# Schools struggling with cybersecurity amid rise in cyberattacks



Schools across the United States have experienced a significant surge in cyberattacks during the past five years, particularly since the onset of the COVID-19 pandemic. An investigation by The 74 reveals a concerning trend among district leaders to obscure details about these attacks, leaving the affected students, parents, and staff uninformed about the risks associated with breaches of sensitive information.

The detailed analysis conducted by The 74 examined over 300 cyberattacks targeting K-12 schools, identifying a pattern where school administrators often issued reassurances that sensitive data had not been compromised, only to later retract those statements months or even years later when faced with evidence to the contrary. In particular, personal data related to special education accommodations, mental health issues, and incidents of student misconduct have been among the types of information exposed.

The investigation highlights a critical reality in cybersecurity response protocols within schools: when a cyberattack occurs, the first responders are often not from law enforcement or the public but rather from insurance companies and their legal teams, prioritising the minimisation of potential lawsuits from parents and staff. This approach often leads to a prioritisation of legal considerations over transparency.

Ransomware gangs, which specifically target the education sector, have been particularly aggressive. Companies like Rhysida conduct systematic campaigns that involve stealing data and threatening to release it unless a ransom is paid. Such incidents have notably escalated; in 2023, there were 121 reported ransomware attacks on U.S. educational institutions, a number considered to be under-reported, with a global perspective indicating a 70% year-over-year increase in similar attacks, making 2023 a record year for incidents in the education sector.

Daniel Schwarcz, a professor at the University of Minnesota, provided insight into the legal manoeuvring that often follows these breaches. In an interview with The 74, Schwarcz noted that the reliance on breach coaches – legal professionals appointed to handle the crisis and protect school systems from liability – often leads to communications that walk a fine line between vague reassurances and misleading claims about the extent of the breaches.

The obfuscation of critical information leaves students and families unaware of their potential exposure to identity theft and other forms of cybercrime. While the aftermath of these attacks should ideally involve prompt disclosure to affected individuals, many school officials choose to maintain silence, even signing agreements to pay ransom demands behind closed doors, further complicating transparency.

A further analysis reveals that school districts may fail to disclose data breaches as legally required under various state laws, with many incidents not reported to relevant authorities, or dealt with in such an opaque manner that communities affected by the breaches remain unaware of the full implications of the attacks.

In some instances, schools that reported cyberattacks initially described them in ways that downplayed the severity. For example, emails sent to parents following an attack might use vague language such as "anomalous activity" instead of directly addressing the situation as a cyberattack.

In various responses to the findings of The 74, education leaders have defended their positions, claiming that a lack of transparency has been motivated by a desire to preserve the integrity of ongoing investigations, rather than an intention to mislead. They highlight efforts made on their part to notify affected individuals promptly, yet discrepancies persist between their internal records and public communications, raising concerns among watchdogs and affected community members.

Moreover, there is an increasing reliance on insurance companies to navigate these crises, creating a situation where the financial implications of a breach could overshadow ethical considerations. Industry experts have raised concerns that this relationship may lead to decisions prioritising monetary outcomes over the welfare of students whose data may be compromised.

Federal efforts to bolster school cybersecurity and public accountability are underway, but as of now, school districts continue to grapple with the ramifications of cyberattacks in an environment that often lacks clear regulatory enforcement. The complex interplay between law enforcement, legal counsel, and insurers leaves many school officials ill-equipped to manage the fallout from cyberattacks effectively, ultimately sidelining the interests of those most affected.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/> - This article provides statistics on cybersecurity incidents in education, highlighting the increasing number of attacks and the challenges faced by educational institutions in responding effectively. It supports the claim that schools have experienced a significant surge in cyberattacks.
* <https://cmitsolutions.com/richardson-tx-1049/blog/8-eye-opening-statistics-about-cybersecurity-in-education/> - This blog post discusses the high incidence of cyberattacks in the education sector, ranking it among the most targeted industries. It corroborates the trend of increased cyberattacks on schools, particularly during the pandemic.
* <https://www.varonis.com/blog/education-cybersecurity-statistics> - This article highlights the prevalence of cyberattacks in education, noting that nearly two-thirds of facilities reported attacks in 2024. It supports the claim that ransomware attacks have escalated significantly in recent years.
* <https://www.k12cybersecure.com/map/> - The K-12 Cyber Incident Map tracks publicly disclosed cybersecurity incidents in U.S. K-12 public schools, providing evidence of the rising number of attacks and supporting the claim of increased cyber threats against schools.
* <https://www.cisa.gov/insights/spotlight/education-sector-cybersecurity> - CISA's insights on the education sector highlight the vulnerability of schools due to extensive personal and financial data, supporting the claim that schools are prime targets for cyberattacks.