Our identity lifecycle management solution, RapidIdentity Lifecycle, empowers K-12 districts to handle increasing cybersecurity threats, yet are required to work with reduced technology budgets. Despite the increase in cyberattacks and the risk of data breaches, very few educational institutions have implemented identity lifecycle management to secure their data. As a result of COVID-19, how much of your overall technology budget is currently allocated towards student access to critical resources and data protection—and an additional 35% don’t plan to increase their spend.

Very few educational institutions have implemented identity lifecycle management, so reliance on manual processes is leaving them ill-equipped to protect themselves from security risks. 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 and DDoS and ransomware attacks. An identity-centric approach to IT and cybersecurity is essential for districts to minimize any cyber threats and keep their digital tools up-to-date.

Data collected from Nov. 24, 2020 - Jan. 7, 2021. Since the onset of COVID-19—nearly all (92%) K-12 organizations have experienced a cyber security incident and 99% plan to continue providing virtual learning post-pandemic, which means the increase in remote access to resources could potentially amplify any cybersecurity incident. 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 for districts to minimize any cyber threats and keep their digital tools up-to-date.

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.

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 and DDoS and ransomware attacks. An identity-centric approach to IT and cybersecurity is essential for districts to minimize any cyber threats and keep their digital tools up-to-date.

92% of K-12 organizations are expected to increase their spending on student data security once COVID-19 restrictions are lifted, how does your organization plan to deliver learning to students?

98% of educational institutions are online learning, 92% in-classroom, 6% hybrid:

- 100% physical
- 75% virtual
- 25% in-classroom
- 1% hybrid

As a result of the pandemic, districts have increased reliance on remote access to appropriate resources. Only 9% have implemented identity lifecycle management, so reliance on manual processes is leaving them ill-equipped to protect themselves from security risks. 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 and DDoS and ransomware attacks. An identity-centric approach to IT and cybersecurity is essential for districts to minimize any cyber threats and keep their digital tools up-to-date.

Another way to increase cybersecurity budgets is by focusing on multi-factor authentication. 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.

Identity lifecycle management solutions empower K-12 districts to handle increasing cybersecurity threats, yet are required to work with reduced technology budgets. Despite the increase in cyberattacks and the risk of data breaches, very few educational institutions have implemented identity lifecycle management to secure their data. As a result of COVID-19, how much of your overall technology budget is currently allocated towards student access to critical resources and data protection—and an additional 35% don’t plan to increase their spend.

Very few educational institutions have implemented identity lifecycle management, so reliance on manual processes is leaving them ill-equipped to protect themselves from security risks. 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 and DDoS and ransomware attacks. An identity-centric approach to IT and cybersecurity is essential for districts to minimize any cyber threats and keep their digital tools up-to-date.

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.

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 and DDoS and ransomware attacks. An identity-centric approach to IT and cybersecurity is essential for districts to minimize any cyber threats and keep their digital tools up-to-date.

92% of K-12 organizations are expected to increase their spending on student data security once COVID-19 restrictions are lifted, how does your organization plan to deliver learning to students?

98% of educational institutions are online learning, 92% in-classroom, 6% hybrid:

- 100% physical
- 75% virtual
- 25% in-classroom
- 1% hybrid

As a result of the pandemic, districts have increased reliance on remote access to appropriate resources. Only 9% have implemented identity lifecycle management, so reliance on manual processes is leaving them ill-equipped to protect themselves from security risks. 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 and DDoS and ransomware attacks. An identity-centric approach to IT and cybersecurity is essential for districts to minimize any cyber threats and keep their digital tools up-to-date.