I. Introduction

Background of the Study

Data breaches are becoming a bigger worry in today's tech-driven world, affecting people, businesses, and sectors everywhere. The over-reliance on digital platforms has exposed flaws that bad actors take advantage of, leading to serious repercussions like identity theft, monetary loss, and damage to one's reputation. Because breaches involving sensitive student and instructor data raise ethical and security issues, this problem is especially important in the education sector.

PowerSchool, an online student information portal widely utilized in K–12 schools across North America, experienced a serious data breach in December 2024 (Collier, 2025; Page, 2025). Names, addresses, birthdates, Social Security numbers, and some medical alert details were among the sensitive information compromised in this incident, which impacted 75 school boards in Canada (Page, 2025). Concerns regarding corporate accountability and transparency were raised by PowerSchool's tardy revelation of the compromise (Collier, 2025). This study explores the breach's media coverage, economic effects, and ethical repercussions, emphasizing important factors for the educational technology industry.

Ethical Considerations

This paper explores the ethical issues related to the PowerSchool breach, including:

- **Privacy:** Exposure of students' Social Security numbers, medical records, grades, and other personal data.
- **Security:** Lack of fundamental cybersecurity measures, such as multi-factor authentication.
- **Transparency:** PowerSchool's delayed breach disclosure and its impact on stakeholder trust.
- **Handling of Sensitive Information:** The ethical duty of EdTech companies to protect student data.

II. Methodology

Source Selection

Sources for this analysis were selected from reputable news outlets, cybersecurity reports, and industry discussions. The primary sources include:

- NBC News
- TechCrunch
- CrowdStrike
- Cybersecurity Dive

- TechTarget

Criteria for Analysis

The coverage of the PowerSchool data breach is analyzed based on:

- Bias: Examining how media sources portrayed the breach and PowerSchool's role.
- Truth and Fairness: Evaluating the accuracy and objectivity of reports.
- Economic Considerations: Assessing the financial implications for PowerSchool and affected institutions.
- Competition and Deception: Exploring how the breach affects trust in EdTech providers.
- Emotional vs. Rational Approach: Analyzing whether the coverage prioritized emotional impact or factual cybersecurity discussions.

III. Analysis

Summary of Coverage

The PowerSchool data breach is considered one of the most significant student data breaches to date. According to NBC News and TechCrunch, hackers accessed sensitive personal information, including student grades, medical records, and Social Security numbers. Reports indicate that the breach affected over 62 million students and 9.5 million teachers in the United States, though PowerSchool has not confirmed these figures. The breach originated from a single compromised employee credential, which granted unauthorized access to the SIS system (CrowdStrike, 2025).

PowerSchool initially disclosed the breach in January 2025 but withheld specific details, raising concerns about transparency. A cybersecurity audit conducted by CrowdStrike revealed that the company failed to enforce basic security protocols, such as multi-factor authentication, which allowed the hacker to gain access easily (CrowdStrike, 2025).

Ethical Concerns

Privacy

The breach compromised highly sensitive student information, including Social Security numbers, medical records, and disciplinary records. Schools rely on PowerSchool to securely store this data, but the breach exposed vulnerabilities in the company's cybersecurity practices. The exposure of students' personal data creates long-term risks, including identity theft and unauthorized access to private information.

Security

The CrowdStrike cybersecurity audit found that PowerSchool's systems lacked fundamental security protections. The hacker gained access through a single compromised credential, emphasizing the absence of multi-factor authentication. This security failure is particularly concerning given the sensitivity of student data and the increasing frequency of cyberattacks on educational institutions.

Transparency

PowerSchool delayed publicly disclosing the breach, leaving schools, students, and parents in the dark about the potential risks. Reports indicate that PowerSchool paid a ransom to the hacker in exchange for assurances that the stolen data would be deleted (Abrams, 2025). However, cybersecurity experts caution that there is no guarantee that the hacker did not retain copies of the data. The lack of immediate transparency raises ethical questions about PowerSchool's responsibility to inform stakeholders promptly.

Handling of Sensitive Information

PowerSchool's failure to protect student data highlights broader concerns in the EdTech industry. Schools entrust private companies with sensitive student information, yet there are no universal cybersecurity standards to ensure the protection of such data. The breach demonstrates the urgent need for stricter security regulations and oversight for EdTech providers.

Additional Insights from Cybersecurity Dive

PowerSchool told K-12 Dive that it became aware of a “potential” cybersecurity incident on December 28, 2024, in which a threat actor gained unauthorized access to an unknown amount of student and staff data from its PowerSource service (Merod, 2025). The threat actor is believed to have stolen data from two tables containing family and teacher information from PowerSchool’s Student Information System database, potentially exposing personally identifiable information such as names, addresses, Social Security numbers, and medical data.

Despite PowerSchool stating the incident was not a ransomware attack, Bleeping Computer reported that PowerSchool’s FAQ page acknowledged a payment to the threat actor following the breach. During a Jan. 15 webinar, Doug Levin from K12 SIX emphasized that paying extortion demands endangers the education sector by encouraging future attacks and that there is no guarantee stolen data won't be further exploited.

Speakers raised questions about whether PowerSchool used multifactor authentication for its PowerSource service before the breach. While PowerSchool’s internal systems used multifactor authentication, the PowerSource system did not. This has since been addressed through remediation.

Biases in Coverage

1. Bias Toward Underreporting Risks: Educational institutions often underreport the risks associated with data breaches. The breach highlights a systemic bias where the education sector, particularly K-12 institutions, may not prioritize cybersecurity

as highly as other sectors. This is evident in the fact that PowerSchool, despite being a major provider for over 18,000 organizations and 60 million students, did not communicate the breach to its customers until nearly two weeks after discovering it (Kerner, 2025; Merod, 2025). This delay raises concerns about transparency and accountability in reporting such incidents.

2. Bias in Resource Allocation: There is a noticeable bias in resource allocation towards educational outcomes rather than cybersecurity measures. Many schools may lack the necessary funding and expertise to implement robust cybersecurity protocols. The breach underscores this issue, as attackers exploited compromised credentials that were reportedly available on the dark web for some time before the attack (Merod, 2025). This indicates a failure to adequately invest in cybersecurity defenses, which could have mitigated the risk of such an incident.
3. Bias Against Recognizing Vulnerabilities: The incident reflects a bias against recognizing and addressing vulnerabilities within existing systems. The breach was facilitated through PowerSchool's customer support portal, which allowed unauthorized access due to credential theft (Kerner, 2025). This suggests a lack of proactive measures to secure sensitive access points and highlights a general underestimation of the sophistication of cyber threats facing educational technology platforms.
4. Bias in Stakeholder Communication: The communication strategy employed by PowerSchool also reveals biases in how stakeholders are informed about data breaches. The delayed notification to affected schools and families may reflect a

bias towards protecting corporate reputation over ensuring timely information dissemination to those impacted by the breach (Kerner, 2025; Page, 2025). This can exacerbate feelings of mistrust among users regarding how their data is managed and protected.

Economic Considerations

Cost of Breaches

The financial impact of the PowerSchool breach includes potential lawsuits, regulatory fines, and reputational damage. The breach may also prompt increased cybersecurity spending by schools and educational institutions to prevent future incidents.

Investment in Security

The breach underscores the need for EdTech companies to prioritize cybersecurity investments. PowerSchool's failure to implement multi-factor authentication suggests a lack of commitment to fundamental security measures. Moving forward, companies that prioritize data protection may gain a competitive advantage by building trust with schools and parents.

Competition and Deception

Competitive Advantage

The breach may encourage schools to seek alternative EdTech providers with stronger security measures. Companies that demonstrate robust cybersecurity practices may benefit from increased demand as educational institutions prioritize data protection.

Deceptive Practices

Reports indicate that PowerSchool delayed disclosing the breach and downplayed the extent of the impact. The company's lack of transparency raises ethical concerns about whether EdTech providers adequately inform stakeholders about cybersecurity risks.

Emotional vs. Rational Appeal

Emotional Appeal

News coverage has emphasized the emotional toll on affected students and families. Reports highlight concerns about identity theft and the long-term consequences of stolen personal information. Schools and parents are now forced to navigate the uncertainty of whether student data has been permanently compromised.

Rational Approach

Beyond the emotional impact, some coverage has provided rational discussions on the importance of cybersecurity in education. Reports emphasize the need for improved security standards, increased investment in cybersecurity, and stronger regulatory oversight for EdTech companies.

IV. Conclusion

Summary of Findings

The PowerSchool data breach highlights significant ethical concerns, including failures in privacy protection, security enforcement, and transparency. The company's inadequate security measures allowed a hacker to gain access using a single compromised credential. The delayed disclosure of the breach and the potential ransom payment further raise ethical questions about PowerSchool's response.

Insights and Implications

The breach underscores the urgent need for stricter cybersecurity standards in the EdTech industry. Schools must demand greater accountability from technology providers, and policymakers should implement regulations to ensure student data protection. This case also serves as a warning about the risks of entrusting private companies with highly sensitive information without proper oversight.

Recommendations

- Governments and educational institutions should establish baseline security requirements for EdTech providers to ensure that all platforms adhere to a minimum standard of cybersecurity. This would create a safer digital learning environment by protecting students' data from potential threats and providing a consistent level of security across all educational technology.
- Companies handling student data must implement strict Multi-Factor Authentication (MFA) measures to prevent unauthorized access. By requiring more

than one method of verifying a user's identity, such as a combination of passwords, biometric data, or smartphone verification, MFA significantly reduces the risk of data breaches and protects sensitive student information.

- Organizations should be required to promptly disclose any data breaches and provide clear information on their impact. Transparency in data breaches builds trust, allows affected parties to take necessary protective actions, and holds organizations accountable for their data security practices. This approach fosters a culture of openness and responsibility.
- Schools and EdTech companies must allocate resources to improve their cybersecurity infrastructure and training. Investment in cybersecurity ensures that the technology used is robust against attacks and that staff are adequately trained to handle potential threats. A proactive approach to cybersecurity helps mitigate risks and safeguards student data effectively.

The PowerSchool data breach serves as a critical reminder of the ethical and security challenges facing the education sector. Addressing these concerns requires collective action from schools, policymakers, and technology providers to protect student information and prevent future cyber threats.

References

Abrams, L. (2025, January 7). *PowerSchool hack exposes student, teacher data from K-12 districts*. Bleeping Computer. Retrieved March 8, 2025, from https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/

Collier, K. (2025, January 31). *PowerSchool hack: missed basic security step resulted in data breach*. NBC News. Retrieved March 8, 2025, from https://www.nbcnews.com/tech/security/powerschool-hack-data-breach-protect-student-school-teacher-safe-rcna189029

Kerner, S. M. (2025, January 23). *PowerSchool data breach: Explaining how it happened*. TechTarget. Retrieved March 8, 2025, from https://www.techtarget.com/whatis/feature/PowerSchool-data-breach-Explaining-how-it-happened

Merod, A. (2025, January 10). *PowerSchool data breach possibly exposed student, staff data*. Cybersecurity Dive. Retrieved March 8, 2025, from https://www.cybersecuritydive.com/news/powerschool-data-breach/737024/

Page, C. (2025, February 3). *What PowerSchool won't say about its data breach affecting millions of students*. TechCrunch. Retrieved March 8, 2025, from https://techcrunch.com/2025/02/03/what-powerschool-isnt-saying-about-its-massive-student-data-breach/