Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **March 2021**
Sponsored by **Mimecast**

Cybersecurity in Education

Executive Summary

The education sector faces a growing complex of cybersecurity threats. The industry has been under high attack for several years already, with phishing, ransomware and denial-of-service attacks growing in frequency and ferocity. But what has blown the gates off is the forced move to remote and online learning in response to the health pandemic that began early in 2020. The education sector is ripe for massive disruption through ransomware attacks due to reliance on online learning platforms, and threat actors are taking the opportunity to wreak havoc at the most inopportune times. The lack of systemic preparedness is putting the sector in the crosshairs of threat actors; Microsoft reports that more than 60% of monthly malware attempts in Microsoft 365 are focused on the education sector, a number six times higher than the next closest industry.[1]Students themselves are a dangerous source of insider attacks and weaknesses, which run the gamut from the presumedly innocent sharing of login details for online classes through to unleashing denial-of-service attacks against school districts. In sum, something new and better must be done to enact cybersecurity defenses and develop approaches to safeguard institutions, the data they are responsible for, and the staff, faculty and students who work or study within.

KEY TAKEAWAYS

- The education sector has been ill-prepared to properly address cybersecurity for many years, a consequence of systematic under-investment despite a growing reliance on technology for school and university operations, teaching and research. The sector has long-running characteristics that makes it susceptible to cyberattacks, and the health pandemic from 2020 has only pushed things further towards perfect storm conditions.
- Current cyberthreats in the sector include ransomware, phishing (and its variants), and attacks against third-party vendors. Low staff awareness of cybersecurity principles and defenses is systemic and many IT teams lack the people and financial resources necessary to manage cybersecurity effectively.
- Phishing and ransomware will continue as key attack vectors. Perfectly timed maximum-disruption incidents will be an important objective for threat actors for as long as online learning continues to dominate delivery methods. We expect to see pricing levels of ransom demands increase too.
- Addressing the cybersecurity threats facing the education sector requires new and better solutions, including stronger authentication methods, more effective anti-phishing defenses, and approaches that reduce the impacts and risks of ransomware attacks. Equally important, however, is the need to enlist the people within the sector in the fight against cyberthreats.
- Best practices for cybersecurity preparedness complement solutions for cybersecurity defenses, and include developing a risk assessment for your institution, assessing cybersecurity preparedness of third-party vendors in vendor selection processes, and securing cyber insurance coverage.
- Elevated security protections without improving convenience will fail, because users will look for ways to circumvent protections that make it too difficult to access the services they need.

The lack of systemic preparedness is putting the sector in the crosshairs of threat actors.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Mimecast. Information about Mimecast is provided at the end of the paper.

Why the Education Sector?

The education sector has become a key target for cyberattacks. Threat actors have increased their activity against the education sector for a plethora of reasons, which we look at briefly in this section.

CHARACTERISTICS OF THE SECTOR THAT CREATE AN ATTRACTIVE CONTEXT FOR CYBERATTACK

The education sector presents a set of characteristics signaling opportunity to threat actors. These ingrained and long-running characteristics include:

- Reliance on legacy technology, particularly in higher education. The IT architecture for communication and collaboration, operational processes and student management is often built on legacy systems several decades old. Being among the earliest organizations to embrace the Internet, educational institutions face a significant journey to digital transformation that many have not completed. Yet they are now rushing in order to support the shift to remote learning in response to COVID.
- School districts have the task of selecting their own IT providers, and different departments at the same university often have the right to go their own way in selecting IT systems (or even growing their own). Decentralized approaches confer autonomy for local decision-making (a highly valued attribute in the sector), but by implication, lose out on tighter security compared to when fewer systems and variants are in use. Decentralized approaches proliferate vulnerabilities that threat actors can leverage.
- A dynamic and large user population, where it is expected that almost all students will leave after 2-5 years (in corporate terms, turnover is 20% to 50% per year, in perpetuity). This ever-changing roster of students across multiple systems creates a complex mix of access rights and permissions where mistakes or weak links give threat actors avenues of unauthorized access. Once students have completed their studies, educational institutions often want to stay in contact with an ever-expanding alumni group, which creates its own set of identity management challenges over time.
- The sector has systematically under-invested in cybersecurity and is poorly prepared to handle cybersecurity threats. Few K-12 institutions, for example, have cybersecurity specialists on staff, even though technology has become an ever-larger part of the education scene over the past decade, and some school districts serve more than one hundred thousand students (each one a potential threat or potential attack victim). A study in 2018 of cybersecurity preparedness in 17 industries placed the education sector dead last, as both the least secure and the industry with the highest security vulnerabilities across multiple areas.[2] An earlier research study in 2017 on cyberthreats to small- and medium-sized businesses found that 96% of IT decision-makers believed their organization was susceptible to external cyberthreats, and only 3 in 10 said they were prepared to cope with them.[3] Recent trend lines in successful attacks against the education sector indicate its reality is no better.

The education sector presents a set of characteristics signaling opportunity to threat actors.

- The sector champions a culture of openness and sharing, including ready access to faculty members. Many universities, for example, have publicly accessible directories of professors and adjuncts listing multiple contact details—all of which are useful inputs for cyberattacks and impersonation. Physical access to a campus and its buildings is less strictly controlled than a corporate counterpart. This accessibility can be abused by planting devices for eavesdropping, network sniffing or inserting rogue wireless access points.
- Higher education and research institutions become the place where academics collect and develop cutting-edge data for business, government, and military usage. These educational organizations do not want to run the risk of losing access to that life's work through a ransomware attack, for example, nor jeopardizing current and future research contracts by proving incompetent at data protection. Compromised K-12 student records fetch a high price on the black market due to their value for identity theft.
- Cyberattacks on IT systems cause an immediate disruption to thousands or tens of thousands of people, amplifying the need for rapid resolution. The teaching curriculum in schools and universities is increasingly delivered or supported via digital channels, even when students are on site. If IT systems are disrupted by a cyberattack, teachers cannot teach, the viability of research projects is threatened, and even bus schedules for getting several thousand children to school and safely back home are rendered inoperable.

THE PANDEMIC HAS MADE THINGS WORSE

Within the context of an already vulnerable sector, the COVID-19 health pandemic from 2020 has only made things worse. This includes:

- An investment preference for creating physical spaces and infrastructure for bringing students together in-person, as opposed to creating online learning environments with strong cybersecurity protections. With an ingrained cultural emphasis on investing in classrooms, in-classroom teaching technology (e.g., smart boards), gymnasiums and playing fields, the suddenness of the COVID-19 pandemic and the major pivot it required caught most unprepared for a set of very different requirements.
- A cohort of teachers trained to manage children in a classroom environment, rather than in a remote learning environment. Many teachers have low competence on the cybersecurity threats of remote learning technologies, credential compromise, malicious apps, and even security standards of free apps. These issues have not previously been of high importance, and in an age when even researchers on cybersecurity threats are compromised through targeted attacks, teachers present an easy attack vector. An experiment in Mississippi saw 83% of targeted staff open a simulated phishing message, 48% click the malicious link, and 20% enter their credentials in the phishing page.[4]
- New challenges in how to prove the identity of a student taking a class, sitting an exam, or requesting access to financial information. In fully digital learning environments, the ability to rely on in-person verification is no longer available. Students with an identical twin might previously have been able to obfuscate identity, but in a digital learning environment, identity obfuscation is much easier to pull off.

Many teachers have low competence on the cybersecurity threats of remote learning technologies, credential compromise, malicious apps, and even security standards of free apps.

- Attempting to cope with the unexpected imposition of rolling shelter-in-place and lockdown measures by rapidly adopting new remote learning technologies without a clear sense of the cybersecurity risks involved. Remote video learning systems—such as Zoom—were quickly compromised due to weak or non-existent password usage. Threat actors began plotting denial-of-service and ransomware attacks to hit at the most inopportune and high-leverage times, such as a day or two before a school district was due to begin classes for the new year, or just before significant holidays when IT staff were looking forward to time off (e.g., the ransomware attack on Baltimore County Public Schools at the start of Thanksgiving in 2020)[5]. When all learning is technology-mediated, no technology means no channels for learning. Huntsville City Schools experienced such an incident in December 2020 when a ransomware attack resulted in the school being closed for a week and 23,000 students being told not to use school-issued devices.[6]

REGULATORY OBLIGATIONS

Regulatory obligations increase the risks of cyberattack for educational institutions. In the United States, this is led by the requirements of the Family Educational Rights and Privacy Act (FERPA). It confers three rights on the parents of children under 18 (and then upon the student personally when he or she turns 18 or enrolls in post-secondary education), including the right of access to educational reports, the right of modification in the event of error or when changes are needed, and the right to control disclosure. Any cyberattack that results in the denial of these rights—including ransomware that disables access or a data breach that provides unauthorized disclosure of students' personally identifiable information—threatens the funding received by the school from the United States federal government, and in addition, carries fines of up to US $245 per impacted student record.

Regulatory obligations increase the risks of cyberattack for educational institutions.

There are other regulatory obligations as well, depending on the nature of the educational institution. For example:

- Universities providing healthcare to students, or that include a medical center or medical research facility, will need to comply with the provisions of HIPAA (Health Insurance Portability and Accountability Act) and its subsequent updates in the United States. HIPAA includes privacy and security requirements covering administrative, physical, and technical safeguards for health information that is linked to an individual. Stanford University, for example, suffered several high-profile breaches of health information from three separate medical facilities associated with the university, and carried costs for HIPAA violations even when they were not directly at fault.[7]
- Educational providers accepting payments by credit and debit card must comply with the provisions of PCI-DSS (Payment Card Industry Data Security Standard). Protections are required for payment card information during transmission and storage.

Cybersecurity Threats in Education

There is a plethora of cyberthreats against the education sector. High-level numbers include the following:

- In 2015, Pennsylvania State University faced an average of 20 million cyberattacks per day—an amount "typical for a research university."[8]
- A greater proportion of cybersecurity incidents are composed of data breaches or ransomware attacks, with successful ransomware incidents doubling from 2018 to 2019 and data breaches increasing by 28% over the same timeframe.[9]
- Almost 1,200 publicly disclosed cybersecurity incidents in K-12 schools have been recorded from 2016 to mid-February 2021.[10]
- 30% of people in the education sector took the phish on phishing emails posing as official communications from their organization.[11] This is twice as high as the incident rate across other industries.
- 41% of cybersecurity incidents and breaches in the higher education sector were caused by social engineering attacks, with phishing being the most common method of social engineering.[12]
- 87% of educational institutions have experienced at least one successful cyberattack, and 36% of universities in the United Kingdom are hit with a successful cyberattack every hour.[13]
- In June 2020, Microsoft identified around 7.7 million malware attempts against enterprise accounts in Microsoft 365. Microsoft said 61% of these were from the education sector.[14] In February 2021, it was 10.6 million malware attempts, with 62% in education. [15]

In this section, we take an in-depth look at the types of cybersecurity threats at play.

41% of cybersecurity incidents and breaches in the higher education sector were caused by social engineering attacks.

RANSOMWARE

Ransomware has become a major issue across all industry sectors, with one study finding a sevenfold year-on-year increase in the number of reported ransomware incidents (which means, in addition, that there are many incidents that have not been reported).[16] The education sector has been the target of an increasing number of ransomware attacks over the past five years. For example:

- In 2016, the education sector had the highest rate of ransomware attacks across all industries. It was three times greater than the healthcare industry, and ten times greater than the financial services industry.[17]
- In 2017, the healthcare sector took first place for ransomware attacks (with the NotPetya attack wreaking notable havoc). Higher education was pushed to second place.[18]
- In 2020, the Multi-State Information Sharing and Analysis Center (MS-ISAC) noted growing attacks in the K-12 system. From January to July, 32% of all reported ransomware incidents involved K-12 schools. In August and September, with school districts opening for a new year of teaching, the attack share almost doubled to 57%.[19]

- In 2020, Check Point Research observed a similar trend, with a 20% increase in cyberattacks in the education sector during August and September in comparison to rates earlier in the year. Check Point also noted that the comparative growth rate over the same two-month period for all other industries in the United States was only 6.5%, or about one-third of the education rate. While the rate of attacks against education providers in Europe was different to that of the American attacks, the comparative growth rates between the education sector and all others in Europe were about the same as the American differential.[20]
- In 2020, there were twice as many ransomware attacks against universities in comparison to the 2019 year. In addition, the average ransom demand in 2020 was $447,000.[21]

Examples of ransomware attacks in late 2020 in the education sector include:

- In August, the Clark County School District suffered a ransomware attack that encrypted and exfiltrated its data. Some personal data on current and former employees was published online.[22]
- In September, Hartford Public Schools suffered an attack that encrypted critical systems, including the bus scheduling system for getting students to and from school each day. Reopening the district for the new school year was delayed by one week.[23]
- In November, just prior to Thanksgiving, Baltimore County Public Schools had a ransomware attack that affected its website, email infrastructure, and student grading system. The district closed its online classes for a week, affecting 115,000 students.[24]

In 2020, there were twice as many ransomware attacks against universities in comparison to the 2019 year.

PHISHING, SPEARPHISHING AND BUSINESS EMAIL COMPROMISE

Phishing, spearphishing and business email compromise (BEC) cyberattacks are common and widespread and deliver high effectiveness rates for threat actors. Unlike attacks that require the development of evasive techniques to get through email security filters, phishing and its variants leverage social engineering techniques to simply ask the target victim to perform a simple action. For example, to open an attached document (which is usually obfuscated to appear benign), visit a link (which often conceals a malicious payload or presents a falsified login page), or in the case of business email compromise, change the bank account number on record for an upcoming payroll run or invoice payment. It is widely held that more than 90% of cyberattacks start with a phishing attack.

Examples of phishing attacks in the education sector include:

- In April 2019, Scott County Schools paid $3.7 million into a fraudster's bank account after receiving fraudulent documentation in a business email compromise attack for an upcoming payment to a vendor. They only became aware of the scam two weeks later when the actual vendor questioned why they had not received payment yet.[25]
- In May 2019, a phishing attack successfully compromised account credentials of staff members at the Australian Catholic University. The phishing email pointed to a fake login page for the university, and once staff had entered their credentials, the threat actors were able to access their email, calendar, and bank account details. [26]

- In November 2019, a business email compromise attack on the Manor Independent School District resulted in three payments totaling $2.3 million being paid to the threat actor's bank account. The fraud was discovered in December 2019. [27]
- In August 2020, hackers gained access to an email account belonging to the construction company working for Mehlville School District, probably the result of a credential compromise phishing attack. The hackers then sent different payment details for an invoice to the district in a business email compromise attempt, which successfully resulted in a $334,000 payment going to an account under the hacker's control.[28]
- Beginning around April 2017, a coordinated spearphishing campaign targeted selected academics across more than 27 universities in the United States, Canada, and Southeast Asia, including the University of Hawaii, the University of Washington, and MIT. The spearphishing emails carried malicious software that, once activated, stole research data on projects being carried out under contract to the military.[29]

MULTI-FACTOR AUTHENTICATION-RESISTANT PHISHING

With the rising adoption of multi-factor authentication (MFA) as a safeguard against phishing, threat actors have developed phishing attacks that assume MFA safeguards are in place—and then compromising them too.[30] For example, phishing campaigns usually link to a realistic-but-fake login page, and sophisticated attacks extend this by immediately submitting the captured credentials to the real site and intercepting the resultant SMS-based or authenticator-app-based code entered by the victim on the fake site to gain immediate access with the new credentials to the real site. Another technique gains access to the authentication token for persistent access to applications even after the user has updated their credentials.

Threat actors have developed phishing attacks that assume MFA safeguards are in place—and then compromising them too.

COMPROMISED ACCOUNT CREDENTIALS

Threat actors prize compromised account credentials highly because they enable effective under-the-radar malicious activities. Phishing attacks that capture credentials can then be used to send emails from the compromised account, leveraging the existing trust between the sender's name and the recipients they normally communicate with. Such emails may seek further credential compromise, aim for malware installation, or lay the basis for BEC attacks. Requests that would appear strange coming from unknown people are more likely to result in action when sent from a trusted account. Other forms of compromise, such as hacking attempts and malware, are more likely to trigger security alerts than a login from a different geography using compromised credentials—although even the real geographic region can often be obscured using a VPN.

IDENTITY PROLIFERATION

Every new online service and application used by an educational institution introduces another potential vector for cyberattack, another identity for the IT team to configure and manage, and another password for staff, faculty, and students to work with. These dynamics can lead to further instances of bad password habits—for example, reusing an existing password because that is easier to remember—or even reduce the adoption rates of the new service.

DATA BREACHES

Data breaches result in unauthorized access to details on students, educators, and school operations, and can be caused by human error within an institution, a cyberattack on an institution, or a data breach at a third-party vendor that holds data from across tens, hundreds, or thousands of institutions. Data breaches represented 60% of cybersecurity incidents in the K-12 segment in 2019, the majority of which were due to incidents at third-party vendors rather than at schools directly.[31]

Compromised data on students and educators is often sold for tax fraud, identity theft and other scams.

Examples of data breaches in the education sector include:

- In 2018, an unsecured internet-connected server containing personal data on 368,000 full-time and part-time students at Florida Virtual School was discovered. The server had been unsecured for around two years.[32]
- In 2019, the FBI advised Pearson—a third-party software vendor to schools and educational institutions—that one of its services had been hacked, exposing details on students at more than 13,000 institutions based predominantly in the United States.[33] This breach easily affects tens of millions of students.
- In 2020, a phishing attack at Syracuse University in September resulted in the threat actor gaining access to an email account belonging to an employee of the university. The email account contained personal data on 9,800 Syracuse University students, alumni, and applicants. The post-breach forensics investigation was unable to determine if the unauthorized party ever viewed the personal information in the email account.[34]
- In 2021, when Shorewood School District responded to an open records request from a parent for data on a recent survey, it mistakenly included personal information on the student respondents, including data types such as student name, ID number, school, gender, and ethnicity.[35]

Data breaches represented 60% of cybersecurity incidents in the K-12 segment in 2019.

THE REMOTE LEARNING CURVE BALL

The unanticipated health pandemic of 2020 threw a curve ball into the education sector globally, driving a rapid pivot into online and remote learning during a period of mass fear, panic, and uncertainty. Students suddenly had to learn from home, adjust to life without friends, and live with parents or guardians having to transition to similar working arrangements—and often not in housing situations set up for such demands. Threat actors were quick to latch onto fearmongering as an approach to increase click rates on phishing emails delivering malicious software, ransomware, and credential-compromise links. Remote learning platforms, as the only available delivery method for educators during shelter-in-place and lockdown mandates, were compromised when threat actors guessed or accessed passwords to join online sessions to disrupt the class, harass students and teachers, appear naked, or show pornography or violent images to the students. Students and classroom contexts that would previously never have been available in a physically constrained education world were now digitally available to any threat actor.

COMPROMISE OF THIRD-PARTY SERVICES FOR REMOTE LEARNING

School districts have been quick to embrace online and remote learning platforms to cope with the new demands imposed by the health pandemic. Not all these platforms are sufficiently protected from cybersecurity threats, however, which then impacts the ability of a district to offer schooling when meeting in a classroom is not an option. Third-party providers of these platforms suffered various attacks during 2020, including a denial-of-service attack in Florida that took down the online platform for the Miami-Dade County School District for three days. That attack was launched with an older tool that could have been stopped with even a basic firewall, but no such protections had been put in place.[36]

DENIAL OF SERVICE ATTACKS

Denial of service attacks result in computing infrastructure being unavailable to handle the regular demands it was put in place to service, which in an educational setting includes facilitating remote learning, connecting students and teachers, and performing school and institutional operations. Denial of service attacks increased in frequency in 2020, with one study finding the rate of attack almost doubled year-on-year from Q1 2019 to Q1 2020 and another noting that denial of service attacks formed the main threat type in the United States in July-August 2020 (as schools prepared to reopen for the new school year).[37] The Miami-Dade County School District attack, above, is one such example.

INCREASED ADOPTION OF CLOUD SERVICES

With new requirements for systems to deliver online learning, a rapid push to digital transformation, and challenging levels of IT resourcing, the sector has seen increased usage of cloud services that forgo the need for on-premises infrastructure deployment, maintenance, administration, and costs. In lockstep with the move to the cloud, however, is the need to transform from legacy on-premises cybersecurity platforms to cloud-delivered cybersecurity solutions and platforms for the same reasons.

LOW STAFF AWARENESS OF CYBERSECURITY THREATS

With a culture steeped in going the extra mile to help students learn and prosper, many educators downplay or disregard the threat of cyberattacks or believe it will never happen to them. Low staff awareness of cybersecurity threats includes situations where teachers rely on free software sourced from the internet to assist with online learning, which can come with cyberthreat vulnerabilities or be deliberately compromised and delivered through rogue app stores. A phishing simulation at the Clinton Public School district saw 47% of staff members click on the link inside an email that had obvious red flags for anyone with the eye to notice them.[38] When sophisticated threat actors hit up against unsophisticated educators, it is the threat actors who have the easier pathway.

LOW ORGANIZATIONAL PREPAREDNESS FOR CYBERSECURITY THREATS

Educational institutions face the challenging dynamic of being among the largest organizations (with tens or hundreds of thousands of staff and students), but with the cybersecurity preparedness and resourcing levels of much smaller organizations. This imbalance between need and resourcing has become a systemic issue, with state audits in Maryland, for example, identifying cybersecurity vulnerabilities in its 24 school districts year after year.[39]

Many educators downplay or disregard the threat of cyberattacks or believe it will never happen to them.

LACK OF CYBERSECURITY TALENT IN IT TEAMS

There is a lack of cybersecurity talent in IT teams in the sector, with many school systems not even able to dedicate a full-time employee to cybersecurity.[40] Over the past year, IT teams have been overwhelmed with selecting and deploying remote learning platforms and have had to deal with the rapid pivot to an entirely new way of educating. In response to the financial impacts of COVID, some educational institutions have made drastic reductions in IT staffing and budgetary levels, compounding the problem. Security concerns, principles and approaches have been relegated down the list of priorities.

INSIDER THREATS FROM STAFF, STUDENTS AND PARENTS

Educational institutions face insider threats from staff, students, and parents/guardians. Some students just want to "have a bit of fun," some are "seeing what they can do," while others act negligently and put the organization at risk. K-12 school districts, for instance, entrust part of their cybersecurity posture to students still learning to read and do basic math; expecting the same students to adhere to good cybersecurity practices and use MFA everywhere is a significant challenge. Parents and guardians can also circumvent good security designs because the requirements are too onerous.

Examples of insider threat events and event types include:

- A couple of naked men joined an online class session at a school in the United Kingdom in early February 2021 after students shared the login credentials to the session.[41] Students had been sharing login details via Snapchat and on social media accounts with no privacy settings in place. Similar incidents have happened at many other schools.
- A 16-year-old student in Florida tried his hand at initiating denial-of-service attacks against his school district serving more than 345,000 students. The attacks closed the district for three days of online classes.[42]
- Staff and students with poor password hygiene (e.g., reusing passwords, using short passwords), or refusing to use multi-factor authentication when accessing sensitive data.
- Educators or students taking deliberate action to circumvent and bypass security controls using Web proxies and rogue VPN apps. This is an issue for 42% of K-12 organizations.[43]

Finally, with the growing number of programs offering cybersecurity training to students (in addition to the cohort already studying computer science, software development and electrical engineering), educational institutions run the continual risk of growing their own hacking talent. Some students learning cybersecurity principles and approaches will want to try out their learning against their educational institution, sometimes for malicious intent but more often just for the fun of using their nascent skills.

Some students learning cybersecurity principles and approaches will want to try out their learning against their educational institution, sometimes for malicious intent but more often just for the fun of using their nascent skills.

DEVICE AND APP PROLIFERATION

The sector faces an almost unmanageable tangle of devices and device types that require access to online learning platforms and school/university management systems. In a study carried out before the pandemic hit, the following was noted:[44]

- IT leaders in the K-12 system are, in combination, managing more than 250 unique operating system versions and variants across 11 device types.
- 93% of these leaders have up to five versions of common applications to manage across their district, and in terms of the overall K-12 system, there are 137,000 unique application versions in use, with more than 2.1 million applications targeting the educational space on offer.
- Over 6,400 unique Chrome extensions are being used across the K-12 system.

Another study tracked an increase in the number of applications being downloaded from rogue app stores once the pandemic hit and working/learning from home was required. Even popular applications from trusted vendors are available from rogue app stores, but only after they have been modified to add malware.[45]

GROWING COLLECTION OF IOT DEVICES

Educational institutions have a growing collection of IoT devices, including security cameras, smart boards, and video cameras for students to enable online learning. Many of these devices have unknown and unquantified cybersecurity weaknesses, and if default passwords are not changed, cameras are hacked in other ways, or devices are surreptitiously given extensive permissions by overreaching app requests, they become a vector for attack. Several CCTV cameras at three schools in Blackpool in the United Kingdom were compromised in early 2018, and live streamed in the United States for about an hour.[46]

VULNERABLE, COMPROMISED AND MALICIOUS APPS

As students and teachers adopt mobile devices and apps to support online learning, the risk of entrusting personal and sensitive data to vulnerable, compromised, and malicious apps increases. Android is a widely adopted mobile platform in the education sector, and its high rate of malicious and compromised apps and rogue app stores is a significant concern. One study found that 31% of all apps used in the education sector are high-risk due to cybersecurity and privacy issues, making the sector the most vulnerable industry of those studied.[47]

31% of all apps used in the education sector are high-risk due to cybersecurity and privacy issues.

Threat Outlook

We expect to see the following threat dynamics over the next two years.

- **Continuation of Phishing and Ransomware Threats**
  Phishing and ransomware are easy attacks to perpetuate, effective at ensnaring victims, and profitable for threat actors. Until the interplay between these dynamics changes, threat actors will continue to leverage what is already working against a sector that is ill-prepared to withstand attack. INTERPOL[48] and a joint advisory[49] from the FBI, CISA and MS-ISAC warn of the continuation of cyberattacks in the immediate future.

- **Ongoing Shortages of IT Staff**
  IT teams in school districts are stretched and overwhelmed with the growing set of responsibilities for supporting remote learning platforms, as well as attempting to rapidly address a decade of under-investment in cybersecurity. Only three out of five educational institutions have a full-time cybersecurity specialist on staff, even 12 months after the pandemic altered the educational landscape with remote learning.[50]

- **Creating Disruption Remaining a Major Driver**
  Creating maximum disruption will remain a major driver, with the ability to cripple an entire school district or university a preferred attack pattern. For as long as online learning is the dominant feature of the sector, threat actors with the ability to time a maximum-disruption incident will increase the odds of receiving a prompt financial payoff—because the option to bring everyone into a classroom does not currently exist for many school districts. Teachers and faculty have already been pushed in teaching directions few wanted to go, students are isolated from peers and living through a period of massive disruption during formative years, and IT staff in the sector are ill-equipped, under-trained and under-resourced already. The relentless ongoing escalation of stress levels across the sector from actual threat incidents and the perceived threat of imminent cyberattacks at the most inopportune times, will incur high costs to the health and wellbeing of everyone in the sector.

- **Higher Ransom Demands**
  The pricing of ransom demands against the sector will increase, for several reasons. First, the trend outside of the sector is already evidencing increasing pricing. Second, a higher proportion of school districts carry cyber insurance than organizations in the general market. Third, the downstream costs of disrupting remote education for thousands of students force a quick response by a compromised institution, and if internal cybersecurity procedures and staffing are not top-notch, paying the ransom will often resolve the incident faster. Finally, significant price elasticity remains untested when earlier justifications for paying a ransom demand have been made based on saving less than an hour per person at a compromised university with 1,800 staff and faculty.[51] One study found the average ransom demand against educational institutions in 2020 was $447,000,[52] a number that still has room to grow.

- **Insider Threats and Unauthorized Delegation**
  The education user base—staff, faculty, students, and parents/guardians—is dynamic and contains varying degrees of cybersecurity awareness. If sufficient attention is not paid to the convenience side of stronger cybersecurity protections, the user base will continue to find workarounds that negate the added protections, such as sharing credentials and using weak passwords.

IT teams in school districts are stretched and overwhelmed with the growing set of responsibilities for supporting remote learning platforms.

Solutions to Consider for Improving Cybersecurity in Education

In this section, we outline several solutions to consider for improving the cybersecurity posture of the education sector, given the threats faced.

STRENGTHEN IDENTITY AND AUTHENTICATION METHODS

A successful authentication attempt provides access to the data and functions available in the system to the user of the authenticated account, whether that is the correct owner of the account or a threat actor using compromised credentials. Using stronger, longer, and unique passwords per system as opposed to short and reused passwords is a basic yet massive leap in the right direction, but such a step only mitigates access by a threat actor who does not have the compromised password (e.g., is more likely to render lateral movement, credential stuffing and brute force attacks ineffective). A strong, long, and unique password will still compromise an account if the threat actor knows what it is. Modern identity and authentication approaches rely on biometrics, public-key cryptography, and hardware keys rather than a username and password alone.

STRONG MULTI-FACTOR AUTHENTICATION

Strong multi-factor authentication (MFA) will always be more secure than just a username and password. Several approaches are available for MFA, including sending a unique one-time code by text message or email, using an authenticator app on a mobile phone, relying on a hardware security key, or biometric authentication. Various basic attacks have proven successful in compromising unique codes sent by text and email, and if the code is sent by email to a compromised email account, the threat actor has full access. There are also practical and security concerns in relying on text and phone-based methods, including poor cell coverage areas and reliance on personally owned mobile phones. Several sophisticated attacks have compromised systems relying on codes delivered by authenticator apps too.

Modern authentication approaches rely on biometrics, public key cryptography, and hardware keys.

Hardware security keys that support modern authentication protocols such as FIDO2/WebAuthn cannot be phished and are proven to stop account takeover attempts.[53] They also provide the right balance of security and usability compared to mobile-based authenticators.

Biometric authentication is the only authentication method that can verify the identity of the individual requesting access (versus use of a stolen key or token). It does not require the user to carry any additional devices and cannot be used for unauthorized delegation (aka sharing credentials). Biometrics is quickly becoming one of the most convenient and secure methods of authentication, with suitability for many age groups.[54]

MFA should be used everywhere by everyone, but one-size-fits-all approaches do not work; instead, configure security policies to give users appropriate options. When it comes to privileged access—e.g., staff and faculty accessing systems containing sensitive information on students and staff, or finance personnel accessing systems for approving invoices or making payments—hardware security keys or biometric authentication should be used.

ROOT OF TRUST

A benefit of a hardware security key in the current education market is the provision of a secure root of trust that is not tied to any single device. That is, the security key provides the portable root of trust for each user—such as the keys for the cryptographic functions that are an essential part of modern authentication approaches—regardless of what device they are using to access educational systems and applications. Whether it is a mobile device belonging to a school district, an institution-supplied Chromebook, or a personally owned device at home, the security key remains consistent across all as a portable root of trust.

SHORE UP ANTI-PHISHING DEFENSES

With phishing and its more nefarious, targeted variants being the principal and initial attack vector for data breaches, malware infestations, and credential compromise (among others), shoring up phishing defenses is a requirement of the utmost importance. Anti-phishing solutions cover a range of scenarios and attack methods:

- Internal phishing is a growing problem, which happens when a compromised email account is used to send messages to colleagues and coworkers. Due to the trust already established by the real owner of the email account, the threat actor who has compromised the account is able to send malicious payloads that have a higher likelihood of being clicked or opened.
- Scanning messages for known threats, spam signals, malicious attachments, and other indicators to assess whether a message carries a malicious intent.
- Basic email security hygiene should be checked and confirmed in a process that covers email authentication and security methods leveraging DNS capabilities such as SPF, DKIM and DMARC. These can be set by an appropriately skilled IT professional, and there are third-party service providers that can add agility, robustness and reporting to further enforce the basics.
- Scanning for known threats is necessary but insufficient by itself because newer methods that evade signature-based or likeness-based verification are constantly being developed by threat actors. Advanced threat protection solutions look at the behavior of an attachment when opened or open an attachment first in a protected environment to assess for threats, or re-check a link every time it is clicked to ensure that attachments or links marked safe on delivery remain safe after delivery (e.g., to mitigate post-delivery, time-based weaponization).

Basic email security hygiene should be checked and confirmed in a process that covers email authentication and security methods leveraging DNS capabilities.

Phishing defenses go beyond just email security solutions, however, and are greatly enhanced by wider contextual changes, such as using strong MFA, implementing endpoint security to scan for and assess new threats, hardening trusted communication processes beyond email to verify requests for wire transfers, and training personnel is security awareness to erect a human barrier against social engineering attacks. While total eradication of phishing threats is probably impossible, these wider contextual changes prevent the threat actor from being able to cause harm through leveraging stolen credentials.

SCALE IT TALENT WITH CLOUD SECURITY SERVICES

Cloud security services provide a way of scaling IT talent and reducing the need for all the tasks associated with running on-premises infrastructure. Cloud-based services are less prone to on-premises outages caused by local weather, power blackouts, or loss of internet connectivity (e.g., a backhoe severs the internet connection). Examples of cloud services include:

- Email security services that scan for malicious content, identify abnormal communication patterns, and highlight risk factors in new email messages.
- Identity and access management services to verify credentials, check authenticity, and provide access to the right individual. As cloud services are increasingly used for remote learning and institutional operations, a cloud-based identity and access platform has become the standard across many education institutions to provide scalability, reliability, support for remote access, and lower total cost of ownership.
- A Cloud Access Security Broker (CASB) platform provides policy definition, alerts on policy violations, and notifications of abnormal behavior that could indicate malicious activity, credential compromise, or the early stages of an attack. CASBs can also automatically discover the use of new cloud services and apps and verify currency of security settings on cloud storage services.

Cloud security services offer a scalability of impact that school districts acting alone will not be able to achieve with current IT teams.

Cloud security services offer a scalability of impact that school districts acting alone will not be able to achieve with current IT teams.

VULNERABILITY SCANNING AND AUTOMATED PATCHING

Reducing the attack space for ransomware and other forms of malware benefits greatly by decreasing the number of active vulnerabilities on all devices and systems that can be managed. Attempting to do this manually is a big process; "impossible" would be the best word to describe such an approach. However, there are solutions that offer automatic and regular vulnerability scanning, along with automated patching of identified vulnerabilities. These solutions work because they streamline the process of keeping software up to date, and some patching tools even offer virtual patching capabilities so that any system with an active vulnerability but without an available patch can be automatically isolated to prevent compromise. Native patch management tools are often not up to the job and carry unacceptable failure rates; you will need to compare the efficacy of native and dedicated solutions.[55]

HARDEN CONTROLS AND RESTRICTIONS ON DATA ACCESS

In situations where endpoints are not controlled by the school district or university and thus are not manageable to the same degree, hardening controls and restrictions around data access are critical. Solutions that offer risk-based authentication controls or conditional access enable the definition of policies that give different levels of access to people based on identity, device characteristics, network location, time of day, and other attributes of an authentication request. Such solutions can enforce a limited read-only mode on sensitive data when a staff member uses a non-registered and personal device, for example, versus full edit access (if appropriate) when the staff member is connecting via a managed device and using strong authentication mechanisms.

PROTECTED BACKUPS FOR RANSOMWARE RECOVERY

When a threat actor successfully lands a ransomware attack, the absence of backups as a way of recovery severely limits the options of the victim organization. When Athens Independent School District in East Texas suffered a ransomware attack in August 2020, for example, its ability to recover most data from backup negated the need to pay the ransom demand, even though the district held cyber insurance cover.[56] From first principles, all critical IT systems should be backed up regularly, such as databases of student data, systems for coordinating scheduling for rooms, equipment and transportation, and online learning platforms. These backups, however, are of value only if they are protected from a ransomware attack, because ransomware gangs are just as focused on destroying backups as they are for production systems. Cloud-based backup services with strong and unique access controls separate to those of network servers and cloud services offer compelling value to the sector, but any approach that offers regular backups with secure offline storage will be better than nothing. Having nothing available is negligence.

SECURITY AWARENESS TRAINING TO INCREASE CYBERSECURITY COMPETENCE

Increasing the competence of staff, faculty, and students to identify cybersecurity threats is one of the central tenets in improving cybersecurity readiness. Security awareness training includes:

- Process design recommendations on how to enlist the right support when a victim is under attack, e.g., what a teacher should do with a suspected phishing message, or after they have clicked an innocent-looking URL that was actually malicious.
- Content to inform and educate, e.g., training videos, posters, and email campaigns.
- Assessment methods to gauge training efficacy, e.g., phishing simulations.

In combination, the different aspects of an ongoing security awareness training program seek to create a culture of security. When done right, security awareness training can have a substantial effect on threat rates. One school district in St. Louis, Missouri, for example, used simulated phishing campaigns to assess the effect of its security awareness training program after a successful and costly BEC attack, and saw clicks on malicious links in phishing emails drop by more than seven times.[57]

Increasing the competence of staff, faculty, and students to identify cybersecurity threats is one of the central tenets in improving cybersecurity readiness.

ENCRYPTION OF SENSITIVE INFORMATION AND PERSONAL DATA

What protected backups offer as a mitigation against ransomware incidents, strong encryption of sensitive information also offers against the threat of publication of exfiltrated data as part of modern ransomware attacks that combine data theft, illicit data encryption, and extortion. When encrypted, exfiltrated data is worthless as threat leverage. Storage locations covering student data, personal information on faculty, teachers and staff, and other confidential and private data should be encrypted by design and used alongside data analysis and scanning tools to identify other places where unencrypted data is stored—such as in email accounts and file shares.

MAKE SECURITY MORE CONVENIENT

Although an increase in security protections is critical to prevent cyberattacks, providing users with convenient solutions is just as important. Increasing security without making it more convenient can lead to users circumventing security controls and lack of user adoption of new services. Examples include:

- Single sign-on (SSO) enables access to multiple systems through a single identity, thus eliminating the need for a user to manage multiple usernames and passwords. SSO reduces the number of times a password and additional credentials are requested, reducing password fatigue and the sense of annoyance as users access applications throughout their day. For IT teams, SSO enables a single point of revocation to remove access across systems, thus elevating system-level access controls.
- Self-service password reset gives students, staff, and faculty the ability to recover their own credentials without having to call the help desk for a manual intervention. Particularly at peak times, such as the start of a new school year, self-service password reset is a lifesaver for IT teams—and a good way of reducing operational costs.
- Convenience with MFA requires supporting multiple options in security policies so that if the primary authentication method is unavailable, appropriate alternatives exist for the student, staff, or faculty member. There will be times and situations when a mobile authenticator is not available (e.g., a student loses their phone), or a device does not have a fingerprint reader, or there is no cell coverage for receiving SMS codes, and thus multiple valid options are essential.

Increase security protections but also make security more convenient. Without convenience, adoption and usage will suffer.

Best Practices for Cybersecurity in Education

The right solutions will improve cybersecurity preparedness in the education sector, but solutions alone cannot fully address the cybersecurity threats at play. That requires the synergy of people, processes, and technology, and in this section, we look at the processes or best practices aspect.

DEVELOP A RISK ASSESSMENT FOR YOUR INSTITUTION

This report has profiled the general trends in cyberthreats faced by institutions in the educational sector, but a vague sense of general trends is insufficient to safeguard your organization. Develop a risk assessment for your organization to understand the specific risks and cyberthreats you are facing. Inputs to this risk assessment are likely to include:

- Trends in educational sector cyberthreats, along with warnings and advisories from government and educational cybersecurity agencies. Threats from phishing and ransomware will feature heavily.
- Telemetry from your own network, including recent attack patterns, device usage and currency, and a catalog of apps and services in use.
- Incident reports from your own organization, of successful cyberattacks, and if available, incident reports from other organizations that you collaborate with to get a sense of supply chain threat vectors.
- Third-party cybersecurity consulting services, where feasible, to identify and assess the severity of actual threats.
- Reviews of current cybersecurity controls, along with an assessment of their ability to withstand current and forecasted attack patterns. For example, in the event of a cyberattack, how well would your organization currently be able to respond and assure continuity of essential teaching, research and administrative functions? If a ransomware attack took out your school district, how well and how quickly would you be able to respond and recover?
- Review user access behavior, such as failed login attempts, password resets, and authentication methods in use to learn more about the user population. Examining, filtering, and sorting access logs by type of behavior enables the early identification of potential threat areas and gives an evidence-based approach when seeking ways of hardening authentication requirements.

A comprehensive assessment of actual risks and the efficacy of current mitigations, combined with a sense of the severity and impact of each risk type, provides a prioritized list to work from.

Developing a risk assessment is not a one-time event. At a minimum, revisit and update the risk assessment for your organization annually.

Develop a risk assessment for your organization to understand the specific risks and cyberthreats you are facing.

EVALUATE CYBERSECURITY PREPAREDNESS DURING VENDOR SELECTION

Cybersecurity preparedness is just as important in selecting third-party vendors as any other decision factor, including pricing (even "free" is too expensive if cybersecurity protections are lacking). Include assessment and evaluation questions on cybersecurity preparedness when looking for vendors to manage student records, enable remote learning, perform financial management tasks, and improve cybersecurity. One K-12 school district learned this lesson too late in 2020, when its remote learning platform was shut down by a denial-of-service attack launched by one of its own students; the third-party vendor in question lacked even basic protections to withstand the attack.[58]

Assessment and evaluation questions on cybersecurity preparedness should cover:

- Breach response plans.
- Incident and resolution reports on previous incidents—and corrective actions taken consequently.
- Categories of personal and sensitive information collected, particularly on students, and data protection measures.
- The currency of third-party certifications for security and data protection practices, such as ISO 27001 for information security and/or ISO 27018 for protecting personal data in cloud services. These give strong assurance to the preparedness (albeit not perfection or immunity) of the vendor in question.
- Specific expertise in the education sector, given its unique challenges.
- The adaptability and extensibility of solutions to give multiple security options to users, and a growth path for the educational institution to do more with the solution or platform over time.

Look for vendors with specific expertise in the education sector.

COLLABORATE WITH PEERS IN THE EDUCATION SECTOR

Lack of cybersecurity talent in the education sector is a huge challenge, but it is a wider global and cross-industry challenge as well. Few organizations in any industry have the resources to cover every cybersecurity skill set through in-house staffing. However, there are ways to collaborate with peers across the education sector to multiply strengths and address systemic weaknesses. For example:

- In the United States, the Consortium of School Networking (CoSN)[59] is a professional association for technology leaders in the K-12 school system. It provides targeted resources on emerging technologies and acts as an advocacy group to the government for increased funding for cybersecurity protections in the K-12 sector, among other needs. For IT and cybersecurity in higher education, EDUCAUSE[60] is the professional association in the United States. It maintains active engagement with international sister organizations. In the United Kingdom, the National Cyber Security Centre[61] offers advice and guidance to the education sector, among others. The Joint Information Systems Committee (Jisc)[62] in the United Kingdom is also active in cybersecurity matters for higher education. Look around in your country for peers facing similar challenges, and for government or not-for-profit organizations that are actively at work to equip and enable elevated cybersecurity capabilities.

- In the age of online and remote learning, investigate the availability of webinars, podcasts, blog posts and other resources written by vendors focusing on the education sector, along with peers from schools and universities. Traveling to attend conferences and workshops on cybersecurity is difficult in the current health crisis, but the information is out there and can be obtained in formats suitable for anywhere, anytime reference.
- Seek out technology leaders and cybersecurity professionals in nearby school districts. If the appropriate agreements are put in place between school districts, a staff member in one district with skills in a particular cybersecurity area could contribute expertise or upskill others in other districts. What cannot be addressed acting alone is more likely to be addressed acting in concert with others, and everyone is facing the same set of challenges.

SECURE CYBER INSURANCE COVER

Cyber insurance coverage offers financial protection for an educational institution in the face of a significant cyberattack, and having a risk-weighted approach to ensuring ongoing viability of the institution is a good safeguard. However, the deeper reason for seeking cyber insurance coverage is the visibility it provides into current systemic weaknesses and threat areas for the institution, because an insurance company is financially motivated to assist clients in minimizing their risk profile. The discipline of applying for cyber insurance, including evaluating current state and mitigating the most egregious threat vectors, offers one form of independent audit and verification that appropriate cybersecurity protections have been enacted. And as additional protections are put in place, the pricing of the insurance premium should decrease.

The discipline of applying for cyber insurance offers one form of independent audit and verification that appropriate cybersecurity protections have been enacted.

INCREASE AUTHENTICATION HYGIENE

Practices that increase authentication hygiene complement solutions that harden controls and restrictions on data access (see our discussion in the Solutions section). Increasing authentication hygiene includes taking the following actions:

- Using unique and strong passwords for different systems, combined with strong multi-factor authentication wherever available. Reused passwords and non-usage of multi-factor authentication makes credential compromise attacks and lateral movement attempts simple for threat actors. Single sign-on unifies access to multiple systems through a single credential and gives IT teams the ability to seamlessly revoke access to individuals across all connected systems.
- IT security admins should set security policies that support multiple forms of strong authentication that are appropriate for the institution. Reliance on any single form of MFA, for example, is prone to failure when the factor is missing (e.g., the student left it at home), inaccessible (e.g., there is no biometric reader on a given device), or inoperable (e.g., no cell coverage for receiving the code by text message). Having a short list of viable options keeps MFA in use without resorting to calling the help desk.

- Changing the default usernames and passwords on devices that connect to the internet. Universities and school districts need to do this to reduce the ability of a threat actor to leverage default settings on networking gear used within the institution, and for students studying remotely, a security awareness training module on changing passwords for home routers and home Wi-Fi network devices will be essential. Younger students will need to enlist the help of a parent or guardian to carry out such tasks.
- Early "Zoom bombing" incidents reminded the world of the need to have passwords for online classroom sessions, but there are still cases where passwords are not set because the event is supposed to be one for the community, or where students share login credentials too freely on social apps. Passwords should always be required, and a registration process used when sessions are opened to the wider community. A moderator should be present to identify and authorize entry of all participants.
- Auditing which accounts have admin privileges on different systems, minimizing user accounts that combine day-to-day user functions with admin rights, and enforcing strong multi-factor authentication methods whenever an admin account is used. Based on the audit results, remove admin privileges from user accounts where such rights are no longer required; it is too easy to allow slippage or temporary workarounds to become a permanent fixture and threat foothold. Audits should be carried out regularly at minimum, or ongoing automated monitoring put in place to track the usage of admin accounts.

Remove admin privileges from user accounts where such rights are no longer required.

GOVERN THE INFORMATION LIFECYCLE

Practice strong information governance through archiving, deletion, obfuscation, and other methods of reducing the data estate available for easy access. Failing to archive historical data clogs current systems and creates a much larger footprint of data that can be breached and exfiltrated. Not all data is worthy of being archived, and if no mandatory retention requirements are met, unnecessary and low value data should be deleted. Obfuscation replaces personal data values with meaningless data that must be cross-referenced to another secured system, thereby rendering the data useful for analytical insight but not identification of individuals. Practices such as these reduce the risks of data breaches and the extent of exfiltration. The Australian National University would have benefitted from such practices since a recent data breach compromised 19 years' worth of personal and sensitive data on upwards of 200,000 people.[63]

Next Actions

It is clear that the education sector is under cyberattack, and that schools and higher education institutions need to be doing more to protect themselves. In closing this white paper, we offer three additional pointers:

- Wherever possible, simplify the infrastructure to minimize variation in devices, applications, and connections between systems. Having fewer variations reduces the attack surface available to threat actors, while having fewer places to store sensitive and personal data enables tighter restrictions and controls to be put in place. More begets complexity, and complexity is the friend of threat actors.
- While the IT teams at each school district and educational institution have many tasks to complete, ultimately the advice to "work harder and do more" eventually hits natural capability limits. There comes a time when doing more is not possible; all that can be done with the resourcing available is being done. With the education sector being chronically under-resourced for cybersecurity, the high-level change required is greater funding from the federal or central government and other sources. There are organizations championing greater funding for cybersecurity, such as CoSN in the United States (see above). At a more local level and immediate timeframe, addressing cybersecurity threats more effectively may look like resource-sharing agreements between schools, automating general IT tasks to give more time for cybersecurity matters, and leveraging cloud services that do more for less. For schools that have cybersecurity programs for students, there may be opportunities for cybersecurity internships with the school, and cybersecurity ambassador roles with the wider student population.
- There is a cultural change needed, too, in how educators interact with the digital channels they work through. A level of suspicion about the potential for wrongdoing through digital channels needs to be cultivated, and security awareness training methods are a good way of doing this. Just knowing that threat actors are active and sophisticated, and having a sense of what a threat can look like—e.g., the iTunes gift card scam—gives staff and faculty new tools to detect and evade threats.

Cultivate a level of suspicion in educators about the potential for wrongdoing through digital channels.

Sponsor of This White Paper

MIMECAST

Mimecast makes business email and data safer for more than 36,000 customers and their millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management in a single, fully integrated subscription service. Mimecast reduces risk, complexity, and the cost of managing the array of point solutions traditionally used to protect email and its data.

For customers that are looking to reduce the cost and time to move legacy data, Mimecast Simply Migrate extracts, validates, and transports your legacy data from common archives like Veritas Enterprise Vault and Dell EMC SourceOne to the Mimecast Cloud Archive. Mimecast manages archives in specific geographic regions and ensures that they are tamper-resistant. The result is alignment with your regulatory compliance requirements, support for rapid e-discovery and flexible retention management for managing corporate information. Mimecast Cloud Archive integrates a highly secure data repository, built-in data recovery, simplified storage management and robust e-discovery, compliance, and case management capabilities. It can empower business by reducing risk and cost, empower employees by increasing their productivity, and empower administrators by decreasing complexity.

www.mimecast.com

@mimecast

UK/EUROPE
+44 (0) 207 847 8700
info@mimecast.com

NORTH AMERICA
+1 800 660 1194
+1 781 996 5340
info@mimecast.com

SOUTH AFRICA
+27 (0) 117 223 700
0861 114 063
info@mimecast.co.za

AUSTRALIA
+61 3 9017 5101
1300 307 318
info@mimecast.co.au

---

[1] Microsoft Security Intelligence, Global Threat Activity, February 2021, at https://www.microsoft.com/en-us/wdsi/threats

[2] Webroot, Cyber Threats to Small- and Medium-Sized Businesses in 2017, at https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/2114/9911/0468/SMB-MSP_Survey_US.pdf

[3] Security Scorecard, 2018 Education Cybersecurity Report, at https://securityscorecard.com/resources/2018-education-report

[4] Kim Griffin, Fake Phishing Emails Expose Need for Cybersecurity Training, March 2020, at https://edtechmagazine.com/k12/article/2020/03/fake-phishing-emails-expose-need-cybersecurity-training

[5] Lillian Reed, Alison Knezevich and Liz Bowie, As Baltimore County Recovers from Ransomware Attack, State Audits Have Routinely Found Security Problems in Other Districts, December 2020, at https://www.baltimoresun.com/education/bs-pr-md-baltimore-county-ransomware-20201203-20201204-5g3he4yi2je6npug3vcf7zih3i-story.html

[6] Lee Roop, Huntsville City Schools Will Reopen Monday Without Computers, December 2020, at https://www.al.com/crime/2020/12/huntsville-city-schools-will-reopen-monday-without-computers.html

[7] HIPAA Journal, $4.1m Settlement for 2010 Stanford University Hospital HIPAA Breach, March 2014, at https://www.hipaajournal.com/4-1m-settlement-2010-stanford-university-hospital-hipaa-breach/

[8] Nicole Perlroth, Penn State's College of Engineering Hit by Cyberattack, May 2015, at https://bits.blogs.nytimes.com/2015/05/15/penn-states-college-of-engineering-hit-by-cyberattack/?_r=0

[9] K-12 Cybersecurity Resource Center, K-12 Cybersecurity 2019 Year in Review—Part III. Cybersecurity Incidents: 2019, February 2020, at https://k12cybersecure.com/year-in-review/2019-incidents/

[10] The K-12 Cybersecurity Resource Center, The K-12 Cyber Incident Map, February 2021, at https://k12cybersecure.com/map/

[11] Stacy Campbell, Cybersecurity in Higher Education: Problems and Solutions, 2017, at https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

[12] Impact, 10 Cybersecurity in Education Stats You Should Know, October 2020, at https://www.impactmybiz.com/blog/cybersecurity-in-education-stats-2020/

[13] Ayse Kaya Firat, Privacy and Cybersecurity in Education: A Constant Battle, January 2017, at https://www.rsaconference.com/industry-topics/blog/privacy-and-cybersecurity-in-education-a-constant-battle

[14] Micah Castelo, Cyberattacks Increasingly Threaten Schools—Here's What to Know, June 2020, at https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon

[15] Microsoft Security Intelligence, Global Threat Activity, February 2021, at https://www.microsoft.com/en-us/wdsi/threats

[16] Bitdefender, Mid-Year Threat Landscape Report 2020, July 2020, at https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

[17] Joel Alcon, 13% of the Higher Education Sector Has Been Infected with Ransomware, October 2016, at https://www.bitsight.com/blog/higher-education-infected-with-ransomware

[18] Dan Dahlberg, Ransomware Cyber Attacks: Which Industries Are Being Hit the Hardest?, October 2017, at https://www.bitsight.com/blog/ransomware-cyber-attacks

[19] CISA, Alert AA20-345A—Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data, December 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-345a
[20] Check Point Research, Not For Higher Education: Cybercriminals Target Academic and Research Institutions Across the World, September 2020, at https://blog.checkpoint.com/2020/09/15/not-for-higher-education-cybercriminals-target-academic-research-institutions-across-the-world/
[21] BlueVoyant, BlueVoyant Report Reveals Ransomware is the Number 1 Cyber Threat Facing Higher Education, February 2021, at https://www.bluevoyant.com/news/bluevoyant-report-reveals-ransomware-is-the-number-1-cyber-threat-facing-higher-education/
[22] Jenni Bergal, Cybercriminals Strike Schools Amid Pandemic, September 2020, at https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/09/22/cybercriminals-strike-schools-amid-pandemic
[23] Hartford Public Schools, HPS Opening Postponed: Tuesday Sept 8, September 2020, at https://www.hartfordschools.org/hps-opening-postponed-tuesday-sept-8/
[24] Liz Bowie and Alison Knezevich, Ransomware Attack Cripples Baltimore County Public Schools. No Timeline for Return to Class, November 2020, at https://www.baltimoresun.com/maryland/baltimore-county/cng-co-baltimore-county-schools-closed-network-issue-20201125-drhmnq5ilraplea2h4v7p4pn34-story.html
[25] WKYT News Staff, Scott County Schools Victim of $3.7 Million Scam, April 2019, at https://www.wkyt.com/content/news/Scott-County-Schools-victim-of-37-million-scam-509017341.html
[26] Carrie Fellner, Australian Catholic University Staff Details Stolen in Fresh Data Breach, June 2019, at https://www.smh.com.au/national/australian-catholic-university-staff-details-stolen-in-fresh-data-breach-20190617-p51yif.html
[27] Melanie Barden, FBI Investigating After Manor ISD Loses $2.3M in Phishing Email Scam, January 2020, at https://web.archive.org/web/20200111153128/https://news4sanantonio.com/news/local/fbi-investigating-after-manor-isd-loses-23m-in-phishing-email-scam
[28] Chelsea Sheasley, As Remote Learning Spreads, So Have Cyberattacks. Are Schools Ready?, November 2020, at https://www.csmonitor.com/USA/Education/2020/1103/As-remote-learning-spreads-so-have-cyberattacks.-Are-schools-ready
[29] Dustin Volz, Chinese Hackers Target University of Hawaii, MIT and Other Schools in Pursuit of Military Secrets, March 2019, at https://www.marketwatch.com/story/chinese-hackers-target-university-of-hawaii-mit-and-other-schools-in-pursuit-of-military-secrets-2019-03-05
[30] Catalin Cimpanu, FBI Warns About Attacks That Bypass Multi-Factor Authentication (MFA), October 2019, at https://www.zdnet.com/article/fbi-warns-about-attacks-that-bypass-multi-factor-authentication-mfa/
[31] K-12 Cybersecurity Resource Center, K-12 Cybersecurity 2019 Year in Review—Part III. Cybersecurity Incidents: 2019, February 2020, at https://k12cybersecure.com/year-in-review/2019-incidents/
[32] Benjamin Herold, Florida Virtual School Reveals Huge Data Breaches, March 2018, at https://www.edweek.org/technology/florida-virtual-school-reveals-huge-data-breaches/2018/03
[33] Parmy Olson, Pearson Hack Exposed Details on Thousands of U.S. Students, July 2019, at https://www.wsj.com/articles/pearson-hack-exposed-details-on-thousands-of-u-s-students-11564619001
[34] Michael Sessa, SU Data Breach Exposes Nearly 10,000 Names, Social Security Numbers, February 2021, at http://dailyorange.com/2021/02/names-social-security-numbers-of-syracuse-university-students-exposed-in-data-breach/
[35] Mary Jo Ola, Shorewood School District Mistakenly Releases Student Info While Responding to Records Request, February 2021, at https://www.tmj4.com/news/local-news/shorewood-school-district-mistakenly-releases-student-info-while-responding-to-records-request
[36] Alyse Stanley, Teen Hacker Charged with Paralyzing Miami Schools in Embarrassingly Simple Cyberattack, September 2020, at https://gizmodo.com/teen-hacker-charged-with-paralyzing-miami-schools-in-em-1844968182
[37] Ed Technology, 20% Rise in Cyber-Attacks on Global Education Sector in Last Eight Weeks, September 2020, at https://edtechnology.co.uk/cybersecurity/20-rise-in-cyber-attacks-on-global-education-sector-in-last-eight-weeks/
[38] Kim Griffin, Fake Phishing Emails Expose Need for Cybersecurity Training, March 2020, at https://edtechmagazine.com/k12/article/2020/03/fake-phishing-emails-expose-need-cybersecurity-training
[39] Lillian Reed, Alison Knezevich and Liz Bowie, As Baltimore County Recovers from Ransomware Attack, State Audits Have Routinely Found Security Problems in Other Districts, December 2020, at https://www.baltimoresun.com/education/bs-pr-md-baltimore-county-ransomware-20201203-20201204-5g3he4yi2je6npug3vcf7zih3i-story.html
[40] Micah Castelo, Cyberattacks Increasingly Threaten Schools—Here's What to Know, June 2020, at https://edtechmagazine.com/k12/article/2020/06/cyberattacks-increasingly-threaten-schools-heres-what-know-perfcon

[41] James Richings, Online Lessons at Slough Secondary School are Hacked, February 2021, at https://www.sloughobserver.co.uk/news/19080984.online-lessons-slough-secondary-school-hacked/
[42] Alyse Stanley, Teen Hacker Charged with Paralyzing Miami Schools in Embarrassingly Simple Cyberattack, September 2020, at https://gizmodo.com/teen-hacker-charged-with-paralyzing-miami-schools-in-em-1844968182
[43] Louis Columbus, It's Time to Solve K-12's Cybersecurity Crisis, October 2019, at https://www.forbes.com/sites/louiscolumbus/2019/10/01/its-time-to-solve-k-12s-cybersecurity-crisis/
[44] Louis Columbus, It's Time to Solve K-12's Cybersecurity Crisis, October 2019, at https://www.forbes.com/sites/louiscolumbus/2019/10/01/its-time-to-solve-k-12s-cybersecurity-crisis/
[45] Bitdefender, Mid-Year Threat Landscape Report 2020, July 2020, at https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf
[46] Phil Muncaster, School CCTV Streams End Up on US Website, February 2018, at https://www.infosecurity-magazine.com/news/school-cctv-streams-end-up-on-us/
[47] Ayse Kaya Firat, Privacy and Cybersecurity in Education: A Constant Battle, January 2017, at https://www.rsaconference.com/industry-topics/blog/privacy-and-cybersecurity-in-education-a-constant-battle
[48] INTERPOL, INTERPOL Report Shows Alarming Rate of Cyberattacks During COVID-19, August 2020, at https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
[49] CISA, Alert AA20-345A—Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data, December 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-345a
[50] Susan Grajek and the 2020-2021 EDUCAUSE IT Issues Panel, Top IT issues, 2021: Emerging from the Pandemic, November 2020, at https://er.educause.edu/articles/2020/11/top-it-issues-2021-emerging-from-the-pandemic
[51] Dave Dormer and Stephanie Wiebe, U of C Ransom Payout Better Than Battling Hackers, Expert Says, June 2016, at https://www.cbc.ca/news/canada/calgary/university-of-calgary-cyberattack-part-of-increasing-problem-1.3621505
[52] BlueVoyant, BlueVoyant Report Reveals Ransomware is the Number 1 Cyber Threat Facing Higher Education, February 2021, at https://www.bluevoyant.com/news/bluevoyant-report-reveals-ransomware-is-the-number-1-cyber-threat-facing-higher-education/
[53] Kurt Thomas and Angelika Moscicki, New Research: How Effective Is Basic Account Hygiene at Preventing Hijacking, May 2019, at https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html
[54] Raconteur, The Rise of Biometrics, at https://www.raconteur.net/infographics/the-rise-of-biometrics/
[55] Louis Columbus, It's Time to Solve K-12's Cybersecurity Crisis, October 2019, at https://www.forbes.com/sites/louiscolumbus/2019/10/01/its-time-to-solve-k-12s-cybersecurity-crisis/
[56] Jenni Bergal, Cybercriminals Strike Schools Amid Pandemic, September 2020, at https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/09/22/cybercriminals-strike-schools-amid-pandemic
[57] Chelsea Sheasley, As Remote Learning Spreads, So Have Cyberattacks. Are Schools Ready?, November 2020, at https://www.csmonitor.com/USA/Education/2020/1103/As-remote-learning-spreads-so-have-cyberattacks.-Are-schools-ready
[58] Alyse Stanley, Teen Hacker Charged with Paralyzing Miami Schools in Embarrassingly Simple Cyberattack, September 2020, at https://gizmodo.com/teen-hacker-charged-with-paralyzing-miami-schools-in-em-1844968182
[59] https://cosn.org
[60] https://www.educause.edu/
[61] https://www.ncsc.gov.uk
[62] https://www.jisc.ac.uk/cyber-security
[63] Lisa Martin, Australian National University Hit By Huge Data Breach, June 2019, at https://www.theguardian.com/australia-news/2019/jun/04/australian-national-university-hit-by-huge-data-breach