The Business Value of Kyndryl's DRaaS and Resilience Orchestration Services

RESEARCH BY:

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

Phil Goodwin
Research Director, Infrastructure Systems,
Platforms and Technologies Group, IDC

Matthew Marden
Research Director,
Business Value Strategy Practice, IDC

March 2020 | IDC Doc. #US46022820

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

BUSINESS VALUE HIGHLIGHTS

Click on highlights below to navigate to related content within this PDF.

507%
three-year ROI

24%
more efficient business continuity teams

43%
improvement in RPO

80%
lower cost of business risk and lost productivity and revenue

80%
Hours of lost productive time per year per user

38%
reduced risk of major impactful security event

27%
more efficient cybersecurity teams

12%
more efficient IT infrastructure teams

Executive Summary

Today's digitally transforming enterprises find it imperative to take a holistic view of their business continuance (BC) efforts. Data is the fuel of digital transformation. The absence of fuel is the absence of revenue, making data availability critical to organizational success. Data must be defended and recoverable against a range of threats, from accidental deletion to system failures, natural disasters, employee sabotage, and cyberattacks. Moreover, given that organizations commonly have data spread across on-premises, public cloud, and edge repositories, it is crucial that organizations factor hybrid cloud and multicloud recovery capabilities in their BC planning.

The concepts of business continuance, disaster recovery (DR), and cyber-resilience are classic cases of people, process, and technology. Technology alone is not enough — organizations must consider all three factors to meet business objectives. Digital transformation has fundamentally evolved the execution of the task as the complexity associated with 3rd Platform technologies (i.e., the transition from 2nd Platform [client/server] to virtual infrastructure) such as hybrid multicloud and business operations dependencies on data makes recovery orchestration a "must-have."

IDC best practices recommend that organizations monitor three key metrics regarding data recovery and availability: recovery point objective (RPO), recovery time objective (RTO), and total downtime. IDC research has found the average downtime cost is $48,7001 per critical workload per hour.

Of course, this will vary widely by industry and organizational size and can be millions of dollars per hour for large OLTP financial environments. For this white paper, commissioned by Kyndryl, formerly IBM Infrastructure Services, IDC interviewed organizations that made clear that improvements in downtime can yield significant value that leads to much improved return on investment (ROI).

IDC interviewed organizations using Kyndryl Resiliency Orchestration and/or Kyndryl Orchestrated Disaster Recovery as a Service (collectively referred to as "Kyndryl services" or "Kyndryl") to understand the impact in terms of maintaining business continuity, ensuring data security, and managing operational risk. These Kyndryl customers described achieving more

1. IDC's *Server and Storage Infrastructure Availability Survey*, December 2018

robust and secure business operations while minimizing operational burdens on their IT teams. These benefits carry significant value for these organizations, which IDC quantifies as having an overall value in terms of staff time savings and productivity gains, higher revenue, and lower costs worth an average of $7.65 million per organization per year in these areas:

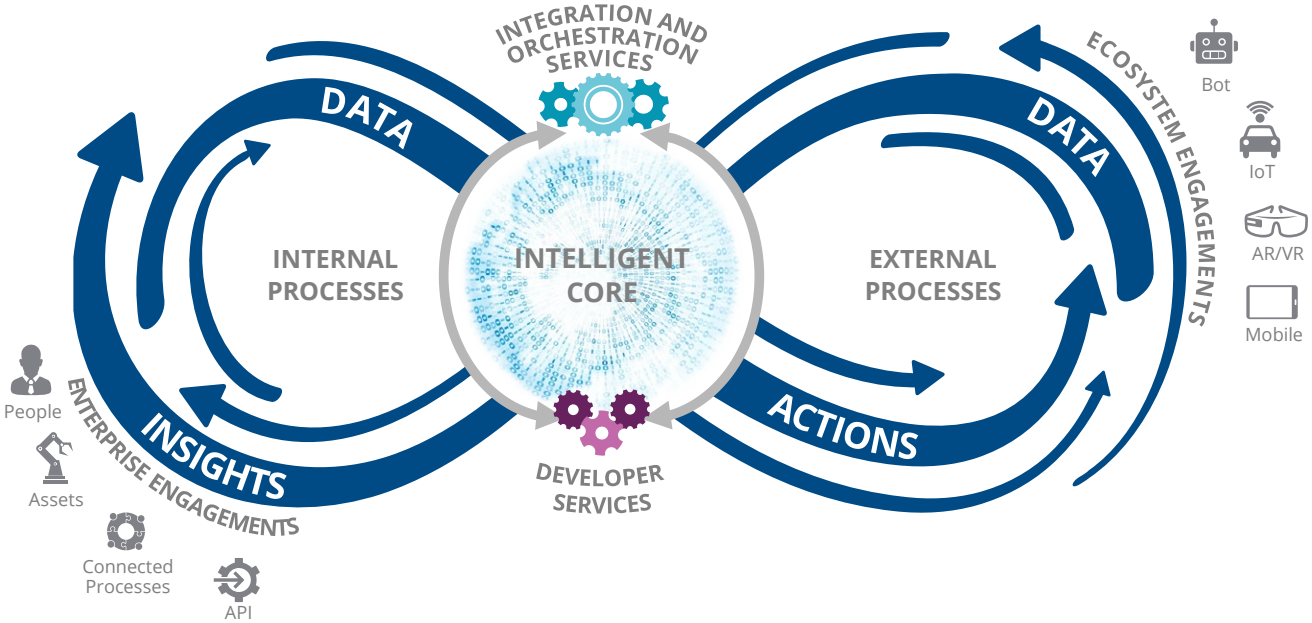
- **Ensuring business continuity** with robust and efficient data backup and recovery capabilities that can keep up with the speed of their businesses
- **Minimizing business operational risk** associated with unplanned outages and data loss, thereby reducing the cost of risk in terms of productivity and revenue losses
- **Making broader IT operations** more efficient and cost effective by providing an IT environment that requires less repetitious staff work and redundant investment in IT infrastructure

Situation Overview

All over the world, enterprises are steadily making their way through digital transformation — the process of integrating technology with all aspects of the business to accelerate business activities, support agility, and capitalize on strategic vision and dynamic opportunities. A key element of digital transformation is becoming a data-centric organization capable of monetizing information. Essentially, hardware, software, and applications are the "factory" of digital transformation; data is the fuel (see **Figure 1**).

FIGURE 1

Digital Transformation Causing an Exponential Jump in Complexity



Source: IDC, 2021

At the same time, digital transformation inherently brings with it new risks that may have been previously unforeseen or that may have complicated the risk profile of well-established business processes. As a result, enterprises seek higher levels of integration between key business support functions and greater data availability to ensure that the business is ready to withstand any type of IT incident or disaster, software or hardware failures, human errors, supplier failures, natural or man-made disasters, and now the growing risk of cyberattacks, which require us to address the new world of cyber-resilience.

Cyber-resilience in the context of digital transformation is more than a product — it is an integrated approach, demanding a new approach of data protection and disaster recovery. Remember, although digital transformation leverages technology to improve business agility and customer impact, the IT impact has significantly increased management complexity. Thus hybrid and multicloud architectures create corresponding complexity for business continuity. Although the public cloud vendors have remarkable uptime, even they have suffered outages and disruptions, resulting in the desire to move from one cloud to another or one region to another. Frankly, having a single cloud provider is an oddity. The business continuity and disaster recovery challenges of cyber-resilience in a digital transformation context include:

- Lack of skills to orchestrate DR operations within the target RPO/RTO
- Inability to fail over a system between on-prem legacy and cloud or between clouds
- Inability to test recovery plan for data spread across legacy infrastructure and clouds
- Lack of cybersecurity skills and confidence to recover from cyberoutages
- High operational costs, including data egress charges
- Lack of monitoring, visibility, and control for governance and compliance

The differentiator — and indeed a requirement — in business continuance offerings is orchestration, which can both simplify hybrid and multicloud recovery and speed the recovery through process automation. Clearly, the complexity of the task demands a programmatic approach to data protection and recovery in the event of a catastrophic event. Time to recover becomes paramount. Data is the fuel of digital transformation. Without that fuel, businesses cease to run, crippling revenue generation and exposing the organization to business risk. The components of a digital transformation cyber-resilience framework are:

- **Identify:** Critical asset and process mapping, risk and readiness assessment, and so forth
- **Protect:** Traditional first-line cybersecurity defenses, blocking known or easily detectable malicious activity
- **Detect:** Security analytics
- **Respond:** Response to security breaches or failure
- **Recover:** Coordinated recovery mechanisms
- **Orchestrate and automate:** Time matters!

Kyndryl's DRaaS and Resilience Orchestration Services Overview

Kyndryl is in a rather unique position, being able to apply business continuance, IT transformation, orchestration, and backup and recovery expertise to business continuance. Kyndryl has over 9,000 customers protected by its disaster recovery and data management services. Annually, it backs up over 3.5 exabytes (EB) of data across 300 Kyndryl Resiliency centers in more than 60 countries.

As Kyndryl looks to deliver business continuance and cyber-resilience services to its clients, five key technologies resonate:

- **Orchestration and automation.** Digital transformation measures downtime in terms of lost revenue; orchestration minimizes restoration times and, by default, lost revenue from data corruption/loss. Manual processes are replaced with predetermined workflows, minimizing complexity and recovery error.
- **Immutable storage.** Write once, read many (WORM) storage prevents changes to be made to backups once they are saved. The approach can reduce storage costs by only writing new copies of point-in-time (PIT) incremental changes.
- **Air-gapped protection.** Isolation separates production environments from the backed-up data at a remote site. The approach prevents protected data from being corrupted by laterally moving malware.
- **PIT copies and data verification.** Point-in-time copies and data verification ensure the configurations and data being protected are valid. This process measures when configurations and data do not match the "golden" versions.
- **Hybrid and multicloud protection and recovery capabilities.**

The Business Value of Kyndryl's DRaaS and Resilience Orchestration Services

Study Demographics

IDC interviewed organizations about their efforts to ensure business continuity and minimize operational risk with Kyndryl's services. Interviews were in-depth in nature and focused on understanding the qualitative and quantitative results achieved by these Kyndryl customers. Study participants had a profile on average of a large enterprise with 56,697 employees and annual revenue of $30.37 billion. They provided experiences from North America and APAC and from a mix of industry verticals, including education (2), financial services (2), healthcare (1), service provider (2), and telecommunications (1), that face challenges in ensuring business continuity and minimizing operational risk that are both common and unique in nature (see **Table 1**).

TABLE 1

Firmographics of Interviewed Organizations

Firmographics	Average	Range
Number of employees	56,697	450 to 256,000
Number of IT staff	2,318	15 to 12,500
Number of business applications	683	6 to 4,500
Revenue per year	$30.37B	$6M to $130B
Countries	United States (7) and Japan (1)	
Industries	Education (2), financial services (2), healthcare (1), service provider (2), and telecommunications (1)	

n = 8, Source: IDC, 2021

Choice and Use of Kyndryl's DRaaS and Resilience Orchestration Services

Interviewed organizations described various considerations in deciding to use Kyndryl's services, including Kyndryl Resiliency Orchestration and/or Kyndryl Orchestrated Disaster Recovery as a Service, but their decisions traced back to needing to ensure business continuity and reduce risk related to data and operations. They know that data-related outages, breaches, and security events can carry not only significant tangible costs in fines, lost revenue, and lower productivity but more intangible costs such as reputation damage and insufficiently responsive business operations that are more challenging to quantify but equally if not more costly. Interviewed Kyndryl customers described the following key points in selecting Kyndryl services:

- **Need to avoid repeating impactful outage:** *"We had some downtime as a result of some viruses that got into our systems . . . We were looking for a solution with Kyndryl's services that would help us be more proactive and help provide us with some consistency in terms of availability."*
- **Supporting uptime for critical systems and applications:** *"We're using Kyndryl Orchestrated Disaster Recovery as a Service because we have certain services that we consider critical that need to have 100% uptime. And so those are our services that we duplicate with the Kyndryl services and we use the orchestration manager to make sure that as new systems come onboard, they meet those same requirements."*
- **Automating to single point of recovery and real-time visibility with dashboard:** *"Our goal with Kyndryl's services was really to automate for more of a single-point recovery if we experience downtime. If we need to bring up a backup, we needed to be able to do that quicker. We also needed to be able to have more robust reporting and have access to a dashboard view of what our environment looks like in real time."*

Study participants moved to Kyndryl services from a variety of vendor solutions and internally developed and supported activities. They invested in these Kyndryl services to support various business-critical applications, including payroll and finance applications, medical records systems, ERP activities, and contact center operations, among others. They are using Kyndryl's services to support a mix of on-premises and cloud-delivered applications, with an average of around 60% of applications run on premises, 30% in a private cloud, and 10% in the public cloud.
All interviewed organizations reported using Kyndryl Resiliency Orchestration services, and six organizations were using Kyndryl Orchestrated Disaster Recovery as a Service at the time of their interviews.

Table 2 suggests the central role of these Kyndryl services for these organizations in providing business resiliency and security for significant numbers of users (40,698 on average), applications (30), virtual servers (793), and storage environments (1,097TB).

TABLE 2

Use of Kyndryl's Services by Interviewed Customers

	Average	Range
Number of applications	30	3 to 125
Number of users of applications	40,698	338 to 128,000
Number of datacenters	19	1 to 113
Number of physical servers	264	2 to 1,500
Number of virtual machines	793	2 to 1,500
Number of terabytes	1,097	2 to 6,125

n = 8, Source: IDC, 2021

Business Value and Quantified Benefits

Interviewed organizations returned repeatedly in interviews to the themes of improving business continuity and minimizing operational risk with Kyndryl's services. They realized that they had to find a way to reduce both quantifiable and less tangible costs associated with outages, breaches, and data loss, and they have achieved this goal with Kyndryl's services. Study participants described the core benefits of using Kyndryl's services:

- **More robust business operations:** *"If I had to name four things that we benefit with from Kyndryl's services — and these are recurring — they are reduced risk, high availability, very high efficiency, and business confidence."*
- **Automation and proactive diagnosis to reduce potential for impactful outages and problems:** "*For us, IT resiliency means the ability to automate and to proactively diagnose issues before they become known to our users and to prevent and reduce downtime as much as possible . . . Right now, Kyndryl's services are right in line with what our expectations are, and the service level has really exceeded our expectations."*

- **Optimization of backup performance in support of reducing operational risk:** *"One of the biggest benefits of using Kyndryl's services is that we can optimize our backup performance, which makes our IT operations more efficient through automated backup and reporting and alerts. Because it's automated and centralized, it helps us better preempt and manage information risk."*

Use of Kyndryl's services has enabled interviewed organizations to achieve significant value through the reduction of risk-related costs and by enabling teams responsible for ensuring business continuity to work more efficiently and effectively and minimizing risk. To understand the relative value of investment in Kyndryl's services, IDC quantified the value attributed to these services based on in-depth interviews for this study. IDC calculates that these benefits will be worth an average total of $7.65 million per year per interviewed organization in the following areas:

- **Risk mitigation — user productivity benefits.** Study participants have substantially limited risk associated with unplanned outages and data loss with Kyndryl's services, thereby improving productivity and reducing revenue losses. On average, IDC calculates that they have lowered these risk-related costs by 80% while also enabling compliance teams to work more efficiently, which translates to an average annual value of $3.24 million per organization.
- **IT staff productivity benefits.** Study participants have enabled teams responsible for business continuity, security, infrastructure, and supporting operations to work more efficiently with Kyndryl's services. IDC projects that these IT staff efficiencies will have a value of $4.36 million per organization per year.
- **Cost reductions.** Study participants have been able to consolidate their infrastructure environments with Kyndryl's services as they have improved their security postures, thereby saving an average of $48,400 per organization per year in costs associated with running their IT environments.

Improving Business Continuity and Security

Study participants can ill afford to allow outages, security breaches, data loss, or other events to affect their ability to ensure business continuity. Their businesses require consistent delivery and high performance of applications and services, and disruptions carry real and tangible costs to the business. Further, the potential loss of customer data or other significant security breach not only carries substantial costs in terms of lost revenue or fines but also reputational damage that can potentially cause longer-term damage to business success. An interviewed financial services organization described the all-too-real risk outages or data loss pose to its business and how it leverages Kyndryl's services to minimize this risk: *"If customer information were exposed, it could be catastrophic if it hits the news. There would be a very expensive cost to that, we may have to pay for credit monitoring and could lose clients. The cost could be steep — in the millions . . . We have less risk with Kyndryl — we peg it at 40% reduced risk."*

Teams tasked with backing up voluminous amounts of data and executing robust and timely recovery efforts when data is lost are challenged by escalating amounts of data and the extent to which data-driven activities have become core to their organizations' business operations. As a result, organizations have not found it easy to help these teams keep up with the pace of business change, which creates either inefficiencies or exposure to data-related risk. Kyndryl's services help interviewed organizations minimize these types of risks in an efficient manner, beginning with teams responsible for ensuring business continuity.

Study participants reported that Kyndryl's services have significantly enabled their business continuity teams. They benefit from functionality such as automated reporting, dashboard tools, and digests, along with knowledge transfer, which helps them work more efficiently and effectively. One study participant commented: *"Kyndryl's services have had an impact on our data recovery and backup efforts because we've been able to establish best practices with a much more standard way of doing it across all lines of business instead of everyone going with their own model."* As shown in **Table 3**, business continuity teams at interviewed organizations are more efficient as a result, which IDC puts at an average efficiency of 24%.

TABLE 3

Business Continuity Staff Impact

	Before Kyndryl's Services	With Kyndryl's Services	Difference	Efficiency with Kyndryl
FTEs per year per organization	60.7	46.0	14.7	24%
Hours per 100 users per year	280.0	212.0	68.0	24%
Value of staff time required per organization per year for equivalent workloads ($M)	6.1	4.6	1.5	24%

n = 8, Source: IDC, 2021

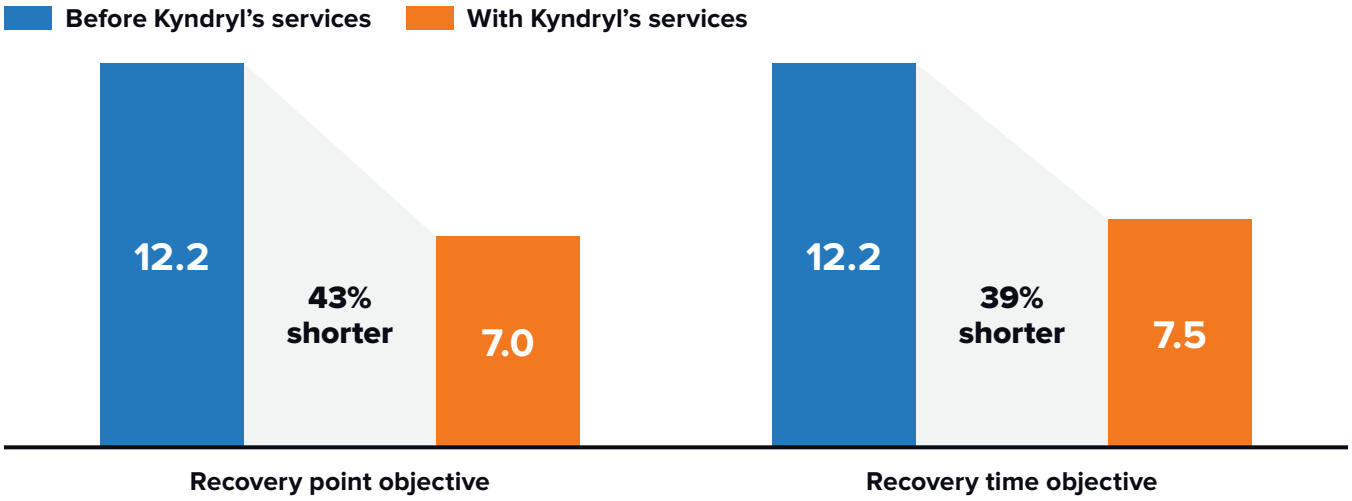
These staff efficiencies are evidenced by significant improvements in key metrics related to business continuity for business organizations. With Kyndryl's services, interviewed customers have improved their recovery point objectives and recovery time objectives (reductions of 43% and 39%, respectively, as shown in **Figure 2**), which minimizes data-related risk when recovery becomes necessary. Meanwhile, study participants also reported that they are completing 43% more data backups, going from an average of 64% to 92% completed within their time objectives, reducing the likelihood that backups either will not complete or will affect ongoing business activities. Study participants spoke to these benefits:

- **More effective data protection teams and proactive responses to issues:** *"Our goal with Kyndryl's services was to cut our RTO by 10% and we've exceeded that in 10 months — we've gone from 1–2 days before to around five hours now . . . Really, our ability to get business-critical applications back online is what's important. We're able to be more proactive and to resolve issues before they become massive."*
- **Ability to support business with improved service-level agreement (SLA) performance:** *"There's been at least a 50% reduction in our RTO objective with Kyndryl's services. If you look at mission-critical applications with an hour of backup SLA, it previously took two hours for recovery, and we can now do it in half the time or less — 30 minutes to an hour."*

FIGURE 2

Key Business Continuity Metrics

(Hours)



n = 8, Source: IDC 2021

Importantly, study participants also translate capabilities gained with Kyndryl's services into more robust security postures and lower overall risk. Like business continuity teams, security teams, including cybersecurity-focused teams, have been strained to keep up with escalating volumes and complexity of attacks. This makes it even more important that these teams can correctly identify actual threats and take necessary action to defuse threats before they become impactful security events.

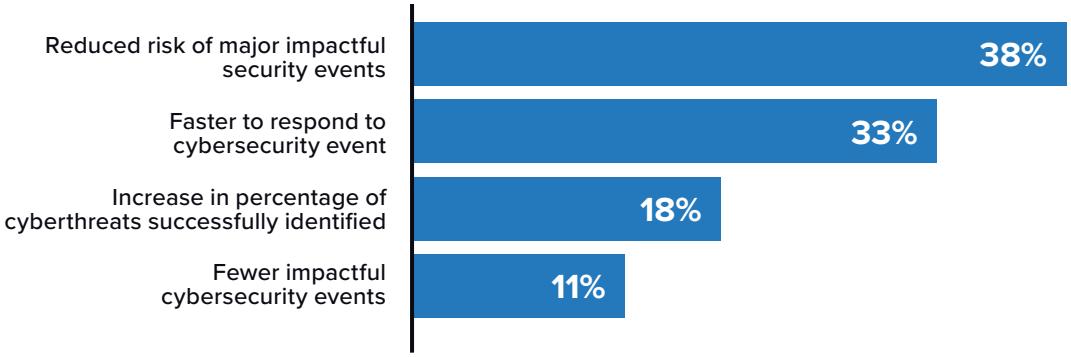
Interviewed Kyndryl customers spoke to the extent to which they have minimized risk related to these types of security events. One study participant explained: *"We can guarantee more higher uptime with Kyndryl's services and haven't had any data loss events in the past four years . . . For addressing cyberattacks, the services and tools that we have from Kyndryl identify when something like that is happening, which is very rare, and it is quicker than our previous systems."*

For interviewed organizations, this results in less risk from responding faster to potential cybersecurity events (33% faster on average) and successfully identifying more cybersecurity threats (18% more). This means both fewer impactful security events (11% fewer) and significantly lower levels of operational risk associated with such events that can carry significant costs. Study participants indicated a 38% lower risk of experiencing significant security events that carry an average total cost of $794,000 per event in terms of lost revenue, reduced productivity, potential fines, and other business operational losses. While interviewed organizations were not necessarily experiencing these types of events before using Kyndryl's services, the ability to further minimize the extent of such risk in a cost-effective and efficient way is very important to strengthening their overall security postures (see **Figure 3**).

FIGURE 3

Key Risk Metrics

(% of improvement)



n = 8, Source: IDC 2021

In addition to providing more robust data environments and security, study participants reported that use of Kyndryl's services has helped make their security teams — including cybersecurity teams — more efficient. With Kyndryl's services in place, these teams are more effective due to enhanced overall capabilities related to protecting data environments and can cover increasing demand from their businesses without commensurate growth to staff size even while freeing up time to work on other IT and business initiatives. One interviewed Kyndryl customer commented: *"Our team is saving probably about 10–15% of their time because they no longer have to do activities like copy data management or complete monitoring. Also, Kyndryl's services allow us to build custom workflows using a recovery automation library. We are reallocating time savings to more important projects and ensuring focus on any kind of intrusion or high-level security event."* As shown in **Table 4**, IDC calculates that cybersecurity teams are an average of 27% more efficient as a result of using Kyndryl's services.

TABLE 4

IT Cybersecurity Staff Impact

	Before Kyndryl's Services	With Kyndryl's Services	Difference	Efficiency with Kyndryl
FTEs per year per organization	40.6	29.5	11.1	27%
Hours per 100 users per year	187.0	136.0	51.0	27%
Value of staff time required per organization per year for equivalent workloads ($M)	4.1	3.0	1.1	27%

n = 8, Source: IDC, 2021

Impact on Business and Operational Risk

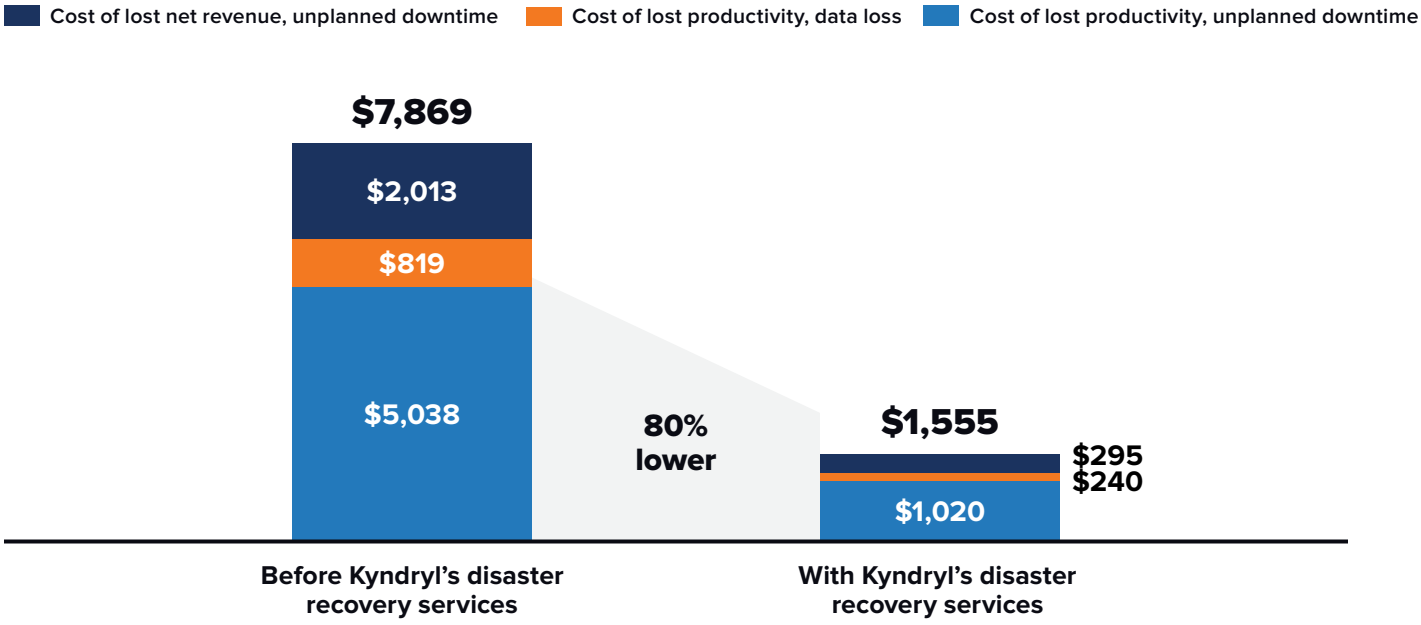
Study participants have significantly reduced business and operational risk with Kyndryl's services. This risk reduction is beneficial in both less tangible and highly tangible ways. From an intangible perspective, study participants often struggled to place a value on the reduced likelihood of a major security event or breach impacting their business operations or reputations. On the other hand, they pointed to specific and tangible ways in which their use of Kyndryl has yielded financial benefits by lowering the cost of lost productivity and revenue. One study participant explained its perspective on the value achieved: *"Our return on investment in Kyndryl's services has been significant. We have reduced downtime, which affects the entire organization, and have the ability to scale up our security without making significant additional purchases."*

As shown in **Figure 4**, benefits from reducing risk with Kyndryl's services are significant; study participants attributed an average 80% reduction in lost productivity and revenue to their use of these Kyndryl services, worth over $6,000 per year per 100 users and $2.57 million per organization. For interviewed Kyndryl customers, this represents a significant amount of value related to improved business continuity and security efforts.

FIGURE 4

Cost of Business Risk per 100 Users per Year

($ per year)



n = 8, Source: IDC 2021

Unplanned outages are inevitable to some extent for organizations operating at scale, but the key is to limit the impact of such downtime on employees and operations and ensure baseline business continuity. Interviewed Kyndryl customers reported accomplishing both. **Table 5** reflects their ability to bring down the frequency of unplanned outages (52% fewer) and resolve outages in less time (58% faster), which results in less employee productive time lost due to outages affecting important business applications and services (80% on average). For study participants, this carries significant value given that each user of IT services covered by Kyndryl's services will lose one fewer hour per year due to these types of outages, which adds up quickly, totaling an average of 43,918 hours of productive employee time gained back per year per organization.

TABLE 5

Unplanned Downtime Impact

	Before Kyndryl's Services	With Kyndryl's Services	Difference	Efficiency with Kyndryl
Number of unplanned outages per organization per year	56.4	27.1	29.2	52%
MTTR (hours)	3.3	1.4	1.9	58%
Hours of lost productive time per year per user	1.4	0.3	1.1	80%
Lost productive time in FTEs per organization per year	29.3	5.9	23.4	80%
Cost of lost productivity per year per organization ($M)	2.1	0.4	1.6	80%

n = 8, Source: IDC, 2021

Study participants also traced a noticeable impact on their business results to their use of Kyndryl's services. For these Kyndryl customers, this links back to the necessity of continuity for the business applications and services used to support their customers. Interviewed organizations spoke to a significant level of benefit in terms of limiting revenue loss associated with outages — avoiding $4.66 million in revenue loss per year per organization (see **Table 6**) — and reduced likelihood of incurring fines or penalties related to the handling of data or compliance issues:

- **Lower risk of major and ongoing fines:** *"Having full backup and restore capabilities gives us higher business confidence. But in terms of data validation, to give you an example, we had an example in the past where we had to pay out millions of dollars in compensation . . . On an ongoing basis, fines have gone down by $100,000–200,000 per year."*

- **Reducing risk of fines:** *"We've reduced risk associated with data loss with Kyndryl's services because it has more features that we didn't have before, like backup recovery and more data is backed up in the cloud . . . Before Kyndryl's services, one of our databases got compromised and our fine was like $20,000. It was a lot. It hasn't happened with Kyndryl."*

Beyond reduced costs associated with unplanned outages and other security issues, having a more robust and secure IT foundation often serves as a business enabler because interviewed Kyndryl customers have the confidence and bandwidth to focus on creating and addressing business demand. One customer explained: "We're increasing revenue with Kyndryl's services because instead of dealing with incidents, we can focus our time on business such as obtaining new clients, which is where our bread and butter is . . . This helps us increase our revenue because when we're dealing with this IT stuff, we can't seek out new clients." As shown in **Table 6**, this results in higher revenue, which study participants put at an average gain of $226,400 per organization per year.

TABLE 6

Business Operations Impact: Revenue

	Per Organization	Per 100 Users
Unplanned downtime impact – revenue losses avoided		
Revenue losses avoided per year	$4.66M	$11,451
Assumed operating margin (%)	15	15
Total operating margin impact per year	$649,300	$1,718
Revenue gains – business enablement		
Total additional revenue per year	$226,400	$556
Assumed operating margin (%)	15	15
Total operating margin impact per year	$34,000	$83

n = 8, Source: IDC, 2021

Use of Kyndryl's services has also helped study participants reduce the frequency and impact of data loss. On average, they reported limiting the frequency of data loss by one-third (33%) and recovering from data loss more than two times faster (57% less time). Overall, this means that they are losing 71% less productive employee time due to data loss (see **Table 7**).

TABLE 7

Data Loss Impact

	Before Kyndryl's Services	With Kyndryl's Services	Difference	Efficiency with Kyndryl
Number of data loss instances per organization per year	949	640	309	33%
MTTR (hours)	1.7	0.8	0.9	57%
Hours of lost productive time per year per user	0.2	0.1	0.1	71%
Lost productive time in FTEs per organization per year	4.8	1.4	3.4	71%
Cost of lost productivity per year per organization	$333,200	$97,600	$235,600	71%

n = 8, Source: IDC, 2021

ROI Summary

Table 8 provides IDC's analysis with regard to the average benefits and investment costs for interviewed organizations from using Kyndryl's services. On average, IDC projects that interviewed Kyndryl customers will realize discounted benefits worth $17.17 million over three years per organization ($42,196 per 100 users) in reduced costs associated with risk and more efficient risk-related IT teams. These benefits compare with average discounted investment costs of $2.83 million ($6,950 per 100 users). These levels of benefits and costs would result in an average three-year ROI of 507%, with breakeven on investment in Kyndryl's services occurring in seven months on average.

TABLE 8

ROI Analysis

	Five-Year Analysis		Three-Year Analysis	
	Per Organization	Per 100 Users	Per Organization	Per 100 Users
Benefits (discounted)	$27.1M	$66,533	$17.2 million	$42,196
Investment costs (discounted)	$3.7M	$9,093	$2.8 million	$6,950
Net present value (NPV)	$23.3M	$57,440	$14.3 million	$35,245
ROI (NPV/investment)	632%	632%	507%	507%
Payback (months)	7.0	7.0	7.0	7.0
Discount factor	12%	12%	12%	12%

n = 8, Source: IDC, 2021

Challenges/Opportunities

Security and resilience are the leading challenges in today's era of multicloud and digital transformation. The pace and volume of security threats and IT vulnerabilities are challenges for organizations of any size to keep ahead of. This places even greater importance on the planning for and deployment of cyber-resilience strategies. An effective cyber-resilience strategy is broad in scope and stakeholders, bringing together different constituents. Key stakeholders include not only security, operations, engineering, legal, and risk professionals but also data owners and line-of-business executives. This requires collaboration and planning across organizations with different priorities and depth of knowledge. This organizational dynamic is a challenge commonly seen in larger organizations, but it can be addressed through C-level strategic planning and priority setting.

Conclusion

Data availability and security are as foundational concepts to data-driven organizations as they ever were. Digital transformation though has introduced complexity to the use case as multicloud and hybrid cloud permeate our IT infrastructure. Threats to our data such as cyberattacks, software or hardware failures, human errors, supplier failures, or man-made disasters are increasing in both intensity and frequency and are more likely to initiate a disaster response than natural causes, the source of our yesteryear concerns. IDC recommends that IT organizations adopt an orchestrated business-resilience program to reduce or eliminate the separation between people, process, and technology for incident response to develop a comprehensive strategy. Remember, given the complexity created by digital transformation and the dependency of business on data, orchestration is the differentiator: time is literally money.

Kyndryl's services are designed to help organizations identify critical assets and their dependencies and risks, protect applications and data, detect threats and vulnerabilities faster, and rapidly respond to and recover from disruptive incidents. Ideally, any such solution should reduce downtime, speed up recovery, and result in an overall cost-of-ownership reduction. Indeed, these results were our findings from the in-depth analysis of Kyndryl customers that have deployed and operated this solution. Although absolute results and numbers will vary by organization, IDC believes these results represent the actual results achieved by these organizations. Based on these results, we also believe that most organizations that properly implement Kyndryl's services can expect to see improved detection of threats and vulnerabilities, faster recovery, less overall downtime, and lower business and operational costs related to risk.

Appendix: Methodology

IDC's standard ROI methodology was utilized for this white paper. This methodology is based on gathering data from current users of Kyndryl's DRaaS and resilience orchestration services as the foundation for the model. Based on interviews with organizations using it, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of Kyndryl's services.** In this study, the benefits included staff time savings and productivity benefits, revenue gains, and cost reductions.

2. **Created a complete investment (five- and three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Kyndryl's services and can include additional costs related to migrations, planning, consulting, and staff or user training.

3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of Kyndryl's DRaaS and resilience orchestration services over a five-year period and a three-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).

- The net present value of the five- and three- year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because the use of Kyndryl's services requires a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

About the Analysts

Frank Dickson

Program Vice President, Cybersecurity Products, IDC

Frank Dickson is a Program Vice President within IDC's Cybersecurity Products research practice. In this role, he leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response and Orchestration (AIRO); Identity & Digital Trust; Legal, Risk & Compliance; Data Security; IoT Security; and Cloud Security. Topically, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

More about Frank Dickson

Phil Goodwin

Research Director, Infrastructure Systems, Platforms and Technologies Group, IDC

Phil Goodwin is a Research Director within IDC's Enterprise Infrastructure Practice, covering research on data management. Mr. Goodwin provides detailed insight and analysis on evolving industry trends, vendor performance, and the impact of new technology adoption. He is responsible for producing and delivering timely, in-depth market research with a specific focus on cloud-based and on-premises Data Protection, Business Continuity and Disaster Recovery, and Data Availability. Mr. Goodwin takes a holistic view of these markets, and covers risk analysis, service level requirements and cost/benefit calculations in his research.

More about Phil Goodwin

Matthew Marden

Research Director, Business Value Strategy Practice, IDC

Matthew is responsible for carrying out custom business value research engagements and consulting projects for clients in a number of technology areas with a focus on determining the return on investment (ROI) of their use of enterprise technologies. Matthew's research often analyzes how organizations are leveraging investment in digital technology solutions and initiatives to create value through efficiencies and business enablement.

More about Matthew Marden

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC @idc @idc idc.com