Paying the price

Ransomware in education

verizon✓

An evolving threat

Ransomware is becoming an inescapable reality for today's educators. Victims pay the price, even when they don't pay the ransom.

For the uninitiated, ransomware is a type of cyberattack that occurs when malicious malware blocks access to, or actually steals, an institution's sensitive data. Victims must pay a ransom to regain access or have their data restored. Ransoms demanded of schools and universities have escalated to the hundreds of thousands of dollars in recent years.

According to Verizon Threat Research Advisory Center (VTRAC) consultants, the number of schools hit by ransomware nearly doubled between 2021 and 2022. The threat shows no signs of slowing down in 2023. In just the first month of the new year, high-profile ransomware attacks targeted schools in Massachusetts, Iowa, and Arizona.[1]

The financial costs of ransomware are staggering. In addition to the ransom itself – like the $250,000 paid by Little Rock schools in late 2022[2] – system upgrades and other associated costs are usually incurred. In 2022 alone, ransomware attacks cost educational institutions about $4 billion just for the associated downtime.[3]

It's hard to know how much financial damage is done when schools don't pay ransoms because the fallout can last for years. Baltimore County Public Schools (BCPS) declined to pay after their 2020 attack, and the cost so far is an estimated $10 million. This includes system upgrades, security updates, investigations and public relations costs, taxes, fees, fines, negotiation services, and insurance premiums. The hack also canceled classes for several days, destroyed payroll and pension programs, and could still generate several lawsuits.[4]

More recent ransomware attacks, like the one Vice Society launched against the Los Angeles Unified Schools (LAUS) in late 2021, could also have several years of costly ripple effects since it's one of the largest districts in the country. LAUSD also refused to pay a ransom, and more than 500 gigabytes (GB) of sensitive student and staff data has already been posted online.

The situation is so dire that the FBI and the U.S. Cybersecurity & Infrastructure Security Agency (CISA) issued formal alerts about the threat of ransomware to schools in January of 2023.[5]

The danger to education is not only pervasive and alarming, but the cyberterrorists who target schools are becoming much more efficient with their techniques. Whether public or private, K-12 or higher ed, schools of every size need to take measures to protect themselves against this evolving cyberthreat.

2,000

Approximate number of schools affected by ransomware in 2022.

— VTRAC

56%

K-12

and

64%

colleges

worldwide report being hit by ransomware.

– 2022 Sophos Global Survey

Contents

Executive summary

Educators are likely very aware that their schools and their districts are major targets for cyberattacks. But the primary goal of educators is, of course, to educate – it's hard to focus on building a robust cybersecurity posture when it's not your chief function, when your financial resources may be limited, and when other priorities demand more of your attention. And with cybersecurity, it's hard to know how much is "enough" until it's too late.

But security is not just an IT department issue, it's something that affects every administrator, school board member, teacher, parent and student. As education comes to rely more on technology and connectivity, bad actors are better positioned to take advantage.

There are a lot of ways hackers can attack, but ransomware seems to be the weapon of choice for hitting schools. In this paper, we'll look at why ransomware is the preferred method of hackers looking to steal from educational institutions. We'll also explore how ransomware has evolved from copycat emails into a highly strategic, trillion-dollar enterprise.

At Verizon, we believe that being cyberaware and understanding our adversaries can be key to protecting ourselves, our customers, and our data assets. So, whether you're a Verizon customer or not, we hope the information provided here can help educators and their schools better understand the cyberrisks of ransomware. Perhaps by learning more about our adversaries, we can all formulate smarter business strategies for greater insight and awareness of today's rapidly evolving security threats.

$4B

Cost to schools in 2022 just for the downtime associated with ransomware.

The Goal

Understand the threat

Avoid risky behavior

Learn about helpful tools

Find out how to stay vigilant

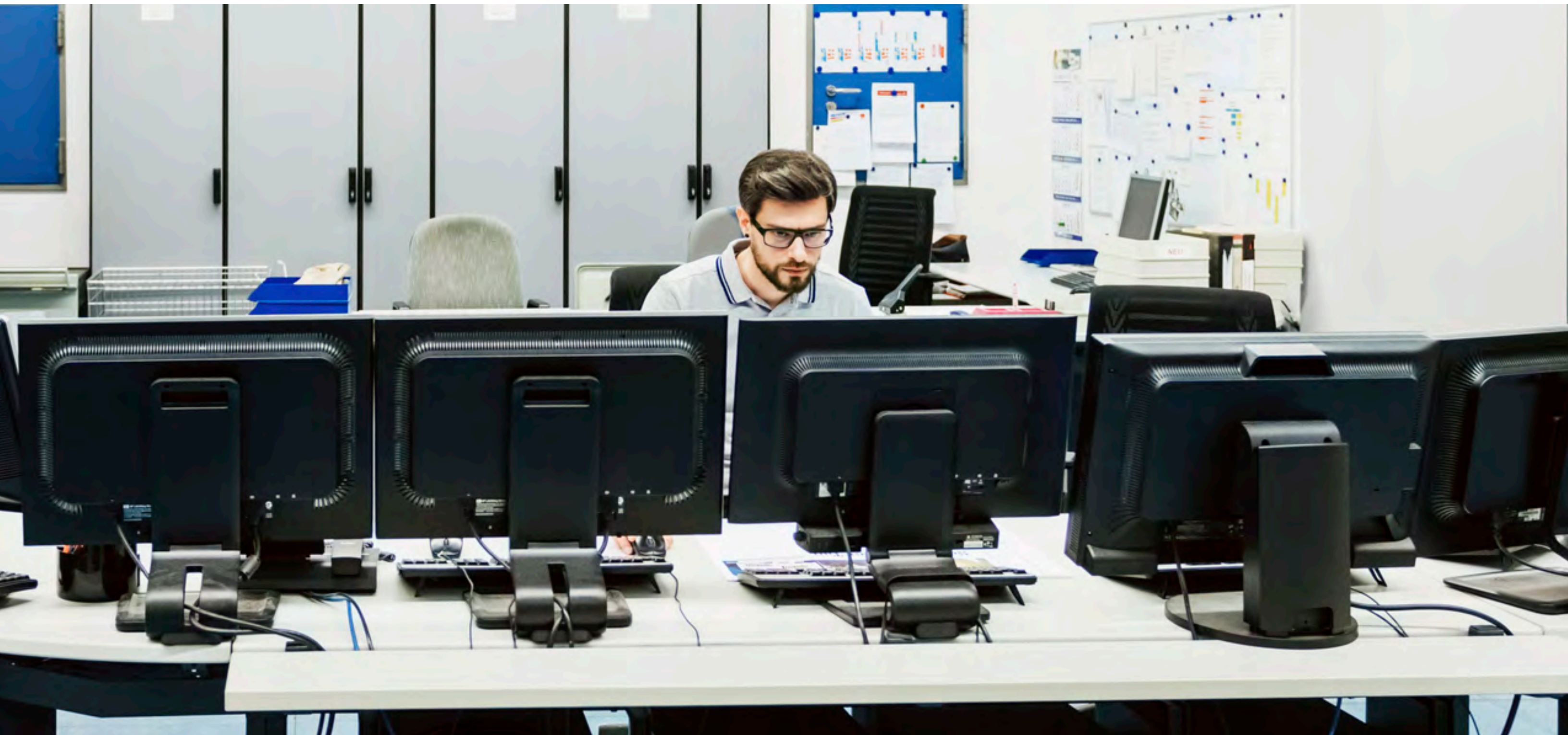
A brief history of ransomware

Ransomware has been around since the late 1980s. Initially it was stored on floppy disks that were mailed out with the idea that curious recipients would simply insert the disks into their hard drives to see what was on them, unwittingly installing the malware. The earliest recorded ransom demands were $189. Then when email became the norm, phishing emails came into vogue. A phishing email is a form of social engineering, where a bad actor sends an email that looks to be a legitimate communication from a recognizable business or friend, but the email is actually a “trojan horse” that tricks the recipient into clicking a link or downloading an attachment. The link or attachment actually installs malware, locking up the recipient’s data. The recipient, now a victim, had to pay a ransom in order to have their data and systems restored. The ransom was usually paid in bitcoin or other cryptocurrency. Sometimes, rather than just blocking access to the victim’s data, the hacker would threaten to expose their victim’s data unless a ransom was paid. The various types of ransomware are given names, like 1989’s AIDS trojan, CryptoLocker, and current plagues like Royal, Vice Society, and LockBit.

From 2013-2018, ransomware went mainstream and was estimated to have done tens of millions of dollars in damage, thanks to big-name strains like Reveton, CryptoLocker and CryptoWall that spread worldwide. That time period also saw the beginning of Ransomware as a service (RaaS), which allows cybercriminals with limited technical skills to purchase ransomware on the dark web.

“It is important to note that when you receive the ransomware note, all of your data has already been compromised. The threat actor has likely already dwelled in your environment for weeks if not months.”

– Jim Meehan, Assoc. Director
Digital Forensics and Incident Response (DFIR)/Global Investigation
Verizon Threat Intelligence



Today, ransomware is an organized crime industry worth trillions of dollars. According to Verizon's 2022 Data Breach Investigations Report (DBIR), ransomware accounts for roughly a quarter of all cyberattacks in the U.S.[6] Ransomware attackers have developed into vast underworld enterprises, nation-states have adopted the tactics as part of governmental cyberwarfare, and bad actors have discovered the benefits of large-scale corporate assaults and supply chain attacks. Ransomware practitioners also utilize double extortion, where hackers exfiltrate their victims' data to a separate location and threaten to leak it, as well as encrypt it and demand a ransom for the decryption. Phishing emails have also evolved – no longer are they easy to spot, with spelling errors and amateurish, copy/pasted business logos. Modern phishing emails look much more professional and legitimate (and enticing).

Ransomware attacks increased more in 2022 than the previous five years combined.

– 2022 Verizon DBIR

These modern-day cybercrime conglomerates come complete with human resource departments, help lines that guide victims through the online payment process, as well as public relations and reputation management. They have affiliates and franchises, and they compete with each other just like "legitimate" corporate entities. And the varying groups even argue publicly over differences in politics.

Cybercriminals are also willing to share their best (or worst) practices with each other, especially after they get caught. The dark web is replete with cautionary tales on how to avoid detection by law enforcement.

Knowing all of this can make it seem like cyberterrorists and ransomware are enemies too overwhelming for a publicly-funded school district or lone university to take on. But there are ways schools and educational systems can protect themselves.

Targeting education

According to the VTRAC team, nearly 2,000 schools were hit by ransomware in 2022. Education is second only to government as the industry most targeted by ransomware, according to Statista.[7] So why are hackers targeting educational institutions? When we think of well-funded institutions, schools, universities, and ISDs aren't usually the ones that leap to mind. In fact, many educational districts are reported to be beleaguered and struggling financially, especially in the wake of the COVID-19 pandemic and the associated lockdowns.[8][9][10]

Along with the more sophisticated methodology of the current ransomware enterprises comes a more strategic approach; before any data is stolen, encrypted and before any ransom demanded, these education predators do their homework. Many cyberterrorists will infiltrate a school system's servers ahead of time to research topics like

- Budget information
- Whether there is cybersecurity insurance
- Any related insurance payout information
- Discretionary fund details
- Bond language
- Financial health
- IT systems
- Data organization
- IT staffing

136%

increase in the average ransom demand in the U.S from 2021 to 2022 – from $375,311 to $887,360.[11]

Bad actors often know from the outset how much money these schools have on hand before they even make the ask, and they've increased their leverage before they start their attack. Their due diligence assures them that there is money for the taking. There is also a belief that bureaucratic institutions always have coffers to go to when embattled, especially when minors are involved.

Unfortunately, there is a perception that education is an easy target. School districts aren't known to have big IT departments, at least not as large as say, financial institutions or retail chains. For-profit entities are likely to have hundreds of people in IT protecting their data infrastructure, whereas a publicly-funded ISD is expected to have a more skeletal staff that a threat actor can exploit. Along with the smaller staffs, public schools tend to have legacy data systems that can also make them more susceptible to cyberthreats.

Schools also have the added element of public pressure; since many are public institutions, they have a duty to disclose when they're hacked. Cyberterrorists know the possibility of embarrassment and humiliation, the pressure of having to deal with the matter publicly, and the likelihood of managing the situation in front of the media, angry parents and unhappy taxpayers is a major inducement to pay a ransom. There's also the chance that, despite the attack, the schools themselves will be held accountable. Returning to the case of the Baltimore County Public Schools, even though they were insured, the school system itself has been found partly responsible due to failure

to comply with IT recommendations made in 2008. Therefore, insurance is paying out only $2 million of the expected $10 million in damages, and the lack of compliance revealed by the hack is likely to harm BCPS even further down the line.[12]

Universities aren't exempt, either. Nearly 64 percent of higher education organizations were affected by ransomware in 2022 – that's an increase of 44 percent from the previous year.[13] One high-profile ransomware attack saw the University of California, San Francisco (UCSF) paying $1.1 million because officials estimated it would cost them at least $10 million to rebuild their systems if they didn't pay.[14]

College campuses are basically small cities, complete with banking institutions, restaurants, housing complexes, mail centers – each representing hundreds of points of vulnerability and millions of endpoints overall. The multiple departments and divisions make it very difficult to create consistency with their security across the university.

> "Many of these attacks on the education sector can be attributed to a single ransomware group – Vice Society."
>
> – Abdul Abufilat,
> Consultant
> Verizon Threat
> Intelligence

Other threats

Ransomware is not the only method hackers use to attack schools, even though it is the most common. Other tactics seen in education include:

DDoS

Distributed Denial of Service, or Dos, are a common type of attack on all levels of Education venues. The goal is to overwhelm a system with traffic as a way to shut it down. Money made off of DDoS attacks usually involves blackmailing businesses to avoid the deluge or stop attacks in progress. Like ransomware as a service (RaaS), DDoS attacks can be purchased via a "Software as a Service" (SaaS) model - a DDoS on demand. DDoS attacks in education are typically used for disruption, often by students looking to avoid tests or classes or just cause a little mischief. For example, the entire Pinellas County School district in Florida was shut down for two days by a DDoS attack by a high school student who simply wanted to know if he could accomplish it. (The student was discovered, expelled, and turned over to law enforcement.)[15] Sometimes DDoS attacks are used as means of protest against school policies or make political statements.

$8T

Cybercrime is the world's third-largest economy after the U.S. and China, expected to top $8 trillion in 2023.

— World Economic Forum (WEF)

Phishing

While phishing can be used to launch ransomware, the social engineering emails are also an effective cyberattack of its own. A phish can be used to acquire data or other resources through a fraudulent solicitation in an email, text or on a spoofed website.

Video conferencing disruptions

During pandemic lockdowns when remote learning became the norm, video conferencing disruptions became the norm as well. These attacks interrupt teleconferences and online learning, often with pornographic or hate images and threatening language. Like DDoS, they tend to be more about disruption than financial gain.

Data theft

Like Phishing, data theft can be a component of ransomware, but it can also be a standalone tactic. It can be done maliciously or for financial gain, where the hacker will blackmail the victim over the contents of the data, to avoid having the data publicized, or to retrieve the data itself.

To pay or not to pay?

Some school districts, like Little Rock in Arkansas, pay the ransom. Some, like Baltimore and Los Angeles, don't. Obviously, there is no easy answer and there are a lot of factors that must be considered in these decisions: Insurance, legislative requirements, and the circumstances of each particular attack. And of course, when dealing with criminals, there's no guarantee the cyberattackers will hold up their end of the bargain even if a ransom is paid. There are no hard and fast rules about whether ransomware demands should be met, and every cost/benefit analysis yields unique results.

In some places, the decision on whether to pay is made for you. In 2022, North Carolina and Florida banned any government entities from making payments associated with ransomware. The next few years should reveal whether the legislation helped curtail ransomware attacks in those states. At the federal level, the U.S. Department of the Treasury bans payment to certain sanctioned hacker groups.

Regardless of location and circumstance, when a ransomware attack happens, professional cybersecurity guidance should be sought.

2

states have made it illegal for government entitities to make payments related to ransomware.

Conclusion: Defense tactics

No one has an infinite amount of money to spend on cybersecurity. But it pays to be proactive. Perhaps the most straightforward way to avoid a data breach is to train the staff. Teachers, support staff, admins, coaches – anyone with a login should be taught to avoid phishing emails and bogus links. Human missteps are still far and away the biggest reason ransomware is so successful. Malicious links can come from emails, texts, and even phone calls, but they can be avoided. Regular IT awareness training for staff and students should be conducted to ensure everyone with access is taught to

- Create strong, unique passwords
- Use multi-factor authentication
- Never share logins or passwords online, in emails, via texts, or by phone
- Avoid clicking links in emails from someone they don't recognize
- Go to sites to verify information rather than clicking through from emails

It takes a combination of appropriate human behavior and tech tools to properly protect data. Other best practices include

- Keeping all software and operating systems up to date and patched
- Removing any unnecessary access to administrative systems
- Conducting regular penetration and vulnerability testing to objectively test security posture
- Creating redundant, offline systems that are backed up frequently. Using a host-based firewall
- Considering and researching cybersecurity insurance
- Getting advice from cybersecurity consultants if possible
- Building a strong incident response plan

The government is working to help. When CISA issued its ransomware warning for education in January of 2023 (the advisory is available here and its companion digital toolkit is provided here – all links shown are also listed in the "References" section below.), it included several other helpful reports and resources offering guidance and standards for cybersecurity in education. The U.S. Government Accountability Office also issued recommendations around cybersecurity in education in October of 2022, available here.

The 2021 Infrastructure Investment and Jobs Act (IIJA) allocated roughly $1 billion in federal grants to improve state and local government cybersecurity between 2022 and 2025. Each state is required to match a certain percentage of grants. To secure funds, they must submit a plan to CISA with a statewide planning committee.

82%

of data breaches involve the human element, including social attacks, error, and misuse; but social attacks like phishing and pretexting were responsible for the majority.

– 2022 Verizon DBIR

"Most often, these attacks keep happening because somebody on staff clicks something they shouldn't."

– David Kennedy,
Principal Consultant
Verizon VTRAC

Educating the educators

A good cybersecurity posture is important, but it also pays to stay current with cyberthreats, especially to education. Verizon and VTRAC offer monthly threat briefings that you can attend at no charge and regardless of whether or not you are a Verizon customer. Register for the monthly briefings by clicking this link. You can also see recordings of previous briefings here.

The VTRAC team is also involved with providing incident response plans for Verizon's Rapid Response Retainer solution, which allows schools and universities to stay ahead of cyberrisks, secure data and systems, contain threats and quickly recover from breaches.

Verizon's Data Breach Investigations Reports (DBIR) can also help you stay cyberaware. You can download the reports online. There is also an education snapshot of the DBIR.

To learn how Verizon can help protect learning institutions, visit Verizon's security and protection site. Verizon offers solutions for

- Cyberrisk Management
- Endpoint Security
- Identity & Access Management (IAM)
- Incident Response & Forensics
- Managed Detection and Response Services
- Network & Cloud Security
- Web Security

You can also click here to find out about other ways Verizon is innovating education.

Referenced links

CISA Ransomware in Education Advisory:
https://www.cisa.gov/protecting-our-future-partnering-safeguard-k-12-organizations-cybersecurity-threats

CISA K-12 Cybersecurity Toolkit:
https://www.cisa.gov/partnering-safeguard-k-12-toolkit

U.S. General Accountability Office recommendations for cybersecurity in education:
https://www.gao.gov/products/gao-23-105480

Register for monthly VTRAC threat briefings:
https://www.brighttalk.com/channel/15099/

See recordings of previous VTRAC threat briefings:
https://www.verizon.com/business/resources/reports/verizon-threat-research-advisory-center/.

Verizon's Data Breach Investigations Reports (DBIR):
https://www.verizon.com/business/resources/reports/dbir/

DBIR Education Snapshot:
https://www.verizon.com/business/resources/reports/dbir/2022/data-breaches-in-education/

Verizon security and protection solutions:
https://www.verizon.com/business/products/security/

Verizon education solutions:
https://www.verizon.com/business/solutions/public-sector/education/

About the VTRAC team

The Verizon Threat Advisory Center (VTRAC) brings together experts from the military, law enforcement, and IT backgrounds who are well-versed in criminal and civil investigative requirements. They are also payment card industry-approved Qualified Forensics Investigators (QFI) and Qualified Incident Response Assessors (QIRA). The team leverages its expertise in investigations, forensics and discovery to help companies create effective incident response plans. They specialize in analysis of risk to information, especially threats and vulnerabilities. VTRAC members are located throughout the Americas, Asia-Pacific, and Europe/Middle East.

About Verizon

Verizon is an education partner committed to helping build secure, connected campuses. We have more than 25 years of industry experience, nine security operations centers, six forensics labs and one of the largest IP networks in the world. A recognized leader in managed security services, we monitor billions of security events (on average) each year to improve our threat library and inform our teams. Our world-class team of security experts is always ready to help you meet your security challenges. Verizon can help you strengthen, secure and modernize your network infrastructure to mitigate and respond to threats. Our security solutions and experienced consultants can help you combat today’s most destructive cybersecurity threats. We can help you with your institution’s security transformation journey, bringing the network, innovative solutions, and expertise in security and higher education to keep your university securely connected.

[1] https://www.techtarget.com/searchsecurity/news/365530004/Ransomware-attacks-on-public-sector-persist-in-January

[2] https://arktimes.com/arkansas-blog/2022/12/06/little-rock-school-district-to-pay-250000-ransom-to-computer-hackers

[3] https://www.fenews.co.uk/fe-voices/how-to-combat-ransomware-threats-in-the-education-sector/#:~:text=According%20to%20a%20report%2C%20ransomware,to%20prevent%20future%20security%20incidents.

[4] https://abcnews.go.com/US/baltimore-schools-failed-fully-act-security-recommendations-cyber/story?id=96671802

[5] https://www.cisa.gov/protecting-our-future-partnering-safeguard-k-12-organizations-cybersecurity-threats

[6] https://www.verizon.com/business/resources/reports/dbir/

[7] https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/

[8] https://www.cnbc.com/2022/10/05/colleges-struggle-with-enrollment-declines-underfunding-post-covid.html

[9] https://www.washingtonpost.com/education/2020/10/07/how-covid-19-has-affected-school-budgets-so-far-what-lies-ahead-without-more-federal-aid/

[10] https://www.npr.org/2020/05/26/858257200/the-pandemic-is-driving-americas-schools-toward-a-financial-meltdown

[11] https://www.cybersecurityconnect.com.au/critical-infrastructure/8698-us-schools-falling-victim-to-an-increasing-amount-of-ransomware-attacks

[12] https://www.scmagazine.com/brief/ransomware/report-baltimore-school-system-lacked-defenses-prior-to-2020-cyberattack

[13] https://assets.sophos.com/X24WTUEQ/at/pgvqxjrfq4kf7njrncc7b9jp/sophos-state-of-ransomware-education-2022-wp.pdf

[14] https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/?sh=4458f31f18a8

[15] https://www.infosecurity-magazine.com/news/teen-crashes-florida-school/