Mitigating Cybersecurity Risk Amid the Coronavirus (COVID-19) Outbreak

Title	**Mitigating Cybersecurity Risk Amid the Coronavirus (COVID-19) Outbreak**
Date	**May 2020**
Author	**Valerie Haley, Retirement Plan Services Associate**

Over the past few months the coronavirus pandemic has drastically transformed the way we live and work, with many businesses being forced to abruptly shift operations due to stay at home orders. As of April 2020, more than 300 million people in the United States were placed under state or local directives to stay at home. Even as some areas begin to relax restrictions, telecommuting will likely continue for many long after the pandemic ends.

Thousands of employees have moved from professionally managed networks to what are often basic and non-secure home setups. In order to ensure continuity of service, many organizations have relaxed protocols to allow employees to access sensitive information from their home offices.

Adjusting to remote work can be fraught with challenges under the best of circumstances, but doing so during a global pandemic raises a host of potential cybersecurity vulnerabilities for plan sponsors. Retirement plan sponsors must continue to meet their fiduciary duties even during times of emergency, and evaluate whether their cybersecurity policies need to be adjusted in light of the current circumstances.

Personally identifiable information (PII): such as social security numbers, dates of birth, and email addresses.

Participant enrollment data: such as individual account balances, direct deposit information, compensation, and other financial information.

Electronic protected health information (EPHI): such as information about health status, healthcare provisions, healthcare related payment data.

COVID-19 and the Rise of Cyber-Attacks

Plan sponsors should be aware that cyber criminals are taking advantage of the COVID-19 pandemic. The World Health Organization warned in February that cyber criminals had begun exploiting the current pandemic in an attempt to access sensitive data. In March, the Federal Bureau of Investigation issued an alert warning of an increase in fraudulent activity tied to the coronavirus, particularly in the area of cyber-crime.

Even prior to the coronavirus pandemic, retirement plans were considered attractive targets for criminals seeking to gain access to plan assets and participant data. Now more than ever, cybersecurity is a major concern for plan sponsors, as retirement plans are exposed to increased risks relating to privacy, security, and fraud.

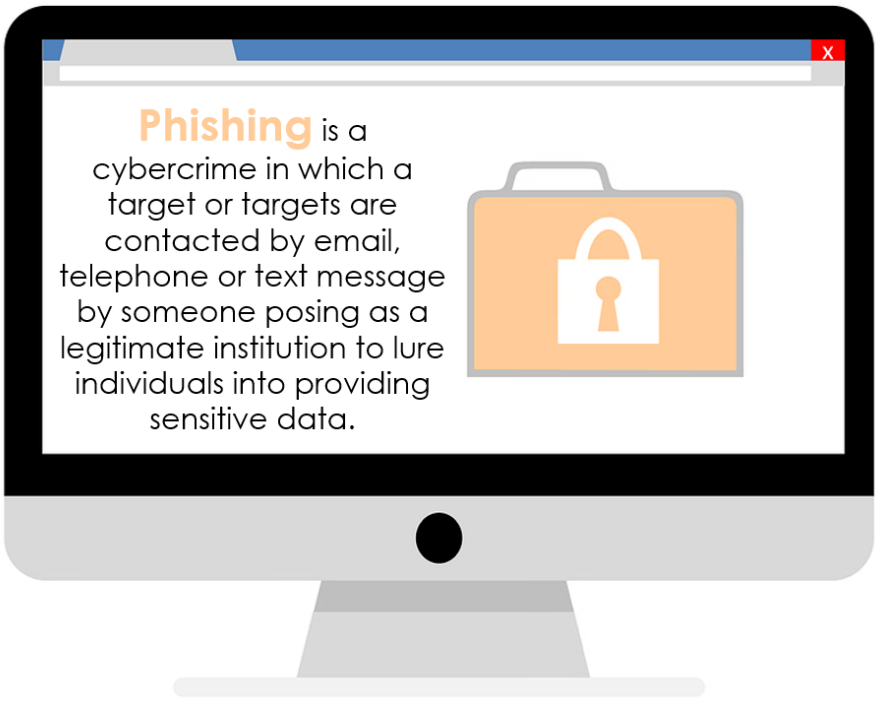
Cyber-Attack Threats to Be Aware Of:

- **Phishing** where criminals purporting to be from a reputable source contact a target, often by email, in order to obtain sensitive information.
- **Ransomware** where criminals encrypt and seize an entire hard drive and will only release it for a ransom.
- **Wire transfer email fraud** where cyber criminals pretend to be senior executives asking employees to transfer funds.
- **Malware** via external devices where harmful software is stored on an external drive that is inserted into and executed on a network computer.

There are many known and emerging methods used by cybercriminals to access the information described above. One of the most common methods is known as “Phishing”. The following are two examples of how phishing schemes can occur with regards to retirement plans[i]:

EXAMPLE 1: An email claiming to be from a plan sponsor’s top executive was sent to the human resources department requesting sensitive employee data. HR responded by sending the requested information before realizing it was sent from a fraudulent outside party.

EXAMPLE 2: An email claiming to be from a plan recordkeeper was sent to participants, resulting in the sharing of sensitive account information. As a result, participant accounts were breached and unauthorized distributions were made from accounts.



The threats discussed above highlight the importance of establishing strong internal cybersecurity protocols. However, a company's cybersecurity is only as strong as the cybersecurity of its third-party service providers. When it comes to cybersecurity, third-party due diligence is an important step that many plan sponsors often neglect to consider.

For plan sponsors, conducting third-party due diligence is not only prudent from a security perspective but also from a liability perspective. It has become increasingly important to recognize the potential legal liability plan sponsors face when it comes to cybersecurity breaches, and the important role due diligence can play to mitigate those threats and ensure fiduciary compliance.

Detailed Service Provider Due Diligence

Plan sponsors have a fiduciary duty to prudently select and monitor service providers, and cybersecurity is increasingly being viewed as a top consideration. In a recent report from Cerulli, data security was designated as a top concern by 80% of retirement plan specialists, and it was selected as the single most important factor when evaluating vendors. Plan sponsors themselves, especially those who may now be working from home, should exercise vigilance when managing sensitive data due to the increased security vulnerabilities.

> “A sponsor could be liable if the claimant establishes that it failed to follow a prudent process to safeguard the plan data
>
> Joan Neri, counsel at Drinker, Biddle & Reath

According to Joan Neri, counsel at the Drinker, Biddle & Reath ERISA practice, in the event that a breach or fraud occur, “a sponsor could be liable if the claimant establishes that it failed to follow a prudent process to safeguard the plan data.” By carefully selecting and monitoring third-party service providers and implementing and adhering to internal cybersecurity protocols, plan sponsors can prevent breaches and reduce liability.

Source: Cerulli Associates. “U.S. Retirement Markets 2019: Looking Toward Holistic Solutions for Participants and Plan Sponsors.”

Plan sponsors should carefully review how their current service providers handle cybersecurity and what additional measures, if any, they have implemented in light of the coronavirus pandemic. Plan sponsors should also take this opportunity to review the provisions of their recordkeeper or third-party agreements, as some may offer guarantees that cover cyber-attack losses up to a certain point.

Another step plan sponsors should take is to confirm whether their current fiduciary insurance policies cover cyber breaches and whether purchasing more comprehensive cyber insurance is necessary or feasible. Cybersecurity insurance is an evolving area and plan sponsors must evaluate their needs in this ever-changing environment.

The coronavirus pandemic underscores the importance of being proactive rather than reactive, and that same principal holds true for developing an effective approach to cybersecurity. The rapid and widespread transition to remote-working has undoubtedly placed additional stress on many businesses, but properly securing remote-working arrangements and confirming internal and external cybersecurity policies are crucial measures to ensure business continuity. While there are many challenges facing plan sponsors at this time, proactively developing and safeguarding your cybersecurity policies is a prudent action to minimize potential losses and liabilities and demonstrate compliance.

What You Can Do

In times like these, cyberattacks are more prevalent but there are steps plan sponsors can take to address risks. According to the Department of Labor (DOL) Advisory Council Cybersecurity Report, there are four key areas that plan sponsors should focus on to protect against cyber-attacks, Data Management, Technology Management, People Issues, & Service Provider Management. In each of these categories we've provided recommended actions that plan sponsors and fiduciaries can take to protect data related to retirement plans:

Data management:
Protect and control data

- Use a secure VPN connection when accessing sensitive data remotely.
- Retain only the data that is needed.
- Control and limit access to plan data.

Technology management:
Maintain up to date technology

- Use secure cloud-based systems along with advanced encryption technology.
- Use security software to monitor against potential threats.

Service provider management:
Perform due diligence on plan data security of service providers

- Assess the cybersecurity programs that third-party providers implement to protect employee plan data.
- Review service provider agreements to confirm whether they contain cybersecurity related provisions.

People Issues:
Properly train and manage personnel

- Train all personnel interacting with plan data or information systems.
- Train plan participants on how to protect their accounts and data (e.g. password security, two-factor authentication, how to identify suspicious emails).

References

Advisory Council on Employee Welfare and Pension Benefit Plans. (2016, November). Cybersecurity Considerations for Benefit Plans. Retrieved from https://www.dol.gov/sites/dolgov/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf

Barney, L. (2019, November 22). Retirement Plan Sponsors Need Strong Cybersecurity Defenses. Retrieved from https://www.plansponsor.com/in-depth/retirement-plan-sponsors-need-strong-cybersecurity-defenses/

Burnoski, S. P., & Steedly, K. (2019, July 8). Protect Your Employee Benefit Plans from a Cyber-Attack. Retrieved from https://www.applegrowth.com/protect-your-employee-benefit-plans-from-a-cyber-attack/

Employee Benefit Plan Audit Quality Center/AICPA. (2018, May). Cybersecurity and employee benefit plans: Questions and answers. Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/employeebenefitplanauditquality/resources/accountingandauditingresourcecenters/downloadabledocuments/cybersecurity-and-ebp-questions-and-answers.pdf

Mervosh, S., Lu, D., & Swales, V. (2020, March 24). See Which States and Cities Have Told Residents to Stay at Home. Retrieved April 7, 2020, from https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.html

The Federal Bureau of Investigation. (2020, March). Internet Crime Complaint Center (IC3): FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic. Retrieved from https://www.ic3.gov/media/2020/200320.aspx

The World Health Organization. (2020, February). Beware of criminals pretending to be WHO. Retrieved from https://www.who.int/about/communications/cyber-security