Ransomware, Schools and Parents

A study of parents' attitudes and experiences with cyberattacks on American schools

kaspersky BRING ON THE FUTURE

Introduction

Security researchers have been reporting on a trend in which cybercriminals have set their sights on public school districts across the country, often seeking profit by targeting victims' networks with encrypting malware and holding their valuable data for ransom. Ransomware attacks, previously more commonly experienced by larger businesses, have expanded their reach over the past two years to smaller organizations, including small businesses, local governments and school districts.

The development prompted the FBI and CISA to issue a warning about the threat and its potential to compromise sensitive data and disrupt classes. Members of Congress followed by urging the Department of Education to invest more in cybersecurity. According to government data, ransomware attacks on schools doubled to reach 57% of all ransomware incidents this past fall, up from 28% over the prior spring and summer.

Experts say cybercriminals view schools as desirable targets, since they may be less likely to have fully-developed IT security operations or system backups. They also note that the abrupt switch to online learning last spring led to the accumulation of significantly more student data, as well as a lot more employees and students who require network access but are not trained in IT security. In the event of an incident that blocks access to digital resources, a school may feel pressure to respond quickly, in order to maintain operations.

In the event of an incident that blocks access to digital resources, a school may be more likely than other organizations to view the maintenance of daily operations as an urgent necessity. Given the crucial role they play in a community, they also may feel added public pressure to do so. In the eyes of attackers, all of these factors make schools good candidates to simply pay up, rather than suffer any lost time.

The attacks come from multiple criminal groups, using a variety of malware tools, and sometimes demand tens of millions of dollars in a single attack. For example, the Conti ransomware gang recently encrypted systems at Broward County Public Schools in Florida and threatened to release sensitive student, teacher and employee data unless the district paid them $40 million. According to Kaspersky researchers, Conti is one of the usual suspects behind the current wave of attacks. Elsewhere, a Las Vegas-area district with more than 300,000 students saw private student information released after it declined to pay the ransom.

By surveying parents about their experiences, this study sought to gain a clearer picture of the situation from the perspective of a key group of stakeholders. Kaspersky partnered with Opinion Matters to find out exactly how many parents are experiencing attacks on their children's schools, and captured their perceptions of the state of preparedness among schools and students.

The results show that parents are very aware of the problem because so many of them are experiencing it directly. Overall, the report found that, while parents and schools demonstrate mostly promising levels of awareness and preparation, there is room for improvement when it comes to communication and to following expert guidelines.

Key findings from the study include:

- 55% of parents said their school has been hit with a cyberattack during their child's time there. 41% said there have been multiple attacks.
- In spite of expert warnings that it's never a good idea, 72% of parents want their child's school to pay the ransom in the event of an attack, while only 28% of parents said their school should never pay.
- On average, parents surveyed would be willing to have their child's school pay $475,687.
- 80% of schools communicate with parents and students about cyber preparedness.
- Only 34% of parents whose school was targeted were notified immediately by the school, while 57% heard about it from another source and 8% heard from the school much later.
- Parents' greatest worry is the compromise of their children's sensitive data (43%), while just 11% worried most about the cost to taxpayers or increased tuition.
- 20% of schools do not provide best practices related to cybersecurity for students and parents.

Research Methodology

Opinion Matters conducted the survey of 1,014 USA-based parents of school-age children, equally split among parents with children in elementary, middle and high school grade levels, between May 4, 2021 and May 11, 2021.

72%

of parents reported that they would want their child's school to pay a ransom.

Research Findings

Parents are very willing to pay ransoms

Security experts agree that ransomware victims should never pay criminals to unlock their data and devices and instead should immediately contact law enforcement. For one thing, payment only encourages the criminals and helps fund their operations, further perpetuating the problem. For another, payment does not guarantee the return of stolen data or that cybercriminals won't extort you again. Previous Kaspersky research found that 17% of ransomware victims who paid never got their data back. Whether they paid or not, only 29% of all victims were able to restore all of their encrypted or blocked files.

In spite of those realities, 72% of percent of parents reported that they would want their child's school to pay a ransom, in the event of an attack, in order to prevent the leak of student personal information, such as social security numbers, birthdays, addresses, school records, etc., and/or to keep school running. This is significantly higher, even, than the 53% of global ransomware victims who reported, in the earlier survey, actually paying the ransom in 2020. Only 28% of parents said their school should never pay.

Twenty-nine percent of parents said they would want the school to pay more than $100,000, including 5% who would pay between $1 and $20 million, and 11% who would pay any amount requested.

A significant number of parents were willing to have their school pay smaller amounts, with 11% who were willing to pay only $5,000, another 10% who would go up to $10,000, 10% who would pay between $10,000 and $50,000, and 12% who would pay $50,000 to $100,000.

Larger schools may be a more attractive target to cyber thieves than smaller ones, based solely on what parents are willing to pay. Parents with kids at a school with more than 1,000 pupils said they would want the school to pay over 25x more on average for a ransom than parents at schools with 50 or fewer pupils ($1,202,633 versus $46,492).

The most common concern among surveyed parents was the compromise of a child's sensitive data (43%), followed by compromise to school's IT system (22%), closing of the school for a week or more (17%), and cost to taxpayers or increased tuition (11%).

"Unfortunately, just paying the ransom seems to be an easy answer that people tend to look for. Fortunately, insurance companies are beginning to refuse to pay out on these claims. One of the reasons the ransomware problem has snowballed into so large a problem is because people are ready to pay. Maintaining security practices to prevent ransomware incidents can be difficult and have some cost, but it is not impossible."

Kurt Baumgartner
Principal security researcher
Kaspersky

"Given the sensitivity around protecting young students, parents and authorities are likely to cave into financial demands in the event of a wide, distributed breach of data. With our virtual delivery format and heightened anxieties, teachers and admins are being observed for their instant responses and this ultimately presents a major vulnerability."

Ali Hirji
Research and project lead
AI Hub & Centre for Cybersecurity Innovation at Durham College

Parents confirm: Schools are under attack

It's one thing to hear from security vendors and police about cybercrime but quite another to learn directly from the victims about just how prevalent the issue is. The survey confirmed that cyberattacks are indeed hitting schools at a significant rate. Fifty-five percent of parents said their school has been hit with a cyberattack during their child's time there.

Forty-one percent of schools that were attacked were targeted multiple times, while 59% were targeted only once.

Fifteen percent of respondents said the last time their child's school was hit by a cyberattack was this school year while 22% said the last time their child's school was hit by a cyberattack was within the past two years.

Interestingly, small schools appeared to be targeted more often this year. Parents with a child in a school with 51-100 pupils were the most likely to say the last time the school was hit by a cyberattack was this school year (18%), while respondents whose child was in a school with more than 1,000 pupils were the least likely to be hit this year (8%).

Parents were mixed on whether they thought their schools were prepared for future attacks. Only 39% said they believe their school is very prepared, while 29% said they view the school as "somewhat prepared."

In any case, parents worry about the problem. Sixty-seven percent were somewhat (37%) or very (30%) concerned that their child's school might be hit. Only 8% said they are not at all concerned.

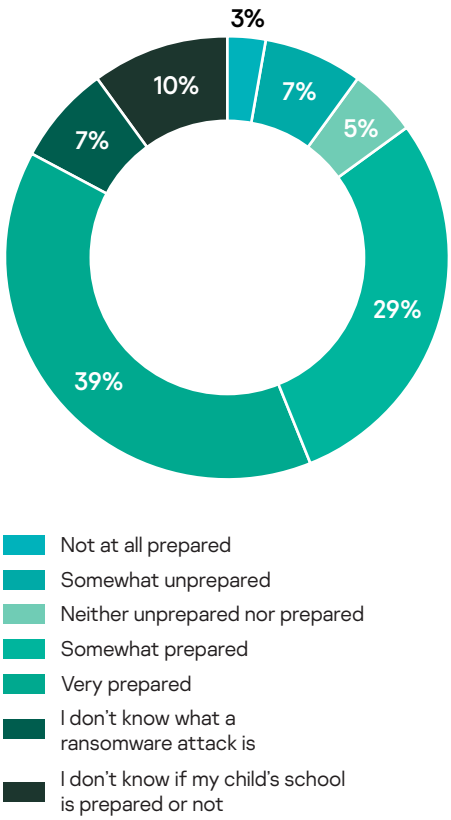
Experts note that stolen student data can be used to threaten their privacy in other ways, beyond the potential payoff of the initial ransomware attack.

"Access to student data can be used to find the missing pieces to other social media accounts and inevitably leak access into other environments," said Ali Hirji, research and project lead at the AI Hub & Centre for Cybersecurity Innovation at Durham College. "Students are hyper digital. Even in face to face learning experiences, they still rely on digital tools, and accessing this data can provide the keys to so many other platforms."

55%

of parents said their school has been hit with a cyberattack during their child's time there.

How unprepared or prepared do you believe your child's school is for protecting against a ransomware attack?



School responses: Room for improvement

Communication in the aftermath of a cyberattack is paramount. Yet only 34% of parents whose school experienced a cybersecurity incident were notified immediately by the school. Fifty-seven percent of parents heard about it first from another source, such as their child (10%), other parents (13%), the local news (14%), or social media (20%). Eight percent said they first heard about the incident from the school, but not until long after the incident.

"It's important for schools to notify parents of cyberattacks and communicate generally on these issues for a few reasons," said Kurt Baumgartner, principal security researcher at Kaspersky. "For one thing, it's an issue of privacy and safety. These criminals regularly employ threats of and actual data leaks that can be embarrassing to anyone, including kids. For another, parents and school district staff need to be aware that they are constant targets.

"Taxpayers also need to be kept informed. Folks need to understand why measures such as offline backups, multi-factor authentication, anti-malware suites and other security mechanisms are necessary on school networks."

Elementary schools appear to be doing a slightly better job at post-incident response than high schools. Thirty-seven percent of elementary school parents said they heard immediately, compared to 32% for middle school and 33% for high school.

Meanwhile, larger schools (schools with more than 500 students) communicated quickly at a slightly higher rate, reaching out immediately 36% of the time, compared to 33% among schools with 500 or fewer students.

Only 34%

of parents whose school experienced a cybersecurity incident were notified immediately by the school.

57%

of parents heard about a cyberscurity incident first from another source.

Promising signs on awareness and preparation

There are a number of things school IT administrators can be doing to minimize the risk ahead of time, including strengthening their defenses, creating data backups and training teachers, staff and students. Parents appear to have an overall positive impression of the steps their schools are taking. More than two-thirds (68%) said they think their school is somewhat or very prepared, with 29% reporting "somewhat prepared" and 39% "very prepared".

According to parents, 80% of schools have communicated in some way about their cybersecurity preparedness, through some combination of email (30% of schools), phone calls (32%), school apps (28%), student handbooks (25%), PTA meetings (11%) or communication when a student first receives a Chromebook (24%). Very few parents appear to be in the dark. Only 6.9% said they don't know what a ransomware attack is and only 9.6% don't know if their school is prepared or not.

Respondents with a child in high school were most likely to state that their child's school has not communicated to them in any way about its cybersecurity preparedness (26%), followed by respondents with a child in elementary school (20%) and finally respondents with a child in middle school (16%).

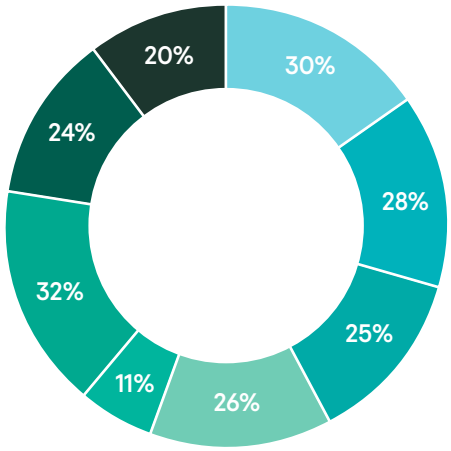
Larger schools appear to have more opportunity for growth in this area compared to smaller schools. Parents with a child in a school with more than 1,000 pupils were the most likely to state that the school has not communicated to them in any way about its cybersecurity preparedness (27%), while respondents whose child is in a school with 51-100 pupils were the least likely to say the same (8%).

Schools are also providing information to parents and students on best practices in order to protect themselves and help protect the school's networks. Thirty-seven percent of parents said their schools provided such information in student handbooks, while 29% said their schools offer courses for students. Thirty-nine percent provided tip sheets or other basic info for parents, while 38% provided a brief training to students during school hours.

Parents are also playing their part. Seventy-five percent of parents said they talk with their children at least regularly about practicing good security hygiene, addressing topics such as the importance of using strong passwords.

There's still plenty of room for improvement. Twenty percent of schools have not communicated with parents in any way about their cybersecurity preparedness, and 20% also do not provide best practices for students and parents.

In what forms, if at all, has your child's school communicated to you about its cybersecurity preparedness, such as information about its IT staffing, security tools and data backup?



- Email that outlines digital best practices taken by the school
- Message in the school app
- Included within the Student Handbook
- Call or email following a cybersecurity incident
- Through the PTA
- Call from administration at the beginning of the school year
- Communication sent home when student first receives a Chromebook
- N/A my child's school has not communicated in any way about its cybersecurity preparedness

75%

of parents said they talk with their children at least regularly about practicing good security hygiene, addressing topics such as the importance of using strong passwords.

Looking Ahead

Researchers say these attacks are likely to continue into the 2021-22 school year.

"The attacks have become higher volume and more brazen over the past year," said Baumgartner. "If history repeats itself, ransomware attacks on school systems will continue to intensify."

"I don't think cybercriminals are under any illusion that public institutions are low on funds, period," added Hirji. "It is more about the reputation and setting off panic within the population. It's a volume game – hit more and more public institutions, see more outcry and ultimately pressure for payments. Economies of scale, if you will."

There are a number of steps school IT administrators can take to prepare:

- Always keep software updated on all the devices you use to prevent ransomware from exploiting vulnerabilities.
- Focus your defense strategy on detecting lateral movements and data exfiltration to the internet. Pay special attention to the outgoing traffic to detect cybercriminals' connections. Back up data regularly. Make sure you can quickly access it in an emergency when needed.
- Do not pay the ransom if a device has been locked. Instead, contact your local law enforcement agency and report the attack. Visit kaspersky.com to find the latest decryptors and ransomware removal tools.
- Try to find out the name of the ransomware Trojan. This information can help cybersecurity experts decrypt the threat and retain access to your files.
- To protect the school network, educate teachers and staff with dedicated training courses.
- Create short, bite-sized student training courses that incorporate gamification to incentivize and reward students showing an interest in a career in cybersecurity.
- Use solutions like Kaspersky Endpoint Detection and Response and Kaspersky Managed Detection and Response, which help identify and stop an attack at an early stage, before attackers reach their final goals, and have a remediation engine that is able to roll back malicious actions.
- Additional resources are available via this digital learning toolkit for educators and in this Complete Security Checklist for Remote Learning
- Additional ransomware statistics are available here

Additionally, Kaspersky recommends the following steps for parents and students to take to protect themselves and their classmates:

- Avoid clicking links in spam emails or on unfamiliar websites and do not open email attachments from senders you do not trust.
- Never insert USBs or other removal storage devices into your computer if you do not know where they came from.
- Protect your computer from ransomware with a comprehensive internet security solution like Kaspersky Internet Security.
- Backup your devices so your data will remain safe in the event of a ransomware attack.
- Use strong, unique passwords across each of your accounts and use multifactor authentication whenever it's offered.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them. Learn more at usa.kaspersky.com.

usa.kaspersky.com

kaspersky BRING ON THE FUTURE