kyndryl / veeam

How comprehensive backup and recovery for cyber resilience supports digital transformation

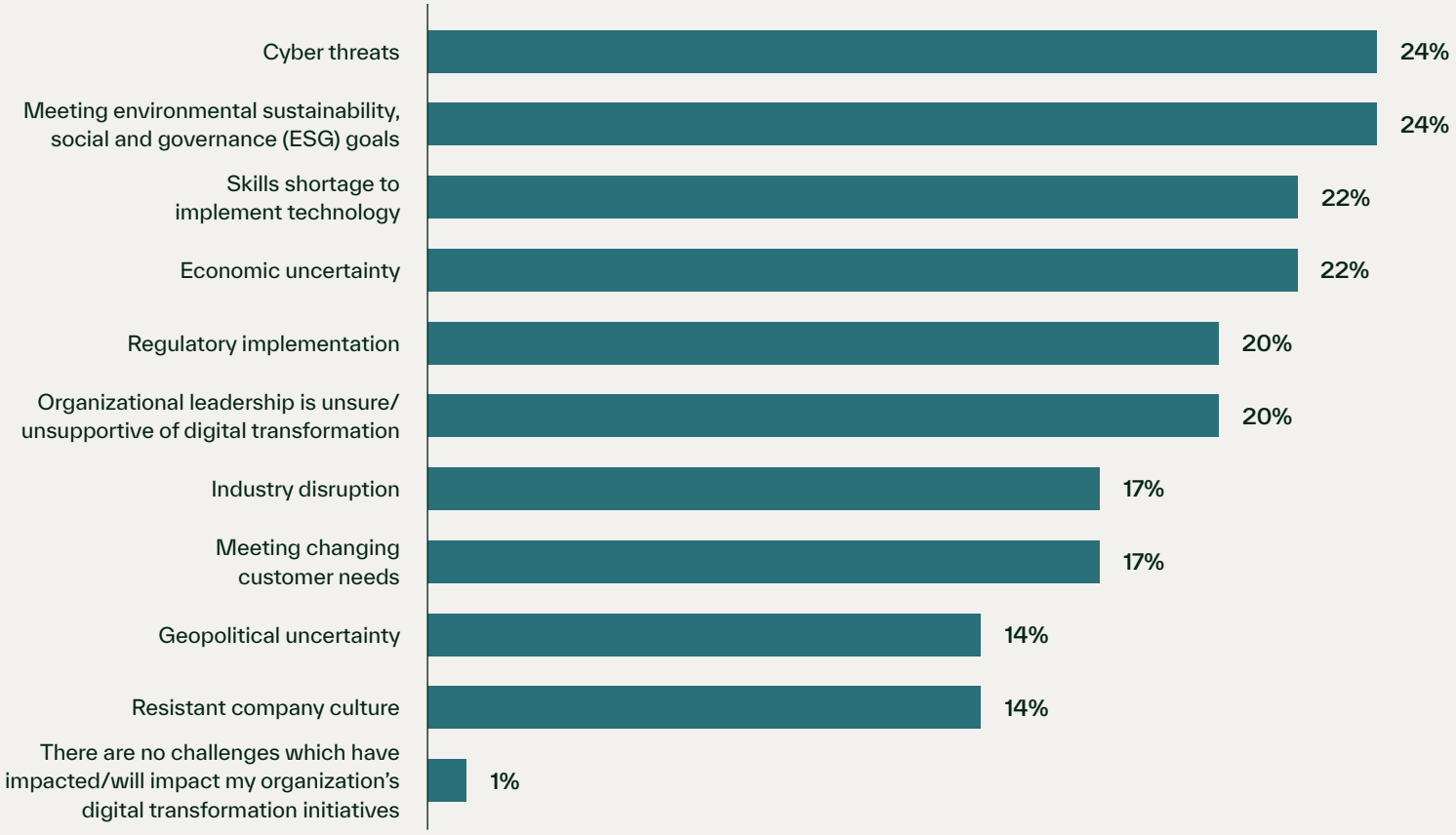
Contents

Executive summary

It's no surprise that cyberattacks continue to plague organizations. Over the past two years, cybersecurity events ranked as the most common cause of outages, according to Kyndryl alliance partner Veeam's 2024 Data Protection Trends report.1 Additionally, the survey respondents, which included 1,200 business and IT leaders, said cyberattacks were the most impactful of the events they experienced.

Cyberattacks have become so prevalent and impactful that they're hindering the ability of organizations to modernize and transform. Veeam's survey asked respondents what the top challenge to (Chart A) transformation would be over the next 12 months and, unsurprisingly, found cyber threats ranked as the number one challenge. This was ahead of meeting ESG goals, skills shortages, economic uncertainty and other concerns.

Of the below business/IT challenges, when it comes to your organization's ability to achieve your digital transformation initiatives which do you believe will be the biggest challenges over the next 12 months?



https://vee.am/DPR24

Data Protection Trends 2024 Report-published by Veeam in January 2024
N=1,200 unbiased IT Leaders and implementers responsible for their organizations data protection strategies

Image 1: When achieving digital transformation initiatives, what will be the biggest challenges over the next 12 months?[1]

Ransomware remains a major problem

One of the more prevalent and headline-grabbing cyber-security events continues to be ransomware. There have been many publicly reported instances over the past year of ransomware attacks crippling organizations that have been forced to shut down operations because access to their IT systems was locked.

According to the Veeam report, 3 out of 4 organizations suffered at least one ransomware attack in the preceding 12 months. While organizations may do everything in their power to anticipate, protect against, and withstand an attack, they sometimes overlook the crucial step of preparing for recovery from an attack.

To illustrate this, Veeam asked respondents if their organization had to failover 50 servers—a relatively small number—due to a disaster or cyber event, how long would it take from starting the recovery of the first server until the last one was online? Only 32% of respondents believed it would take under a week (Chart B). This is worrisome because even one week of unplanned downtime at an organization can incur high costs, send shockwaves throughout its teams, attract unfavorable publicity and hurt performance.

Organizations recognize this is a challenge. Eighty-five percent of organizations reported an "availability gap" between how fast they could recover and what the business processes required. Furthermore, 76% of organizations recognize a "protection gap" between how much data they could afford to lose and how often their data is protected.

If your organization had to fail over 50 servers due to a disaster or cyber event, how long do you estimate it would take from starting the recovering of the first server until the last server was online?

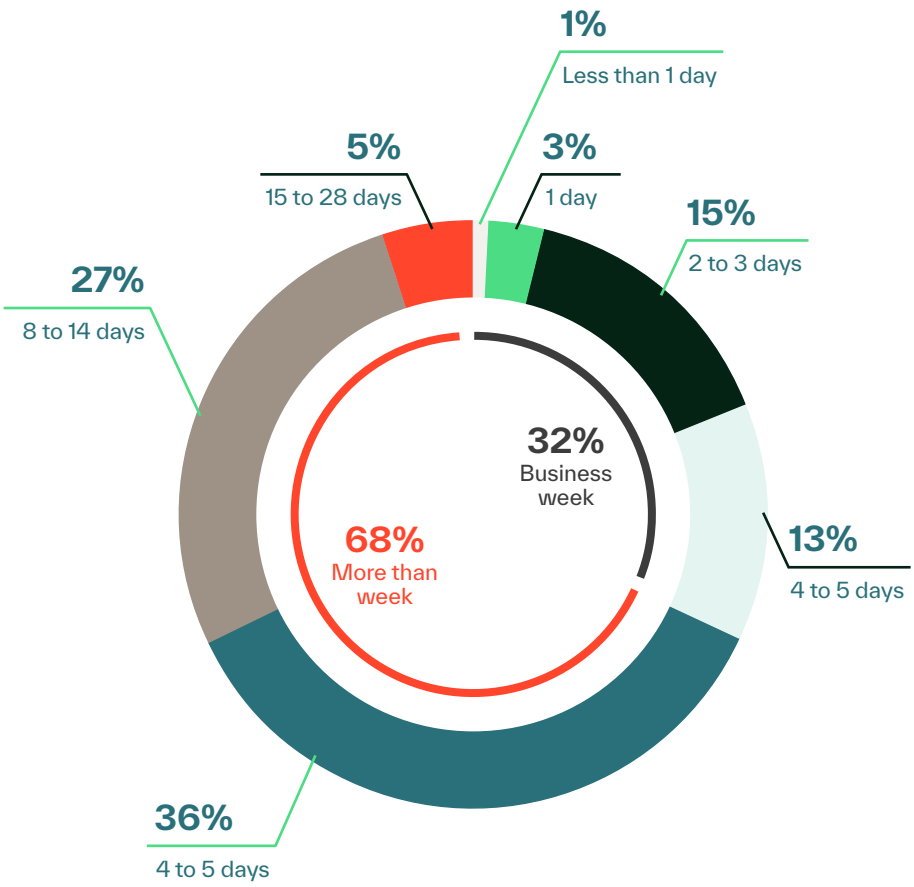


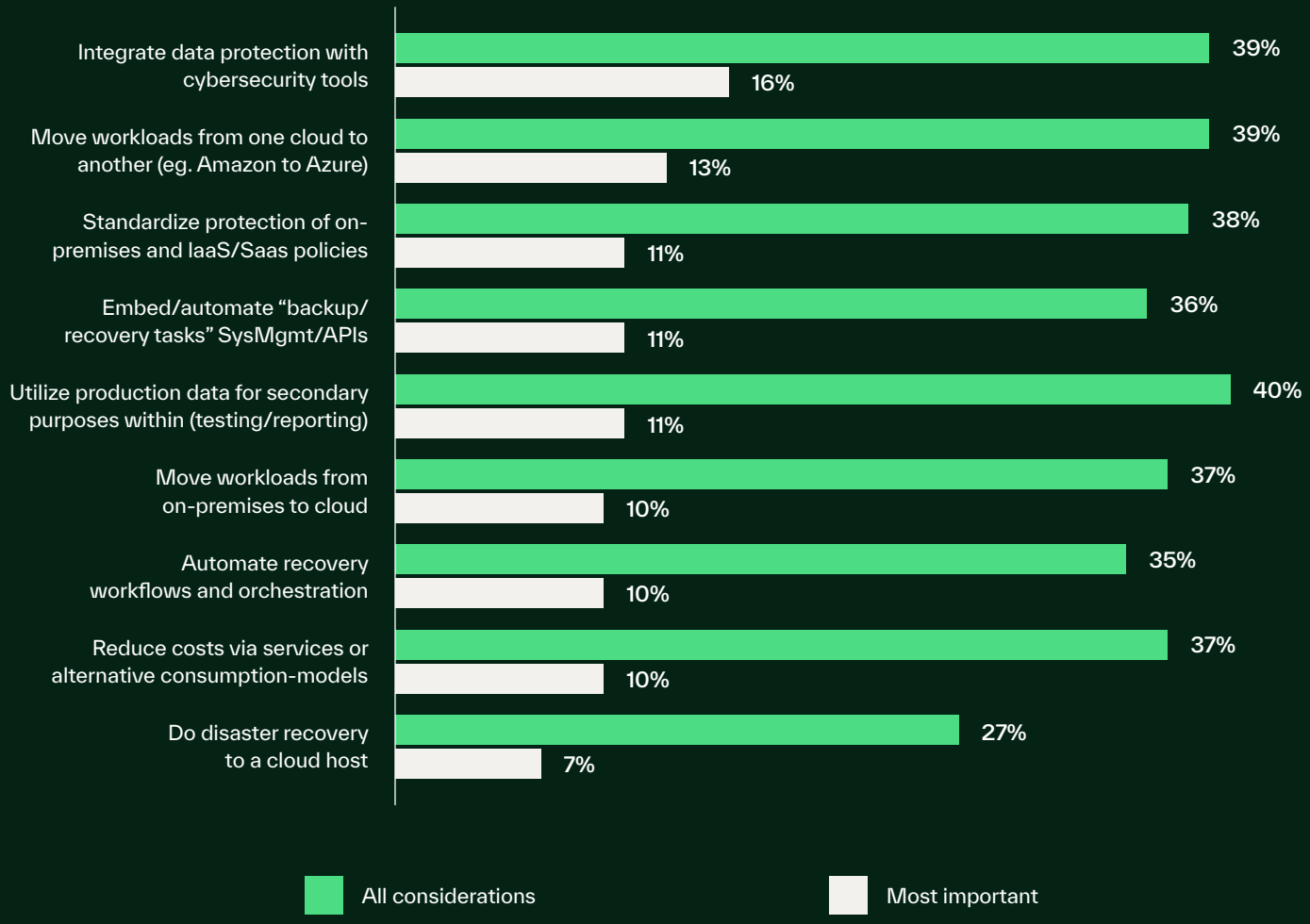
Image 2: Recovery time estimates after failover of 50 servers due to disaster or cyber event[1]

Shifting towards cyber resilience

To combat these attacks, organizations need to shift to a mindset of cyber resilience, which emphasizes the need for strong recovery capabilities. They require solutions and an approach that can effectively merge both data protection and cybersecurity practices.

Emphasizing this point, when Veeam asked respondents what they considered to be the defining aspects of modern or innovative data protection solutions for their organizations, the ability to integrate data protection with cybersecurity tools ranked as the most important (Chart C).

Which would you consider to be defining aspects of a "modern" or "innovative" data protection solution for your organization? Most important?



https://vee.am/DPR24

Data Protection Trends 2024 Report-published by Veeam in January 2024
N=1,200 unbiased IT Leaders and implementers responsible for their organizations data protection strategies.

Image 3: Which do you consider the defining aspects of a "modern" or "innovative" data protection solution?[1]

A strong approach that combines data protection and cybersecurity toolsets with the expertise to implement and manage solutions will help organizations ensure they can anticipate, protect against, withstand, and, importantly, recover from attacks.

However, integrating data protection with cybersecurity tools requires specific skills. That makes the fact that nearly half (47%) of the surveyed IT leaders and implementers for data protection intend to seek a new job outside of their current organization rather concerning. In contrast, just 1 in 3 intend to remain in role or organization, while another 1 in 5 are undecided. Veeam rightly notes that it's incumbent on senior leadership to retain their existing data protection talent, to ensure their preparedness for cyber resiliency and other disaster preparation. Losing those experts puts the organization at a significant disadvantage when crises inevitably strike.

Also crucial, and in addition to retaining existing expertise, is recruiting data protection talent that brings new skills in safeguarding the hardening of data protection against cyber criminals. Likewise, it is key to acquire new knowledge to protect modern production workloads that reside in clouds (such as those using Microsoft 365®), Kubernetes containers, or other IaaS and PaaS architectures.

The value of Kyndryl and Veeam

Together, Kyndryl and Veeam can bring solutions and services that help bridge the gap between data protection and cybersecurity under the banner of cyber resilience. Veeam's market-leading solution is able to deliver:

— Comprehensive backup and recovery: Veeam provides backup and recovery capabilities for all major workloads, including virtual machines (VMs), physical servers, cloud instances, and modern workloads like containers and Kubernetes.

— Cloud data management: Veeam offers seamless integration with major public cloud providers (for example, AWS, Microsoft Azure®, Google Cloud) for backup, recovery and data mobility across hybrid cloud environments.

— Ransomware protection: Veeam solutions incorporate advanced features like immutable backups, air-gapped repositories, and security-rich restoration to help protect against ransomware attacks and help ensure data recoverability.

— Intelligent data management: With capabilities like capacity planning, data analytics, and automation, Veeam enables organizations to intelligently manage their data across its lifecycle, optimizing storage utilization and helping to reduce costs.

— High-speed recovery: Veeam Instant Recovery and Instant Restore technologies allow for near-instantaneous recovery of VMs, databases, and individual items, minimizing downtime and data loss.

— Centralized management: Veeam provides a centralized management console for monitoring, reporting, and managing backup and recovery operations across the entire IT environment, simplifying administration and helping ensure compliance.

— Scalability and flexibility: Veeam solutions are designed to scale seamlessly, supporting large and distributed environments while offering flexible deployment options (on-premises, cloud or hybrid).

With Kyndryl, the world's largest IT infrastructure services provider, customers can receive the platform and expertise to prepare their organizations for disruptions, thereby bolstering their ability to transform continually. Kyndryl is named a Leader in the 2024 NelsonHall NEAT vendor evaluation for Cyber Resiliency Services in the Overall, Cyber Consulting & Strategy Construction, Incident Response & Backup Services, and Managed Cyber Security Services market segments.

Together, Kyndryl and Veeam can bring solutions and services that help bridge the gap between data protection and cybersecurity under the banner of cyber resilience. We believe that Veeam, an eight-time Gartner®3 Magic Quadrant™ Leader for Enterprise Backup and Recovery Software Solutions, offers comprehensive high-speed backup and recovery solutions that help organizations protect against ransomware and other IT outages through a scalable centralized management platform.

About the report

The 2024 Data Protection Trends report is Veeam Insight's fifth annual issue. It summarizes data protection strategies spanning from 2020 to 2026 gathered from more than 13,000 organizations. The survey included 1,200 business and IT leaders who were asked about their IT and data protection plans and strategies. Register for a complimentary copy of the Veeam 2024 Data Protection Trends report.

About Veeam Software

Veeam's solutions are designed to protect cloud, virtual, physical, SaaS and Kubernetes workloads with fast recovery from any cyber-attack, reducing risk and accelerating ransomware recovery. The company helps organizations get back to business without paying ransom. Veeam counts 77% of the Fortune 500 as its customers.

Why Kyndryl?

Kyndryl designs, builds and manages the systems that the world depends on every day, serving thousands of enterprise customers in more than 60 countries. We offer deep expertise in securing complex mission-critical systems. Kyndryl helps businesses become operationally resilient, building trust and mitigating enterprise risks through our integrated security and resiliency framework, and strong knowledge of cyber resilience and regulations. Kyndryl Cyber Resilience Services helps customers through integrated services designed for end-to-end protection and resilience.

Learn more

Kyndryl and Veeam Software together deliver cyber resiliency solutions, including backup, recovery, automation and innovation for hybrid and multi-cloud environments. Find out more about the Kyndryl and Veeam alliance, or visit kyndryl.com.

1 The 2024 Data Protection Trends report, Veeam Insights *https://go.veeam.com/wp-data-protection-trends-2024*

2 NEAT vendor evaluation for Cyber Resiliency Services in the Overall, Cyber Consulting & Strategy Construction, Incident Response & Backup Services, and Managed Cyber Security Services market segments NelsonHall, 2024 *https://www.kyndryl.com/content/dam/kyndrylprogram/cs_ar_as/cyber-resiliency-neat.pdf*

3 Gartner, Magic Quadrant for Enterprise Backup and Recovery Software Solutions, Michael Hoeck, Jason Donham, Chandra Mukhyala, Rene Rodriguez, 6th August 2024. The name of the report was changed from Magic Quadrant for Data Center Backup and Recovery Software in 2016 to Magic Quadrant for Data Center Backup and Recovery Solutions in 2017 and to Magic Quadrant for Enterprise Backup and Recovery Software Solutions in 2021.