PlanPILOT

Better Outcomes, Less Risk

# Prevalence of Cybersecurity

## Understand, Prevent, Implement

PlanPILOT

# Prevalence of Cybersecurity

## Understand, Prevent, Implement

## EXECUTIVE SUMMARY

Until recently, cybersecurity in the retirement industry had been a desensitized topic amid thousands of cyberattacks that occur to institutions each year. With increasing reliance and connected services on the internet for retirement plan sponsors and their providers, there is preeminent risk for cyberattacks and cyberwarfare. According to the World Economic Forum's 2019 Global Risks Report, cyberattacks are one of the greatest risks facing institutions each year and will continue to escalate. In late 2018, the ERISA Advisory Council asked the Department of Labor to provide procedures and guidance on how cyberattacks can be mitigated along with security frameworks that can be implemented to protect data. In order to mitigate these risks of a potential cyberattack, plan sponsors and providers must first understand the types of risk that exist, implement frameworks, and establish prevention techniques.

PlanPILOT

# Understanding Cyberattacks

It is important to first understand the terms that accurately inform plan sponsors of the impact a cyberattack can have on the security of their data. The SPARK Institute has developed definitions identifying "Security Breach" and "Cyber Fraud" for the standard of the recordkeeping industry. They illustrate these terms as:

**Security Breach:** Unauthorized acquisition, disclosure, modification or use of unencrypted personal data, or encrypted personal data where the encryption key has also been compromised; and a likely risk of identifying theft or fraud against the data subject. This includes the following:

- Attacks on a recordkeeper's network or information system that results in participant records to be stolen.
- Intrusion of a recordkeeper's external cloud account that results in encrypted personal data being stolen.
- Loss of an unencrypted laptop that stores personal data where there is reasonable basis to believe that the loss may result in identity theft or fraud.

**Cyber Fraud:** Confirmed compromise of a participant's financial account through unauthorized acquisition of information that results in wrongful financial or personal gain or illegal access to bank accounts. For example:

- Participant discloses their account credentials via phising email link, which are then used to compromise the participant's online account and withdrawal of their funds.
- An attacker takes over a participant's account and changes their information and /or attempts to transfer money.
- Attacker gain's access to a participant's account through impersonating their identity to the recordkeeper's call center.

PlanPILOT

# Frameworks

Coupled with an understanding of the types of risks and cyberattacks that can occur, plan sponsors should also seek to identify methods to mitigate these risks. The SPARK Institute has come up with "a framework for cybersecurity disclosure by plan providers".

The 16 control objectives include:

- Risk assessment and treatment;
- Security policy;
- Organizational security;
- Asset management;
- Human resource security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition development;
- Incident and communications management;
- Business resiliency;
- Compliance;
- Mobile;
- Encryption;
- Supplier risk; and
- Cloud security.

PlanPILOT

# Preventative Measures

With SPARK's frameworks, plan sponsors can outsource to different providers and compare them. In addition, external auditors can create reports analyzing how recordkeepers have kept these control objectives to the standards. With this framework in place, it will foster the utmost security for providers and protect participants' data.

Lastly, preventative measures and requirements noted by ERISA should also be considered. These requirements include:

- Retaining only the data that is needed; if certain data elements can be redacted, remove them
- Maintain an inventory of records that are retained regardless of format, and where to find them
- Outline a clear process for moving records, and track location on inventory during the move
- Delete records that are no longer needed; confirm service providers have done so, as applicable.

PlanPILOT

# Implementing the Best Security Practices

With a basic understanding of the types of cyberattacks that are prevalent, the framework to mitigate the risks, and guidance on preventative measures, a logical next step is **identifying ways to best implement security practices**.

There are a variety of ways employers can help protect plan assets. It is imperative that employers encourage participants to actively engage with their retirement accounts. Providing email addresses to the recordkeeper for all plan participants and educating employees on the risks of cyberattacks is also crucial. Employers should work alongside recordkeepers so they are trained on the processes for loans and distributions and are actively communicating with participants about the types of transactions that are occurring. Employers should be on top of their personnel and actively read the communications from their recordkeeper and other providers.

In addition, plan sponsors should oversee if plan providers are enforcing the basics of security, such as enforcing stricter password policies and alternative security questions. Plan sponsors should review "default credential" policies for newly eligible participants to ensure defaults are expired after the initial enrollment period for those that do not engage with their online accounts. This is especially crucial because of an increase in the ability of fraudsters to circumvent basic security practices, including email and SMS-based 2-FA. Recordkeepers should evaluate and implement more advanced authentication and security practices to prevent this from happening.

**With these new standards in place, plan sponsors and recordkeepers will be better positioned to conform to fiduciary requirements, as well as to protect the data of their participants and clients from cyberattacks. It is hopeful these standards set a strong presence in the industry.**

# Cybersecurity: How to Defend Your Retirement Plan

**Watch our video to learn more about why cybersecurity is important, the main types of cyberattacks, the impacts if an attack happens, and how plan sponsors can protect their plan and plan participants.**

PlanPILOT

# Contact

PlanPILOT
223 W. Jackson Blvd., Suite 800
Chicago, IL 60606

(312) 973-4911
info@planpilot.com
www.planpilot.com

Copyright © 2019. PlanPILOT, LLC. All Rights Reserved.