PowerSchool Incident Review Call

for Superintendents and Charter School Leaders
January 13, 2025

North Carolina Department of PUBLIC INSTRUCTION

Agenda

- Review of the PowerSchool Data Breach Incident
- Support for PSUs and Next Steps
- Submit Your Questions

Review of the PowerSchool Data Breach

Chief Information Officer Vanessa Wrenn

Review of the Incident

- Around 2 p.m. on January 7, PowerSchool sent an email notifying all North Carolina public schools (PSUs) and DPI about a cybersecurity incident impacting student and teacher data across their entire client base.
- The incident is contained and the data is destroyed.
- The Dark Web is being monitored by law enforcement agencies.
- PowerSchool worked with two cybersecurity companies to gain assurance of data destruction.
- All NC PSUs who have ever been on PowerSchool were part of the incident, impacting records from Summer 2013 to the present.

Review of Incident

- No actions by PSUs or NCDPI could have prevented this event. The threat actors used PowerSchool administrative access with a back door entry at the cloud level.
- This is a global incident.
- Analysis of the student and teacher data shows some student SSNs were compromised.
- Many more Teacher SSNs are impacted.
- All legal notifications will be conducted by PowerSchool.
- PowerSchool indicates an internal goal for notification by the end of January.

Timeline of Events

- **Dec. 28:** PowerSchool was notified by threat actors that student and teacher data had been accessed.
  - Forensics show threat actors gained access on Dec. 19.
  - PowerSchool began working with two specialized cybersecurity companies, Crowdstrike and CyberSteward, to begin forensics and ensure containment.

- **Dec. 28 - Jan. 7:** PowerSchool gained assurances and put security mitigations in place to ensure the SIS has no more ongoing threats or system compromises.
  - PowerSchool contacted PSUs and DPI.
  - DPI requested log files and confirmed PowerSchool information working with the NC Government Local Information Systems Association IT Strike team.
  - Parent awareness templates were provided.

What We Know

- The incident occurred when a PowerSchool contracted employee's credentials were compromised via malware allowing unauthorized access to an administrative maintenance tunnel.
- Unauthorized access to the maintenance tunnel by the threat actor allowed the ability to log into each instance, cloud hosted by PowerSchool.
- The threat actor used a database export manager to download student and teacher tables.
- PowerSchool paid the threat actors working with CyberSteward.

NCDPI's Support and Next Steps

Chief Information Officer Vanessa Wrenn

Support and Next Steps

- PowerSchool will provide breach notification for each impacted user.
- PowerSchool has created a website to support schools, parents, and educators.
- PowerSchool is establishing a call center.
- PowerSchool is working on plans regarding protection of individuals with more to be shared as finalized.
- PowerSchool will conduct a webinar for PSUs with time to be determined.
- DPI General Counsel, Allison Schafer will conduct a meeting with local board attorneys.

Support and Next Steps

- PSU technology leaders will receive a spreadsheet detailing the student and teacher data elements and the number of records associated with each data element to better understand the data that was compromised.
- This will show if a PSU had student SSNs and the number teacher SSNs.
- The spreadsheet classifies each data field as either Directory Information (DI) or Personally Identifiable Information (PII).
- Contact your technology director for more information about the Teacher and Student Data Field Tables.

Support and Next Steps

NCDPI will provide office hours for PSU technology directors to understand the impacted student and teacher data.

Tuesday, January 14, 2025

- 11:00 a.m. -11:30 a.m.
- 1:00 p.m. -1:30 p.m.

- **Wednesday, January 15, 2025**
  - 11:00 a.m. - 11:30 a.m.
  - 3:00 p.m. - 3:30 p.m.
- **Thursday, January 16, 2025**
  - 10:00 a.m. -10:30 a.m.
  - 3:00 p.m. - 3:30 p.m.
- This information will be shared with technology leaders via email.

Resources

- https://ncdoj.gov/protecting-consumers/protecting-your-identity/free-security-freeze/
- PowerSchool FAQ
- PowerSchool resource site
- PowerSchool Direct Contact
  - Megan Veverk - megan.veverka@powerschool.com

Submit Your Questions