Bond Case Briefs

Municipal Finance Law Since 1971

More U.S. Cities Brace for 'Inevitable' Hackers.

Majority of top 25 U.S. cities have, or are looking to buy, cybersecurity insurance

Hackers are constantly probing for "the one flaw overlooked" in Houston's computer networks, the official responsible for safeguarding the fourth-largest U.S. city's system said.

"Compromise is inevitable," said Christopher Mitchell, chief information security official, at a Houston City Council hearing last month. His presentation helped persuade local lawmakers they needed a $30 million cybersecurity insurance plan with a $471,400 premium, an example of a burgeoning trend across the country. Policies vary, but insurance can cover hackers' extortion demands, legal liabilities, computer-forensics expertise and costs for problems like having government services knocked off line.

A majority of the 25 most-populous U.S. cities now have cyber insurance or are looking into buying it, according to a Wall Street Journal survey. A ransomware attack on Atlanta earlier this year—one of the biggest reported breaches of a city's network—served as a warning to officials everywhere of the constant barrage from hackers. Cities and even library systems are being hacked more often than people realize, but many heard about Atlanta.

"It got a lot of people nervous and got a lot of people coming to the market and saying, 'Hey, I'm really interested in buying this,' " said Brad Gow, global cyber product leader at insurer Sompo International Holdings Ltd.

Cities including Boston, Nashville, Tenn., Washington, D.C., and San Jose, Calif., are actively researching cyber insurance. Dallas, San Diego, Denver and Detroit are among those that already have cyberpolicies; none have filed claims.

"I wanted A to Z to have it covered," said Mark Barta, risk management director in Fort Worth, Texas, which got a $5 million cyberpolicy with a $99,570 premium last year. "I didn't want to be in a situation on a Monday morning hearing this happened, and saying, 'What do I do next?' "

Some cities—including New York, Chicago and Philadelphia—declined to say whether they have cyber insurance. Some, like San Antonio, have cyber coverage through an existing property policy. Others say they are self-insured, which can entail creating a special fund to cover losses.

Seattle is self-insured and doesn't have additional cyber insurance, but reviews its need for coverage every year and is currently soliciting quotes, a spokeswoman said.

"There has been an increase in cyberattacks facing state and local governments this year," Andrew Whitaker, Seattle's chief information security officer, said in a statement.

Insurers writing cybersecurity policies for cities include Sompo, American International Group Inc., Lloyd's of London and Axis Capital Holdings Ltd.

Atlanta has a cyber-insurance policy that took effect Jan. 1, less than three months before hackers

managed to freeze city computer systems. The city refused to pay a $51,000 ransom, but hacks can entail many other costs, from the emergency response to building stronger defenses. Mayor Keisha Lance Bottoms has estimated that Atlanta was facing more than $20 million in costs following the attack.

An Atlanta spokesman said officials have begun submitting claims but didn't respond to questions about the monetary value of those claims or whether the carrier, AIG, has issued any payments.

Cyber insurance has recently been a fast-growing market for U.S. corporations worried about attacks. Mr. Gow said his business—which insures Fort Worth, Charlotte, N.C., and soon, Houston, according to the cities—is also seeing strong public-sector growth. Overall, Sompo's cyber business has grown 30% a year since 2014, he said.

Cities are generally a "tough class" for underwriters, Mr. Gow said. One challenge municipalities face is hiring and retaining top IT staff. "There are not enough of these men and women around for the Fortune 500, much less for all the towns and cities and states that need these talents," he said.

Houston's cyber insurance—three $10 million policies from different insurers—is intended to cover many potential problems, including costs due to an interruption of city services and the expense to restore, re-create or re-collect lost or damaged data, officials say.

It would also cover costs tied to ransomware attacks like the one that struck Atlanta. Mr. Gow said it often makes sense to give in to lower-cost extortion demands.

"As a rule, if it's manageable—under $5,000 or $10,000 or $20,000—it's better for everyone, as distasteful as it is, to pay the ransoms," he said.

Though the Houston City Council unanimously approved the plan, one member had questions about the nearly $500,000 premium. Council member Jack Christie embraced the insurance plan. "We've been attacked, and the defense system so far has worked," he said. "Because the intensity has picked up, we need this insurance against that."

Los Angeles doesn't carry a policy, an official said. The city has, however, spent the last several years on an "aggressive strategy to improve protection," said Reuben Wilson, general counsel for public safety in the mayor's office, at a June meeting of the U.S. Conference of Mayors in Boston. This includes creating an operations center to monitor for threats citywide, he said.

On an average day, Los Angeles sees 45 million unauthorized access attempts that are blocked automatically by firewalls, Mr. Wilson said. But firewalls and antivirus software don't catch all of the latest attacks, he said, and the city's cybersecurity analysts neutralize about 2,000 intrusions each week before any harm is done.

Many cyber incidents happen when an employee opens an attachment or clicks on a link that inadvertently gives hackers access to the network.

"Humans fall for stuff, humans make mistakes," said Austin Morris Jr., chief executive of an insurance brokerage in Huntingdon Valley, Pa. He said such scenarios generally don't allow an insurer to deny coverage.

The risk hit home in San Francisco two years ago when hackers infiltrated systems at the city's transportation agency, causing it to turn off ticket vending machines as a precaution. While San Francisco has a $50 million cyberpolicy for its public-health department, the city wants to cover the entire municipal government.

Risk managers are working with brokers to learn about other cities' policies, and San Francisco has also hired a consultant to help quantify its risk so it can get sufficient coverage. The hackers are always evolving, said Michael Makstman, San Francisco's chief information security officer.

"This is their work, day in and day out, to try to attack," he said. "We do X, then they react with Y. We do Y, and then they react with Z."

The Wall Street Journal

By Scott Calvert and Jon Kamp

Updated Sept. 4, 2018 5:20 p.m. ET