KPMG

Risk and security in the wake of COVID-19

Steps CISOs can take now to keep businesses operating

Concern over the scale and impact of the COVID-19 challenge is compelling companies to consider the actions they need to take now to maintain their business. The chief information security officer (CISO) has key roles to play in helping to support the Chief Information Officer (IT) and ensure their organization can function as containment measures are implemented.

Can your company function effectively through remote working?

Government and health officials are strongly recommending social distancing to help contain the spread of the virus and are encouraging businesses to allow employees to work from home whenever possible. As a CISO, you need to help ensure your company's employees can work remotely and are confident that they will be able to perform their jobs away from the office. Achieving this flexibility may require you to revisit decisions on access rights, entitlements and risk posture.

Questions to ask yourself:

1. Have you scaled your VPN concentrators, portals, and gateways to handle the large number of colleagues who will need to work remotely?
2. Have you tested the infrastructure to determine whether it can handle the expected loading?
3. Are there single points of failure in the infrastructure? Can you provide additional resilience?
4. Do you need to relax access controls or provide additional remote login accounts or credentials?
5. Is there sufficient help desk capacity to handle any questions from users who are unable to login or unfamiliar with remote working?
6. Is there a pool of laptops available to supply employees who need them to work remotely? Can more be procured and installed to meet demand? How should the allocation be prioritized?
7. Do you have limitations on video and audio teleconferencing bridges? If so, can you do anything to scale up that infrastructure?
8. Do you need to consider alternative cloud-based conferencing and teleworking solutions?
9. Do all staff members have the necessary access numbers/links to allow them to access bridges? Is training material readily available?
10. In the event that help desk staff has to work from home, can your help desk operations function remotely?

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 increasing demand?
- 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 allow their loads to be transferred to another call center location?

Are you dependent on key IT personnel?

Some employees may become infected, be unable to travel, or have to care for family members. Consequently, you need to plan for a significant level of absenteeism:

- Have you ensured key team members are practicing social distancing?
- Can you isolate your staff into NB teams or work in shifts?
- What would happen if key information technology (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, can you ensure that there are "break glass" procedures in place to allow other administrators access to key systems?

Are you prepared to manage insider threat risk in an extended work-from-home (WFH) situation?

Your oversight abilities may diminish and employees may become disgruntled. Organizations need to adjust their strategy for protecting their assets from unintentional and intentional misuse:

- Have you determined areas of unacceptable risk (e.g., legal/regulatory risks), which in no circumstance should be conducted in an extended WFH situation? Initialize business continuity efforts on these activities.
- Can you identify controls that can be loosened, such as opening up access to collaboration solutions, allowing remote print, and allowing email to personal addresses? Can you monitor any changes to infrastructure and policy?
- Use of non approved technology (Shadow IT) will be pervasive and is likely unavoidable. Have you reiterated leading practices to reduce your risk, particularly where sensitive data is involved? Do you understand contractual requirements and the impact of recent privacy laws?
- Controls will be bypassed, intentionally and unintentionally. Are you ready to focus detection tactics on identifying situations that are intentional/malicious?
- Are you prepared to perform remote forensic data collection in a social-distanced way? Does your BYOD policy allow for investigation of employee-owned and managed equipment?

What would happen if a data center is disrupted?

Data centers may be impacted by the virus, too. A positive test may result in an evacuation and deep clean of the building. Likewise, 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?
- Are you dependent on key individuals (including contractor support) for the operation of the data center? How can you manage that dependency?

Are you able to scale your cloud capabilities?

Cloud-based services may experience additional demands, requiring you to scale up 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 that 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 were unable to operate? (This includes disruption to your key managed-service providers.)
- What steps could you 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 alternative sourcing strategy if they did fail?

What would happen if there is a cyber incident?

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

- Have you made it clear to employees where to access definitive information on COVID-19 and your firm's response to the virus?
- Have you warned your staff of the increased risk of phishing attacks using COVID-19 as a cover story?
- 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 alert to the possibility of an IT failure given the changing demands on your infrastructure or an opportunistic cyberattack:

- Would you be able to coordinate the incident remotely and do you have the necessary conferencing facilities and access to incident-management sites/processes and guides?
- Are you dependent on key individuals for the incident response, and if so, what can you do to reduce that dependency?
- Are you confident that your backups are current and that, in the worst case, you can restore key corporate data and systems?

Are you making the best use of your resources?

You will need to be able to function with limited employees, so you need to clearly identify the priority tasks your team really needs to focus on:

- Have you prioritized your team's activities? Are there tasks that 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 staying close to your business partners?

During this pandemic, IT Leadership and the CISO should be more engaged than ever with the business to re-assess business priorities, communicate issues with service levels and continuity, and be flexible to shift IT resources to the most pressing business priorities.

- Are you openly communicating with the business to understand changing priorities and re-allocating IT resources to focus on what's most important?
- Are you able to rapidly assess cyber security scaling current technology or put in place new technologies?
- Can you conduct rapid targeted cyber risk assessments where there are new threats/risks identified-loosening controls, new protocols with vendors?

Are you setting an example?

Amid all of these organizational 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 and social-distancing 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? Do they know whom to contact in an emergency? Do you model the behaviors that you expect of your team? What would happen if you were incapacitated? Who would step in?

COVID-19 is creating much uncertainty and concern. CISOs, working closely with their colleagues, can play a key role by following a rational and methodical approach to business continuity that can help organizations maintain their business operations in these challenging times, while protecting the safety and health of their people.

Contact us

If at any time you need help, please use the information below to get connected to an specialist for more advice and support contact:

Steve Bates
Global Leader
CIO Center of Excellence
KPMG International
E: sjbates@kpmg.com

Tony Buffomante
Global Co-Leader
Cyber Security Services
KPMG International
E: abuffomante@kpmg.com

Matthew Miller
Principal
Cyber Security Services
KPMG in the US
E: matthewpmiller@kpmg.com

Glenn Siriano
Principal
Cyber Security Services
KPMG in the US
E: gsiriano@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities

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 endeavor 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 situation.