AHT SCHOOL RISK REPORT:
Cyber Liability in Private and Independent Schools

AHT INSURANCE

Cyber, cyber, cyber! There's so much noise about the threats of data breaches in the media today that is hard to get a good sense of the real threat and exposure to schools. In this edition of the **AHT School Risk Report**, we intend to separate fact from myth and help you make a better informed decision about the cyber exposure facing your school and what risk management steps you should take.

Let's start with the big headlines:

> ***"Cyber insurance coverage is readily available and relatively affordable!"***
>
> ***"Data breaches can be very expensive and time-consuming to deal with and overcome!"***

But even though more than 30 insurance companies are actively writing cyber insurance, there are vast differences in coverage and cost among them.

With respect to the insurance market, while coverage has been available for about 15 years or so, we are still very much in a "Wild West" phase. Unlike property or general liability forms which have been standardized by organizations such as the Insurance Services Office (ISO), there is really no standardization of coverage, forms or terminology. Many insurance policies are put together with à la cart selections. All of this presents a myriad of options and a very large number of challenges to both the insurance broker and insurance buyer.

- So what does cyber insurance cover? There are many common misconceptions.
- How do you know how to select the right policy and the right limit?
- What steps should you take to mitigate data breaches?
- Who should you call and what steps should you take when a data breach occurs?
- What responsibility does your board have in managing cyber exposure?

Before any of these questions can possibly be answered, we need to first look at the fundamental question for schools regarding cyber liability:

The first question that often comes to mind is how much exposure does my school really have? We frequently hear comments such as "We don't have that much sensitive data" or "A third party vendor manages my database, my IT systems, or processes payroll or credit card transactions." While these can be very accurate statements, significant exposure still remains.

Data breaches come in many forms and through different avenues. A breach can come from an outside hacker, an insider, a vendor, electronically or in paper format. However, if your privacy and security policy isn't written correctly, some of these events may not be covered. Below are a few examples of some very real and very unfortunate data breach situations that have occurred with schools around the nation.

OUR "PAPERLESS" SOCIETY…

For a self-assessment, take a quick look around your office. How much printed data do you have that is non-public information stored around your office? More often our paperless society is just the opposite and this can create several openings for unintentional breaches.

The Breach:

Take the case of 2002 Brenda Scott vs. Minneapolis Public Schools.

Outside of a Minneapolis Middle School, one of the attending students noticed papers that were blowing around in the wind about ten feet from the school dumpster, intact. The papers included copies of a seventh grader's assessment-summary report, including his intellectual and functional abilities, IQ score, psychological assessment data, behavioral information as well as family history.

Needless to say, over the next several weeks the students who discovered the papers began teasing the seventh grader calling him "dumb," "stupid," and "retarded."

In one action, the school unintentionally released non-public student information they thought they had properly disposed of.

The Result:

The school had violated the state's Government Data Practices Act by failing to establish appropriate safeguards for records containing a student's private data. Due to a school's strict liability when it comes to protecting student data, the jury ended up finding the district liable for $60,000 in past damages, $80,000 in future damages and $45,000 in legal fees to the family. From a liability standpoint, this had the potential to be a much higher payout.

This situation is not uncommon and highlights the ethical and legal ramification of failing to protect paper copies of private data.

Risk Implication:

As the example above proves, data breaches do not have to be in just an electronic form. Many carriers are wising up to this exposure and have started to exclude any data breaches from their general liability policy. So how do you get this exposure covered? The answer is most often: a properly endorsed privacy & security liability policy—some unendorsed policies do not cover physical (paper) driven breaches, so it is important to review this in your policy with your broker.

CHAOS FROM THE INSIDE: "IT WAS AN ACCIDENT!"

Whether it's a password that is shared with the wrong contact, a mis-sent email, a laptop or external hard drive lost, or even an unlocked computer left on overnight, accidental data breaches can occur at any moment. One of the most common causes of loss outside of external hackers arise from unintentional staff mistakes. According to recent report by NetDiligence, Staff Mistakes were the second most frequent cause of loss of data breaches. Mistakes can also be made by some of the most trusted vendors and advisors.

The Breach:

One such accidental breach from a vendor came from the actions of a school district's law firm. In November of 2014, Seattle Public Schools District's law firm accidentally released around 8,000 student records to the legal guardian of a student at Roosevelt High School who had records about his sister's special education plan. When the school district's law firm replied, they accidentally provided the guardian with thousands of unrelated records of other students—presumably of every special education student in the Seattle Public School District. The records included disciplinary actions, disabilities, home addresses, schedules, bus routes, race, age, birth dates, etc.

The Result:

Due to the recent nature of the Seattle Public School District's breach, the final costs associated with it are still unknown, and much of it may be able to be recouped by suing their law firm; however, derivative class action lawsuits may also come back against the school board for a breach of duty in their vetting of the securities measures of their vendor relationships.

Risk Implication:

How a school manages its vendor relationships is also of critical importance in the area of cyber risk. As we've seen in cases such as Target and the Home Depot, the best internal security plans and IT risk management can be destroyed by the mistakes of an external vendor.

Remember when dealing with external vendors who will have access to your computer network or work in rooms that contain private information, it is important to ask the following questions:

- Do you check on your vendors control procedures prior to allowing them access?
- Do you have a guideline on what separates good vendor's system's controls from mediocre?

Talk to your AHT broker for these risk management tools as well as how your policy would respond from an unintentional act.

DATA BREACHES FROM OUTSIDE FORCES

This is the most common thought of exposure in regards to cyber data breaches are hackers from the outside. This is certainly one of the more common causes of loss in regards to data breaches, accounting for around 30% as the most frequent cause of loss according to a 2014 NetDiligence report. Indeed, whether it is an outside hacking group, or sometimes more commonly, students breaching school systems, it is important to make sure these liabilities and notification requirements are handled accordingly.

The Breach(es):

In El Paso's Independent School District, an outside hacker in 2011 gained access to their internal network's database which included names, addresses and Social Security Numbers for approximately 63,000 students and 9,000 employees.

In 2011 in Palatine, IL, the Illinois Department of Education reported two laptop computers belonging to a state contractor containing information, including social security numbers, of 7,800 special education students and 2,600 teachers from 42 suburban Chicago school districts were stolen from a car at a Palantine hotel.

In 2012, a private school's Salesforce data containing their list of their fundraising benefactor's information, including names, email addresses and donation sizes was hacked by an outside organization.

The Result:

The end results of these breaches are still unknown in terms of total cost and some could be quite severe. Of particular concern to schools is the potential for latency claims and identity theft.

Risk Implication:

Many hacking organizations target student data (especially social security numbers and birth dates) to use for identity theft purposes. Often times, parents are not monitoring their child's credit report since they have not yet established a credit history.

As schools aggregate the data on many hundreds or thousands of young people, the potential exposure of the stolen personally identifiable information may not become known for many years until the students reach the age of majority. For example, if there were a breach of personally identifiable information on a series of 12-year-olds additional claims may not come forward for six years in the future. And when students disperse to colleges around the country, a school may have to comply with dozens of different state beach notification laws to properly inform students that their information has been compromised.

However, it is important to review state laws with your broker before a breach occurs to determine the appropriate limit, identify what is personally identifiable information according to your state and begin implementing a contingency plan in the event of a breach to help reduce your costs.

SO I'M EXPOSED…NOW WHAT?

Unlike other exposures that insurance professionals deal with, privacy and security risks require much more stringent and diligent risk management efforts. And in many cases, unlike other exposures, these proactive measures may have very little to do with an incident actually occurring. Put another way, despite your best efforts at risk mitigation risk avoidance and so forth cyber breaches are still very likely to happen.

This poses an unnerving challenge to most board members and officers, as in the example of Target, a large data breach often results in an officer's dismissal due to their inherent breach of duty in their management of the security measures taken.

Obtaining a proper privacy and security (cyber) policy can help transfer some of the risk to an insurance carrier as long as the policy is written in the way you intend to cover the exposures you wish to transfer.

Many insurance buyers are opting to elect cyber coverage due to the guidance and resources the carriers can provide for both before and after a loss occurs. Whether it's the crisis management expertise in dealing with the adverse media concerns from a breach, developing proper internal procedures, or even a pre-hack penetration test of your IT systems, different carriers can offer tremendous resources that are included in your premium payment.

The most important aspect in all this of course is to have your trusted brokerage firm/advisor help navigate you and your board through this exposure to plan for accordingly.

AHT Insurance is one such brokerage firm that has deep experience in the area of addressing privacy and security related exposures with their clients. Our long standing affiliation with TechAssure as a founding member and continued involvement in the technology industry provides our schools with unique access to expertise and direct market placement and representation that can help position your school for the most favorable outcome.

Contact us today to review your data breach exposures.

ABOUT THE AUTHORS

Derek Symer

Principal, Senior Vice President
dsymer@ahtins.com

Derek Symer brings a special understanding of independent schools to AHT Insurance, thanks to more than a decade of experience in this space. Derek has helped grow AHT's Education practice and his work within this sector has given him insight into the multitude of risks facing educational organizations today. These risks range from management and professional liability, to campus safety, cyber and international risks. Derek is a Principal at AHT and earned his CPCU designation in 2008.

Outside of AHT, Derek has served president of the Dartmouth Club of Washington, D.C., which earned the 2006 Dartmouth Club of the Year Award under his leadership. He also has been honored as the Dartmouth Club "President of the Year" and has served on the Dartmouth Alumni Council. His other interests include playing the guitar, painting and tennis.

Prior to joining AH&T in 2003, Derek worked in the office of historical research at the Holocaust Memorial Museum in Washington, D.C.

Brian King

Assistant Vice President
bking@ahtins.com

Brian King is deeply involved in AHT’s Education practice in the Northwest. Brian focuses on insurance and risk management solutions for technology based clientele, independent school organizations and other nonprofits. He is particularly experienced at helping his clients identify, plan, and design innovative risk management solutions addressing their exposures across all avenues of their operation.

Outside of the office, Brian’s interests include hiking, drawing, golf and being with his wife and newborn daughter.

Brian joined AHT in 2014 with five years of experience across all aspects of the insurance industry including retail, underwriting, and wholesale insurance brokerage capacities at multi-national corporations.

REFERENCES

- Betterly, Richard S. “Cyber/Privacy Insurance Market Survey.” The Betterly Report. 2014
- 2002 Brenda Scott vs. Minneapolis Public Schools (No. A05-649).
- NetDiligence 2014 Cyber Claims Study
- Cassuto, Dan. “Thousands of students affected by Seattle data breach.” November 11, 2014. www.king5.com
- Loria, Gaby. “Thousands of EPISD Students, Employees At Risk of Identity Theft.” August 31, 2011 www.kvia.com
- Associated Press. “Education department laptops swiped in Palatine”. June 27, 2011. www.dailyherald.com
- Basu, Eric. “Target CEO Fired – Can You Be Fired If Your Company Is Hacked?” June 14, 2014 www.forbes.com