KPMG

COVID-19
What CIO and CISO can do

March 2020

Concern over the scale and impact of the COVID-19 pandemic is growing, leading organizations to consider their response, and the actions they need to take now to maintain their business. The CIO and CISO have vital roles in making sure the organization can function as pandemic containment measures are implemented.

Can your business function effectively through remote working?

You need to ensure your business can work remotely and flexibly, and that employees are confident in being able to do so. This may require you to revisit decisions on access rights, entitlements and risk posture. Questions to consider:

- Have you scaled your VPN concentrators, portals and gateways to handle a large number of colleagues who will need to work remotely?
- Have you considered the potential key suppliers, contractors and vendors, who will have to access and the additional scale that will bring in?
- Have you tested the infrastructure to find out whether it can handle the expected loading?
- Are there single points of failure in the infrastructure, and can you provide additional resilience?
- Do you need to relax access controls or provide additional remote login accounts or credentials?
- Is there sufficient help desk capacity to handle any queries from users who are unable to login, or unfamiliar with remote working?
- Where employees require access to laptops for remote working, is there a pool of laptops available or can more be procured and installed to meet demand, and how should allocation be prioritized?
- In cases where the pool of equipment is limited, have you considered essential services and splitting access to them via alternative access solutions (e.g., O365 and One Drive vs. in-house applications)?
- Have you considered the ability to whitelist only specific applications during this period and block all non-essential services?
- Do you have limitations on video and audio tele-conferencing bridges, and can you do anything to scale that infrastructure?
- Do you need to consider alternate cloud-based conferencing and teleworking solutions?
- Do all members of staff have the necessary access numbers/links to allow them to access the bridges, is training material readily available, should you establish a helpline?
- Can you remote your help desk operations if the help desk staff have to work from home?
- Have you prepared simple guides to be distributed to staff on key help desk related queries:
  - How do I login?
  - How do I change my password?
  - How do I access key services?
  - How can I get help from the help desk?
  - Who are my key contacts if I have a crisis?

Are you able to scale digital channels to deal with demand?

Restrictions on travel and the spread of the virus may lead to new patterns of demand, and higher traffic on digital channels.

- More customers and clients may expect to transact with you through digital channels, can you scale those systems and services to deal with changing demand?
- How would you monitor loading and performance, and who can make the decisions to scale capacity, or create dynamic choices on prioritization if capacity is an issue?
- Are you clear which services you may need to shed, or how customer journeys may need to alter if systems are overloaded?
- Are you dependent on key call centers, and if those call centers are closed or inaccessible, can customers and clients interact with you through other channels?
- Is there the option to allow call center staff to work remotely, or to transfer their loads to another call center location?
- Have you considered the interactions between call centers and service/help desks and the impact of any outsourcing arrangements?
- Have you discussed the arrangements with key suppliers of those services, and how will they prioritize your needs against those of other clients?

Are you dependent on key IT personnel?

Sadly employees may be infected or may find themselves unable to travel or to have to meet family caring commitments; you should plan for a significant level of absenteeism.

- What would happen if key IT personnel (including contractors) are unable to travel, or are ill with the virus... are you dependent on a small number of key individuals?
- How could you reduce that dependency, for example, ensuring that there are "break glass" procedures in place to allow other administrators access to critical systems?
- What about the Security team? Who are the key individuals, and if the CISO is not available, then who will make the calls on the security posture and the acceptable risks to the firm?

What would happen if disruption to a data center occurs?

- Data centers may be impacted by the virus too. A positive test may result in an evacuation and deep clean of the building; transport infrastructure disruption may prevent access, and data center staff may be unable to work.
- In the event that one of your data centers is evacuated, do you have disaster recovery plans in place to deal with the disruption, and have you tested those plans?
- How quickly can you failover to an alternate site, and who manages that process?
- Are you dependent on key individuals (including contractor support) for the operation of the data center, and how can you manage that dependency?

Are you able to scale your cloud capabilities?

There may be additional demands on cloud-based services, requiring you to scale the available computing power, which may incur additional costs. Other services may show reduced demand.

- Are you able to monitor the demand for cloud computing services, and manage the allocation of resources effectively?
- Have you made arrangements to meet any additional costs which may be incurred from scaling or provisioning other cloud services?

Are you dependent on specific suppliers?

- Your suppliers and partners will also be under pressure, and their operations disrupted too.
- Who are your critical suppliers, and how would you manage if they are unable to operate, including disruption to your key managed service providers?
- Are there steps you could take now to reduce that dependency, including using your team resources?
- Are you discussing the implications with your key suppliers, and do you have the right points of contact with those suppliers?
- Have you identified which IT suppliers may come under financial pressure, and what would be your alternate sourcing strategy if they did fail?

What would happen if there 's a cyber incident?

Organized crime groups are using the fear of COVID-19 to carry out highly targeted spear-phishing campaigns and set up fake websites, leading to an increased risk of a cybersecurity incident.

- Have you made it clear to employees where to get access to definitive information on the COVID-19 pandemic and your firm's response to COVID-19?
- Have you warned staff of the increased risk of phishing attacks using COVID-19 as a cover story?
- If you're dependent on alternative systems or solutions, including those procured as cloud services, who would you handle a security incident involving those systems?
- Do you need to change your approach to security operations during the pandemic, including arrangements for monitoring of security events?

What would happen if there 's an IT incident?

While COVID-19 dominates the news, you should still be aware of the possibility of an IT failure given the changing demands on your infrastructure, or an opportunistic cyber- attack.

- Would you be able to co-ordinate the incident remotely, and do you have the necessary conferencing facilities and access to incident management sites/processes and guides?
- Do you have a virtual war room setup, in case physical access is limited or restricted?
- Are you dependent on key individuals for the incident response, and if so, what can you do to reduce that dependency?
- How does the emergency/incident response crisis management structure change if key incident managers/ recovery leads are unavailable?
- Are you confident that your backups are current, and that in the worst case you can restore vital data and systems?
- How would you deal with a widespread ransomware incident, when large parts of your workforce are home working?

Are you making the best use of your resources?

You will need to be able to function with limited employee numbers and be clear on the priority tasks your team needs to be able to complete.

- Have you prioritized your team's activities, are there tasks which you can defer and release staff for contingency planning and priority preparation tasks?
- Do you have the ability to access emergency funds if you need to source equipment, or additional contractor/ specialist support rapidly?
- If you are placed under pressure to reduce discretionary spend to preserve cash, are you clear on which spend must be protected and where to make those savings?

Are you setting an example?

Amongst all of these organizational considerations, you are still a senior manager, and your team will look to you for leadership and support.

- Have you made sure your team is implementing sensible hygiene practices, including offering flexible and remote working to meet changing needs?
- Do you have up to date points of contact details for all of your team? Is your team aware of who to contact in an emergency?
- Do you model the behaviors you expect of your team, and what would happen if you were incapacitated? Who would step in for you?

Stay safe and good luck.

If you have any questions or would like additional advice, please contact us.

Contacts

KPMG AG
Räffelstrasse 28
Postfach
CH-8036 Zurich

kpmg.ch

Matthias Bossardt
Partner, Head of Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Thomas Bolliger
Partner, Head of Information Governance & Compliance

+41 58 249 28 13
tbolliger@kpmg.com

Yves Bohren
Director
Cyber Security

+41 58 249 48 95
ybohren@kpmg.com

Nicolas Tinguely
Director
Cyber Security

+41 58 249 21 44
ntinguely@kpmg.com