PULSE | IDENTITY AUTOMATION

K-12 DISTRICTS MUST FACE MOUNTING CYBERSECURITY CHALLENGES

Due to the COVID-19 pandemic, many educational institutions are using remote or hybrid learning models. This growing digital footprint has created a prime opportunity for an increase in cyberattacks. Malicious actors are taking advantage of districts' increased reliance on digital tools to extort money through DDoS and ransomware attacks. An identity-centric approach to IT and cybersecurity is essential to ensure a safe online environment for continuous virtual learning now and after COVID is behind us.

We surveyed 100 technology leaders in K-12 to understand:

- **Their current level of concern for cyber threats**
- **How they plan to deliver learning post-pandemic**
- **What security technologies have been implemented**

Data collected from Nov. 24, 2020 - Jan. 7, 2021

Respondents: 100 Educational Services leaders

92% of K-12 organizations are suffering from cyberattacks

Since the onset of COVID-19—nearly all (92%) K-12 organizations have experienced a cyber threat. Specifically, 82% have been the victim of a phishing attack, and over half (54%) have endured malware/ransomware attack.

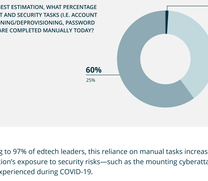
SINCE THE ONSET OF COVID-19 IN MARCH, WHICH OF THE FOLLOWING CYBERSECURITY THREATS HAS YOUR ORGANIZATION EXPERIENCED?
(MULTI-SELECT)

In addition, K-12's digital footprint will continue to grow as 99% of districts plan to keep delivering some form of virtual learning post-pandemic, which means the increase in cyberattacks will likely not abate.

ONCE COVID-19 PANDEMIC RESTRICTIONS ARE LIFTED, HOW DOES YOUR ORGANIZATION PLAN TO DELIVER LEARNING TO STUDENTS?

While nearly all (92%) of these organizations have suffered a cyberattack and 99% plan to continue providing virtual learning, less than half (42%) are moderately or significantly concerned that cyberattacks will continue to rise once COVID-19 restrictions are lifted, but they should be! The bigger the digital footprint, the bigger the target on schools' backs.

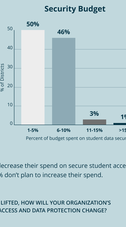
TO WHAT EXTENT IS YOUR ORGANIZATION CONCERNED THAT YOU'LL FACE AN INCREASE IN CYBER THREATS ONCE COVID-19 RESTRICTIONS ARE LIFTED?



Very few educational institutions have implemented identity lifecycle management, so reliance on manual processes is exacerbating security risks

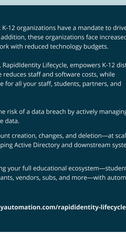
In order to protect digital resources, edtech leaders have focused on multi-factor authentication (88%). While 68% of edtech leaders report using automated access management, this typically involves writing custom scripts which can lead to operational challenges that impact instructional time. Only 9% have implemented identity lifecycle management.

WHICH OF THE FOLLOWING SECURITY TECHNOLOGIES HAVE YOU ALREADY IMPLEMENTED AT YOUR ORGANIZATION?



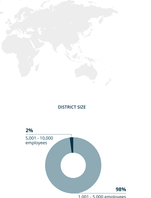
As very few organizations have implemented identity lifecycle management to secure their edtech stack, almost all (99%) are still completing at least a quarter of their IT and security tasks manually.

IN YOUR BEST ESTIMATION, WHAT PERCENTAGE OF YOUR IT AND SECURITY TASKS (I.E. ACCOUNT PROVISIONING/DEPROVISIONING, PASSWORD RESETS) ARE COMPLETED MANUALLY TODAY?



According to 97% of edtech leaders, this reliance on manual tasks increases a K-12 organization's exposure to security risks—such as the mounting cyberattacks they've experienced during COVID-19.

TO WHAT EXTENT DO YOU AGREE THAT RELYING ON MANUAL PROCESSES TO COMPLETE SECURITY TASKS RESULTS IN SECURITY GAPS AND GREATER EXPOSURE TO CYBERSECURITY THREATS?



Despite the increase in cyberattacks and the risk manual processes present, low and decreasing security budgets in the majority of K-12 organizations leave them ill-equipped to protect themselves

Right now, the majority (96%) of respondents have allocated 10% or less of their budget towards securing access and protecting data.

AS A RESULT OF COVID-19, HOW MUCH OF YOUR OVERALL TECHNOLOGY BUDGET IS CURRENTLY ALLOCATED TOWARDS SECURING STUDENT ACCESS TO CRITICAL RESOURCES AND PROTECTING THEIR DATA?

Almost half (46%) of organizations plan to decrease their spend on secure student access and data protection—and an additional 35% don't plan to increase their spend.

ONCE COVID-19 RESTRICTIONS ARE LIFTED, HOW WILL YOUR ORGANIZATION'S SPENDING ON SECURE STUDENT ACCESS AND DATA PROTECTION CHANGE?

At Identity Automation, we understand that K-12 organizations have a mandate to drive innovation in support of hybrid learning. In addition, these organizations face increased cybersecurity threats, yet are required to work with reduced technology budgets.

Our identity lifecycle management solution, RapidIdentity Lifecycle, empowers K-12 districts to do more with less. RapidIdentity Lifecycle reduces staff and software costs, while providing a safe, seamless digital experience for all your staff, students, partners, and vendors by:

- Protecting student data and mitigating the risk of a data breach by actively managing each application or service containing sensitive data.
- Enhancing efficiency by automating account creation, changes, and deletion—at scale, seamlessly closing security gaps and keeping Active Directory and downstream systems up-to-date.
- Maximizing instructional time by providing your full educational ecosystem—students, faculty, parents, staff, contractors, applicants, vendors, subs, and more—with automated access to appropriate resources.

To learn more, visit: https://www.identityautomation.com/rapididentity-lifecycle

Respondent Breakdown

REGION

TITLE

DISTRICT SIZE

Insights powered by PULSE