Resilience Risks That Imperil Financial Services Operations

Pathfinder

November 2021

Commissioned by

kyndryl™

451 Research

S&P Global
Market Intelligence

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About the Author

Eric Hanselman

Principal Research Analyst

Eric Hanselman is the Principal Research Analyst at 451 Research, a part of S&P Global Market Intelligence. He has an extensive, hands-on understanding of a broad range of IT subject areas, having direct experience in the areas of security, networks, application and infrastructure transformation and semiconductors. He coordinates industry analysis across the broad portfolio of 451 Research disciplines, contributes to the Information Security and Cloud Native Channels, and is a member of the Center of Excellence for Quantum Technologies.

The convergence of forces across the technology landscape is creating tectonic shifts in the industry, including 5G, SDN/NFV, edge computing and DevSecOps. Eric helps 451 Research's clients navigate these turbulent waters and determine their impacts and how they can best capitalize on them. For more than 20 years, Eric has worked with segment leaders in a spectrum of technologies, most recently as CTO of Leostream Corporation, a virtualization management provider. Prior to that, Eric guided security offerings for IBM and Internet Security Systems. At Wellfleet/Bay Networks and NEC, he was involved in the introduction of many new technologies ranging from high-performance image analysis to rollouts for IPv6.

Eric holds a patent in image compression systems. He is also a member of the Institute of Electrical and Electronics Engineers (IEEE), a Certified Information Systems Security Professional (CISSP) and a VMware Certified Professional (VCP), and he is a frequent speaker at leading industry conferences. Eric majored in Chemistry at Reed College.

Executive Summary

Enterprises have been moving rapidly to adopt new models of infrastructure to support the more distributed, dynamic and digital nature of their businesses. That infrastructure expansion has strained their traditional security and operational resilience capabilities. The combination of these stresses can greatly increase risk if the full extent of the hazards that they create aren't fully understood and addressed.

These problems are particularly acute in financial services, where expanding regulatory requirements add to operational concerns. The combination of constantly advancing cybersecurity threats and ever-increasing new streams of data – in addition to hidden challenges like concentration risk that new supply chains and infrastructure models can create by cloaking dependence on shared third parties – can leave organizations at even greater risk if they don't address these challenges.

Key Findings

- The pandemic increased awareness around the significance of business continuity.
- The urgency of implementing resilience is fading, which might cause enterprises to shift priorities, but the need for resilience remains, raising risk for those that fall into this trap.
- Financial services organizations face additional regulatory pressure to ensure business continuity and resilience.
- Hybrid infrastructure can be effectively managed to deliver business agility and enhance resilience.
- Many hidden elements of operational risk can be mitigated while achieving improvements in operational efficiency.

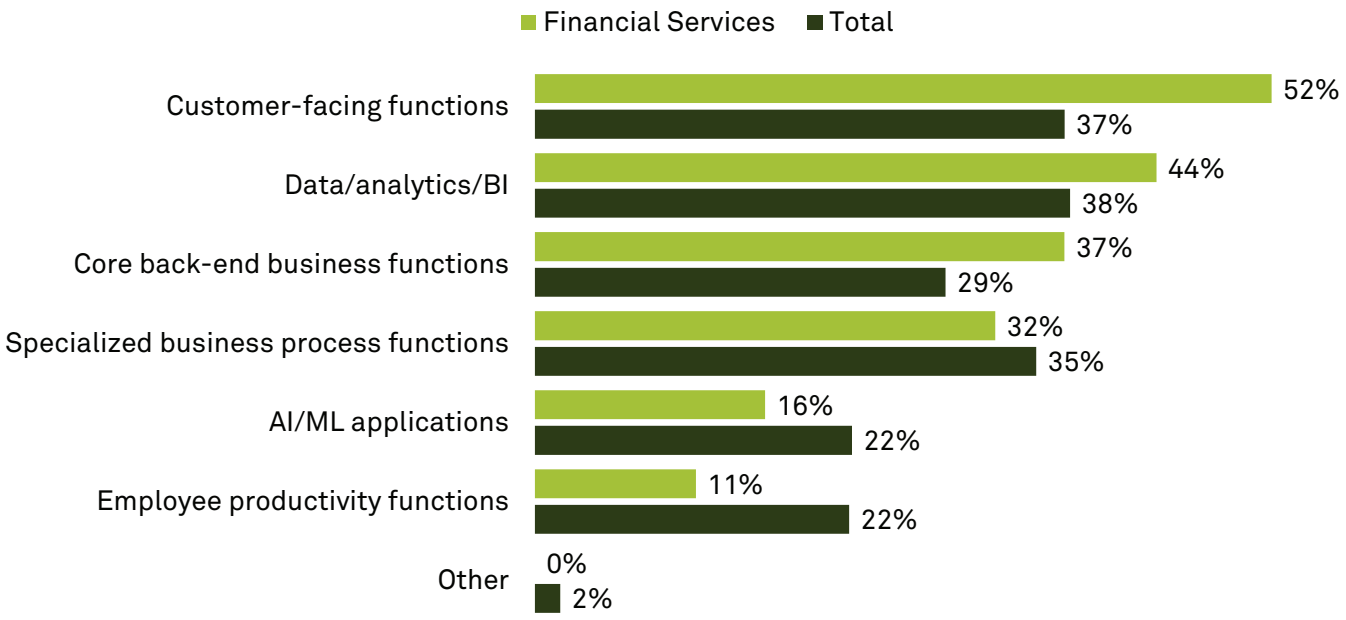
Digital Finance Imperatives Require Resilience to Manage Risk

Financial organizations' business imperatives to get closer to clients through projects such as mobile banking and digitization are driving the adoption of new infrastructure choices such as cloud computing. Firms need to expand their capabilities to ensure that their infrastructure is flexible enough to keep their businesses competitive and meet new regulatory requirements, while keeping their systems resilient to support them.

The need for greater resilience in IT infrastructure has always driven organizations to pursue improvements in their systems and operating procedures, but new requirements from financial services regulators around the globe are increasing the sense of urgency here. Meanwhile, the effects of the global pandemic have only intensified the drive to heighten levels of resilience. A challenge that many financial services organizations face is that they are attempting to improve their resilience at the same time that the infrastructure they support is growing more complex. As part of their resilience enhancements, they must control that complexity.

Financial services firms are reporting notably higher priority for projects around customer-facing applications and expanded data use, according to a recent 451 Research study. The Voice of the Enterprise: Digital Pulse Workloads and Key Projects study results indicate that these types of projects, which typically have greater requirements for extended infrastructure, are topping their lists to a greater degree than the average enterprise. Improving customer experience for these applications requires placing workloads closer to end users to ensure adequate performance. At the same time, it also drives the need to distribute enterprise data.

Figure 1: Application Priorities for Financial Services Organizations



Q. Which of the following application types is your organization prioritizing this year? Please select up to two.
Base: All respondents (n=504); Financial services respondents (n=62)
Source: 451 Research's Voice of the Enterprise: Digital Pulse, Workloads and Key Projects 2020

The need to improve application performance for a more dispersed set of customers is one of the motivations for increased use of hybrid multicloud strategies. The ability to leverage different services and analytical capabilities can create additional motivations. They are useful options, but they also increase the challenges that IT teams must address.

There are three important areas to be aware of:

1. The first challenge relates to the extension of infrastructure beyond existing operational boundaries. These new realms are generally beyond the visibility, controls and protections of existing systems and procedures. Organizations must either extend their existing systems or work out how to integrate native cloud capabilities to maintain operational effectiveness.
2. The second challenge is the expansion and evolution of cybersecurity threats and the additional attack surfaces that new infrastructure elements create. That increase is driven by a number of factors. There is the addition of new resources, and these bring with them additional control and management interfaces and expanded network connectivity, all of which have to be protected. The increased complexity of cybersecurity management comes in addition to new operational models and native controls that can offer different security characteristics than those on-premises. There is also an associated risk from potential configuration errors that could inadvertently expose data or open avenues for attackers.
3. Regulatory requirements are always a challenge for financial services firms, and the expansion of these requirements around technology is the third area where organizations can see increasing strain. A growing number of financial regulatory bodies are establishing cyber protection and resilience requirements. These extend the historic focus on financial operating capacity into assessing the impact tolerance of IT infrastructure and its ability to withstand technical failures.

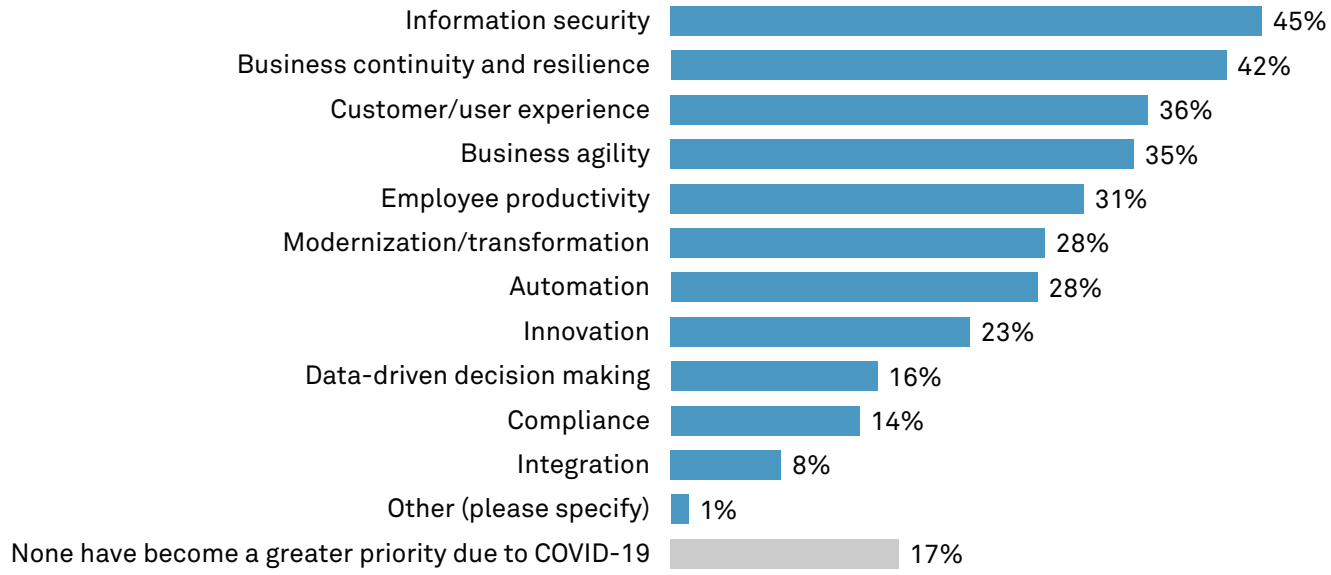
All of these challenges require that organizations improve their ability to manage, secure and optimize their operational capabilities to address today's pain points and be ready for the future.

Continuity and Resilience Become Top Priorities

One of the benefits that the pandemic-related upheaval brought was an increased focus on resilience and continuity. Emergency planning capabilities were put to the test as organizations worked to deal with urgent changes. It's something that another 451 Research Voice of the Enterprise (VotE) study tracked as the pandemic proceeded.

In October 2020, business continuity and resilience was selected as the number two overall technology objective that had become a greater priority for respondents due to the pandemic (see Figure 2). It's an indication of the focus that was created by the need to keep businesses running with the dramatically altered conditions that they faced.

Figure 2: Technology Objectives, October 2020



Q. Which of the following technology objectives, if any, have become a greater priority for your organization due to the influence of the coronavirus (COVID-19) outbreak? Please select all that apply.

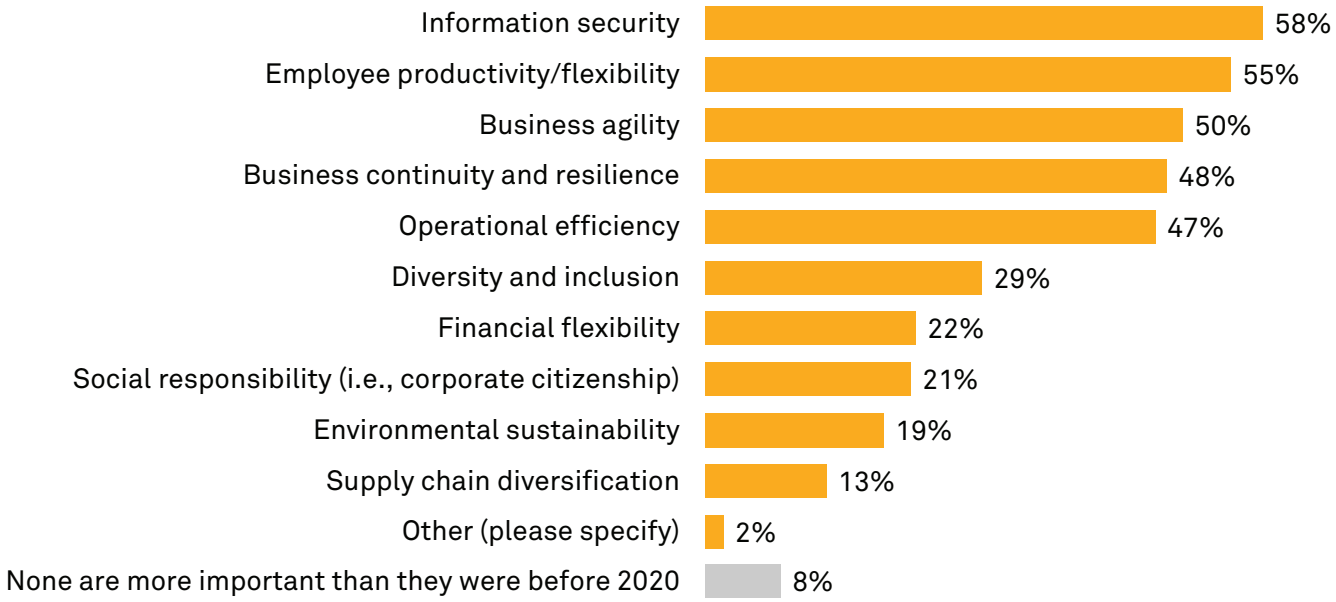
Base: All respondents (n=371)

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey October 2020

Organizations, much like the people that run them, have shifting priorities, and the urgency of the moment had faded by the next iteration of the study, conducted in July 2021 (see Figure 3). Business continuity and resilience slipped down the list of current priorities, as businesses looked more closely at managing business agility and employee productivity. For financial services organizations, the effect seems larger. While the sample size is relatively small, among financial services respondents, business continuity went from being a strong second priority to being the sixth most important of the set of responses. The margin of error is larger at these small sample sizes, but the shift in focus seems clear.

The focus on security remains strong, as it topped the list of objectives in both studies, but these results are an indication that businesses may be getting distracted by near-term concerns. Security objectives have strong and constant drivers in financial services, both through internal traditions and with regulatory requirements. A strong light was shown on business continuity and resilience by the immediate disruption of the pandemic, and now increasing regulatory requirements are coming into play as well. But there isn't the same history and organizational experience around focus on resilience for many financial services firms, and that can increase risk as they expand to new forms of infrastructure. If they don't continue to invest at the levels required to maintain that most critical of capabilities – being ready when customers need them – their business could suffer.

Figure 3: Technology Objectives, July 2021



Q. Which of the following business objectives – if any – are now more important to your organization's decision-making process than they were before 2020? Please select all that apply.

Base: All respondents, excluding 'don't know' responses (n=420)

451 Research's Voice of the Enterprise: Digital Pulse, Business Reinvention and Transformation 2021

Hidden Elements of Risk Exposed

Delivering on the requirement for business continuity is complicated in hybrid IT environments by elements of risk that can be considerably harder to discern than in traditional IT infrastructure. The risks associated with adding new IT infrastructure elements through cloud service providers can appear simple – businesses integrate third parties regularly and have established vetting processes. But as recent headlines have shown, there is additional risk with IT service providers due to the opacity of their supply chains. These are areas that can be more complex to fully discern. It means that organizations have to expand the scope of their resilience planning to account for these additional factors.

Another risk area that can be difficult to fully assess in new infrastructure models is concentration of facilities and suppliers. Much like issues with path diversity in complex telecommunications networks, it's necessary to understand how much shared infrastructure various cloud providers utilize. It's not uncommon for different cloud providers to host portions of their environments in the same third-party facilities. They may depend on the same suppliers for systems and equipment. Businesses need to think beyond the simple logic of service-provider diversity to ensure that their environments can deliver the resilience they expect.

One of the vulnerabilities that the pandemic laid bare in some circumstances is operational risk. The unanticipated changes it created strained processes to the breaking point, as personnel weren't available and facilities closed. The difficulty with understanding operational risk is that gaps in processes can be triggered by complex interactions that weren't foreseen in their planning and implementation. This is an area where it can be difficult for an organization to know what it doesn't know about hidden dependencies.

Managing Risk in a Hybrid IT World

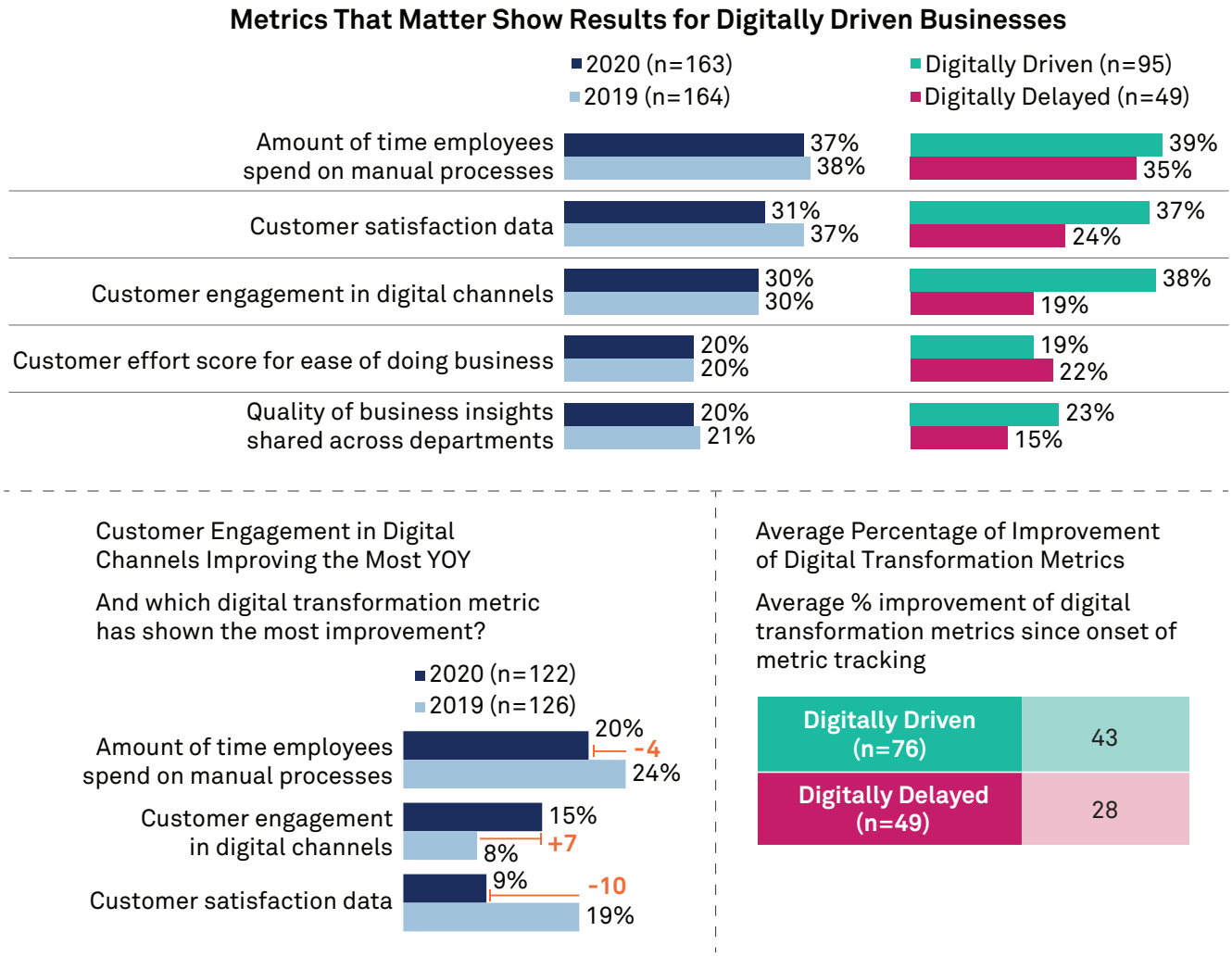
To manage risk in increasingly complex IT infrastructure, it can be helpful to focus on the areas of most significant value. Rather than focusing exclusively on controls for infrastructure elements, attention should be given to one of the areas of greatest business value – data – and understanding how to protect it effectively. The first step for many in assessing data protection is evaluating data security, but this approach risks overlooking an equally crucial aspect of data value: its availability. Data protection has to be looked at holistically if it's going to be effective.

Shifting Data Protection Strategies

Simply identifying and locating data sources and repositories can be a challenging and time-consuming task for organizations, but it's a critical one. Digitization can make significant improvements in business competitiveness, and data is what fuels that engine. It's a fuel that is much more valuable as businesses depend on it as a key element of digital transformation efforts, so it requires even greater protection.

In a recent VotE Digital Transformation study, digitally driven firms – defined as those with formal digital transformation strategies and/or typically early adopters of technology – reported significantly greater improvements in a range of metrics than those that had not made similar investments (see Figure 4). Those metrics included the amount of time that employees spent on manual tasks, as well as customer satisfaction and the quality of business insights.

Figure 4: Digital Transformation Delivers Results



Q. How is your organization measuring its digital transformation progress beyond traditional metrics (e.g., amount of increased revenue and cost reductions)? Q. Which one digital transformation metric has shown the most improvement since you began tracking it?

Base: Digital transformation leaders and learners

Q. Approximately how much has this metric improved – if at all – since you began tracking it? (% improvement)

Base: Digital transformation leaders and learners who are tracking digital transformation metrics

Source: 451 Research's Macroeconomic IT Spending, Digital Transformation 2019 & Digital Transformation 2020

Better data management is needed to protect those competitive benefits, and can also be a driver to achieve the benefits of digital transformation. Comprehensive identification of data across increasingly hybrid infrastructure is crucial to protecting and managing it, and can also be a pathway to greater utilization of that data across the organization. When organizations know the full breadth of their data resources, they're better able to put them to work, and data management can ensure that they'll be able to provide that value reliably. That's a building block to improving the value of overall digitization efforts.

While digital transformation has increased the value of data, changes in the nature of cyberattacks are shifting the priorities around the types of data protection being deployed. Air-gap technologies are now not only critical for regulatory compliance; they also address urgent needs to deal with the impacts of data-focused attacks such as ransomware incidents. The immutability that air-gap technologies provide can mitigate such risk. They can be complex to manage, however. To achieve effective isolation of resources and data while still delivering broad availability, managed offerings can be a path to implementing these approaches efficiently.

A big part of data protection strategies is the ability to ensure that data is available wherever it's needed. An organization's infrastructure agility depends on data being available to feed workloads across the environment to ensure performant interactions with customers. Data replication, protection, distribution and synchronization are just as important as availability.

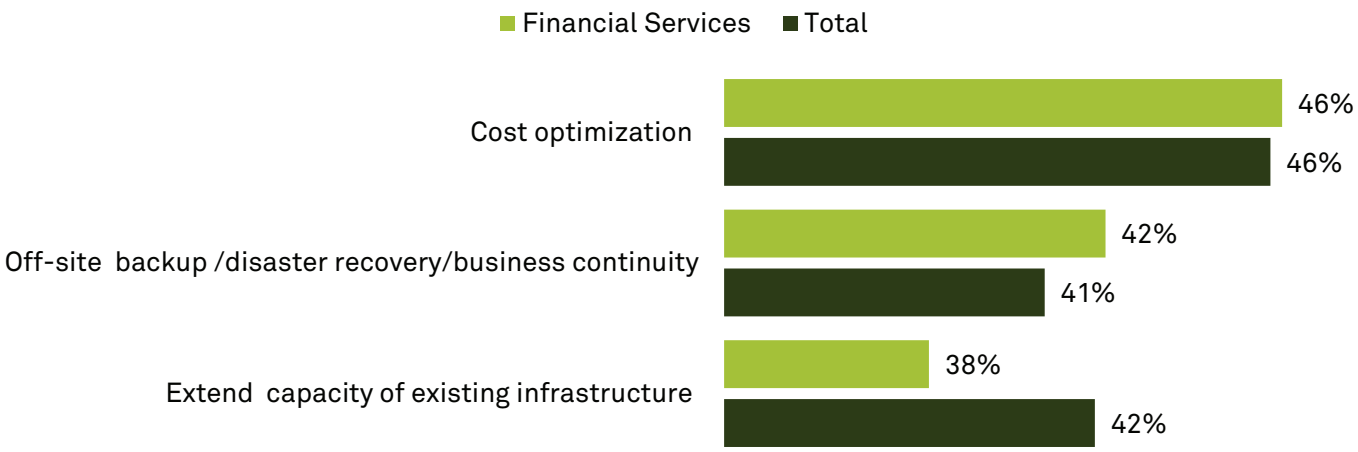
Data protection capabilities are also the linchpin for managing compliance in complex IT environments. By knowing where data is stored and managing access to it, a range of compliance mandates can be met more easily. Consolidating data management can reduce the amount of work needed to complete compliance-related tasks. Where data sovereignty concerns are in play, effective data management can more clearly identify data flows and locations.

Building in Infrastructure Resilience

The complexity of hybrid multicloud infrastructure patterns might seem daunting, but, when effectively managed, they can offer significant advantages in terms of business continuity and resilience. The ability to shift workloads to new environments offers a fundamental operational improvement that can mitigate the impact of natural disasters, infrastructure failures and cyberattacks. It's an advantage that financial services organizations recognize and appreciate.

In a recent VotE Cloud, Hosting and Manage Services study, financial services organizations ranked business continuity/disaster recovery higher as a driver for hybrid IT architectures than the broader market did. It was their number-two driver for hybrid IT, where the average respondent ranked it third after cost optimization. That's an indication of the importance of multicloud capabilities to financial services organizations as they look to improve their availability and resilience.

Figure 5: Top Three Use Cases for Hybrid IT



Q. Which of the following use cases are driving your organization's implementation of hybrid IT environments? Please select up to 3.
Base: Have hybrid IT, considering or planning to have, abbreviated field (n=183)
Source: Voice of the Enterprise: Cloud, Hosting & Managed Services, Vendor Evaluations 2020

Achieving high levels of infrastructure agility depends on the comprehensive use of automation. Automation offers scale and standardization in infrastructure operations, and has historically been underutilized in most enterprises. The ability to ensure operational repeatability and reduce the risk of human error is a key part of not only making operations more efficient, but also improving the speed of recovery in the event of an incident.

Automation allows for the rapid replication of failing elements in new environments, reducing outage times. Automation is also a means of abstracting away the operational differences among various elements of a hybrid multicloud infrastructure. When properly implemented, it can translate requirements into the native capabilities of the different cloud resources in use.

Enhancing Cybersecurity and Remediation by Meeting Evolving Visibility and Control Needs

The greatest challenge in delivering effective security in distributed environments is not the task of dispersing controls, but rather establishing visibility across these extended infrastructure elements. Ensuring that the telemetry needed to establish situational awareness is available is a critical first step in security management.

Organizations need to work at creating the means to integrate information from new infrastructure into their existing security systems. In some cases, this may require translating or transforming those streams from their native formats in order to maintain the context that is associated with them. Loss of context with new security streams can be just as much of a problem as not having the data itself. Visibility is key part of an organization's ability to identify impacts and their severity, and shorten the reaction time to remediate them and lessen their effects.

Hybrid environments will have varying control capabilities, and organizations need a means to address these differences. Establishing control abstractions that can be translated into the native capabilities in each infrastructure realm is a way to ensure that equivalent controls are implemented across the entire infrastructure. This can also be a way to identify gaps in capabilities, where the full control requirements may not be available in certain places. As such, it presents an opportunity to evaluate how to deploy banking applications with the necessary protections prior to deployment. It can identify appropriate locations for applications before deployment as well, enabling organizations to understand the real costs of different infrastructure options.

The goal in securing hybrid infrastructure has to be the implementation of effective controls that can protect data and workloads, and also be operationally efficient. Compliance with regulatory requirements should be a by-product of the security implementation – not the goal. Starting with compliance requirements can lead to a patchwork of controls and systems, with each looking to address specific needs, rather than a comprehensive design that offers the controls that regulations require. By focusing on the broader capabilities and operational workloads, organizations can build systems that provide the protections they need while managing staffing levels to support them.

Cyber protection and recoverability requires good planning and preparation. It also calls for automation of the recovery processes at the data, application and infrastructure levels if it is to offer true operational resilience and business continuity.

When security environments have the visibility and controls they need, they can effectively address the threats they face. It's important for organizations to actively expand their understanding of new threats. Adversaries are investing in new tools and tactics, and effective protection plans must do the same. Incorporating threat intelligence and services from security providers can be an effective catalyst to drive risk assessments around new threats and threat actors as they emerge. Security capabilities cannot be static if they're going to remain effective over the long term. Security is a critical part of business continuity and resilience planning for any financial services firm.

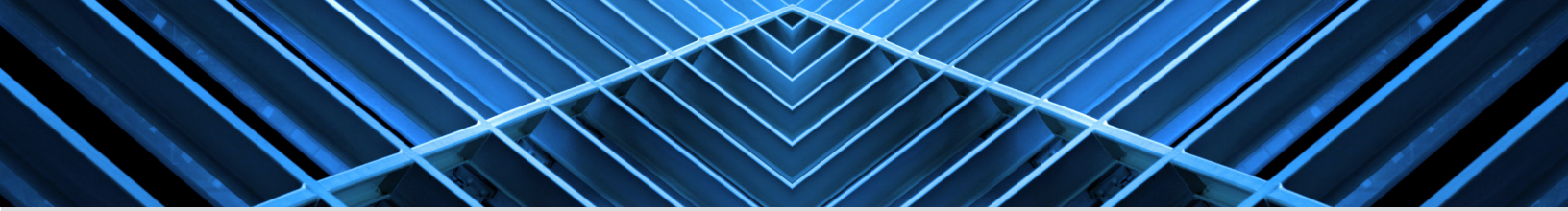
Conclusions

The challenges that financial services organizations face are more acute within the turbulent conditions that exist today. Organizations are being pressed to grow and adapt to new market realities while ensuring that their infrastructure is scalable, performant and secure. They have to do this in the face of greater regulatory requirements to prove themselves resilient, all while addressing expanding customer requirements.

While this sounds like a monumental task, it's one that is achievable with reasonable planning and a real understanding of the risks involved. By building successful data strategies to meet the requirements of modern digital financial services, forward-looking firms can become successful digital enterprises.

Critical issues for financial services organizations to keep in mind include the following:

- Identifying the best execution venue for an application – such as placing workloads closer to end users to ensure adequate performance – will help improve overall customer experience.
- Extension of the banking infrastructure beyond existing operational boundaries signals a need for new controls and protections to ensure the tolerance of the infrastructure and its ability to withstand technical failures.
- Management of risk in increasingly complex IT infrastructure should not solely be focused on infrastructure elements – data protection must be holistic for it to be effective.
- Infrastructure agility calls for automation, which offers operational repeatability, operational efficiency and reduced risk**,** and which supports data, application and infrastructure recoverability.



content provided by: kyndryl

In a complex heterogeneous cloud environment, achieving operational resilience demands an integrated approach to detect and respond to threats, safeguard data, ensure high availability, and quickly recover critical business processes and systems in the case of a disaster. An integrated cyber resilience strategy and plan comprising the skills, services, and technologies that support growing compliance requirements is the first step in creating such an orchestrated platform.

Kyndryl Security and Resiliency provides a comprehensive range of platform-agnostic services to assist businesses in developing and implementing enterprise-wide cyber resilience policies to help them de-risk their journey to cloud. Kyndryl's expertise, processes and technologies help enterprises keep their critical systems secure, available, reliable, and recoverable across heterogeneous environments, regardless of their size and complexities, while supporting evolving compliance needs.

Kyndryl's Security & Resiliency services help clients across the world design, build, transform, and manage cyber security and resiliency capabilities – ranging from integrated threat management platform with detection, protection, response and recovery to hybrid platform recovery with data protection, disaster recovery, high availability, cyber resilience service, and IT resilience orchestration services. For more information, please visit https://www.kyndryl.com/services/business-continuity

About Kyndryl

Kyndryl is the world's largest IT infrastructure services provider. The company designs, builds, manages, and modernizes the complex, mission-critical information systems that the world depends on every day. Kyndryl's nearly 90,000 employees serve over 4,000 customers in more than 60 countries around the world, including 75 percent of the Fortune 100. For more information, visit www.kyndryl.com.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence