4 Proactive Measures for Ensuring Pension Plan Cybersecurity

INTRODUCTION

As pension plans increasingly move to digital technology for their integrated pension administration systems, the need to prioritize cybersecurity and protect plan assets and beneficiaries becomes paramount. Pension plans deal with significant amounts of confidential data, making them attractive targets for cybercriminals. Pension administrators are expected to be proactive in recognizing, preventing, and minimizing the impact of cyber risks. This INSIGHT explores practical measures that plan administrators can take to enhance protection against cyber risks for pension plan assets and beneficiaries.

WHAT IS CYBER RISK?

Cyber risk refers to the potential financial loss, operational disruption, or reputational damage resulting from unauthorized access, malicious use, failure, disclosure, disruption, modification, or destruction of information technology systems, infrastructure, or data. Examples of cyber risks include hacking, malicious software, phishing emails, social engineering, and inadvertent information disclosure. Both internal and external risks pose a threat to pension plan administrators and their third-party service providers – including actuaries, IT consultants, and payroll providers.

PROACTIVE MEASURES FOR CYBER RISK MANAGEMENT

Mitigating pension plan cyber risk requires the following four proactive measures:

1. Pension and Cyber Risk Governance

Pension plan administrators should incorporate the management and monitoring of cyber risk into their governance and risk frameworks. This involves integrating measures into pension governance policies and terms of reference, including cybersecurity training for pension committee members. Administrators should familiarize themselves with industry-accepted practices for plan governance and cyber risk, establishing an ongoing process to identify educational requirements and necessary skills. Plan administrators should ensure they have up-to-date hardware and software, employ information technology expertise, develop best practices, and regularly monitor systems and networks for unusual activity or unauthorized access.

2. Well-Defined Roles and Responsibilities

Clear roles and responsibilities related to cyber risk should be defined within the pension governance policies and risk framework. This includes identifying key stakeholders, such as the plan sponsor and third-party service providers, and describing their roles, responsibilities, and accountabilities in managing cyber risk.

3. Cybersecurity Provisions in Third-Party Service Contracts

Plan administrators should be aware of the cyber risks associated with using third-party service providers and ensure that suitable cybersecurity provisions are included in service contracts. These provisions should align with the plan administrator's risk mitigation objectives and address the provider's cyber security policies.[1]

4. Cyber Insurance

Purchasing cyber insurance is a proactive measure that helps minimize financial loss in the event of a cyber incident. Insurers should communicate openly with the insurer to understand the scope of coverage and any exclusions. It is important to have a clear understanding of the risks to be insured and implement commensurate security protocols.

REACTIVE MEASURES FOR CYBER RISK MANAGEMENT

In addition to proactive measures, pension plan administrators should have strategies in place to respond to and report cyber incidents. This includes developing an incident response or resiliency plan to swiftly address incidents and restore business capabilities. It is crucial to identify and assess the sensitivity of personal information involved, the population affected, and the probability of misuse to determine the severity of a cyber incident. Administrators should establish clear reporting processes for notifying plan beneficiaries, regulators, and other relevant parties about cyber incidents, ensuring transparency, and taking appropriate action to mitigate the impact.

CONCLUSION

In an increasingly digital landscape, pension plan administrators must prioritize cybersecurity to protect plan assets and beneficiaries. Implementing proactive measures such as protective controls, pension and cyber risk governance, well-defined roles and responsibilities, cybersecurity provisions in contracts, and cyber insurance can enhance protection against cyber risks. Additionally, having reactive measures like incident response plans and effective reporting procedures ensures swift and effective action in the event of a cyber incident. By continuously reviewing and updating their approach to cyber risk, pension plan administrators can effectively safeguard pension plan assets and members' interests in the digital age.

ABOUT VITECH

Vitech is a global provider of cloud-native benefits and investment administration software. We help our Insurance, Retirement, and Investment clients expand their offerings and capabilities, streamline their operations, gain analytical insights, and transform their engagement models. Vitech employs over 1,400 professionals, serving the world's most successful insurance, retirement, and investment organizations. An innovator and visionary, Vitech's market leadership has been recognized by industry experts, such as Gartner, Celent, Aite-Novarica, and ISG. For more information, please visit vitechinc.com.

1 Ashley Dunning, Michelle McCarthy, "Cybersecurity Risk Management for Pension Plan Administrators: Tips for Staying Ahead of the Hackers," Nossaman LLP, August 2, 2023, https://www.nossaman.com/podcast-public-pensions-investments-briefings/