Focus: Local Government Technology

Cyber Insurance

Is your public entity properly protected?

By Edward J. Cooney, MBA, MEL JIF Underwriting Manager;
Vice President - Account Executive, Conner Strong & Buckelew

Cyber insurance has been around for more than a decade, but new cyber risks are emerging daily. No entity is immune to cyber risks. The need to have the right cyber insurance is becoming more critical for public entities as more and more attacks are directed toward the public sector.

Symantec's *2018 Internet Security Threat Report* noted that the public sector leads all industries in email-based malware attacks. In fact, one of every 120 emails received by public sector workers will be infected with malware, and one in every 38 users will receive an email phishing attempt.

Data breaches are still the most feared and devastating types of cyber incidents. The Ponemon Institute's *2018 Cost of a Data Breach Study* found the average cost of a data breach for the public sector is $75 per capita, up 5% since 2017. To put that in perspective, if a town has 3,000 citizens, the average cost could be $225,000 ($75 x 3,000)–and that is before any claims are filed by affected individuals, which could escalate the total cost into the millions.

In New Jersey, cyber-attacks against municipalities and public entities continue to gain momentum. The Municipal Excess Liability Joint Insurance Fund (MEL JIF) found that 40% of all cyber incidents reported by members from 2013-2018 were due to malware infections from email phishing attempts and accounted for 80% of claim costs. Law enforcement agencies reported the most incidents, 20%, which accounted for 40% of claims costs. Actual data breaches accounted for 16% of reported incidents.

Ensuring protection

So, what can you do to ensure sure your public entity is protected? Purchase cyber insurance coverage. This sub-category of insurance covers businesses and individuals against internet-based liability and risks. However, shaping the policy to fit your specific needs can be a challenge.

"There really is no such thing as universal coverage for cyber insurance and the market is very volatile with many companies selling different kinds of coverage at different prices," explains Marc Pfeiffer, a technology consultant for the MEL JIF and Assistant Director of the Bloustein Local Government Research Center at Rutgers University.

"The first step is to have the experts collaborate," says Pfeiffer. "IT departments, outside contractors/consultants, municipal managers, and agency attorneys need to work with their risk managers to assess their current technology to identify risks their organization may face. Only then can they determine their cyber risk management needs."

Locking In Your Choice

Regardless of what your cyber risk profile looks like, cyber insurance will fall into one of two main categories: First-Party and Third-Party coverage.

First-Party coverage encompasses internal expenses incurred by the entity and should include:

Ransom: Payment (in any currency, including cryptocurrency) to an attacker to release data or access to systems following a ransomware event.

Restoration: Restoring computers, hardware, software, and data back to pre-incident status, including the initial estimates for the repair.

Business Interruption: Intangible costs for lost revenue and the extra expenses incurred above and beyond normal (like property insurance).

Incident Response: Funding to cover specialized cyber legal counsel, forensic computer vendors, notification and credit monitoring/call center for potentially affected individuals and public relations.

Third-Party coverage handles external expenses related to claims and lawsuits brought by employees, individuals, etc., and legal defense. This should also include:

Network Privacy/Security Liability: Violations of rights of privacy and/or privacy law due to unauthorized release or misuse of Personally Identifiable Information (PII), Protected Health Information (PHI), and confidential corporate information of a third party.

Electronic Media Liability: Incidents libel, slander or defamation arising from personal injury due to communications in email, social media, websites, etc.

Professional Liability: For professional exposures, this covers wrongful acts and financial injury when providing a service to another entity.

Where's the catch? As with any insurance product in the marketplace, there are nuances you should be aware of:

PCI-DSS: Most policies do not automatically provide coverage for violations of the Payment Card Industry Data Security Standards (PCI-DSS). If your agency processes credit cards through your network (as opposed to using an external processor) this coverage is critical.

Contingent Business Interruption: Most cyber policies include coverage for business interruption to computers/networks but may not include "contingent interruption" that originates from a third-party provider, such as a colocation facility or cloud service provider.

Social Engineering: This crime-type loss occurs when an attacker, often using false impersonation, convinces the end-user to send funds (also known as Business Email Compromise). Check with your risk manager to see how this is covered.

Response Coach Deductible: Many insurers will have a response coach to help you triage an incident, but you may be deterred from reporting due to a high deductible. Zero ($0) cost deductibles for the response coach are available in the marketplace.

Notification Costs: Pay attention to the notification costs limit. Many insurers offer this in either dollars or individuals. There is no right way, but a $1,000,000 limit may not mean the same as a 100,000 individuals limit.

Panel Providers: Many insurers have a panel of providers you can use following an incident. Non-panel providers may not be covered so be sure to check before engaging a provider. Some insurers will offer coverage for non-panel providers.

Although First and Third-Party coverage will pay for most expenses related to cyber incidents, the most valuable part of the policy can be the incident response system following an attack. Insurers should have a pre-contracted panel of cyber attorneys, computer forensic firms, public relations firms, etc. The attorney will be the first person you work with and will lead you through the entire incident response.

REAL STORY: A person clicks on a spoofed link in a phishing email and unknowingly downloads ransomware to the device which then spreads to other devices on the network. The personal information of hundreds of individuals was compromised. A breach counsel and forensics team was engaged. Notification was sent to all affected individuals and a call center and credit monitoring service had to be setup.

COST: +$125,000

Understanding the different coverage options and recognizing the downside (which can be found in every policy) are also critical to this equation.

Security training

As technology becomes more integrated into daily municipal operations the need to protect against cyber risks increases. The bottom line is that public entities need to know their risks, manage them with technology leadership, proficient technical management and regular employee security training.

"Cyber insurance should supplement a strong risk management program," explains Joseph Hrubash, MEL JIF Deputy Executive Director. "The MEL has been proactive in this area by establishing a comprehensive cyber risk management program that affords financial incentives tied to compliance."

The cyber insurance field is evolving as quickly as new risks emerge. A cyber insurance policy needs to be reviewed at least once a year to ensure that you are protected against risks that could cost your entity and the taxpayers millions of dollars.

@ For more information about cyber insurance visit:
Rutgers University: http://blousteinlocal.rutgers.edu/reports/
MEL JIF: https://njmel.org/mel-safety-institute/resource-center/public-officials/public-officials-cyber-risk-control/

REAL STORY: A network connected printer had an open port to the internet. \A cyber intruder found the port and downloaded ransomware to the network. The attack left the entity offline for nearly a week.

COST: +$50,000

MEL JIF is slated to hold its **Annual Risk Management** session at the League Conference, **Wed. Nov. 14 at 3:45 p.m.**