The Beacon

LOCKTON® RETIREMENT SERVICES

CYBER SECURITY AND YOUR RETIREMENT PLAN: BEST PRACTICES FOR ERISA FIDUCIARIES

AUTHORS

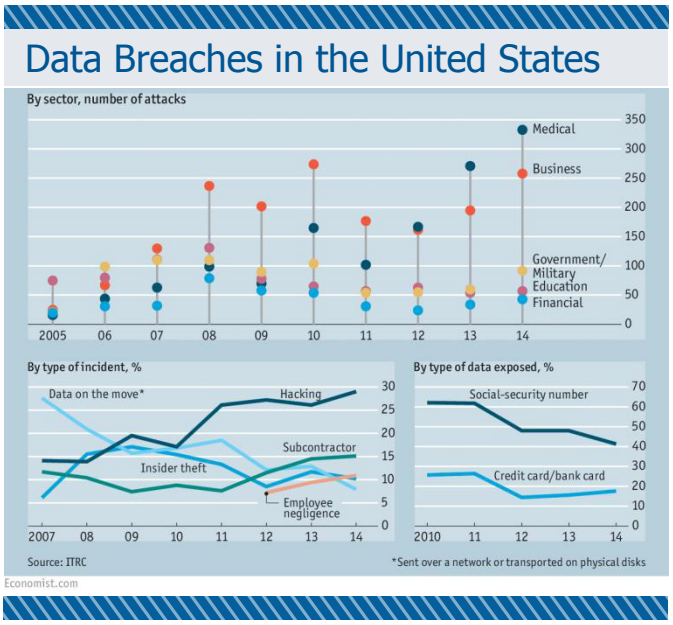
SAMUEL A. HENSON, JD
Vice President
Director,
Legislative & Regulatory Affairs

RICK UNSER, AIF, QPFC, CRPS
Vice President
ERISA Risk Management
Consultant

As if retirement plan fiduciaries didn't have enough on their plates, now the risk of potential cyber-attacks means that plan data security must become a key fiduciary focus. The more information technology becomes integrated into retirement plan operations, the greater the risk that sophisticated cyber-attacks will exploit vulnerabilities and cause wide scale or high-consequence events and harm or disrupt services. When that happens, what fiduciary exposure would you have?

A Growing Threat

Cyberspace is particularly challenging to secure. Criminals can operate from anywhere in the world, cyberspace connects to most physical systems, and the management of vulnerabilities in complex networks is increasingly difficult. Experts predict there will be 6.8 billion connected devices in use this year, a 30 percent increase over 2015[1]. By 2020, that number will jump to more than 20 billion connected devices[2]. For every human being on the planet, there will be between two and three connected devices. The system is growing so rapidly that the ability to identify threats is lagging severely behind. On average the time between an attack and the data owner noticing it is 205 days[3]. Juniper research predicts that the rapid digitization of consumers' lives and enterprise records will increase the global cost of data breaches to $2.1 trillion by 2019, nearly four times the estimated cost of breaches in 2015[4].



[1] http://www.gartner.com/newsroom/id/3165317
[2] Id.
[3] http://www.economist.com/news/business/21677639-business-protecting-against-computer-hacking-booming-cost-immaturity
[4] http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Retirement Plans Are a Huge Target

In 1974, the year that ERISA was enacted, retirement plans operated with paper and pencil recordkeeping, fax machines were state of the art, and the internet was something out of a science fiction novel. Today, the retirement plan experience is almost entirely digital. That, combined with the nearly $17 trillion dollars held in employer sponsored retirement plans in America, makes the system a prime target for cyber-attacks[5]. The increased use of the internet to conduct financial transactions has also increased the opportunities for fraud and other financial crimes. Generally speaking, the threat can be quantified into two categories:

- Theft of retirement savings from accounts.
- Theft of personally identifiable information (PII) and data.

The Department of Labor has never issued formal guidance on how ERISA's fiduciary requirements apply to the protection of PII, the remediation of security breaches, or the preservation of plan administration integrity. That doesn't mean that no such fiduciary obligation exists.

Practical Steps for Fiduciaries

ERISA requires plan fiduciaries to act prudently in the plan participants' best interests. In addition, ERISA gives plan sponsors the duty to monitor service providers. These duties require consideration of all stakeholders who share, access, store, maintain and use PII. That list is long and includes participants, plan sponsors, plan administrators, third party administrators (TPAs), record keepers, investment advisors, other service providers, trustees and other fiduciaries. Issues to be considered include privacy policies which address who may have access to PII, procedures for disseminating information concerning PII security breaches, and remediation practices when breaches result in financial harm to plan participants and/or beneficiaries. To help get your arms around the cyber security policies of your retirement service providers below are a few questions that will help start your cyber due diligence:

- Describe your corporate culture relating to cyber security. Please include a description of any management or executive roles that are involved.
- Describe your information security policy?
- Describe your privacy policy?
- Do you use encryption to secure Personally Identifiable Information (PII). If yes, please describe.
- Do you use Multi-factor Authentication (MFA) to determine who has access to sensitive data? If yes, please describe.
- Do you have a regular penetration test to examine the resilience of your network and systems? If yes, please describe.
- What is your company's policy about storing PII on laptops or removable devices?
- How does your service agreement or contract address cyber liability and/or privacy breaches?

[5] https://www.ici.org/research/stats/retirement.

- Do you have a data breach incident response plan?
- Do you purchase cyber insurance?

As the world of cyber risk is broad and quickly evolving this list of questions is not meant to be definitive, but a good starting point for your process.

Be Proactive

Advisors and service providers can prepare strategies to not only help fiduciaries protect plan assets, but also mitigate the risk of harm from potential attacks. Secure participant access programs, data collection policies, employee training, and service provider contract negotiations form the basis for these strategies. In addition, insurance may mitigate much of the costs associated with a breach. As retirement plans continue to embrace technology in pursuit of enhanced sponsor and participant experiences, cyber risks will continue to increase. While it's unlikely that any fiduciary can fully insulate itself, implementing the appropriate security measures can significantly mitigate risks.

LOCKTON®

www.lockton.com