A Federal Anchor Unmoored:

Why Student Data Is at Risk

Overview

As headlines swirl around the potential elimination or drastic restructuring of the U.S. Department of Education (ED), the conversation has largely centered on politics, funding, and classroom oversight. But there's a quieter crisis emerging — one that lives in code, servers, and unpatched systems: the cybersecurity of America's education sector.

This isn't just an operational concern. It's a matter of national security.

The Department of Education has long served as the federal convener, funder, and cyber policy anchor for school districts, higher education institutions, charter schools, and EdTech providers. These entities collectively manage vast stores of sensitive information — not just academic records, but also health histories, immigration status, financial aid data, and more. Remove the centralized infrastructure that ED provides, and you risk exposing that data — and the students behind it — to heightened cyber threats with diminished safeguards.

A Federal Anchor Unmoored

Historically, ED has long partnered with federal agencies such as CISA and DHS to ensure that cybersecurity guidance for schools aligns with broader national strategies. It has played a crucial role in translating evolving federal cyber guidance into actionable standards for schools — often underfunded and under-resourced — to follow.

If that anchor is pulled, what remains is a policy vacuum. Without federal guardrails, states will be forced to create their own. Some will rise to the challenge. Many will not. The result? A fractured landscape of inconsistent policies, variable enforcement, and a growing number of vulnerable entry points for cyber actors to exploit. The unintended consequences of inadequate cybersecurity controls are insufficient privacy safeguards – a key aspect of protecting the confidentiality of student and family data.

This isn't hypothetical. We already see uneven cyber maturity across the education sector. Charter schools and small districts — especially those lacking dedicated IT or security staff — are among the most exposed.

Funding Pipelines in Peril

ED’s influence isn’t just about policy — it’s about dollars. Grants administered through Title I, Title IV-A, and CARES have played a vital role in enabling schools to implement key cybersecurity protections. Multi-factor authentication, breach detection software, and network security upgrades have all been supported through these programs.

Without ED’s stewardship, the future of these funding pipelines becomes murky. And the impact won’t be evenly felt — the hardest hit will be the same institutions already struggling to keep pace. Charter school networks and under-resourced school districts that lack the capacity to navigate complex grant processes may be cut off from the support they need to operate safely in a digital-first world.

Add to this the potential dissolution of ED’s Office of Educational Technology — a guiding force on responsible AI integration and digital equity — and the loss becomes even greater.

Student Data in the Crosshairs

One of ED's most important functions is oversight of FERPA, the federal law that protects student privacy. In a decentralized system, FERPA enforcement would likely fall to the states. But state agencies vary widely in capability, funding, and regulatory enforcement.

This opens the door for inconsistent protections and for EdTech vendors to exploit gaps in oversight. Without strong federal accountability, parents may no longer have assurance that their children's data is safe from misuse or unauthorized sharing.
And the risk isn't theoretical, it's unfolding in real time.

One day after the Department of Education's Office of Federal Student Aid (FSA) abruptly laid off nearly half its workforce in March, students and families across the country lost access to FAFSA. Though the outage was quickly resolved, it rattled confidence. Internally, many questioned whether the agency, now operating with skeletal teams, could effectively handle future technical failures, particularly those with national reach and personal consequences.

But the implications go far beyond service disruptions. A leaner workforce means a loss of institutional knowledge — the quiet, hard-earned know-how required to secure complex systems and anticipate evolving cyber threats. Former employees have warned that this knowledge gap could not only impair operational continuity but cost the agency — and the students it serves — dearly.

And make no mistake: cybercriminals are already watching. Between 2016 and 2022, more than 1,600 cyber incidents were reported in K-12 districts alone, from ransomware to phishing attacks, according to the nonprofit K12 Security Information Exchange (K12 SIX, *The State of K-12 Cybersecurity: 2022 Year in Review*, https://www.k12six.org/research). Education has become one of the most frequently targeted sectors by cybercriminals — a trend that continues to accelerate.

A Call for Local Leadership and the Right Partners

If federal leadership fades, local leaders must step forward. The responsibility for cybersecurity readiness, privacy protection, and incident response will rest squarely on the shoulders of school boards, superintendents, CIOs, and EdTech executives.

That starts with assessments — knowing where vulnerabilities live and how to address them. It means deploying privacy audits, building vendor risk management programs, and running simulations to train staff for when — not if — an attack comes.

It also means finding the right partners. Large bureaucracies and one-size-fits-all vendors won't cut it. What's needed are small, specialized firms with deep experience operationalizing federal cyber frameworks and a proven ability to execute.

The Classroom Is a Critical Frontline

As we enter an era of decentralized oversight, we cannot afford disconnected defenses. Fragmentation may be inevitable, but vulnerability doesn't have to be.

Now is the time for a coordinated, community-driven response. It's time for school systems to own their cybersecurity futures and to surround themselves with partners who can help them navigate it with precision and purpose.

School boards, superintendents, and EdTech providers must lead a new era of decentralized but coordinated cyber resilience. Student safety — both online and offline — depends on swift, smart action.

The classroom is now a frontline of national security. It is a digital battleground. And our students deserve every safeguard we can give them.

About TWW

The Wright Way Enterprises (TWW) is certified as an SBA 8(a) and HUBZone small business and DC Certified Business Enterprise (CBE), stewarding organizations in addressing the dynamic needs of an ever-changing global economy. Founded in 2020, TWW's comprehensive capabilities fortify federal and private infrastructure. The impact-driven consultancy specializes in program management, auditing, cyber risk management, and compliance. TWW's vision is to be globally trusted advisors in delivering robust solutions that protect data, preserve vital resources, ensure compliance, and optimize operations for excellence. For more information, visit www.twwenterprises.com.