INFORMATION MEMO

Coverage for Cyber and Computer-Related Risks

Learn more about how the League of Minnesota Cities Insurance Trust (LMCIT) liability, property, crime, bond, and auto coverages respond to cyber and other computer-related risks.

RELEVANT LINKS:

Learn more about protecting your city from computer-related risks in the LMC information memo, *Computer and Network Loss Control*.

See also the NetDiligence eRisk Hub, a web-based portal containing information and technical resources that can assist in the prevention of network, cyber, and privacy losses.

I. Cyber and computer-related risks

Cyber risks are an increasingly important consideration for cities, just as for private entities. Unlike the common practice of private insurers, LMCIT does not issue a separate coverage document for cyber risks. Instead, LMCIT's approach is to build coverage for cyber risks into LMCIT's standard liability, property, crime, bond, and auto coverages. The standard LMCIT coverages are designed to respond to members' cyber and other computer-related risks, including:

- Liability claims made against the member resulting from a data security breach or other computer-related errors, acts, or omissions.
- Payment card industry (PCI) fines and penalties and data security breach regulatory fines and penalties resulting from a data security breach claim.
- Cyber-related property damage, including the cost to restore or replace equipment destroyed due to virus or hacking intrusion; costs to reproduce or restore intangible electronic data; and loss of revenue, extra expense, and expediting expense resulting from unauthorized intrusive codes or programming.
- Data security breach response expenses incurred by the member, including legal and information technology consulting, providing notice to affected persons, credit monitoring and identity theft services, and other reasonable expenses incurred to respond to a breach.
- Theft of city funds by electronic means.

Coverage for these exposures is provided under several separate coverage parts. For coverage to apply for all these exposures, the member would need to have all of the following LMCIT coverages: municipal liability, property, bond, and auto coverages.

RELEVANT LINKS:

See LMC information memo, *LMCIT Liability Coverage Guide*.

A. Liability coverage

The LMCIT municipal liability coverage applies to claims resulting from data security breaches or other computer-related risks, and the standard limit is $2 million per occurrence (the LMCIT liability coverage is on a claims-made basis). However, there are a couple annual aggregate limits to be aware of.

- There is a $3 million annual aggregate (total amount of coverage for the year, regardless of the number of claims) for third-party liability claims arising out of data security breaches.
- A $250,000 annual aggregate/sublimit (part of and not in addition to the $3 million data security breach aggregate) for PCI fines and penalties and data security breach regulatory fines and penalties resulting from a data security breach claim.

Examples of data security breach claims include:

- City is sued for invasion of privacy or a data practices violation resulting from the actual or potential unauthorized access by an outside party of private or confidential data that was stored in the city's computer system.
- City fails to prevent a hack into an emergency dispatch, traffic light, or water tower system, and the incident doesn't necessarily involve the unauthorized acquisition of personal or confidential data.
- A city employee loses a laptop from which a criminal accesses the city's employee files, including employee names with Social Security numbers and other confidential information. One of the employees incurs damages as a as a result of the unauthorized acquisition of data.
- A city's accounts receivable system that contains names and credit card numbers is hacked. An individual incurs damages as a result.

The LMCIT liability coverage also applies to other types of computer-related liability claims members can face that don't involve a data security breach. The $3 million data security annual aggregate does not apply to these types of claims. Examples include:

- City employee uses city's email system for sexual, racial, or other harassment of another employee.
- City employee subscribes to a job-related listserv where she or he comments about a vendor and gets sued for defamation.
- City employee uses city's web access to view pornography; another employee sees it and sues the city on a hostile environment claim.
- City's website infringes on a copyright or trademark and the city is sued.

RELEVANT LINKS:

See LMC information memo, *LMCIT Property, Crime, Bond, and Petrofund Coverage Guide*.

B. Property coverage

The property coverage applies for cyber-related property damage claims. There are several important aspects of this coverage:

- It covers the cost to reproduce or restore electronic data that's been damaged or destroyed by unauthorized intrusive codes or programming, such as a virus, hacker, or similar attack. A $1 million per occurrence limit applies, and it can be increased by endorsement if necessary.
- It covers loss of revenue, extra expense, and expediting expense resulting from unauthorized intrusive codes or programming, up to a $500,000 per occurrence limit.
- It covers data security breach response costs, like legal and information technology consulting, providing notice to affected persons, credit monitoring and identity theft services, and other reasonable expenses incurred to respond to a breach. Expenses are subject to a $250,000 annual aggregate limit, and it can be increased to $500,000 for an additional premium charge.

See LMC information memo, *LMCIT Property, Crime, Bond, and Petrofund Coverage Guide*.

C. Crime coverage

Members that have property coverage with LMCIT also receive standard crime coverage for no additional premium charge. The crime coverage applies for loss of money resulting from theft by an outside party, including theft by electronic means, such as wire transfer fraud.

The coverage also includes losses resulting from credit card fraud that are not otherwise reimbursable by the issuer, owner, or holder of the card. However, following a credit card fraud loss that involves a point-of-sale terminal, the coverage terms may be restricted unless and until further action is taken by the member to prevent future losses by installing and converting to credit card chip technology.

The standard crime limit is $250,000 per occurrence, but can be increased for an additional premium charge.

See LMC information memo, *LMCIT Property, Crime, Bond, and Petrofund Coverage Guide*.

D. Bond coverage

LMCIT bond coverage is an optional coverage available to members of the property/casualty program. Bond coverage applies for theft of city funds by an internal party, including theft by electronic means. Bond limits are available between $50,000 and $1 million per occurrence.

RELEVANT LINKS:

See LMC information memo, *LMCIT Auto Coverage Guide*.

E. Auto coverage

The LMCIT auto physical damage coverage responds to auto damages caused by a computer virus or hacking attack.

II. Further assistance

LMCIT Underwriting Department
651.281.1200
800.925.1122

Contact the underwriting department for additional information or questions about coverage for cyber and computer-related risk.