Protecting your plan

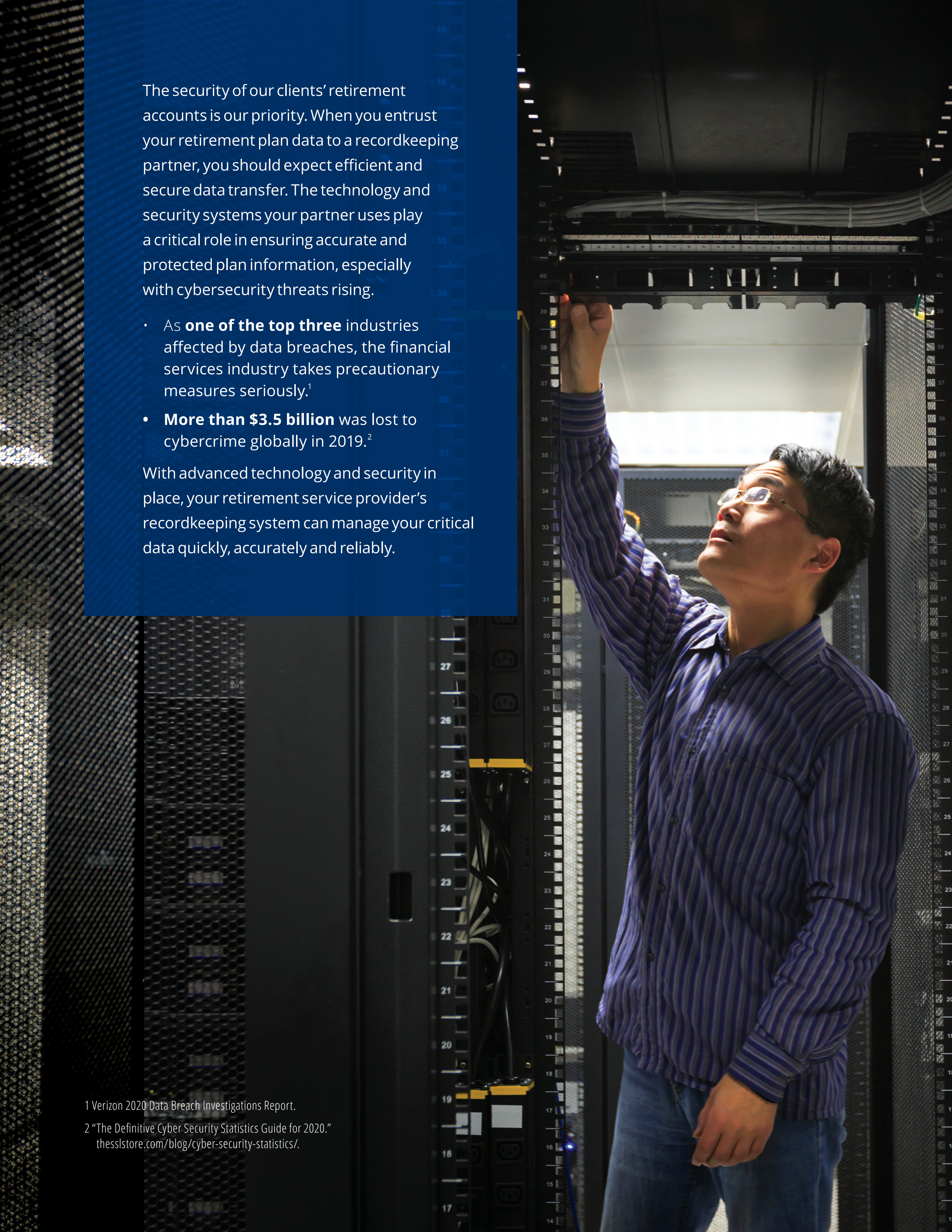
Leveraging recordkeeping technology to maximize security

EMPOWER RETIREMENT®

The security of our clients' retirement accounts is our priority. When you entrust your retirement plan data to a recordkeeping partner, you should expect efficient and secure data transfer. The technology and security systems your partner uses play a critical role in ensuring accurate and protected plan information, especially with cybersecurity threats rising.

- As **one of the top three** industries affected by data breaches, the financial services industry takes precautionary measures seriously.[1]
- **More than $3.5 billion** was lost to cybercrime globally in 2019.[2]

With advanced technology and security in place, your retirement service provider's recordkeeping system can manage your critical data quickly, accurately and reliably.



[1] Verizon 2020 Data Breach Investigations Report.

[2] "The Definitive Cyber Security Statistics Guide for 2020." thesslstore.com/blog/cyber-security-statistics/.

Not all systems and technology platforms are created equal

A recordkeeping system's technological and security capabilities are critical, and when they function as expected, you can focus on your core business — worry free.

The right technology platform can create efficiencies and maximize effectiveness through three foundational requirements:

- **Speed**
- **Accuracy**
- **Reliability**

As you begin your due diligence and evaluations of potential recordkeeping partners, you can determine whether those core requirements can be met by asking these important questions:

- Does your recordkeeping partner have full control of its recordkeeping system, or is it reliant on others?
- Does the recordkeeping system use a multiple- or single-system environment?
- Are the trust and recordkeeping systems separate or integrated?
- Is your sensitive data protected with proven authentication and encryption technology within a secured environment?

Once you have these answers — and know that your partner has a sole focus on recordkeeping and verified data security protocols — you can make your choice with confidence.

Why a systems and technology platform matters

While speed, accuracy and reliability are universally positive attributes of any system and technology platform, they are especially important in a recordkeeping environment because providers must be able to:

- React and respond quickly to policy and regulatory changes.
- Avoid errors that could compromise personal participant data.
- Proactively protect against cybersecurity threats.

The system and technology that a retirement service provider has in place can strongly influence how well they are able to meet their obligations in those and other areas of importance. For instance, if a provider owns and controls its own platform, it can eliminate the need to wait on third parties, which means upgrades and enhancements can happen in a more timely fashion.

Enhancing a technology platform with cloud enablement helps businesses better manage data, and using automation further improves resiliency, speed, scalability and accuracy.

We believe there are certain other attributes that have — for the most part — become a ticket to play; any providers should be able to check these boxes. A couple examples include operating a server-based environment as opposed to an outdated mainframe system and having real-time transaction functionality rather than using a potentially slower batch-processing method.

But that only scratches the surface in terms of how you should evaluate a retirement provider's systems and technology platform to determine the best choice for your specific plan needs.

The integration advantage

Retirement service providers generally offer both traditional participant recordkeeping and trust account recordkeeping. If this applies to your plan, it's important to understand how the two work together.

With an integrated system, you may gain advantages because it:

- More easily reconciles recordkeeping and trust data.
- Minimizes issues related to out-of-balance scenarios.
- Provides an opportunity for added customization.
- Unifies and completes reporting for you.

If a provider is operating separate systems, speed, accuracy and reliability can be compromised as there can be:

- An increased chance of you having to spend more time and resources on the administration of your plan due to difficulties in producing consolidated reporting.
- A greater risk for errors related to reconciliation and more potential for out-of-balance scenarios to occur.
- Less of a likelihood that you can count on any customization during the onboarding process.

SECURITY THREAT ⚠

Separate systems can create additional data transfer endpoints — all of which must be secured against a breach

A single-system solution

It is important to understand the differences between multiple-system and single-system environments. With a single system you can:

- Benefit from easier transaction processes.
- Increase speed and efficiency.
- Improve your experience with information views via a single source.
- Invest in new features, such as cloud enablement, rather than in maintenance.
- Reduce delivery time for enhancements.

According to PLANSPONSOR, seven of the 12 largest recordkeepers have not integrated their platforms after acquiring or merging with other providers. When a provider operates through multiple systems, it can create the potential to negatively impact speed, accuracy and reliability:

- Exposure to more systems can lead to greater risk of errors, and a breakdown of one system may affect the entire chain of systems.
- The speed at which you can access information across many systems may be affected due to the difficulties and complexities inherent in a multi-system environment.
- Your provider may not be able to meet your expectations in terms of platform upgrades due to complexities and expense, and you may not benefit from investment in innovation because of high maintenance costs.

SECURITY THREAT

Multiple systems connected to your network create multiple entry points for cybercriminals

Size and scale

As part of your due diligence, it's important to consider a system's size — specifically, its processes, capabilities and ability to grow with your business. The size of the recordkeeping organization with which you partner may also influence data delivery speed and data security strength.

You'll want to choose a partner that is large enough to offer economies of scale while providing performance and efficiency to your business. Additionally, you want a partner that can afford a comprehensive security program and has the agility and flexibility to respond to changing security requirements.

To help you determine whether your prospective partner offers the size and scale to support your plan, look at the following areas as indicative measures:

- The talent and knowledge of its system's professionals
- A chief information security officer (CISO) along with clear security policies and education in place and dedicated plans for:
  - — Information security
  - — Business continuity
  - — Compliance and risk

Security

When it comes to cybersecurity, complexity is the enemy. That's why it's important to ensure that recordkeeping is your partner's core business and not a sideline. When recordkeeping is the foundation of everything a partner does, you can expect that its investments in technology and innovation are designed specifically for the recordkeeping function. A singular focus allows for fortified protection against vulnerabilities and security threats.

Independent security assessments are a good way for organizations to confirm the status of their controls at time of testing. Some of these assessments result in security certifications, which can provide you with greater confidence regarding your recordkeeper's data protection capabilities. It's important to understand the certification and the scope of the organization's systems or services covered by the certification.

A comprehensive defense-in-depth strategy begins with a foundation of security controls to guard against external threats and vulnerabilities. Verification of controls is validated through rigorous testing of control objectives identified within the scope of SOC 1 and SOC 2 reports.

AICPA SOC 2 Type I and Type II security reports are the most frequently requested proof of compliance and security program thoroughness among prospective and existing clients. SOC 2 reports or ISO 27001 certification represent parts of a defense-in-depth information security program and are "close cousins" as they share 96% of the same controls. Unlike a single-page ISO 27001 certification, a SOC 2 report details information regarding the scope of the environment and assets tested, test output with quantities of issues noted by the audit firm, and management remediation plans.

Our SOC 2 report is evidence of our adherence to controls and shows our commitment to protecting data. Both compliance controls and security testing are necessary parts of a comprehensive information security risk-reduction program. Their primary function is to reduce the amount of risk that an organization faces.

Cybersecurity has evolved and modern protection is critical. When you entrust your retirement plan data to your recordkeeping partner, efficiencies and secure data transfer should be expected. Third-party verification of information security is recommended, and having a recordkeeper with a security guarantee is critical to keep plan sponsor and participant account information safe and secure. Security guarantees typically include that a company will restore losses from your account that occur as a result of unauthorized transactions through no fault of the plan sponsor.

But the fact remains that cybersecurity threats are constantly evolving, and it's critical to find a partner committed to staying ahead of such threats. Investigating the following questions can assist in finding a partner whose cybersecurity protocols can help keep plan and participant information and assets safe:

- Are the organization's security protocols regularly tested and verified by a trusted, independent third party?
- Does the organization offer a security guarantee to protect assets from unauthorized transactions?
- Is the organization engaged in business activities other than retirement plan recordkeeping?

The answers to these questions can be crucial in determining whether a prospective partner maintains the appropriate level of data protection, risk management and cybersecurity safeguards to meet your needs.

The security of your retirement plan's accounts is our priority. We value your business and your trust in choosing Empower Retirement. As your trusted partner, we stand behind our online and mobile security with the Empower Retirement Security Guarantee.

This guarantee states we will restore losses to your account that occur as a result of unauthorized transactions through no fault of your own.

RELIABILITY RISK

Ask prospective providers if they have system redundancies at alternate sites to help ensure business continuity in the event that the primary site is slowed or disabled

Questions to ask

About technology

Make sure the providers that you evaluate can offer the essential information you need when they answer these questions:

- Describe your underlying system. Is it mainframe based or server based?
- How often are updates and enhancements made to your recordkeeping system?
- Does your system update using batch processing or real-time functionality?
- Do you have networking and application monitoring systems in place?
- How do you pass encrypted files?
- Do you transmit and store passwords and passcodes in an encrypted format?
- How are your systems integrated?
- Do you use next-generation firewall technology to protect your network?
- Can you provide a description of your firm's data security systems?
- Which compliance audits and third-party security assessments do you use to test your security program and reduce risk?
- Do you have a plan in place for resiliency that accommodates significant spikes in web traffic?

About data

As you look more closely at data security, make sure the providers in consideration can effectively respond to these critical questions:

- Do you have solid processes around patching, anti-virus and anti-malware that are effectively designed and effectively operating?
- Have you implemented strong encryption in the appropriate areas for data both in motion and at rest?
- Do you have a robust data loss-prevention program in place?

About security

- Do you have mature controls against threats within all the following functions: identify, protect, detect, respond and recover?
- Do you have a strong security training program for your employees and users?
- Are there strong authentication practices in place for privileged users?
- Do you conduct independent assessments to confirm your security posture?
- How do you manage attempted data breaches?
- What are your disaster recovery and business continuity plans?
- Can your organization's security program easily adapt to change?
- Is your commitment to protecting data reinforced by a formal security guarantee?
- How is your firm investing in cloud technology — and what advantages and account-holder protections are being pursued?

Best practices for plan sponsors

- Provide your recordkeeper with accurate, up-to-date contact information for your participants.
- Set up forced Transport Layer Security (TLS) with your recordkeeper and other third parties with whom you send/receive sensitive emails.
- Set up IP safelisting.
- Provide security awareness training.
- Have an ongoing phishing program.
- Ensure your recordkeeper is in your Incident Response Plan.
- Share information about any compromises with your security team.
- Share information about any compromises of your participants' identity.

Best practices for personal account protection

At a minimum

- Register and claim your account.
- Provide all available emails and phones.
- Create a strong, unique password.
- Use multi-factor authentication.
- Monitor your account.

Better

- Turn on auto-updates.
- Watch out for phishing.
- Review your credit reports.
- Freeze your credit.
- Use a password manager.

Best

- Do not "remember this device."
- "Lock down" your account.
- Avoid oversharing online.
- Store and transfer data cautiously.
- Eliminate the paper trail.

For more information, please contact your Empower Retirement representative

FOR PLAN SPONSOR AND FINANCIAL PROFESSIONAL USE ONLY.

The charts, graphs, screen prints and examples contained in these materials are for ILLUSTRATIVE PURPOSES ONLY.

The research, views and opinions contained in these materials are intended to be educational, may not be suitable for all investors and are not tax, legal, accounting or investment advice. Readers are advised to seek their own tax, legal, accounting and investment advice from competent professionals. Information contained herein is believed to be accurate at the time of publication; however, it may be impacted by changes in the tax, legal, regulatory or investing environment.

Securities offered and/or distributed by GWFS Equities, Inc., Member FINRA/SIPC. GWFS is an affiliate of Empower Retirement, LLC; Great-West Funds, Inc.; and registered investment adviser, Advised Assets Group, LLC. This material is for informational purposes only and is not intended to provide investment, legal or tax recommendations or advice.

Unless otherwise noted: Not a Deposit | Not FDIC Insured | Not Bank Guaranteed | Funds May Lose Value | Not Insured by Any Federal Government Agency