McKinsey Digital

After the first wave: How CIOs can weather the coronavirus crisis

Chief information officers must act swiftly to manage IT through the pandemic in a pragmatic way.

by Sven Blumberg, Peter Peters, and Christian Stüer

© Erik Isakson/Getty Images

"The new normal is not clear yet, but we need to start moving toward it."

The implications and repercussions of the COVID-19 crisis are far from certain. But as the quote above suggests, technology leaders are now starting to think about how to get past the first wave of crisis management.

This humanitarian crisis is still unfolding: quarantines, lockdowns, and harrowing images of hospitals straining under the weight of sick patients all underscore the devastating human effects of the pandemic. The economic picture for many countries is dire. As we wrote recently, COVID-19 is a crisis that requires companies to address lives *and* livelihoods. CIOs have a critical role to play because social distancing and the lockdown of economies require technology not just to maintain business activities but also to lead businesses.

CIOs must still focus on emergency measures and navigating through the chaos of the first wave of this crisis. But the economic implications require CIOs to start thinking ahead as well and to position their organizations and businesses to weather the downturn.
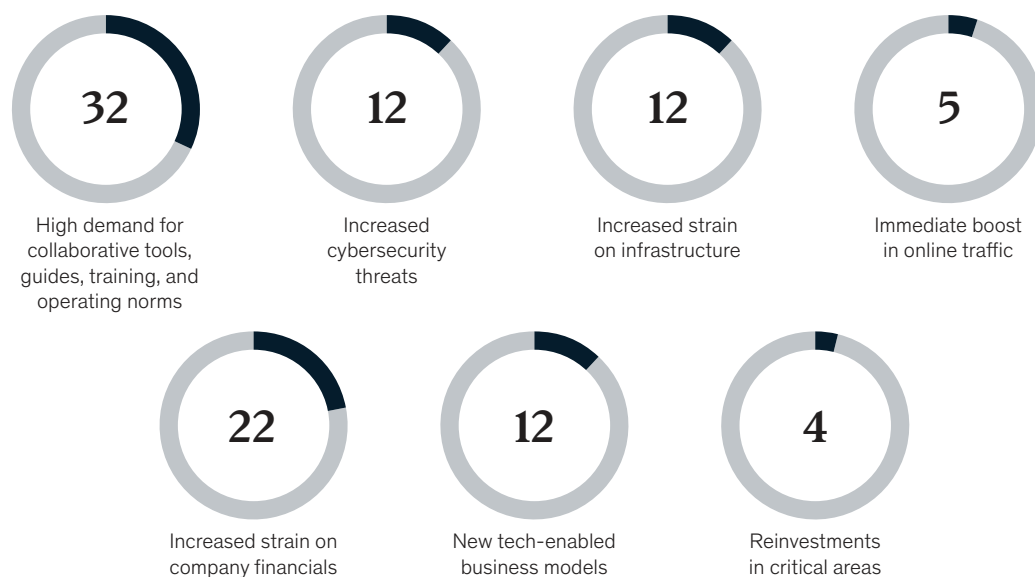
CIOs are already balancing important priorities across horizons. Polls we conducted during two recent webinars with more than 150 IT leaders highlighted their top concerns: putting in place collaboration tools and operating norms for working from home at scale, a near-term priority, and the increased strain on financials, a medium- and longer-term consideration (Exhibit 1).

Given the gloomy economic outlook, CIOs may be tempted to take a radical slash-and-burn approach in an attempt to shore up IT. That would be a mistake. While containing costs must be a crucial element of the second-wave response, CIOs have an opportunity to accelerate programs and push priorities that can help position the business to succeed when the downturn ends. There's no point in winning the battle but losing the war.

Exhibit 1

High demand for collaborative tools and operating norms and increased strain on company financials are the top concerns for chief information officers.

Top technology concerns for organizations,[1] %

32	12	12	5
High demand for collaborative tools, guides, training, and operating norms	Increased cybersecurity threats	Increased strain on infrastructure	Immediate boost in online traffic

22	12	4
Increased strain on company financials	New tech-enabled business models	Reinvestments in critical areas

[1]Question: Which of these are key concerns for you and your organization? Percentage of 161 participants attending 2 McKinsey webinars.
Source: McKinsey webinar, March 20 and 26, 2020, "The CIO moment: Leadership through the first wave of the coronavirus crisis"

As CIOs begin to shift their focus toward the next wave of the crisis, they should concentrate on three dimensions (Exhibit 2):

— Stabilize emergency measures.

— Scale down in the interim.

— Pivot to new areas of focus.

These moves will require a corresponding reprioritization of the project portfolio.

Stabilize emergency measures

We expect that the emergency measures taken as an immediate response to the COVID-19 lockdown will be sustained as long as the crisis continues. CIOs should prioritize four areas on this front.

Strengthen remote-working capabilities

Companies moved at mind-boggling speed to support remote work. It's now important to revisit those emergency measures to understand what must be updated, changed, or replaced to deal with issues that continue to hurt productivity.

First, organizations must review their ad hoc vendor-selection procedures in light of the alternatives in the market, increase network capacity, implement scalable support processes, and tighten controls that can secure and deploy temporary solutions at scale.
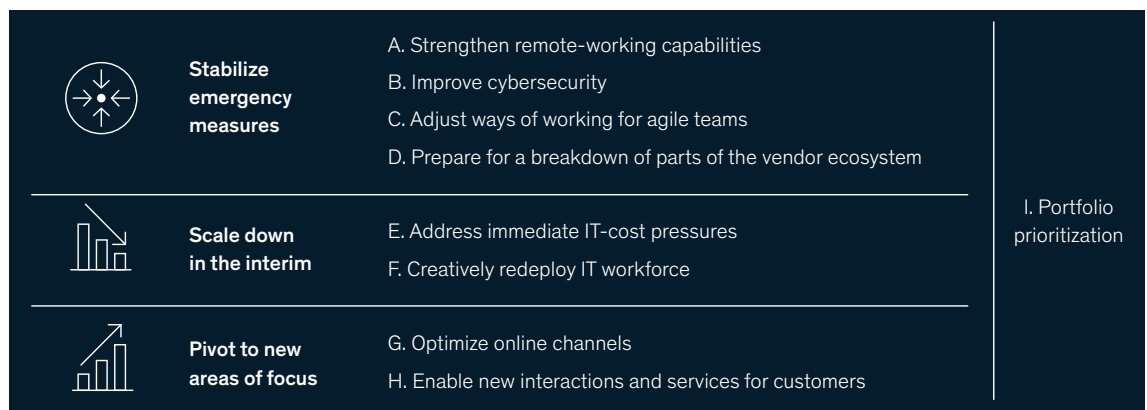
Second, CIOs will need to address the needs of special user groups, such as contact centers, users of critical systems, and employees of finance functions, to ensure that they can continue to operate in an effective way remotely. For contact centers, this may mean changing the routing of calls to a dedicated COVID-19 subteam to adjust for changes in questions from customers. Users of critical systems may need to build up redundancy in their remote-working setups. One energy company can now run an entire trading floor from the homes of employees, though with limited access to information and slower decision support.

Finally, hardware supply-chain interruptions have already proved to be a significant challenge as peaks in short-term demand for devices and IT hardware confront a breakdown of international logistics. It might be an option, if not a necessity,

Exhibit 2

Chief information officers in the next phase will need to take swift actions along three dimensions.

9 actions to weather the crisis

Stabilize emergency measures	A. Strengthen remote-working capabilities B. Improve cybersecurity C. Adjust ways of working for agile teams D. Prepare for a breakdown of parts of the vendor ecosystem	
Scale down in the interim	E. Address immediate IT-cost pressures F. Creatively redeploy IT workforce	I. Portfolio prioritization
Pivot to new areas of focus	G. Optimize online channels H. Enable new interactions and services for customers	

Technology leaders should continue to focus on people-based initiatives that heighten the awareness of risk.

to reprioritize demands by their importance—for example, prioritizing critical "tier 0" users, such as traders in banks or board members; reducing services; determining which of them can be migrated to the cloud; and using alternative purchasing channels and geographies.

Improve cybersecurity
In general, social engineering and insufficient security measures for remote work are the two main cybersecurity risks that organizations face during this time of crisis.

In recent weeks, we have seen an increase in COVID-19–focused social-engineering cyberattacks, which have exploited the current confusion and decreased the effectiveness of the "human firewall" (for instance, the verification of uncertainties with colleagues sitting nearby). CIOs, working with their chief information-security officers, must shore up their cyber protocols to deal with compromised credentials and data, as well as intellectual-property theft, fraud, and other crimes.

To address these problems, technology leaders should continue to focus on people-based initiatives that heighten the awareness of risk. The initiatives may include placing messages on lock screens or pop-up windows and creating secure, dedicated, quick, and effective two-way communication channels to the security team. To support these solutions, organizations need to beef up key processes, such as IT capacity to help employees install and set up security tools, not to mention implementing at scale security technologies such as multifactor authentication-and-control mechanisms that provide remote access to on-premise applications (for instance, teller interfaces).

Adopt new best practices for agile ways of working
Co-location is an important factor for agile ways of working to be productive. Remote work obviously introduces real challenges, such as disrupting a team's continuous alignment, limiting interactions, and complicating agile ceremonies—all of which threaten to drive productivity down. Furthermore, remote environments amplify any previous lack of clarity in roles, responsibilities, and objectives.

Yet there are some companies that have transitioned their digital units almost seamlessly to remote settings, where individual team members feel that they are working more productively than before. One tech company, for example, has fostered an outcome-driven culture that empowers teams to undertake their work outside traditional working hours. In weekly review meetings, they are still held accountable for getting things done.

When we looked more closely at companies that have moved beyond shifting employees to work from home during the first wave of the crisis, we found four differentiating factors: they changed the structure of teams to create smaller agile ones of around five people, strengthened direction setting through leadership, emphasized cultural elements and delegated decisions, with clear accountability, to individual team members, and expanded the use of technology that promotes effective collaboration.

Prepare for a potential breakdown of parts of vendor ecosystems

IT-outsourcing and offshoring vendors, as well as shared-service centers, may well shut down at times. To address that risk, CIOs are strongly advised to make their vendor dependencies and individual situations transparent—both their location and the fallback options. Mitigation efforts should be prepared not only with existing vendors but also with alternative sources in different regions. A McKinsey survey found that some global capability centers already launching mitigation measures report that "full" (more than 80 percent) production capacity can be maintained for an average of 40 days during the crisis.

Scale down in the interim

Meanwhile, CIOs must address the immediate pressures on IT costs and creatively redeploy the IT workforce.

Address immediate IT cost pressures

With revenues and margins for many businesses plummeting during the crisis, cost pressures on IT will increase. In addition, emergency decisions to manage the initial crisis response might have increased costs—both operational and capital expenditures. Technology and IT departments will be asked to find short-term cost-reduction opportunities to mitigate those effects. CIOs should therefore consider some guiding principles:

— *Be aggressive in IT cost reductions* not only to free up capital but also to invest in capabilities for the "new normal" (more remote work, more online interaction, and more automation). We have found that IT costs can typically be reduced by up to 30 percent quickly.

— *Fully exploit areas of flexibility* to address cost pressures quickly before cutting into capabilities that might affect the future business. In practice, this means deferring nonessential projects and investments that can be reversed, before

considering more permanent and potentially damaging changes.

— *Quickly build a task* force to establish the baseline and full potential of cost-reduction measures that then can be deployed in line with the developing business situation. Additionally, define thresholds when cost-reduction measures affect business operations and align on them with stakeholders.

Creatively redeploy the IT workforce

Disruptive changes in customer behavior and emergency responses have dramatically shifted workloads within organizations. Many on-site operations have been drastically reduced and long-term software-transformation efforts paused, but call centers and online channels still must be scaled up rapidly to meet demand. These realities must guide CIOs when they redeploy their people—which includes reevaluating the role of outsourcing partners. Other examples include back-filling for colleagues most affected by the crisis (for instance, those who must take care of small children or affected family members) and filling roles left open by external workers affected by the crisis.

In the past week, we have also seen many highly inspiring examples of companies repurposing their capabilities to help society cope with the crisis. Tech companies have partnered with the World Health Organization, pooling tech talent to work on projects tackling challenges caused by COVID-19. Another recent example: SAP set up a team of 40 developers and created an emergency web application in 24 hours for the German Federal Foreign Office to manage the repatriation of citizens abroad after the legacy system became overloaded.

We believe this kind of thoughtful and creative redeployment helps organizations cope with the crisis, strengthens the sense of contribution and purpose among employees, and keeps them engaged during a period of remote work.

Pivot to new areas of focus

Looking ahead, CIOs must also bolster the online channels of their organizations and support new interactions and services for customers.

Bolster online channels

With people forced to work at home and to minimize visits to brick-and-mortar stores, online sales and service channels are experiencing a massive spike in traffic—in China, we have recently seen increases of 200 to 300 percent. In the medium term, the traffic baseline for online behavior will probably rise as a result. For now, organizations must act to optimize and bolster their existing online channels to improve customer interactions and solidify retention.

The management of traffic spikes is the most pressing matter for online channels. Mildly invasive short-term measures might include expanding hardware capacity, decreasing or redistributing loads (for instance, by running promotions during off-peak hours), technical optimization (such as horizontally scaling the caching layer), or rerouting of traffic to scalable cloud solutions.

Support new interactions and services for customers

Some companies have responded quickly to the new digital customer behavior by establishing new products, such as mortgage deferrals and crisis-related insurance, or shifting customer interactions to online channels. A government in Western Europe, for example, embarked on an "express digitization" of quarantine-compensation claims to deal with a more than 100-fold increase in volume. Sometimes this effort is about taking loads from call centers, but more often it addresses real new business opportunities. To engage with consumers, for example, retailers in China increasingly gave products at-home themes in WeChat.

Technology departments must anticipate and prepare to offer more of these kinds of digital services, products, and channels. The key to reaching customers will be creating suitable access interfaces between internal IT systems and external social platforms and accelerating the integration of new vendors and distributors.

Portfolio prioritization

Given the enormous pressures CIOs are facing, the entire project portfolio must come under scrutiny to measure the tangible impact it can deliver and how it fits in with the new priorities. One CIO, for example, said that he has already committed himself to continuing only projects that are already nearly complete, reshaping or reducing in scope other projects, and applying a much more rigorous process to the selection and advancement of projects.

We believe that CIOs should apply a crisis checklist to review portfolio projects systematically against key criteria, including these: "Are we still able to deliver, either internally or with potentially affected vendors?" "In what way does the project address new business priorities?" "Does the project assume functioning supply chains?"

With a clear crisis checklist in place, CIOs and their teams can objectively continue, stop, defer, or ramp down projects to maintain focus on what really matters. As the crisis continues to unfold and CIOs develop greater clarity about what the next normal will look like, they will need to adjust their criteria.

———

CIOs are already under a lot of pressure. After the first shock and successful response, however, CIOs must now handle multiple planning horizons in parallel to manage the current crisis, prepare for the downturn, and ultimately position the business for success when the recovery comes.