

## Publication

---

01/06/2023

### Cybersecurity Issues for Retirement Plans

Neal Gerber Eisenberg partners David Wheeler and Linda Hoseman discussed the biggest cybersecurity issues facing retirement plans and offered best practices for developing effective policies and procedures in a recent webinar.

Plan communications increasingly take place via electronic methods, and the plans themselves carry sensitive participant data – making them ripe targets for cyberattacks. As a result, the industry was clamoring for direction on cybersecurity. Plans were also seeking guidance on striking a balance between ease of access for participants and keeping plan assets safe, Hoseman said.

In April 2021, the Department of Labor (DOL) released cybersecurity best practices guidance for retirement plan sponsors and fiduciaries subject to the Employee Retirement Income Security Act of 1974 (ERISA) that outlined best practices for maintaining cybersecurity and protecting workers' retirement benefits, which Wheeler and Hoseman also discussed in the webinar.

#### What Should Fiduciaries Do?

Some questions remain around whether plan fiduciaries – broadly defined as any person who exercises discretionary authority over administration of a plan or its assets or a person who provides investment advice for compensation, whether direct or indirect – are liable as

---

#### CLIENT SERVICES

Labor & Employment

Compliance

Audits, Data Mapping & Asset Leveraging

Cybersecurity & Data Privacy

---

#### RELATED PEOPLE

Linda L. Hoseman

David A. Wheeler

fiduciaries for hacks of participant data. In any case, plan fiduciaries should strive to minimize the risk of cyberattacks by implementing cybersecurity protections to minimize the risk of cyber incidents that impact participants' financial and data assets, Wheeler and Hoseman said.

While retirement plans face the same types of cybersecurity risks that other industries face – identify theft, phishing, malware and ransomware – fiduciaries should take care because they could be found personally liable for a breach, Hoseman said.

While there is no way to eliminate all risk when it comes to cybersecurity, fiduciaries can manage and reduce risk – and fulfill their fiduciary duties – by developing strong processes and training policies for employees. Another benefit of having a good process in place is being able to use it as a defense in a fiduciary breach lawsuit if needed.

### **What Does the Process Look Like?**

Wheeler shared several best practices for plans looking to establish or revamp their cybersecurity policies and procedures.

Fiduciaries should take stock of what data they have, and from there, they can then develop a cybersecurity policy that includes frequent testing, updating and employee training, Wheeler said. Critically, plans should revisit and review policies frequently.

Any cybersecurity policy should also include an incident response plan that would apply if a breach does occur.

As part of breach preparations, Wheeler suggested fiduciaries conduct a risk assessment. However, Hoseman said this is an area where the DOL best practices guidance does not provide clear steps as to how that

assessment should be handled – but Hoseman suggests fiduciaries can borrow guidance from the Health Insurance Portability and Accountability Act (HIPAA), especially that law's breach notification process.

In the event of a breach, plans should follow HIPAA's guidance and assess the nature and extent of the data involved, such as the types of identifiers and the likelihood of re-identification, because bad actors could impersonate the people whose data was compromised.

Plans should try to identify the unauthorized person who used the data, or to whom the disclosure was made, whether the data was acquired or viewed and the extent to which the risk to the data use or disclosure has been mitigated.

### **Third-Party Vendors**

Working with third-party vendors can also pose major cybersecurity risks for plans. Hoseman said fiduciaries should develop procedures for working with vendors early in the hiring or RFP process and determine whether a vendor's cyber insurance will flow through to the fiduciary or whether the vendor will take on the notification process in the event of a breach.

Retirement plan advocacy organization SPARK Institute has developed strong standards for comparing third-party vendors, Wheeler said, and recommended that plans refer to those standards when engaging with them.

Another resource that plans can use when evaluating third-party vendors is the Systems and Organization Controls (SOC) 2 Report. For these reports, independent auditors assess the extent to which a vendor complies with the trust service principles based on the systems and processes they have in place.

The report addresses and defines the criteria for managing customer data based on five “trust service principles”:

- Security – firewalls, authentication, intrusion prevention and detection
- Availability – performance processing, disaster recovery and incident response
- Processing Integrity – processing monitoring and quality assurance
- Confidentiality – encryption and access controls
- Privacy – access control and access rights, disclosure restriction and retention

### **Best Practices and Prevention**

To prevent cybersecurity attacks and minimize risk, plans should review the DOL’s guidance discussed earlier in addition to the proposals from the 2016 ERISA Advisory Council’s report. These contain a strategy for plan fiduciaries that covers:

- understanding the plan’s data,
- developing security frameworks, both for inside and outside plan sponsor organizations, and
- keeping the process dynamic

Wheeler also encouraged plans to implement frequent training sessions to increase employees’ awareness of threats and attack attempts.

### **Looking Ahead**

In 2023, plan fiduciaries will have to navigate a patchwork of state privacy and cybersecurity laws. In the absence of federal cybersecurity and privacy regulation, state preemption issues are still evolving, so plans must



stay abreast of the laws applicable to the various jurisdictions in which they operate.

If you have any questions regarding cybersecurity and retirement plans, please contact David Wheeler, Linda Hoseman or your Neal Gerber Eisenberg attorney.

This version of the program recording does not qualify for CLE credit. To request the recording qualified for CLE credit, please contact [events@nge.com](mailto:events@nge.com).

*The content above is based on information current at the time of its publication and may not reflect the most recent developments or guidance. Neal, Gerber & Eisenberg LLP provides this content for general informational purposes only. It does not constitute legal advice and does not create an attorney-client relationship. You should seek advice from professional advisers with respect to your particular circumstances.*