Public pension systems undertake a tremendous fiduciary duty

Retirement systems acknowledge security upgrades are needed

Better identity management improves both security and service

There is a better way to secure state and local government employees’ personal information before it is compromised

Better identity management improves both security and service

Rather than leaving government employees’ information susceptible to breaches in outdated systems, it is imperative for program leadership to identify and mitigate the potential for account takeovers. A multi-pronged approach to securing state and local retirement systems is essential, and should incorporate these five factors:

1. Review and refresh security standards
   Incorporate low tech elements such as training, mandatory password updates, and multi-factor authentication.

2. Access and analyze “fresher” data
   Ensure members update their profiles regularly for accuracy, including addresses and other contact information, linked accounts, beneficiaries and login challenge questions.

3. Ensure digital identity across all channels and devices
   Consider all endpoints, from desktop PCs to mobile devices to landline phones, so that no matter how a member chooses to interact with the system, they can be clearly identified.

4. Leverage technology and security expertise
   Use updated technology to monitor and manage systems and data across your enterprise.

5. Balance security with fluidity
   Be flexible and ready to adjust to the unique needs of a broad demographic of members. A digital native may be used to online tools but a retiree may feel more comfortable with a phone call.

In the U.S., there are:

62 State-level Pension Funds

Nearly 21 million government employees use these systems

With a total of more than $4 trillion in state-administered and local-administered government pension plans

More than 5,500 local funds

19% of total retirement savings assets in the U.S. are in state and local government pensions

At least half of the public retirement systems are at risk

LexisNexis® Risk Solutions surveyed the Retirement Systems Directors, Managers, CIOs and CTOs responsible for protecting state employees’ PII from cyber threats and breaches*

Many systems are older and in need of non-intrusive security upgrades

40% of those surveyed said they upgraded their systems in the last year

50% said that their retirement systems do not require multi-factor authentication for login

50% said they never require their members to change passwords

93% of respondents said it is important for state and local retirement systems to evaluate identities through a multi-faceted identity assessment process

50% said they require their members to change passwords

50% said that their retirement systems do not require multi-factor authentication for login.

There is a better way to secure state and local government employees’ personal information before it is compromised

There is a better way to secure state and local government employees’ personal information before it is compromised

Better identity management improves both security and service

Rather than leaving government employees’ information susceptible to breaches in outdated systems, it is imperative for program leadership to identify and mitigate the potential for account takeovers. A multi-pronged approach to securing state and local retirement systems is essential, and should incorporate these five factors:

1. Review and refresh security standards
   Incorporate low tech elements such as training, mandatory password updates, and multi-factor authentication.

2. Access and analyze “fresher” data
   Ensure members update their profiles regularly for accuracy, including addresses and other contact information, linked accounts, beneficiaries and login challenge questions.

3. Ensure digital identity across all channels and devices
   Consider all endpoints, from desktop PCs to mobile devices to landline phones, so that no matter how a member chooses to interact with the system, they can be clearly identified.

4. Leverage technology and security expertise
   Use updated technology to monitor and manage systems and data across your enterprise.

5. Balance security with fluidity
   Be flexible and ready to adjust to the unique needs of a broad demographic of members. A digital native may be used to online tools but a retiree may feel more comfortable with a phone call.

For more information, call 888.579.7638 or visit risk.lexisnexis.com/government

---

*Survey results from 2019

1 https://en.m.wikipedia.org/wiki/Public_employee_pension_plans_in_the_United_States
3 Ibid
4 Ibid
5 Ibid

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX.

Copyright © 2022 LexisNexis Risk Solutions. NXR14097-01-0322-EN-US