KPMG

COVID-19

How to prevent, detect and respond to cyber incidents during uncertain times

April 2020

As the current COVID-19 situation develops, organizations must reconsider preventive measures and actions to take should a cyber incident occur. The CISO and CRO have vital roles in making sure their organization is ready to prevent, detect and respond to cyber incidents in a timely manner while pandemic containment measures are implemented.

Has your organization already put in place preventive measures prior to working remotely?

With pandemic containment measures implemented due to COVID-19, companies have enabled remote working to keep the business running while also encouraging employees to follow social distancing guidelines. As most of the organization's employees and third-party contractors cannot work from office premises, it is imperative that an organization has implemented enough proactive measures to prevent cyber incidents during this challenging time. This is important to protect the business and digital assets.

Some questions to consider:

— Are there any additional risks your organization is exposed to when enabling additional/enhanced remote working?

— Have you secured VPN, portals, and gateways?

— Have you performed a quick Vulnerability Assessment & Penetration Testing (VAPT) before making services remotely accessible?

— Have you whitelisted only specific applications for remote access while blocking all non-essential services?

— Have you performed access review and used proper privileged access provisioning?

— Have you implemented multi-factor authentication to gain access to your enterprise internal network and privileged account for remotely accessible services such as Office365?

— Have you deployed and properly configured perimeter security devices such as the firewall, web application firewall (WAF) and intrusion detection and prevention systems (IDS/IPS), which help to keep your enterprise systems and network safe from attacks?

— Do you have security solutions such as endpoint detection and response (EDR) platforms, next-gen antivirus (NGAV) software, data loss prevention (DLP), web content filtering and security and user/entity behavior analytics (UEBA/UBA) solution to prevent malware infection or data leakage?

— Have you deployed and properly configured mail server content scanning and filtering to identify potential phishing email and malicious attachments?

— Have you made sure to keep all your security solutions up to date with latest signature and threat intelligence (wherever possible), and plan for patch deployment on the most exposed systems?

- Have you limited employee access to data and information as well as the authority to install software while working remotely?
- Have you deployed and properly configured mobile device management (MDM) and implemented bring your own device (BYOD) policies if your organization's data and information are accessed via mobile or other personal devices?
- Have you made online backup copies and maintained a secondary offline backup copy for all business-critical data and information?
- Have you ensured to encrypt data whilst at rest? Most modern devices have encryption built in, but encryption may still need to be turned on and configured.

Have you educated your employees and third-party contractors on working remotely?

During the situation, it is crucial to ensure all employees and third-party contractors are well informed on precautions to take while working remotely.

Some questions to consider:

- Have they been informed to ensure contact details in the HR portal/centralized database is up to date in the event an emergency contact is required for business purposes?
- Do they understand the risks of connecting organization devices to public Wi-Fi or leaving organization devices unattended, especially in public places?
- Do they know what to do if a device is lost or stolen?
- Do they know how to transfer files using only the organization's storage or collaboration tools, rather than via other means?
- Have employees been warned of the high risk of phishing attacks using COVID-19 as a cover story? Ensure they are aware of the following:
  - Never click on unverified links
  - Do not open untrusted email attachments
  - Avoid submitting and giving out personal data
- Do they know how to report suspicious emails and whom to contact should an incident occur?
- Are they aware about other precautionary steps to take? Some to be considered are:
  - Use a VPN when using public Wi-Fi. This also helps web browser activities pass through the organization's web content filtering
  - Only download from trusted sites
  - Backup data on an organization provided network, cloud storage or encrypted hard drives.
  - Never use unfamiliar USBs
  - Keep software and operating systems updated
- Do they know to watch out for announcements and follow instructions carefully if needed for scenarios such as a critical patch update for widely exploited security vulnerabilities?

Is your organization truly prepared to detect and respond to cyber incidents during the current COVID-19 situation?

Organizations face the risk of increased cyber-attacks during this challenging time as hackers are targeting our increased dependence on digital tools.

Some questions to consider:

- Have you discussed with your IT Security team and key stakeholders about high-level roles and responsibilities, communication channels to use during a crisis and whom to reach out to?
- Is your IT Security team putting in extra effort to monitor and triage alerts generated by security solutions put in place in order to detect any intrusion and other malicious activities?
- Is your IT Security team collecting COVID-19 related indicators of attack (IOAs) and indicators of compromise (IOCs) and making use of threat intelligence from security solutions and open source intelligence (OSINT) to look out for any possible malicious activity on endpoints, servers, and within the organization's network?
- Have you identified and actioned upon blind spots in security monitoring results due to the recent changes in network to allow working from home (WFH) and remote access?

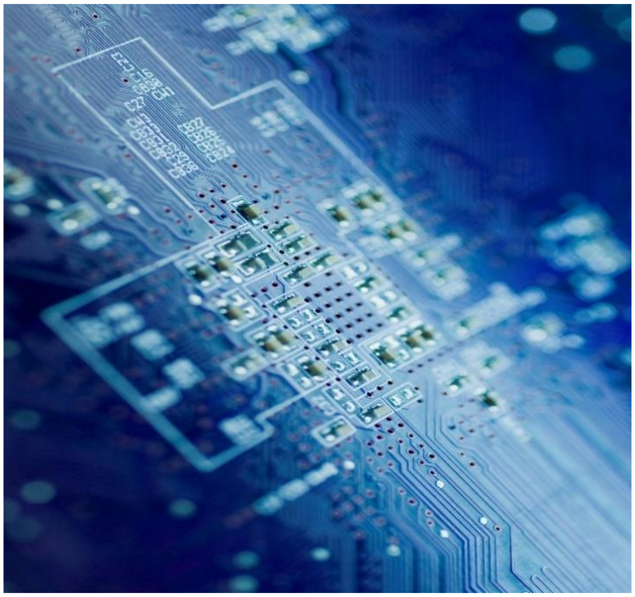
- Have you dedicated IT Security resources to monitor security advisory as published by various vendors and security solutions provider? Evaluate risk and release patches accordingly, and develop a workaround in cases when no patch is available such as the Windows zero-day vulnerability.
- Are guidelines or procedures readily available for your IT Security team to follow should your organization face a cyber incident?
- Have you identified and updated the contact information of key stakeholders who need to be informed if a cyber incident were to occur?

How does the current COVID-19 situation affect your organization's prevention, detection and response capability?

The Movement Control Order (MCO) implemented by the Malaysian government can make preventing, detecting and responding to cyber incidents even more challenging. This may result in organizations needing new strategies, approaches and requirements to respond should a cyber incident occur.

Some questions to consider:

- Have you changed your approach to security operations and arrangements for monitoring of security events?
- Can your IT Security team monitor, detect and respond to security alerts remotely?
- How will you arrange with key individual(s) such as vendors and contractors that you depend on to support your operation or systems should they be infected by a cyber incident? How can you manage this dependency?
- Who will be responsible for decision making updating senior management/Board members if individuals such as the CISO are unavailable?
- Have you scheduled daily virtual calls with key stakeholders to discuss the threat landscape in the current situation, daily findings from security monitoring and key issues to highlight?
- Have you considered what would happen if data centers are impacted by the current COVID-19 situation? It may result in evacuation and deep clean of the building, transport infrastructure disruption may prevent access, and data center employees may be unable to work.
- Have you considered how your IT Security team will isolate and collect evidence from affected endpoints and servers should a cyber incident occur as the team will be working remotely?
- How will you communicate remotely with point-of-contacts should a cyber incident occur and your communication channels such as email is down?
- Have you onboarded an independent third party to be on standby to assist in performing digital forensic analysis and incident response? This is important in the case where you do not have enough in-house skillsets or relevant employees available because of the COVID-19 situation.



Contact us if you have any questions or would like customized guidance.

www.kpmg.com.my/CyberResponse

Contact us

For more information, contact us:

Chan Siew Mei
Head of Advisory
KPMG in Malaysia

T : +603 7721 7063
E : siewmeichan@kpmg.com.my

Tan Kim Chuan
Head of Forensic
KPMG in Malaysia

T : +603 7721 7052
E : ktan@kpmg.com.my

Yogesh Beniwal
Associate Director, Cyber Response Lead
KPMG in Malaysia

T: +603 7721 7844
E : ybeniwal@kpmg.com.my

www.kpmg.com.my/CyberResponse

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.