
At Sobel & Co., we take our responsibility for educating our clients and colleagues very seriously. As such, we regularly share articles, research, study results and other important resources to help you remain informed and alert to challenges impacting the Employee Welfare and Pension Benefit Plan area.

One topic that remains at the top of the list of hot issues is the continuous threat of cybercrime to the financial sector. As we all know, the number and sophistication of malicious incidents has increased dramatically over the decades and is expected to continue to escalate. In fact, cyber-risks faced by employers and service organizations today are more severe and egregious than at any time in the past according to Alan Brill, Senior Managing Director of Cyber Security and Investigations at Kroll. To understand the magnitude, despite the inability to accurately calculate exact losses, the government and private sector estimates that the costs of cybercrime to the U.S. economy have ranged from millions of dollars to hundreds of billions of dollars, with the projection that the costs to an individual victim organization can range from $1 million to $52 million.

This challenge is not limited to traditional financial, banking and accounting providers but is equally as potent for those in charge of plan administration, including plan sponsors, fiduciaries and service providers who regularly face the fact that they must be prepared for a cyberthreat. While benefit plans typically are excluded from an organization's overall cybersecurity plan, the reality is that benefit plans often maintain and share sensitive employee data and asset information across multiple, unrelated entities as part of the benefit plan's administration process. This makes the plan a prime target for any cyberthreat!

Recognizing the danger that could result when employee benefit plans are overlooked in regards to their vulnerability to cybercrimes, the Department of Labor ("DOL") Advisory Council on Employment Welfare and Pension Benefit Plans (DOL ERISA Advisory Council) recently issued a detailed report, "Cyber Security Considerations for Employee Benefit Plans," ("DOL report") that hones in on this area of concern. Because the capabilities of cybercriminals remain at an all-time high, combating this challenge must be a top priority for everyone involved.

The DOL report focuses solely on the relationship between cybersecurity and pension and welfare benefit plans, offering information and suggestions to help plan administrators and fiduciaries to develop, implement and manage the strategies that are most relevant for them as they launch their own cybersecurity program.

Those of you who are actively engaged in this area are urged to consider the importance of implementing a cybersecurity plan to safeguard benefit plan data and assets, as well as to help you with the decision regarding the selection or retention of a service provider.

Remember, individual data and information, as well as the potential to access assets, will always be valuable to criminals - so cybersecurity threats will continue to exist, growing and evolving, in direct correlation to the advantages of such activity!

Here are some of the critical suggestions that are included in the Report:

1. Focus on the data – in other words, focus on what *could be done* with this information. Next, understand who has access to the sensitive data and then decide what is the minimum amount of information they need to access to accomplish their job.

2. Be aware of the significant threats facing employee benefit plans from ransomware, phishing expeditions, wire transfers, mail fraud and malware application via external devices.

3. Consider how your data is transmitted. Encryption is now an essential component for any organization's cybersecurity, especially when transferring data between multiple parties or moving data to or from the cloud.


Even when vigorously employing all the appropriate strategies, obstacles to launching a cybersecurity plan include limits that exist on both the resources and the technical expertise, as well as the lack of awareness of the complexity surrounding the topic. Even when consulting cybersecurity experts, it is almost impossible to expect the complete elimination of risk. Instead, organizations can follow some guidelines offered to complement their existing cybersecurity approach or to assist in creating one if none exists.

The first set of guidelines as presented in the DOL report (called the Framework) outlines the functions any organization must establish to identify, protect, detect, respond and recover on an ongoing basis. These functions enable each organization to embrace a comprehensive understanding of its complete risk management lifecycle. The second step is for the organization to focus on the actual implementation of a risk management program. To do this efficiently, the organization needs to consider whether its existing plan is being implemented only on a partial basis, is risk-informed, and is repeatable and adaptive. These insights spotlight the ability of the organization to execute efficiently. Lastly, in phase three, the organization must focus on developing a profile that highlights the business drivers combined with a risk assessment to determine what is essential for the organization's success.

Ultimately, the Framework provided in the report is distilled to seven steps that are relevant for most employee benefit plan decision makers:

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

Cyberthreats due to compromised data and assets have become commonplace news that we are exposed to daily. The repetition of these criminal acts should not lull us into boredom and should never become just "background noise." No one is immune, and certainly data-rich employee benefit plans can be a main target! Benefit plan participants may be subject to identity theft, privacy breaches and theft of assets. As a plan sponsor or fiduciary, you must take your role seriously. The experts say you should be asking yourself, "W*hen* will my plan be the victim of a cyberattack," instead of wondering *if* it will be a victim. The important conclusion from the DOL is *what* will you do about it?

Cyber threats cannot be eliminated, but they can be managed. For more details, download the entire report, published in November 2016 and entitled "Cyber Security Considerations for Benefit Plans" authored by the Advisory Council on Employee Welfare and Pension Benefit Plans as presented to the United States Secretary of Labor, at:

https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf?cm_em=elizabeth.harper@sobel-cpa.com&cm_mmc=AICPA:CheetahMail-_-EBPAQC_Alert-_-FEB17-_-EBPAQC_Alert_380&utm_source=EBPAQC_Alert_380&utm_medium=email&utm_content=ebp18&utm_campaign=ebpaqcalertfeb17

As always, please feel free to contact Elizabeth Harper at Elizabeth.harper@sobel-cpa.com, Ken Bagner at Kenneth.bagner@sobel-cpa.com or Jim Mottola at james.mottola@sobel-cpa.com