White paper

Reading, writing and ransomware:

The evolving threat to education

verizon

Executive summary

Ransomware has transitioned from sporadic, newsworthy attacks to a professionalized, ongoing and pervasive threat to education. The financial and operational fallout from these attacks is staggering, far exceeding the cost of the ransom payment. As an industry uniquely vulnerable due to its reliance on public trust, mission-critical services, and sensitive student data, education has become a highly strategic target. This report, leveraging data from the Verizon 2025 Data Breach Investigations Report (DBIR) and other trusted sources, provides an updated view of the ransomware landscape, the specific tactics employed against schools and universities, and the proactive strategies required for effective mitigation.

Key findings include:

- The overall median ransom payment has decreased globally, but attackers are making significantly higher demands in education, demonstrating a calculated strategy to exploit the public pressure on schools to restore services.
- The primary initial access vector for ransomware has shifted from human-centric phishing to the exploitation of vulnerabilities in internet-facing devices, a tactic that has grown almost eight-fold in the past year.
- The third-party supply chain has become a major attack surface, with over half of all K-12 cyberattacks now originating from a third-party vendor.
- Traditional defenses like backups and multi-factor authentication (MFA) are no longer sufficient on their own, as attackers have developed sophisticated methods to bypass them.

This report will explore these trends in detail, offering a new framework for understanding and combating modern ransomware threats through a combination of technical controls, updated employee training, and robust incident response planning.

An evolving threat

The threat of ransomware has become an inescapable reality for today's educators, demanding a reassessment of cybersecurity strategies. It is no longer a matter of if an institution will be targeted, but when. These attacks, in which malicious malware blocks access to or steals sensitive data, have grown dramatically in both frequency and sophistication, leaving a trail of staggering financial and operational costs. The Verizon 2025 DBIR confirms this trend, revealing that ransomware was present in **44%** of all breaches reviewed, a notable **37%** increase from the previous year.[1] This data represents a significant escalation from the threat landscape described in early 2023, where high-profile attacks were already a monthly occurrence in states like Massachusetts, Iowa, and Arizona.[3]

This problem is particularly acute in education. In 2024, a survey of cybersecurity and IT leaders showed a significant portion of educational institutions were impacted by these attacks. Specifically, **63%** of lower education organizations and **66%** of higher education organizations were hit by ransomware.

The financial fallout of these attacks is complex and often contradictory. While the Verizon 2025 DBIR reports that the global median ransom payment declined to **$115,000** in 2024, down from the **$150,000** reported the previous year, this general trend does not apply to education.[1] Instead, external research reveals a starkly different reality, with a median ransom payment of **$6.6 million for lower education** and **$4.4 million for higher education**.[4] This significant disparity suggests that attackers have strategically identified education as a high-value target. Unlike private industry, which has become more resilient to ransom demands, educational institutions face immense public pressure to restore critical services, a factor that attackers have calculated into their demands. This public-facing role, where schools are "beholden to municipalities, communities and the students themselves," creates an environment where the pressure to pay is much higher.[4]

Beyond the ransom itself, recovery costs have soared, demonstrating that victims pay a heavy price even if they refuse to negotiate. Median recovery costs for K-12 education surged to **$3.76 million** and for higher education to **$4.02 million** in a single year, highlighting the massive financial burden of system rebuilding, investigations, and public relations.[5] This is exemplified by the 2020 Baltimore County Public Schools (BCPS) attack,

where the total recovery cost reached **$9.68 million**.[7] This updated analysis reveals a critical detail: despite having insurance, the district only received a $2 million payout because it had failed to comply with prior IT recommendations, reinforcing the fact that financial consequences are tied directly to an organization's proactive security posture.[3]

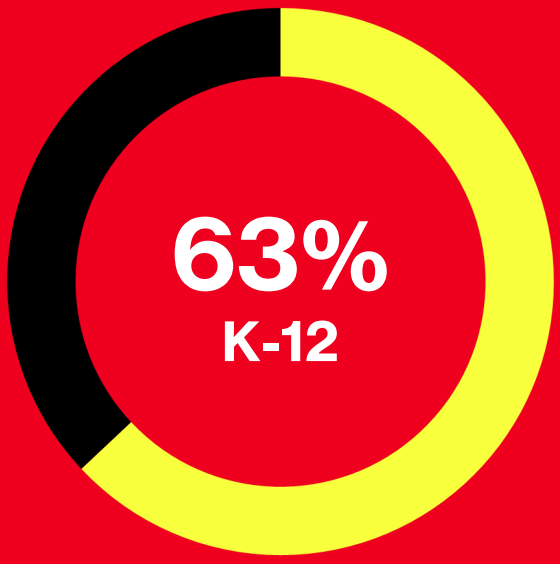
Recent high-profile attacks underscore the growing complexity of the threat. The Los Angeles Unified School District (LAUSD) successfully contained a subsequent attack after its 2021 breach, but this victory is an exception rather than the rule.[3] The most calamitous recent example involves a breach at education software provider PowerSchool, in which a hacker extorted the company and leaked the sensitive data of a staggering **62.4 million students and 10 million teachers**.[10] This case highlights the cascading threat of third-party risk, where an attack on one vendor can compromise data across countless educational institutions. Recognizing this evolving threat, federal agencies have shifted their guidance from broad warnings to a more targeted, intelligence-driven approach, releasing specific advisories on groups like the Medusa and Interlock ransomware groups, rather than the general alerts of the past.[12]

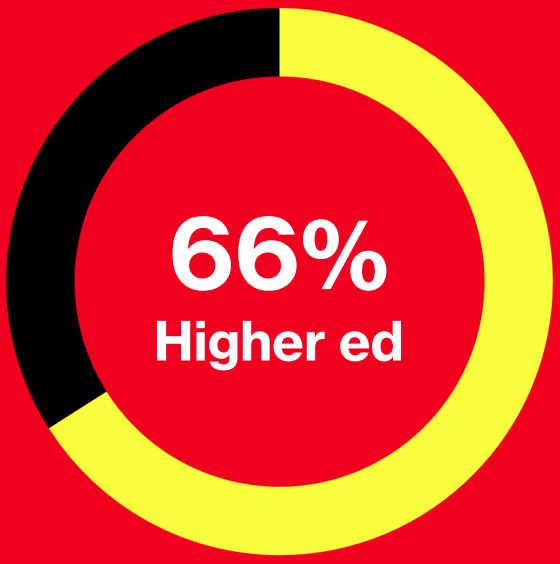
279%

The average cost to recover from an attack skyrocketed from $1.06M in 2023 to $4.02M in 2024.[1]

38%

Confirmed attacks fell 38% in 2024 compared to 2023, indicating a shift to more focused, high-impact targets rather than widespread campaigns.[1]





63% of K-12 schools and 66% of higher education organizations were hit by ransomware in 2024[1]

A brief history of ransomware

The narrative of ransomware has evolved dramatically from its rudimentary origins in the late 1980s. Initially spread via floppy disks, these early attacks were simplistic and limited in scope, with ransom demands rarely exceeding a few hundred dollars.[3] With the advent of the internet, phishing emails became the primary vector, where attackers would use social engineering to trick recipients into installing malware that encrypted their data. While initially crude, these phishing lures have undergone a significant transformation, becoming a sophisticated tool of modern cybercrime.[3]

Today, ransomware is a trillion-dollar organized crime industry, operating with a level of professionalism that mirrors legitimate businesses. This professionalization has given rise to the Ransomware-as-a-Service (RaaS) model, where technically limited individuals can purchase and deploy sophisticated ransomware kits on the dark web.[3] The resilience of this model was demonstrated by the international law enforcement takedown of the LockBit group in early 2024. While the operation temporarily disrupted LockBit's infrastructure, the group quickly re-emerged, and other prominent groups, such as Royal, have rebranded as BlackSuit to evade law enforcement scrutiny, demonstrating the adaptability of the RaaS ecosystem.[1]

In this new era, the human element, traditionally considered the weakest link, has become a more subtle and sophisticated vulnerability. The original guidance in the white paper about spotting phishing emails by looking for "spelling errors and cheesy, copy/pasted business logos" is now largely obsolete.[3] The Verizon 2025 DBIR found that the presence of synthetically generated text in malicious emails has **doubled in the past two years**.[1] This means that modern phishing emails are often perfectly crafted, contextually accurate, and designed to bypass traditional detection methods. This new reality requires a fundamental shift in a school's security awareness training. The focus must move from simply teaching users to spot a suspicious email to empowering them to verify every request that involves sensitive data, financial transfers, or password changes, regardless of how legitimate the request may appear.

The complexity of modern ransomware attacks extends to how initial access is gained. Attackers rarely conduct a full, end-to-end breach on their own. Instead, a robust ecosystem of specialized cybercriminals has emerged. Initial access brokers, for instance, specialize in gaining a foothold in an organization's network and then selling that access to the highest bidder on dark web marketplaces. The primary method for gaining this initial access is often through infostealer malware, which vacuums up stored passwords, cookies, and other valuable data from compromised devices.[2] This multi-stage, collaborative approach to cybercrime demonstrates that ransomware is not a solitary act but a highly strategic and interconnected enterprise.

Education as a target: the strategic attacker

Education has long been a target for cybercriminals, but the motivations and tactics behind these attacks have become more nuanced and calculated over time. Attackers have learned to exploit the unique vulnerabilities of schools and universities, from their mission-critical services to their financial constraints.

The fundamental reason education is a prime target is rooted in its public nature and the immense pressure to maintain continuity. Research shows that schools are "beholden to municipalities, communities and the students themselves".[4] This creates an environment where an attack that disrupts payroll, student records, or online classes can lead to widespread public outcry, a fact attackers leverage to pressure institutions into paying a ransom.[3] The sheer volume of irreplaceable, sensitive data held by schools, including student and staff personally identifiable information (PII), medical records, and financial aid data, makes them a veritable gold mine for identity theft and extortion.[10] Compounding this are the perennial challenges of limited IT budgets and a skeletal IT staff, a vulnerability that attackers are adept at exploiting.[3]

A significant development in the modern threat landscape is a strategic shift in the preferred methods of attack against education. While the historical data has correctly identified phishing as a primary entry point, new research suggests a change in adversary tactics. **Exploited vulnerabilities** are now the leading root cause of ransomware attacks in education, providing an initial foothold for **44%** of lower education and **42%** of higher education attacks.[4] This trend is corroborated by the Verizon 2025 DBIR, which found a **34%** increase in vulnerability exploitation as a general initial access vector.[1]

The most dangerous aspect of this shift is the specific type of vulnerability being targeted. The Verizon 2025 DBIR reports an almost **eight-fold increase** in attacks targeting internet-facing edge devices and Virtual Private Network (VPN) appliances, a tactic that allows attackers to bypass a network's perimeter without interacting with a user.[6] This highlights a dangerous parallel reality: while the human element remains a consistent risk, attackers are now actively and successfully targeting unpatched perimeter devices for faster, automated access. A security strategy focused solely on user training is therefore no longer sufficient; it must now equally prioritize the rapid patching of all internet-facing assets.

This strategic shift extends to the exploitation of the educational supply chain. With the rapid adoption of EdTech, a school's digital perimeter is no longer just its own network, but the collective security posture of its hundreds or thousands of integrated applications and vendors. The K12 SIX organization reports that a staggering **55%** of all cyberattacks on K-12 schools now originate from a third-party vendor, a threat that was tragically demonstrated by the PowerSchool breach affecting millions of students and teachers.[10] A robust security program must now be centered on rigorous vendor vetting, ongoing risk assessments, and a clear understanding of the security controls in place across all third-party integrations.

Other threats to education

A modern cybersecurity strategy for educational institutions must extend beyond the well-known threats of ransomware and phishing to address a new wave of subtle yet highly effective attack vectors. These threats often represent foundational steps in a larger attack chain, targeting the convergence of personal and professional data that has become a hallmark of the modern digital landscape.

One of the most insidious threats is the proliferation of **infostealer malware**. This type of malware is designed to steal valuable data, such as stored passwords, browser cookies, and cryptocurrency wallet information, from compromised devices.[2] This data is then sold on dark web marketplaces, providing initial access for follow-on attacks, including ransomware.[2] The Verizon 2025 DBIR found a direct link between infostealers and ransomware, with **54% of ransomware victim domains** appearing in credential dumps.[2] This new reality is exacerbated by the prevalence of "bring your own device" (BYOD) policies. An analysis of infostealer logs revealed that **46% of compromised systems** with corporate logins were non-managed, personal devices.[2] This finding demonstrates that an employee's personal device, if not properly managed and secured, can become an unmonitored entry point for a devastating attack, blurring the traditional line between an individual's personal and professional digital life.

The rise of new attack vectors has also exposed vulnerabilities in what were once considered foundational security controls. Multi-factor authentication (MFA) is still a crucial defense,[3] however this control is no longer a silver bullet. Attackers have developed new MFA bypass techniques, such as **"Prompt bombing,"** where a user is spammed with authentication requests until, out of frustration, they accept one to make the alerts stop.[14] Another common technique is an **Adversary-in-the-Middle (AiTM)** attack, where a phishing site steals an MFA session token, providing the attacker with persistent access.[14] This requires educational institutions to re-evaluate their authentication strategies to include not just MFA, but also conditional access policies that scrutinize every login for signs of unusual behavior.

MFA bypass

MFA bypass tactics like prompt bombing are top techniques.

Phishing

4x

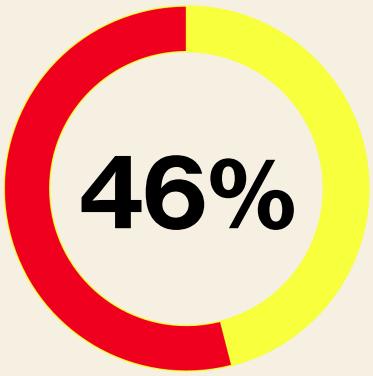
Training makes employees four times more likely to report phishing.

Finally, the increasing use of generative AI (GenAI) in the workplace has introduced a new and subtle threat: unintended data leakage. While GenAI tools offer efficiency, they also pose a significant risk to data confidentiality. The Verizon 2025 DBIR found that **15% of employees** routinely accessed GenAI systems on their corporate devices, often to summarize documents or assist with coding.[1] The more concerning finding is that a majority of these users were operating outside of company policy: **72% used personal email addresses** to log in, and another **17% used their corporate emails without integrated single sign-on (SSO)**.[1] This behavior creates a dangerous scenario where a user might paste sensitive student or staff data into a public-facing model, which could then be absorbed and potentially exposed to others. This new risk demands clear policies and training on how to use GenAI tools appropriately, alongside technical controls to prevent unintended data sharing.

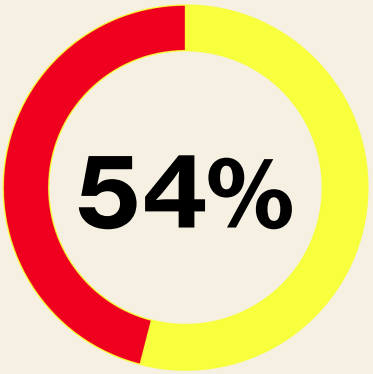
New threat classes

Recent and more subtle threats often go unmonitored. But data around abstract concepts like BYOD risk and GenAI leakage offers concrete, numerical justifications for new policies, training, and technical controls.

Infostealer malware



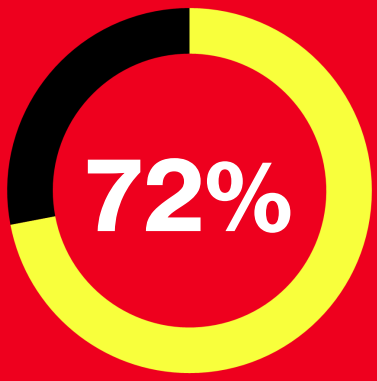
Corporate logins that come from non-managed, personal devices.[2]



Ransomware victim domains that appeared in infostealer credential dumps.[2]

GenAI data leakage

Employees that use GenAI on corporate devices.[1]



Users who log in to personal emails on corporate devices.[1]

To pay or not to pay: a nuanced calculus

The question of whether to pay a ransomware demand is one of the most difficult decisions an educational institution can face. There is no easy answer, and the calculus has become more complicated, moving beyond a simple cost-benefit analysis to include legal, financial, and operational considerations.

The notion that paying a ransom is a quick fix is a dangerous fallacy. While a district might be tempted to pay to restore services, the reality is that payment offers no guarantee. Since 2024, recovery efforts have become more protracted, with only **30%** of educational institutions fully recovering within a week of an attack, a decline from previous years.[4] This suggests that even when a ransom is paid, the process of restoring systems is not a simple matter of hitting a "restore" button.

Furthermore, a critical assumption that many school districts make is that having a backup is a sufficient defense. However, modern attackers have adapted their tactics to neutralize this key defense. A staggering **95% of attackers attempted to compromise their victims' backups**, and they were successful **71% of the time**.[4] This finding fundamentally changes the nature of the threat: it is no longer just an attack on an organization's production systems but a strategic assault on its ability to recover. As a result, the financial burden of a breach with compromised backups is massive, ballooning to **4-5 times higher** than if the backups had remained intact.[4] This underscores the critical need for isolated, offline, and segmented backups as the new standard for a viable disaster recovery strategy.

The legal landscape surrounding ransom payments has also grown more complicated, particularly for public institutions. While North Carolina and Florida had banned government entities from making ransom payments,[3] new analysis reveals a nuance in this legislation: while North Carolina's law is broad and applies to public schools and universities, Florida's law, as of early 2025, appears to exclude these educational entities from the ban.[17] Despite this distinction, the existence of such laws signals a growing trend at the state level to prohibit payments, creating a "difficult position" for public entities with poor backups and a high-pressure environment.[17] At the federal level, the U.S. Department of the Treasury's ban on payments to sanctioned hacker groups adds another layer of legal complexity, reinforcing the need for expert professional guidance in the event of an attack.[3]

Conclusion: defense tactics for today's threats

The modern ransomware threat requires a fundamental shift in defense strategy, moving from a reactive to a proactive and data-driven posture. The key to mitigating these attacks lies in understanding the evolved tactics of adversaries and deploying controls that address the full attack chain, from initial access to recovery.

Prioritize Vulnerability Management

The data clearly indicates that attackers have shifted their focus to exploiting internet -facing assets for initial access. The Verizon 2025 DBIR reports that the median time for a vulnerability to be mass exploited is just **zero days**, while the median time for an organization to patch it is a far longer **32 days**.[6] This critical mismatch highlights the ineffectiveness of a purely reactive patching strategy. Educational institutions must adopt a risk-based approach, prioritizing the patching of all perimeter devices and services that are exposed to the internet, such as VPNs, firewalls, and web applications, to close the most critical window of opportunity for attackers.

Empower the Human Firewall

While vulnerability exploitation is on the rise, the human element remains a consistent factor in breaches. However, the purpose of security awareness training must be re-evaluated. The Verizon 2025 DBIR found that training has a limited effect on preventing users from clicking on malicious links but a profound effect on a school's ability to respond. Employees who received phishing awareness training within the past 30 days were a staggering **4x more likely to report phishing attempts**, with a reporting rate of **21% vs. 5%** for their untrained counterparts.[1] This means that the goal of training is not just to prevent the initial click, but to turn every employee into an early warning system, allowing the institution to detect and contain a threat before it escalates.

Rethink Third-Party Risk

The K12 SIX organization found that a majority of K-12 school cyberattacks – a startling **55%** – originate from third-party vendors.[15] This statistic proves that a school's digital security is only as strong as its weakest vendor. Institutions must adopt a rigorous approach to vendor risk management, including a live inventory of all connected applications, standardized security-focused onboarding processes, and continuous monitoring to ensure vendor compliance.

Secure the Recovery Plan

Ransomware gangs are strategically targeting backups, with a **71%** success rate in compromising them, a statistic that renders traditional backup strategies obsolete.[4] A new standard for recovery must be established, centered on the principle of isolation. This means implementing and regularly testing redundant, offline, and segmented backups that cannot be reached or compromised by a threat actor who has gained a foothold in the primary production network.

Leverage Resources

The federal government has allocated significant resources to help local and state entities, including schools, bolster their defenses. Educational institutions, particularly those at the state and local levels, should actively pursue this funding by working with their state's Cybersecurity Planning Committee to submit a plan to CISA and FEMA.[19]

Next steps: educating the educators

Verizon remains a dedicated partner to the educational community, committed to helping schools and universities build secure, connected campuses. With more than 25 years of industry experience, a global network of security operations centers, and a world-class team of security experts, Verizon helps institutions strengthen their security posture and respond to threats effectively.[3]

To help educators stay current with the ever-evolving threat landscape, Verizon and the Verizon Threat Research Advisory Center (VTRAC) offer monthly threat briefings and a wealth of resources, regardless of customer status.[3] The annual Data Breach Investigations Report (DBIR) provides an invaluable, data-driven look at the current state of cybercrime, helping institutions make smarter, more informed decisions about their security strategies.[3] Verizon also offers a range of solutions tailored to education, including cyber-risk management, incident response and forensics, and managed detection and response services, all designed to help institutions navigate the security transformation journey and protect their data assets.[3]

Helpful links

Verizon's Data Breach Investigations Reports (DBIR) can also help you stay cyberaware. You can download it at https://www.verizon.com/business/resources/reports/dbir/

Register for VTRAC's monthly briefings by clicking this link. You can also see recordings of previous briefings here.

To learn how Verizon can help protect learning institutions, visit https://www.verizon.com/business/products/security/. 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

Find out other ways Verizon is innovating education by visiting verizon.com/education.

Appendices

Appendix A: About the VTRAC Team

The Verizon Threat Research Advisory Center (VTRAC) is composed of experts from military, law enforcement, and IT backgrounds. The team is well-versed in criminal and civil investigative requirements, holding certifications as Qualified Forensics Investigators (QFI) and Qualified Incident Response Assessors (QIRA).[3] VTRAC leverages its deep expertise in forensics, investigations, and discovery to help organizations create effective incident response plans and analyze their unique threat and vulnerability landscape. The VTRAC team is globally distributed, with members in the Americas, Asia-Pacific, and Europe/Middle East regions.[3]

Appendix B: About Verizon

Verizon is a leader in managed security services, monitoring billions of security events annually to refine its threat library and inform its teams.[3] With one of the world's largest IP networks, nine security operations centers, and six forensics labs, Verizon provides innovative security solutions and consulting services to help educational institutions strengthen their infrastructure, mitigate threats, and quickly recover from breaches. Verizon's expertise is focused on helping institutions protect their networks, endpoints, and data, ensuring a secure and connected learning environment.[3]

Works cited

1. 2025 Verizon Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
2. 2025 DBIR: Breaches, Ransomware, and Stolen Credentials — The Invisible Economy of Access - Prey Project https://preyproject.com/blog/verizon-dbir-data-breach-report
3. Most Educational Organizations Paid More Than the Original Ransom Demand, Says Sophos Survey https://www.sophos.com/en-us/press/press-releases/2024/09/most-educational-organizations-paid-more-original-ransom-demand-says
4. Sophos report highlights rising ransomware recovery costs in education sector https://www.edtechinnovationhub.com/news/sophos-rising-ransomware-recovery-costs
5. The Verizon 2025 Data Breach Investigations Report (DBIR): Six Trends You Can't Ignore https://blog.qualys.com/qualys-insights/2025/04/22/the-verizon-2025-data-breach-investigations-report-dbir-six-trends-you-cant-ignore
6. Baltimore County schools ignored warnings before 2020 cyberattack, audit finds https://statescoop.com/baltimore-county-schools-ransomware-attack-2020-inspector-general/
7. Maryland IG Finds Baltimore Schools Partially At Fault For Hack - Government Technology https://www.govtech.com/education/k-12/maryland-ig-finds-baltimore-schools-partially-at-fault-for-hack
8. Out of Crisis, Opportunity: LAUSD's Fight Back From the Ransomware Brink https://www.govtech.com/security/out-of-crisis-opportunity-lausds-fight-back-from-the-ransomware-brink
9. Ransomware attacks in education jump 23% year over year - Higher Ed Dive https://www.highereddive.com/news/ransomware-attacks-education-jump-23-percent-h1-2025/754011/
10. K12 Cybersecurity 2025: Protecting Schools from Cyber Threats - UDT https://udtonline.com/how-schools-can-strengthen-cybersecurity-in-2025/
11. Official Alerts & Statements https://www.cisa.gov/stopransomware/official-alerts-statements-cisa
12. Verizon 2025 DBIR Highlights: Third-Party Threats Double and System Intrusion Is 81% to Blame - Fortra https://www.fortra.com/blog/verizon-2025-dbir-highlights-third-party-threats-double-and-system-intrusion-81-blame
13. Breaking Down the 2025 Verizon Data Breach Investigations Report - SpyCloud https://spycloud.com/blog/verizon-2025-data-breach-report-insights/
14. Back to School, Not Back to Breaches: How K-12 Schools Can Secure Student Data in 2025 https://www.schoolday.com/back-to-school-not-back-to-breaches-how-k-12-schools-can-secure-student-data-in-2025/
15. #StopRansomware Guide | CISA https://www.cisa.gov/stopransomware/ransomware-guide
16. Ransomware: To Pay or Not to Pay? It Just Got More Complicated - McDermott Will & Emery https://www.mwe.com/insights/ransomware-to-pay-or-not-to-pay-it-just-got-more-complicated/
17. Florida prohibits state agencies from paying cyber ransoms https://www.floridabar.org/the-florida-bar-news/florida-prohibits-state-agencies-from-paying-cyber-ransoms/
18. State and Local Cybersecurity Grant Program Fact Sheet https://www.cisa.gov/resources-tools/resources/state-and-local-cybersecurity-grant-program-fact-sheet
19. CISA, FEMA announce over $100 million in FY2025 cybersecurity grants to help states, tribes, local governments boost defenses - Industrial Cyber https://industrialcyber.co/cisa/cisa-fema-announce-over-100-million-in-fy2025-cybersecurity-grants-to-help-states-tribes-local-governments-boost-defenses/