yubico

WHITE PAPER

Graduating from legacy MFA to modern authentication

The critical need for increased security across education

Contents

The critical need for security in education

$6.62 Billion

cost of ransomware downtime in education[1]

45%

of education institutes hit by ransomware[2]

$3.79 Million

cost of a data breach in higher education[3]

166

K–12 cybersecurity incidents in 2021[4]

The education sector currently faces the highest volume of cyberattacks of any sector.[5] From sophisticated malware to phishing and ransomware, cyberattacks are a significant source of interruptions to school operations. The webhost attack in 2022, for instance, took 3,000 K–12 public schools offline, and the UMass Lowell attack shut down campus for nearly a week.[6] One estimate suggests that cyberattacks cost U.S. education institutions $6.62 billion in downtime in one year, to say nothing of recovery or other costs.[7]

In 2020, the University of California San Francisco (UCSF) paid a $1.14 million ransom to decrypt research data related to a coronavirus vaccine.[8] In higher education, breach costs have risen to an average $3.79 million, while Baltimore County Public Schools spent over $8.1 million to recover from a security breach—only a portion of which was covered by cyber insurance, the impact of which would delay other planned projects.[9]

The growing risk of attack continues to impact the cyber insurance market, with educational institutions facing increased premiums and new baseline security requirements in order to maintain coverage. Most insurers now require multi-factor authentication (MFA).

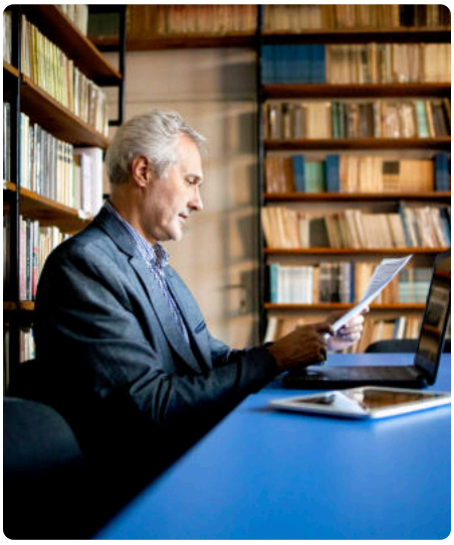
Further, education institutions may be subject to the requirement for phishing-resistant MFA as part of Executive Order (EO) 14028, the new Cybersecurity Maturity Model Certification (CMMC) 2.0 framework, changing state laws, and the recommendations that will follow the K–12 Cybersecurity Act of 2021.

With the rising rates of cyberattacks, both regulations and cyber insurance requirements are pushing educational institutes to adopt MFA, but there are systemic barriers to adoption that must be overcome, from training challenges to budget pressures—an obstacle that is particularly acute for school districts as American Rescue Plan Act (ARPA) stimulus funds come to an end. As institutions plan their rollout of MFA to staff, faculty, and/or students, it is important to recognize the need for a plan that balances security with resource challenges and end-user flexibility.

Evolving compliance and privacy laws

The pandemic accelerated a shift in the way education is delivered, collecting more digital data than ever before about students, from personal details and academic records, to new data points on physical or social-emotional well-being held in internal and third-party systems. The result of this digital transformation has placed enormous pressure on administrators to ensure that learning environments are secured, and to ensure that student privacy remains protected.

Educational institutions are subject to an increasing number of data privacy and data security standards and regulations beyond the scope of long-standing student privacy regulations such as the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), the Children's Internet Protection Act (CIPA) and the Protection of Pupil Rights Amendment (PPRA). The EU General Data Protection Regulation (GDPR) has had wide reaching implications for every industry,



including education, with similar state-level regulations such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CPDA) having implications for any for-profit educational institutions—in addition to the more than 130 state laws that apply specifically to student privacy.[10]

In May of 2021, the White House issued Executive Order (EO) 14028, Improving the Nation's Cybersecurity, outlining new expectations & guidelines for Zero Trust and phishing-resistant multi-factor authentication (MFA) for federal agencies, with downstream implications for any educational institutions that partner with the government.[11] Zero Trust urges organizations to trust no one or no thing unless properly verified before being given access to sensitive resources. Zero Trust is a framework designed to minimize uncertainty in enforcing least privilege access to systems and services.

The same pressure comes from the revised Department of Defense (DoD) CMMC 2.0 framework, which has implications for any educational institutions who work with or receive grant money from the federal government.

> "A lot of higher education institutions are contracting with the federal government to do a number of different types of research projects, and that could be anything from vaccine research to aerospace programs, and these are really important contracts to these higher education institutions. They can really impact the bottom line of these schools. If you don't meet the standards that CMMC requires, there is a chance that you could lose your government contract, which is a very big deal.
>
> **– John Farley, Managing Director, Cyber Practice Group Leader[12]**

In October 2021, The White House signed the K–12 Cybersecurity Act into law to strengthen the cybersecurity of public and private schools across the country.[13] The study and subsequent recommendations are meant to shed light on the challenges that educational institutions face, likely to include commentary on the lack of cybersecurity standards in education, the broad spectrum of devices and systems that need to be protected, and the lack of resources to implement stronger protections.[14] While compliance with the Act recommendations will remain voluntary, it is likely that the recommendations will become a requirement for cyber insurance.

Evolving cyber insurance requirements

In response to the uptick in the number and sophistication of cyberattacks, cyber insurance risk models have had to adapt—it has simply become too easy for an attacker to steal user credentials when legacy authentication approaches are used. In fact, 61% of data breaches can be traced back to credentials in some way.[15] But an increasing number of attacks has far-reaching implications across the entire insurance industry, with premiums rising by 150–300%, even if the insured meets the minimum security requirements of the insurer.

Most cyber insurance quotes and renewal terms will come with a cyber risk vulnerability report—a report to help educational institutions assess risk, but also a means for insurers to find glaring weaknesses in security posture. While minimum requirements will vary, simple password authentication isn't going to be enough to meet cyber insurers' minimum requirements—the risk is simply too high.

Higher education and K–12 schools can face a shortage of cybersecurity insurance capacity and increased cost for coverage if MFA isn't satisfactorily deployed across the entire ecosystem. Restrictions could include reduced sublimits, higher deductibles, and narrower coverage terms. Cyber policy non-renewals may also be a potential outcome, which can expose a school to significant risk if targeted by hackers, phishing attacks, or ransomware attacks.

The challenges with legacy MFA

Not all forms of MFA are created equal—at protecting against cyberattacks, in terms of the friction created for end users or IT support teams, or the ability to seamlessly work with the technology stack.

Security

Current authentication and security solutions, including usernames and passwords and mobile-based authenticators, are no longer effective to protect educational institutions against modern cyber threats. Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, revealed that a SMS-based one-time-password (OTP) only blocked 76% of targeted attacks and a push app only blocked 90%.[16] That's, at minimum, a 10% penetration rate. With this approach, it's not a matter of if you will be attacked—it's a matter of when.

With legacy MFA such as SMS, OTP, and push app, the second factor is tied to the mobile device. This is a red flag, because of four aspects. (1) There can be availability challenges with mobile devices sending codes in a timely manner due to poor connectivity or unreliable services. (2) There is no real guarantee that the private key ends up on a secure element on the mobile device. (3) The OTP or private key could be intercepted in some way (such as via SIM swapping), and (4) It is impossible to ensure proof of possession—or in NIST terms—impossible to prove it is impersonation-resistant.

Account takeover prevention rates

0%
Security key (YubiKey)

10%
On-device prompt

24%
SMS code

21%
Secondary email

50%
Phone number

User experience

Cloud-based SaaS applications such as Google GSuite and Microsoft Office 365, accelerated adoption of online learning platforms, and user mobility have accelerated digital transformation across the academic sector. Faculty, staff, and students need secure and quick access to email, applications, and data from any location—on or off-campus, and from any device.

Beyond security, legacy mobile authentication creates friction in the user experience if users are not able to seamlessly authenticate. Authentication is a mission-critical service, and if users can't log into the apps or devices they use, they can't do their job.

Any authentication solution has to be reliable and seamless to use for every user, without common points of failure related to connectivity, device battery, cell reception, hard token battery, or even a password. Any authentication solution that relies on "something you know" (a password) is going to be subject to human error—lost, forgotten, or mistyped details that add friction to the authentication experience, potentially locking users out of accounts.

While educational institutions may prioritize or even mandate mobile-based MFA, there are almost always edge cases of users that can't, don't, or won't use mobile authentication. These include restrictions imposed by teachers unions on using personal mobile devices for work purposes, faculty and staff that don't have smartphones, or faculty and staff that won't use their personal mobile devices—situations which create MFA gaps if the fall back option is username and password.

IT burden

In education, the high number of temporary faculty and staff and large student body often makes IT support a pinch point in any MFA deployment.

Any form of legacy authentication such as usernames and passwords, and mobile authentication applied and enforced at scale, will require ongoing policy enforcement, user training and IT support. Even the easiest forms of 2FA and MFA mobile authentication—OTP, TOTP, 2FA apps—create a huge support burden if codes are delayed, users get locked out of their accounts, or users need to register new devices.

Due to the high cost and poor security of legacy authentication, educational institutions are moving toward passwordless authentication—authentication that does not require the user to provide a password at login.

Modern, phishing-resistant authentication with the YubiKey

The YubiKey is a hardware security key, manufactured by Yubico, that offers easy-to-use two-factor, multifactor, and passwordless authentication at scale. The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.[17]

The YubiKey uses modern protocols such as FIDO U2F and FIDO2 open authentication standards, with the hardware authenticator protecting the private secrets on a secure element, entirely eliminating phishing-driven credential-based attacks and supporting a user-friendly login flow.

Let's face it, it's frustrating to have to enter passwords or one-time passcodes all the time. And, as we all know, employees frustrated by a poor experience will not only be less productive and engaged, but also more likely to circumvent the process or increase the IT support burden—all of which are expensive outcomes.

A single YubiKey works across multiple devices including desktops, laptops, mobile, tablets, notebooks, and shared workstations, enabling users to utilize the same key as they navigate between devices. YubiKeys are also easily re-programmed, making them suitable for temporary faculty and administration staff. They also enable self-service password resets, significantly reducing IT support costs and increasing user productivity.

The YubiKey is a cost-effective and scalable solution that works out-of-the-box with nearly 1,000 apps and services, enabling strong two-factor, multi-factor and passwordless authentication to help get educational institutions to 100% MFA at any stage:

4x faster logins

Zero account takeovers

92% support reduction

One key to all

The YubiKey can be deployed in-person or shipped to users, with the option for admins to pre-enroll users or allow for self-enrollment via a web portal. YubiKeys integrate seamlessly with existing identity and access management (IAM) and identity provider (IDP) solutions such as Microsoft, Okta, DUO, Ping, and more than 1,000 applications and services out-of-the-box, including Google Suite, Microsoft Azure, Microsoft Office 365, Box, Jamf, and identity and credential management (ICAM) solutions, eliminating rip and replacement of existing solutions.

DUO box Google jamf Microsoft okta Ping Identity

Building a flexible and resilient MFA program in education

Recognizing the challenges in education, YubiKey has worked with K–12 and higher education clients on a phased approach to deployment that offers flexibility regardless of where institutions are in their authentication journey. The goal is to develop an MFA program that helps get institutions to 100% MFA quickly and seamlessly, offering a choice of MFA options, with a plan to deploy YubiKeys to greater numbers of users over time.

Identity gaps

Identify where you have MFA gaps. These could be staff or faculty that are still using username and password-based authentication, and can't, don't, or won't use mobile-based authentication. The security gaps can be highly risky, leaving an open door for hackers to get in. Understanding where you have these gaps can then help you determine how best to close them.

Secure privileged users

Strengthen authentication across your institution. A risk-based approach often begins with privileged users, internet-facing systems, remote access and email accounts. Privileged users include those with direct access to high-risk systems or applications such as IT admins, or even users with access to highly targeted applications such as payroll. YubiKeys can also be deployed to remote or hybrid workers, providing a more secure and faster approach than legacy authentication.

Replace or strengthen hardware-backed TOTP

OTP and TOTP codes sent via email and SMS are vulnerable to cyberattack and are a source of user friction, reducing productivity and, in the case of educators, interrupting class time. Many common authenticator apps store credentials within the mobile device app, introducing another element of risk. Strengthen existing TOTP processes by replacing insecure mobile-based authentication methods such as SMS or authenticator apps with the Yubico hardware-backed authenticator to generate the TOTP.

Secure faculty, staff, and students

Provision and deploy YubiKeys to segments of the community in a phased approach: executive staff, HR & payroll, administrative and support staff, educators, then all in-person and online learning students.

Palo Alto Unified School District (PAUSD) Protects Student Data with YubiKeys

PAUSD, located in Silicon Valley, had an incident where student grade information was being exposed on a third party website related to compromised credentials of a teacher's account.

Today, all PAUSD staff use YubiKeys in their daily computing activities. Student information databases are protected by the YubiKey at the staff level, as well as personal data at the parent and guardian level.

Summary

The education sector is faced with the growing threat of targeted and costly cyber attacks, with new pressures from regulators and insurers to step up security. As a result, institutions are looking to implement MFA for all users, prioritizing some or all use cases from administrative right down to the student body.

The YubiKey is uniquely designed to help educational institutions achieve 100% MFA no matter what stage they are at in their security readiness, ensuring compliance with cyber insurance mandates and evolving regulations.

Sources

[1] Comparitech, Ransomware attacks on US schools and colleges cost $6.62bn in 2020, (August 31, 2021)

[2] Sophos, The State of Ransomware in Education 2021, (Accessed April 26, 2022)

[3] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021)

[3] CyberArk, The CyberArk 2022 Identity Security Threat Landscape Report, (April 12, 2022)

[4] K12 Six, The State of K–12 Cybersecurity: Year in Review, (Accessed April 25, 2021)

[5] Check Point, Cyber Attacks Increased 50% Year Over Year, (Accessed April 26, 2022)

[6] Alyson Klein, Thousands of School Websites Went Down in a Cyberattack. It'll Happen Again, Experts Say.

[7] Comparitech, Ransomware attacks on US schools and colleges cost $6.62bn in 2020, (August 31, 2021); Alex J. Roughandeh, As Classes Resume at UMass Lowell After Cyberattack, MIT Cyber Expert Weighs In, (June 21, 2021)

[8] Joe Tidy, How hackers extorted $1.14m from University of California, San Francisco, (June 29, 2020)

[9] IBM, 2021 Cost of Data Breach Report, (Accessed April 26, 2022); Amy Simpson, BCPS ransomware recovery efforts come with $8.1 million price tag, (June 15, 2021)

[10] Kara Arundel, Why student data remains at risk-wand what educators are doing to protect it, (December 14, 2021)

[11] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021)

[12] Elizabeth Blosfield, Education Providers Face Challenges With Growth in Cyber Threats, Insurance Costs, (March 2, 2022)

[13] The White House, Statement of President Joe Biden on Signing the K–12 Cybersecurity Act into Law, (October 8, 2021)

[14] K–12 Cybersecurity Act Signed into Law

[15] IBM, 2021 Cost of Data Breach Report, (Accessed April 26, 2022); Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021)

[16] Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[17] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.