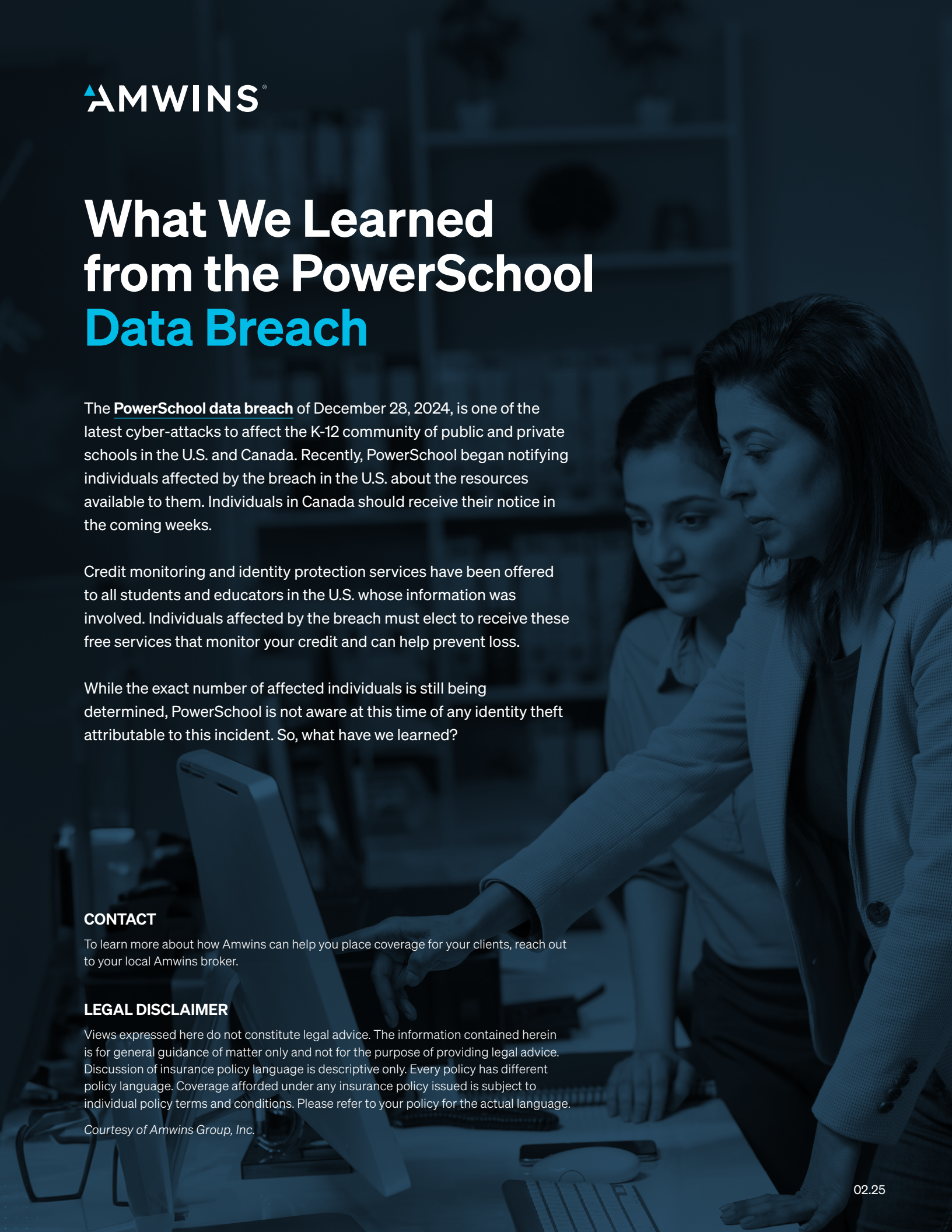
AMWINS

What We Learned from the PowerSchool Data Breach

The **PowerSchool data breach** of December 28, 2024, is one of the latest cyber-attacks to affect the K-12 community of public and private schools in the U.S. and Canada. Recently, PowerSchool began notifying individuals affected by the breach in the U.S. about the resources available to them. Individuals in Canada should receive their notice in the coming weeks.

Credit monitoring and identity protection services have been offered to all students and educators in the U.S. whose information was involved. Individuals affected by the breach must elect to receive these free services that monitor your credit and can help prevent loss.

While the exact number of affected individuals is still being determined, PowerSchool is not aware at this time of any identity theft attributable to this incident. So, what have we learned?



CONTACT

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

LEGAL DISCLAIMER

Courtesy of Amwins Group, Inc.

02.25

Social engineering may have been a factor

Social engineering, a form of deception used to manipulate individuals into divulging confidential information or inducing fraudulent monetary transfers, has become one of the most frequent causes of financial loss. According to **Education Week**, PowerSchool's PowerSource customer support portal was accessed using compromised credentials, exposing the personal information of millions of students and teachers.

Over the past decade, social engineering has evolved from rudimentary email scams to advanced tactics including deep fakes and real-time impersonation. You can learn more about how cyber and crime insurance policies respond to social engineering **here**.

Vendor management is key

Vendor security controls are just as important as an insured's. Many businesses and entities rely on others to support their business operations, so it's important to ensure that any vendors, suppliers or others who have access to a company's or entity's system take security seriously and do not offer a compromising entry path for threat actors.

It's also important to review vendor contracts often and ensure mutual understanding of the terms. Even if liability is contractually transferred, ambiguity around details may still exist. It's imperative to understand the expectations of applicable jurisdictions following a cyber incident as contracts may not supersede regulatory requirements.

It is also reasonable for organizations to require their vendors to purchase their own cyberliability insurance policy. It's important to have an insurance professional review both the insurance requirements in the service contract as well as understand how the insured's and vendor's cyber insurance policies interact. Never assume the policy another organization carries will cover you for your losses. Most policies will only cover the named insured's losses and may not extend to backstop the transfer of liability as intended in the contract. There is no industry standard cyber insurance policy.

Remember, every company is susceptible to a cyberattack. These attacks can result in costly delays and the degradation of a product or performance. Having multiple, vetted vendors can save critical time and money in the event one of them is compromised by a cyber incident.

And, finally, before incurring costs related to any incident, it's critical to partner with your cyber security carrier. Often there is no coverage for costs incurred without the carrier's consent. Generally, the carrier will have a breach response team ready and available to assist your client with guidance around what type of services and which vendors they may need to engage.

Timely reporting is vital

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 insurer, policy form or particular wording of each policy. Cyberliability policies are predominantly claims made and reported policies, meaning that the insurer is only responsible for paying claims both made AND reported to them within the policy period. Therefore, it is critical to advise insureds to do the following as soon as possible after an alleged or actual cyber incident is discovered.

Notify the insurer promptly. Many cyber policies have specific requirements for 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" can ensure timely reporting in the event of a loss. Additionally, notice to an insurer opens the lines of communication and allows access to response and/or legal professionals to help insureds navigate the situation. It is highly advised to give notice of any cyber incident to the insurer as soon as possible, even if it is uncertain it could trigger coverage. It's better to hear that the incident does not give rise to a covered claim than to hear it would have been covered but for the late reporting.

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.
- Don't make any assumptions about the applicability of coverage, just turn it in.
- Notify the carrier according to the guidelines of the policy terms and conditions.
- Work with the breach coach to determine next steps.

Amwins is here to help

The best defense is a good offense. As a leading cyber liability wholesale broker, Amwins has the expertise, resources and products to help protect your clients from a myriad of cyber risks. We stay on top of emerging threats and work with you to create a tailored solution that meets your client's needs.

We offer our clients discounts with industry-leading cyber security service providers who can help insureds improve their risk profile and we stay vigilant for our clients, offering the following advantages:

- 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; we continually strive 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.

Insights provided by:

- Megan North, EVP with Amwins Brokerage in Seattle, WA