

Cyber suite for public entities

A comprehensive safety net to guard against data breaches, computer attacks, liability, and more

If you depend on technology and the internet for everyday interactions among staff, students, and teachers, your school is vulnerable to cybercrime.



eRiskHub®: for a stronger stance — and faster recovery

Liberty Mutual's eRisk Hub portal has all the tools you need to plan ahead for cyber threats — and manage them competently when they happen. Resources include:

- Incident response plans
- Online security training
- Risk assessments
- Best practice reports and expert-led webinars
- Industry news
- Additional contacts and resources

Call on our experts
for 24/7 claims
support, resources,
insights, and more.

Drawn by quantities of personal data and limited defenses, hackers are exploiting school systems and finding new weak points as remote learning becomes more common. Because hackers find new ways in as quickly as technology evolves, it's critical to choose robust coverage.

Why choose Liberty Mutual's cyber suite?



Experience

Our deep experience in cyber coverage means you can be confident we'll anticipate and manage your cyber risks. You can rest easy knowing we're constantly monitoring how risks change and responding accordingly with new solutions.



Affordable pricing

Tight budgets shouldn't prevent your school or entity from securing protection from this very real threat. That's why we make coverage affordable for public entities of all sizes and situations.



Cyber Suite coverage details

Availability: Cyber Suite is an optional coverage endorsement designed to be attached to a CGL policy.

Limits: \$50,000 – \$5,000,000 aggregate limit

Deductibles: A per-occurrence deductible applies, ranging from \$1,000 – \$10,000, depending upon aggregate limit.

Sublimits: Sublimits apply to selected coverages and vary depending upon aggregate limit.

First-party coverages. Covers expenses incurred by responding to cybercrime.

- **Data compromise response expenses.** Covers expenses arising from a personal data compromise (data breach), and includes the following:
 - **Forensic IT review (information technology).** Cost of hiring outside computer experts to determine the nature and extent of the breach. Sublimit is 50 percent of aggregate limit.
 - **Legal review.** Cost of professional legal advice on how to respond to a personal data compromise. Sublimit is 50 percent of aggregate limit.
 - **Notification to affected individuals.** Costs incurred when providing notification of a personal data compromise to affected individuals. Subject to aggregate limit.
 - **Services to affected individuals.** Cost of providing the following services to affected individuals: informational materials, toll-free telephone help line, credit report and monitoring, and identity restoration case management. Limited to 12 months from date of notice.
 - **Public relations.** Cost of implementing the recommendations of a professional public relations firm, designed to retain relationships with affected individuals. Sublimit is \$5,000.
 - **Regulatory fines and penalties.** Any fine or penalty imposed by law, to the extent such fine or penalty is legally insurable. Sublimit is 50 percent of aggregate limit.
 - **PCI fines and penalties.** Any payment card industry (PCI) fine or penalty imposed under a contract. Sublimit is 50 percent of aggregate limit.
- **Computer attack.** Covers expenses arising from computer attacks on your computer system. Includes the following:
 - **Data restoration.** The cost of hiring a professional firm to replace lost or corrupted data from electronic sources. Subject to aggregate limit.
 - **Data re-creation.** The cost of hiring a professional firm to research, re-create, and replace lost or corrupted data from non-electronic sources. Subject to aggregate limit.
 - **System restoration.** The cost of hiring a professional firm to restore the computer system to pre-attack functionality. Subject to aggregate limit.
 - **Loss of business.** The loss of business income and extra expenses incurred during the restoration period. Sublimit is 50 percent of aggregate limit.
 - **Extended income recovery.** The component of business income that has not returned to historical levels after recovery. Subject to loss of business sublimit.
 - **Public relations.** The cost of hiring a professional public relations firm to assist in developing communications to outside parties following the computer attack. Sublimit is \$5,000.
- **Cyber extortion.** The cost of hiring a professional firm to investigate and negotiate a cyber extortion threat. Sublimit varies based on aggregate limit.
- **Misdirected payment fraud.** Funds lost as a result of criminal deception of the insured or the insured's financial institution to induce the insured or the financial institution to send money or divert a payment to a fraudulent destination. Sublimit varies based on aggregate limit.
- **Computer fraud.** Funds lost by the insured as a result of an unauthorized party gaining access to the insured's computer system and using that access to enter or alter data, causing money to be sent to a fraudulent destination. Sublimit varies based on aggregate limit.

Third-party coverages. Covers legal costs resulting from cybercrime.

- **Data compromise liability.** Covers defense and settlement costs in the event that individuals affected by data compromise sue the insured. Subject to aggregate limit.
- **Network security liability.** Covers defense and settlement costs in the event that a third party sues the insured over a network security incident. Subject to aggregate limit.
- **Electronic media liability.** Covers defense and settlement costs in the event that a third party sues the insured, alleging the insured's electronic communications resulted in defamation, violation of a person's right of privacy, interference with a person's right of publicity, or infringement of copyright or trademark. Subject to aggregate limit.