



# Five data protection mistakes and how to avoid them



## What keeps you up at night?

Traditional data protection methods fall short of today's business demands. Significant operational challenges that include potential downtime and data loss, the complexities of managing multi-cloud infrastructures, and the costs associated with creating secure architectures, heighten the risk of slow recovery — and could leave you without adequate protection for your data assets.

The need for smarter and faster defenses across your entire IT environment is now an imperative. Protecting against evolving threats while keeping operations simple and efficient is a daily challenge.

Discover how you can gain additional benefits including data mobility, immutable backups, and regular testing of data resilience. In short, "forewarned is forearmed", and being aware of a potential problem or danger in advance allows you to prepare for it.

---

## Your checklist: Be prepared for potential pitfalls

Experts agree that there are multiple, very basic system weaknesses that can wreak havoc on even the most secure data environments. But the same experts also agree that building a culture that embraces and is committed to adhering to the key principles of IT security will be key to your ongoing success.

| Data protection misstep  | How to avoid potential errors   |
|--|---|
| <p>✓ <b>Failing to back up data frequently</b> can result in permanent loss during outages or cyberattacks.</p> <p>Unreliable backup products, often associated with low-cost or free solutions, lack robust features, resulting in backups that are neither secure nor dependable. Additionally, sub-optimal backup times, such as scheduling during high-traffic periods or when data is frequently modified, can lead to incomplete backups. Compatibility issues also arise as businesses evolve, with new systems and software sometimes not aligning with existing backup solutions, preventing proper data capture and restoration. Finally, human error, including incorrect backup configurations, accidental file deletions, or ignoring backup schedules and alerts, can significantly disrupt the backup process, further compromising data protection.</p> <p><b>Bottom line:</b> Ignoring backups can be catastrophic.</p> | <p>Regular maintenance and testing ensure you're prepared for disasters such as cyberattacks or natural calamities.</p> <p>Utilize continuous data protection (CDP) with near-real-time replication, ensuring that your data is always protected without relying on traditional backup windows.</p> <p>Reliable data backups and successful restoration are critical for business continuity. Follow these best practices to protect your data and minimize disruptions:</p> <ul style="list-style-type: none"><li>— <b>Ensure your solution meets compliance needs</b>, such as immutable backups that prevent unauthorized changes. Discuss recovery speed, downtime expectations, and storage locations (cloud, local, or hybrid) with your IT provider.</li><li>— <b>Check backup status daily</b> and address failures immediately. Advanced systems can alert you if backups become unresponsive.</li><li>— <b>Periodically restore files</b> to confirm data integrity and retrieval efficiency.</li></ul> |

## Data protection misstep

## How to avoid potential errors

- ✓ Using simple, reused, or default passwords increases the risk of unauthorized access.

To enhance security, follow these best practices for password management and authentication:

- Train employees to create strong passwords, avoid reuse, recognize phishing scams, and maintain secure login habits.
- Integrate with secure identity and access management (IAM) solutions that support role-based access control (RBAC) to limit unauthorized access.
- Encourage users to create complex passwords with uppercase and lowercase letters, numbers, and special characters. Avoid common words and personal details.
- A reputable password manager can generate, store, and manage strong passwords across all accounts, reducing the risk of password reuse.
- Adding multi-factor authentication (MFA) to accounts provides an extra security layer by requiring additional verification, such as a one-time code or biometric authentication.
- Lock accounts after multiple failed login attempts to prevent brute-force attacks.
- Regularly review login attempts and access patterns to identify and respond to suspicious activity promptly.

- ✓ Ignoring software updates

Running outdated software exposes systems to known vulnerabilities.

Developers frequently release software updates to address security vulnerabilities such as patch security loopholes. If you ignore updates, you'll remain exposed to any weaknesses, increasing the risk of a cyberattack that could impact you and your organization.

Stay informed and regularly update your device to ensure optimal performance and security. Regular updates keep your software secure, efficient, and user-friendly, ensuring optimal performance and protection against cyber threats.

Focus on nondisruptive testing capabilities to allow your businesses to safely test software updates, patches, and configurations without impacting production environments.

Other software update considerations include:

- Improving speed and efficiency
- Fixing bugs that could cause crashes or malfunctions
- Enhancing functionality with improved tools and capabilities
- Ensuring compatibility with newer systems and devices
- Creating a more user-friendly experience with better usability
- Preventing user frustration caused by outdated or inefficient software

## Data protection misstep

## How to avoid potential errors



### No disaster recovery plan

A structured backup and recovery plan is essential to safeguard critical business information, maintain compliance, and ensure operational continuity.

Not having a data recovery plan can lead to severe consequences, including irreversible data loss, business disruption, and financial setbacks.

Key risks can include:

- **Hardware failures, accidental deletions, or cyberattacks** that can erase critical files forever — leaving you without backups
- **Loss of essential data** that can halt operations, reduce productivity, and lead to revenue losses
- **Failure to protect sensitive data** that can result in legal repercussions and regulatory penalties
- A major data breach or loss that can **erode customer trust** and tarnish your company's credibility
- **Outdated or fragmented data** without regular backups, leading to poor — and costly — decision-making

A **comprehensive disaster recovery solution** with automated failover, failback, and recovery orchestration simplifies testing and ensures business continuity with minimal downtime.

To mitigate risks, your data recovery plan should include:

- **Regular, automated backups** of critical data to multiple locations, including off-site storage
- **Identification and prioritization of sensitive data** that requires extra protection
- **Regular testing of backup systems** to ensure data can be restored successfully
- **Disaster recovery plans** to recover data in the event of a major disaster such as a fire or flood
- **Educating employees** on data handling best practices and backup procedures



### Insufficient employee training

Untrained employees are more likely to fall for phishing and social engineering attacks.

This vulnerability could potentially compromise sensitive information by clicking malicious links, revealing login credentials, or downloading malware due to their lack of awareness about cyber threat identification. In turn, this can lead to financial loss, damaged reputation, or legal consequences for the organization.

The following are other risks associated with inadequate employee training:

- Without proper awareness, employees could fall prey to social engineering tactics such as phone scams or impersonation attempts, divulging confidential information to malicious actors.
- Mishandling sensitive data due to lack of training on data privacy practices can lead to significant data breaches.
- Employees not trained on strong password practices may use easily guessable passwords, leaving their accounts — and your business — **vulnerable to hacking attempts**.
- Failing to train employees on data protection regulations can result in **legal penalties** if sensitive information is compromised.
- Time spent dealing with security incidents caused by untrained employees can **disrupt workflow and impact productivity**.
- A data breach resulting from inadequate employee training can significantly **harm a company's reputation** and customer trust.

Initiate **automated testing features** that enable **regular cyber recovery and disaster recovery drills**, helping businesses train IT teams and validate response plans without disruptions. Training should also include **phishing identification, password hygiene, social engineering tactics, and safe data handling practices**.

- Develop training specific to different employee roles and responsibilities, addressing their unique security risks.
- Encourage employees to report suspicious activities and provide a safe environment to ask questions about cybersecurity concerns.



## Software and solutions that safeguard your data — and your business

Imagine never having to worry about your data and applications being vulnerable to outages, cyberattacks, or disasters. HPE GreenLake and offers a powerful, automated solution for data protection, rapid recovery, and seamless workload mobility across environments.

By eliminating concerns over outages, cyberattacks, and disasters, you can free up your IT teams to focus on business growth. Choose HPE Zerto for standalone Software and HPE GreenLake for a cloud-managed experience. Whether strengthening disaster recovery or enhancing cyber resilience, these solutions provide the flexibility and peace of mind needed to keep your business running smoothly.

Visit [HPE.com](https://www.hpe.com)

### Learn more at

[HPE.com/Zerto](https://www.hpe.com/Zerto)

### [Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50012353ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

