Don’t be the next ransomware victim.

Ransomware countermeasures article

Protect your school district with these best practices.

Aging infrastructure, outdated devices, student privacy laws, IT complexity—when it comes to managing technology, district and IT leaders have their hands full.

Now add ransomware to the list of concerns and it’s easy to see why so many leaders struggle not only to keep up with technology trends, but to protect themselves from the risks that technology brings.

Why K–12 districts are particularly vulnerable

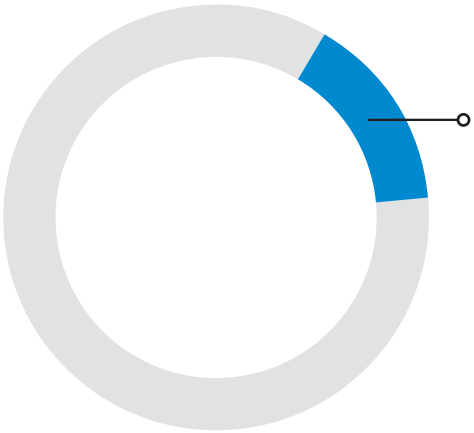
Not surprisingly, the rise of ransomware attacks has matched the rapid proliferation of digital technology in K–12. In many school systems, IT leaders manage hundreds of operating systems, apps, extensions and devices. One 2019 survey found that K–12 IT leaders secure on average 11 device types, 258 unique operating-system versions and over 6,000 unique Chrome OS™ extensions.[1]

This complexity has made it difficult for district and site IT leaders to take the steps necessary to secure their networks and data. According to a 2017 survey conducted by the Consortium for School Networking and the Education Week Research Center, only 15% of IT leaders have implemented a cybersecurity plan in their own district.[2] The fact is that most IT leaders are spread too thin and simply don’t have the time or resources to adequately prepare for a ransomware incident.

K–12

IT leaders manage on average:

- 11 device types
- 258 unique OS versions
- 6,000+ Chrome OS extensions[1]



15%

Only 15% of IT leaders have implemented a cybersecurity plan in their own district.[2]

verizon

A five-step approach for protecting yourself against ransomware

The challenge that many district and IT leaders face is figuring out how to maximize IT security with limited resources. Instead of paying ransoms or legal fees, districts would be better off using their budgets to improve their cyber hygiene and adopt recommended best practices.

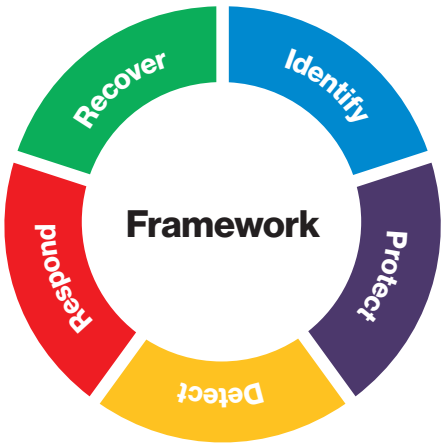
One of the best ways to achieve a high level of cyber hygiene is to use the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a guide for building a strong cybersecurity foundation.

The NIST Cybersecurity Framework is a standardized framework for securing critical infrastructure and can be a valuable resource for improving security and governance for school districts.

While the framework provides exhaustive guidance, following even its broad recommendations can change your district's cybersecurity and risk management posture from reactive to proactive.

50%

Approximately 50% of U.S. companies use the NIST Cybersecurity Framework to help manage cyber risk.[3]



How the NIST Cybersecurity Framework works

The NIST Cybersecurity Framework consists of five steps, or functions, that work together to form a security life cycle. Each function is essential to creating a viable security posture and successfully managing cybersecurity risk.

1. Identify

The Identify function can help you understand the cybersecurity risk to systems, people, assets, data and capabilities, which in turn can be used to create an approach for managing those risks.

Recommended actions:

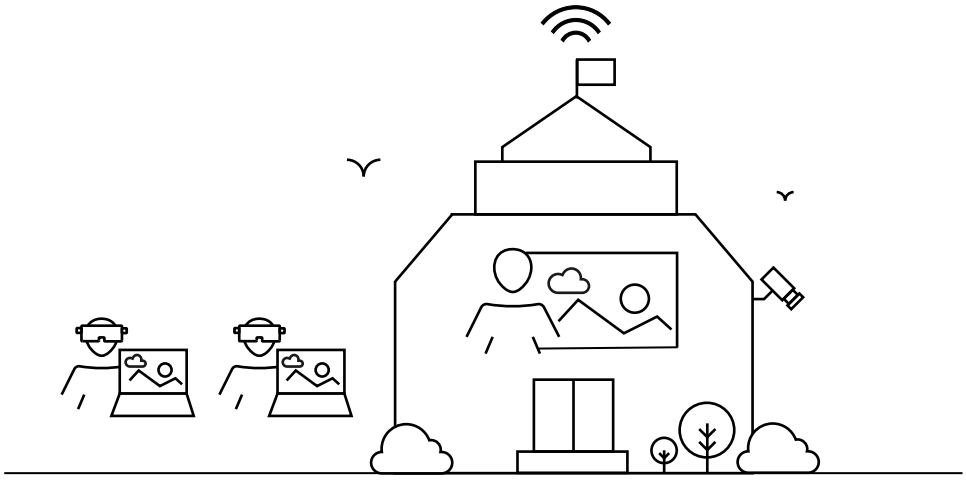
- **Identify and control access**
  Identify and control who has access, or should have access, to your district's information and technology.
- **Conduct full background checks, even on yourself**
  Many victims of identity theft find out they have been compromised only after doing a background check, which can uncover false information tied to your identity.
- **Set up individual user accounts for each employee**
  For all accounts, require employees to use strong, unique passwords.
- **Create policies and procedures for information security**
  Use these policies to identify acceptable practices and expectations and create a handbook that can be used to train current and new employees.
- **Create a ransomware playbook**
  A playbook can help you formalize your strategy for proactively managing risk and for responding in case of an attack.
- **Conduct tabletop exercises**
  Simulations can be used to determine readiness and uncover vulnerabilities.

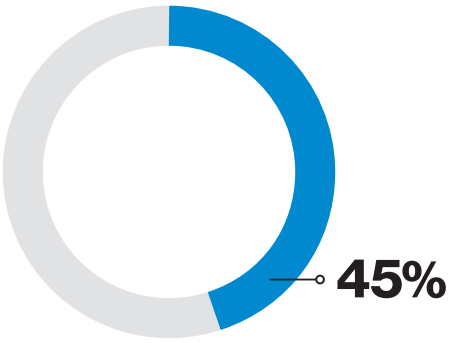
2. Protect

Using the Protect function, you can develop and implement measures to improve overall cybersecurity safeguards and prevent potential ransomware incidents.

Recommended actions:

- **Limit employee access to data and information**
  Give employees access to only the information they need to do their jobs and keep the number of people who have access to all data at a minimum.
- **Apply patches promptly**
  Keep all hardware, mobile devices, operating systems, software and applications—including cloud locations and content management systems—patched and up to date. Consider using a centralized patch management system to simplify patching,
- **Validate backup processes**
  Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure that they are operational. Ideally, backups should be stored offline on a separate system that cannot be accessed from a network.
- **Block executables and disable macros**
  Scan incoming and outgoing emails to detect potential threats and block executable files from getting to end users. Disable macro scripts from Microsoft Office® files transmitted via email. Think about using Microsoft Office viewer-type software to open Microsoft Office email files instead of the full application.
- **Block email attachments**
  Use strong spam filters to stop phishing emails from getting to end users, and employ email authentication technologies such as Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC) and Domain Keys Identified Mail (DKIM) to counteract email spoofing.
- **Remove local admin privileges**
  Remove local admin rights and apply the principle of “least privilege” to systems and services. Give your non-admin users explicit rights to specific administrative tasks.
- **Implement an awareness and training program**
  Provide social engineering and phishing training that helps employees learn to identify suspicious emails. Teach users to never click on links or open attachments in suspicious or unsolicited emails and to be careful when visiting unknown websites.





Almost half of K–12 IT leaders say their district does not widely follow a formal password policy.[4]

3. Detect

Activities that are part of the Detect function can help you identify the occurrence of a cybersecurity event quickly.

Recommended actions:

- **Deploy file integrity monitoring**
  A good change-monitoring tool can help detect a ransomware attack by monitoring files to see if and when they change, how they change and who changed them.
- **Install and update anti-virus solutions**
  Be sure to install, use and regularly update anti-virus and anti-malware software on all the devices used in your school system.
- **Educate and sensitize users**
  Conduct regular detection training and use gamified "phishing tests" to help your employees avoid common ransomware traps.
- **Have a reporting plan**
  Ensure that staff know exactly where and how to report suspicious activity.

4. Respond

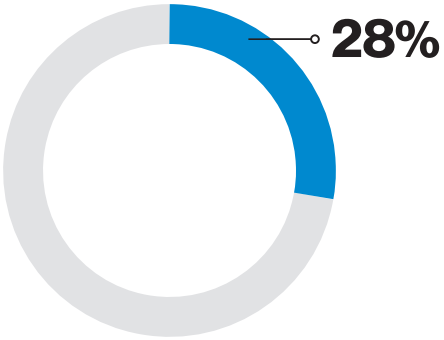
While complete protection is impossible, these Respond function actions can help you move swiftly to help mitigate the effects of a ransomware incident.

Recommended actions:

- **Block command-and-control (C2) server access**
  Blocking network access to any C2 servers used by ransomware can prevent data from being encrypted.
- **Recall known phishing emails**
  Recall all emails suspected of propagating the ransomware in order to keep the attack from spreading further.
- **Take infected systems offline**
  To prevent further spread of ransomware and damage to data, shut down or take offline any system believed to be affected.
- **Make file shares read only**
  Ransomware can only encrypt files it can access, so lock folders to read-only whenever possible and limit users' read/write access to only the folders they need.
- **Check encrypted file ownership**
  If you can identify where the ransomware originates, you can then look for computers on your network using that account and either revoke the user account's access to shares or isolate the infected computers from the network.

NIST: Assessing vulnerabilities, reducing risk

The NIST Cybersecurity Framework helps K–12 organizations understand their cybersecurity risks (threats, vulnerabilities and impacts) and how to reduce these risks with specific measures. The framework also identifies strategies and tactics for responding to and recovering from cybersecurity incidents, and outlines actions IT leaders can take to determine the root causes of an attack and how to make necessary improvements.



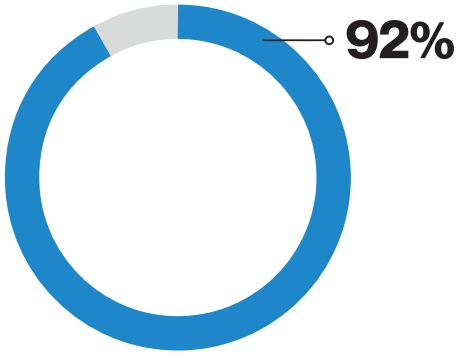
Ransomware and ransomware-like malware attacks make up 28% of all K–12 cyberattack incidents.[5]

5. Recover

Should preventive measures fail, these recommended Recover function activities can help you restore any capabilities or services as quickly as possible.

Recommended actions:

- **Get expert help**
  An experienced advisor can guide you through the steps necessary to recover from a ransomware attack.
- **Find out if a decryptor is available**
  Security researchers have broken the encryption algorithms for some types of ransomware, so check the availability of decryption tools from resources such as No More Ransom!.
- **Restore files from regularly maintained backups**
  Before implementing any backup strategy, be sure to verify that the data you are restoring from is not infected. If you use cloud services, you may be able to roll back to unencrypted data since many retain previous versions of files.
- **Find out if sensitive data has been affected**
  Some types of sensitive data, such as electronic protected health information (ePHI), may require additional reporting and/or mitigation measures.



Financial motives account for 92% of education breaches, a number that has increased over the past two years because of rising ransomware attacks.[6]

To pay or not to pay?

Deciding whether to pay a ransom is not an easy thing to do, and there are risks no matter what the choice. The official policy of the U.S. government is that organizations should not pay ransoms to criminal actors for a number of reasons.

- Paying a ransom does not guarantee that you will get access to your encrypted data. In some cases, victims were not given the decryption keys after a payment was made
- Some organizations that have paid ransoms have been targeted again
- In some cases, victims have paid a ransom only to find that they had to make an additional payment to access their data
- Rewarding cybercriminals with a ransom payment unavoidably encourages this particular criminal model

However, when faced with the inability to function, a district must evaluate all options in order to lessen the impact and protect students, teachers and staff, and parents. Victims who choose not to pay will want to thoroughly evaluate the technical feasibility, time frame and potential cost of rebuilding systems and data from backup.

Additional steps that every district should take

Apply for supplemental funding or grants to bolster cybersecurity.
While the use of technology in schools has exploded, funding for cybersecurity has lagged. Grants can help make up the difference, and several resources are available. For starters, check out Grants.gov and use the keyword “cybersecurity” (spelled with and without a space) to search for funding opportunities.

Join information-sharing efforts.
In K–12 education, leaders are always ready to share ideas or best practices. Reach out to peers from nearby or similar districts to find out what measures they are taking to protect against ransomware. If possible, create a formal group that can work to create feasible cybersecurity plans.

Share cybersecurity vendor costs with neighboring schools or districts.
A cybersecurity vendor can make a big difference in your IT security posture, so look for opportunities to spread the cost of hiring one across cooperative groups of schools or districts. This kind of cost-sharing can deliver big gains for a relatively small investment.

$1 million

In one of the highest K–12 ransoms ever delivered, cybercriminals demanded a $1 million ransom from Moses Lake School District in Washington.

Don’t wait until it’s too late.

Last year, hundreds of schools across the U.S. had to either pay ransoms, cancel classes or suffer outages to critical systems, including internet access, email, school and district websites, curriculum and assessment resources, payroll and HR tools, and more.

That’s why 47% of K–12 districts and schools are now making cybersecurity a budget priority.[7] Yet protecting against ransomware cannot be achieved by simply spending more money. What’s needed is a deep understanding of constantly evolving threats and the cybersecurity expertise to put foundational security measures in place.

The good news is that you don't have to do this all on your own. There are several industry-experienced IT and security services you can engage with that offer tremendous expertise and resources, especially for cybersecurity professional development.

- Cybersecurity experts can work directly with your IT leaders to assess your systems, identify vulnerabilities and create a plan for strengthening your cybersecurity posture
- Experts can also work with IT leaders to build ransomware prevention and cyber hygiene training for administration, staff, paraprofessionals, aides and students
- Getting serious about security also requires you to keep up to date with the latest threats and best practices. Outsourced cybersecurity professionals who are in the trenches every day can provide up-to-the-minute guidance on current and emerging threats

47%

Forty-seven percent of K–12 districts and schools are making cybersecurity a budget priority.[7]

What's next:

Read "The Way Forward" and discover the critical next steps to strengthening your cybersecurity ›

verizon✓

1 *Cybersecurity and Education: The State of the Digital District in 2020*. Endpoint Security Trends Report, K-12 Edition, Absolute, 2020.

2 Herold, Benjamin. "Schools Struggle to Keep Pace With Hackings, Other Cyber Threats." *Education Week*, November 28, 2017. https://www.edweek.org/ew/articles/2017/11/29/schools-struggle-to-keep-pace-with-hackings.html

3 https://www.nist.gov/video/cybersecurity-framework-0

4 "Survey: What School District Tech Leaders Are Saying About Cybersecurity." *Education Week*, March 19, 2019. https://www.edweek.org/ew/articles/technology/2019/03/20/rural-school-districts-lag-behind-in-cybersecurity.html

5 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/

6 *2020 Verizon Data Breach Investigations Report*, May 2020. https://enterprise.verizon.com/resources/reports/dbir

7 *Cybersecurity and Education: The State of the Digital District in 2020*. Endpoint Security Trends Report, K-12 Edition, Absolute, 2020. https://www.path.absolute.com/education/cybersecurity-and-education-digital-district-2020?utm_medium=website&utm_source=abt