Purchasing Cyber Coverage

We are now in an environment in which cyber threats are a real risk that we all have to take seriously. Click here for some facts about data breaches and cyber coverage highlights.

When purchasing cyber coverage for your school, there are no two coverage forms that are the same. This makes it very hard to compare coverage and identify the areas that are really important. Click here to review some of the common insuring agreement language that is very important to be familiar with when comparing companies.

To risk assess your school district, ask the following questions:

1. What Personally Identifiable Information (PII) do you have in your possession?
2. What Protected Health Information (PHI) do you have on electronic media as well as hard files?
3. Does your school back up your data on a daily basis?
4. Do you have exposure to Payment Card Industry (PCI) fines or awards due to a breach in security?
5. Does your policy include a "hammer" clause? If there is a hammer clause, this could severely limit your coverage.
6. Do you have 24-hour access to a breach hotline?

And there is much more. The limits and coverage available to Wisconsin schools vary from each carrier. Our recommendation is to obtain several options and then make a decision on what you need to properly protect your district.

An additional coverage that has been recently added to several coverage forms is the Fraudulent Impersonation, or some carriers call it Cyber Deception. This is an enhancement available on the cyber form as well as your Crime Insurance. In one school district, a hacker penetrated the schools' cyber security system and attempted to falsely represent the business manager at the school. The hacker, while impersonating the school employee, attempted to obtain financial information from the school's banking partner. Thankfully, this was intercepted and no loss of funds occurred, but this incident certainly raised the alert level to these potential incidents.

For more information on all aspects of insurance, visit the WASB Insurance Plan Endorsed Agency Program Online Library. You will find links to important information related to employee benefits, human resources, property and casualty, and risk management.

This information is brought to you by one of the WASB Insurance Plan's Endorsed Agencies: TRICOR Insurance, Inc. For more information, contact John Gibson at 608-288-1800 x1714 or john@tricorinsurance.com.

TRICOR® INC. INSURANCE

WASB INSURANCE PLAN

Insuring Agreement Terms:

Privacy Liability:

Covers the cost associated with a breach for defense and indemnity

Regulatory:

Covers fines and penalties from state, federal agencies including HIPPA.

Security Breach Response:

This provides coverage for the IT Forensics, Lawyers, Notifications, PR firm, Credit Monitoring, Call Centers, etc. This is the coverage that notifies schools of a breach, secures your network, and notifies the attorney general in all states you do business. This is the triage center for a claim.

Security Liability:

Suits and costs that arise due to a distribution of malicious code

Media Liability:

This coverage applies to your website and print material for copyrighted material, liable, slander, and if someone were to hack your site and add malicious information

Extortion:

This is for if a hacker were to request funds either to stop a disruption or prevent a disruption in your network. Example #1 – your network is locked and they request funds to give you the password to unlock your network. Example #2 – hacker tells you they will launch a DDOS attack (denial of services attack) if your do not pay bitcoin. (DDOS attack will overload your network with information and then the network will go down)

Business Interruption / Data Restoration:

This is coverage provided to the insured if their network has been damaged and they are down for an extended period of time. They will be able to recoup the funds they would have earned during the time they were down. The data restoration is provided to restore data that was damaged or deleted etc. during a breach.

PCI Assessments (Payment Card Industry):

The PCI fines and assessments are assessed if the insured is not in compliance with the PCI rules of accepting cards, or there is a breach of card information. The PCI will typically make the insured aware that they need to amend their practices, and if they don't they will start getting fines/ penalties. Typically we are working with tier 3 and tier 4 retailers.

Cyber Deception:

The coverage provides reimbursement for release of funds due to deceptive instructions to release a wire transfer to a fraudulent bank account. Example – Accounting department receives an email that looks like it is coming from the President of the organization. The email is requesting an invoice be paid, and provides a wire transfer number. The accounting department releases the funds, but soon after it is discovered the email was fraudulent. The policy can reimburse the insured if the dual controls for releasing funds was followed.

Terms regarding Payment Card Industry (PCI), as defined by Visa:

Merchant Level	Description
1	Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant — regardless of acceptance channel — processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year.

What are the penalties for non-compliance?

The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine along until it eventually hits the merchant. Furthermore, the bank will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business. It is important to be familiar with your merchant account agreement, which should outline your exposure.

Source: https://www.pcicomplianceguide.org/pci-faqs-2/