

What You Need to Know: Canvas Cyber Event

The **recent cyber breach of Canvas**, a web-based learning management system (LMS) used by educational institutions, is again raising concerns that the country's public and private schools and universities are prime targets for cybersecurity incidents. And while the threat actor ShinyHunters claims to have stolen personally identifiable information (PII) as well as billions of communications, affected institutions lack detailed information about exactly what data was exposed.

According to the U.S. Department of Education, **school districts experience an average of five cyber incidents per week**. This most recent attack is similar to last **year's attack on PowerSchool**, when a customer support portal was accessed using compromised credentials, exposing the PII of millions of students and teachers.

Based on current reporting, the Canvas incident involved data exfiltration without encryption-based malware. The threat actors have demanded a ransom and could attempt to extort individually impacted institutions. Social engineering attempts as well as attempts to gain unauthorized access to school systems where the same password may be used for Canvas and internal school systems, could also follow so it's important for schools and universities to remain aware.

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.



Reporting

In events like this, it is important to note that cyber policies vary greatly and may not all apply uniformly (or at all) depending on the paper, form or particular wording of each policy. And while Canvas, owned by Instructure, is reportedly working with affected schools and universities to resolve the outage and ensure the security of the system, there may be potential coverage implications resulting from this incident.

Therefore, it is **critical to advise insureds to do the following as soon as possible** after an alleged or actual cyber event is discovered.

- ➔ **Notify the insurer promptly.** Many cyber policies have limits on when an incident must be noticed to an insurer (often triggered by the discovery of an incident by an executive or employee). Insurers add these requirements so their position is not prejudiced by latent reporting. With the time-sensitive nature of cyber claims, this point is critical. Even a “Notice of Circumstance” ensures timely reporting in the event of a loss. Additionally, notice to an insurer opens the lines of communication and allows access to response professionals and/or legal professionals to help insureds navigate the situation.
- ➔ **Engage their broker.** If there is a suspected impact to an insured, it is important they:
 - Discuss with their broker what may be covered under the policy.
 - Notify the carrier according to the guidelines of the policy terms and conditions.
 - Work with the breach coach to determine next steps.
- ➔ **Work with the carrier prior to engaging outside vendors or legal services.** Often policies do not respond to costs incurred without consent or prior approval. Transparency and communication with the carrier as the situation unfolds is critical for a successful resolution.

Amwins is here to help

Don't hesitate to contact your Amwins professional lines broker with any questions or account needs during this time. We will leverage our full arsenal of expertise, market relationships and resources to deliver the best result for you and your clients.

As true cyber insurance specialists, the brokers in Amwins' national professional lines practice group stay vigilant for our clients, and offer the following advantages:

- Adept at navigating policy wording and market trends to secure the right coverage for accounts of all sizes and complexities.
- Exclusive amendatory endorsements with key carrier partners to ensure consistency and quality in our cyber and technology E&O product offerings.
- Proprietary digital quoting platform to streamline the quote process and offer competitive, vetted, and comprehensive quote options on a given risk.
- Exclusive cyber solutions and continually striving to develop innovative products and offerings as the market allows – standard is not our baseline.

Having an experienced wholesale broker on your side to help you navigate a cyber event can lead to a more efficient claims process and lead to a better result for your clients.