INSIGHT

Building Digital Security for Public Pension Systems

INTRODUCTION

Today's roughly 6,000 U.S. public pension systems play a vital role in helping millions of active (working) members and retirees build wealth and long-term retirement security[1]. As the pool of retirees increases due to the current trend of baby boomers leaving the workforce, pension systems have been replacing their legacy platforms with modern public administration systems (PAS) to support robust member self-service, advanced CRM, and targeted member campaign management. However, pension systems' increased digital footprint and significant assets ($4.5 trillion, with $323 billion in annual benefit distributions)[2] have made them attractive targets for cyberattacks as well as identity fraud. In this Insight, we explore the benefits of public pension systems' enhanced member self-service for their growing constituencies, in conjunction with digital security protocols for comprehensive cybercrime management.

MEMBER SELF-SERVICE BENEFITS

One of the most necessary and visible benefits of pension systems' digital transformation is the enhanced member self-service resulting from next-generation PAS. Omnichannel member self-service puts administrative capability into the hands of plan members and other constituents for 24/7 servicing. It also empowers members to take charge of their account administration and makes them more proactive about their retirement planning, freeing system staff to tend to more important tasks and greater vocational development.

Another value proposition of member self-service is an advanced member experience, which provides members with more personalized engagement throughout their digital journeys. These experiences can include improved account viewing, end-to-end encryption for secure email, and other features for seamless interaction, which ensure that members get the most appropriate advice, answer, or product.

MEMBER SELF-SERVICE SECURITY CHALLENGES

The proliferation of member self-service as well as the migration of members and administrators to remote work due to the pandemic has presented cybercriminals with additional opportunities to commit fraud and cyber theft. Pension administrators need to closely monitor and improve their online defenses while evaluating existing solutions to either upgrade or replace them. This includes prioritizing technologies to balance comprehensive fraud management and an intuitive experience for users.

The shift to a larger online presence for member registration and account interaction made it easier for bad actors to create fake identities and perpetrate crimes. To fully manage fraud, pension administrators must remain alert to suspicious activity and consistently improve existing measures by bolstering current defenses or developing effective alternatives. Modern PAS platforms must provide enhanced auditing capabilities and intelligence in helping administrators monitor account activity.

PENSION CYBER THEFT SPECIFICS

Pension security breaches have most often resulted from staff and member email accounts being compromised. Other widespread forms of cyber theft include phishing and ransomware attacks. A common approach by cybercriminals starts with a simple phishing email that results in a pension administrator acting on the "request," leading to a compromise of member account information.[3] This opens the door to fund theft, as well as ransomware incidents.

Another security concern specific to pension funds is their reliance on external partners – including actuaries, IT consultants, and payroll providers – that can leave pension systems vulnerable to multiple lines of attack and member identity fraud. Identity fraud overall reached extremely high levels in 2021, with $56 billion stolen from roughly 49 million consumers.[4] The ongoing pandemic also contributed to the increase in incidents, as thieves exploited new vulnerabilities presented by remote transactions.[5]

EFFECTIVE PREVENTION

Today's public pension systems need to implement effective identity verification (IDV) while maintaining the enhanced, omnichannel member experience. The National Institute of Standards and Technology (NIST) has provided guidelines in managing three levels of digital identity to prevent fraud:

- Level 1 (IAL1): There is no requirement to link the member to a specific real-life identity. Any attributes provided in conjunction with the member's activities are self-asserted, or should be treated as self-asserted including attributes Credential Service Providers (CSPs) assert to a Relying Party (RP). Self-asserted attributes are neither validated nor verified.
- Level 2 (IAL2): Evidence supports the real-world existence of the claimed identity and verifies that the member is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing. Attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL2 can support IAL1 transactions if the member consents.
- Level 3 (IAL3): Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained CSP representative. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL3 can support IAL1 and IAL2 identity attributes if the user consents.

A suitable standard from the three NIST levels should be adopted based on the risk to the member account. Multifactor identification (involving individual members' username and password, token, or authenticator app, and even biometrics), device and location verification, and voice and keyboard analytics are some of the authentication technologies that pension administrators must deploy. For absolute security, pension systems must establish a dynamic digital identity protocol with four key capabilities – an identity-based representation, secure resource access, continuous trust evaluation, and adaptive access control.

Although public pension administrations have made considerable progress in upgrading their security measures, additional efforts are still necessary to strengthen the "middle layer" of pension system technology architecture (i.e., the layer used to integrate front-end and back-end applications). Other unique challenges for pension system cybersecurity include legacy systems that still require upgrades to become compatible with modern security solutions, limited resource allocations for advanced security applications, and plan trustee buy-in for major security overhauls and expenditures.

CONCLUSION

Public pension systems' online self-service continues to evolve, and this evolution should accelerate as member rolls further expand. While intuitive omnichannel self-service remains the gold standard for pension systems, it must be developed in tandem with impenetrable cybersecurity to repel bad actors and foil potential attacks. Balancing members' heightened digital experience expectations with cybersecurity threats needs to be a standard practice among system administrators, to secure public pensions systems for a future-focused digital age.

ABOUT VITECH

Vitech is a global provider of cloud-native benefit 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 1,600 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] U.S. Census Bureau Data, Public Plans Data, December 2021
[2] Ibid.
[3] "Phishing and Ransomware Risks on the Rise for Pension Funds, Says Expert," Benefits Canada, Sept. 2, 2021
[4] "Total Identity Fraud Losses Soar to $56 Billion in 2020," 2021 Identity Fraud Study, Javelin Strategy & Research, March 23, 2021
[5] Ibid.