Gallagher

Insurance | Risk Management | Consulting

Threats and Consequences of K-12 Cyber Attacks

New Cyber Threats

Cyber extortionists have recently turned to "threats of violence, shaming and bullying of children" to induce school districts and other educational institutions to pay ransoms, according to an Alert Advisory from the Department of Education. Similar attacks have been reported in three states. These new tactics are in addition to more common threats of disclosing personally identifiable information, destroying important data or crippling computer networks, all of which create a myriad of problems for school administrators.

To illustrate the impact of this latest cyber threat, 30+ schools in the Columbia Falls School District, MT, were forced to shut their doors for three days, after they were hacked, private information compromised, and extreme threats were received demanding a six-figure ransom. The attack came from the group Dark Overlord, which has also perpetrated other high-profile hacks. The group has proven to be unreliable with honoring promises after receiving ransoms; however, it has also failed to deliver on threats of violence.

Ransomware Attacks

Another trend impacting K-12 institutions is the escalating number of ransomware attacks. Unfortunately, a ransomware attack may manifest itself in a myriad of possible consequences. Focusing on the obvious cyber extortion demand alone is a common pitfall that many victims make when addressing this threat. Some of the potentially bigger concerns that may arise include:

1. Breach of Confidential Information
2. Damage to Data
3. Theft of Funds
4. Business Interruption / Extra Expense
5. Reputational Risk
6. Bodily Injury

K-12 Cyber Risks

With restrictions on security budgets and large amounts of private information, schools have long been considered low-hanging fruit for cyber criminals. K-12 institutions face constant threats from outsiders seeking to exploit vulnerabilities to gain access and achieve their purposes. It is important to recognize and guard against these risks, and to have adequate insurance in place as part of a holistic cyber risk management program.

Prudent Pre-Breach Actions

The key areas of a comprehensive cyber risk management plan include: cyber security readiness; classification and protection of PII; regulatory compliance; pre- and post-breach preparation; and vendor management.

To highlight pre-breach preparation, organizations should have an Incident Response Plan that involves every functional area with responsibility for managing cyber risk. The organization should select several qualified privacy attorneys, in the event that a conflict arises. Many cyber insurance policies designate privacy attorneys that may be used, while others allow flexibility in counsel selection.

Prudent Incident Response

The following steps should be taken when a breach occurs to properly position the organization and to ensure that insurance will apply:

a. Contact a pre-selected privacy attorney immediately to establish privilege and begin the investigation. This attorney will work to ensure relevant information is preserved.
b. Engage a forensics investigator with guidance of the privacy attorney. This selection may require insurance company's approval. The privacy attorney will engage the forensic investigator to protect the exchange of information under privilege.
c. The insurance company may require immediate notification and notice should also be given to the insurance broker. These notices should only include the facts that are available. Updates should be provided as they become available.

Cyber security and risk management has become a critical concern for k-12 institutions, oftentimes ranking first or second in priority. Institutions are constantly seeking solutions to manage their evolving vulnerabilities to cyber risk. Unfortunately, even the most vigilant network security and comprehensive privacy policies can be vulnerable to increasingly smarter hackers, rogue employee activity, social engineering, vendor negligence and human error. Therefore, all educational institutions must take a holistic approach to cyber security and risk management.

To learn more, please join Gallagher's Cyber expert for a robust breakout session January 17th, at the Wisconsin State Education Convention. https://wasb.org/timetable/event/breakout-session-330-430-pm/

Nancy Moon Area Vice President

Gallagher

Insurance | Risk Management | Consulting

mobile: 262.853.6356 | direct: 262.792.2240
nmoon@ajg.com
www.ajg.com

245 S. Executive Dr., Brookfield, WI 53005