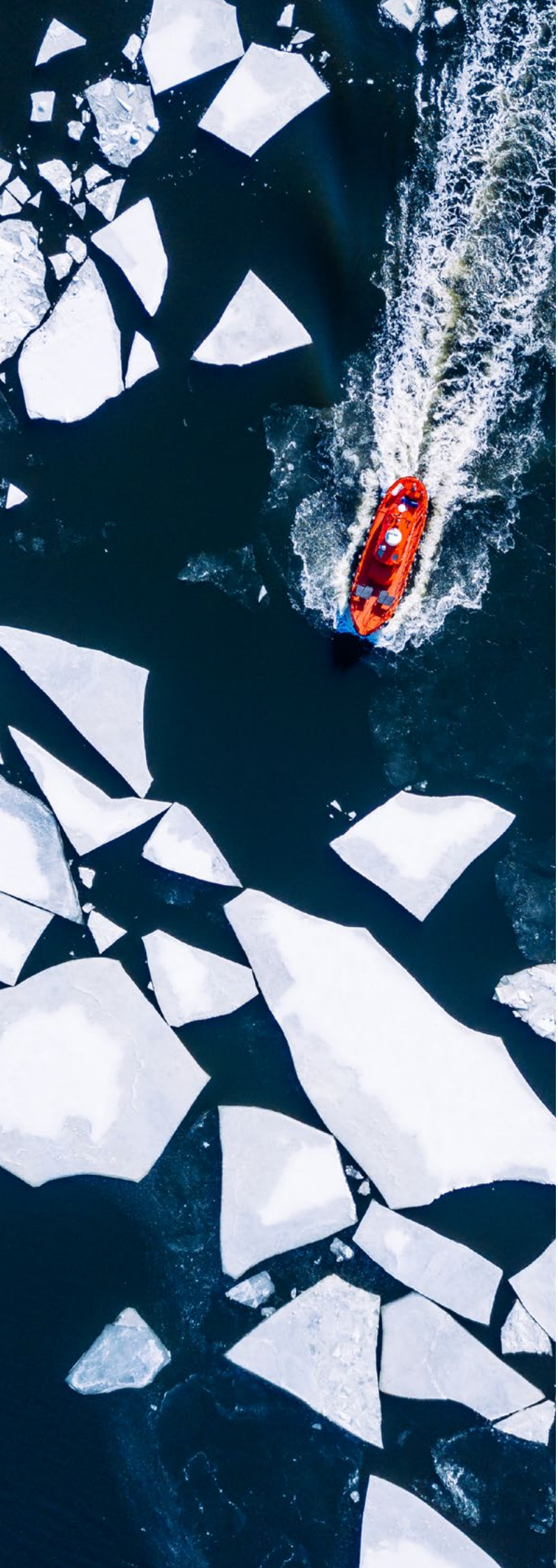

Expert Insights

—

A CIO’s guide to extreme challenges

Four steps to radical agility and resilience

IBM **Institute for Business Value**

IBM

Expert on this topic

Fletcher Previn

Chief Information Officer
IBM

As IBM’s Chief Information Officer, Fletcher Previn leads a global team of more than 12,000 employees. The team’s mission is to prioritize user experience and provide secure, global IT for 350,000 IBM employees worldwide. Under his leadership, Fletcher has helped IBM pioneer new ways of delivering IT across one of the world’s largest networks, helped establish an agile culture, and embedded design into operations (DesOps). Fletcher has been with IBM since 2006.

As the COVID-19 pandemic and other recent environmental disasters demonstrate, massive disruption to any aspect of life can arise suddenly.

Key takeaways

Every crisis brings with it an element of the unknown. We can't possibly plan for every contingency. But we can try.

Based on our experience at IBM, we have put together a four step Action Guide for the CIO: (1) Modernize the applications environment, (2) Modernize network capacity, (3) Modernize the workplace, and (4) Modernize operations.

When business continuity is called into question, all attention shifts to the CIO. Resiliency is a mindset we need to encourage and promote.

CIOs have the opportunity to help keep their organizations together, navigate the current stresses and strains, and help employees, customers and partners come out the other side.

Into the unknown

In crisis, we don't have the luxury of figuring things out from scratch. We need to anticipate in advance how to react and make good decisions quickly. Time wasted undermines a successful response.

Every crisis brings with it an element of the unknown. We can't possibly plan for every contingency. As the COVID-19 pandemic and other recent environmental disasters demonstrate, massive disruption to any aspect of life can arise suddenly, with follow-on effects that are both long-lasting and difficult—and often as not, also impossible to anticipate.

For businesses, revenue streams may disappear overnight. Top customers may come under extreme strain, partners might suddenly be unreliable, and regulators may be missing in action. Key executives and other stakeholders might be unavailable. Business-as-usual decision making processes may become broken. And time to recovery may be anyone's guess.

How can businesses and communities continue to function when employees, communications networks, and the ability to work together are suddenly disrupted? (See sidebar, "Insight: In a crisis, private yields to public.") And how can they do so while limiting negative impact on employees, clients and the communities they serve?

Insight: In a crisis, private yields to public

Companies focused on winning in the marketplace must change gears instantly during a public health crisis or in the wake of a major environmental disaster. Decisions suddenly need to focus on the common welfare. Doing otherwise can be not only detrimental to operations, it can do irreparable harm to the organization's reputation and brand integrity.

As with operational decision making, public policy should be well thought out in advance of disaster, with organizational assets and resources pre-factored into alternative design, development and distribution patterns. We need to ask ourselves how might our company function for the public good when called upon to do so?

In the midst of crisis, it is difficult to forge strong partnerships with the public sector because of the level of consensus and coordination required. Public-private partnerships should be in place before disaster strikes, with governance established, so response can be quick and decisions made without encumbrance.

For example, IBM has a long history of strong collaboration with government laboratories in pushing the limits of supercomputing. Therefore, in the midst of the COVID-19 pandemic, IBM and its public sector partners shifted priorities to make an unprecedented amount of computing power available—currently more than 330 petaflops and counting. This additional computing capacity enables researchers worldwide to rapidly develop pandemic and disease-related insights. The COVID-19 High Performance Computing Consortium partners include NASA, MIT and RPI, the Lawrence Livermore, Argonne, Oak Ridge, Sandia and Los Alamos National Laboratories, the National Science Foundation, and other industry partners.[1]

Two critically important applications of this supercomputing capacity could include new potential therapies, as well as a possible vaccine and developing predictive models to assess how the disease is progressing. The consortium will collaborate on reviewing proposals from researchers worldwide, making supercomputing resources available to projects that can make the most immediate impact, and providing technical assistance to researchers utilizing the systems.

Reality of the now

It has been estimated that as of March 19, 2020, as many as 88 percent of global organizations have encouraged or required employees to work from home.[2] While the situation in each country is constantly changing, if the 88 percent estimate is accurate for the United States, this would represent more than 127,000,000 people now working from their home or other non-standard location.[3]

In a 2018 analysis by the US Bureau of Labor Statistics, 29 percent of US workers indicated they had the requisite setup and equipment to successfully work away from the office, and only 5.3 percent usually did so—as few as 8 million workers.[4] Almost 120 million American workers may be trying to maintain operations and productivity without the systems and structures —or day-to-day experience—to successfully conduct their work remotely. A massive challenge for any organization. And of course, a major risk.

Enterprise IT is the mechanism that can keep a business operational and effective even under the current extreme and unprecedented conditions—such as the ones we are all experiencing today. And in this, CIOs are central.

While CIOs of course, planned in advance for disruptions that were anticipated, they—we—hopefully built capacity, redundancy and flexibility to deal with disruptions that were not. But even in the most risk-averse planning for the unknown, the current situation has been improbable and profoundly unique.

Being CIO of a company like IBM has meant that some aspects of preparedness were long-established. For decades, we have had a deeply diverse, technically literate workforce. Our teams are accustomed—and immediately prepared—to work remotely. Moving to almost 100 percent remote working was a challenge. But not nearly as great a challenge as for other organizations largely unused to and unequipped for remote working.

Achieve resiliency through scale, speed, and flexibility.

It's likely that you as a CIO have already triaged for immediate business continuity and productivity. However, there are steps you now need to take to harden systems and structures for the remote working environment to bolster resilience, stability and security.

To help guide the way with reference to our experience at IBM, my team and I have put together a four-step Action Guide for what's next for the CIO. Four steps to radical agility and resilience. I hope it's helpful.

Step 1. Modernize your applications environment: Fully commit to cloud-based flexibility

No one can afford to waste computing resources on capacity that's not being used. But that doesn't mean you can't plan for redundancy at scale. Modern cloud-based environments provide extra compute capacity that you pay for only when needed.

To properly prepare:

- *Embrace hybrid multicloud design*. Multicloud design patterns and service brokerage models allow commodity workloads to be delivered by multiple providers. While you may enjoy preferred relationships, you should also have options to shift workloads across clouds and cloud providers without hampering performance.
- *Shift to "as-a-service" strategy.* Use cloud-based tools, applications and platforms. Many software-as-a-service (SaaS)-based solutions are delivered at scale across the globe, further reducing the risk of service disruption.
- *Use partners to supplement provisioning and capacity.* Shift and share responsibility for infrastructure with your cloud partners. Cloud-based architectures provide elasticity and burstable capacity, and reduce the risk of single points of failure.
- *Know your cloud provider's service priorities.* Cloud providers serve thousands of other clients. How will your make its triage decisions for capacity in times of peak utilization? CIOs need to know and plan accordingly.

Step 2. Modernize your network capacity: Build out for sudden demand

As with compute power, it's crucial to plan ahead for surges in bandwidth need and potential availability constraints during unexpected events. This includes adopting modern approaches to networking, authentication and security, such as:

- *Use software-defined wide area networks (SD-WAN).* They will enable you to build excess capacity without taxing limited resources.
- *Exploit a zero-trust security strategy.* Contextual and multi-factor authentication will enhance security and reduce reliance on Virtual Private Networks (VPN).
- *Optimize traffic using split-haul VPNs and endpoint EDR.* Take advantage of modern remote access architectures by using split tunnel VPN combined with advanced endpoint detection and response (EDR) capabilities. Together these techniques provide full endpoint visibility without requiring all VPN traffic to be backhauled into the corporate network. In addition, selectively routing high traffic workloads across SD-WAN can further optimize performance and keep unnecessary traffic off the corporate backbone.
- *Keep Points of Presence (POPs) close.* The telecommunications point of presence (PoP) should be physically close, co-locating servers with PoPs, if possible. This helps reduce latency, provides additional carrier diversity, capacity, and redundancy options, and can be a valuable asset in making dynamic routing decisions based on real-time traffic needs. PoPs also provide the ability to "private peer" with partners and avoid sending that traffic over the internet.
- *Employ virtualized appliances.* Virtualized VPN appliances are now available from most major networking companies. While the total concurrent user capacity of each virtual appliance may not be at parity with a dedicated hardware appliance, virtual appliances can quickly add capacity without needing to ship hardware—a distinct advantage when supply chains are disrupted.

Events such as the COVID-19 pandemic can suddenly transform everyone into a remote worker.

- *Establish private peering for high bandwidth consumers.* Avoid routing excessive traffic over the internet by using dedicated connections for partners that consume the most bandwidth.
- *Invest in carrier diversity.* As with ensuring access to multiple clouds, each VPN hub should have access to at least two different carriers for redundancy, as should critical office buildings.

Step 3. Modernize the workplace: Create agility for productive employees

Many workers, especially knowledge workers, should be able to work productively anywhere—the office, a client location, while traveling, and from home. Sudden disruption of *work location* should not disrupt *work*—as long as we have modernized our workplace and workforce enablement practices.

- *Define a strategy for remote work.* Define clear guidance, rules, and policies. Train employees on remote etiquette—virtual meetings are different than in-person meetings—and how your company's culture will inform the way they work remotely.
- *Create a digital environment for remote work.* Provide tools that enable distributed teams to collaborate and contribute. Allow employee choice for aspects of the work environment that are less critical, such as which specific devices or email clients they use. But standardize critical productivity platforms, such as communications tools and virtual collaboration spaces.
- *Provide cybersecurity training specifically for remote work.* The risks of working from home are different than those in the office. Be sure to update policies and training regularly to account for changes in technology and ways of working.
- *Empower senior leaders to lead from anywhere.* Some tools, such as WebEx-enabled leadership teams or boards, can help. While senior leaders may rarely think of themselves as "work from home" employees, events such as the COVID-19 pandemic can suddenly transform everyone into a remote worker.

Step 4. Modernize operations: Decide now how you will decide then

Excellent planning only goes so far. Each unexpected event will have its unique moments, requiring on-the-spot decision making. While the decisions themselves can't be made in advance, *how* you analyze, collaborate, come to conclusions, and coordinate efforts *can* be mapped out. The same applies to channels of communications and guidelines for how to adapt to unforeseen constraints.

- *Employ agile methods.* Apply the underlying principles of agile methodology, not just in software development or to application design projects, but across the workforce and at leadership levels. Modern ways of working are supported by modern tooling. Make the needed investments in a productive, modern environment for your workforce.
- *Define minimum viable meetings (MVMs).* Pare meetings to their essential core by pre-defining teams, meeting structure and duration in advance. Senior leaders also need a pre-defined channel for conveying the latest on the health of the company's digital estate, including capacity, cyber, and usage trend data. This will enable quick, effective decision making during a crisis. For example, during the current health crisis, my IBM CIO team meets three times per day to share a current snapshot of IBM's digital estate, and then shifts resources as needed, based on time zones and demand. Also, I meet twice daily with a joint group of leaders from across IBM, including cyber experts, legal representatives, privacy gurus, and others.
- *Practice governance by design.* This includes contextual controls that don't introduce friction and aren't subject to user interpretation. These controls function less like legalistic rules and more like highway guardrails: we trust employees to drive their own "cars," but we define the parameters of the "highway" on which they drive.
- *Train your teams and leaders in advance.* Everyone should know how things will work in an emergency. Run simulations, conduct operations drills, allow teams to practice, and model behaviors they should imitate.

What's most important NOW

When business continuity is called into question, all attention shifts to the CIO. The events of the past few months have brought unprecedented impacts to global business operations and the global workforce. Companies are scrambling to implement contingency plans for risks they never saw coming. Because a modern economy is built upon data insights and technology, CIOs are under enormous pressure to deliver.

There are more resources available to CIOs than ever before. Application providers, cloud infrastructure providers, services and data partners, suppliers, customers, and regulators all have a vested interest in helping each other transform risks and unknowns into more familiar steady states and business as usual. Resiliency is a mindset. Only on the far side of crisis can we look back and recognize the seeds of opportunity. The time for leadership is now. As a CIO, you are now at the center of the arena.

Notes and sources

1 COVID-19 High Performance Computing Consortium. March 2020. https://www.ibm.com/covid19/hpc-consortium

2 Gartner HR Survey of 800 global HR executives. Published March 19, 2020. https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88--of-organizations-have-e

3 U.S. Bureau of Labor Statistics. Accessed March 28, 2020. Total US workforce in 2018 was 144,295,000. https://www.bls.gov/news.release/flex2.t01.htm

4 U.S. Bureau of Labor Statistics. Published September 30, 2019. Twenty-nine percent of wage and salary workers could work at home in their primary job in 2017–18, and 25 percent did work at home at least occasionally. https://www.bls.gov/opub/ted/2019/29-percent-of-wage-and-salary-workers-could-work-at-home-in-their-primary-job-in-2017-18.htm; U.S. Census Bureau 2018 American Community Survey. Published October 18, 2019. 5.3% of US worked usually worked from home in the past week. https://www.enotrans.org/article/2018-acs-survey-while-most-americans-commuting-trends-are-unchanged-teleworking-continues-to-grow-and-driving-alone-dips-in-some-major-cities/

About Expert Insights

Expert Insights represent the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
April 2020

67031367USEN-00