NYSAC
NEW YORK STATE
ASSOCIATION OF COUNTIES

Cybersecurity Insurance Challenges for Public Entities

OCTOBER 2022

MICHAEL ZURLO
NYSAC President

STEPHEN J. ACQUARIO
Executive Director

PAUL LUTWAK
NYSAC IT Task Force Chair

Counties Working For You

515 Broadway, Suite 402
Albany, NY 12207

www.nysac.org

518-465-1473

Cybersecurity Insurance Challenges for Public Entities

In the past three years, counties and local governments with cybersecurity insurance have seen their premiums increase to double or triple the rates they were paying in 2019. At the same time, they found they were paying more for less: less robust coverage and new limits on the different aspects of their coverage, from ransomware to third-party credit monitoring services. They also had to fill out increasingly long and cumbersome applications and fulfill new requirements. And sometimes, despite these hoops, increased costs, and new limits, local governments or counties still may be denied the insurance they are looking for.

For municipalities that do not have cybersecurity insurance, incidence of cyber breaches are increasing pressure to acquire insurance as market conditions are making is more challenging to qualify for it.

This document sets forth considerations for counties and local governments as they explore potential cybersecurity insurance options.

The Cybersecurity Challenges Facing Insurance Companies

From the insurance companies' perspective, the cybersecurity market is volatile and unpredictable, with increased and complex risks that are difficult for their insureds (governments, schools, hospitals, banks, and other businesses) to manage.

A recent Forbes article illustrated the point, noting, "Warren Buffet, the sage of Omaha, who made his fortune in the insurance industry said, 'The insurance business doesn't like surprises.' Virtually all surprises in insurance are unpleasant ones. Any leader involved in buying, and selling, cyber insurance these days has seen some very unpleasant surprises indeed. Ransomware is involved in the vast majority of cyber insurance claims, and reported ransomware attacks surged more than 50% from 2020 to 2021. Average ransomware payments reached a staggering $812,000 in 2021. Attackers have demanded, and major companies have reportedly paid, tens of millions of dollars in major hacks that year."

Based on these experiences, insurance companies are being extra careful before committing to ensure cybersecurity risks. They are asking their actuaries, underwriters, analysts, claims adjusters, and reinsurers to study and predict all of the various risks associated with cybersecurity. Unfortunately, these insurance experts deem municipalities as a high cybersecurity risk right now, which is why it's important for municipal leaders to begin strengthening their cybersecurity efforts.

Cybersecurity Controls Examined by Insurance Underwriters

To qualify for cybersecurity insurance, public entities (as well as most businesses and organizations) must have controls in place to manage the risks of a cybersecurity breach. Different insurance carriers may weigh these controls differently during the underwriting process. Among the controls an insurance company may ask about in the application process include the following.

- multifactor authentication (MFA)—security technology that requires multiple methods of authentication for signing on to systems and/or email
    - for employee email
    - for remote work access
    - for administrative access controls (for back-end systems)
- endpoint detection and response services—security tool that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware
- robust antivirus—technology program designed and developed to protect computers from malware like viruses, computer worms, spyware, etc
- segregation of end-of-life software from the network—protects your systems from software programs that are no longer supported or updated by the developer
- up-to-date, redundant, and offline backups—capturing a copy of your databases so that they can be restored in the event of a loss or cyber incident
- formal cyber policies for procurement of third-party technology service—purchases should require and incorporate cybersecurity protections
- specified insurance requirements for third party software/hardware/services—contracts should include cybersecurity liability protections
- appointment of a designated chief information security officer (CISO)
- security awareness and training programs—to educate your employees on ways to identify and avoid cyber threats
- frequency and/or procedure (or any) of phishing exercises

Insurance underwriters assign a cyber risk (or evaluation) score based on answers to questions about these controls. If an organization cannot check all the necessary boxes, it will likely face higher rates, reduced coverage, or a rejected application. Even if an organization has instituted all of these controls, they are not impenetrable. No matter how much training and education that is provided, human error still accounts for many breaches.

While these safeguards are important, putting them in place is a resource intensive endeavor that is stretching many IT departments. “We almost need two IT departments at this time. One that provides services and one that protects the network,” said Madison County IT Director Paul Lutwak, president of the New York State Local Government IT Directors Association and chairman of the NYSAC IT Task Force.

Questions that Municipalities Need to Ask about Cyber Insurance Coverage

Like the government’s other insurance policies, cyber coverage is designed to manage the overall risk of loss to a county or local government. Cybersecurity and ransomware insurance may help protect your local government against losses resulting from a cyber attack. The cybersecurity insurance market is volatile and there are a range of levels and categories of coverage as well as technical and governance requirements—and all insurance company’s coverage policies are different.

It is important to note here: insurance can be complicated. Having cybersecurity insurance does not mean that a municipality will not have costs if they are involved in an incident or breach. There are deductibles and limits that could make the local leader ask why they have any insurance at all. That's why it's important to scrutinize any potential cybersecurity insurance policy to understand what is covered in the event of a loss.

Given the current volatility of the current cybersecurity insurance market, many municipalities are asking whether it is more cost effective to buy insurance or to self-insure. There are a range of levels, categories, and limits of coverage as well as technical and policy requirements to qualify for insurance.

Many large public entities may already self-insure their governments for property and casualty, health care, and/or workers compensation. Advantages of being self-insured include cost savings, flexibility, focused risk management, and greater control of the insurance plan. It's estimated that as much as 20 percent of cyber insurance premiums go to administration, overhead and profit. As counties and local governments explore cybersecurity insurance, self-insurance is often part of their analysis.

Like the government's other insurance policies, cyber coverage is designed to manage the overall risk of loss to a county or local government. A cybersecurity and ransomware insurance policy may help protect local governments against losses resulting from a cyber attack, but it is not a panacea and there will still likely be out of pocket expenses.

The first thing that local leaders should do is explore their existing property/casualty insurance policies to see if their business continuity, liability, and property damage coverages may include the costs associated with a data breach or cyber incident.

Next, local leaders need to consult with their insurance broker, attorney, chief information officer (CIO), chief information security officer (CISO), information technology (IT) director, and IT service provider to identify their current cyber practices in place and potential coverage needs.

Questions Your Team Should Ask

Some of the specific questions this team should discuss and consider include the following.

- Is your local government looking for first-party coverage, third-party coverage, or both?
- What are the specific coverages in the event of ransomware?
- Does the coverage include data breaches (theft of personal information), cyber attacks on your data held by vendors and other third parties, and general cyber attacks (breaches of your network)? What are the levels of coverage for each?
- Does the coverage defend you in a lawsuit or regulatory investigation (such as a HIPAA violation) and for how much? Look for "duty to defend" wording. Are defense costs inside or outside coverage limits?
- Does your local government need multiple cyber coverage plans?
- Does your local government comply with Security Breach Notification Laws?
- What are the cybersecurity control requirements for insurance (see control requirements above)?
- Does the insurer provide cybersecurity risk management training or any other offerings, such as webinars and/or technical assistance?
- What incidents are covered and what is excluded by your policy?
    - Forensic expenses?
    - Notification expenses?
    - Regulatory fines and penalties?
    - Credit monitoring and ID theft repair?
    - Public relations expenses for reputation risk?
    - Business interruption/denial of service?
    - Is there an exclusion or limit on ransomware coverage?
    - Other coverages/exclusions?

Pooling the Purchase of Cybersecurity Insurance

NYSAC was asked to explore the possibility of organizing a collective of county governments for the purposes of the joint procurement of cybersecurity insurance.

We distributed a County Cybersecurity Insurance Survey to NYSAC members to gauge interest in exploring a joint procurement and ascertain what levels of insurance, if any, they already carry. We received responses from 26 public entities (23 counties, 1 city, and 2 towns).

The responses included some interesting results.

- 1 entity buys $500K in coverage, 12 buy $1M, 2 buy $2M, 1 buys $3M, 5 buy $5M, and 5 do not buy coverage
- these 26 entities are served by 13 different carriers
- renewal or expiration dates vary by entity

We then asked those entities who were still interested in exploring this program of pooled insurance to submit their most recent cybersecurity insurance application or fill out a new one we supplied. We received responses from 13 entities.

Our goals with this proposed cybersecurity insurance purchasing program are to:

- achieve the most competitive premium rates for participating entities,
- improve coverage for participating counties/municipalities, and
- standardize requirements and coverage policies across participants.

Thus far, brokers have indicated that there is little or no appetite on the part of the current insurance market to develop a pooled purchase program for public entities. The degrees of risk vary too dramatically, and the controls in place across entities are not at a standard level of acceptance for insurance underwriters.

The Future of the Cybersecurity Insurance Market

While the future of the cybersecurity insurance market for public entities is difficult to predict, we are confident that insurers and public entities alike are exploring ways to more predictably understand and manage the risks associations with the IT systems that run the business of government.

One such tool may be technology itself, with services or solutions that automate the cybersecurity risk assessment of public entities, and potentially standardize the application process in ways that help insurance analysts and underwriters identify the controls that are in place so that they can better estimate risks and more accurately price the risk and resulting premiums.

In the meantime, there is a steep learning curve on the part of public entity leaders, many of which are in ongoing discussions with their IT professionals to understand and prioritize the controls that need to be put into place to protect their IT assets from the potential risks associates with cyber incidents.

The United Voice of New York's Counties

New York State Association of Counties

515 Broadway, Suite 402
Albany, NY 12207

www.nysac.org

518-465-1473