The growing ransomware threat to school districts

A look at the recent trends

Ransomware trends article

Ransomware—in which cyberattackers encrypt or lock down a victim's files or networks and demand a ransom to restore access—is a growing problem for public schools.

Cyberattackers hit dozens of school districts last year—from the Pacific Northwest to the Florida Panhandle—disrupting operations and causing financial losses.

Some school districts were forced to temporarily close when cyberattackers locked them out of their data. Others paid tens of thousands of dollars to get access to their files.

62

Sixty-two reported ransomware incidents in K–12 institutions in 2019[2]

A growing threat—but hard to quantify

Ransomware was responsible for 80% of malware-related incidents in the overall education sector in 2019, according to the *2020 Verizon Data Breach Investigations Report.* That's up from 48% the previous year.[1]

The K–12 Cybersecurity Resource Center reported 62 ransomware incidents at K–12 institutions in 2019—a huge jump from 11 in 2018.[2] And the center notes that those numbers are almost certainly low.

Ransomware is notoriously underreported in all sectors. "The estimate is less than 10% is getting reported," said Matthew O'Neill, Assistant Special Agent in Charge with the U.S. Secret Service, which investigates financial and electronic crimes.[3] Reporting is low because many organizations prefer to deal with the problem quietly.

We may learn about a larger percentage of cases involving public school districts because their boards have to meet publicly, and their challenges are often aired by the news media. Still, some K–12 cases likely go unreported.

Each of the 62 known attacks on school districts represents multiple individual schools. That means hundreds of schools and tens of thousands of students, teachers and other school employees were potentially affected.

The problem has become alarming enough that in July 2019, the U.S. Department of Homeland Security's cybersecurity unit warned state and local governments that they should beef up their defenses against ransomware.

Why target school districts?

Anyone can potentially be a victim of ransomware, from individuals on home computers to hospitals to big businesses. Lately, cyberattackers have also been targeting school districts. Why target schools when much richer payoffs might be had by taking on, say, banks?

One reason is that school districts often don't have the sophisticated defenses and resources of a bank. Schools often have older IT systems that are more susceptible to intrusion. They have limited time for training, leaving employees more vulnerable to phishing scams directed at email accounts. And they have hundreds of children using computers.

"They have limited budgets for computer security. It's not something they think of before the fact," said O'Neill.

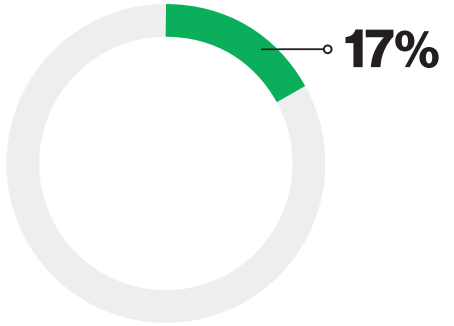
They also have lots of valuable data—for instance, personally identifying information on students, families and staff that could be used to steal identities.

"That's a prime target for any cyberattacker," O'Neill said.

When they are attacked, schools usually have limited options for data recovery, leaving them more likely to succumb to a ransom demand. And they have a pressing need to remain open, as well as political pressure to respond quickly to fix the problem.

"They just want to be up and running," the agent said.

The surge in distance learning in schools—with students and teachers sometimes using their own devices and connecting to school resources through home routers—has only increased districts' vulnerability.



In publicly reported attacks in recent years on state and local governments, only about 17% paid the ransom.[4]

Who is behind the attacks?

Ransomware attackers can be lone wolves, but most of those who are targeting school districts or other large organizations are part of organized crime groups, O'Neill said.

By studying tactics, techniques and procedures used in an attack, investigators can often get a general idea of the type of group behind it. That doesn't mean they can stop them, though.

Because attackers typically demand payment in untraceable cryptocurrency, such as Bitcoin, it's difficult to establish attribution. Threat actors often live in countries beyond the reach of U.S. law enforcement, and they are continually evolving their techniques to try to stay one step ahead of law enforcement and cybersecurity experts.

How do they break in?

The main way cyberattackers get into networks is through phishing—using email to trick an employee into clicking on an attachment or link, which allows malware to be downloaded onto the network. Malicious PDFs can also be a source of malware.

Another avenue is Remote Desktop Protocol servers, which cyberattackers can break into through a brute-force attack or by buying credentials on the dark web. Attackers also take advantage of unpatched vulnerabilities in widely used applications such as Adobe® Flash,® Acrobat Reader® or JavaScript.®

To pay or not to pay

When school districts are hit by ransomware, they must decide whether to pay the ransom or not. Paying can cost tens of thousands of dollars or more. Not paying typically equates to doing without the affected data. Law enforcement professionals generally urge them not to pay because that rewards criminals and increases the likelihood of future attacks.

Because reporting on ransomware is so spotty, it's not clear how frequently ransom is paid. A report by cybersecurity company Recorded Future said that in publicly reported attacks in recent years on state and local governments, only about 17% paid the ransom.[4]

Some victims do opt to pay, though, because the costs of recovery without a decryption key can greatly exceed the cost of the ransom. Also, they want to get back to business quickly. Many have purchased cybersecurity insurance, which helps cushion the costs.

The percentage of organizations worldwide purchasing cybersecurity insurance grew from 35% in 2011 to 75% in 2018.[5]

But do cyberattackers hold up their end of the bargain if you pay ransom? Surprisingly, yes.

The cyberattackers run their organization as a business. "It's almost like the bad actors want to provide this customer service of decrypting the data," O'Neill said. "They don't want the reputation of having people pay the ransom and not getting their data back." This is done to encourage other victims to pay the ransom.

That doesn't take care of the problem, though.

They don't pay up 100% of the time, and even when when they do, flaws in the encryption process can mean some data is lost.

Even if decryption is successful, districts will have more work to do.

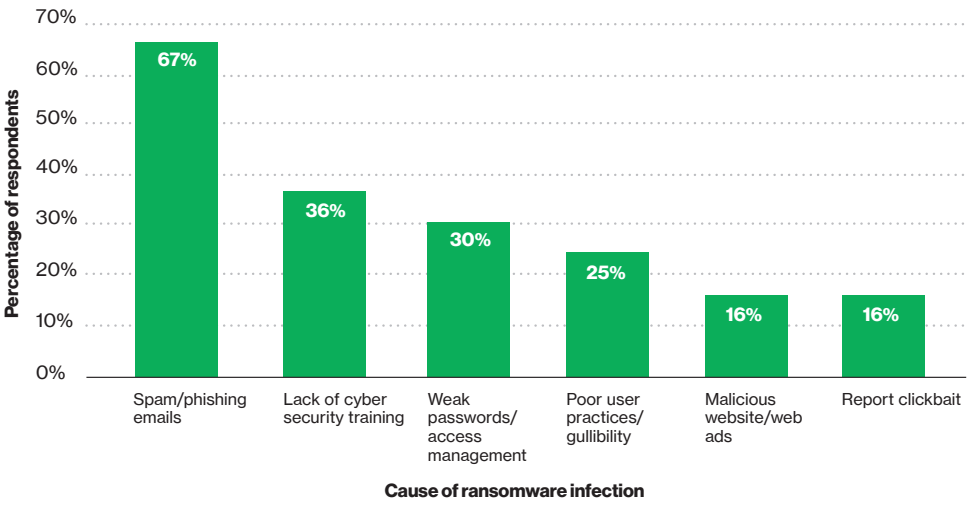
They will need to rebuild servers, update computers and devices, and make certain the bad actors haven't left a "back door" that allows attackers to come back in for a repeat visit. And they should assume the criminals made copies of their data.

"These cyberattackers ... could have exfiltrated the data they've encrypted. So the decryption of a victim's system doesn't necessarily mitigate a possible data breach or the future monetization of the stolen data," said O'Neill.

In fact, cyberattackers sometimes try to force the hand of victims who refuse to pay by threatening to publish their stolen data—which means that all sorts of sensitive data about students, teachers and other school personnel could wind up on the dark web.

Key insight: Decryption doesn't mean a district's problems are over. Cybercriminals sometimes make copies of a district's data or leave a "back door" open so they can re-enter.

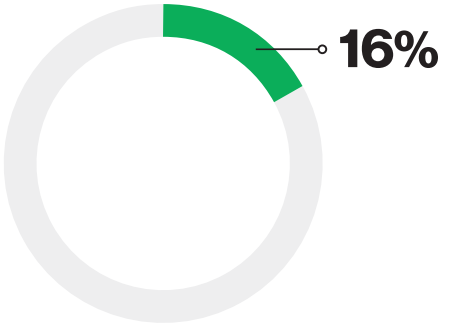
Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2019



Source: Datto, State of the Channel Ransomware Report 2019, page 9,via Statista.

A history of ransomware

- **1989:** The first "ransomware" attack occurs when a biologist sends diskettes supposedly containing information about AIDS to attendees at a World Health Organization AIDS conference; the diskettes in fact contain a Trojan that encrypts file names on the recipients' computers
- **2006:** The Archiveus Trojan, which encrypts the files of the My Documents directory, is launched; victims must make purchases from certain websites to regain access
- **2008:** Bitcoin gives cyberattackers a powerful new tool, as they can demand ransom using hard-to-trace digital currency
- **2012:** A Trojan called Reveton is introduced, eventually hitting half a million computers
- **2013:** The first known ransomware attack against a local government agency occurs when the Swansea Police Department in Massachusetts is hit with CryptoLocker, encrypting files on network shares and effectively preventing the police from accessing data within those files
- **2017:** WannaCry ransomware hits over 200,000 networks in 150 countries, including the National Health Service in the United Kingdom; it encrypts systems and demands Bitcoin currency payment
- **2019**: At least 100 U.S. state and local governments, including school districts or other educational institutions, are victimized by ransomware[6]



Sixteen percent of data breaches were of public sector entities.

–2019 Verizon Data Breach Investigations Report

What is ransomware?

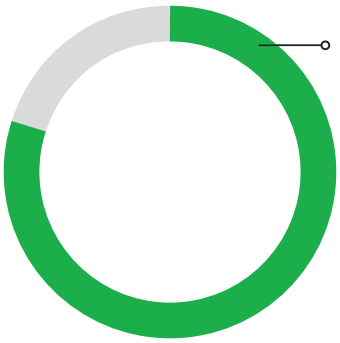
Ransomware is a type of malware that prevents users from accessing their computers or files stored on their computers. Cyberattackers demand that their victims pay a ransom before they'll provide access.

Ransomware generally falls into three categories.

- **Crypto ransomware:** Encrypts files on a computer so users can't access them
- **Locker ransomware:** Doesn't encrypt files but locks users out of their devices
- **Wiper:** Wipes the hard drive of infected computers, so that the files aren't recoverable even if a ransom is paid

Cyberattackers' choice of weapons is continually evolving as criminals try to outsmart cybersecurity experts. A sampling of methods includes:

- **CryptoLocker:** First seen in 2007 and spread through email attachments, this ransomware is thought to have affected around 500,000 computers
- **WannaCry:** Exploited a vulnerability in Windows,® affecting users in 150 countries in 2017 and causing an estimated $4 billion in financial losses worldwide
- **SamSam:** Developed and released in late 2015, it has been used against healthcare organizations, governments, schools and private businesses
- **Ryuk:** Used in a number of the attacks on state and local governments and school districts in 2019, as well as large enterprises, it disables the Windows System Restore option and encrypts network drives
- **Robinhood (or Robbinhood):** Used in several recent high-profile attacks on city governments, including Baltimore, Maryland, and Greenville, South Carolina



Ransomware was responsible for 80% of malware-related incidents in the education sector in 2019.

—2020 Verizon Data Breach Investigations Report

What can schools do?

To cope with this new challenge, school district leaders need to arm themselves with the best possible information to protect their data and avoid spending taxpayer money on ransoms or recovery efforts.

What's next:

To learn more about how to protect your district, read our report on countermeasures that school districts can take to help keep their networks secure.

Download the report on countermeasures ›

verizon✓

1 *2020 Verizon Data Breach Investigations Report.*

2 Levin, Douglas A. (2020). "The State of K-12 Cybersecurity: 2019 Year in Review." Arlington, VA: EdTech Strategies, LLC/The K-12 CybersecurityResource Center. Available online at: https://k12cybersecure.com/year-in-review/

3 Teleconference interview, March 10, 2020, with Verizon and MRM.

4 Liska, Allan. "Early Findings: Review of State and Local Government Ransomware Attacks." Recorded Future, May 10, 2019. https://www.recordedfuture.com/state-local-government-ransomware-attacks/

5 Information Security and Cyber Risk Management, Zurich North America and Advisen Ltd., October 2018, Statista.

6 Liska, Allan. "State and Local Government Ransomware Attacks Surpass 100 for 2019." Recorded Future, December 20, 2019. https://www.recordedfuture.com/state-local-government-ransomware-attacks-2019/