PLAN SPONSOR
Digest

Issue 2, 2024 Your Challenge, Our Solutions™

Cybersecurity: Lessen the risks for plans and participants

In the last few months alone, major computer-hacking enterprises have been publicized. Hours before President Biden met with Ukrainian President Zelenskyy in December, Russian hackers disabled mobile phone access to 24 million customers and destroyed 10,000 computers and 4,000 servers. While some attacks make the news—and may even be sanctioned by foreign governments—the majority of cybersecurity incidents fly under the radar. There are actions that retirement plan administrators and plan participants can take to protect themselves from loss.

Employer Plans and IRAs could be attractive targets

"Because that's where the money is." That's what infamous criminal Willie Sutton replied when asked why he robbed banks. Following that logic, it makes sense that attempts would be made at retirement plan assets. According to the Congressional Research Service, by the end of 2022 nearly $38 trillion was held in U.S. employer-sponsored retirement plans and IRAs. Because this is where a lot of money is, these plans and accounts present an enticing target for criminal mischief.

But threats to plans and IRAs can come in many forms. Risks don't necessarily originate with well-organized crime cartels or expert hackers. Risks can also arise "opportunistically," for example, with a stolen or misplaced phone or with a relative who seizes a chance to exercise undue influence on a cognitively-compromised senior. Regardless of how money or data can be stolen, there are ways to stop it.

The Department of Labor offers some help

In April 2021 the Department of Labor (DOL) released three pieces of guidance to help plan administrators and individuals protect retirement plan assets. Although this isn't new, the concepts are still highly relevant. Even as methods to protect assets improve, the strategies to undermine these methods will also become more sophisticated. All of us should become familiar with steps we can take to shield ourselves from hackers. Here are some of the highlights of the DOL's cybersecurity guidance.

Tips for hiring a service provider

The first component of this three-part guidance helps employers and fiduciaries prudently select service providers with strong cybersecurity practices and monitor their activities. The Employee Retirement Income Security Act of 1974 requires this diligence, and these Tips for hiring a service provider give detailed information on how to meet this requirement.

Employers routinely rely on third-party service providers to administer various aspects of their retirement plans. This could include accountants,

Continued on page 2

Continued from page 1

recordkeepers, payroll processors, and others—including, perhaps a bit paradoxically, those who provide resources on cybersecurity. Unlike some governmental guidance, this DOL release is relatively short. Without covering all the tips, here are some that may resonate with plan sponsors.

- Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions. This may be where a reputable cybersecurity firm can help. They can identify recognized industry standards regarding, for example, information security and processing integrity.
- In any contract with a service provider, look for provisions that allow you to review audit results that demonstrate compliance with applicable industry standards. Keep in mind that, not only do you want to keep plan assets safe, but you also want to have some recourse if the provider fails to perform in ways that the contract provides.
- Related to having recourse, you should determine if the provider has adequate insurance coverage to cover losses caused by security breaches. Your compliance or legal advisors should also review insurance coverage—your own as well as your service providers'—to ensure that it meets your needs. Such coverage may include errors and omissions liability insurance, cyber liability and privacy breach insurance, and fidelity bond/ blanket crime coverage.

This guidance also contains a list of provisions that a contract with service providers should include, such as prompt notification of any security breaches, compliance with record retention and destruction standards, and obtaining an annual independent audit of the provider.

Cybersecurity program best practices

The DOL's second component, cybersecurity program best practices, is intended for "recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire." So not only should service providers implement these best practices, but employers should strongly consider using them to evaluate potential service providers. Here are just a few of the items that a sound cybersecurity program should include.

- Formal, well-documented processes – "A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information." The program should include detailed written procedures and standards that are:
  - Approved by senior leadership,
  - Reviewed at least annually (and updated as needed),
  - Effectively explained to users,
  - Reviewed by an independent auditor who confirms compliance, and
  - Documented to assess the security of the program's systems and practices.

Continued on page 3

Continued from page 2

The guidance lists numerous specific policies that should be addressed as part of the program.

- **Annual risk assessments and independent audits —** As security risks continually change, providers must design and adhere to an effective risk-management schedule. And having an independent auditor assess an organization's security controls "provides a clear, unbiased report of existing risks, vulnerabilities, and weaknesses."
- **Clearly defined and assigned information security roles and responsibilities —** Effective cybersecurity programs must be managed at the senior level and executed by qualified personnel.
- **Cybersecurity awareness training conducted at least annually for all personnel and updated to reflect risks identified by the most recent risk assessment —** This point emphasizes that employees are often an organization's weakest link for cybersecurity. An effective training program for employees will set clear expectations and will educate everyone to respond to a potential threat. As cumbersome and tedious as such training can sometimes be, it is critical in combatting identity theft and other fraudulent behavior.
- **Encryption of sensitive data stored and in transit —** A system should implement current, prudent standards for encryption keys, message authentication, and hashing to protect the confidentiality and integrity of the data at rest or in transit.

Online security tips

The last component focuses on retirement plan participants and on IRA owners (and their beneficiaries). Online security tips reminds individuals about basic rules to reduce the risk of fraud and loss to retirement accounts. Follow the link to get more details on implementing these tips.

- Register, set up, and routinely monitor your online account.
- Use strong and unique passwords.
- Use multi-factor authentication.
- Keep personal contact information current.
- Close or delete unused accounts.
- Be wary of free Wi-Fi.
- Beware of phishing attacks.
- Use antivirus software and keep apps and software current.
- Know how to report identity theft and cybersecurity incidents.

Maintaining cybersecurity is a constant challenge

Whether you are an employer, a service provider, or an account owner, security threats can appear without warning and from every imaginable angle. As long as "that's where the money is," you can expect that the bad guys will continue to use their "talents" to steal from others. But at least we have some helpful resources to thwart them and protect our assets.

Automatic enrollment may be required in 2025

A significant provision in the SECURE 2.0 Act of 2022 requires certain employers to adopt an automatic-enrollment feature in their 401(k) or 403(b) plan for the 2025 plan year. In its ongoing quest to increase the number of U.S. workers covered by an employer-sponsored retirement plan, Congress is requiring many employers to automatically sign up their employees for salary deferrals unless the employee opts out. Although this rule doesn't affect employers until the 2025 plan year, it's not too early to consider how this provision may affect you, if at all.

First, let's look at which employers are not affected by the new law. The employer will not have to automatically enroll employees in any of these situations.

- If a qualified cash or deferred arrangement (CODA) was in place before the enactment date of the SECURE 2.0 Act (which was December 29, 2022). Qualified CODAs include 401(k) and 403(b) plans.
- If the plan is a governmental or church plan.
- If the business has existed for less than three years.
- If the employer normally employs no more than 10 employees. (Employers will have to adopt an automatic-enrollment feature for the taxable year that begins one year after the close of the taxable year in which the 10-employee limit is exceeded.)

For those employers who must adopt an auto-enrollment feature in 2025, the following rules apply.

- The initial deferral amount must be at least 3% (and no more than 10%) and must increase by at least 1% each year until reaching 10%.
- The automatic increase is normally capped at 15%.
- The auto-enrollment component must be an eligible automatic contribution arrangement (EACA) and must allow for permissible withdrawals.
- Participants may make an affirmative election to defer more or less than the default percentage, or to opt out entirely.
- Participants who do not make an investment election must have their contributions invested in a manner consistent with the DOL's rules for qualified default investment alternatives (QDIAs).

Automatic-enrollment plans are good for employees, and they can be good for employers, as well. Credible studies find that default enrollment increases overall participation and that auto-increases tend to "stick." That is, employees do not generally object to (or reverse) the increased deferrals that apply to their wages. But while this feature can benefit employees and employers alike, they do require additional administration. Employers who must comply with this provision in 2025 may wish to work with their recordkeepers or third party administrators to prepare for it now rather than waiting until the eleventh hour.

24-20-00929_20181-CC (04/24)