



Cyber Insurance

What municipalities need to know

Joy Tozzi, Chair of the Municipal Excess Liability Joint Insurance Fund (MEL JIF), Chair, MIDJIF, and Business Administrator of Robbinsville Township; and Edward Cooney, MBA, Partner and Sr. Account Executive, Conner Strong & Buckelew, and Underwriting Manager, Municipal Excess Liability Joint Insurance Fund (MEL JIF) and MEL Cyber Task Force



Cybercrime is on the rise. Municipalities and public entities are being targeted with greater frequency than ever before. The *Asbury Park Press* reported earlier this year about incidents that impacted the towns of Union Beach, East Windsor, and Middletown, but there are many more occurring that are not public knowledge.

The New Jersey Municipal Excess Liability Joint Insurance Fund (MEL JIF), which represents 70% of public entities in the state, reports that 1 in every 10 public entities are the victims of cyber-attacks each year, but that may only represent the tip of the iceberg since many incidents are never reported. The MEL JIF has an extensive Cyber Risk Management program that offers planning, guidance, insurance, and resources to JIF members and free educational materials to all public entities.

Solving the cyber safety puzzle

Municipalities that have strong cyber risk management and education programs in place can help reduce the frequency and scope of cyber incidents, but that is only one part of the cyber safety puzzle.

Having the right cyber insurance policy can make a huge difference in the time, manpower, and financial expenditures that result from a cyber-attack. Research reports indicate that more than 60% of organizations now purchase cyber insurance, which is significantly higher than just a few years ago.

However, despite the purchasing growth many organizations are still struggling to understand what cyber insurance is, what their cyber risks are, and why they need cyber insurance protection.

What is cyber insurance?

Cyber insurance responds to privacy and network security matters, such as failures to protect confidential data of employees or breaches of your network via the all too

Cyber Insurance

well-known phishing attacks delivering ransomware. In a privacy matter, you may be required by law to notify the individuals affected or you may be faced with lawsuits for failing to protect such data. A ransomware event may render your network useless for a week or much more, requiring you to hire forensic experts for remediation and resolving interruptions to your operations. In general, these costs and more are covered by a cyber insurance policy.

The bottom line is that if a hacker wants to break in, most likely they will.

Why do you need cyber insurance?

Regardless of where you work or live, chances are you can probably recall a cyber event in the news. In 2022 hackers made their presence known breaching security measures to attack companies and organizations of all sizes, including the tech powerhouse Microsoft, the international news organization NewsCorp, and even The Red Cross.

Some quick statistics from IBM's 2022 Cost of a Data Breach report reveal:

- 83% of organizations have had more than one breach.
- \$4.35 million is the average cost of a data breach (\$9.4m in U.S.).
- It takes 277 days on average to identify and contain a breach.

You may be asking yourself, "Why do I need cybersecurity, I'm not like these valuable targets?"

While some cyber criminals are specifically attacking for destruction, political destabilization, or activist actions, Verizon's 2022 DBIR report indicates roughly 86% of attacks are



Cyber Insurance Preparation

The following is a quick guide to help you prepare to obtain or renew cyber insurance.

1. Get technology support with security knowledge or a security consultant.
2. Start conversations at least six months prior to allow for planning, shopping, and budgeting.
3. Establish minimum cybersecurity controls (these are just the bare minimum):
 - **Multi-Factor Authentication (MFA).** (See article on page 6.) Apply to the following areas, in order of importance:
 - All remote access (including email)
 - Privileged users inside the network
 - Data back-ups
 - **Data Back-Up.** Must be off-network or segmented from regular network.
 - **Patch Management.** Have a procedure to manage security patches, and establish a practice of implementing them ASAP (1 week to 1 month is common practice depending on criticality).
 - **Defensive Tools.** Utilize firewalls, antivirus, and anti-malware tools.
 - **Training.** People are our greatest weakness, so all users should be regularly trained and tested.
 - **Endpoint Detection & Response (EDR).** EDR tool should be deployed to detect and remove security threats.
 - **Passwords.** Have a password policy requiring complex passwords change regularly, including lockout protocols.
 - **Incident Response Plan (IRP).** An incident response plan will help guide actions to take during a stressful cyber event to ensure operations are stabilized and quickly recovered.

financially motivated. One attack left a ferry service out of commission for days and partially disrupted for much longer. A famous band's unreleased album was stolen by attackers for extortion purposes. Thousands of printers were taken over to continually print inappropriate messages.

The bottom line is that if a hacker wants to break in, most likely they will. As noted earlier, most attacks are financially motivated and only a minority of attempts are successful. Considering these patterns, your minimum strategy is to not be an easy target.

Preparing for cyber insurance purchase or renewal

The bottom line is that you need to be prepared and make sure that the policy you have, or the one you are seeking, meets your basic needs and provides the right level of coverage for your particular public entity.

While all MEL JIF members have cyber insurance, many public entities in other pools or who are on their own continue to operate without cyber

coverage. Many of these uninsured entities could not obtain coverage because they did not have one or more of the minimum cybersecurity controls (see box) in place.


Why is this preparation so important?


A recent article at Governing.com reported, "Securing cyber insurance coverage is becoming increasingly difficult for U.S. cities and counties as insurers raise prices and insist clients meet various best practices to get or renew coverage."

In addition, they noted that insurers are requiring risk assessments that often include long and often complicated applications that detail the entity's cybersecurity training and defenses.

Preparation also helps ensure that the information you provide is accurate to avoid denial of a claim. Insurancejournal.com reported on a potentially precedent-setting lawsuit between Travelers and one of their insureds over whether the insured misstated their security controls—

particularly the use of MFA—on the application for cyber insurance. If the court sides with the insurance company, the insured would be left without coverage for their cyber loss. Even though this lawsuit doesn't involve a municipality, the ramifications could affect all entities seeking cyber insurance in the future.

By following these guidelines, working with your IT department, security consultants, or even insurance company cybersecurity engineering teams, you will be able to better understand and correctly convey your security position when renewing or applying for cyber insurance. 

 Municipal Excess Liability Joint Insurance Fund has a comprehensive risk control program that includes cybersecurity consulting, employee training, vulnerability scanning and penetration testing. The MEL JIF also offers insurance deductible reductions for compliance with its cybersecurity framework. For more information visit <https://njmel.org/>

BARK AVENUE • RED BANK, NJ
 FASHIONABLE PETS • PARAMUS, NJ
 FURRYLICIOUS •
 WHITEHOUSE STATION, NJ



THE PET SHOPPE • MIDDLETOWN, NJ
 SHAKE A PAW • GREEN BROOK, NJ
 SHAKE A PAW • UNION, NJ
 PETCENTER • OLD BRIDGE, NJ

New Jersey Pet Stores Provide Happy, Healthy Puppies from Licensed and Inspected Breeders

USDA LICENSED & INSPECTED



Breeder



USDA LICENSED & INSPECTED



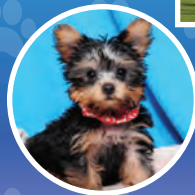
Breeder



USDA LICENSED & INSPECTED



Breeder



New Jersey Pet Stores Provide

- Full Breeder Disclosure and Transparency
- Consumer Protection and Extensive Warranties
- Veterinary Certified Health Checks and Records
- Local Business Owners Who Care For Our Puppies, Our Customers and the Communities We Serve
- Great Selection of Puppies in a Friendly Meet and Greet Atmosphere

Visit our website NJResponsiblePetStores.com

DON'T BAN US!! SUPPORT OUR REGULATED, LICENSED AND INSPECTED BUSINESSES!!



Already Banned from New Jersey Pet Stores!!!!