kyndryl

Unblocking Cyber Resilience: The Power of Mass Recovery Modeling

Contents

Executive summary

In an era where cyber incidents are not a matter of if but when, understanding recovery times is crucial for business continuity, it's not uncommon for businesses to assume that recovery will take a matter of hours when, in reality, it can require weeks. This creates a dangerous gap in business continuity planning, putting companies at real risk of operational disruption, financial losses, reputational damage, and regulatory non-compliance.

At Kyndryl, we believe accurately predicting recovery times for groups of business systems is a vital pillar of any modern cyber resilience strategy. However, as enterprise IT environments grow more complex and interconnected, gaining this level of awareness can be challenging.

This motivation prompted the development of Mass Recovery Modeling (MRM). Our methodology is thorough: we gather data from across the backup and recovery ecosystem, subsequently employing sophisticated techniques to accurately forecast system restoration timelines during significant incidents. Such incidents may encompass cyberattacks or conventional disasters, such as data center inundations or fires.

MRM extends beyond the scope of individual recovery time objectives (RTOs) to encompass the intricate dynamics of multiple interconnected systems in the context of mass recovery scenarios.

This insight enables organizations to enhance their capacity to respond quickly and effectively to cyber incidents. As the likelihood of such incidents continues to rise, MRM provides a robust solution that helps businesses tackle these challenges directly. This minimizes the adverse effects of cyber disruptions, ultimately reinforcing their stability, growth, and competitiveness.

Introduction

Imagine a global enterprise brought to a standstill by a cyberattack, struggling for weeks to restore operations. This scenario underscores the critical need for accurate recovery time prediction.

With threats on the rise, it's not a question of whether an organization will experience an adverse event but when. This makes it paramount for businesses to embrace cyber resilience as a cornerstone of their IT and operational strategy.

Cyber resilience goes beyond traditional cybersecurity, focusing not just on protecting data and systems but also on ensuring business continuity after a cyber incident. It's a proactive approach to mitigating risk, giving organizations the ability to anticipate, protect against, withstand, and recover from any cyber-related event.

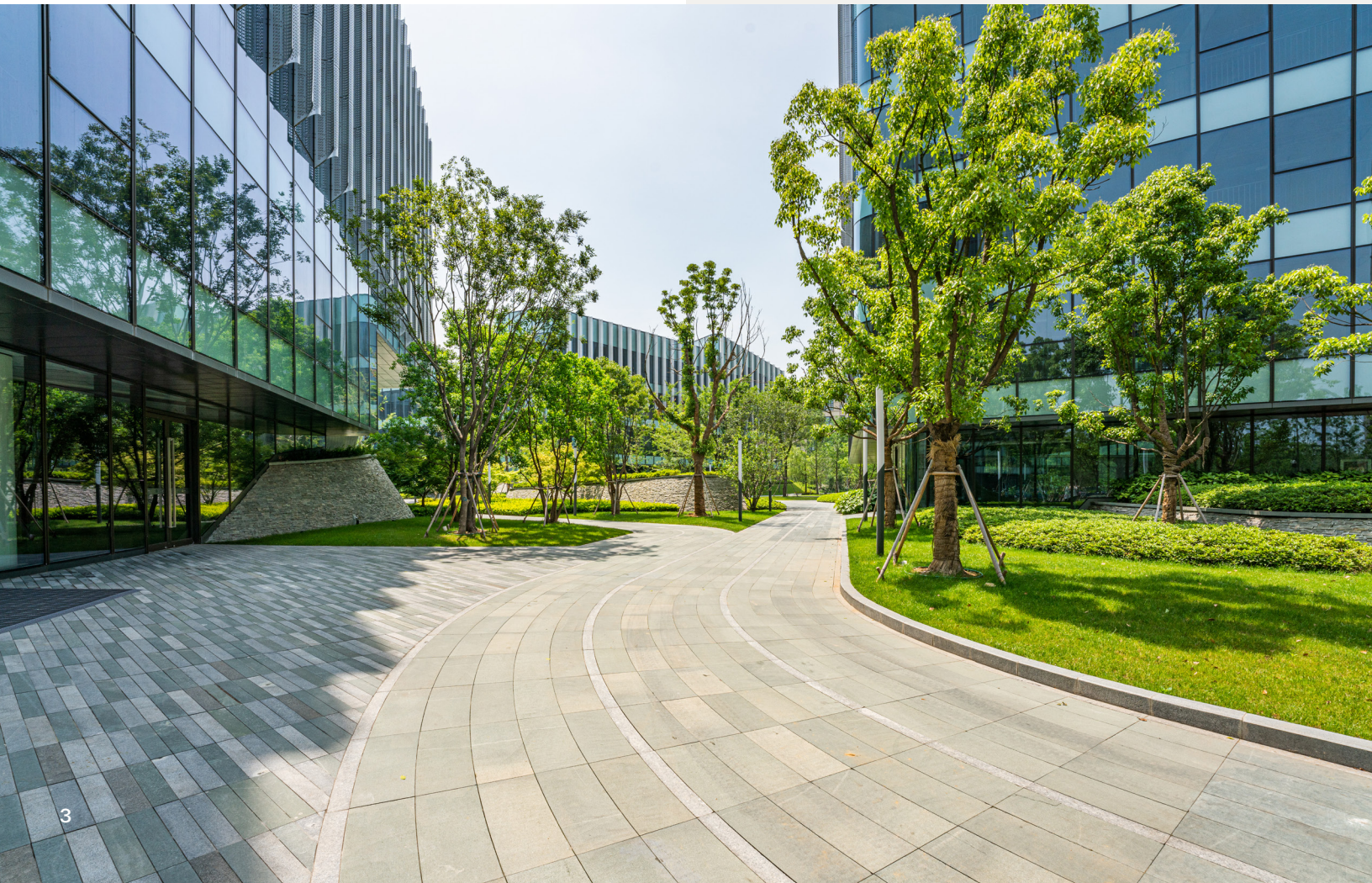
Predicting recovery time is crucial for maintaining cyber resilience and ensuring overall business continuity. Most companies are well aware of the threats that cyberattacks or other significant incidents pose to their operations. However, far fewer understand how long it will take to fully restore systems and data after such an attack or incident.

This represents a significant oversight. The longer an organization takes to contain and resolve a security incident or disaster, the greater the costs in lost revenue, reduced productivity, and reputational harm.

Shaping a solid recovery strategy requires more than simply understanding the RTO for individual systems. When a major incident disrupts multiple interconnected systems, it can often take significantly longer to restore full operations than individual RTOs might indicate. This is where a mass recovery model can truly make a difference.

Mass Recovery Modeling provides significant advantages by enabling timely and comprehensive data restoration during major disasters or cyber-attacks. Kyndryl's approach to MRM employs techniques to offer a clearer understanding of backup and recovery capabilities while accurately estimating the probable time to fully recover from a major incident.

In this paper, we examine the forces driving the need for increased cyber resilience, the challenges to accurately calculating recovery times, and how Kyndryl harnesses years of experiences to deliver effective cyber assessments.



Market trends

Cyber resilience as a strategy

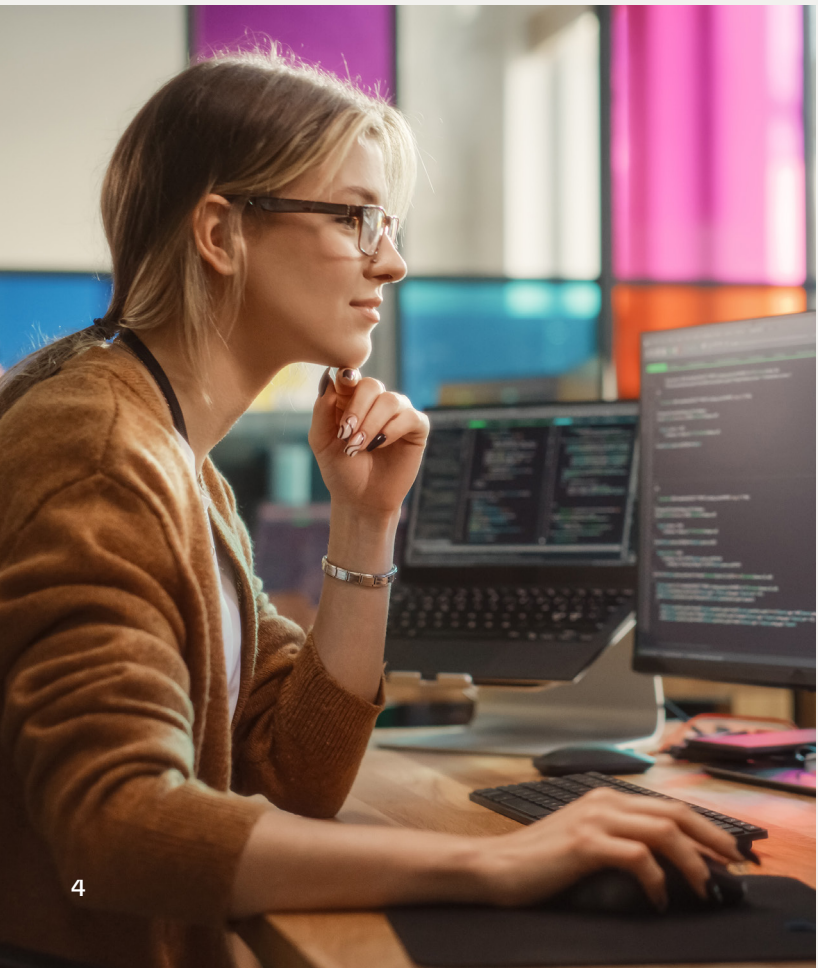
Based on a Kyndryl survey with a worldwide panel of IT decision makers and risk and compliance professionals, 71% of respondents said they have experienced a cybersecurity-related event.[1] The traditional reactive defense model—characterized by perimeter protection and incident response—is giving way to a more holistic strategy that prioritizes continuous adaptation, rapid recovery, and comprehensive business continuity.

This transition necessitates a fundamental rethinking of how organizations protect digital assets and secure critical information in an increasingly unpredictable threat landscape. Cyber incident recovery has emerged as a vital part of this strategy, enabling businesses to decrease downtime and lessen the business impact of cyber-related disruptions.

Changing regulatory landscape

Businesses must adapt their cybersecurity strategies to ensure compliance with emerging national and regional regulations. One of the most recent regulations is the EU's Digital Operational Resilience Act (DORA), which went into effect in early 2025.

Focusing on the financial services sector, DORA and other worldwide cyber requlations aims to ensure that firms can withstand, respond to, and recover from various operational disruptions and threats. It mandates financial institutions to establish robust resilience frameworks, including comprehensive cyber recovery strategies.



Inaccurate RTOs threaten business continuity

The rapid recovery of enterprise data and systems is crucial for cyber resilience. However, RTOs can vary significantly across a company's operations. At Kyndryl, we frequently collaborate with customers whose IT environments encompass tens to hundreds of millions of files, databases, or extensive collections of virtual machines. Many of these customers are unaware of how long it will take to fully recover their systems until they confront a large-scale disaster or security incident firsthand.

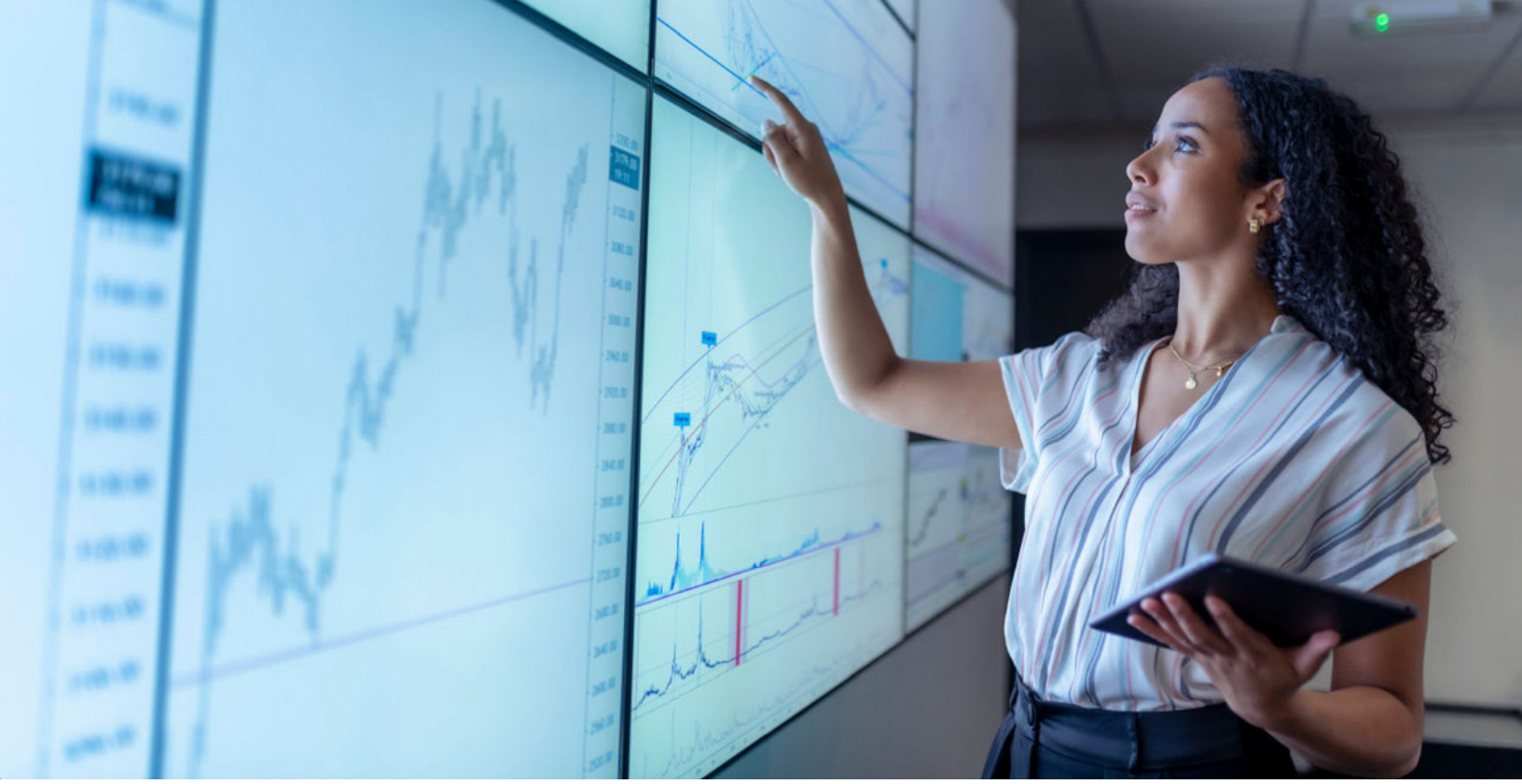
Companies often assume they are comfortable with how long a restore will take. They expect that if they've invested in backup and replication solutions, it will take only hours to return to normal operations. However, most companies can only restore their environment over the course of weeks.

This mismatch is often caused by incorrect assumptions regarding underlying data recovery, server, and network capabilities. Commonly, recovery strategies rely on sending snapshots or backups of files, databases, and similar objects across networks (VLAN or SAN) to backup servers.

Therefore, the overall speed of backup and recovery is highly dependent on the capacity of the underlying server, network, and storage systems. Competing demands on these resources can significantly extend recovery times when multiple systems need to be restored simultaneously.

When companies make assumptions about recovery times based on isolated, per-system RTOs, they run a significant risk of failing to recover data and servers swiftly in the event of a mass failure or attack. The potential consequences are severe: missed RTOs, compliance targets, and service-level agreements (SLAs), as well as data loss and downtime that lead to high costs in productivity and revenue.

Organizations require a better method to measure real-world recovery times, enabling them to understand their risks and invest in the necessary infrastructure to meet their objectives. MRM provides a valuable approach to gaining this level of insight.



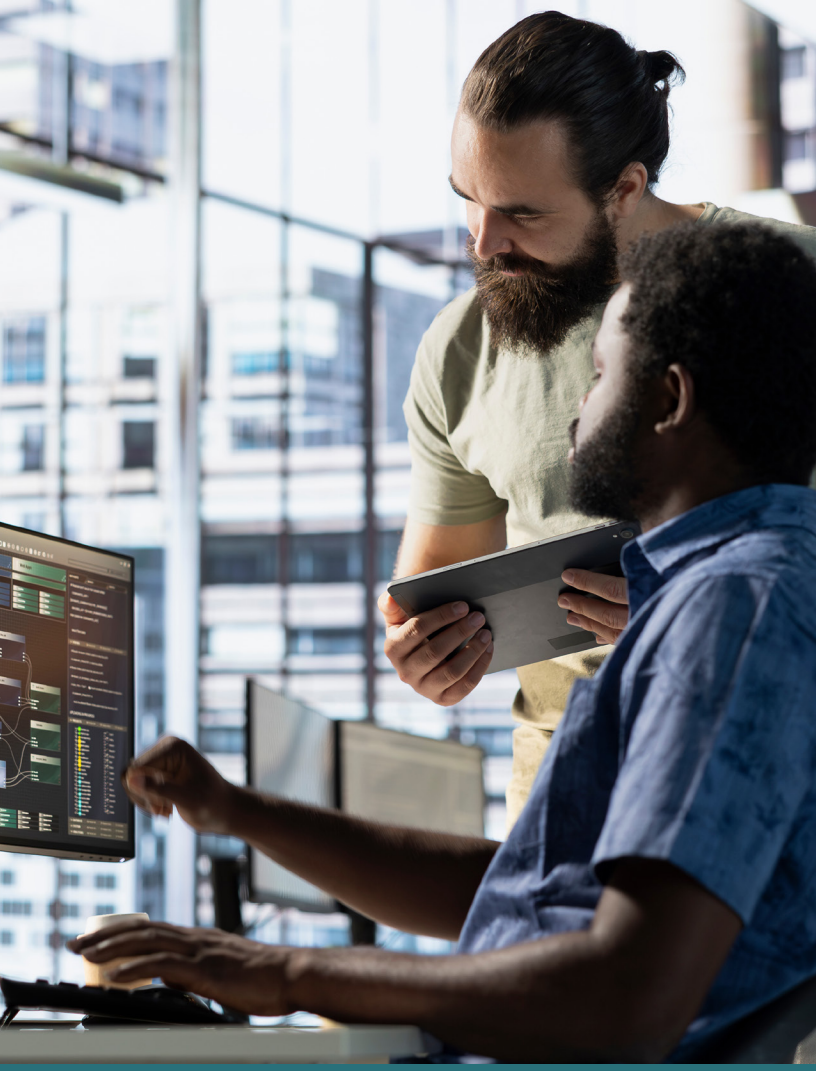
Kyndryl's approach

Kyndryl's MRM approach provides insight into the real-world time required to perform backups and restorations for a selected data group. We analyze various factors influencing recovery time, such as data volume, storage location, network bandwidth, and storage performance. Our extensive roster of hosted customers worldwide offers us a uniquely rich dataset regarding predicted and actual recovery times, which informs our analytics and enhances the accuracy of our forecasts.

This approach enables us to create a highly accurate estimate of recovery times. Customers can then use this as a baseline to evaluate whether their current data and server recovery capabilities meet business requirements related to RTO and other SLAs. They also gain insight into what changes can be implemented in their environment to accelerate recovery and enhance business continuity. With a clearer understanding of how systems will compete for limited resources during recovery, organizations can also enhance their planning to prioritize the recovery of their most critical systems first.

When collaborating with customers to implement MRM, we generally adhere to a seven-step process:

1. **Risk Assessment:** Conduct thorough risk assessments to identify vulnerabilities and potential threats.
2. **Technology evaluation:** Evaluate the effectiveness of existing technologies and tools used for cyber recovery.
3. **Compliance review:** Ensure that recovery strategies comply with relevant regulations and industry standards.
4. **Process review:** Review the processes for data backup and recovery to ensure they are robust and can handle various types of incidents.
5. **Critical systems first:** Prioritize recovery efforts for critical systems and data that are essential for business operations.
6. **Data collection:** Collect data from backup and recovery environments. We gather information from multiple hardware and software components, including servers, restore sources, software configurations, and restore targets, and combine this information with data points on network bandwidth and historical recovery times.
7. **Predictive modeling:** Based on our analysis, we estimate recovery times for various scenarios and combinations of systems. These models can provide precise recovery time values or specified recovery time ranges, such as 1-5 hours. Customers can evaluate different methods and their effects on recovery times, enabling them to assess the trade-off between recovery speed and depth of protection more effectively.



Case studies

At Kyndryl, we have assisted numerous organizations in successfully implementing recovery time prediction models. By applying MRM, these companies have gained a better understanding of recovery times for various applications and datasets, which empowers them to adapt their recovery strategies to minimize business disruption during cyber incidents and other large-scale disasters.

Suggested next steps

Creating a clearer understanding of RTOs is a vital step in enhancing recovery capabilities. For businesses seeking to achieve this visibility, Kyndryl suggests:

- Applying MRM to achieve a more comprehensive understanding of real-world RTO and its alignment with business requirements.
- Periodically validating the data protection architecture RTO, especially after upgrades and major system changes.
- Scheduling regular consultations with Kyndryl to remain informed about the latest recovery techniques and technologies. This involves implementing actionable recommendations to enhance recovery strategies using operational insights from Kyndryl Bridge.

Conclusion

In today's escalating threat landscape, accurately predicting recovery time is not just good practice—it's a business imperative. Organizations that continue to base their recovery strategies on assumptions rather than data are operating with a perilous blind spot.

Kyndryl's MRM provides the visibility and precision companies need to make informed decisions about backup and recovery. It helps them maintain business continuity, meet increasingly stringent regulatory requirements, and minimize the financial and reputational impacts of cyber incidents.

Call to Action

Ready to enhance your cyber resilience? Contact Kyndryl today to discover how our Mass Recovery Modeling can safeguard your business.
kyndryl.com/us/en/services/cyber-resilience/incident-recovery

Talk to an expert about taking the next step in your cyber resilience journey.

Request a consultation

Authors

Adam Dutton
Associate Director, Security and Resilience

Adam Dutton is a principal consultant with over 20 years of experience in development, technical and operational management, and consulting

Allen R Downs
Vice President, Incident Recovery

Allen Downs is Vice President Incident Recovery Domain at Kyndryl, developing Cyber Recovery Strategy to address the cross Industry Critical Business Process Recovery

Emilio Griman
Vice President, Cyber Incident Recovery

Emilio Griman is leading the strategic technology investments and projects to support business growth, profitability, and risk reduction at Kyndryl

Mikael Lindström
Director, Principal Architect and Technology Advisor

Mikael Lindström is Director, Principal Architect and Technology Advisor and a subject matter expert on emerging technology, design elements, cyber recovery and data protection at Kyndryl

Sanjeev Gupta
Director – Sales Enablement and GTM Activation

Sanjeev Gupta is Director - Sales Enablement, GTM activation and an expert in Cyber Resilience, Data Center and IT Sustainability at Kyndryl

kyndryl

[1] ***Survey findings: What IT decision makers say about the state of IT risk***, Kyndryl 2023