

DATA BREACH AND CYBER RELATED Protection

Have you sent an email today? Accepted payment via credit card?

Your everyday business operations require you to handle a lot of electronic data. And while computers are a part of everyday life, all this data can put your business at risk. Make sure you're covered in the event of fraud, data loss or data theft with Jewelers Mutual Insurance Company.

Data Compromise – Response Expense

This coverage helps you meet state and federal requirements, including notification, in the event of a data breach. Covered expenses could include legal counsel, forensic IT reviews, credit monitoring and identity restoration services when data on clients, employees or others is stolen, electronically "hacked" or lost through accidental or inadvertent release.

Data Compromise – Response Expense, Defense and Liability

Additional coverage expands Data Compromise to cover defense and liability costs for legal actions taken against your business resulting from a data breach.

Computer Fraud and Funds Transfer Fraud

Protects your business in the event of fraudulent transfers, payments or deliveries from your account.

Identity Fraud Expense Coverage

Covers your business in case of identify fraud, including loss of income resulting from time off work to meet with law enforcement or credit agencies and reasonable attorneys' fees to defend related lawsuits.

Electronic Commerce (E-Commerce)

Coverage includes restoration or replacement of e-commerce data that is destroyed or corrupted as well as business income loss and extra expense caused by suspension of e-commerce activity.

Top 5 Myths about DATA COMPROMISE COVERAGE

Think you don't need data breach and cyber protection? Take a look at the truth behind these common myths and ask yourself, "Is it worth the risk?"

1. I'm not at risk because I don't maintain any personally identifying information on my computers.

If you have employees, you're at risk. Social security numbers used for payroll and any health information collected for benefits programs are considered data.

2. I'm not at risk because I don't conduct business over the Internet.

While big data breaches that make the headlines typically involve hacking information online, the majority of data breaches actually involve lost or stolen physical files or electronic media such as thumb drives or laptops.

3. Breaches happen only to large companies and public entities.

Small businesses experience data breaches — and they may actually be more susceptible because they don't have resources available to focus on protecting data.

4. Laws requiring notification of personal data breaches apply only to large businesses.

Currently 46 states have legislation requiring notification, and they apply to businesses of all sizes.

5. If we have a personal data breach, we can just send a "we're sorry" letter to our customers and they will understand.

While that might satisfy legal requirements, you may be left with a public relations nightmare. Affected individuals could expect some sort of compensation. To soften the fallout, many companies that experience a breach offer a toll-free information line, credit monitoring services and identity recovery services.

Note: The descriptions above are a brief summary of coverage. The language is not part of any of the described insurance policies and is not a substitute for the actual policy language. Because of regulatory restrictions, not all coverage is available in all U.S. states. Underwritten by Jewelers Mutual Insurance Company, Neenah, Wisconsin. Coverage is subject to underwriting review and approval, and to policy terms and conditions.