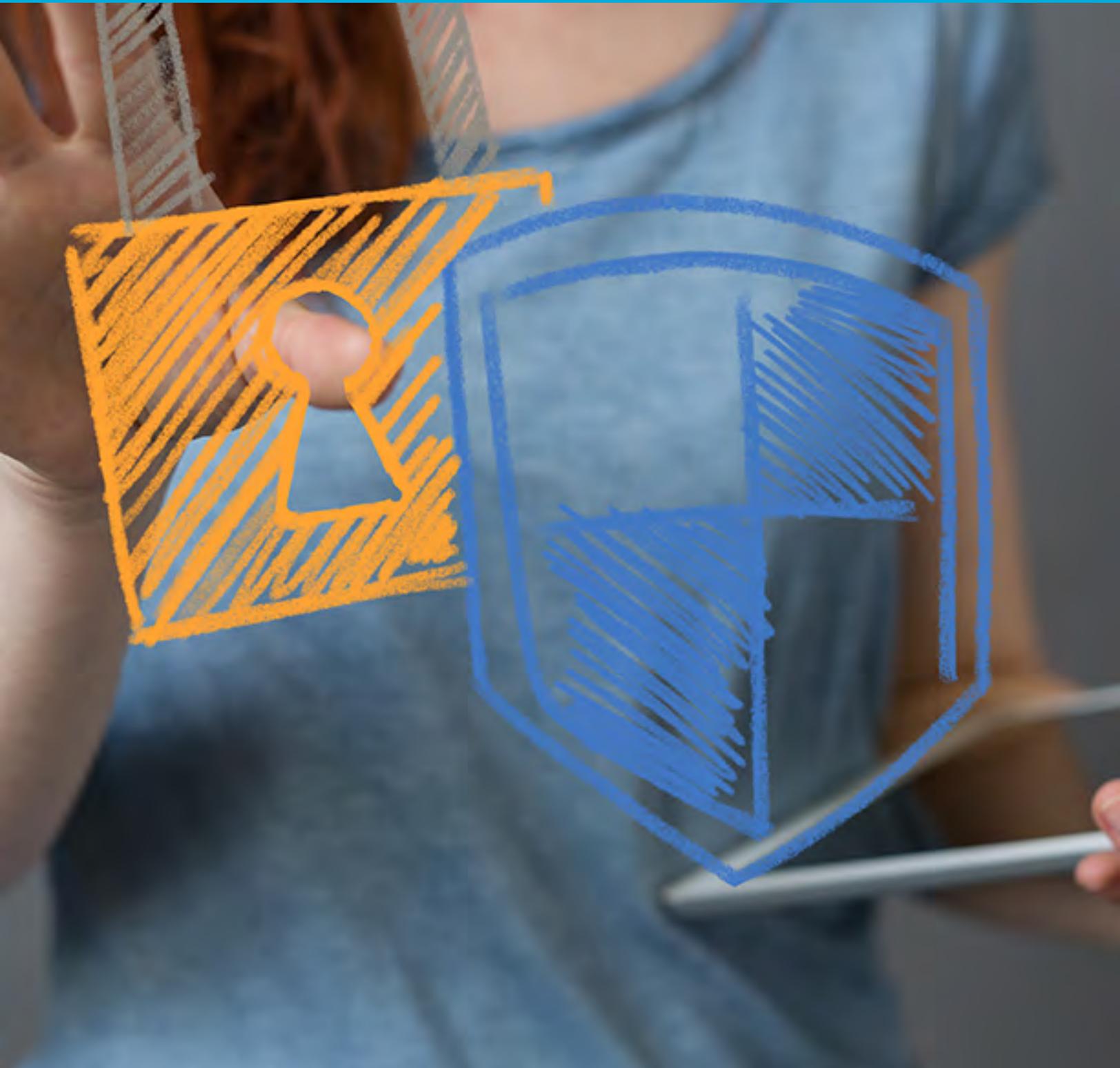


Data Protection, the Cloud, and Immutable Storage

For State and Local Government and Education IT Professionals



- 
- 3 Why Immutable Storage Should Be Part of Every Government Agency's Recovery Strategy
 - 5 Data Protection and Risk Management for State and Local Government in the Cloud Era
 - 7 School Is Back in Session: Is Your School's Data Safe?
 - 9 4 Reasons Cloud Backups Should Be Part of Your School's Data Protection Plans

Why Immutable Storage Should Be Part of Every Government Agency's Recovery Strategy



Whether you work in central or local government, you know ransomware is a clear and present danger as an IT pro. That's likely because you or industry colleagues have directly experienced an attack. Just look at the numbers. Sophos' *The State of Ransomware in Government 2021* reports that [ransomware hit 34 percent of local government organizations in 2020](#). That number rises to 40 percent for central governments and non-departmental public bodies (NDPBs). Even worse, *69 percent of local government organizations hit by ransomware said the cybercriminals succeeded in encrypting their data*. Sadly, 42 percent of those jurisdictions whose data was encrypted paid the ransom.

Regardless of size, there are steps every governmental body—and every other type of organization for that matter—should take to protect its data. And not just from ransomware, but from every other potential form of attack. That includes backups that use immutable storage, which we'll cover further on in this post. But let's start with the basics.



Start by Strengthening Your Cyber Defenses

The first step toward protecting your data is making sure it isn't accessible to bad actors slipping past your defenses, from your perimeter to your data center. Plan your budget to include the strongest possible cyber defense technologies you can afford, from threat detection and monitoring to email filtering and firewalls. This technology investment will pay off in spades over time and will undoubtedly pay for itself just by preventing a single successful cyberattack.

Put a Disaster Recovery Plan in Place

Preparation is the best way to ensure that you can recover quickly and easily if an attack is successful. We've put together [a checklist for IT disaster recovery planning](#) to help you with that effort. And once you have a plan in place, test it regularly so you are confident that you can recover your data if and when an actual attack occurs.

Back Up Your Data Regularly

Recovering your data requires diligent backups. It doesn't matter whether the loss results from a system crash, malware infection, or ransomware attack. But ransomware is still the headline of the day and should be among your chief concerns, as evidenced by the stats in paragraph one above. That's why IDC says that every IT

organization needs to put a system in place that assures data recovery without ever paying a ransom. IDC also says that this system should include [encryption, immutability, air gap, a 3-2-1-1 backup strategy, and the ability to scan backups for malware](#). That brings us to the headline of this post, immutable storage.

New Risks, New Rules for Backups: 3-2-1-1

You're likely familiar with the old "3-2-1" rule for data protection: Keep three copies of your data, one primary and two backups. Two copies are stored locally on two formats (network-attached storage [NAS], tape, or a local drive, for example), with one copy stored offsite in the cloud or secure storage.

Unfortunately, according to Forbes, [most ransomware attacks target backup systems when they encrypt endpoint data to prevent recovery](#). That's why StorageCraft, an Arcserve company, is aligned with [IDC's recommendation that organizations institute the new 3-2-1-1 backup rule, with the last "1" referring to immutable storage](#).

Why Immutable Storage Matters

Immutability is a critical element of successful ransomware protection. In short, immutability is when data is converted to a write-once, read many times format that—of most significant importance—can't be altered. Immutability differs from data encryption in that there is no key, so there should be no way to "read" or reverse the immutability.

Immutability is also crucial when deployed with other data protections, such as continuous data protection. Continuous data protection can capture data on each write at very short intervals, even measured in seconds. When you store that data in immutable form, your organization has a "snapshot" of your data that can't be altered. With the right technology, like [StorageCraft OneXafe](#), and good restore and recovery practices, you can get access to your unadulterated data within minutes of a breach.

Ensure Recovery for Your Governmental Organization

With responsibility for protecting your central or local government agency's data resting on your IT team's shoulders, now is the time to put the plans and solutions in place that ensure you can be confident in recovery. And, if you're looking for expert help in figuring out the best solution for your situation, [talk to a StorageCraft engineer](#).



A recent Washington Post feature says that ransomware is the invisible threat that's sweeping the nation. But if you're in IT—especially in state and local government—it really isn't invisible. You're probably very aware of the threat. The Post article says that, while the significant attacks make the front page, [local government agencies like school districts, city halls, and police departments are the most vulnerable to ransomware.](#)

Those vulnerabilities can lead to costly consequences. Recent research shows [79 individual ransomware attacks on government organizations in 2020, potentially impacting 71 million people and costing an estimated \\$18.88 billion in downtime and recovery costs.](#) Those are taxpayer dollars. The same research includes a map with attacks spread across almost every state in the country. And no agency is safe from hackers—ransomware attacks hit agencies ranging from Tillamook County in Oregon to the Florida Keys Mosquito District. If you're an IT pro responsible for your organization's data protection and risk management, we want you to know there is hope, and it comes from the cloud.



Start With Cybersecurity, Recovery, and Data Protection

The pandemic pushed state and local governments everywhere to shift many of their employees to remote work. These employees are now accessing government information and systems from anywhere, exposing new vulnerabilities. Network-based security isn't enough to stop threats anymore.

StateTech, a publication for state and local IT leaders, says [a zero-trust approach, strong backups to combat ransomware, and built-in security features are critical elements for cyber resilience.](#) Let's look at each of these aspects of cyber resilience and what they mean for your organization.

Zero Trust: Access Control Without an Edge

Zero trust is a security model that requires all users to be authenticated, authorized, and continuously validated for security configuration and posture before being granted access—and retaining access—to your applications and data. It can be an effective cybersecurity tool for today's onsite and remote workforces. With zero trust, implicit trust—think saved passwords with instant access to applications—is removed from your

infrastructure. Trust levels are explicitly and continuously calculated and adapted, enabling just-in-time, just-enough access to resources. According to [Gartner](#) Distinguished VP Analyst Neil MacDonald, “Zero trust is a way of thinking, not a specific technology or architecture. It’s really about zero implicit trust, as that’s what we want to get rid of.”

Strong Backups: The Key to Risk Management, Resilience, and Recovery

You’ve just read the government ransomware statistics at the top of this post. Because it’s impossible to prevent all ransomware attacks—all it takes is a click on a malicious link or a download of an infected file—the best way to beat the bad guys is to make sure recovery is always possible. [We recommend that you follow IDC’s new 3-2-1-1 rule for backups](#), replacing the outdated 3-2-1 rule. Put simply, the rule says to keep three copies of your data, with two copies stored locally on two formats (NAS, tape, or local drive) and one copy stored offsite in the cloud or secure storage.

The added “1” refers to [immutable storage](#). Immutability—an essential element of successful ransomware protection—is when data is converted to a write-once, read many times format. Immutable files—including backups—can’t be altered. Unlike data encryption, there is no key, so there should be no way to “read” or reverse the immutability. When paired with other data protection elements, immutability can capture data at each write at very brief intervals—measured in seconds. With your backups stored in immutable form, you can be confident that you can recover your data following a successful ransomware attack.

Security Features That Lock Down Your Data

Among the data protection elements that can contribute to your ability to recover from ransomware—and any other kind of attack—is solid data backup and recovery software like [StorageCraft ShadowXafe](#). Solutions like ShadowXafe give you dependable, complete physical and virtual system backup and disaster recovery, with the ability to boot backup images as virtual machines (VMs) in milliseconds. ShadowXafe backs up your data directly to the cloud and includes cloud-based management from anywhere, anytime with StorageCraft OneSystem. With tight integration with [StorageCraft Cloud Services](#), ShadowXafe makes true one-click disaster recovery as a service (DRaaS) possible, with complete, orchestrated one-click failover. That means your organization can be back up and running in no time.

Dive Into Data Protection and Risk Management in the Cloud Era

Ready to take a deep dive into high-value information that can help you make your organization more secure? [Learn more about StorageCraft’s total business continuity solutions.](#)



School Is Back in Session: Is Your School's Data Safe?



The [K-12 cyber incident map](#) put out by the K-12 Cybersecurity Resource Center should make every IT pro that is responsible for his or her school's data protection take pause. Schools in every state suffered attacks. Here's a statistic that is even more frightening: As of this writing Microsoft Security Intelligence's global threat activity map says [there were 89,916,978 devices with malware encounters in the last 30 days!](#)

Scroll down the same Microsoft webpage a bit and you'll see a bar chart with "most affected industries" from enterprise malware encounters, also in the last 30 days. If you're an IT pro working in education, that very, very long bar at the top shows the scale of the problem. [There were 5.6 million encounters in education, nearly 63 percent of all incidents.](#) The next affected industry shown on the bar chart, business and professional services, faced a mere 856,000 incidents. That means education was hit eight times more frequently than business and professional services! So, the pop quiz of the day is, how do you protect your data now that school is back in session? Here are a couple of tips.



Teach Your Teachers About Cybersecurity

Verizon's 2021 Data Breach Investigations Report concludes that [85 percent of breaches involved a human element.](#) That means no matter what malware prevention and data protection technologies you put in place, one click on a malicious link or infected attachment and your school's data could be locked up and held for ransom.

That's why it's worth creating a cybersecurity training course for teachers and other school employees. An online approach may be best so the training can fit into everyone's schedule. The course should cover how attacks that compromise student data can cause long-term issues—like identity theft—and provide specific guidance in these topics:

Ransomware

Make sure your teachers and staff understand how ransomware works and recognize common attacks that target student data and other elements of school networks.

Phishing

Explain what phishing is, its impacts, and how to spot common educational phishing schemes. Training should also include instructions for specific steps that should be taken if someone receives a potential phishing scam and how to respond if someone falls victim to a successful phishing attack.

Password safety

Make sure everyone understands the importance of using strong passwords, changing passwords regularly, and making sure all devices used for teaching are password-protected.

Wi-Fi

Share processes for safely connecting remotely and explain why public and unsecured wi-fi networks risk exposing student data.

Device updates

Updates and patches are frequently released to help keep devices secure. Help your teachers and staff understand the importance of keeping the software on the devices they use up to date.

Like their students and everyone else, teachers will pay closer attention to the training if they know there will be a quiz at the end. Test your teachers regularly to make sure they understand data security policies and procedures.

Leverage Immutable Storage for Your Backups

When it comes to the human side of data protection all you can do is make sure everyone understands their role. But on the technology side, there are some vital steps you can take immediately to ensure that your school's data is always protected and can always be restored. For example, StorageCraft, an Arcserve company, offers [OneXafe](#), an efficient storage infrastructure for backup and archival data that takes immutable snapshots of your data. Immutable snapshots can't be encrypted or deleted by ransomware attacks. So, if you ever need your data, you can be certain it can be restored.

OneXafe gives your school a single infrastructure that integrates advanced features and backup capabilities that are simple to use. You also benefit from OneXafe's encryption of your data at rest and disaster recovery with wide-area network (WAN) optimized replication. OneXafe can also reduce your storage costs with inline deduplication that can deliver up to 10x data reduction rates, depending on the type of data. And it offers a scale-out approach that helps you overcome budget constraints by letting you add storage only when you need it.

Get the Facts

With tight budgets and IT time constraints a little expert help can go a long way. A little expert help can go a long way. Consider [talking to a StorageCraft data protection expert](#) for ideas you can put in place to protect your data no matter what now that school is back in session.



4 Reasons Cloud Backups Should Be Part of Your School's Data Protection Plans



If you're an IT pro responsible for your school's data, you are likely already facing severe challenges. Threats keep growing, but budgets are always tight—[over half \(54%\) of educators and administrators surveyed say budget is a large or medium barrier in strengthening their institution's cybersecurity posture](#). You always have to wring the most out of whatever technology investments you make.

At the same time, ransomware hackers have ramped up their efforts and expanded their arsenal, focusing more of their attacks on schools. [The FBI says that at the beginning of the last school year, the majority of ransomware attacks reported—57 percent—involved K-12 schools compared to 28 percent of all ransomware incidents from January through July](#). While we all might ask ourselves why these bad actors target schools, the Cybersecurity and Infrastructure Security Agency (CISA) says the answer is straightforward: [they want to cause disruptions and steal data](#). You know the extent of the problem. Now, let's talk about some of the reasons the cloud should be part of the solution you put in place.



1. Remote and Hybrid Learning Work Better in the Cloud

First and foremost, cloud computing directly helps students, teachers, and administrators. For students, especially in our new world of remote and hybrid learning, the cloud offers access to learning materials with just an internet connection. Teachers can easily upload lessons and directly support their students. And administrators can more easily collaborate to improve the students' learning experience. Video conferencing capabilities help everyone in education, and it isn't going anywhere, with [45 percent of parents saying they would still opt for partial virtual learning given the chance](#).

2. The Cloud Simplifies IT in Education

Managing servers, networks, and devices is time-consuming and can, at times, be overwhelming for IT pros in education. More and more schools are seeing the advantages of outsourcing specific functions or workloads or all of your school's IT environment to an offsite provider. That means you no longer need to spend time managing servers and buying, maintaining, and ensuring you have enough space on those servers. And the cloud offers administrators predictable costs, a critical need in a time of shrinking school budgets.

3. Security Is Stronger in the Cloud

Unfortunately, all those devices connecting to the cloud also bring added security risks—patches may not be up to date, and the wi-fi being used may not be secure, to name two. And, of course, there are still millions of other attack vectors that could come your way at any time. That's why the cloud is critical to better data protection: Cloud providers make massive investments in data security. For example, StorageCraft, an Arcserve company, partner [Google Cloud automatically encrypts your data in transit outside of physical boundaries not controlled by Google](#). That adds a new level of security that wasn't available in the past.

4. Recovery is Always Possible with Immutable Storage

Even if you secure every device, all it takes is a click on a malicious link or attachment to let the bad guys into your network and lock up your data with ransomware. Even worse, hackers are even targeting backups with these attacks today. If your primary data and your backups get locked up, every aspect of education in your school comes to a screeching halt. That's why StorageCraft recommends that you [update your backup strategy to follow the new 3-2-1-1 rule](#). Put simply, the 3-2-1-1 rule says to keep three copies of your data—primary storage and two backups. Store two copies locally on two formats, and store one copy in the cloud. The extra “1” refers to immutable storage. Stored immutable backups can't be altered or deleted, so your data is always safe in the cloud and you can be confident that you can recover—quickly—from almost any disaster.

Conclusion

It's hard enough running an IT department in today's education environment. Isn't it time you reduced your risks and put a solution in place that ensures your school is safe from ransomware—and every other form of attack? Find out how by [talking to a StorageCraft backup and disaster recovery expert today](#).





StorageCraft Technology LLC
8855 Columbine Road, Suite 150,
Eden Prairie, Minnesota 55347



Learn More
StorageCraft.com



Contact
801.545.4711
Sales@StorageCraft.com



More Stories
StorageCraft.com/Resources