# Technology and How Your Data is Being Infected During the Pandemic

**Guest Speakers**

**Suaran Singh Sidhu**
Partner
LAW Partnership (Malaysia),
associated firm of
Eversheds Harry Elias LLP

**Tan Weiyi**
Partner
Eversheds Harry Elias LLP
(Singapore)

**Rhys McWhirter**
Of Counsel
Eversheds Sutherland
(Hong Kong)

**Date: 29 April 2020**

**Time: 10 a.m. - 11 a.m.**

LAW
PARTNERSHIP

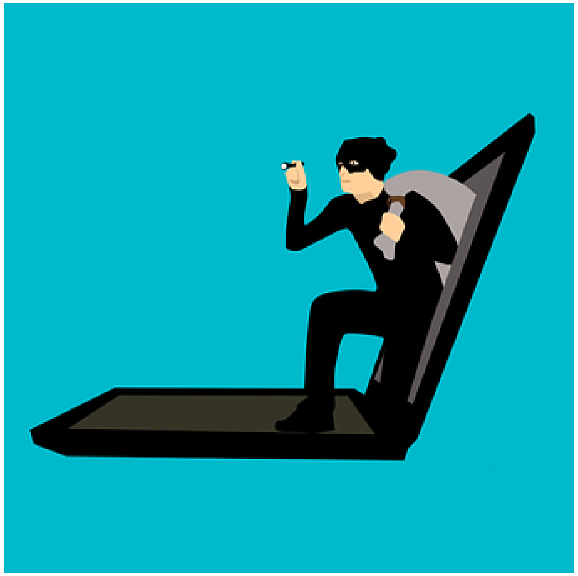
# Part One
Cybersecurity threats arising from new norms during the pandemic

# Covid-19: Virus Offline and Online?

## How the Coronavirus Affects Your Cybersecurity

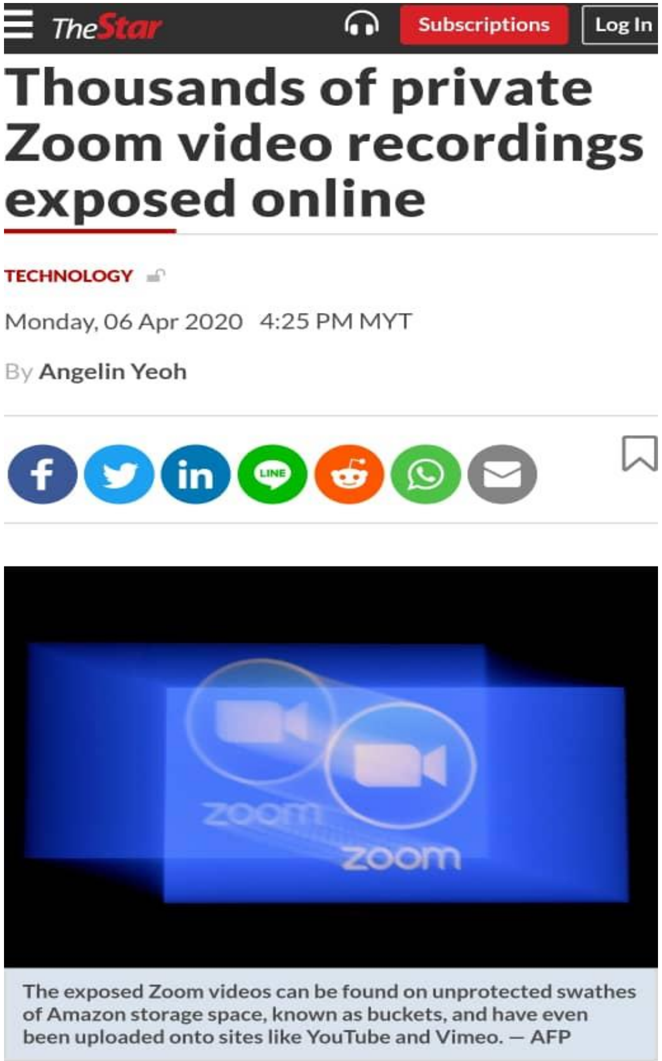
# Common Cyberattacks in the Time of COVID-19

1. Attacks on compromised applications (ie. Zoom)
2. Scams / Phishing / Malware



# App Attacks – Compromised Applications

# "Zoom-Bombing"



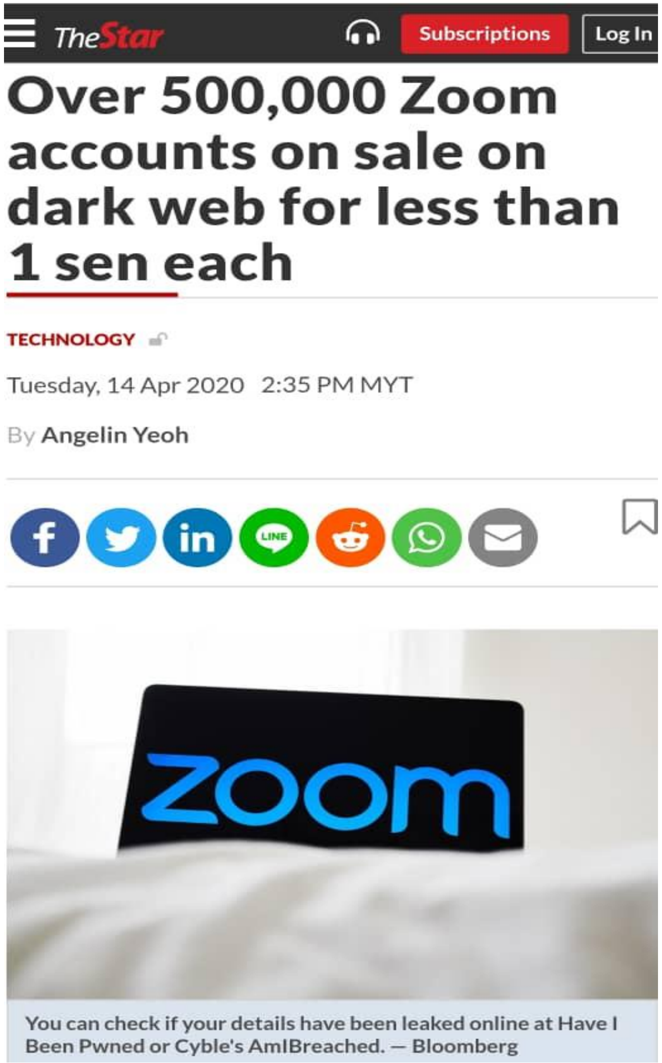
## Thousands of private Zoom video recordings exposed online

TECHNOLOGY

Monday, 06 Apr 2020 4:25 PM MYT

By Angelin Yeoh

The exposed Zoom videos can be found on unprotected swathes of Amazon storage space, known as buckets, and have even been uploaded onto sites like YouTube and Vimeo. — AFP



## Over 500,000 Zoom accounts on sale on dark web for less than 1 sen each

TECHNOLOGY

Tuesday, 14 Apr 2020 2:35 PM MYT

By Angelin Yeoh

You can check if your details have been leaked online at Have I Been Pwned or Cyble's AmIBreached. — Bloomberg

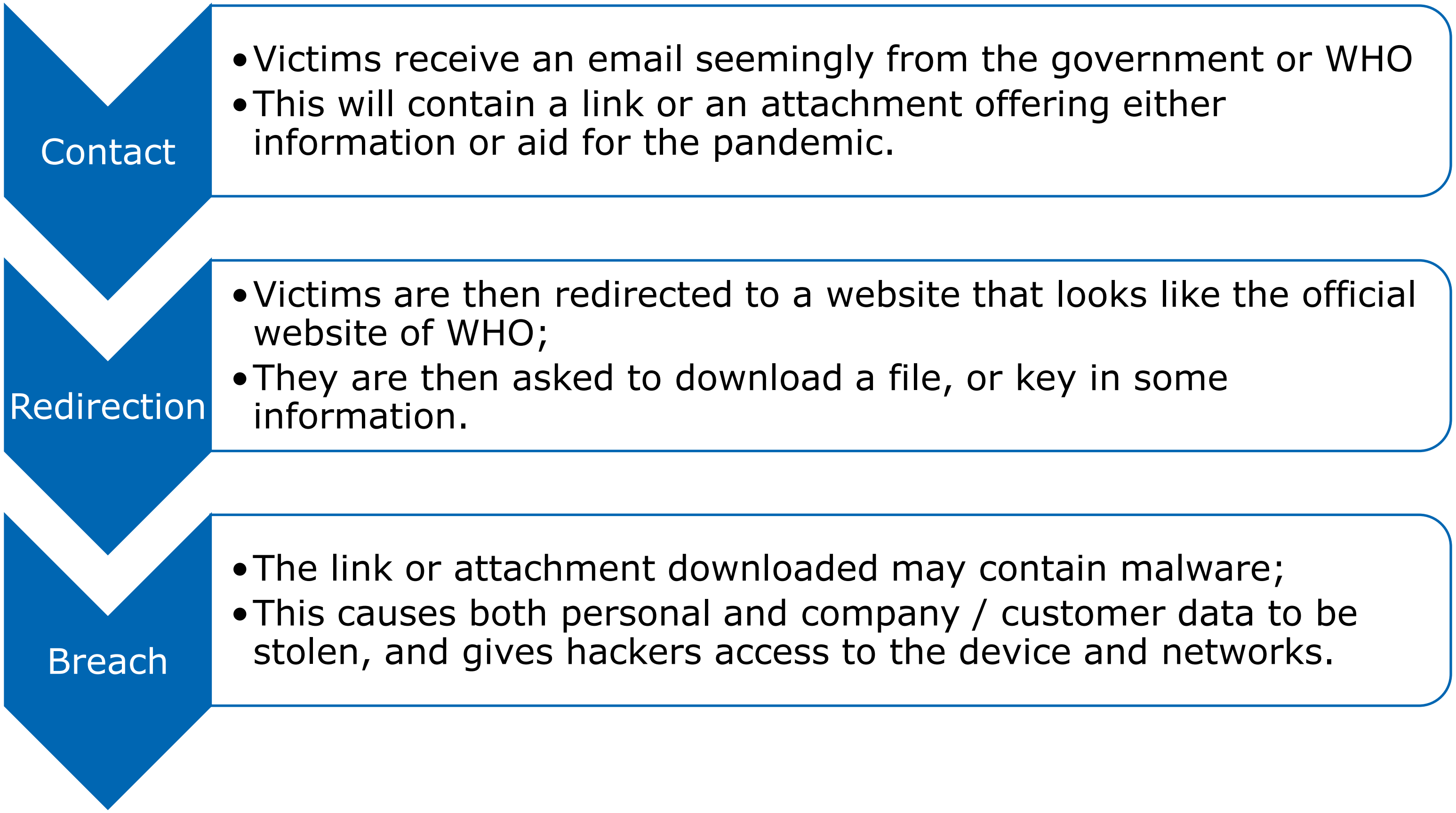
*Source: The Star Online, 6.4.2020 & 14.4.2020*

- A recent circular from the Malaysian National Security Council ("**NSC**") has warned government agencies against using the Zoom video conferencing application.

- NSC highlighted that the Zoom app contains a flaw which may enable hackers to compromise the app / listen in on users' conversations.

# Phishing, Scams and Malware

# How is Phishing Done?



Contact

- Victims receive an email seemingly from the government or WHO
- This will contain a link or an attachment offering either information or aid for the pandemic.

Redirection

- Victims are then redirected to a website that looks like the official website of WHO;
- They are then asked to download a file, or key in some information.

Breach

- The link or attachment downloaded may contain malware;
- This causes both personal and company / customer data to be stolen, and gives hackers access to the device and networks.

# Modus Operandi – Exploiting the Pandemic

- Emails and / or messages posing as trusted entities such as the World Health Organisation ("**WHO**");

- Links circulated with coronavirus-related domain names, seemingly with information and updates on the pandemic;

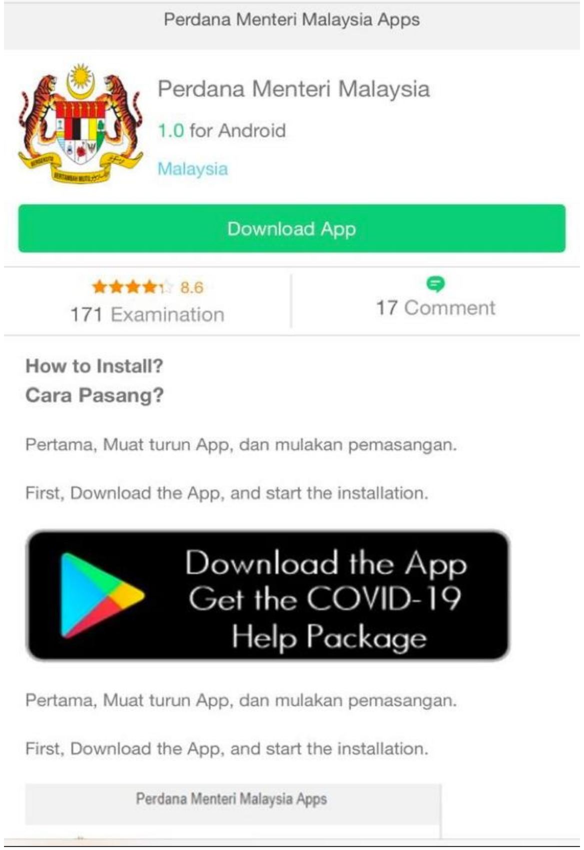
  - Eg.: *cdc-coronavirus[.]com / cdc-coronavirus[.]com*

# Modus Operandi – Exploiting the Pandemic

- Malicious applications purporting to have been launched by government organisations;
  - Eg.: “Perdana Menteri Malaysia App”
- Business E-mail Compromise (“**BEC**”) scams.

# Example – A Malicious Application

Sample Images: ”Perdana Menteri Malaysia App” as identified by the National Cybersecurity Agency of Malaysia (“**NACSA**”)



Perdana Menteri Malaysia Apps

Perdana Menteri Malaysia

1.0 for Android

Malaysia

Download App

★★★★☆ 8.6

171 Examination

17 Comment

**How to Install?**
**Cara Pasang?**

Pertama, Muat turun App, dan mulakan pemasangan.

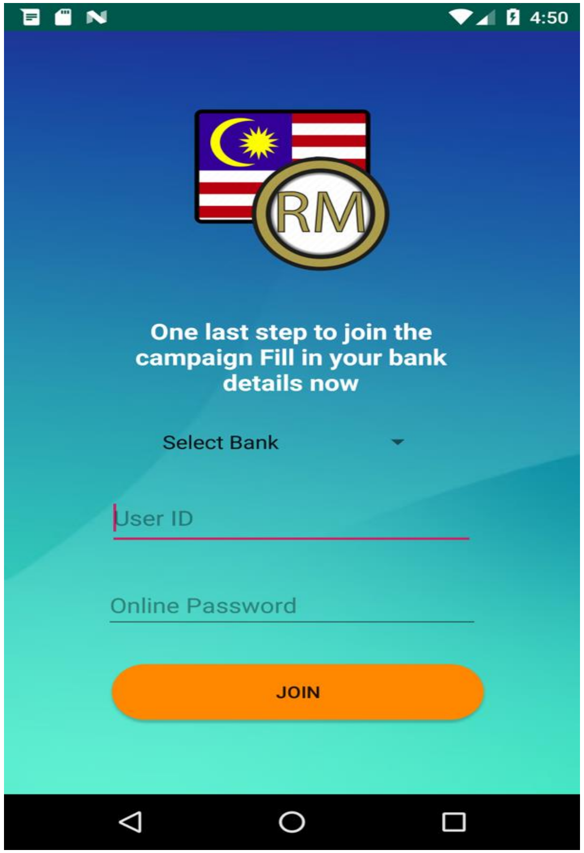
First, Download the App, and start the installation.

Download the App
Get the COVID-19
Help Package

Pertama, Muat turun App, dan mulakan pemasangan.

First, Download the App, and start the installation.

Perdana Menteri Malaysia Apps



4:50

**One last step to join the campaign Fill in your bank details now**

Select Bank

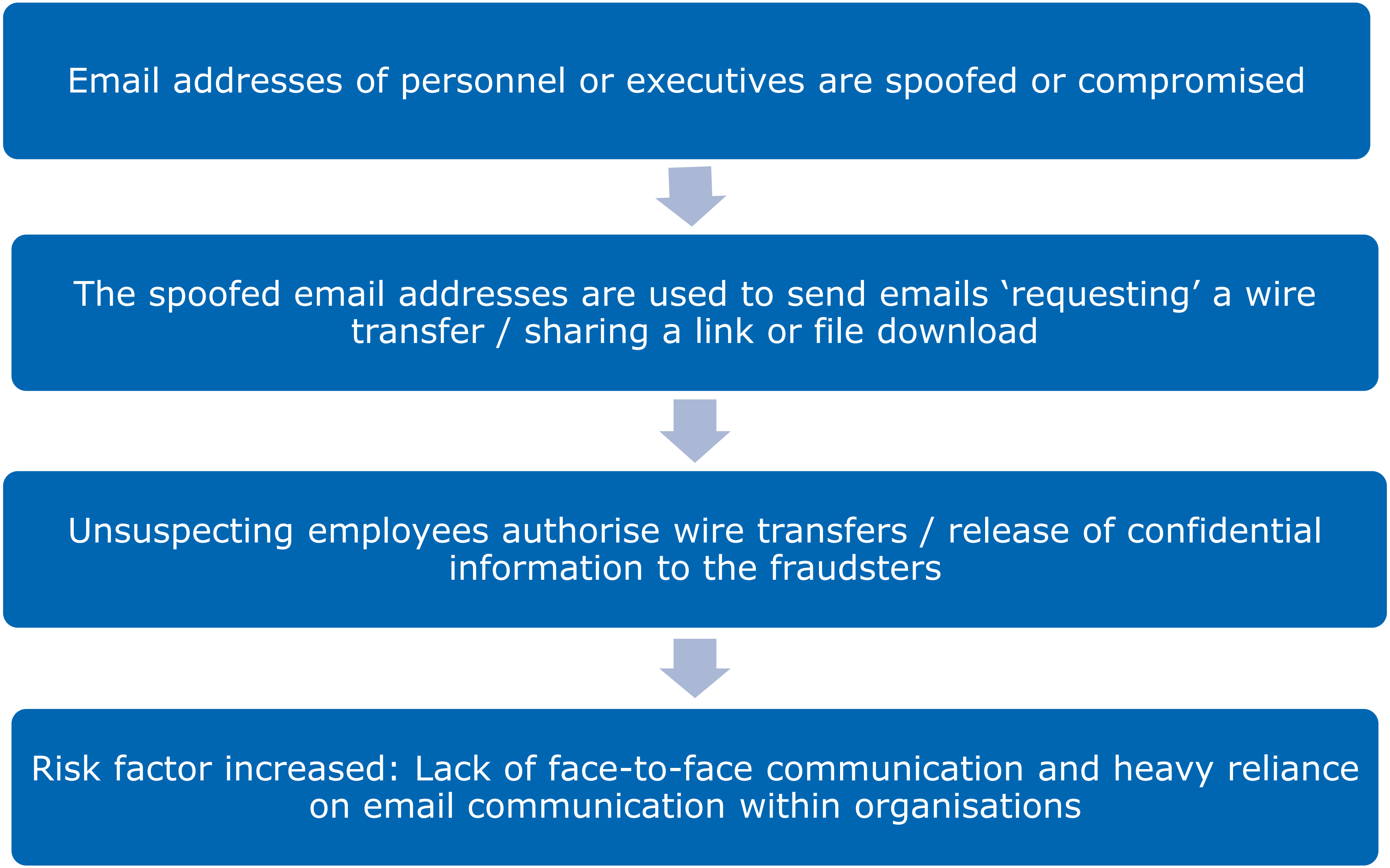
User ID

Online Password

JOIN

*Source: NACSA, 2.4.2020*

# Business Email Compromise ("BEC") Scams



Email addresses of personnel or executives are spoofed or compromised

The spoofed email addresses are used to send emails 'requesting' a wire transfer / sharing a link or file download

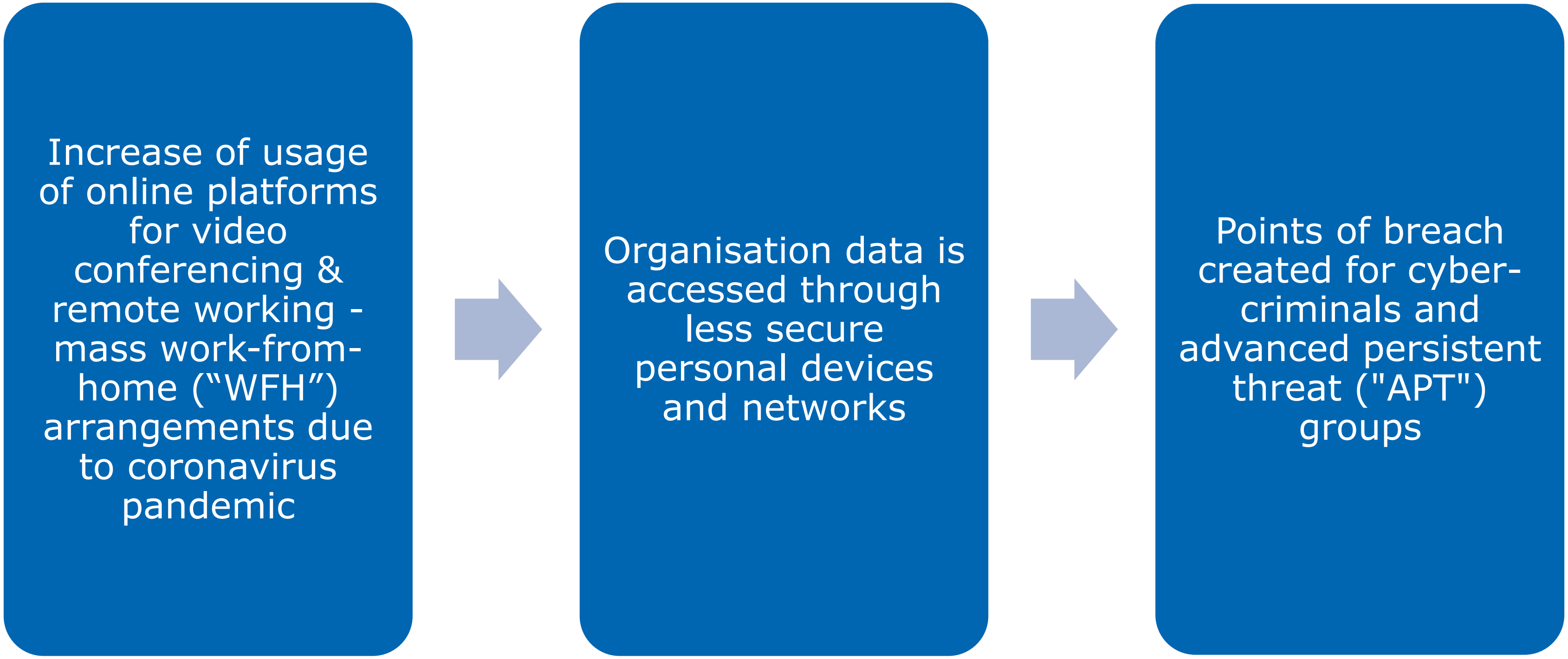
Unsuspecting employees authorise wire transfers / release of confidential information to the fraudsters

Risk factor increased: Lack of face-to-face communication and heavy reliance on email communication within organisations

# How Secure is Your Company's Teleworking Infrastructure?

| | |
|---|---|
| **Green -** least likely to be a weak target for hackers, low risk levels to sensitive data | • Readily equipped with secure digital infrastructure for WFH;<br>• Work devices for all employees to work remotely;<br>• Employees are well-trained in WFH best practices for cybersecurity |
| **Yellow -** a likely target for hackers, a serious risk level to sensitive data | • Digital infrastructure able to handle WFH arrangements with minor slow-downs / interruptions<br>• Employees use a mix of work and personal devices to work remotely |
| **Red -** lowest hanging fruit for hackers, highest risk level to sensitive data | • Digital infrastructure configured for office working / not well-equipped for access from multiple points when employees WFH<br>• Most / all employees WFH on personal devices<br>• No standard cloud-based database for storage of company / customer data |

# Why Companies are More Susceptible to Cyberattacks when Teleworking – an Overview



Increase of usage of online platforms for video conferencing & remote working - mass work-from-home (“WFH”) arrangements due to coronavirus pandemic

Organisation data is accessed through less secure personal devices and networks

Points of breach created for cyber-criminals and advanced persistent threat ("APT") groups

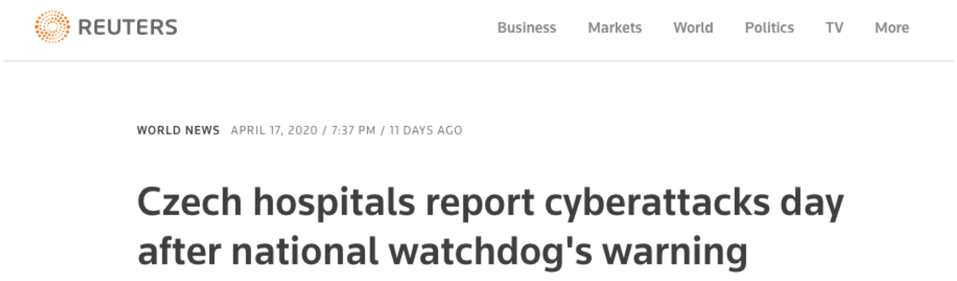
# Problems You Could Face

1. Overload of company servers / networks when accessed remotely by many employees

2. Employees work from personal devices and home networks

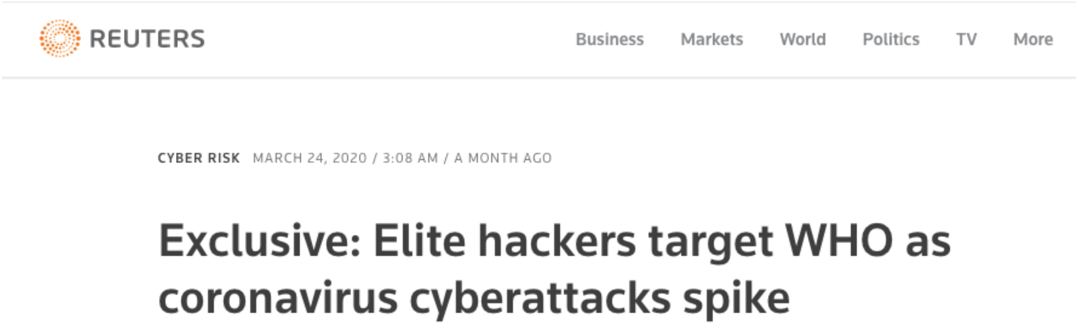
3. Employees tend to mix work with personal browsing when working from home

# Real-World Examples



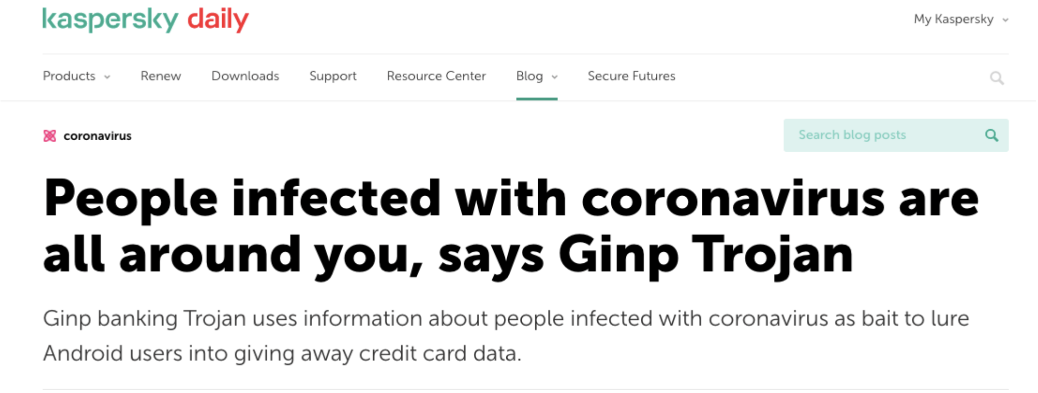
WORLD NEWS APRIL 17, 2020 / 7:37 PM / 11 DAYS AGO

Czech hospitals report cyberattacks day after national watchdog's warning



CYBER RISK MARCH 24, 2020 / 3:08 AM / A MONTH AGO

Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike



People infected with coronavirus are all around you, says Ginp Trojan

Ginp banking Trojan uses information about people infected with coronavirus as bait to lure Android users into giving away credit card data.

*Sources: Reuters 2020, Kaspersky 2020*

# Cybersecurity Breaches – a Force Majeure Event?

- Cyber attacks could severely impact companies’ business workings and their abilities to perform contractual obligations.

- Many force majeure clauses, being regarded as “boilerplate” clauses, are unlikely to cover cyber attacks as these are not normally a key consideration for companies in negotiating contractual terms.

- In the current climate, it would be wise to revise your contracts’ force majeure clauses to protect your company from civil suits over a contractual failure caused by a cyber attack.

# Sample Force Majeure Clause

*"Neither Party shall be liable for any delay or failure to perform its contractual / professional obligations in respect of this Agreement if such delay or failure is due to an act, omission or circumstance over which neither party could not reasonably have exercised control or could not, by reasonable diligence, have avoided ("**Force Majeure Event**"). Force Majeure Events shall include, but shall not be limited to, acts of God (including fire, floods or any other natural disasters) acts of Government or any regulatory or statutory bodies, any epidemics, any acts of war, insurrection, terrorism or riots, and / or any cyber-attacks or cybersecurity breaches suffered by the Parties.*

*If any delays or failures caused by a Force Majeure Event are continuous for a period of more than thirty (30) days, then either Party shall have the right to terminate the Agreement which the Force Majeure Event has affected in the manner as abovementioned, by giving fourteen (14) days written notice to the other Party."*

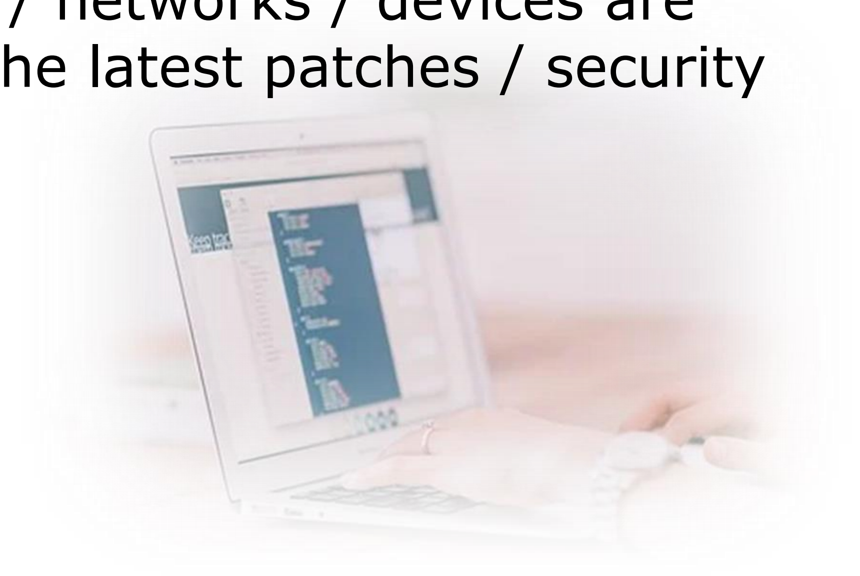
# Building Your Online Immunity - How You Can Protect Yourself and Your Company

# Tips on Protecting Your Company Online

1. To devise a detailed plan for your company in the event of a cybersecurity breach

2. Ensure all employees access company servers using a secure VPN

3. Ensure all company servers / networks / devices are constantly configured with the latest patches / security updates



# Tips on Protecting Your Company Online

4. Ensure teleconferencing / communication / e-mail applications used are secured with end-to-end encryption

5. Encourage employees to save all work documents on the company’s secure cloud database, instead of on their computers

6. Conduct remote briefing sessions on cybersecurity best practices to increase employee awareness

# Tips for Responding to a Breach

1. Take immediate steps to isolate and cut off the compromised account / device from the rest of the network

2. Take steps to stop the breach – ie. blacklist IP address where the threat originated, reformat and restore affected assets

3. Assess the damage that has been done / collate all relevant information

4. Notify all stakeholders / parties affected

5. Make a report to the relevant authorities – ie. NACSA Malaysia

# Relevant Agencies / Reporting Information

## NACSA

- Online complaint form: www.nacsa.gov.my/incident_report.php
- E-mail: aduan@nacsa.gov.my
- Telephone: +603-8064 4829

## CyberSecurity Malaysia

- Online complaint form: https://www.mycert.org.my/portal/online-form?id=7a911418-9e84-4e48-84d3-aa8a4fe55f16
- E-mail: cyber999@cybersecurity.my
- Helpline: 1-300-88-2999 (9am – 9pm)
- 24-hour helpline: +6019-2665850
- SMS: CYBER999 REPORT EMAIL COMPLAINT to 15888
- Via the "Cyber999 App" available on the App Store / Google Play Store

# Part Two

## Data Protection and Confidentiality Concerns

# The Pandemic has resulted in new norms

1. Work from Home Arrangements

    – Use of Personal Devices

    – Use of Third Party Platforms

2. Collection and disclosure of data to government authorities and commercial partners

    – Collection of personal data by companies

    – Use of contact tracing apps

# Privacy Risks and Confidentiality Concerns arising from Work From Home Arrangements

# 1. Use of personal devices

- Consumer-grade antivirus protection may not be sufficient against sophisticated cyberattacks

- Lack of control by the company over security features of personal devices

- Employees, for ease of accessibility during remote work, may forward confidential business or client information (including personal data) to personal accounts

- Risk of theft of devices containing confidential business or client information (including personal data)

## 2. Use of Third Party Platforms and Apps

- Working from Home
  - Zoom
  - Skype
  - Microsoft Teams

- Contacting family and friends
  - Whatsapp
  - Facetime
  - Telegram
  - WeChat
  - Social Media (Facebook, Instagram)

# Addressing privacy and confidentiality concerns

## 1. Strengthen the IT infrastructure supporting your company's WFH policy

- Consider using a virtual private network ("VPN") to access all internal / company databases and cloud storage systems
- Ensure all company databases and/or networks that are being accessed by employees remotely are configured with the latest updates and security patches
- Test remote access and continuity of operation capabilities

## 2. Review IT security polices and procedures

- There may be a need for additional security policies because the security controls which exist in the office environment may not exist in a remote environment.
- Review BYOD policies

# Addressing privacy and confidentiality concerns

## 3. Ensure that employees are adequately briefed and trained

- Remind employees:
  - Of their responsibilities to safeguard company networks and proprietary and confidential information
  - As far as possible, to keep work data on work computers
  - To avoid sharing sensitive / personal information online wherever possible, even via online teleconferencing applications

# Privacy Concerns arising from the Collection and Disclosure of Personal Data

# Collection and disclosure of personal data

## 1. Government Agencies

- Collection of personal data to monitor and mitigate the spread of the virus
  - Health information
  - Travel History
  - Information about a person’s contacts for tracing purposes

## 2. Commercial Partners

- Requests for sharing of personal data to support virus prevention and management efforts

# Privacy Risks

1. Legal Basis for the Collection and Disclosure of Personal Data

    - Key question is whether there is an appropriate lawful basis to capture the information

    - Consent may not be the most appropriate, though it may apply in some cases

    - Most relevant legal basis for processing is the necessity for the performance of a task for public interest

2. Consider how to mitigate the legal risks of sharing sensitive information

    - Information gathering should be proportionate and reasonable response

    - Data minimization

    - Contractual controls

# Singapore – Personal Data Protection Commission

## Advisory: Collection of Personal Data for COVID-19 contact tracing

- Organisations may collect personal data of visitors to premises for purposes of contact tracing and other response measures in the event of an emergency
- No consent required
- Necessary to respond to an emergency that threatens the life, health or safety of other individuals
- NRIC numbers may be collected to accurately identify individuals
- Organisations must comply with Data Protection Provisions
  - Make security arrangements to protect the personal data from unauthorised access or disclosure
  - Ensure that personal data is not used for other purposes without consent or authorisation under the law
- Sample notice

# Contact Tracing Apps

## What is it?

- To help contain the spread of Covid 19, this app is to inform someone if they have been in contact with someone positive of Covid-19
- Bluetooth contact tracing uses a relative signal strength indicator to detect when one device is near another, and for how long.

## What actually is contact trancing?

The World Health Organisation (WHO) defines contact tracing as the identification and follow-up of persons who may have come into contact with a person infected with a contagious disease, to help the contacts to get relevant care and treatment.

# Contact Tracing apps

**Some of the countries implementing these:**

- China – App assigns a colour code that reflects health condition and travel history

- South Korea – App tracks movement of confirmed COVID-19 cases

- Israel – App warns people if they have crossed paths with another patient

- Taiwan – App creates digital fence using smartphone data to enforce quarantines

- Singapore – TraceTogether https://www.youtube.com/watch?v=buj8ZTRtJes#action=share

- Malaysia- CovCT

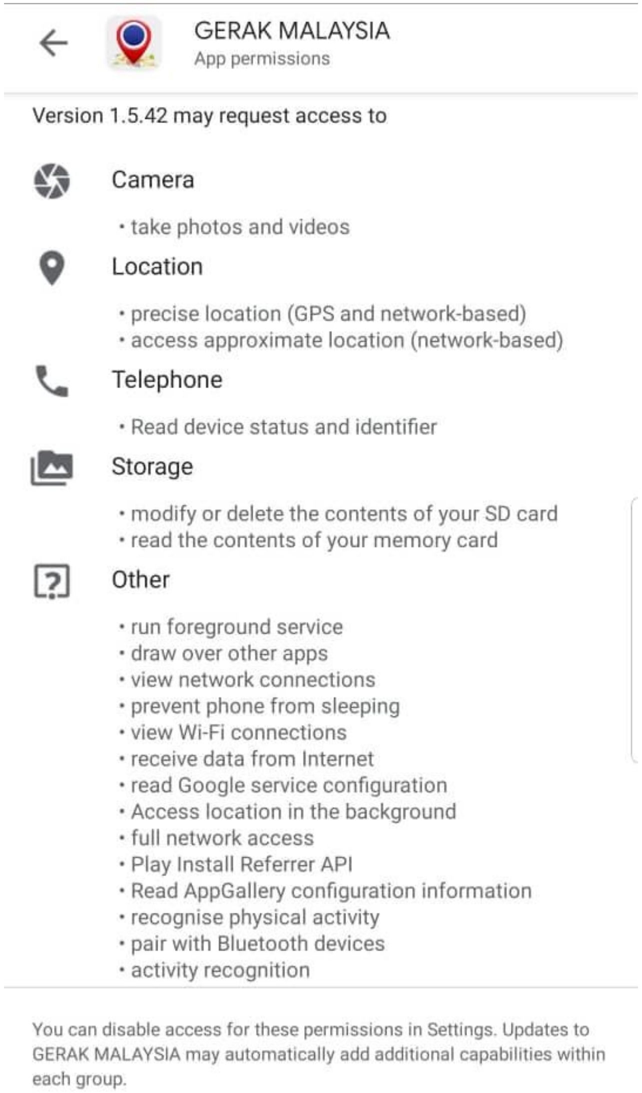
# Gerak Malaysia App

## What is it?

- an app to help authorities to keep track of Malaysians' movements throughout the country. (Contact tracing apps)

- Malaysians wanting to travel interstate need to apply for permission via this app from 26th April 2020 onwards. (**Restricted to those stranded in their hometowns after MCO was announces and wish to return to their home/workplace)**

# Permissions requested by the Gerak app



GERAK MALAYSIA
App permissions

Version 1.5.42 may request access to

Camera

- take photos and videos

Location

- precise location (GPS and network-based)
- access approximate location (network-based)

Telephone

- Read device status and identifier

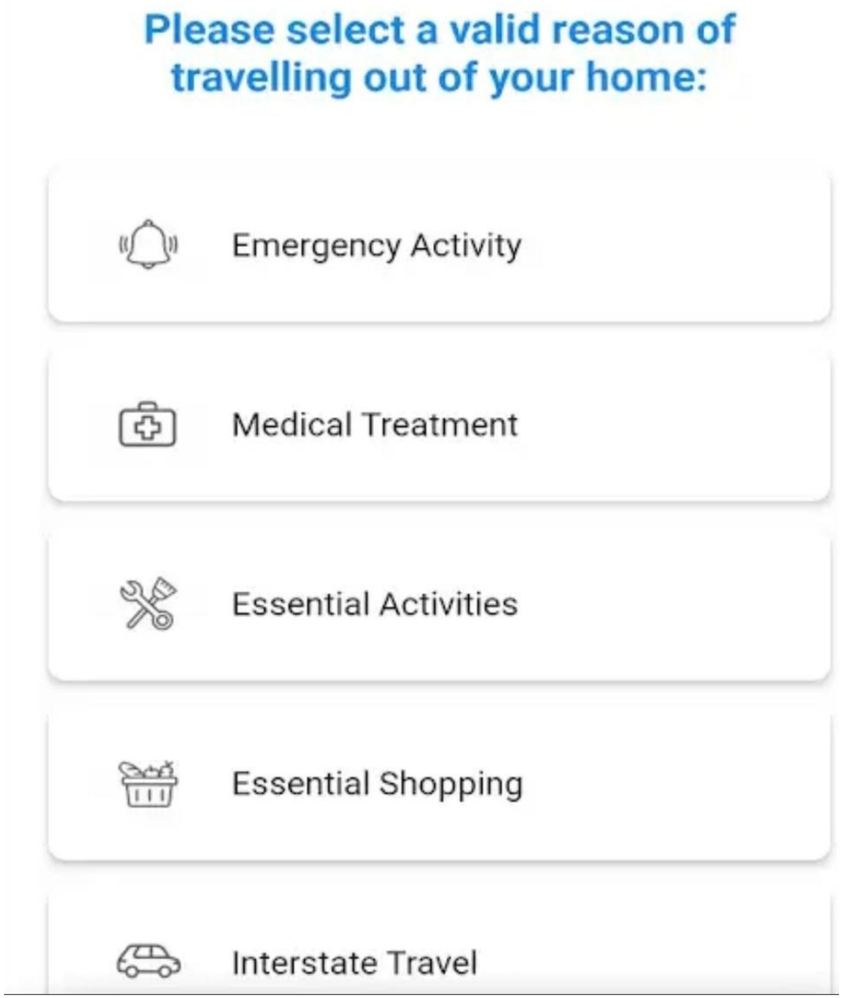
Storage

- modify or delete the contents of your SD card
- read the contents of your memory card

Other

- run foreground service
- draw over other apps
- view network connections
- prevent phone from sleeping
- view Wi-Fi connections
- receive data from Internet
- read Google service configuration
- Access location in the background
- full network access
- Play Install Referrer API
- Read AppGallery configuration information
- recognise physical activity
- pair with Bluetooth devices
- activity recognition

You can disable access for these permissions in Settings. Updates to GERAK MALAYSIA may automatically add additional capabilities within each group.



Please select a valid reason of travelling out of your home:

Emergency Activity

Medical Treatment

Essential Activities

Essential Shopping

Interstate Travel

# Europe

1. Recommendation of European Commission 8 April 2020
   - Common European Union toolbox for the use of technology and data to address the COVID-19 crisis
2. Objectives:
   - To protect privacy and maintain data protection
   - Ensure that these efforts do not lead to surveillance and stigmatization
3. Mobile apps should:
   - Strictly limit the processing of data to combatting COVID-19
   - Ensure regular review of whether the processing of personal data remains necessary
   - Take measures to ensure that, once processing is no longer strictly necessary, the processing is effectively terminated and the personal data is irreversibly destroyed.
4. National apps must be:
   - Voluntary
   - Approved by the national health authority;
   - Privacy-preserving, through the use of encryption; and
   - Dismantled as soon as they are no longer needed

# Addressing privacy concerns
# Collection and use of personal data

1. Ensure that information gathering is proportionate and reasonable
    - Only collect what is necessary in the circumstances

2. Adhere to the PDPA and PDPC advisories

3. Use sample notices

4. Contractual controls where personal data is shared with commercial partners

5. When using contact tracing apps, know how your personal data will be dealt with

# Part Three:
# Business Continuity Technology Considerations

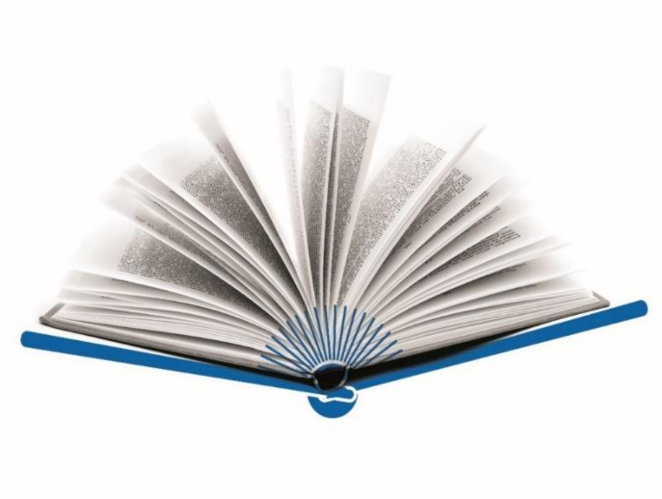
# Introduction

- Covid-19
- Business continuity via a technology lens
- Managing technology risks with key third party service providers

# What does Business Continuity mean in relation to your Technology Solutions?

- What is Business Continuity vs a Business Continuity Plan?

- What about a Disaster Recovery Plan – is this the same or different?
  - DR is not the same as BC
  - DR is a key component of a BCP



# Covid-19 Technology Checklist

- Check-in with your service providers!
- Review and consider your key vendor contracts
- Where are your data centres located? Can you visit your co-location data centres?
- Check the capacity of your infrastructure and other services (e.g. SaaS) for higher utilisation
- Check your software licence allocations – do you require more? Named Users vs Concurrent licences?

## Key Components of a BCP

- Business Impact Assessment
  - Why is this important? What is a critical business function?
- Recovery Point Objectives vs Recovery Time Objectives
  - RTO v RPO – what is the difference?
  - How does it differ to “Availability”?
- Testing and Updates
  - How often should you test your BCP?
- What kind of BCP should you have?
  - Customised v Generic

# Regulatory Considerations

– Business Continuity Plans (and business continuity generally) are a regulatory requirement for certain sectors

HONG KONG MONETARY AUTHORITY
香港金融管理局

SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

保險業監管局
Insurance Authority

# Additional contractual considerations

- Force Majeure Events
- Notification obligations
- Disengagement and Transition-out requirements
- Data back-ups / recovery / portability

**Suaran Singh Sidhu**
**Partner - LAW Partnership (Malaysia), associated firm of Eversheds Harry Elias LLP**
**suaransidhu@law-partnership.com**

Suaran Singh Sidhu is the Head of Technology, Media and Telecommunications of LAW Partnership. He has extensive experience in cybersecurity, information technology (IT) and personal data protection laws, and regularly advises on legal matters in the fields of entertainment, media and telecommunications. Suaran provides his insight and knowledge on regulatory compliance issues, cybersecurity, and the practices and policies in the Asia-Pacific region and where PDPA in Malaysia is concerned, Suaran advises on compliance requirements, provides training, conducts privacy audits, and formulates privacy roadmaps for clients.

## Guest Speakers

**Tan Weiyi**
**Partner - Eversheds Harry Elias LLP (Singapore)**
**weiyitan@eversheds-harryelias.com**

Tan Weiyi is a Litigation and Dispute Management Partner of Eversheds Harry Elias LLP. Weiyi handles complex cross-border disputes and corporate investigations, and represents clients in litigation, mediation and arbitration proceedings relating to a range of commercial disputes. Weiyi also advises and represents clients in investigations and enforcement actions, focused on corruption, financial fraud and other white-collar criminal offences. Weiyi also regularly advises on privacy issues, both generally and in the context of internal investigations and regulatory disclosures. She is a Certified Privacy Manager with the International Association of Privacy Professionals and has assisted multinational clients in the design and implementation of their data privacy compliance programmes.

**Rhys McWhirter**
**Of Counsel - Eversheds Sutherland (Hong Kong)**
**rhysmcwhirter@eversheds-sutherland.com**

Rhys is an Of Counsel at Eversheds Sutherland and leads the Commercial and Technology, Media and Telecoms (TMT) practice. He has extensive experience in drafting and negotiating high-value and strategic commercial and technology agreements and has acted for both government and private sector clients, particularly financial institutions throughout Asia-Pacific on complex commercial and digital transformation projects. Rhys has advised various clients on a broad range of commercial and TMT transactions, including complex supply and service agreements, FinTech, technology outsourcing & digital transformation and data privacy projects, and has acted for many FinTech start-ups across Asia on various emerging technologies such as blockchain and cryptocurrency.

**law-partnership.com**