Bond Case Briefs

Municipal Finance Law Since 1971

For Small County Governments, Tackling Cybersecurity Basics Can Go a Long Way.

The local governments can face unique challenges when it comes to protecting their computer systems from threats.

To a small county with limited resources, it may sound intimidating to overhaul and adopt new cybersecurity standards.

But if county officials begin by taking small steps to improve their government's overall cyberhygiene – such as using secure passwords and training employees on cyber threats – they may be surprised how quickly they fall in line with industry best practices.

Cybersecurity experts shared tips on how local governments could apply the National Institute of Standards and Technology's cybersecurity framework to their networks on Friday at a panel discussion at the National Association of Counties legislative conference in Washington, D.C.

"Attacks are exploiting vulnerabilities we've known about for a really long time… like the fact we don't do secure passwords very well, we don't do user training," said Patrick Woods, the security assurance lead for state and local government at Amazon World Services.

The NIST framework was designed as a voluntary guide for businesses, organizations and federal, state and local governments to help promote the protection of critical infrastructure and manage cybersecurity-related risks.

Compliance with the framework "comes organically when you start nailing those fundamentals," Woods said.

Ensuring that county information technology officials have a working relationship with those overseeing the budget can be critical to ensuring cybersecurity efforts receive sufficient funding, said Barry Condrey, the chief information officer for Chesterfield County, Virginia.

"If the budget department doesn't understand your cyber posture, you're missing the boat," Condrey said. "Make sure you align with the people who control the money."

Condrey shared his state's experience developing security standards for Virginia's voter registration systems and the difficulties encountered by individual counties.

Virginia lawmakers in 2019 approved legislation directing the state's Board of Elections to draft regulations securing the state's voter registration system and requiring local electoral boards to develop their own security plans.

When stakeholders met to discuss potential development of minimum security standards, Condrey said about one-third of the governments represented didn't have a person on staff who was responsible for information technology security across the government. Officials were also worried

about the time and resources that would be needed to develop and meet the new requirements.

Once the state adopted the standards, Condrey said officials were not able to act immediately because they missed the budget cycle for the year. He recommended that any efforts to implement new security standards be closely tied to budget discussions so that there is money to pay for initiatives.

“Anytime a state tries to impose its will on local government, particularly with an unfunded mandate, it generally does not go well,” he said.

Route Fifty

by Andrea Noble

FEBRUARY 28, 2020