The bridge to possible

Cisco Education Thought Leadership

Why a new approach to security is needed in education

© 2023 Cisco and/or its affiliates. All rights reserved.

The shift to virtual and hybrid teaching, learning, work, and services brought on by the continuing pandemic has only accelerated cybersecurity risks for education institutions of all levels. While data breaches are common across all industries, the risk for education is particularly acute given the sensitivity of students, faculty, staff, and research data. The increase in individuals accessing school systems outside of the campus and on personal devices has increased the threat surface exponentially, as has the proliferation of third-party, cloud-based applications and services. Adding in the fact that many institutions are understaffed and/or have insufficient security measures in place makes universities and schools attractive, easy, and lucrative targets for cybercriminals.

A recent report from **Inside Higher Ed** outlined the increase in cyberattacks on colleges and universities worldwide that bring significant operational and financial costs, with 74% of attacks on higher education institutions succeeding. In one instance, the University of San Francisco paid a $1.14 million ransom to avoid the release of stolen student data.[1] In the United Kingdom, the University of Hertfordshire suffered a devastating cyberattack that knocked out its IT systems, including Office 365, Teams, and Zoom, local networks, Wi-Fi, email, data storage, and VPN.[2]

Schools face this challenge as well. In October 2021, the Conseil des écoles publiques de l'Est de l'Ontario (CEPEO) in Ottawa, Canada, experienced a cyberattack that breached the personal data of current and former employees dating back to 2000, including social security numbers, bank account details and credit cards numbers, and dates of birth.[3] More recently, the South Redford School District outside of Detroit, Michigan, experienced a cyberattack in September 2022 that put the personal data of over 3,000 students at risk, forcing the district to close school as they researched the source and impact of the attack.[4]

Addressing new challenges and environments

Education IT and security leaders need to shift away from traditional security approaches, which assume that data inside the network is trustworthy. This assumption no longer holds true as the proliferation of mobility, personal devices, IoT, and cloud adoption increases the risk and complexity of secure data management. The new security strategy must follow a zero-trust model, which considers all resources to be external and continuously verifies trust before granting only the required access.

[1] Ransomware Attacks Against Higher Ed Increase: Inside Higher Ed; July 22, 2022

[2] Cyberattack on UK university knocks out online learning, Teams and Zoom: ZDNET; April 16, 2021

[3] Ottawa French public school board paid hackers ransom after data breach: Global News; November 30, 2021

[4] What we know about a cyberattack in South Redford School District that caused classes to be canceled: Click on Detroit; September 21, 2022

Nearly three quarters of cybersecurity attacks on universities are successful. The operational and financial costs of these attacks are substantial.

© 2023 Cisco and/or its affiliates. All rights reserved.

The bridge to possible

This new strategy supports security resilience, which is the ability to protect the integrity of the institution to withstand unpredictable threats or changes, and then emerge stronger. Security resilience moves from siloed, standalone security that focuses on threat prevention and treats all alerts and threats equally, to security resilience that focuses on detection/ response/ recovery, is connected, and considers context. This new approach helps organizations support workers anywhere and anytime, using a cloud-centric approach for the enforcement of security policy so that data and devices are protected. It also includes reducing complexity and improving the user experience by consolidating multiple disparate security capabilities and delivering them from the cloud.

Why Cisco

Uncertainly has become the new normal for our customers, and they are making investments to strengthen their security resilience. With its commitment to education and a complete portfolio of solutions to meet the needs of global education institutions, Cisco® helps customers to leverage existing investments collectively and realize the benefits of security resilience.

For more information

To learn more about education and technology, visit cisco.com/go/education, and to learn more about security resilience, visit our security resilience page.

Zero trust is the security strategy of the future. This strategy ensures people, data, and devices are protected regardless of location.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C11-3581153-00 05/23