Checklist for Managing Cyber Risk in Retirement Plans

RETIREMENT INSIGHT SERIES

Key points to consider to implement a prudent process

Plan fiduciaries should have cyber protocols in place, before any breach occurs. Given the rise in cyberattacks, fiduciaries who fail to take prudent action to protect data and assets may be exposed to considerable risk. Service providers should also have an efficient way to provide plan sponsors with the assurance of cybersecurity best practices. Although there is not a single solution for cyber protection, there are a number of industry best practices to consider implementing to create effective safe guards.

Common Cyberattack Strategies

	What it is	This is really happening
Ransomware attacks	Criminals encrypt a hard drive for ransom	Usually spread by clicking on an infected e-mail attachment, using infected software apps or external storage devices, or visiting a malicious web site
Phishing attacks	Seeking user interaction to infiltrate a network	Uses e-mail, instant messages or text messages that appear to come from reputable sources to steal sensitive information or contains links to web sites that distribute malware
Wire transfer e-mail fraud	Imposters pose as senior executives requesting wire transfers	Uses an e-mail address that appears very similar to a trusted e-mail and requests fund transfers (e.g., a hacker determines jill.smith@email.com is a trusted e-mail address and sends from jill.smith@email.com)
Malware	Harmful software migrates to a network when an external/ thumb drive is inserted	Can plant a keystroke tracker that captures IDs and passwords, as they are being typed
Plan data theft	Theft of plan data, rather than direct plan funds	Stolen PII can be used to obtain fraudulent loans, etc.
AICPA fraud findings	AICPA published a list of 45 actual fraud cases to improve audit quality	Cases include plan sponsor and recordkeeper insiders: • Skimming from distributions • Creation of fake participants for benefit allocations and subsequent distributions • Payment of personal credit card from forfeitures • Tampering with contribution allocations to redirect to a personal account • Redirection of investment earnings into own account balance

Cybersecurity Checklist

Understanding these key elements can help plan sponsors develop a cybersecurity risk management process.

Data management	• Conduct regular and periodic (such as annual) in-depth assessments of risks • Ask what data is held? How? Which ways can data be accessed? How is data transferred? Can unrelated parties disrupt the data flow? • Create strategies to prevent, detect, and respond to threats • Consider using a cybersecurity expert • Measure progress • Test compliance
Threat assessment	• Conduct regular and periodic (e.g., annual) assessments of risks • Consider the nature and sensitivity of data and technology • Understand how and where data is stored and for how long • Determine internal and external threats • Ensure controls are in place • Evaluate potential impact of a data compromise • Review effectiveness of the structure to manage cybersecurity risk
Defense design	• Create strategies to prevent, detect, and respond to threats • Evaluate data and consider a "data diet" that collects/shares only essential data • Design access controls through multiple levels, including credentials, authentication, authorization, firewalls, perimeter defenses, tiered access, and system hardening • Utilize data encryption and restrict/eliminate use of removable storage data • Install software to monitor intrusions, loss, or export of data and ensure data backup and retrieval • Develop an incident response plan • Consider a third-party framework, such as the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Health Information Trust Alliance (HITrust), and the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY)
Effective implementation	• Implement and monitor the process with procedures and periodic testing, including any software and hardware installation and management • Document the process with formal written policies and periodic reporting, as well as training for all officers and employees

(continues)

Cybersecurity Checklist (continued)

Service provider evaluation	• Define security obligations in service agreements, including how the provider will share threat information • Ask about SPARK best practice compliance • RFPs should look for SPARK certifications, consider service providers whose cybersecurity policies and procedures have been vetted and awarded a SAFETY ACT designation or certification, and require SOC 2 audit results • Establish vetting procedures that include information about the provider's cybersecurity plan, who oversees it, what breaches have occurred, and responses • Ensure automatic notification and audit obligations
Trustee and custodian Sheltered Harbor participation	• An industry-driven consumer protection strategy against significant cyber risk that establishes standards and monitors adherence to promote enhanced resiliency of consumer banking accounts • Banks serving as trustees and custodians may be members
Insurance	• Review policies for insurance coverage of a cyber breach – existing fiduciary coverage may not be enough (more than 60 carriers offer standalone cyber insurance policies) • Identify potential gaps in traditional insurance for damages and litigation fees, costs for responding to cyber threats, and reimbursement of lost revenues • Remember that cyber insurance should trigger coverage at the first sign of a breach (first-party coverage)

Keep the dialogue going. Discuss strategies for managing cyber risk with your plan advisor and service providers.

1. Listen actively. Note concerns for follow up.
2. Engage your network. Reach out to learn what others are doing to protect their plan data and plan assets.
3. Share intelligence.

INVESTMENTS

For more information

Defined Contribution Investment Only (DCIO)
877-742-6951, option 1
nylinvestments.com/dcio

1778624 IIB031-19 IIB38i-08/19