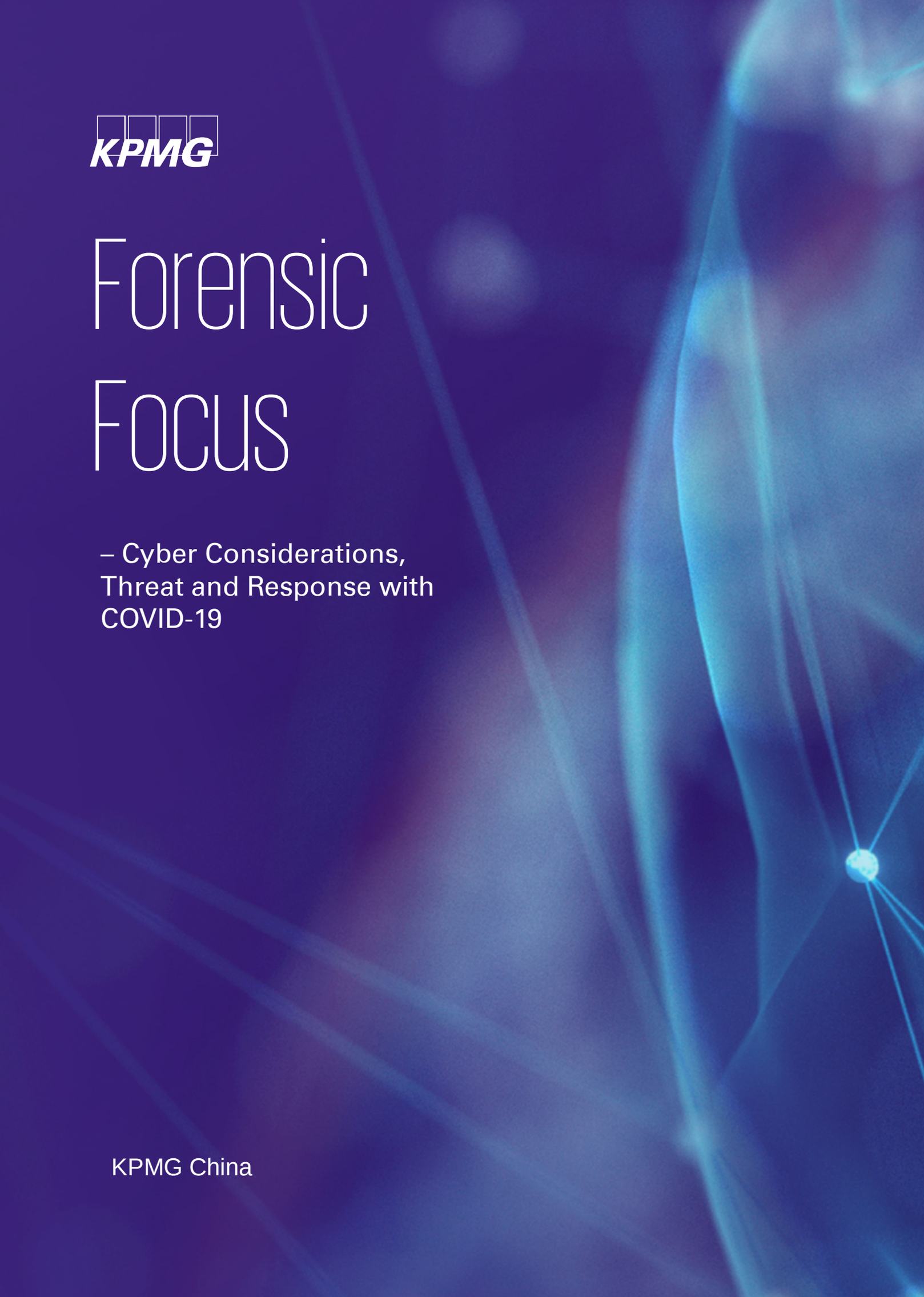
KPMG

Forensic Focus

– Cyber Considerations, Threat and Response with COVID-19



KPMG China

The Considerations for CIO and CISO

COVID-19 pandemic is changing our lives. People are concerned, and with that concern comes a desire for information, safety and support. Organized crime groups are exploiting the fear, uncertainty and doubt which COVID-19 brings to target individuals and businesses in a variety of ways.

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 tohandle 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 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 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 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 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 corporate data and systems?
- How would you deal with a widespread ransomware incident, when large parts of your workforce are home working?

The Threat

Since mid-February, KPMG member firms have seen the rapid build-out of infrastructure by cybercriminals used to launch COVID-19 themed spear-phishing attacks and to lure targets to fake websites seeking to collect Office 365 credentials.

Examples of campaigns mounted include:

- COVID-19 themed phishing emails attaching malicious Microsoft documents which exploit a known Microsoft vulnerability to run malicious code.
- COVID-19 themed phishing emails attaching macro-enabled Microsoft word documents containing health information which trigger the download of Emotet or Trickbot malware.
- Multiple phishing emails luring target users to fake copies of the Centre for Disease Control (CDC) website which solicit user credentials and passwords.
- A selection of phony customer advisories purporting to provide customers with updates on service disruption due to COVID-19 and leading to malware download.
- Phishing emails purporting to come from various government Ministries of Health or the World Health Organization directing precautionary measures, again embedding malware.
- COVID-19 tax rebate phishing lures encouraging recipients to browse to a fake website that collects financial and tax information from unsuspecting users.

Many existing organized crime groups have changed their tactics to use COVID-19 related materials on health updates, fake cures, fiscal packages, emergency benefits and supply shortages.

Typical giveaways that an email may be suspect include:

- Poor grammar, punctuation and spelling.
- Design and quality of the email isn't what you would expect.
- Not addressed to you by name but uses terms such as "Dear colleague", "Dear friend" or "Dear customer".
- Includes a veiled threat or a false sense of urgency.
- Directly solicits personal or financial information.

Of course if it sounds too good to be true, it probably is.

The Response

There are some key steps you should take to reduce the risk to your organization and your employees, particularly as you move to remote working:

- Raise awareness amongst your team warning them of the heightened risk of COVID-19 themes phishing attacks
- Share definitive sources of advice on how to stay safe and provide regular communications on the approach your organization is taking to the COVID-19 pandemic
- Make sure you set up strong passwords, and preferably two-factor authentication, for all remote access accounts; particularly for Office 365 access
- Provide remote workers with straightforward guidance on how to use remote working solutions including how to make sure they remain secure and tips on the identification of phishing
- Ensure that all provided laptops have up to date anti-virus and firewall software
- Run a helpline or online chat line which they can easily access for advice, or report any security concerns including potential phishing
- Encrypt data at rest on laptops used for remote working given the risk of theft
- Disable USB drives to avoid the risk of malware, offering employees an alternate way of transferring data such as a collaboration tool

Also, make sure that your finance processes require finance teams to confirm any requests for large payments during the COVID-19 pandemic. This confirmation can help to guard against the increased risk of business email compromise and CEO frauds. Ideally, use a different channel such as phoning or texting to confirm an email request.

Ensure that you apply critical security patches and update firewalls and anti-virus software across your IT estate, including any laptops in use for remote working. You should expect organized crime groups to exploit any failures in the maintenance of IT systems during this pandemic.

Make certain that you back up all critical systems and validate the integrity of backups, ideally arranging for off- line storage of backups regularly. Expect an increased risk of ransomware during the COVID-19 pandemic as organized crime groups exploit COVID-19 themed phishing.

Lastly, work with your incident and crisis management team to strive to ensure your organization has an alternate audio and video conferencing environment available. This alternate platform will be needed if you do have a ransomware incident that disrupts your IT systems. And will also provide additional redundancy if your primary conferencing provider has capacity or availability issues.

Contacts

Paul Pu

National Leader, Forensic KPMG China
Tel: +86 (21) 2212 3780 Email: paul.pu@kpmg.com

Dakai Liu

Partner, Forensic Cyber Response
KPMG China
Tel: +86 (21) 2212 3371
Email: dakai.liu@kpmg.com

Kevin Jin

Partner, Forensic
KPMG China
Tel: +86 (21) 2212 3266
Email: kevin.y.jin@kpmg.com

Clark Zhu

Partner, Forensic
KPMG China
Tel: +86 (10) 8553 3650
Email: clark.zhu@kpmg.com

Carter Zhang

Director, Forensic
KPMG China
Tel: +86 (21) 2212 3153
Email: carter.zhang@kpmg.com

kpmg.com/cn/socialmedia

For a list of KPMG China offices, please scan the QR code or visit our website: https://home.kpmg.com/cn/en/home/about/offices.html.