UNITRENDS
A Kaseya COMPANY

eBook

The *7 Deadly Sins* of Backup

Your organization's data is the lifeblood of your business. From powering decision-making to driving customer insights and fueling innovation, data enables your organization to operate efficiently and stay competitive. In today's data-driven world, safeguarding this valuable asset is more important than ever.

In 2024, the global average cost of a data breach soared to a record-breaking $4.88 million, marking a 10% increase from last year. This sharp rise indicates the growing financial impact of data breaches on businesses worldwide.

Data loss can occur due to technical glitches, employee mistakes, cyberattacks or natural disasters. Losing critical data can lead to downtime, financial losses, lost opportunities, non-compliance and even reputational damage. Despite advances in technology, data loss disasters are still common and expensive. Even with a backup system, many companies overlook hidden risks and mistakes that can turn a small hiccup into a catastrophic disaster.

This eBook, "The 7 Deadly Sins of Backup," is thoughtfully crafted to help businesses like yours identify and avoid the most common yet dangerous backup mistakes. By recognizing these pitfalls, your organization can build a resilient data protection strategy and ensure you're fully prepared when disaster strikes. In this eBook, we'll explore the seven deadly mistakes that businesses make and how Unitrends backup and disaster recovery solutions can help protect your business against them.

In 2024, the global average cost of a data breach soared to a record-breaking **$4.88 million**, marking a 10% increase from last year.

The 7 deadly sins of backup

Data loss can happen in many unpredictable ways and when you least expect it. Cyberattacks, malicious insiders, technical failure and human error are a few examples that can occur without warning. While you can't always control when these threats occur, you can control how well you back up and protect your organization's invaluable data. Below, we've highlighted the critical backup errors that put your business at risk. By taking proactive steps to avoid these common backup mistakes, you can significantly reduce the risk of data loss disasters.

1. Skipping backup tests — A recipe for disaster

Sin: Backups are created but never tested.

If you think just backing up your data is enough, think again. Without regular testing, your backup is just a false sense of security. Unverified backups may fail when restoration is needed most, putting your business at significant risk of costly data loss and downtime.

Remediation: Schedule periodic test restores to ensure your backups are valid, complete and can be restored quickly. Frequent testing of your backups will help identify any issues that could impact restoration and take the necessary steps to prevent data loss and ensure business continuity. This should be part of a disaster recovery drill.

HOW UNITRENDS CAN HELP

Unitrends Recovery Assurance automatically performs top-tier application recovery testing, eliminating manual intervention and management hassles. It fully restores applications, runs detailed analytics and tracks both recovery time and recovery point to ensure your systems are ready when needed. If any recoveries fail, it identifies the root causes so you can fix them fast.

With our proactive and automated testing, you can spot issues early, always know where your latest good backup is and be fully prepared for recovery when disaster strikes. Stay ahead of risks and ensure recovery readiness — without the manual work.

2. Putting all your eggs in one storage basket

Sin: Storing backups in a single location (e.g., on-premise only).

Relying on a single storage location for your backups is a risk waiting to happen. While a single location may seem convenient and cost-effective in the short term, it leaves your data vulnerable to unexpected events. Whether your organization's data is stored on-premises or in the cloud, a single point of failure could lead to complete data loss in the event of a physical disaster, cyberattack or system failure.

Remediation: Adopt a multilocation backup strategy to protect your data effectively. At Unitrends, we strongly recommend that you follow the 3-2-1 rule for disaster recovery: 3 copies of your data, 2 different types of media and 1 copy off-site (and even better—immutable!). Leverage cloud-based backups, as they offer the advantage of geographic redundancy, which ensures your data is protected against physical or natural disasters, such as fires or floods, at your primary location.

HOW UNITRENDS CAN HELP

Unitrends Forever Cloud is purpose-built for off-site, long-term retention and disaster recovery. This automated long-term data retention solution saves hours of IT time. It ensures data is backed up immutably and retained in compliance with recovery point objective (RPO) and stored in accordance with data retention and other regulatory requirements — without the manual hassles of media-based solutions like disk or tape.

3. Backups that are too late to save the day

Sin: Setting backup intervals that are too infrequent increases the risk of data loss between backup intervals.

Many businesses set up backup frequencies based on the convenience of their IT teams rather than data requirements. Infrequent backup cadence can lead to data loss in the event of accidental deletion, hardware or software failure, or cyberattacks. The wider the gap between backups, the more data you stand to lose when disaster strikes.

Remediation: Backup frequencies will vary between companies depending on how much data an organization can afford to lose in the event of a disaster. Evaluate your organization's RPOs and adjust the backup frequency to match the criticality of the data. For some companies, daily backups are sufficient, while for others, backups every few hours may be necessary. For business-critical systems, real-time or near-real-time backups may be needed.

HOW UNITRENDS CAN HELP

Unitrends SLA Policy Automation controls the initiation and flow of backups and backup copies through a single, simple policy. You simply set RPOs, define where backup copies should go and how long they should be kept. Unitrends automates the entire underlying process, including the analytics and business-level reporting of compliance with those SLAs. With SLA policy automation, it is easy to establish multiple SLA policies to protect the different assets across your environment.

4. Ransomware: The threat you can't ignore

Sin: Relying on traditional backup methods without considering ransomware resilience.

Ransomware is one of the biggest threats businesses face today. Yet, many organizations fail to consider how ransomware can affect their backup strategy. If your backups are not secured against ransomware, a malicious attack could encrypt or destroy them, rendering them useless at a critical moment. In the past year, about 95% of organizations targeted by ransomware reported that threat actors targeted their backups during the attack.

Remediation: Protect your backups from ransomware by storing them in environments that ransomware cannot access. Employ immutable backups or air-gapped storage, which cannot be changed or deleted by ransomware. Also, integrate malware scanning into your backup process to detect potential vulnerabilities early, prevent reinfection from restored data and ensure data integrity.

HOW UNITRENDS CAN HELP

Unitrends backup appliances are built on hardened Linux-based architecture, making them impervious to Windows-targeted malware. To ensure your backups are truly safe, Unitrends provides the Unitrends Forever Cloud, a dedicated service for secure, off-site data retention within an immutable cloud architecture. While you can access and import the data back to your local appliance, neither the appliance nor any other source can modify or delete data stored in the cloud.

Our solutions use adaptive and predictive artificial intelligence (AI) to scan all backup and replication data, identifying and alerting IT to potential ransomware threats. Application-level Recovery Assurance testing automates backup validation, ensuring you can recover with confidence.

5. SaaS data in danger — Don’t leave it unprotected

Sin: Assuming that cloud or Software-as-a-Service (SaaS) providers, such as Microsoft, Google or Salesforce, handle backups of their SaaS applications

SaaS applications are critical to business operations, yet many businesses fail to back up the data from these cloud platforms. They mistakenly believe that the service provider is responsible for safeguarding their data. However, SaaS providers follow a shared responsibility model, where protecting the infrastructure is their responsibility, but data protection is the customer’s responsibility.

Remediation: Implement third-party backup solutions designed specifically for SaaS applications. Cloud providers typically offer only short-term retention or point-in-time recovery; therefore, it’s important to tailor backup policies to meet your compliance and operational needs. Third-party backup solutions protect the data stored in cloud applications, enabling long-term data retention and easy recovery of deleted or corrupted files.

HOW UNITRENDS CAN HELP

Unitrends cloud-to-cloud backup and recovery solutions offer simple and secure data protection for your Microsoft 365, Google Workspace or Salesforce data. Our SaaS backup solutions provide automated, daily backups, ensuring your data is up to date and recovery-ready if the need arises. Unitrends makes data recovery quick and hassle-free with flexible recovery options, including end-user self-service, point-in-time restore, granular search-based restore, Shared Drives restore and cross-user restore. You can easily manage your SaaS backups for Microsoft 365, Google Workspace or Salesforce through the SaaS Backup module within UniView.

6. Neglecting compliance can cost you big

Sin: Using default or outdated retention policies that don’t comply with regulatory requirements or business needs.

Businesses may overlook the need to regularly review and update retention policies. This can be due to a lack of understanding of evolving regulations, changes in the business’s data landscape or simply because the policies were initially set up and then forgotten. As data grows and regulations change, outdated retention policies can no longer align with compliance needs or operational requirements.

Remediation: Review and update retention policies regularly to ensure they meet legal and operational requirements. Your IT team should assess both regulatory requirements and your organization’s operational needs to ensure retention policies are up to date. Consider long-term archiving solutions to ensure regulatory compliance while optimizing costs.

Sin: Failing to comply with industry regulations, insurance requirements or corporate governance policies for backup and recovery.

Data protection regulations are often complex, leaving businesses unsure about which ones apply to them and how to stay compliant. As a result, backup and data retention policies may not be properly updated to meet changing requirements.

Remediation: Incorporate compliance requirements into your backup strategy to ensure backups are securely stored and retained for the mandated duration. Automate audit logging to track backup activities and provide documentation during compliance audits.

HOW UNITRENDS CAN HELP

Unitrends Forever Cloud offers cost-effective, fully automated, off-site and long-term data protection. Easily meet long-term data retention requirements for compliance and audits while enjoying the benefits of cloud backup. Our customizable retention options allow you to choose how long to retain data: 90 days, annually (1 to 7 years) or indefinitely.

Unitrends Unified BCDR provides automated disaster recovery testing both locally and in the Unitrends Cloud. Our Recovery Assurance software integrates with your backup appliance to automatically test and verify your recovery objectives and service-level agreements (SLAs) in advance.

Unitrends provides instant lab spin-up for testing, data analysis and development sandboxes. These instant labs enable you to scan for malware, test updates, run compute-intensive reports and conduct business analytics, all without affecting your production environment.

In a recent incident, a large manufacturing company faced a ransomware attack that encrypted over 780 VMs and data from their other backup vendor. Before recovery, their cyber insurance provider required independent third-party scans to identify the intrusion point and assess recovery health. Using Unitrends Data Copy Access, the company automated the spin-up of isolated labs to recover VMs in batches for analysis. Third-party scans confirmed the data was clean and met audit requirements. Once cleared, automated orchestration from Data Copy Access pushed the machines live into the production environment.

7. Partial backups, complete catastrophe

Sin: Failing to back up all critical data, such as application configurations, system states or metadata.

One of the most critical mistakes businesses make is failing to back up everything critical for their business operations. Incomplete or partial backups — whether of certain file types, databases or entire systems — can leave significant gaps in your data recovery plan, resulting in catastrophic consequences in the event of a crisis. This can happen as a result of businesses failing to fully assess their data landscape, thereby only backing up what they deem essential. Misconfigurations in backup software can also result in certain files or applications being left out.

Remediation: Conduct a thorough audit of your environment and ensure all critical data, including databases, files, system and application configurations, are included in the backup process. Missing elements like metadata can lead to incomplete restores or prolonged downtime.

HOW UNITRENDS CAN HELP

Unitrends backup and disaster recovery solutions provide complete data protection no matter where it lives — on-premises, in the cloud, within SaaS apps or on endpoints. Our industry-leading solutions, including dedicated backup appliances, cloud-to-cloud SaaS backup and direct-to-cloud solutions for endpoints and cloud workloads, are built to protect your data against ransomware, data loss and downtime.

With UniView's centralized platform, you can seamlessly manage backup and recovery solutions for your data centers, endpoints and SaaS applications from one place. BackupIQ, our intelligent alerting engine, allows you to set thresholds that prioritize alerts for issues affecting your recovery SLAs, like skipped backups or replication, ensuring faster response to critical problems.

Take control of your data before it’s too late

The stakes have never been higher when it comes to data protection. We’ve uncovered the seven most dangerous mistakes organizations can make in their backup strategies. From poor planning and neglecting testing to relying solely on cloud services without considering a robust recovery strategy, these deadly sins are not just theoretical — they’re real-world mistakes that have cost businesses time, money and reputational damage.

But the good news is, with awareness comes the power to act.

Avoiding these deadly sins of backup is key to building a robust data protection strategy. Data loss disasters can strike at any time. However, with the right backup and recovery solution in place, your business can recover quickly and continue business as usual, even in the face of adversity.

Schedule a personalized demo today to discover how Unitrends strengthens your data protection strategy.

SCHEDULE A DEMO

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

18102024

UNITRENDS
A Kaseya COMPANY