The 3 Major IT Risk Drivers
Your Organization Should Watch Out For

Businesses globally are increasingly moving to multicloud and hybrid cloud environments due to their numerous benefits. However, these technologies come with some key challenges that can put your organization at risk.

Protecting your data in the cloud: **Would you risk IT?**

Key data protection challenges associated with multicloud or hybrid cloud strategy:

- Lack of visibility into your data
- Complex and susceptible since data spans across multiple cloud providers
- Introduces new threat vectors and data risks

80% of organizations have experienced at least one severe cloud security incident in the past year.[1]

The **Three Major Risk** Drivers in Your IT Organization

Your data in the cloud is constantly at risk due to the following three reasons:

1 Human-driven risks

Whether unintentional or deliberate, human actions significantly contribute to data loss in SaaS application environments.

HUMAN ERROR
Over 80% of data breaches involved a human element, including phishing and the use of stolen credentials, as per Verizon's 2022 Data Breach Investigations Report.[2]

MALICIOUS INSIDER ACTIVITY
Over 70% of cybersecurity professionals feel their organization is "moderately to extremely vulnerable" to an insider attack.[3]

HACKERS
Global cyberattacks increased by 38% in 2022 compared to 2021.[4]

2 Technology-driven risks

As reliance on new-age technology solutions grows, technology-driven risks also grow, increasing the chances of exposing your organization to a wide range of threats.

SYNC ERRORS
Sync errors due to weak connectivity, technical glitches or reliance on third-party applications can result in losing the information you need most.

VIRUS, MALWARE AND RANSOMWARE
Around 300,000 new malware pieces are created daily.[5] It is estimated that ransomware attacks will strike businesses every two seconds by 2031.[6]

RELIANCE ON NATIVE TOOLS
Over 40% of cloud engineering and security professionals revealed that cloud-native services increase complexity, further complicating their security efforts.[7]

3 Process-driven risks

SaaS data protection is complicated since it involves numerous parties, technologies and processes that must come together to achieve the desired results.

LACK OF AN INCIDENT RESPONSE (IR) PLAN
Businesses with an IR plan experienced an average of $2.66 million lower breach costs compared to those without an IR plan.[8]

SECURITY MISCONFIGURATIONS
Cloud misconfigurations are responsible for 15% of initial attack vectors in security breaches.[9]

NON-COMPLIANCE
Fines, penalties and settlements due to non-compliance cost companies hundreds of millions of dollars.[10]

Key steps to reducing risk with Spanning

Spanning Backup is a purpose-built, cloud-native backup and recovery solution, providing enterprise-class, end-to-end data protection for Google Workspace, Microsoft 365 and Salesforce.

Spanning helps prevent, anticipate and mitigate account compromise and data loss through:

1. **ROBUST SECURITY**
Spanning leverages industry-standard, application-level security (OAuth 2.0) instead of less secure privileged service accounts and passwords.
2. **PHISHING DEFENSE**
AI-enabled email security for protection against phishing, business email compromise (BEC), account takeovers (ATO) and more.
3. **SPANNING DARK WEB MONITORING**
Identify, analyze and proactively monitor your organization's compromised or stolen credentials on the dark web.
4. **END USER SELF-SERVICE RESTORE**
Empower end users to quickly find and perform non-destructive data restores without IT intervention.
5. **AUTOMATED DAILY AND ON-DEMAND BACKUPS**
Eliminate time spent tediously managing backup schedules, reduce the chance of inconsistencies and errors, and streamline compliance.
6. **CUSTOMIZABLE CLOUD RETENTION TERMS**
Easily customize policies based on your needs to meet regulatory or compliance requirements and SLAs.

Sources

1. https://go.snyk.io/state-of-cloud-security-2022.html
2. https://www.verizon.com/business/en-gb/resources/reports/dbir/
3. https://www.cybersecurity-insiders.com/portfolio/insider-threat-report-prospectus/
4. https://www.securitymagazine.com/articles/98810-global-cyber-attacks-increased-38-in-2022#:~:text=Rounding%20out%20the%20top%2Dfive,28%25%20increase%20over%202021).
5. https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref
6. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/
7. https://go.snyk.io/state-of-cloud-security-2022.html
8. https://www.ibm.com/reports/data-breach
9. https://www.strongdm.com/blog/cloud-security-statistics
10. https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

Download the eBook to learn about these risk drivers and the steps to overcome them in detail.

SPANNING
A Kaseya COMPANY