REGION FOCUS: WORLDWIDE

The Business Value of Kyndryl Security and Resiliency Services

Harsh Singh
Senior Research Analyst,
Business Value Strategy Practice, IDC

Phil Goodwin
Research Vice President, Infrastructure Systems,
Platforms and Technologies Group, IDC

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

Executive Summary

Every organization looks to make strategic investments in IT to make itself more agile, resilient, and profitable. Frankly, IT vendors can make it difficult, penning market messages that are more creative than constructive. Conducting like-for-like comparisons of complex solutions is rarely easy. Solution vendors often complicate comparison by offering subjective statements of value that allude to potential benefits that a product or service may provide to end-user organizations when what is needed are objective, transparent, and direct metricized expectations of potential outcomes to be realized. Simply put, vendors use too many words and not enough numbers. Organizations long for quantifiable measures of value.

To assist IT buyers in making sound decisions, IDC endeavors to independently calculate the business value of specific solutions based on extensive and objective criteria (see the Appendix). This study is intended to help IT buyers that are evaluating resiliency services by quantifying the business value that current users of the services have experienced.

Cybersecurity, data protection, and digital business resilience are among the most urgent needs for modernization and enhancement within nearly every organization. The "why" is simple. Malicious cyberattacks have become more numerous and sophisticated as the ill-gotten gains grow. A popular tool of today's hacker is ransomware, the pervasiveness of which has become so ubiquitous that every organization can expect to deal with it at some point. The pain of ransomware attacks motivates cultural change within organizations regarding their stances on the topic of resiliency, driving a renewed and greater urgency to improve preparedness.

Kyndryl Security and Resiliency Services is designed to help companies embed highly effective levels of cyber-resilience into their broader IT infrastructure to manage rapidly evolving operational risks, protect business-critical infrastructure, mitigate the business impacts of security incidents, and rapidly recover from security incidents when they occur. To determine the real-world effectiveness of this offering, IDC conducted research that explored the value and benefits for organizations using Kyndryl to support and enhance their security and disaster recovery (DR) efforts. The project included interviews with six companies that had experience with or knowledge about its benefits and costs.

Business Value Highlights

Click each highlight below to navigate to related content within this document.

- **568%** five-year ROI
- **9 months** to payback
- **30%** more efficient disaster recovery and data protection teams
- **39%** faster time to respond to security threats
- **35%** more efficient cybersecurity teams
- **22%** more security threats identified
- **93%** reduction in unplanned downtime
- **66%** reduction in data loss–related productivity issues
- **$7.68 million** total revenue gained/ protected annually
- **15%** more efficient compliance teams

Based on extensive quantitative and qualitative data derived from these interviews, IDC calculates that study participants will realize significant business value of $10.7 million per organization with a very substantial 568% five-year return on investment (ROI) by:

- Limiting organizational risk by providing quick and effective identification of and response to security threats and incidents
- Improving the efficiency of security-related teams, including cybersecurity, IT infrastructure, compliance, and application development
- Mitigating data loss and minimizing any potential financial impacts associated with data breaches
- Reducing the incidence of unplanned downtime, which leads to improved end-user productivity and better business results

Situation Overview

Cyberattacks were once a rare event suffered by a few unfortunate nation-states. The 2013 Target breach spread awareness of cyberattacks from Pennsylvania Avenue to Main Street as ordinary citizens felt the effects of the attacks. However, when cybercriminals monetized ransomware with bitcoin, a pervasive threat was born that impacts every organization.

Today's "ransomware" attacks have evolved to encompass a larger group of malicious attack techniques, including:

- **Data encryption**
  Attackers apply encryption to user data and then demand ransom payment for the decryption key and/or decryptor software.
- **Data scrambling**
  Attackers scramble data by changing values in structured data sets or databases and then demand a ransom payment for descrambling.
- **Data exfiltration**
  Attackers appropriate data and then demand ransom to not post it on the dark web, sell it to competitors, notify a company's customers, or threaten other nefarious use.

When leveraging data encryption or data scrambling, attackers have learned to attack the backup first, by either encrypting or destroying backup data sets. Data backups provide the opportunity to mitigate malicious effects of the attacker. However, if the backups can be compromised, an urgency is created for the compromised organization to pay the ransom.

As cyberattacks are an inevitability, response planning and preparedness are mandatory. Although disaster recovery solutions continue to be important, they fail to address the elevated complexity of a cyberattack. Natural disasters and hackers impact IT systems, software, and data differently.

Some key differences are:

- Natural disasters do not selectively corrupt portions of your data or look to reestablish persistence after recovery; hackers do. Thus, backup data must be analyzed and scanned before a restore can commence.
- Disasters occur at a specific point in time and are very clear, enabling organizations to determine a specific data recovery point. Cyberattacks are stealthy and intentionally obfuscated, occurring over days, weeks, or months, meaning there is no single clean restore point. Organizations must curate, or selectively determine, restore points for various data elements.
- With natural disasters, damage is obvious; in contrast, hacking is covert and requires forensic analysis, which is a critical step for cyber-recoveries.
- Natural disaster events do not change much over decades and can even be somewhat predictable. Hackers are forever innovating and varying attacks, and the needed defenses and responses are constantly changing.

The dynamic nature and severe threat of cyberattacks render current IT capabilities inadequate. Businesses are engaging services organizations that specialize in cyber defense and recovery preparedness to help. These services organizations bring a breadth of knowledge from numerous situations and keep their clients proactively engaged in preparedness.

Kyndryl Security and Resiliency Services Overview

Kyndryl Security and Resiliency Services provides an integrated cyber-resilience approach designed to enable IT practitioners to anticipate, protect against, withstand, and recover from adverse cyberevents.

The Kyndryl Security and Resiliency Services portfolio includes:

- **Security Assurance Services**
  Assess and benchmark resilience maturity, gain visibility into significant threats and vulnerabilities, and manage compliance.
- **Zero Trust Services**
  Protect critical business data and applications in a cyber-resilient infrastructure.
- **Security Operations and Response Services**
  Discover and respond to a detected incident.
- **Incident Recovery Services**
  Mitigate impact of disruption with capabilities to automatically recover critical business processes and data.

Kyndryl delivers its services in an integrated building block approach to help clients minimize risk and improve success through these platforms:

- **Kyndryl Consult** brings decades of IT modernization and mission critical knowledge, operating best practices, and implementation experience to realize your transformation journey, and keep you secure and resilient at every stage.
- **Kyndryl Bridge** is an open integration platform that leverages Kyndryl's core strengths, data-driven insights and expertise, to provide more visibility into and control of your complex technology environment. Customers can run more stable and reliable technology operations with automation to create more fluid, dynamic, and responsive environments that empower enterprises to adapt rapidly to changing business landscapes.
- **Kyndryl Vital** a designer-led co-creation experience, that brings partners and customers together to solve complex business problems.

The Kyndryl solution is designed to combine technology with expertise to address cyberthreats proactively to keep attackers out as well as to react quickly if they do penetrate the defenses.

The Business Value of Kyndryl Security and Resiliency Services

Study Firmographics

IDC conducted research that explored the value and benefits of using Kyndryl Security and Resiliency Services to improve security and DR efforts and operations. The project included six interviews with organizations that were using this solution and that had experience with or knowledge about its benefits and costs. During the interviews, companies were asked a variety of quantitative and qualitative questions about the Kyndryl solution's impact on their IT and security operations, core businesses, and costs.

Table 1 (next page) presents the aggregated firmographics of interviewed organizations. The organizations that IDC interviewed had a base of 64,333 employees with annual revenue of $5.27 billion, indicating the involvement of several large enterprises. This workforce was supported by an IT staff of 404 managing 276 business applications using 10,000TB of available storage. In terms of geographic distribution, four companies were based in the United States with the remainder in India and Spain. There was a good mix of vertical markets represented including financial services, healthcare, food and beverage, information technology, retail, and transportation. (Note: All numbers cited represent averages.)

TABLE 1

Firmographics of Interviewed Organizations

Firmographics	Average	Median	Range
Number of employees	64,333	12,250	6,000 to 309,000
Number of IT staff	404	225	48 to 1,500
Number of business applications	276	68	50 to 1,300
Number of terabytes of storage available	10,000	8,000	425 to 30,000
Revenue per year	$5.27B	$1.74B	$500M to $21.90B
Countries	United States (4), India, and Spain		
Industries	Financial services, healthcare, food and beverage, information technology, retail, and transportation		

Source: IDC's Business Value research, March 2023

Choice and Use of Kyndryl Security and Resiliency Services

The organizations interviewed by IDC described their rationale for selecting Kyndryl Security and Resiliency Services to serve as a robust foundation for embedding cyber-resilience into their broader IT and operational strategies for managing rapidly evolving cyberthreats and related risks. Study participants commented that Kyndryl gave their organizations the ability to adapt to new hybrid working models during the pandemic, which necessitated finding new ways to protect their business from cyberthreats and malware. Healthcare organizations appreciated that their patient data was protected by a better ability to manage aspects of their ecosystem by using existing network and communications frameworks. In addition, interviewed organizations appreciated that the solution was able to improve their disaster recovery operations and reduce regulatory and compliance risks. They noted that Kyndryl offered a number of synergies with the move to cloud and software as a service (SaaS).

Study participants elaborated on these and other selection criteria:

Helped companies adapt to the new hybrid working models:

"The pandemic increased the need for cyber-resilience like never before. Because we shifted to a hybrid work model, we wanted to make sure that our IT security would be very resilient to any kind of attack, not only from a business [perspective] but also from an HR perspective. We wanted to protect business from cyberthreats and malware, so we decided that for this hybrid model, the technology that was most appropriate was Kyndryl."

Ensured that patient data was protected:

"Kyndryl's product aligned to serve our needs specifically within healthcare. It's important to us to maintain patient data. It's also important that different parts of the ecosystem from our network and communication system are managed effectively. What we found with Kyndryl solutions were offerings that would lessen the amount of risk that we faced from a cybersecurity perspective. It helped with thinking about how to automate some of the repeatable/mundane tasks and get into an automation space to be more compliant and handle daily operational tasks."

Improved disaster recovery operations:

"One of the reasons is cyberthreats. The second reason is we want to find out, when it comes to disaster recovery, what will be the best practices suitable for our industry."

Reduced regulatory risks and cloud migration friction:

"In 2019, there was a massive data breach with Capital One, and they were fined about $80 million. For this kind of economy, that kind of fine is not pocket change. That's one of the biggest factors in our decision — not directly, not even indirectly, but it's a big one. Second, [there are] a lot of changes within the organization: moving to cloud, moving to SaaS. So [there are] a lot of synergies, looking especially at resiliency, or any kind of threats. The question was: How can we be better in terms of aligning with the transformation modernization and, of course, couple that with cybersecurity? So that's where we have security teams that work hand in glove with IT and, of course, with the business."

Table 2 (next page) describes the organizational usage associated with the interviewed companies' deployment of various solutions in the Kyndryl Security and Resiliency Services suite. Note that there was a substantial Kyndryl footprint across all companies as evidenced by an 88% user base, with 67% of revenue supported by Kyndryl applications. On average, across all companies, there were 54 business applications supported by 714 physical servers and 1,405 virtual servers. Additional metrics are presented.

TABLE 2

Kyndryl Security and Resiliency Services Environment

	Average	Median
Number of business applications	54	40
Percentage of applications on premises	22	16
Percentage of applications on public cloud	49	48
Percentage of applications on private cloud	29	28
Number of datacenters	12	3
Number of physical servers	714	80
Number of virtual servers	1,405	1,000
Number of geographical locations (countries)	52	7
Number of sites/branches	104	82
Percentage of users	88	81
Percentage of revenue supported by applications	67	100

Source: IDC's Business Value research, March 2023

Business Value and Quantified Benefits

IDC's Business Value model quantifies the benefits for organizations that were using Kyndryl Security and Resiliency Services to support their cyber-resilience, regulatory compliance, and disaster recovery efforts. Study participants reported that they were able to limit organizational risk by providing quicker and more effective identification and response to security threats and incidents. In part, this was accomplished by improving the overall efficiency and effectiveness of their security and security-related teams, including cybersecurity, IT infrastructure, and compliance teams. With these enhanced capabilities in place, Kyndryl customers were able to mitigate data loss and the negative financial impacts associated with data breaches. In addition, they reduced the incidence of unplanned downtime, leading to improved end-user productivity. All of these benefits combined to produce better business results for interviewed organizations.

In their comments to IDC, study participants described them in detail:

Improved disaster recovery that allows hospitals to operate more smoothly:

"Disaster recovery is the biggest business benefit for us. There's less downtime, fewer service-impacting interruptions impacting the physicians' ability to access the various applications that they need in order to deliver care. There's less time waiting, which means we see a higher degree of patient satisfaction and less need to use downtime for procedures."

Digital transformation that is fostered by improved protection and compliance:

"Kyndryl understands the traditional architecture and the transformations needed to move to the cloud. One of the challenges of digital transformation or modernization is: How do you move a traditional system to the cloud? You can't take a 1950s-model car and turn it into an EV. It has to be redesigned. Similarly, how do you take a traditional application that's been around 10, 15, or 20 years and move that into Azure or AWS? Kyndryl understands that transformation is needed. They also understand the vertical, especially the financial vertical. They understand what's involved in terms of business, use cases, cybersecurity and, of course, regulations to ensure compliance. These are the benefits that Kyndryl brings to the table."

More efficient IT security teams:

"Zero trust services is one benefit we've gotten from Kyndryl Security and Resiliency Services. Also, we were able to make our IT operations and responses more efficient. This has enabled us to implement additional AI-powered capabilities."

More resilient applications that enable quick recovery:

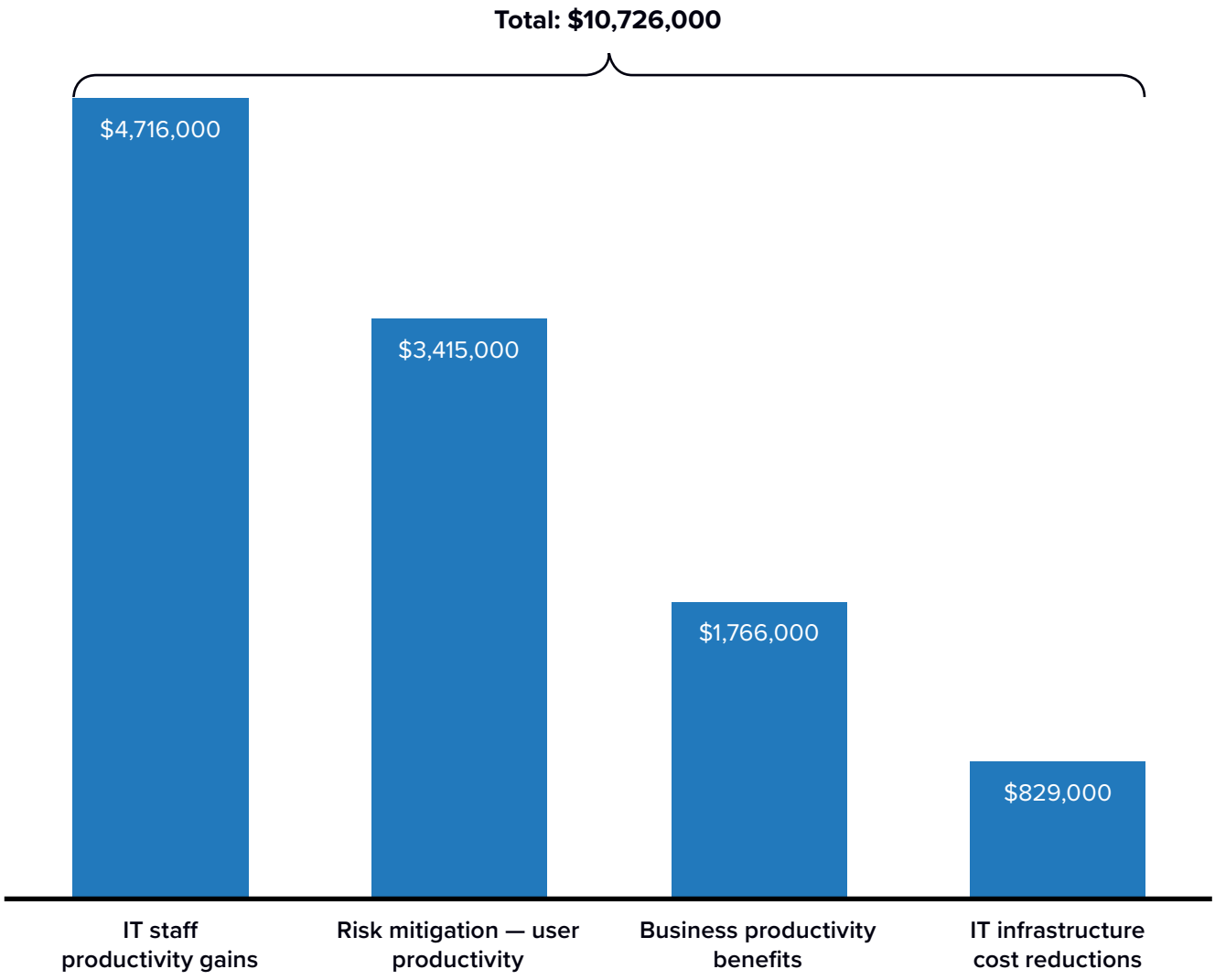
"From an IT perspective, it's the cloud management and modernization with security services. What that's enabled us to do is, as we've moved and added different workloads into the cloud, add more resiliency. It's also added the ability for the system to be architected for a good level of disaster recovery. Further, it's ensured that we're maintaining security and general due diligence in terms of operational effectiveness."

Based on interviews with the six intensive users of Kyndryl Security and Resiliency Services, IDC quantified the estimated return on investment that study participants will realize over five years at an average of 568% along with annual average benefits of $10.7 million for each organization (see **Figure 1,** next page).

FIGURE 1

Average Annual Benefits per Organization

(Total $ of value per year)



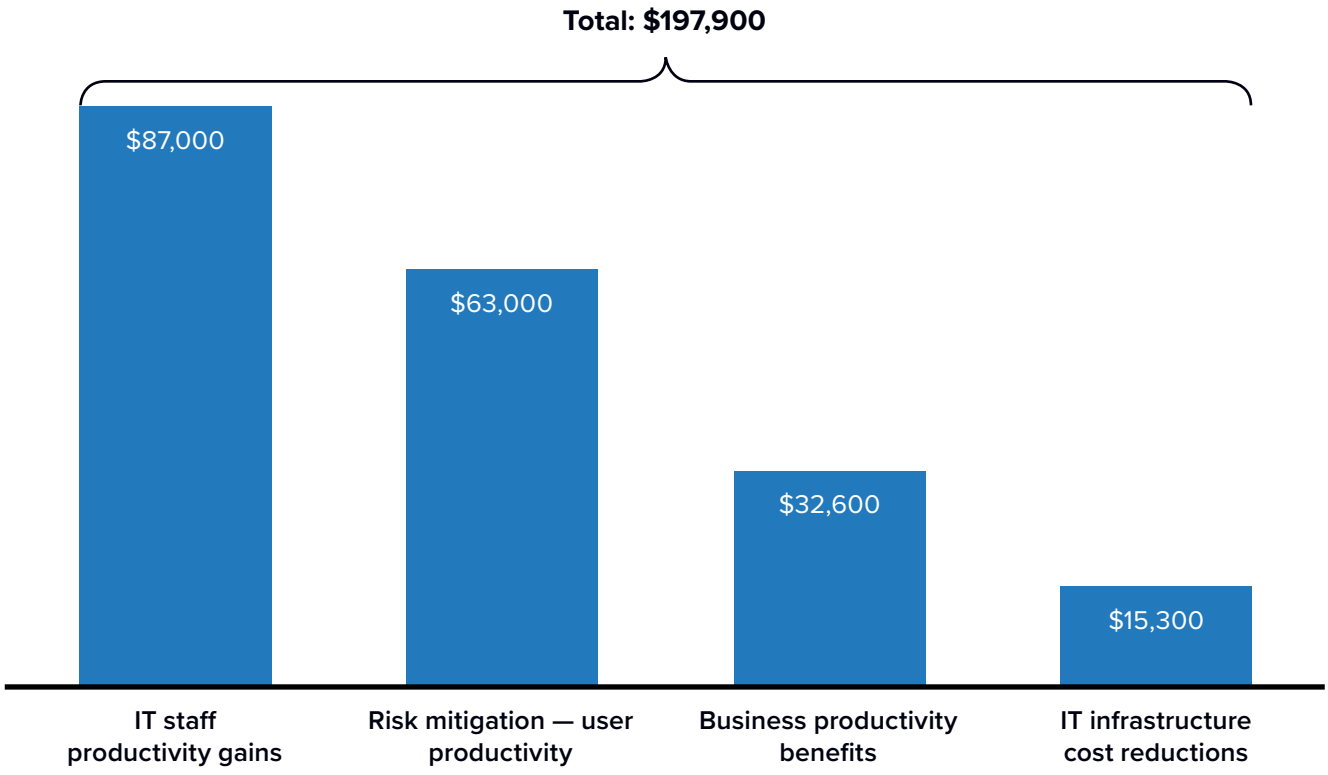
n = 6; Source: IDC's Business Value research, March 2023

Figure 2 (next page) presents the same data — that is, average annual benefits broken out on a per application basis. As shown, this amounted to $197,900 per organization.

FIGURE 2

Average Annual Benefits per Application

(Total $ of value per year)



n = 6; Source: IDC's Business Value research, March 2023

Improvements in Security and DR Postures

Data security and integrity are critical checklist items for all organizations. The accelerated move toward digital transformation has introduced the notion of cyber-resilience as a key priority for C-suite managers. In addition, companies need to ensure compliance with a complex web of industry and regional regulations. To effectively meet these challenges, organizations need to proactively implement technology and policies to enhance their risk, compliance, and security profiles.

The Kyndryl Security and Resiliency Services portfolio of solutions is designed to address these needs by providing an integrated cyber-resilience approach that enables companies to anticipate, protect against, and quickly and effectively recover from adverse cyberevents if and when they occur. With the shift to hybrid work and an increasingly sophisticated and constantly changing threat landscape, organizations must also ensure robust continuity and recovery in the face of any disruption.

Interviewed organizations confirmed that Kyndryl Security and Resiliency Services addressed many of the challenges that companies in a variety of vertical markets are grappling with. In their comments, they noted that Kyndryl offered end-to-end services that could support multiple and varied third-party SaaS applications, including Azure and AWS, while conferring the ability to differentiate between false positives and false negatives. They also appreciated that Kyndryl provided better visibility and insights into cyberattacks and helped track their origins while providing improved analytics and insights compared with previous solutions. In addition, companies pointed out that this functionality better enabled their ability to reduce downtime and protect against ransomware while establishing and working in the framework of a zero trust environment. They also noted that staff were freed up to work on other operational and strategic projects.

Study participants elaborated on these and other benefits:

End-to-end services:

"We have multiple different third-party SaaS applications. We're using both Azure and AWS, and when there are operational or cybersecurity issues, this is where Kyndryl Security and Resiliency Services will need to get 'eyes on glass.' What that means is looking at exactly [what] the event is about and making sure it's not a false positive or false negative because there may be other things not related to security or just operations. If and when they've validated that it is some kind of security incident, Kyndryl would reach out to the vendors or the business hosts to be the point of contact. Then Kyndryl would try to understand or resolve the particular event in a proper, timely manner that we spelled out."

Better visibility and insights into cyberattacks:

"When we have a cyberattack, the most difficult thing is to track its origin, providing analytics and insight. With the old solution, it was difficult to know the nature of an attack, to track where it was coming from, and to know how we could protect against it. We were mixing and merging solutions to figure out how to mitigate the risk when we had attacks where we didn't have the right kind of analytics."

Reduced downtime and proactive protection against threats:

"The biggest benefit is protection against ransomware. Kyndryl can help go to downtime procedures or utilize some type of mechanism where you can revert to the previous state. That's enabled us to not have as much downtime or be impacted by ransomware. The other thing from a healthcare perspective is breach of data: protecting HIPAA data, confidential patient data that we always want to maintain utmost security about, and also getting better in terms of the framework that we utilize. Kyndryl Security and Resiliency Services also offers a zero trust environment that helps eliminate any sort of risk and make sure that the right individual has the right level of access needed. The final thing is managed services, through the use of Kyndryl proprietary software that identifies trends or potential gaps or anomalies in your security architecture environment."

More time to work on other operational and strategic projects:

"Rather than having to look at the approving, safeguarding, or ensuring that we're 'safe' from using a certain application, or looking at what that process may be, we've been able to focus our solution engineers on business-enabling cybersecurity efforts or training campaigns, doing more penetration testing, ensuring that our systems go through their annual or biannual cycle to ensure that it's still secure and patched as well. So, we've been able to focus on operational and strategic efforts and partnerships with other business units and third-party healthcare companies."

To get a full and complete picture of the impacts of Kyndryl, IDC evaluated specific ways that the solution improved the performance of various teams, beginning with disaster recovery and data protection teams. Interviewed companies told IDC that teams focused on disaster recovery and data protection gained more tools to help them recover quickly from an event. They appreciated access to services to facilitate being more proactive with their protection setup.

Table 3 quantifies the impacts for disaster recovery and data protection teams. After adoption, interviewed companies saw a 30% improvement in team productivity. IDC calculated that this translated into an annual business value of $2.02 million for each organization.

TABLE 3

Disaster Recovery and Data Protection Team Impact

	Before Kyndryl Security and Resiliency Services	With Kyndryl Security and Resiliency Services	Difference	Benefit
Disaster recovery and data protection teams (FTE per organization per year)	67.8	47.7	20.2	30%
Staff time cost per year	$6.78M	$4.77M	$2.02M	30%

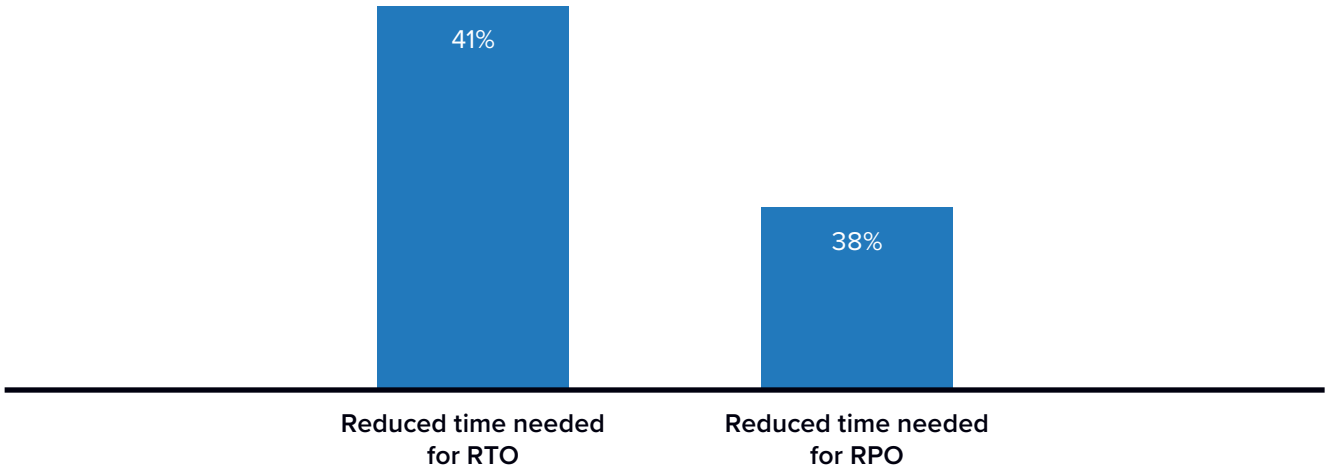
Source: IDC's Business Value research, March 2023

IDC then drilled down on DR performance. Here Kyndryl offered its customer base a variety of disaster recovery features such as allowing organizations to snap back to a pre-event state, a feature that allows for quicker disaster recoveries. As shown in **Figure 3** (next page), after adoption, companies experienced a 41% reduction in the time needed for recovery time objective (RTO) and a 38% reduction in the time needed for recovery point objective (RPO).

FIGURE 3

RTO/RPO Impact

(Percentage improvement)



n = 6; Source: IDC's Business Value research, March 2023

IDC then evaluated benefits for cybersecurity teams. Kyndryl Security and Resiliency Services offered these teams a combination of features and services that allowed them to be more efficient in the day-to-day tasks involved in dealing with potential threats. As shown in **Table 4**, after adoption, companies saw a 35% improvement in cybersecurity team productivity. This amounted to an annual business value of $1.88 million for each organization.

TABLE 4

Cybersecurity Team Impact

	Before Kyndryl Security and Resiliency Services	With Kyndryl Security and Resiliency Services	Difference	Benefit
Cybersecurity (FTE per organization per year)	53.7	34.9	18.8	35%
Staff time cost per year	$5.37M	$3.49M	$1.88M	35%

Source: IDC's Business Value research, March 2023

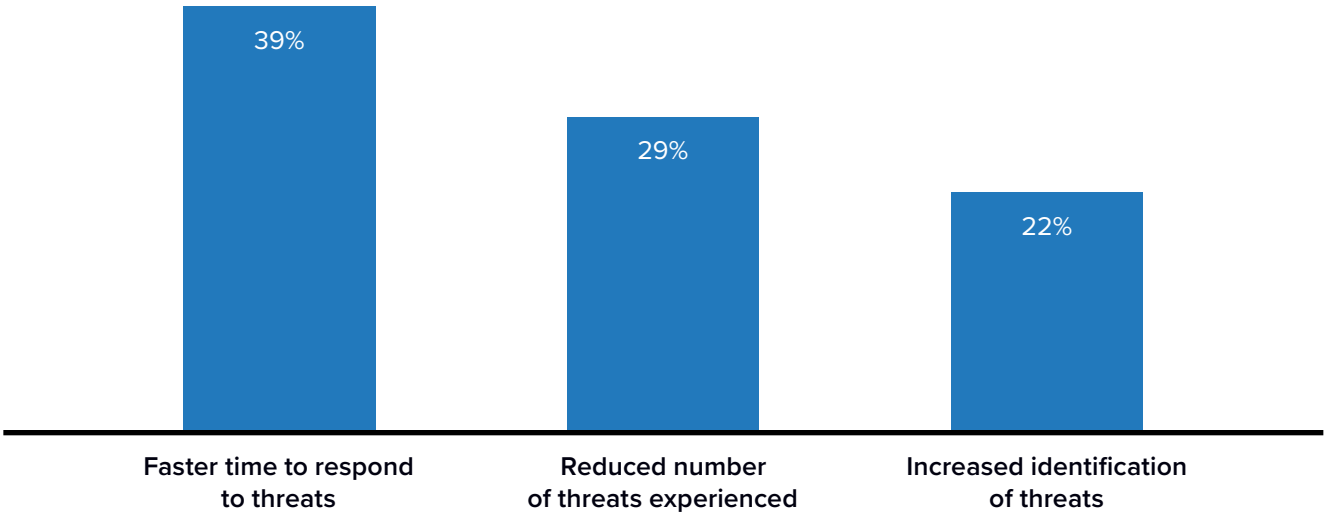
A core value proposition of Kyndryl is the ability to anticipate, protect against, withstand, and recover from adverse cyberevents with Security Assurance Services. With the use of a zero trust framework, both malicious insider threats and advanced outsider attacks are managed by removing access from users, applications, and infrastructure with validation only through strict access authentication. Organizations told IDC that Kyndryl was able to help them modernize their cyberthreat operations so they could reduce the number of attacks and the time needed to respond.

Figure 4 shows cybersecurity threat impact. After adoption, organizations were able to respond to threats 39% faster. In addition, the number of threats experienced was reduced by 29%, accompanied by a 22% increase in their identification.

FIGURE 4

Cybersecurity Threat Impact

(Percentage improvement)



n = 6; Source: IDC's Business Value research, March 2023

IT infrastructure teams play an important role in helping implement and backstopping a viable security posture. Interviewed organizations told IDC that Kyndryl enabled their IT infrastructure teams to modernize their cyberthreat operations, thereby helping them reduce both the number of attacks experienced and the time needed to respond.

Table 5 (next page) quantifies these impacts showing that interviewed companies saw a 12% improvement in team productivity and effectiveness after adoption. This amounted to an annual productivity-based business value of $110,800 for each organization.

TABLE 5

IT Infrastructure Team Impact

	Before Kyndryl Security and Resiliency Services	With Kyndryl Security and Resiliency Services	Difference	Benefit
Management of IT infrastructure productivity impact (equivalent FTEs)	9.5	8.4	1.1	12%
Staff time cost per year	$950,000	$839,200	$110,800	12%

Source: IDC's Business Value research, March 2023

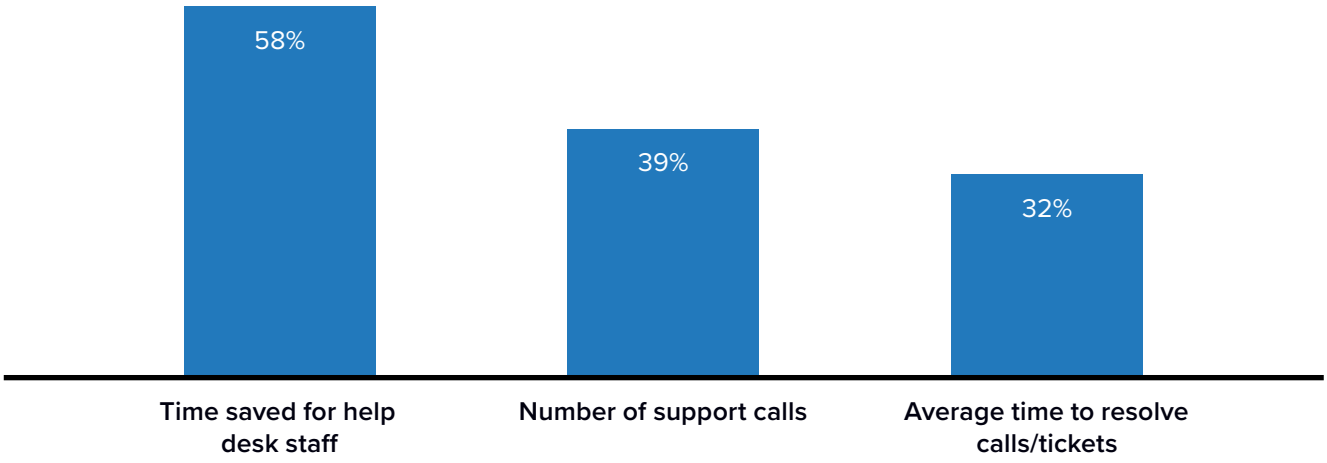
Study participants reported that their organizations saw fewer help desk trouble tickets and requests once Kyndryl had been implemented. This was related to the fact that they experienced fewer attacks or disruptions involving key business applications and other workloads.

Figure 5 quantifies these improvements. As shown, after adoption, the staff time involved in help desk operations was dramatically reduced (58%). In addition, the overall number of support calls was reduced by 39% and the average time to resolve calls or tickets was reduced by 32%.

FIGURE 5

Help Desk Impact

(Percentage improvement)



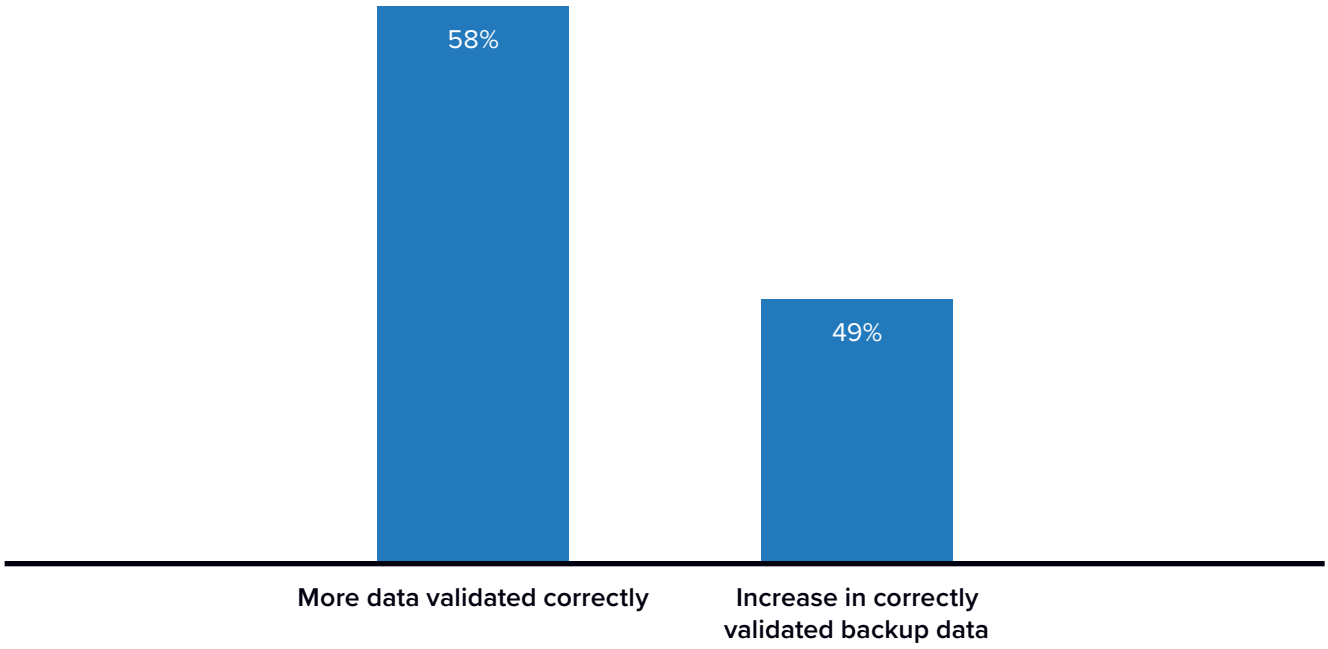
n = 6; Source: IDC's Business Value research, March 2023

Another important functional area that IDC evaluated was business resiliency — the ability for companies to quickly marshal the necessary resources to bounce back from and withstand major disruptions under normal operating conditions. More traditional DR strategies are often unable to keep up with changing recovery requirements, and this may result in businesses being exposed to outages that cause irreparable damage. In this IDC evaluation category, organizations reported they were able to effectively validate more of their data than before (see **Figure 6**). After adoption, companies saw a substantial increase in validated backup data (49%) and in overall data that was correctly validated (58%).

FIGURE 6

Data Validation KPIs

(Percentage improvement)



n = 6; Source: IDC's Business Value research, March 2023

IDC then evaluated the cost impacts of Kyndryl adoption. Interviewed organizations noted that they were able to improve their cost profiles with respect to other security and DR solutions by switching to Kyndryl's consolidated offerings. IDC calculated the security solution cost savings per application and projected those costs out for a five-year period (see **Figure 7**, next page). As shown, the Kyndryl solution offered a 26% reduction in cost savings compared with previous or alternative solutions.

FIGURE 7

Five-Year Security Solution Cost Savings per App

(Cost of Kyndryl/other security and disaster recovery solutions)

n = 6; Source: IDC's Business Value research, March 2023

Business Improvements

Interviewed companies told IDC that when cyber-resilience and DR were more effective and simplified, they experienced direct and measurable benefits for their business operations. In their comments, interviewed companies noted that, with Kyndryl, they were more confident in their ability to protect their organizations in terms of both business continuity and business recovery. They stressed that the use of effective automation ensured operational efficiency and reduced risks associated with infrastructure and applications. Study participants pointed out that better data visibility made managing data classification and protection easier, thereby enhancing both certification and compliance. The key area of application development was also called out, and companies reported that their developers gained more confidence in their environments, which accelerated the process of development and testing.

They elaborated on these benefits:

More confident in the ability to protect the organization:

"The biggest benefit is business continuity and business recovery. If we have a business disruption, we can mitigate the impact. Now, we are trusting the services and we can be confident. We know we are not so open to any kind of threat or malware. … That confidence was not there before. Also, from a financial point of view, we needed to build effective data strategies and adopt automation to ensure operational efficiency to reduce risk to both infrastructure and applications. We're much more resilient now and can ensure continuity."

Better visibility that makes it easier to be compliant:

"The risk is huge. The business relies on a data foundation. If we have risk to data, everything will collapse. We have some KPIs on risk and compliance related to data risk and data loss and also what we call asset classification and protection. All our assets, all our items, are part of the master data — business data, application data, transactional data. They're prone to risk, so we're tracking them. With Kyndryl Security and Resiliency Services, we're able to manage data classification and protection and do certification and compliance. We're able to have data governance in place."

More developer confidence in the environment:

"Kyndryl Security and Resiliency Services has helped with our general confidence. When we build a company solution ourselves, we have the capability to build or to test the product in the environment that Kyndryl is managing. So Kyndryl has sped up the process there, both from a development and testing standpoint."

Ability to help IT be more compliant with business audits:

"The IT department is much more confident. Right now, we have security standards and frameworks adapted to Kyndryl. This makes IT more comfortable in terms of compliance and certifications. In terms of audits, if we want to have internal or external audits, it's easier for IT to provide proof and evidence as to how the organization is solving certain issues. There is clarity, whereas before, there was none. From an audit perspective, it was always a disaster."

IDC then quantified these anecdotal observations in several key areas. An important aspect of business resiliency is the ability to mitigate and reduce the incidence of unplanned downtime. Study participants reported that they were able to reduce these impacts for both end users and customers because Kyndryl gave them more management tools.

Table 6 (next page) quantifies reductions in unplanned downtime. As shown, the annual frequency of unplanned outages was reduced by 73%. Further, when disruptive events did occur, they were remediated 73% faster. These two improvement areas combined for an overall staff productivity boost of 93% and an annual business productivity savings of $3.65 million.

TABLE 6

Unplanned Downtime Impact

	Before Kyndryl Security and Resiliency Services	With Kyndryl Security and Resiliency Services	Difference	Benefit
Frequency per year	12.3	3.4	8.9	73%
Time to resolve (hours)	7.9	2.1	5.8	73%
Hours lost per user	2	0.2	1.9	93%
Lost productivity due to unplanned outages (FTE impact)	56.3	4.2	52.1	93%
Value of lost productivity	$3.95M	$293,800	$3.65M	93%

Source: IDC's Business Value research, March 2023

By reducing the amount of downtime in their customer-facing applications, organizations were able to protect more revenue. Interviewed organizations reported that less business and operational risk stemming from potential outages had direct impacts on their overall revenue picture. As shown in **Table 7**, on average, organizations received total additional annual revenue of $550,200 as a direct result of Kyndryl adoption.

TABLE 7

Unplanned Downtime Revenue Impact

	Per Organization
Business impact — Revenue protected from reduced downtime	
Total additional revenue per year	$550,200
Assumed operating margin	15%
Total recognized revenue per year — IDC model*	$82,500

* The IDC model assumes a 15% operating margin for all additional revenue. Source: IDC's Business Value research, March 2023

IDC then looked at business resiliency impacts with respect to data loss and data breaches. Study participants reported that their organizations saw fewer data loss incidents with Kyndryl (see **Table 8**). After adoption, the number of incidents occurring was reduced 37%. In addition, when events did occur, they were able to be resolved 46% more quickly. This translated into an overall productivity-based business value of $123,400.

TABLE 8

Data Loss Impact

	Before Kyndryl Security and Resiliency Services	With Kyndryl Security and Resiliency Services	Difference	Benefit
Number of data loss incidents per year	18.9	11.9	7	37%
Time to resolve (hours)	3.1	1.7	1.4	46%
Hours lost per user	0.1	0.03	0.1	66%
Lost productivity due to unplanned outages (FTE impact)	2.7	0.9	1.8	66%
Value of lost productivity	$186,900	$63,600	$123,400	66%

Source: IDC's Business Value research, March 2023

Similar benefits were seen with respect to data breaches that could have a very significant impact on customer experience. Reducing the number of data breaches is important for the business in terms of protecting revenue streams, and Kyndryl adoption offered measurable impacts in this area. Total annual revenue saved or protected from data breaches was calculated by IDC at $4,223,000 (see **Table 9**, next page).

TABLE 9

Data Breach Revenue Impact

	Per Organization	Per Application
Business impact — Revenue protected from reduced downtime		
Total additional revenue per year	$4,223,000	$78,000
Assumed operating margin	15%	15%
Total recognized revenue per year — IDC model*	$633,500	$6,100

* The IDC model assumes a 15% operating margin for all additional revenue. Source: IDC's Business Value research, March 2023

Kyndryl also had a significant impact on application development teams. These teams are tasked with delivering highly functional software on which their businesses depend. Interviewed organizations tied Kyndryl's productivity-related benefits to their efforts, and as a result, teams felt more confident in working in their development and testing environments.

Table 10 quantifies these benefits. As shown, after adopting Kyndryl, these teams experienced a 7% boost in productivity. This essentially means that teams of 46.9 FTEs could do the work of 50.2 FTEs, and companies could avoid hiring 3.3 additional FTEs. This amounted to an annual productivity-based business value of $328,300 for each organization.

TABLE 10

Application Development Team Impact

	Before Kyndryl Security and Resiliency Services	With Kyndryl Security and Resiliency Services	Difference	Benefit
Application development (FTE per organization per year)	46.9	50.2	3.3	7%
Equivalent value of application development team productivity (cost per year per organization)	$4.69M	$5.02M	$328,300	7%

Source: IDC's Business Value research, March 2023

One of Kyndryl's core value propositions relates to providing better visibility into data in order to enhance compliance efforts and better manage data classification and protection. Organizations reported that Kyndryl Security and Resiliency Services gave them better visibility into the full spectrum of their data, thereby allowing both IT and the business management to ensure better compliance.

Table 11 quantifies these benefits. As shown, after adoption, compliance teams experienced a 15% boost in productivity. This amounted to an annual business value of $596,300 for each organization.

TABLE 11

Compliance Team Impact

	Before Kyndryl Security and Resiliency Services	With Kyndryl Security and Resiliency Services	Difference	Benefit
Compliance teams (equivalent FTEs)	56.5	48.0	8.5	15%
Staff time cost per year	$3.96M	$3.36M	$596,300	15%

Source: IDC's Business Value research, March 2023

Because study participants were able to achieve greater business confidence in their data protection and disaster recovery setup, they felt more comfortable introducing new products or applications. This had positive impacts on business operations and revenue. As shown in **Table 12**, on average, companies using Kyndryl received total additional annual revenue of $2,906,000.

TABLE 12

Business Operations and User Impact

	Per Organization	Per Application
Business impact — Revenue from better addressing business opportunities		
Total additional revenue per year	$2,906,000	$53,600
Assumed operating margin	15%	15%
Total recognized revenue per year — IDC model*	$435,900	$4,200

* The IDC model assumes a 15% operating margin for all additional revenue. Source: IDC's Business Value research, March 2023

ROI Summary

IDC's analysis of the financial and investment benefits related to study participants' use of Kyndryl Security and Resiliency Services is presented in **Table 13**. IDC calculates a total discounted five-year benefit of $37.5 million per organization ($692,400 per application) based on improved cross-organization cyber-resilience, better IT team productivity, and improved business results. These benefits compare with projected total discounted investment costs of $5.6 million per organization ($103,700 per application) over five years. IDC calculates that at these levels of benefits and investment costs, these organizations will achieve a five-year ROI of 568% and break even on their investment in approximately nine months.

TABLE 13

Five-Year ROI Analysis

	Per Organization	Per Application
Benefit (discounted)	$37.5M	$692,400
Investment (discounted)	$5.6M	$103,700
Net present value (NPV)	$31.9M	$588,800
ROI (NPV/investment)	568%	568%
Payback period	9 months	9 months
Discount factor	12%	12%

Source: IDC's Business Value research, March 2023

Challenges/Opportunities

Ransomware and other types of cyberattacks are the malaise of the day. As companies implement digital transformation to become digital first and derive revenue directly from digital products, the pace and volume of security threats and IT vulnerabilities will only serve to increase the threat to an organization's susceptibility. 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, 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.

However, it is important to note that Kyndryl and other vendors offering resiliency services are only a portion of the solution. The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) recommends a framework to guide organizations in addressing the cyberthreat. "Identify, protect, detect, respond, and recover" has become the standard approach that organizations take; resiliency services are strongest during the respond and recover phases. Identification, protection, and detection will require other software, hardware, and services vendors to build a complete cyberattack-ready solution.

Conclusion

Cyberattack is a top-of-mind concern for every organization, regardless of size or industry. It is an issue that garners attention across the organization, including executives, IT staffs, and line-of-business leaders. Moreover, it has become a fact of life and will only continue to evolve with technology.

Being cyberprepared demands the highest possible degree of digital resilience. Resilience goes beyond just recovering from attacks; it is a holistic endeavor to minimize any downtime or business consequences from cyberevents.

Digital resilience also goes beyond technology — it requires people and processes to effectively deploy the technology and respond agilely to unforeseen circumstances. IT organizations are realizing that the DIY or "go it alone" approach to digital resilience leaves them vulnerable to what they don't know. Engaging with a qualified organization that has the breadth of experience and expertise to ensure digital resilience greatly diminishes the odds of serious consequences from attacks. However, evaluating such organizations can be challenging due to broad-ranging solution differences and competing claims.

To assist IT buyers in differentiating between solutions, IDC conducts business value studies to assess the results from users of those solutions. While there are no assurances for any given organization, these assessments are a good indicator of what can be achieved. Our assessment of Kyndryl revealed a number of interesting results as reported by Kyndryl users: IT staff productivity improvement of $4.7 million, $3.4 million in risk mitigation, $1.8 million in business productivity gains, and $0.8 million in IT infrastructure cost reduction for a total of $10.7 million in benefits per organization. Additional benefits were seen in the areas of reduced downtime, faster recoveries, improved compliance, and more. Organizations in this study achieved an ROI of 568% and a nine-month payback, numbers that easily justify the investment.

Appendix: Methodology

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from current users of Kyndryl Security and Resiliency Services.

Based on interviews with these organizations, 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 Security and Resiliency Services.** In this study, the benefits included IT cost reductions and avoidances, staff time savings and productivity benefits, and revenue gains.
2. **Created a complete investment (five-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Kyndryl Security and Resiliency 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 Security and Resiliency Services over a five-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 productivity savings. For purposes of this analysis, 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-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 Kyndryl 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 IDC Analysts

Harsh Singh

Senior Research Analyst, Business Value Strategy Practice, IDC

Harsh Singh is a senior research analyst for IDC's Business Value Strategy Practice, responsible for developing return-on-investment and cost-savings analysis on enterprise technological products. Harsh's work covers various solutions that include datacenter hardware, enterprise software, and cloud-based products and services. Harsh's research focuses on the financial and operational impact these products have on organizations that deploy and adopt them.

More about Harsh Singh

Phil Goodwin

Research Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

Phil Goodwin is a research vice president within IDC's Enterprise Infrastructure Practice, covering research on data management. He 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. Phil 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

Frank Dickson
Program Vice President, Cybersecurity Products, IDC

Frank 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

Message from the Sponsor

kyndryl™

Kyndryl is the world's largest IT infrastructure services provider, serving thousands of enterprise customers in more than 60 countries. The company designs builds, manages, and modernizes the complex, mission-critical information systems that the world depends on every day.

Kyndryl Security and Resiliency provides the expertise, services, and technologies that help enterprises anticipate, protect against, withstand, and recover from adverse conditions, stresses, attacks, and compromises of cyber-enabled services. Our integrated approach helps customers embed cyber resilience into the broader IT and operational strategy, underpinned by cloud and zero trust principles.

For more information, visit www.kyndryl.com/us/en/services/cyber-resilience

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 Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200