Cybersecurity and the Cloud

K-12 schools may never be the same. And cybercriminals are making the most of it.

Many school infrastructures have been breached by malicious actors exploiting the rapid shift to online and hybrid learning. Outdated network configurations and undetected software vulnerabilities are only helping them in their nefarious endeavors.

When most schools turned to virtual or hybrid learning during the pandemic, millions of students and educators turned to the cloud. Soon it became clear that investing in a robust and resilient IT infrastructure such as cloud technology was a smart and necessary move. The cloud enabled schools and districts to adapt quickly in times of crisis and continue learning for students at scale.

Yet the pandemic has magnified K-12 cybersecurity challenges and complexities. Unsecure networks and personal devices were accessing district cloud environments—trading sensitive school data—like never before.

Compounded Threats

While K-12 IT had mainly focused on firewalls and content filters, now they had to contend with virtual meeting "bombings", malicious third-party apps, and various other online safety incidents. IT staff must also monitor where logins are coming from and possibly compromised accounts. And—in the case of online or hybrid learning—educators have a harder time identifying cybersafety signals such as cyberbullying and self-harm. And all this on top of the already pervasive threats of phishing and malware.

Three Main Areas of Concern

Amy McLaughlin, Project Director for the Cybersecurity and Smart Education Networks by Design (SEND) initiatives at CoSN, points to three main areas of concern for schools:

1. **Endpoint Management**: With so many devices running on home networks, it is a significant challenge for schools to maintain and monitor these devices.
2. **Targeted Attacks**: Phishing efforts allow hackers to compromise school networks and key services.
3. **Unmanaged Software**: Teachers and students introducing unmanaged software into school networks can pose significant risks.

Copyright © Clarity Innovations, Inc. All Rights Reserved.
Created with generous support from CDW-G and Intel.
* Other names and brands may be claimed as the property of others.

Cloud-based collaboration apps make it challenging for schools and districts to detect the unsafe sharing of content and sensitive personal data. So school IT has to step up their game, making up for such issues as: loss of visibility as to what users are accessing and how; data breaches and data loss; threats from inside the school infrastructure and misuse of cloud services; videoconference bombing; and sophisticated malware and phishing attacks.

So the time is now for IT administrators to evolve infrastructures and cybersecurity strategies to protect student data especially as the use of cloud technology and apps has increased exponentially.

Evolving Needs

Students—whether at school or at home—need effective connections to apps, data, and their school communities. Budget constraints and unpredictable demand often result in poor performance and an inability to connect to resources. Meanwhile, educators need to engage and retain students without overloading them with new user interfaces or login procedures.

Integrated cloud security solutions should help IT and security teams to gain traffic visibility, effectively control applications and the flow of data across networks and multi-cloud environments, and comply with regulations. Teams should also be able to leverage automation that detects, responds to, and prevents advanced threats.

Common Online Threats

According to the Federal Bureau of Investigation (FBI) and the Department of Defense's Defense Technical Information Center, some of the most common types of online threats are:

- **Data Breach**. Data breaches often occur with confidential information, such as students' records, that may be inappropriately viewed or used by an individual who should not have access to the information.
- **Denial of Service**. A Denial of Service attack, also known as a Distributed Denial of Service attack, occurs when a server is deliberately overloaded with requests such that the website shuts down. Users are then unable to access the website.
- **Spoofing/Phishing**. Spoofing refers to the dissemination of an email that is forged to appear as though it was sent by someone other than the actual source. Phishing is the act of sending an email falsely claiming to be a legitimate organization in an attempt to deceive the recipient into divulging sensitive information after directing the user to visit a fake website.
- **Malware/Ransomware**. Malware is illicit software that damages or disables computers or computer systems. Ransomware is a form of malware in which perpetrators encrypt users' files, then demand the payment of a ransom for the users to regain access to their data.
- **Removable Media**. Media devices that can be connected to computers, such as thumb drives, CDs, DVDs, and external hard drives, also pose challenges to cybersecurity.

Copyright © Clarity Innovations, Inc. All Rights Reserved.
Created with generous support from CDW-G and Intel.
* Other names and brands may be claimed as the property of others.

Cloud and Clear

Students not aware of emerging cyberthreats may be less careful and click on disguised phishing links. Teachers who haven't been properly trained on the latest cybersecurity trends may not be aware that a link is actually malicious. Both situations give cyber criminals access to a district's cloud environment—all without anyone being in a school building.

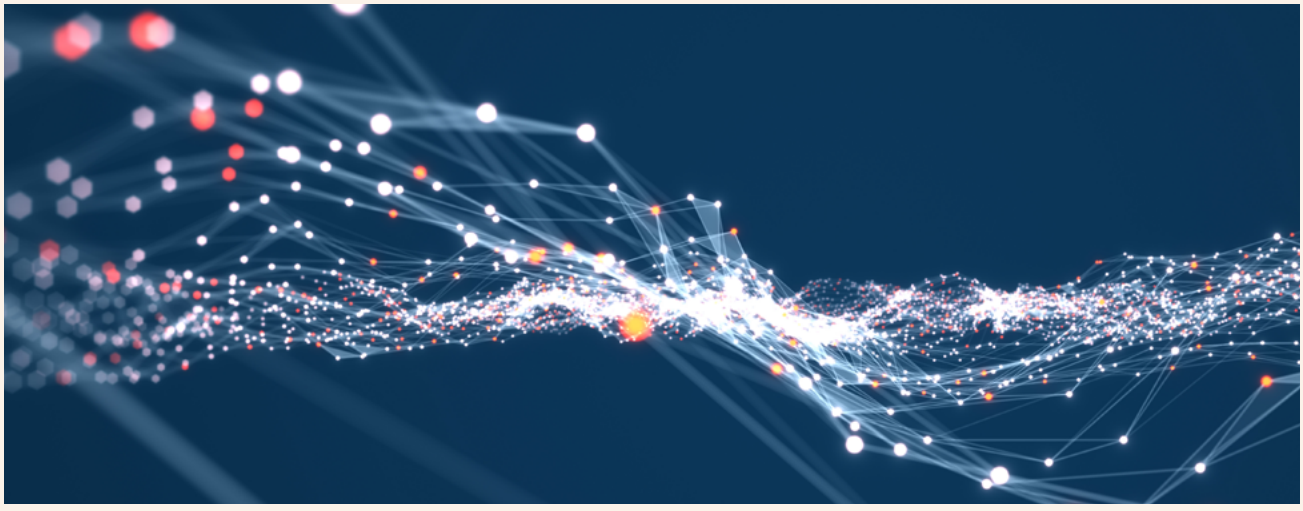
Districts must be ready to monitor their cloud environments more closely, as most student and staff activity will take place in these applications, and will need to face new and more advanced cybersecurity threats than before. Malware incidents are taking place in the cloud on student and staff accounts—perhaps even from unmanaged personal devices—but haven't been detected and disclosed. This is likely due to the fact that most districts are only able to detect malware attacks on their network, leaving them blind to threats in their cloud applications.

Protect and Serve

To protect their networks and cloud-based systems as part of an overall preparedness program, schools and school districts can do the following:

- Develop and promote policies on responsible use;
- Store data securely to ensure that the whole school community's data is kept private and to comply with the Family Educational Rights and Privacy Act (FERPA);
- Create firewalls and an approved list of individuals who have access to the school's or school district's networks and systems; and,
- Monitor networks continually to assess the risk from cyberthreats.

Other ways that IT teams can beef up their cloud security approaches include: understanding vendor security mechanisms, setting up appropriate permissions and controls, utilizing single sign-on and multifactor authentication, and providing cloud governance and compliance training.



Copyright © Clarity Innovations, Inc. All Rights Reserved.
Created with generous support from CDW-G and Intel.
* Other names and brands may be claimed as the property of others.

Don't Be Late to the (Third) Party

After transitioning to the cloud, school officials have been surprised to find how much personal information students share.

There are more third party cloud applications connected to district cloud environments as a result of the free or reduced pricing that vendors offered at the start of the pandemic. Millions of students and teachers now rely on these newly adopted apps for video conferencing, online chat, digital lessons, and bulletin boards. IT departments must audit their school's environment and see all the apps that have been granted risky permissions, potentially granting unauthorized access to cybercriminals.

This is why K-12 school districts have adopted cloud security tools to keep students safe and their information secure.

While newer cloud security tools must be implemented by IT staff to detect and prevent external and internal cybersecurity threats, some of these same tools can also monitor cyber safety risks. With less in-person interaction and supervision by teachers, and more apps being used by students, more risky interactions may go undetected.

Any school using Google for Education or Office 365 for Education, for instance, must have a cloud security solution in place to protect personally identifiable information and must be in compliance with FERPA, COPPA, and other regulations. Unfortunately, many IT managers in K-12 education think that their firewall and/or gateways are enough to keep data stored in the cloud secure.

Cloud Security Solution Requirements

- **Data Loss Prevention**: Schools that operate in cloud applications without a cloud security solution are not in compliance with government regulations requiring K-12 school districts to protect student data from malicious and accidental loss.
- **Malware and Threat Protection**: A cloud security solution helps IT and system admins quickly see risks and delete or quarantine them before they can lead to bigger issues.
- **User Monitoring**: K-12 education system admins need cloud security tools to see and control account behavior such as suspicious logins, suspicious sharing and downloads of files containing sensitive information, and more.
- **Content Scanning**: IT staff need visibility into the content that is being stored and shared on the cloud. The system should unshare, quarantine, or delete these types of files and automatically notify the proper administrator to take action.
- **No Gateways, Agents, or Proxies**: A cloud security solution follows students anywhere they're saving, sharing, and sending as well as anywhere they have logged in with their Google for Education account.

Copyright © Clarity Innovations, Inc. All Rights Reserved.
Created with generous support from CDW-G and Intel.
* Other names and brands may be claimed as the property of others.

CDW-G PEOPLE WHO GET IT
intel

Moving Forward: With Caution

Schools face a myriad of challenging hazards and threats. And while the cloud has brought with it unparalleled ease and functionality to help students and teachers to continue education despite online and hybrid learning scenarios, the risks to critical operations and the sensitive personally identifiable information of students, teachers, and staff cannot be ignored. Mitigating these and other risks is crucial as districts look to expand online learning initiatives and deploy IT infrastructure capable of supporting hybrid learning environments in the "next normal" of education.

School infrastructures are dealing with an unprecedented amount—and variety—of data and applications, coming from both inside and outside the school domain. And now that most schools are either planning to resume schooling in classrooms or adopting hybrid schedules, school IT are examining their infrastructures and seeing clearly the weaknesses and needs as they move forward to an uncertain educational landscape.

K-12 Blueprint Security Toolkit

Learn more about K-12 cybersecurity best practices and solutions from CDW-G by visiting the **Security** toolkit.

Copyright © Clarity Innovations, Inc. All Rights Reserved.
Created with generous support from CDW-G and Intel.
* Other names and brands may be claimed as the property of others.