



COVID-19

What the CIO and CISO can do to help

KPMG in Ghana

April 2020

Concern over the scale and impact of the COVID-19 pandemic is growing, leading organisations to consider their response, and the actions they need to take now to maintain their business. The Chief Information Officer (CIO) and Chief Information Security Officer (CISO) have vital roles in making sure the organisation 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 prioritised?
- 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 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 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 prioritisation 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 prioritise your needs against those of other clients?

Are you dependent on key IT personnel?

Sadly employees may be affected or may find themselves unable to travel or to have to meet family care-giving 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?

organised 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 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 needs to be able to function.

- 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 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 organisational 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?

Working from home during these unprecedented times, has its pros and cons. The protection of customer and organisations information is absolutely critical and is the responsibility of all employees.

The following are some guidelines that organisations can share with their employees to ensure that customer and organisations information is protected:

General guidance – Working from Home

- When working outside of the office, be aware of your surroundings. Don't allow unauthorized people to overhear you discussing work or see your documents or screens.
- Never leave your laptop or confidential documents unattended when working from home. Ensure when you step away from your work space that you lock the screen. Do not allow friends or family to use office devices.
- Ensure you use a secure VPN connection (i.e. Cisco AnyConnect Secure Mobility Client) if using public WiFi to access the internet from your laptop.
- Only use the organisations approved software. If in doubt, please consult with your helpdesk or IT Team.
- Do not share confidential information with third party sites or through technology solutions that are not approved for use by the organisation.
- To ensure that your colleagues have access to documentation in case you are out of the office, always save documents to your approved organisation storage system and do not store them locally on your laptop.
- Make sure that you have at least one delegate who can access your folders, documents and tasks, and keep them up to speed.
- Don't allow your mobile devices to auto-connect to open WiFi networks.
- Disable Bluetooth on your mobile devices when it is not in use.
- When using conference call facilities (including Skype and Teams) where discussing confidential matters, situate yourself away from (or disable) voice assistant devices, such as Alexa and Google.
- Immediately report actual or suspected security events or suspicious activity (including any potential loss of the organisation or customer information) in accordance with your organisations policies.

Protecting confidential information when working remotely

- Make sure remote access is permitted in your client contract.
- Don't take hard copy confidential documents home unless absolutely necessary.
- Don't forward work email to your personal email account and don't send customer or organisation information to your own (or a colleague's) personal email accounts.
- When working with customers and third parties make sure you are using the organisations approved collaboration tools (e.g., Microsoft Teams or Zoom). For any exceptions you must consult with your IT Team or CISO.

Be alert to email and telephone scammers

- Scammers may try to obtain access to your private information by tricking you into thinking the person asking has a legitimate right to the information. It may be via a phone call, text message, email or even letter. If you fall prey to this, you are at risk of giving confidential information away, sending payments to a scammer or downloading malware to a device.
- **Phishing - what to lookfor:**
 - Hover the mouse over the link and the URL details will come up. This will show if the URL is valid and will take you to the expected site. If it does not appear to be valid, do not attempt to access the site.
 - Only open email attachments sent by addresses you trust, and always be careful which links you click on in your emails.
 - Never answer email requests for passwords, security codes, pin codes, etc. You can test whether there is a real need for a response by opening up a new web page in your browser and typing in the URL or searching for the website of the entity that is purportedly seeking your security information. You can then proactively check whether you have any notifications.
 - Even if an email looks genuine you should proactively contact the sender through their official website and never use telephone numbers or links provided in an email unless you are positive that it is legitimate.



— SMS phishing - what to look for:

- Fraudsters send a text message to an individual's mobile phone in an attempt to get them to divulge personal information, or call a fake number posing to be their bank or other authoritative entity.
- Don't click on links in text messages unless you are 100% certain that they are genuine and well-intentioned.
- Don't call back a number provided in a text message. For example, if the message asks you to call regarding fraudulent activity on your account, call your bank directly to report the message and find out if there really is an issue.

— Voice phishing - what to look for:

- Criminals may persuade victims to hand over personal details or transfer money over the telephone. They may already know many details about you, such as your name, address, date of birth, phone number and even your mother's maiden name, all of which they have gathered from freely available online directories or social media. It is therefore critical to ensure that you only share additional information with trusted entities.

WiFi home network

- Place the router as close as possible to the middle of your house or apartment to minimise how far the wireless signal range extends beyond your home.
- Keep your router software up to date. Change the default password of your router.
- Enable or install a firewall in order to protect your systems from malicious hacking attempts against your home network.

Social Media

- Personal information is valuable to cyber security scammers, so think before posting online. Consider what a post reveals, who might see it and how it might affect you or others. It may give hackers just enough information to be able to change your passwords (e.g., if they know your child's birthday or mother's maiden name) or call you and trick you into handing over your credit card details.
- Always be wary of sharing location details online.

Stay safe and good luck.

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

Contacts

Andrew Akoto

Partner and Head of Advisory

KPMG in Ghana

T: +233208174629

E: aakoto@kpmg.com

Sam Aluko

Associate Director, IT Advisory

KPMG in Ghana

T: +233501324121

E: samuelaluko@kpmg.com

Eugene Minnaar

Associate Director, Forensics

KPMG in Ghana

T: +233501324323

E: eugeneminnaar@kpmg.com

Prince Yawson-Adjei

Manager, IT Advisory

KPMG in Ghana

T: +233501324198

E: pyawson-adjai@kpmg.com



© 2020 KPMG, a partnership established under Ghanaian law, is a member of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International") is a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular.