McKinsey Digital

Current as of April 24, 2020

COVID-19 response checklist for CIOs and IT leaders

The COVID-19 crisis has affected communities, businesses, employment, and economies all over the world. While the top priority is to save lives and support victims and families, we must also act to protect the livelihoods of our community members.

Our response checklists offer practical solutions to help IT leaders and decision-makers take care of their people and navigate their organizations through an uncertain time. As technology organizations balance their efforts between immediate preparedness and planning for the "next normal," this set of checklists focuses on the first two of five stages along the crisis response cycle: Resolve and Resilience. Guidance on the later stages of the cycle will be available in the future.

Disclaimer: These lists are indicative, not exhaustive.

Immediate actions that can help stabilize core business operations and technology, and help prepare for recovery

The following critical actions are based on discussions with organizations in Europe and North America on top-of-mind technology priorities for CIOs.

1 Take care of your people

- ◯ Support your employees by creating a safe work environment and launching initiatives such as flexible work arrangements and paid leave
- ◯ Ensure that backups are in place for critical staff members
- ◯ Verify how on-site operations can be continued remotely or in emergency mode (data-center hosting, end-user device swap)
- ◯ Work with contractors to establish policies and incentives to reduce risk, including identifying contractor locations and travel history

2 Communicate confidently, consistently, and reliably

- ◯ Establish an IT response team to coordinate efforts across the organization
- ◯ Appoint accountable owners to communicate with key stakeholders in departments other than IT
- ◯ Establish basic communications processes, tools, roles, and plans to convey key messages to stakeholders, but recognize that these are not a substitute for action
- ◯ Create channels to field questions and get feedback, such as chat apps, help desks, town hall–style conference calls, and virtual office hours

3 Make work-from-home work

- ◯ Ensure availability of additional devices, if required, by increasing stock or creating a bulletproof ramp-up plan
- ◯ Evaluate and close gaps in technology to enable remote work (eg, obtain enough software licenses)
- ◯ Conduct a test run to assess remote and work-from-home setups with representatives of all user groups (eg, business, operations, IT developers)
- ◯ Prepare help desk for additional volume and enable effective remote-agent model, both offshore and onshore
- ◯ Create contingency plans in case offshore centers become unavailable (eg, halt some projects to support business as usual if offshore resources cannot work)

4 Promote new ways of working

- ◯ Experiment with the working model for people and processes, and quickly refine it—determine how to maintain critical IT functions, especially incident coordination, with a smaller team working from home (eg, establish red/blue/green teams)
- ◯ Create a contact list of response-team members to create transparency on roles and responsibilities
- ◯ Establish a clear cadence for daily and weekly meetings and ceremonies
- ◯ Provide virtual training and best practices about work-from-home tools, tricks, and software

5 Take charge of security

- ◯ Ensure consistency of hard-drive images across all remote employees; ensure that all workers have full access to required software and devices (eg, VPN)
- ◯ Ensure that patches are applied on time
- ◯ Run vulnerability-management solutions regularly to identify and fix vulnerabilities quickly
- ◯ Be alert for shadow IT solutions that provide quick fixes at the cost of security (eg, free online collaboration tools)
- ◯ Identify and stress-test new threats emerging from changes to the operating model
- ◯ Host training sessions on cyberthreats specific to the ongoing pandemic (eg, spear phishing), starting with high-risk user groups
- ◯ Confirm that third-party vendors are taking adequate steps to remain secure and that their entire ecosystem meets minimum viable security standards
- ◯ Discourage and sanction any use of nonapproved equipment (eg USB sticks), apps, data transfers to non-company devices, and services while ensuring that business processes run smoothly without this equipment

6 Stabilize critical infrastructure, systems, and processes

- ◯ Prepare a list of known vulnerabilities and single points of failure and identify the circumstances in which outages may happen (eg, message queue capacity and network bandwidth)
- ◯ Identify customer journeys and processes that are most prone to incidents, and develop plans to fix the issues
- ◯ Consider stress-testing select components and applications outside business hours
- ◯ Resize capacity based on first-wave evidence—strike a balance between under- and overprovisioning including network, transactional systems, customer-facing apps

7 Scale up capacity of customer channels

- ◯ Increase load capacity of customer-facing websites and solutions to support higher volumes
- ◯ Expand dedicated phone lines to manage COVID-19–related calls
- ◯ Promote automated / conversational solutions (such as chatbots) through IVR rerouting, communication, and training, quickly ironing out any pain points to ensure stickiness