Best practices for plan sponsors

hooker & holcombe

Cyber-attacks are on the rise. Is your retirement plan protected?

Cyber-crime is on the rise worldwide. As a result, growing numbers of organizations are taking critical steps to protect their valuable electronic data from hackers and other cyber criminals — a process known as cybersecurity. It's serious business, and a trend retirement plan sponsors and committees should pay attention to.

In 2015, IBM's chair, president and CEO Ginni Rometty said, "Cyber-crime is the greatest threat to every company in the world.[1]" Last year, billionaire investor and businessman Warren Buffett echoed that sentiment, claiming that "cyber-attacks are a bigger threat to humanity than nuclear weapons.[2]" In short, cyber-crime is extremely dangerous, and many businesses are vulnerable to cyber-attacks — some without even knowing it.

Why is cybersecurity important?

Thanks largely to the proliferation of high-profile cyber-attacks and data breaches that hit organizations in 2017 (including Equifax, which exposed the personal information of nearly half of Americans), information security research firm and publisher Cybersecurity Ventures predicts that, **by 2021, cyber-crime will cost the world $6 trillion annually**.[4] A single successful cyber-attack can cost an organization more than $5 million, or $301 per employee, according to the Ponemon Institute. Clearly, the costs related to cybersecurity threats are significant.

Beyond the expenses related to a potential cyber-attack, there are a number of reasons why retirement plan sponsors and committees should focus on specific cybersecurity efforts to protect their plan assets and information. For starters, if you think your plan isn't a target, think again. It's not a matter of if, but when your plan gets hacked.

Here's why: Recently, cyber-attackers have begun to set their sights on plan sponsors themselves rather than their recordkeepers and custodians because they know that the former typically lack the sophisticated cybersecurity defenses of their vendors.

Cyber-criminals also know that retirement plan sponsors and their vendors manage large amounts of money, and in so doing, collect highly sensitive personal data from plan participants and their beneficiaries, including names, address, birthdates, and Social

Security numbers. This information is extremely valuable to hackers because most of it is permanently associated with an individual and can't be changed or cancelled like a credit card or bank account information.

Participant data such as account balance, direct deposit and compensation/payroll information is also at risk, and therefore, potentially vulnerable to a cyber-attack if not properly handled and protected by plan sponsors and their third party vendors. Therefore, it's critical for sponsors to address cybersecurity within their own organizations, as well with vendors such as recordkeepers, trustees, TPAs and investment advice providers, which receive personal data from the plan.

Some examples of cyber threats to retirement plans might include fraudulent distribution or loan requests, or ransomware attacks and phishing techniques where a hacker might obtain log-in credentials (i.e., through a stolen laptop or mobile device storing personal data and passwords) to access participants' account information online.

What is my responsibility?

While retirement plan information is protected under specific regulations, there are no comprehensive laws that protect plan sponsors and service providers against

Regulations & cybersecurity	
Fiduciary obligations	The selection and monitoring of service providers is a fiduciary act
	The decision makers must act prudently and solely in the interest of the plan participants and beneficiaries
	Plan fiduciaries are liable for failing to prudently select and monitor service providers
	This may include prudence in selecting and monitoring service providers to ensure they maintain adequate cyber security practices and protocols
ERISA & electronic distribution of plan information	If plan notices are disseminated electronically, the plan sponsor (and not the service provider) is required to protect the confidentiality of personal data
	Similarly, plan sponsors are required to take measures to ensure websites with plan information are secured to protect the confidentiality of personal information

cyber-threats, like there are for group health plans (i.e., the Health Insurance Portability and Accountability Act, or HIPAA). Nonetheless, plan sponsors must act in a fiduciary capacity under the best interest clauses of the Employee Retirement Security Income Act (ERISA), the law that governs retirement plans. In addition, sponsors must adhere to the data privacy requirements for electronic notices. The chart on this page breaks down the regulatory guidelines for plan sponsors' fiduciary duties related to cybersecurity and electronic distribution of plan information.

Several states also have laws governing the protection of employees' Social Security numbers and employers' responsibilities to notify employees in the event of a security breach. However, these laws are designed to regulate the employer rather than the plan sponsor, so ERISA would likely take precedence in a retirement plan-related cyber-attack.

What can I do to protect plan assets and information?

Most organizations take a reactive approach to cyber-attacks, addressing them only after an incident has occurred. However, that can be expensive, complicated, and mostly ineffective. Plan sponsors have an opportunity to proactively address and manage cyber-security risks using a variety of tactics to improve their ability to prevent, detect and respond to cyber-attacks.

First off, assume that your company's retirement plan will be attacked. When setting up defenses against cyber-threats, consider addressing the following questions:

- What is our internal risk?
- Where does our data go and how is it transmitted and stored (e.g., to third parties, or maintained on a server or in the cloud)?
- Have we done appropriate due diligence on our vendors, and any partners with whom they may share data?
- What is our organization's definition of a "breach"?
- What is our vendors' definition of a "breach," and what would prompt them to disclose that to us?
- How do we monitor our internal processes and procedures, and that of our external partners, on an ongoing basis?
- Do contracts and agreements cover indemnification, notification procedures (i.e., does the vendor have to notify us when it discovers a breach, or only after the breach has been contained), and remediation?
- What is our process for when we experience a breach?

In addition, plan sponsors should:

- Implement a specific process for addressing and fixing cybersecurity concerns, which would include, for example, identifying potential security gaps in how they share information with third party vendors.
- Make sure they have appropriate cyber-liability insurance coverage to help mitigate damages from potential attacks, and that they understand what the policy covers. Ideally, the coverage should be as broad as possible.
- Consider hiring an outside cybersecurity firm with retirement plan experience to conduct periodic audits and ensure participants' data is secure.
- Put processes and stop gaps in place to restrict access to plan systems, applications, data and other sensitive information.
- Develop a cybersecurity risk management strategy specific to their retirement plan, which addresses the sponsor's response to a breach (including appropriate notices and remediation methods).

Moreover, sponsors should also encourage plan participants to:

- Regularly check accounts for unauthorized activity.
- Protect passwords and login information. Participants should choose strong passwords, change them regularly, and avoid accessing retirement savings accounts using shared computers or open Wi-Fi networks.
- Protect laptops and other devices with encryption.
- Participants should be instructed to read plan-issued materials and keep their contact information up to date. Accurate contact information ensures they can be contacted as soon as possible in the event of a data breach so they can take immediate action.
- Consider consolidating retirement savings when changing jobs. Fewer open retirement saving accounts means reduced odds of exposure to a data breach.

Cyber threats are evolving and becoming more sophisticated every year. As such, plan sponsors must do their best to try to stay one step ahead of hackers by heightening their cybersecurity defenses to protect the personal information of participants and their beneficiaries.

Retirement plan fiduciaries can take proactive steps to help secure sensitive retirement plan data. The challenge for many is knowing where to start. We hope this article provided several key steps plan sponsors and retirement committees can take to boost their cybersecurity protections and fortify their plans against insidious cyber-attacks.

[1] Morgan, Steve. "Top 5 Cybersecurity Facts, Figures and Statistics for 2018." Jan. 2018.
[2] Oyedele, Akin. "BUFFETT: This is the number one problem with mankind." May 2017.
[3] Crowe, Jonathan. "10 Must-Know Cybersecurity Statistics for 2018." Feb. 2018.
[4] Morgan, Steve. "Cybercrime Damages $6 Trillion By 2021." Oct. 2018.