State and Local Government Retirement Systems Are Under Cyber Threat

In the rapidly evolving cyber threat landscape, public pension plans are more susceptible than ever to account takeovers. Cybercriminals, hacktivists and even relatives threaten to access personally identifiable information (PII) and redirect funds of state and local government employees.

Public pension systems undertake a tremendous fiduciary duty

In the U.S., there are:

62
State-Level Pension Funds[1]

Nearly
21 million
government employees use these systems[2]

With a total of more than
$4 trillion
in state-administered and local-administered government pension plans[3]

More than
5,500
local funds[4]

19%
of total retirement savings assets in the U.S. are in state and local government pensions[5]

Retirement systems acknowledge security upgrades are needed

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

50%
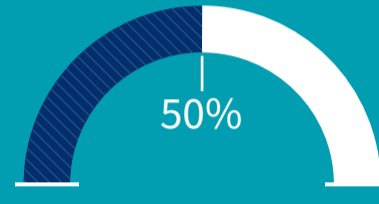
At least half of the public retirement systems are at risk

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

49% of those surveyed said they upgraded their systems in the last year

But, the other half of government employee systems are older and more susceptible to account takeover

30% said they haven't upgraded in more than **2 years**

19% said they haven't upgraded in more than **2 years**, some more than **5 years**

Limited, or the absence of, identity access management significantly increases the chances of a personal data breach using stolen or hacked 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 never 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

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Rather than leaving government employees' information susceptible to breaches in outdated systems, it is imperative for program leadership to identify and mitigate the potential for account takeovers.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:
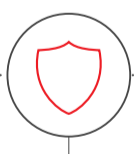
Review and refresh security standards

Incorporate low tech elements such as training, mandatory password updates, and multi-factor authentication.
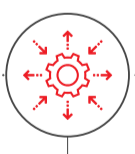
Access and analyze "fresher" data

Ensure members update their profiles regularly for accuracy, including addresses and other contact information, linked accounts, beneficiaries and login challenge questions.

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.
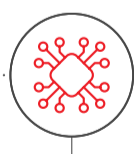
Leverage technology and security expertise

Use updated technology to monitor and manage systems and data across your enterprise.
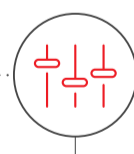
Balance security with fluidity

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

LexisNexis
RISK SOLUTIONS | Government