



INFORMATION MEMO

Coverage for Cyber and Computer-Related Risks

Learn more about how the League of Minnesota Cities Insurance Trust (LMCIT) liability, property, crime, and bond 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](#).

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, and bond 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, which are discussed below. For coverage to apply for all of these exposures, the member would need to have all of the following LMCIT coverages: municipal liability, property, crime, and bond coverages.

This material is provided as general information and is not a substitute for legal advice. Consult your attorney for advice concerning specific situations.

RELEVANT LINKS:

Learn more about the LMCIT liability coverage in the 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. (As a reminder, 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.
- 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 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 limit would 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.
- A hacker attack or virus disables the city's 911 or fire beeper system; a citizen whose house burns down sues the city for damages based on the city's negligent failure to safeguard its systems.

RELEVANT LINKS:

Learn more about the LMCIT property coverage in the LMC information memo, [LMCIT Property, Crime, Bond, and Petrofund Coverage Guide](#).

Learn more about the LMCIT crime coverage in the LMC information memo, [LMCIT Property, Crime, Bond, and Petrofund Coverage Guide](#).

- A hacker hijacks the city’s email system and uses it in a “denial of service” attack to a company that sells products over the web, resulting in a substantial loss of sales. The target company sues the city for negligently failing to take reasonable steps to safeguard the city’s system, which may have allowed the attack to occur.

B. Property coverage

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

- The LMCIT property coverage covers the cost to reproduce or restore electronic data that’s been damaged or destroyed by unauthorized intrusive codes or programming; i.e., a virus, hacker, or similar attack. A \$1 million per occurrence limit applies to this coverage. This limit can be increased by endorsement if necessary.
- There is also coverage for loss of revenue, extra expense, and expediting expense resulting from unauthorized intrusive codes or programming, up to a \$500,000 per occurrence limit.
- The LMCIT property coverage also includes coverage for data security breach response costs. This includes coverage for 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. Coverage for data security breach response expenses is subject to a \$250,000 annual aggregate limit. This limit can be increased to \$500,000 for an additional premium charge.

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 (e.g., 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.

RELEVANT LINKS:

Learn more about the LMCIT bond coverage in the LMC information memo, [LMCIT Property, Crime, Bond, and Petrofund Coverage Guide](#).

LMCIT Underwriting
Department
651.281.1200
800.925.1122

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).

II. Further assistance

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