointly purchase or create insurance coverage that would otherwise be unavailable or excessively expensive.

Such pools have been around for some time, and discussions with respect to utilizing them in the context of cyber threats are picking up steam. Where companies can take true advantage of these mechanisms is to layer in additional risk mitigation tools such as threat information sharing and statutory liability protection. Combining those aspects could lead to a very powerful collective defense tool.

Here is how it can work:

1. A group of similarly situated companies agree to form a risk purchasing or retention group in order to obtain cyber security insurance.

2. The companies agree to use certain security standards or technologies (for instance, SANS 20 controls, "detonation chambers," information sharing via dedicated "private clouds," the recent National Institutes of Standards and Technologies (NIST) voluntary cyber security framework, etc.)

3. The companies then pool their resources either to jointly purchase an existing cyber insurance policy or to create a pool of insurance that they would collectively maintain.

4. The risk group also agrees to pursue SAFETY Act protections for the standards it has created and committed to adhering to. For those who are unfamiliar with the SAFETY Act, it is a law administered by the Department of Homeland Security. Under the SAFETY Act, companies that sell or deploy cybersecurity products or services may obtain liability protections in the form of either (a) a maximum cap on liability equal to a specific amount of insurance, or (b) a presumption of immediate dismissal of claims arising from cyber-attacks and related to the approved products or services.

5. As part of the agreement, any company that fails to adhere to the security standards will be asked to leave the group at the next renewal period.

This proposal can potentially be extremely valuable to the most vulnerable companies, namely small and medium-sized businesses that do not have the resources to create their own robust cyber defenses. By pooling not only their financial resources to buy additional insurance but also their technical capabilities to create a common defense, this concept will work to strengthen the bonds between businesses and allow them to collectively respond to and mitigate otherwise devastating cyber-attacks.

Further, this arrangement also potentially allows for more of the insurance funds to be used for "first party" losses the company has *directly* suffered (e.g., damaged equipment, lost data, business interruption, etc.) rather than losses suffered by third parties.

The pool arrangement also enables companies to collaborate and establish a baseline of security that each would commit to maintaining, and also allows for regular reviews to determine what security controls need to be adjusted. The companies could even work with public/private partnership resources within the Department of Homeland Security and other federal agencies such as NIST to help them refine their programs and policies in order to achieve a greater cyber "maturity" level than they might have otherwise reached.

Another benefit of this pool concept is that the insured group can take advantage of the cyber-information sharing platform, recently created by the Cyber Information Sharing Act (CISA). The pools would be prime candidates to benefit from that platform, and would likewise make excellent candidates to serve as information sharing and analysis organizations, or "ISAOs," within the CISA framework.

The pooling concept gives companies an excellent opportunity to take charge of their security profile, and do so in a way that both mitigates the likelihood of a successful attack as well as increase resources to respond to or mitigate losses. Further, these pools can serve as an excellent collective effort that can more fully take advantage of the public/private partnership benefits offered through the CISA legislation and the ISAO concept.

Briefly, I would also like to touch upon one other potential area of interest to the Council. Specifically, critical for the operators/administrators of employee

benefits plans is the inclusion of appropriate cybersecurity obligations in agreements with third parties who assist in the administration of the plans.

As previously noted, cyber-criminals are infinitely devious and inventive. They, like any corrosive force of nature, will seek out and exploit weak points and will use the path of least resistance in order to achieve their goals.

With respect to information security, this means that cyber-criminals work to find vulnerable points of entry into computer systems, and from there conduct their nefarious activities. As we have seen time and again, third-party entities have been attacked as a way to conduct cyber financial crimes and other illegal and destructive electronic activities. Examples include gaining access to support vendors, public relations firms, and, at times, even law firms.

As such, it is critical then for employee benefit plan operators and administrators to consider cybersecurity when negotiating and implementing contracts with third parties who will have access to plan information or otherwise can impact its operation.

The following are some examples of steps that benefit plan operators and administrators can undertake to ensure higher levels of security from their third-party affiliates:

- Use of the SAFETY Act: As I previously mentioned, the SAFETY Act is a liability mitigation tool administered by the Department of Homeland Security. What I did not mention is that employee benefit plan operators and administrators can require third parties to obtain these protections. Doing so will carry two benefits. First, operators and administrators will have the comfort of knowing that the third parties have had their cybersecurity programs vetted by the Department of Homeland Security. This will provide a level of confidence in the security measures being undertaken by the third party that cannot be gained through another program. Second, the liability protections of the SAFETY Act "flow" to the customer. So in the case of benefit plan operators and administrators, they will gain key liability protections simply by using a SAFETY Act approved third-party vendor. No other law offers that level of protection.

- Clearly define security obligations: We have seen situations where contracts with third-party administrators or providers of information services vaguely define who is responsible for which security measures and what exactly

those security measures will consist of. At best, this leaves benefits plan operators and administrators with uncertainty as to who is managing specific security features. At worst, it can leave material gaps in security and no specifically defined remedy for a third party's failure to secure its systems. Benefits plans must now include defined security obligations (such as the previously mentioned "SANS 20" controls) as "boilerplate" in their third-party agreements.

- Automatic notification and audit obligations: Employee benefits plan operators and administrators must adhere to the old adage "trust but verify" when it comes to cybersecurity. Companies are not necessarily obligated by law to disclose every breach, much less every "material breach" that occurs on their systems. In the absence of such statutory or regulatory obligations, benefits plan operators and administrators should include specific notification requirements, so that there is awareness of possible threats and therefore the potential need for additional security measures. The same is true for information security audit requirements of third parties. Just because a company represents that it undertakes certain cybersecurity measures or that cyber-attacks upon it are limited does not mean that companies should be taken at their word. Benefits plan operators and administrators should include in their third-party agreements the right to conduct periodical information security audits to ensure that such measures match the expectations.

More could be said, but the point is clear: operators and administrators of benefits plans should specifically spell out obligations and expectations in their agreements with third-party service providers.

Conclusion

Thank you for the opportunity to address the Council on cybersecurity issues. I am happy to answer any questions you might have regarding my thoughts.