SCHOOL INSURANCE NEWSLETTER

Data and Cyber Breach

It is estimated that data and cyber breaches will cost $6 trillion in 2021 (*Aon, Reinsurance News*). Many districts have already experienced some type of breach. Most of the claims have been of four types: 1) Fraudulent instruction: improper payment of invoices, 2) Extortion; ransomware installed in system, 3) Removal of bank funds and 4) Access to personal information. Some types of losses may also be included in a district's Crime coverage.

Those districts that purchase Cyber insurance in addition to what is provided by a risk pool, may have serious claim problems because of an "other coverage" or "other insurance" clause in either or both policies. Similar insurance that does not coordinate can be a nightmare.

Because Cyber insurance coverage is relatively new, unlike with other coverages, there are no standards. Each policy is worded completely differently, and different labels may apply to the same coverages. Below are some of the terms used by insurance companies.

Business Interruption: Income loss, Extra expense, Forensic expenses, Shared system loss (contingent business interruption)

Crisis Management: How a district deals with an unexpected harmful event

Credit Monitoring and Repair: Assists individuals whose personally identifiable information has been impacted

Cyber & Data (Privacy Information Security): Written, electronic, telegraphic, cable, teletype or telephonic activity

Data Breach or Security Breach: Unauthorized access or disclosure of information and computer data

Data Recovery: Costs to restore data

eCrime: Fraudulent Instruction, Funds Transfer, Telephone Fraud, Extortion, Cryptojacking, Invoice Fraud

Fines & Regulatory: Fines for statute violations

Forensic Expenses: Expenses to investigate sources of breach

Funds Transfer Fraud, Fraudulent Instruction: Transfer of District funds without consent or through misrepresentation

Liability & Defense: Damages to others and legal costs

Notification # or $ Limit: Either number of notifications or $ limit for advising customers of security breach

Phishing: Fraudulent practice of sending emails to induce individuals to reveal personal information

Privacy & Information Security: TASB RMF term for Cyber crime

Ransomware or Extorsion Threats: Software designed to block access until ransom paid-Data, Unauthorized access, Employee access, Malicious code, Interruption of system

Reputation Repair: Public relation costs necessary to reaffirm District reputation

Retroactive Date: Date on which coverage begins. May be prior to inception if previous coverage

Security Breach: Unauthorized access, Denial of service, Malicious code

Social Engineering: Deception to obtain confidential or private information