COVID-19: What the CIO and CISO can do to help.

17 March 2020

The scale and impact of the Covid-19 pandemic pose significant threats to business continuity. As they seek to maintain and strengthen their Enterprise Resilience, we believe firms should consider a full range of operational, financial and strategic factors. The CIO and CISO have vital roles to play in ensuring operational resilience, by making sure the organisation can continue to function effectively as pandemic containment measures are applied across the world

Can your firm function effectively through remote working?

- Have you scaled your VPN concentrators, portals and gateways to handle the large number of colleagues who will need to work remotely?
- Have you consider 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 test 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 prioritised?
- In cases where the pool of equipment is limited, have you considered essential services and access to them been split via alternative access solutions (e.g. O365 and One Drive vs. in-house applications)?
- Have you consider the ability to whitelist only specific applications during this period and block all non-essential services?
- Do you have limitations on video and audio teleconferencing 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 help line?
- Can you remote your help desk operations in the event that help desk staff have to work from home?
- Have you prepared simple guides to be distributed to staff on couple of key help desk related queries:
  - How do I get logged in?
  - 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 greater 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 make dynamic choices on prioritisation if capacity is an issue?
- Are you clear which services you may need to shed, or how customer journeys may need to be altered if systems are overloaded?
- Are you dependent on key call centres, and if those call centres are closed or inaccessible, can customers and clients interact with you through other channels?
- Is there the option to allow call centre staff to work remotely, or to allow their loads to be transferred to another call centre location?
- Have you considered the interactions between call centers and service / help desks and impact of any outsourcing arrangements?
- Have you discussed the arrangements with key suppliers of those services, and how will they prioritise 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 having 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 key 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 a data centre is disrupted?

Data centres 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 centre staff may be unable to work.

— In the event that one of your data centres 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 centre, 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 additional cloud services?

Which suppliers are you dependent on?

Your suppliers and partners will also be under pressure, and their operations may be disrupted too.

— Who are your critical suppliers, and how would you manage in the event 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 own 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 is a cyber incident?

Organised crime groups are using the fear of COVID-19 to carry out highly targeted spear phishing campaigns and set up fake web sites, leading to an increased risk of a cyber security 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 are 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 is an IT or cyber incident?

While COVID-19 dominates the news, you should still be alive to 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 changed 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 key corporate 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 really needs to be able to complete.

- Have you prioritised 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 rapidly source equipment, or additional contractor/specialist support?
- If you are placed under pressure to reduce discretionary spend to preserve cash, are you clear on which spend must be protected and where savings could be made?

Are you setting an example?

Amongst all of these organisational considerations, you are still a senior manager and your team will look to you for leadership and for 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, and they aware of who to contact in an emergency?
- Do you model the behaviours you expect of your own team, and what would happen if you were incapacitated… who would step in?

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

Eric Wessleman:
Digital
M:+31 6 15073957

William Koot:
Digital
M:+31 6 22788700

Johan Albada:
Digital
M:+31 6 51186826

Harish Bharadwaj:
Digital
M:+31 6 83094707

home.kpmg/nl

Designed by CREATE | CRT125805