Held Hostage

Ransomware in higher education

verizon

An evolving threat to higher education

In the first quarter of 2023, Verizon published a white paper titled "Paying the price: the growing threat of ransomware in education." We viewed it as a critical warning about the rapidly-escalating threats to all of education that we saw in the monthly readouts provided by the Verizon Threat Research Advisory Center (VTRAC) in late 2022 and early 2023. The paper also coincided with national alerts from the FBI and the U.S. Cybersecurity & Infrastructure Security Agency (CISA) in early 2023 on the dangers of ransomware to schools.[1]

2,000

Approximate number of schools affected by ransomware in 2022.

— **VTRAC**

According to VTRAC consultants, the number of schools hit by ransomware nearly doubled between 2021 and 2022. While public, private, K-12 and higher education continue to be major ransomware targets, colleges and universities are already leading victims this year,[2] with a list that includes about a dozen colleges and universities in just the first quarter of 2023.

And it could be much more than a dozen since many institutions are private or not part of the public sector, there is a "cone of silence" around many of their data breaches. The schools that don't have a duty to disclose often won't.[3]

The financial costs associated with ransomware in higher education are staggering; since 2018, hackers have demanded nearly $60 million in ransom payments from colleges and universities, with an average of $239,733, and reported amounts ranging from $5,000 to $40 million.[4] But that average is quickly reaching seven figures. The ransom demand for Monroe College, for example, was $2 million.[5] And in addition to the ransom itself, like the $1.1 million paid by the University of California San Francisco (UCSF),[6] resulting system upgrade requirements and other associated costs are usually incurred. When UCSF agreed to pay its ransom, officials publicly said that one of the reasons they agreed to pay was that they'd estimated it would cost them at least $10 million to rebuild their systems if they didn't pay.[7]

64%

of colleges and universities worldwide report being hit by ransomware

— **2022 Sophos Global Survey**

Butler County Community College (in Pennsylvania) didn't pay ransom when they were attacked, and they were forced to cancel classes for a week. The school had to rebuild every single computer owned by the school, remove remote access for students, and restore untold amounts of data to its computer servers – a costly en-

deavor.[8] There is also a financial hardship due to reputational damage associated with not paying. When the University of Colorado refused to pay a $17 million ransom, student grades, social security numbers, medical records, disability statuses, and other sensitive information was publicly posted, along with financial data about the university. Subsequent enrollment for the school was believed to be adversely impacted due to the breach.[9]

Lincoln College in Illinois suffered a ransomware attack in 2022, and even though it paid the ransom, the school couldn't survive the financial setback – coupled with declining enrollment following the COVID-19 pandemic, the 157-year-old school was forced to close.[10]

Whether ransoms are paid or not, the downtime associated with the breaches also comes with a high price. In 2022 alone, ransomware attacks cost educational institutions about $4 billion just for the related stoppages – whether or not they paid.[11] The total average bill for recovering from a ransomware attack in education is $2.73 million – higher than any other industry.[12]

And there's a disturbing new trend associated with ransomware in higher education – targeting students, faculty, or parents directly. Knox College students in Illinois, for example, received a disturbing (and stilted) email letting them know their college networks had been hacked and all of their data was "put for sale" unless the students themselves paid to retrieve their personal data, which included social security numbers and medical records.[13] On top of the financial hardships, a data breach can be a public relations nightmare.

The problem is simply too big to ignore – higher education, whether public or private, small community colleges or large universities, need to protect themselves from this ever-growing threat.

It takes an average of

$2 million

to recover from a ransomware attack, in addition to any ransom that was paid.

— **Sophos 2022 State of Ransomware Study**

Contents

Executive summary

Faculty and staff in higher education are likely already very aware that their colleges and universities are 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, professor, support staff member as well as every 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 against colleges and universities. In this paper, we'll look at why ransomware is the preferred method of hackers looking to steal from higher educational institutions. We'll also explore how ransomware has evolved from slapdash 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 the online dangers we face, we can all formulate smarter business strategies for greater insights and awareness of today's rapidly-evolving security threats.

1,600

estimated days of downtime and

10,987

estimated days of recovery for schools experiencing ransomware attacks.

— **Comparitech**

The Goal

Understand the threat

Avoid risky behavior

Learn about helpful tools

Find out how to stay vigilant

A brief history of ransomware

Ransomware is a type of malicious software, or malware, designed to block access to computer systems or files until a ransom is paid. The history of ransomware dates back to the late 1980s, when a group of hackers called the AIDS Trojan Gang developed a virus that encrypted files on victims' computers and demanded payment to restore access. Initially, floppy disks were used and mailed out with the idea that curious recipients would just insert the disks into their hard drives to see what was on them, unwittingly installing the malware. The earliest ransomware demands were reportedly around $200.

When email became the norm, phishing emails came into vogue. A phishing email (or just “phish”) 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 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 another 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.

“In the beginning, [hackers] used to just hit you with ransomware and ask for money. Now they go into systems and assign themselves privileges and find all your interesting data before they ever attack.”

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

The first known widespread ransomware attack occurred in 2005 with the "GPCode" virus. This malware spread through email attachments and encrypted files on victims' computers, demanding a payment of $300 to decrypt them. The GPCode virus was difficult to crack, and many victims were forced to pay a ransom to regain access to their files.

In 2012, a new strain of ransomware called "Reveton" appeared, which was designed to trick victims into thinking they had committed a crime and were being fined by law enforcement agencies. The Reveton malware would display a message claiming to be from a government agency like the FBI or Interpol, accusing the victim of illegal activity such as downloading pirated software or visiting illegal websites. The message would demand payment of a fine, usually around $200, to avoid prosecution. This tactic was highly effective and allowed the Reveton malware to infect millions of computers worldwide.

In 2013, a new type of ransomware called "CryptoLocker" emerged, which used advanced encryption techniques to lock victims' files and demanded payment in exchange for the decryption key. The CryptoLocker malware spread rapidly through email attachments and infected more than 500,000 computers in just a few months. CryptoLocker was unique in that it actually did provide victims with a decryption key once they paid the ransom, which led many victims to pay the ransom to regain access to their files.

In recent years, ransomware has become increasingly sophisticated and difficult to detect. In 2017, the "WannaCry" ransomware attack infected hundreds of thousands of computers in over 150 countries, using a vulnerability in Microsoft Windows to spread rapidly across networks. The WannaCry malware demanded payment in Bitcoin and caused widespread disruption to hospitals, banks and government agencies.

In 2019, the "Ryuk" ransomware attack caused significant damage to companies worldwide, including a major U.S. newspaper and a large multinational technology company. The Ryuk malware is believed to have been developed by a sophisticated cybercriminal organization and is designed to target high-value targets for maximum profit.

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

— **2022 Verizon DBIR**

$2.73 million

Average cost for recovering from a ransomware attack in education – higher than any other industry.

— **Higher Ed Dive**

Today, ransomware is a highly-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.[14] Ransomware attackers have developed into vast underworld enterprises, nation/states have adopted the tactics, 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 sloppy, copy/pasted business logos. Modern phishing emails look much more professional and legitimate (and enticing).

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. The various 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 educational institutions to take on. But there are ways for schools to protect themselves.

44%

The increase in ransomware attacks on higher education from 2021 to 2022.

— **2022 Sophos Global Survey**

Targeting higher 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.[15] So why are hackers targeting educational institutions? When we think of well-funded organizations, colleges and universities aren't usually the ones that leap to mind. In fact, many colleges and universities seem to be struggling financially, especially in the wake of the COVID-19 pandemic and the associated lockdowns.[16,17,18]

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 is demanded, these online 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
- Financial health
- IT systems
- Data organization
- IT staffing

Bad actors often know from the outset how much money schools have on hand before they even make their demands, 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 targeted institutions will always have coffers to go to when embattled, especially when minors are involved.

Unfortunately, there is a perception that education is an easy target. Colleges and universities 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 state-supported university or private college is expected to have a leaner, less-skilled staff that a threat actor can exploit. Along with the staff shortcomings, higher education may have legacy data systems or lack the digital maturity which can also make them more susceptible to cyberthreats.

$ 136%

Increase in the average ransom demand in the U.S. from 2021 to 2022 – from $375,311 to $887,360.

— **Cybersecurity Connect**

Colleges and universities also have extensive repositories of sensitive data. They boast not only private information about students and faculty but the research data, academic papers and proprietary knowledge bases developed by reputable institutions. Scholarship information, medical records, prescription details, social security numbers, passport data – all of these files could be harmful if made public, and hackers know it.

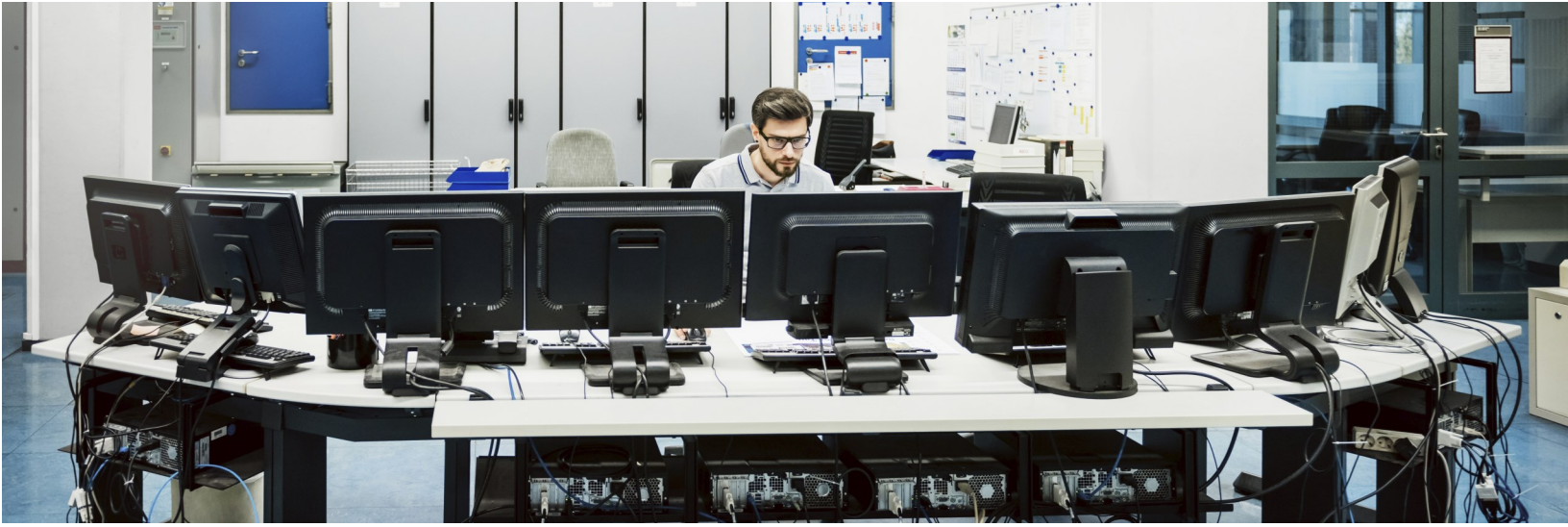
Schools also have the added element of public pressure; since many are publicly supported, they may have a duty to disclose when they're hacked. Add to that the newsworthy tactic of alerting students, faculty and parents of the attack directly, and it can lead to overwhelming public pressure to pay a ransom. There's also the chance that colleges or universities themselves will be held accountable in the court of public opinion.

Campuses are basically small cities, complete with banking institutions, restaurants, housing complexes, mail centers, delivery services – each representing hundreds of points of vulnerability and potentially millions of endpoints overall. And since the vast number – more than 80 percent – of data breaches are caused by human error,[19] each of those many endpoints is a point of weakness.

The multiple departments, halls, departments, and divisions make it very difficult to build consistency with their security across the university. The lack of continuity could create susceptibility.

"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 to higher education

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

DDoS

Distributed Denial of Service, or DDoS, is a common type of attack on all levels of education venues. The goal is to overwhelm a system with traffic and shut it down. Money made off of DDoS attacks usually involves blackmailing businesses to avoid the overflow or stop attacks in progress. Like ransomware as a service (RaaS), DDoS attacks can be purchased. DDoS attacks in education are typically used for disruption, often by students looking to avoid tests or classes or just cause mischief. In one reported case, a DDoS attack that crippled a university's network over four nights was only intended to target a group of residence halls. Eventually it was discovered the attacker was attempting to thwart his rivals in an online video game.[20] Sometimes DDoS attacks are used as means of protesting school policies or making political statements.

Phishing

As addressed previously, phishing is a scam involving an email or other message from a hacker that is disguised as a communication from a friend or reputable business. It's designed to get the recipient to click a malicious link or download a harmful attachment. While phishing can be used to launch ransomware, the social engineering emails are also an effective cyberattack on their 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.

$8 Trillion

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)**

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 or pranks 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, and usually involves a hacker that blackmails a victim over contents of stolen data, to avoid having the data publicized, or to retrieve the data itself.

To pay or not to pay

Some schools like UCSF, pay the ransom. Some, like Michigan State University, do not – even after hackers publicly posted screenshots of student passports, university financial transactions, and research projects related to physics and astronomy.[21]

Obviously, there is no easy answer about handling ransomware demands and there are a lot of factors that must be considered in these decisions: Insurance, legislative requirements, and the circumstances of each particular attack. No two schools have the same IT systems, so no two recoveries will be the same.

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. Reports indicate that paying the ransom only gets colleges and universities an average of 60 percent of their data back.[22] 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 entities 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. Faculty, staff, admins, coaches, students – anyone with a login should be taught to avoid phishing emails and bogus links. Human missteps are still far and away the main reason ransomware is so successful. Malicious links can come from emails, texts, and even phone calls, but they can be avoided. 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 on the phone
- Never click links in emails from someone they don't recognize
- Go to banking or delivery sites to verify information rather than clicking through emails

Other best practices to help prevent ransomware attacks include

- Regular IT awareness training for all faculty, staff and students.
- Keep all software and operating systems up to date and patched
- Regularly remove any unnecessary access to administrative systems
- Conduct regular penetration and vulnerability testing to objectively test security posture
- Create redundant, offline systems that are backed up frequently
- Use a host-based firewall
- Regularly back up data to a secure location that is not connected to the main network.
- Implement multi-factor authentication.
- Consider zero-trust policies
- Have an incident response plan ready in case of an attack. This plan should include steps to
    - ◊ Contain the attack
    - ◊ Recover any lost data
    - ◊ Communicate with stakeholders
- Consider cybersecurity insurance (but do your research on it – premiums, deductibles, and coverage can vary widely.)
- And yes, hire reputable cybersecurity consultants if possible.

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 Threat Research Advisory Center

The federal government is providing support and guidance. 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 2022 Infrastructure Investment and Jobs Act (IIJA) allocated $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.

There's a ransomware attack every 11 seconds,[23] but when colleges and universities work with partners like Verizon using guidance from the FBI and CISA, we can harden our school networks, root out bad actors and protect students, faculty and our institutions of higher learning.

Next steps: 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 advice for best practices to protect against ransomware and 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

As one of the largest network providers in the country and a leading communications partner for education, Verizon is committed to helping create secure, connected campuses. Click here to find out about other ways Verizon is innovating education.

Referenced links

CISA Ransomware in Education Advisory:
https://www.verizon.com/business/resources/articles/how-to-protect-against-ransomware/

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/

DBIR best practices to protect against ransomware attacks
https://www.verizon.com/business/resources/articles/how-to-protect-against-ransomware/

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 (AIRA). 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.cisa.gov/protecting-our-future-partnering-safeguard-k-12-organizations-cybersecurity-threats
2 https://www.blackfog.com/the-state-of-ransomware-in-2023/
3 https://www.csoonline.com/article/3690413/universities-and-colleges-cope-silently-with-ransomware-attacks.html
4 https://www.comparitech.com/blog/information-security/school-ransomware-attacks/#Methodology
5 https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack
6 https://www.fiercehealthcare.com/tech/ucsf-pays-hackers-1-14m-to-regain-access-to-medical-school-servers
7 https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/?sh=4458f31f18a8
8 https://www.bloomberg.com/news/newsletters/2022-05-04/lincoln-college-hack-leaves-students-at-home#:~:text=Take%20Butler%20County%20Community%20College,data%20to%20its%20computer%20servers.
9 https://www.cbsnews.com/colorado/news/colorado-cu-boulder-17-million-ransom-demand-accellion-data-breach/
10 https://www.itgovernanceusa.com/blog/lincoln-college-shuts-down-after-157-years-following-ransomware-attack
11 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.
12 https://www.highereddive.com/spons/inside-higher-educations-ransomware-crisis-how-colleges-and-universities/609688/
13 https://www.nbcnews.com/tech/security/ransomware-hackers-take-demands-directly-college-students-s-sad-day rcna61253
14 https://www.verizon.com/business/resources/reports/dbir/
15 https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/
16 https://www.cnbc.com/2022/10/05/colleges-struggle-with-enrollment-declines-underfunding-post-covid.html
17 https://www.washingtonpost.com/education/2020/10/07/how-covid-19-has-affected-school-budgets-so-far-what-lies-ahead-without-more-federal-aid/
18 https://www.npr.org/2020/05/26/858257200/the-pandemic-is-driving-americas-schools-toward-a-financial-meltdown
19 https://www.verizon.com/business/resources/reports/dbir/
20 https://www.zdnet.com/article/ddos-attacks-students-blamed-for-many-university-cyber-attacks/
21 https://www.freep.com/story/news/education/2020/06/03/michigan-state-hackers-ransom-breachrecords/3134361001/
22 https://universitybusiness.com/colleges-paying-ransom-only-get-60-of-data-back-heres-how-to-protect-it/
23 https://dataprot.net/statistics/ransomware-statistics/#:~:text=There%20will%20be%20ransomware%20attack,two%2Dthirds%20of%20ransomware%20infections.

verizon