

# Anatomy of Education Cyberattacks: A Breakdown of Real Threats and How to Stop Them

## Introduction

Educational IT and cybersecurity professionals have their work cut out for them compared to threat actors. The latter only needs to exploit one vulnerability or compromise a single set of credentials to gain a foothold in school networks, while you, the defender, must get it right every. single. time.

In today's globally connected world, failure to do so increases the risk institutions face that non-compliant devices or phished credentials can open a door to a data breach – one with the potential to cause ripple effects across the entire infrastructure.



***"Knowledge is power."***

– Thomas Jefferson

The quote above rings true for both the good and bad guys alike. It arms the bad guys with insight into the failings of institutional defenses, allowing them to identify and target weak points; conversely, it allows the good guys to understand the nature of the cyberattacks used against them, granting them insight into their opponent's attack plans.

### In this paper, we:



- Break down the cyber kill chain
- Demonstrate how an EDU-focused attack worked
- Align key links with critical protections
- Underscore the criticality of closing security gaps

By holding each phase of the cyber kill chain up to a magnifying glass and carefully examining the anatomy of an attack, EDU support teams can shore up risks while fortifying protections through iterative feedback. **Before we get to the cyber kill chain, let's first identify the key reasons why threat actors target the education sector.**

## Why are schools an attractive target?

Education institutions are increasingly attractive targets for cybercriminals due to limited resources, outdated infrastructure and valuable data. *Schools around the world often struggle to maintain strong security postures* while balancing critical needs like staffing, student services and salaries. Combining financial strain, legacy hardware and software and a rich cache of student and teacher data, creates exploitable vulnerabilities that leave IT under-resourced and overburdened. In short, a domino effect of conditions makes school districts prime targets for threat actors.



### Limited resources

Doing more with less is more than just a saying in education – it's a way of life for all stakeholders, from students to teachers to administration. While the aim of this paper is to focus on threat prevention rather than on constrained budgets, the fact remains that tight budgets overshadow how school districts across the globe are able to maintain robust cybersecurity when those dollars must compete with critical services, like hiring adequate staff, providing student meals or offering competitive salaries.

Though school districts often try their best to earmark funds for specific use cases, unfortunately, limited financial resources sometimes leads to budgeting shortfalls that affect one budgeting structure more than another, requiring administrators to prioritize one critical function at the expense of another crucial one. Threat actors understand this which is a significant reason why their attacks are successful against schools. Some of the contributors to attack success are:

#### **Obsolete computers**

A computer's usable lifespan is generally considered to be 3-5 years. Beyond that, and lack of support for new security features and growing performance issues alongside compatibility problems will continue to minimize usability for students and teachers alike.

#### **Outdated software**

Like hardware, software requires updates to keep security vulnerabilities to a minimum. Though access to the latest code versions is less of a concern with subscription-based apps, the long-term costs may exceed that of perpetual licensing making it difficult to stay up to date year after year.

#### **Single platform dependency**

Solutions tailored to a specific platform are known to provide comprehensive support for the OS it's designed for. Conversely, "one size fits all" solutions often trade lower service costs for cherry picked support that may leave devices undermanaged and under protected.

#### **Overburdened IT personnel**

IT staffing ratios typically average about 100 employees for every 1 IT support person; however, **education typically sees ratios triple that**, at 1 to 300 or more. Understaffing and IT burnout are key factors that contribute to a weak security posture, which negatively impacts compliance in regulated industries like education.

#### **Non-competitive salary**

The average salary range for IT technicians (US) is \$45,000-71,000 with 1-3 years of experience. The range for IT technician roles with the same experience in EDU is \$42,000-63,000. Combined with understaffing concerns, a salary that's **9% less than market value** makes attracting and retaining top talent difficult, which further impacts the security of school networks.

#### **Lack of training prioritization**

Cited among the **top 3 requests from IT personnel** to their supervisors, is some form of structured training to learn new skills and expand their existing knowledgebase. Henry Ford summed up the costs relationship succinctly when he said, *"The only thing worse than training your employees and having them leave is not training them and having them stay."*

## Valuable data

Data in K-12 schools presents a high-value target for cybercriminals due to its sensitivity, longevity and limited resources to protect it. Personally identifiable information (PII) tied to students can be exploited for financial fraud, identity theft and social engineering, often going undetected for years. Combined with the legal, reputational and financial fallout that follows a breach, threat actors see school districts as vaults storing valuable digital treasure without the multi-layered security models that banks employ to keep out thieves.

### Ransom

Among the top reasons driving data theft, is the value it holds for institutions and stakeholders alike. Threat actors are keenly aware of this and use it as a carrot to extort money in exchange for not leaking sensitive data. How much money varies by incident, but the **average cost of a ransomware data breach** ranges from \$4.38-5.37 million. NOTE: *Range reflects incident containment and does not include the ransom payment.*

### Reputation

After an attack is made public, unfortunately, the damage doesn't end there. Inquiries are often made, damaging the institution or school district's public image. Actors understand this and factor this into their attacks, often revictimizing schools with double and triple extortion attempts — no doubt contributing to the **69% surge in global ransomware attacks targeting education** in Q1, 2025.

### Legal

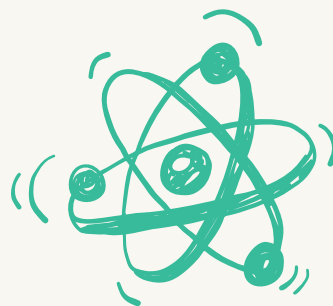
As a regulated industry and one highly reliant on government funding, data breaches must be reported and investigated. Because the burden rests with institutions for safeguarding sensitive student and staff data, unauthorized data exposure can lead to steep fines and loss of access to state, federal or regional funding in the future, stemming from regulatory violations. Additionally, **breaches may also bring civil and/or criminal liabilities** for individuals held responsible for not ensuring that required measures were taken.

### Identity theft

Student data provides threat actors with a boilerplate to build synthetic profiles used in a variety of criminal activities. The most common is financial, discussed in the next section, and the second is to target other individuals in a concerted effort to bully or track students or to obtain more information as their reach extends by **targeting additional victims through social engineering**.

### Financial

Particularly for those under legal age, who often have no established credit or financial history, the allure of student data lies in that **threat actors utilize this PII to engage in unauthorized financial transactions** "for many, many years before the victims learn about it." Furthermore, because of a lack of financial history, school-aged children typically do not have monitoring services in place to detect bank accounts, applications for loans or credit cards opened in their name often not discovered until adulthood.



## What is the cyber kill chain?

Attacks vary because the threats bad actors use are based on the targets selected and their vulnerabilities. Though attacks often share traits, their uniqueness and the variables affecting endpoint security make cybersecurity both an art and a science to decipher.

However, despite the variation of threats that make up an attack, one certainty is the anatomy of an attack or links in the cyber kill chain. Made up of seven phases — from initial preparation to execution — each stage in the kill chain offers cybersecurity teams an opportunity to identify weak points that attackers might exploit.

*"So those are my schemes,  
And these are my plans"  
– Tears for Fears*

Before learning how to read an attacker's roadmap, review the seven phases of the **cyber kill chain**:



### RECONNAISSANCE:

1.

Research and identify targets both online and offline.



### WEAPONIZATION:

2.

Use research gathered to develop and/or procure tools used in later stages.



### DELIVERY:

3.

Malicious tools are actively used against targets to gain access.



### EXPLOITATION:

4.

Once access has been obtained, vulnerabilities and other security gaps are leveraged to extend access further.



### INSTALLATION:

5.

Deployment of malicious code establishes a foundation for the campaign's success.



### COMMAND AND CONTROL:

6.

Communication with compromised devices is established ahead of the final phase of the attack.



### ACTIONS ON OBJECTIVES:

7.

With all preparation and foundational work completed, threat actors execute tools that achieve their goals (gather PII, exfiltrate data, execute ransomware, etc.)

## Model of a ransomware attack targeting EDU

In this section, we review the recent [ransomware attack targeting the Baltimore City Public School \(BCPS\) district](#). It is important to note that this attack is still under investigation by the FBI at the time of writing. As such, because details are limited to what's been publicly released, this example presents one possibility for how a similar attack may unfold in a real-world scenario.

1.

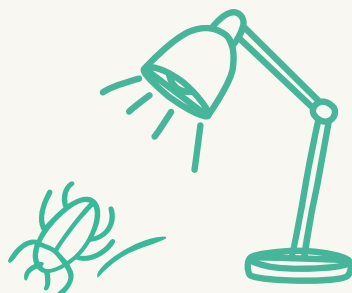
### Reconnaissance

During the intelligence-gathering phase, threat actors gather detailed information about an institution's infrastructure and network environment. This includes identifying vendors, service providers and key personnel through open-source research and social engineering. Reconnaissance can be passive or active, with the latter sometimes triggering alerts through suspicious activity such as an unusual increase in network traffic as the victim's network is scanned. The goal is to profile the target, identify vulnerabilities and improve the chances of a successful attack. Understanding these tactics can help IT leaders detect early warning signs and strengthen defenses.

2.

### Weaponization

Following reconnaissance, threat actors use the intelligence they've collected to tailor tools for the next stage of the attack. This often involves customizing or acquiring malware, including the frameworks and infrastructure that determine how the ransomware will operate. Many attackers now rely on Ransomware-as-a-Service (RaaS) providers, which offer these services as a turn-key business model that lowers the cost and technical barriers to launching attacks. This approach allows threat actors of any skill level to target institutions with advanced capabilities in exchange for a percentage of the extortion amount. Understanding this model can help IT teams anticipate and prepare for evolving threats.



3.

### Delivery

In the delivery phase, threat actors often rely on social engineering tactics like phishing to distribute malicious code across multiple endpoints with minimal effort. Channels such as email, SMS and social media increase the likelihood of success, especially when targeting individual users. Solutions like Jamf for K-12 help defend against these threats by blocking phishing URLs, monitoring device health and enforcing data separation through secure enrollment profiles. If a breach occurs, IT teams can automate data sanitization to protect sensitive school information. These tools support a proactive defense strategy for education environments.

4.

### Exploitation

In the exploitation phase, attackers use malicious code to exploit system vulnerabilities and elevate privileges or utilize phished credentials to gain access to a network, depending on earlier reconnaissance. Sophisticated malware variants are designed to evade detection by masking their processes through encryption. Jamf's solutions help mitigate these attacks by monitoring device health, triggering real-time remediation workflows and disabling compromised accounts. Furthermore, the seamless integration between management, identity and security helps by enabling multi-factor authentication (MFA) to secure credential usage and ensuring devices remain up to date with patches. This layered defense helps IT teams reduce risk and respond quickly to incidents across their environment.



5.

## Installation

In the installation phase, ransomware is deployed to compromised devices, laying the groundwork to carry out the portion of the attack that specifically targets student and teacher data, as well as disruption to various district IT systems. To defend against this phase, IT teams must maintain visibility and enforce compliance by detecting, preventing and remediating threats. Jamf helps by blocking known malware, quarantining harmful code and monitoring device health for security changes. For unknown threats, device logs can be forwarded to a SIEM, enabling deeper threat-hunting and faster incident response in school environments.

6.

## Command and Control

In the command-and-control phase, compromised devices begin communicating with an attacker's server to retrieve file targets and encryption keys, enabling data theft and extortion. Compromised devices are scanned to identify high-value files such as Word, Excel, PDFs and databases, with additional tools sometimes downloaded to support the attacker's future objectives. The goal is to maximize access across school networks. Preventing this communication is critical. Integrated identity and security tools can disable compromised credentials, block access to malicious servers and trigger automated remediation workflows when devices fall out of compliance, helping IT teams defend school environments while limiting the attack's success.

7.

## Actions on Objectives

In the final phase of the cyber kill chain, attackers execute their endgame, which may include data exfiltration, extortion, lateral movement and/or DDoS attacks. Ransomware typically encrypts files, deletes originals and leaves behind ransom demands, with more severe cases involving threats to leak or further exploit stolen data for additional ransom. Each attack is tailored to the threat actor's objectives, making outcomes unpredictable and potentially devastating for educational institutions. Holistic integration of management, identity and security tools can block malicious traffic, prevent data exfiltration and disable compromised credentials. Automated remediation workflows and real-time telemetry ensure only compliant devices have access to district resources, supporting a defense-in-depth strategy.






## Repair cracks in your armor

Security gaps caused by inadequate protections and an overreliance on desktop operating systems leave mobile devices exposed, allowing threat actors to compromise networks.


While mobile devices aren't the only risks behind data breaches, but they remain top targets due to wider workplace adoption and increased use of personal devices to access data. [Jamf Threat Labs research](#) quantifies this risk with *"40% of mobile users running a device with known vulnerabilities."* On vulnerable devices, unchecked risk factors allow threat actors to:

 **Run malicious code on devices**


 **Spy on users without their knowledge or consent**

 **Bypass internal security protections**

 **Pivot attacks from the infected device to compromise networks**

 **Gain access to unauthorized business data**

 **Exfiltrate personal and business data alongside private information**

 **Obtain privacy data without authorization**



Apple is known for blending form and function, style alongside substance. This philosophy extends to a hallmark of their design that is growing in criticality: security and privacy. Several protections are natively included in macOS and iOS-based operating systems to secure devices, users and their data against myriad threats – both at the hardware and software levels.

Threat actors are evolving their attacks with novel threats and emerging malware variants, like the growing Infostealers category. Security based on static signature detection engines alone is challenged to defend against sophisticated threats. Some, like the ransomware that impacted BCPS, show signs of [working with multiple threat actor groups to obtain initial access](#) before having carried out their campaign. Because of its dynamic nature, sophisticated threats may evade protections built into operating systems (regardless of platform), putting devices, stakeholders and data like the [25,000 affected in the BCPS attack](#) at risk of data breaches.

Security plans based on a mature, [defense-in-depth framework](#) are the best chance organizations have to mitigate on-device risk and [protect against web-based threats](#), prevent known attacks and quickly respond to incidents with automated remediation workflows to maintain endpoint compliance.

Through integrating and layering solutions, organizations defend against sophisticated threats with comprehensive protections to catch and mitigate risk through multiple, fail-safe layers. At the same time, these layers of protection extend across the enterprise, providing a baseline of defense for all device and OS types that request access to company resources and data.

According to a recent [Frost Radar: Endpoint Security, 2023 report](#) on Jamf solutions, Frost & Sullivan noted Jamf as a leader in endpoint security because of the defense-in-depth capabilities of our solutions:



**Real-time detection of malicious applications and scripts with recommended user actions**



**Expanded configuration and auditing framework to help customers meet compliance requirements**



**Consistent vulnerability management, threat prevention and policy control**



**Rich endpoint telemetry exported to third-party log collection and analytics tools**



**Security reporting across Mac and mobile platforms including macOS, iOS/iPadOS and Android; web threat protection also extends to Windows and Chromebooks**



**Consistent policy enforcement for both company-issued and personal devices**

## Conclusion

The cyber kill chain gives IT teams a structured lens to anticipate how ransomware attacks unfold, from reconnaissance through data exfiltration and extortion.

As illustrated through the real-world Baltimore City Public Schools incident, each phase exposes how cracks in the armor lead to vulnerabilities that will be exploited if left unaddressed. With limited budgets, aging infrastructure and overburdened IT teams, school districts face significant challenges in defending against sophisticated threats.

Jamf for K-12 supports a defense-in-depth strategy by integrating device management, identity and access, and endpoint security that comprehensively protects EDU's most valuable resources: students, teachers and district data. Our approach empowers support teams to detect, prevent and remediate threats across all Apple and multi-platform environments with parity. Through real-time telemetry, automated workflows and secure access controls, districts can close critical security gaps and enforce compliance. In today's threat landscape, layered protections are no longer optional – it is essential to safeguarding the future of education.

**Ready to see how defense-in-depth works in your environment?**

