

[Newsletters](#)[Webinars](#)[Events](#)[Magazine](#)[Papers](#)[Special: Remote Work](#)
Network[AI](#)[Cloud](#)[Cybersecurity](#)[Education](#)[HHS](#)[Industry](#)[Local](#)

CYBERSECURITY

Cyber Insurance Price Hike Hits Local Governments Hard

Across the United States, many local governments and states — as well as private companies — are discovering their cyber insurance premiums have skyrocketed and that they must meet stricter guidelines

July 28, 2022 • Jenni Bergal, Stateline.org



(TNS) — Horry County, S.C., officials were in for a shock earlier this year, when they discovered their cyber insurance premium would be spiking from \$70,000 last year to at \$210,000.

And if they couldn't satisfy the insurance company's requirements and prove they had the robust controls needed to protect and defend themselves against cyber attacks, they learned, they wouldn't be able to get their \$5 million policy renewed at all.

"The insurance companies have you over a barrel. There was not a lot of negotiation," said Tim Oliver, the county's chief information officer.


ADVERTISEMENT

Across the United States, many local governments and states — as well as private companies — are in the same boat. They're discovering their cyber insurance premiums have skyrocketed and that they must meet stricter guidelines if they want to get coverage or renew their policies.

"Cyber insurance used to be very cheap," said Alan Shark, executive director of the CompTIA Public Technology Institute, a Washington, D.C.-based nonprofit that provides consulting services to local governments. "But things have changed, and insurance companies are increasing rates dramatically and raising the bar and making it harder to get insurance. Some local governments may no longer be able to get it."

Insurance industry officials say the higher premiums for both public and private organizations are a result of rising demand for coverage amid more frequent and costly cyber crime incidents — often ransomware attacks. That means insurers have had to pay out more, which has led them to raise premiums and tighten standards for getting a policy. Some companies also have lowered caps on coverage or limited how many policies they write.

ADVERTISEMENT



August, for example, American International Group, one of the country's largest insurers of cyber insurance, announced that rates for its clients had increased nearly

40% globally and that it was tightening the terms of its policies to address increasing cyber losses.

In the past three years, the number of cyber insurance claims reported in the United States rose by 100% a year, according to a May report by Fitch Ratings, a credit rating agency. In 2021, insurers paid 8,100 claims.

To reduce risk and potential losses, insurers are becoming more diligent during the application process about which safeguards and technology an organization uses to protect itself against cyber attacks, according to Loretta Worters, spokesperson for the Insurance Information Institute, an industry trade group.

“If a government entity or any business really has such vulnerabilities and fails to address them, it will likely result in either a higher premium or non-renewal of coverage,” Worters wrote in an email.

Companies now want to ensure organizations have updated software and firewall protections, a backup system, cyber training for staff and testing for vulnerabilities, among other requirements.

They also are requiring organizations to use multi-factor authentication systemwide, including for remote work. Such security technology confirms a user’s identity before they log in, usually through a randomized one-time password or number sent to a smartphone or email address.

Cyber insurance typically covers a variety of services, such as providing forensic expertise to investigate the attack, legal support, hardware replacement, data recovery and notification of people whose personal data may have been breached. Some policies also include ransom negotiations with the hackers and payment of the ransom.

The insurance changes largely spring from the explosion of ransomware, which hijacks computer systems, encrypts the data and holds it hostage until the victims pay a ransom or restore the system on their own. It typically spreads through phishing, in which hackers email malicious links or attachments and people unwittingly click on

them, unleashing malware.

In 2020, ransomware attacks accounted for 75% of cyber insurance claims in the U.S., according to AM Best, a credit rating agency.

In the past several years, there has been a rash of ransomware attacks on cities, county governments, school districts, police agencies and health care systems. Local governments, especially smaller ones, can be easy prey because they may have fewer resources and staff with cybersecurity expertise.

In 2021, there were at least 77 successful attacks on local and state governments and another 88 on school districts, colleges and universities, according to Brett Callow, a threat analyst for cybersecurity company, Emsisoft. This year, as of late June, there were at least 28 attacks on governments and 33 on schools.

In Baltimore, where thousands of computers were crippled in a massive ransomware attack in 2019, it wound up costing the city at least \$18 million — a combination of lost or delayed revenue and the expense of restoring systems.

The city, which didn't pay the ransom and didn't have cyber insurance, decided to spend about \$835,000 for one year to buy \$20 million worth to cover any additional disruptions to its networks. It continued to purchase cyber insurance annually.

Other local governments choose to pay the ransom because they need their data back quickly and think it's the best option. Some figure it would be too costly and time-consuming to start over from scratch and rebuild everything.

Many local governments see cyber insurance as a necessity in case they're attacked, which makes it even more disconcerting that their premiums have shot up and there are new requirements, according to Rita Reynolds, chief information officer at the National Association of Counties.

In the past year and a half, Reynolds said, instead of answering a few questions from their cyber insurance company when it was time to renew, counties now are being asked to fill out lengthy questionnaires about their security practices.

“Insurance companies are saying higher standards are needed at a higher cost and lower coverage,” she said. “It’s kind of like a perfect storm.”

Reynolds said these new requirements aren’t necessarily a negative as counties try to keep up their cyber defenses, but officials were surprised at how fast it’s happened.

“It caught a lot of us a little off guard,” she said. “Some of the things the insurance companies want are fairly easy to implement, but others can be costly and take time. You can’t just flip a switch.”

Counties want to be secure from cyber attacks and agree that they should be doing all they can to have the proper protections, Reynolds said. But those who don’t — or can’t — may find themselves unable to renew or get cyber insurance.

“Counties are scrambling,” Reynolds said. “And no matter what you have in place, the premiums have doubled, and sometimes tripled.”

Some local governments are switching to self-insurance, in which officials set aside a pot of money in reserve to be used in case of a cyber attack, according to Reynolds. Some are joining insurance pools with similar organizations and shopping for preferable rates.

Oliver, the South Carolina official, said his county didn’t find out about changes in its policy’s requirements until two months before it was time to renew. Fortunately, he said, officials were able to answer “yes” to all the initial questions about security protections. If they hadn’t, they would have been turned down.

Officials then spent the next two months responding to the company’s second questionnaire, which was dozens of pages long, Oliver said. The county was able to resolve issues and make fixes to meet the requirements.

The county council had to approve a budget resolution allowing officials to transfer money from another account to pay the \$210,000 premium because it had budgeted \$70,000 for cyber insurance, he added.

Oliver said he is fortunate that his county, with a population of about 365,000 and about 3,000 employees, has four staffers dedicated to cybersecurity and the resources to pay for the insurance and meet the cyber defense requirements.

But smaller counties, which may not even have an information technology staff, may be unable to do either, he noted.

“They may be out of luck,” he said. “If they can’t get cyber insurance, the only option for a lot of these smaller organizations may be to cross their fingers and hope that they don’t get hit.”

In Lehigh County, Pa., with a population of about 375,000, officials also have had a stressful time getting their cyber insurance policy renewed, said Chief Information Officer Bob Kennedy. About a week before Christmas 2020, they learned that they wouldn’t be renewed because they didn’t have multi-factor authentication on all the computers accessed by staffers remotely.

Fortunately, Kennedy said, the county already was planning to make those changes and had purchased the necessary software. It was able to speed up the timeline and negotiate with the insurer to allow it make the changes in February 2021 rather than January. The premium rose 30%. And this year, he noted, the premium nearly doubled from \$82,000 to \$158,000.

“A lot of things they’re mandating are good things. There’s not too many hoops,” Kennedy said. “But the increased pricing is more of a problem. It’s requiring us to pay premiums that are going up year after year, even if you meet all those requirements.”

In the end, with all of the worry about cyber insurance, there may be a silver lining for local governments, said Reynolds, of the association of counties.

“They are becoming much more savvy about what they need to do,” she said. “With every challenge there’s an opportunity. And in this case, it’s an opportunity for them to improve their cyber defenses.”