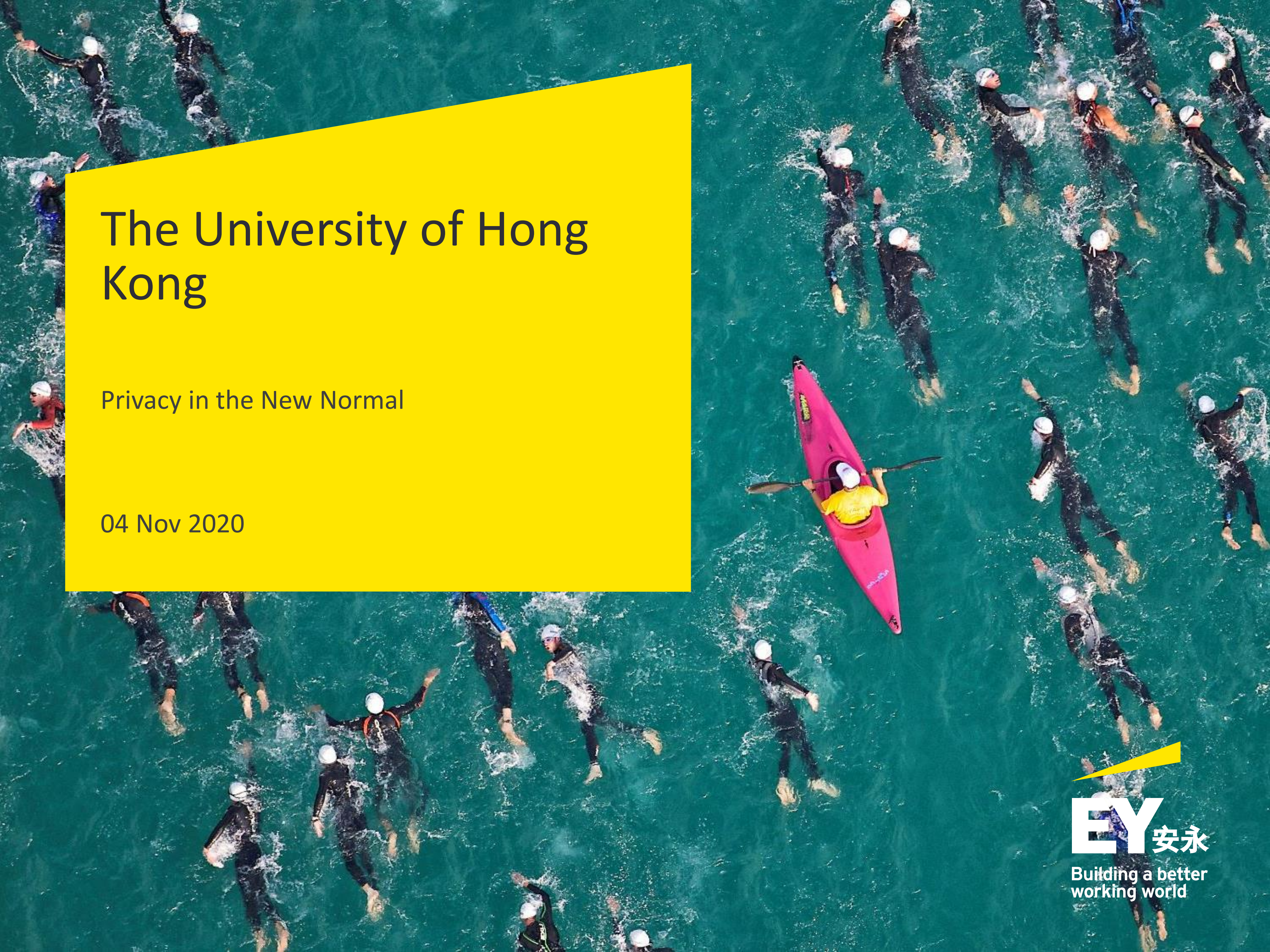
The University of Hong Kong

Privacy in the New Normal

04 Nov 2020



EY 安永

Building a better
working world

Agenda

1. ckground Information
2. What is New Normal?
3. Emerging Cybersecurity Challenges
4. The System & Practices in the University

1 Background Information

Privacy Commissioner for Personal Data (PCPD)

- An **independent statutory body** set up to oversee the enforcement of the Personal Data (Privacy) Ordinance (Cap. 486) which came into effect in 1996

- To **secure the protection of individuals' privacy** with respect to personal data through:
  - Promotion
  - Monitoring
  - Supervision

Personal Data (Privacy) Ordinance (Cap. 486)
Key definitions under the PDPO

- ‘**Personal data**’ means any data -
  - (a) Relates directly or indirectly to a living individual (“**data subject**”)
    - Can be used to identify that person
  - (b) Exists in a form which can be processed and accessed

e.g.

Name	**ID card number**
Phone number	**Medical record**
Address	**Employment record**

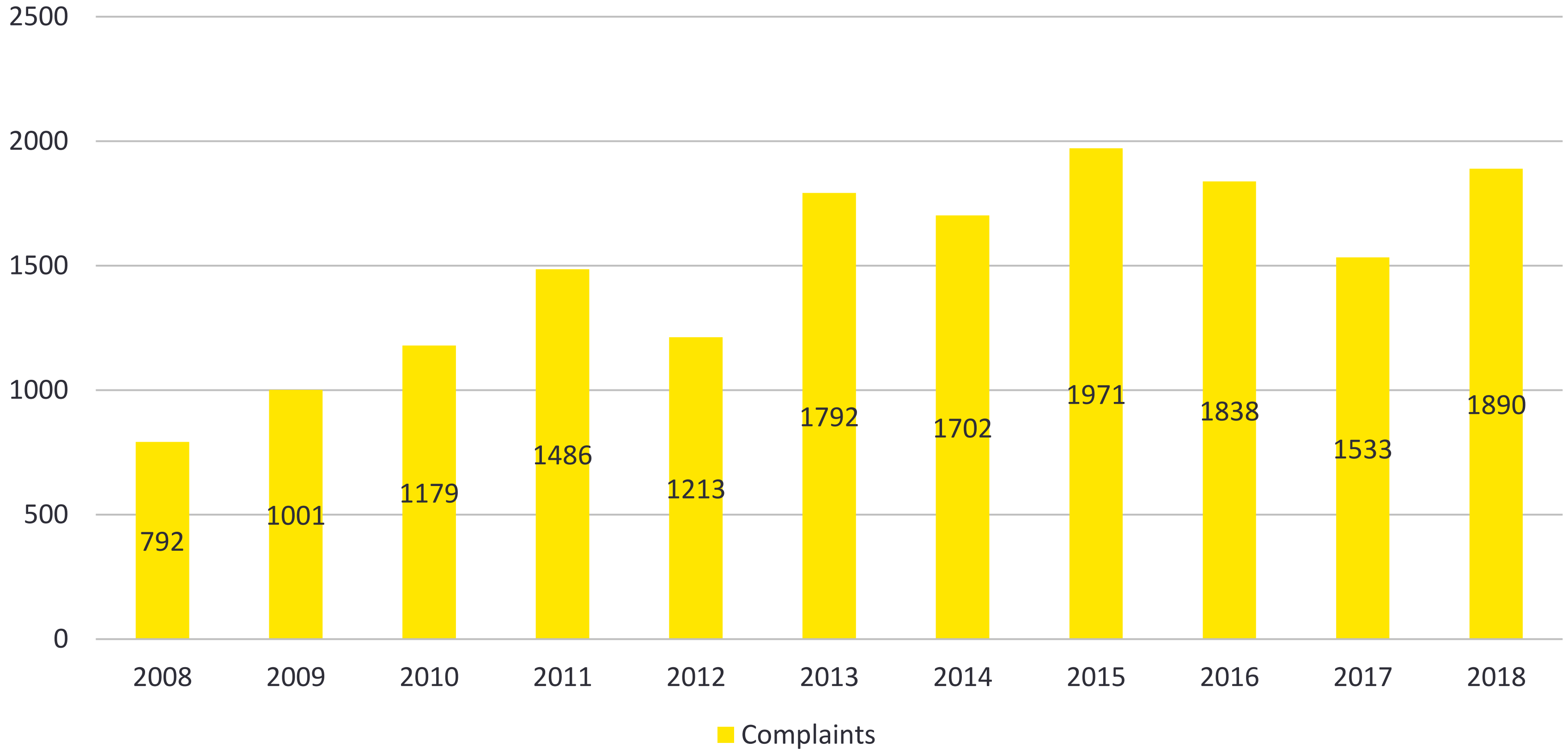
- **Sensitive personal data (with reference to General Data Protection Regulation GDPR)**
  - HKID
  - Health-related data
  - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs
  - Data concerning a person’s sex life or sexual orientation

Personal Data (Privacy) Ordinance (Cap. 486)
Key definitions under the PDPO

- ‘**Data user**’ means a person who
  - Either alone or jointly or in common with other persons, controls the collection, holding, processing, usage
  - Liable as the principal for the wrongful act of its authorized data processor

- ‘**Data processor**’ process data on behalf of the data user, instead of for his/her own purpose(s)
  - Data processors are not directly regulated under the PDPO
  - Data users are required to, by contractual or other means, ensure that their data processors meet the applicable requirements of the PDPO

Number of complaint cases received by PCPD



Source: https://www.pcpd.org.hk/english/complaints/statistics/statistics.html

Personal Data (Privacy) Ordinance (Cap. 486)

Six Data Protection Principles

DPP1: Collection

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function / activity of the data user. Data collected should be adequate but not excessive.

DPP2: Accuracy & Retention

Practical steps shall be taken to ensure personal data is accurate and not kept longer than what is necessary to fulfil the purpose for which it is used.

DPP3: Data Use

Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.

Source: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

Personal Data (Privacy) Ordinance (Cap. 486)

Six Data Protection Principles

DPP4: Data Security

A data user needs to take practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use.

DPP5: Openness

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

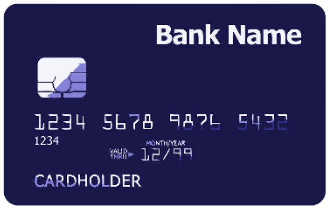
DPP6: Data Access & Correction

A data subject must be given access to his / her personal data and allowed to make corrections if it is inaccurate.

Source: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

What are the hackers usually looking for?

- ID card number
- Passport number
- Credit card information
- Username and password
- Birthday



What are the hackers usually looking for? (Cont'd)

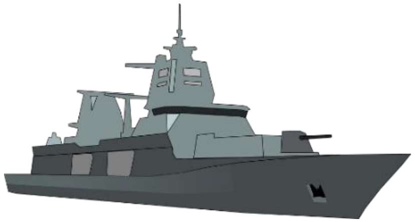
- Student PII (personally identifiable information)
- Cutting edge research
- Technology innovations
- Intellectual property

What are the hackers usually looking for? (Cont'd)

- Direct compromise of **email systems**
- Exposure of **sensitive patient information** in school health care systems
- **DDoS** attacks that interrupted daily operations during key times in the school year
- Costly **ransomware** that resulted in ransom paid for the return of sensitive data
- **Phishing** attack

What are the hackers usually looking for? (Cont'd)

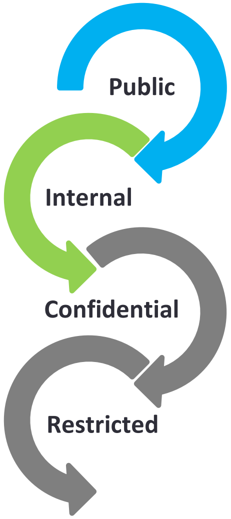
- Hackers have been targeting universities in an effort to uncover maritime technology that is being developed for military use.
- 27 universities were involved
- Focused on **stealing research data**
- The university networks were breached **with phishing emails** that hackers designed to look like real messages from other universities. The emails were secretly packed with **spyware** instead.
- The effort dates back for almost 2 years



Source: fortune - 5 March, 2019

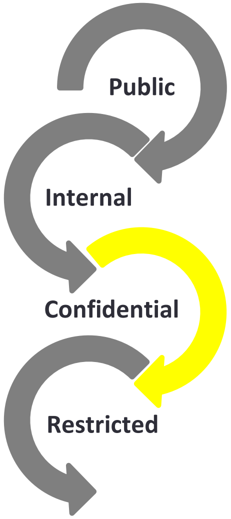
HKU’s Data Classification Scheme

- **Four Levels of Classification**
  - **Public**
    - Open to Public
    - No Restriction on Access
    - Present minimal perceived risk
    - i.e. HKU policies, programme information, press releases
  - **Internal**
    - Non-sensitive operational data/information
    - Disclosures are not expected to cause serious harm to HKU
    - Access may be provided to staff based on respective roles and responsibilities
    - i.e. Staff handbooks, training materials, internal procedures



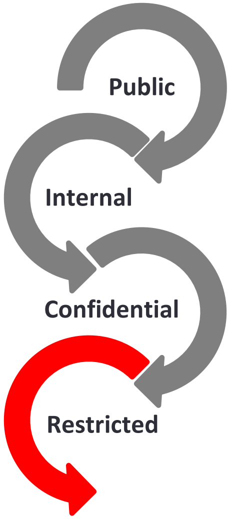
HKU's Data Classification Scheme

- **Confidential**
  - Sensitive data/information intended for use by specific group of authorized personnel within HKU and business partners
  - Assigned on a need-to-use basis
  - Unauthorized disclosure, modification or destruction would adversely affect the business or continuity of operations
  - i.e. Student and staff personal information, unpublished research information, identifiable research subject data



HKU's Data Classification Scheme

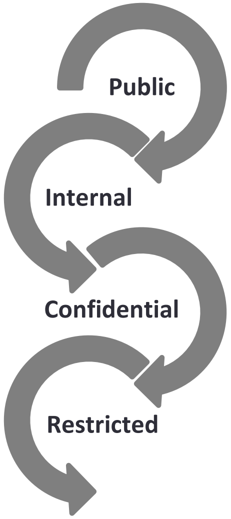
- **Restricted**
  - Data/information that is very sensitive in nature and restricted by HKU, the gov or any other agreements between HKU and 3rd parties
  - Critical to HKU's capacity to conduct its business
  - Used exclusively by limited numbers of predetermined and authorized individuals
  - Financial lost or damage to HKU's reputation
  - i.e. Examination papers before official release, privileged accounts' passwords, sensitive personal data (HKID, credit card information)



HKU’s Data Classification Scheme

- Make good use of the **HKU Data / Information Asset Inventory**

- Categories
- Description
- Responsible Data Steward
- Concerned Data Custodian
- Physical location
- Digital Storage
- IT Application / System name
- System Owner
- Classification
- Security Measures



Public

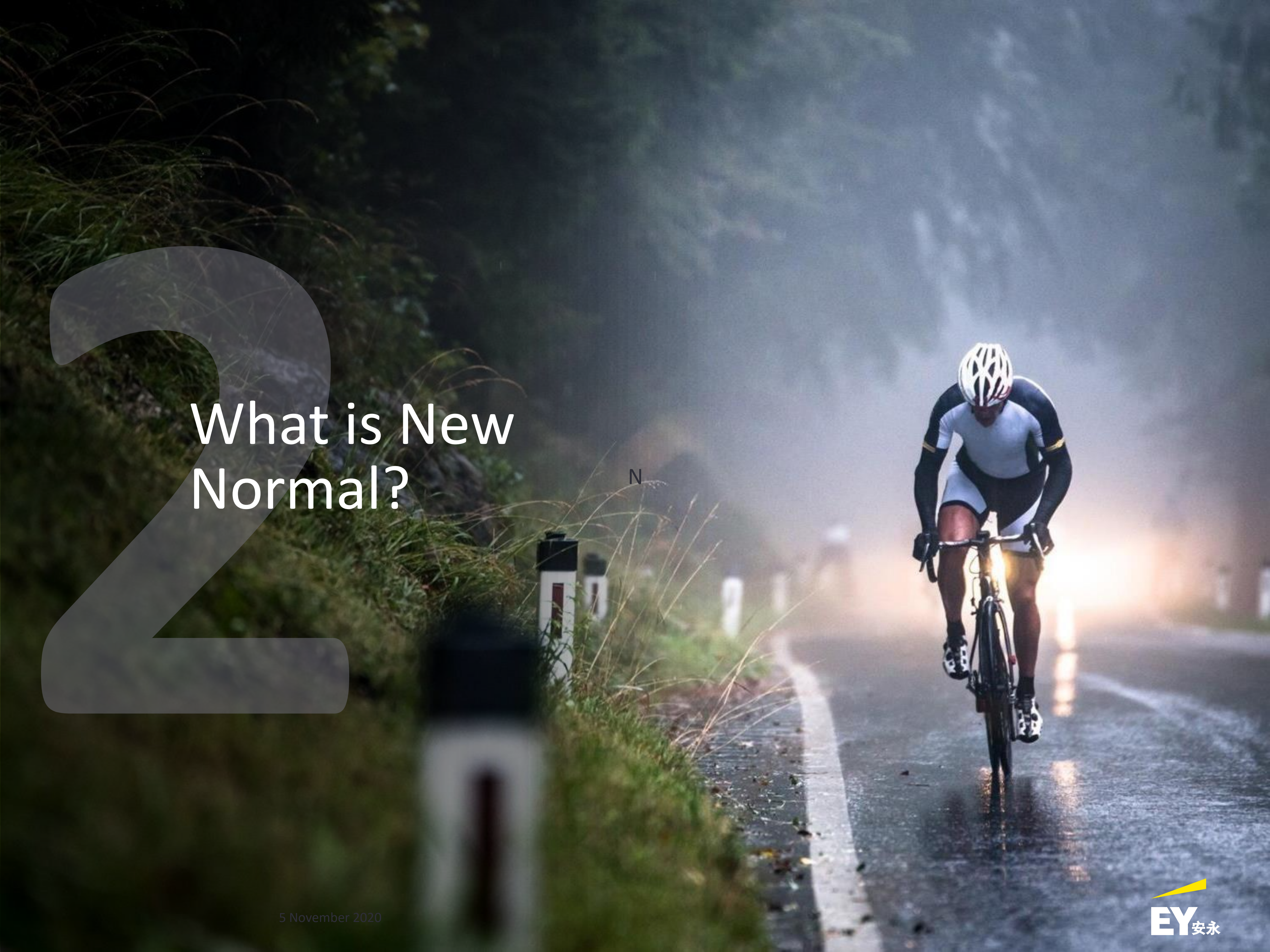
Internal

Confidential

Restricted

Criticality

Storage, encryption mechanism, user access etc.



2 What is New Normal?

N

What is new normal?

New normal

A state to which a **society**, **economy**, **technological environment** etc. settles following a crisis, which differ from the situation that prevailed prior to the start of the crisis.

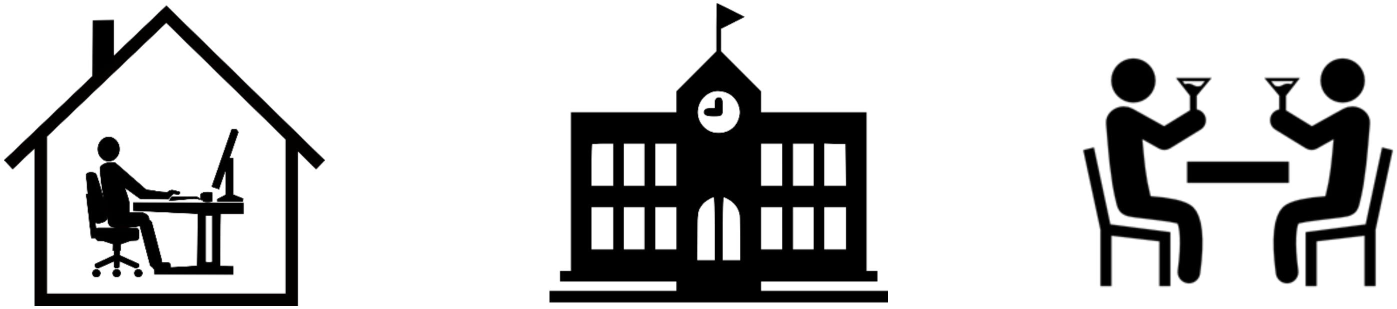
1. Global Financial Crisis (GFC) of 2007/08
2. Aftermath of the 2008-12 global recession
3. COVID-19 pandemic

What is new normal?

COVID-19

The COVID-19 pandemic has popularized the use of this term.

The pandemic has changed the daily life for most people, such as limiting person-to-person contact, social distancing etc.



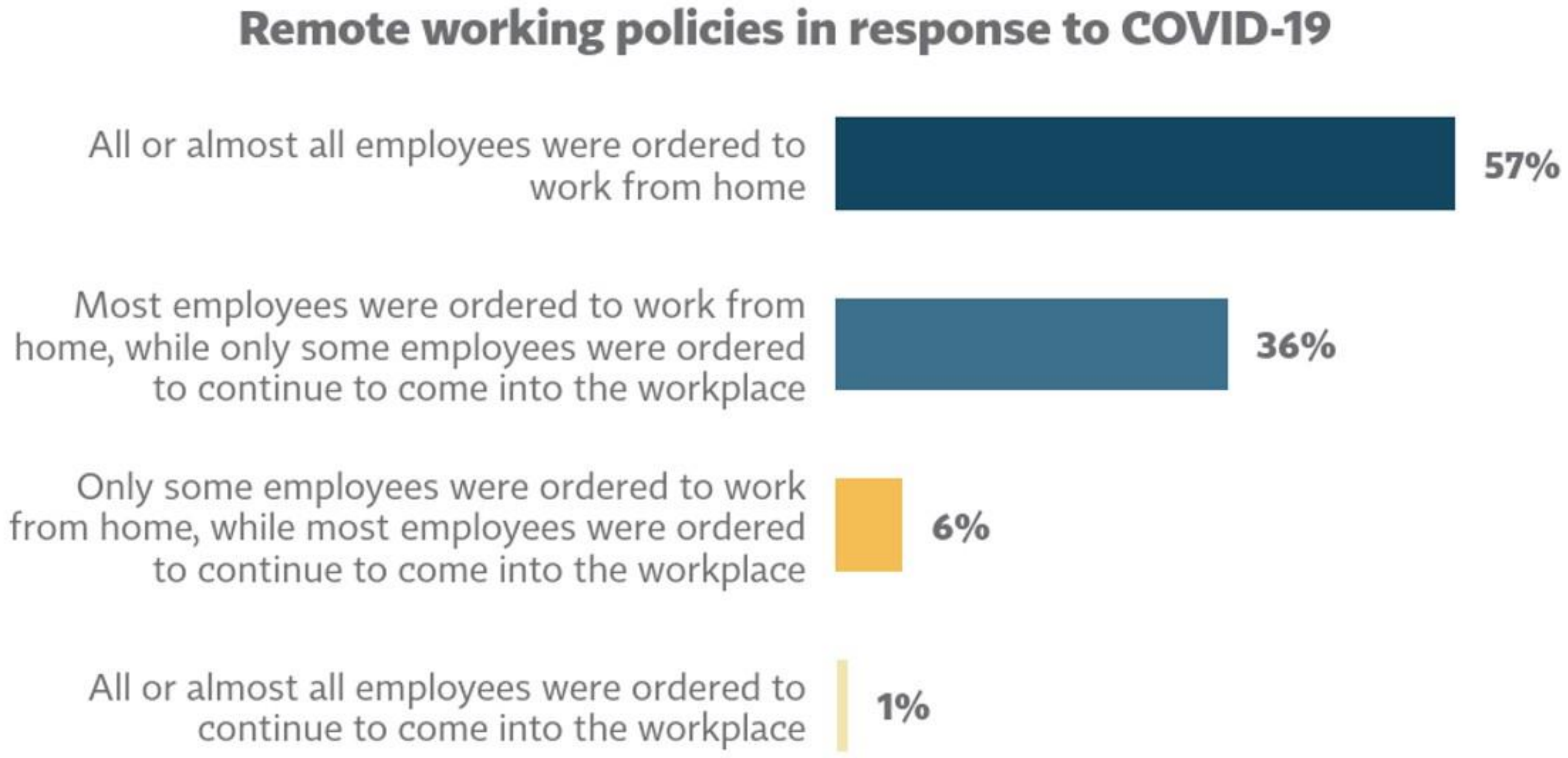
3 Emerging Cybersecurity Challenges

Covid-19 Pandemic introduced...

Work-From-Home

Work From Home (WFH) Overview

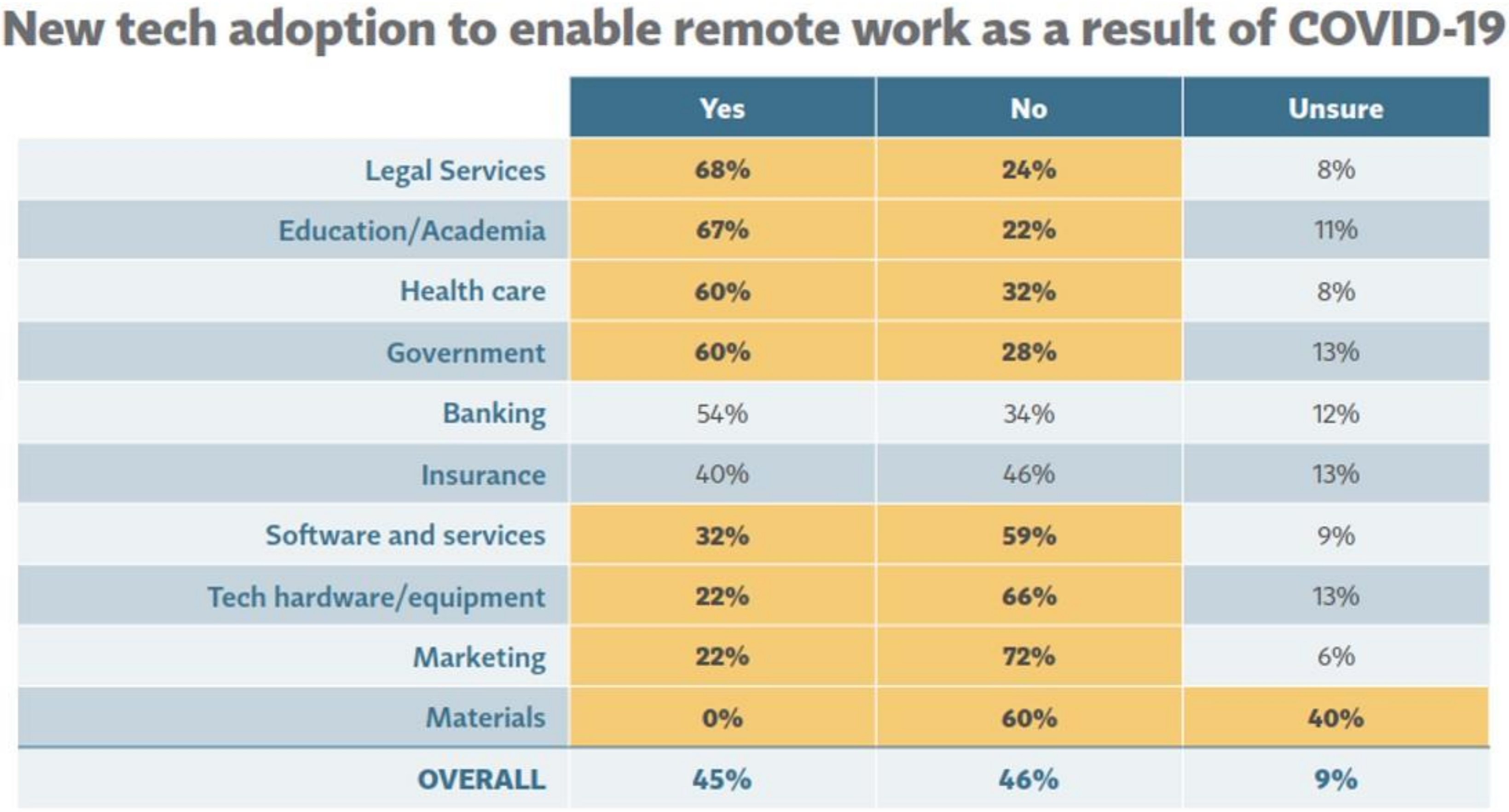
- More than 90% of organizations have put in place a policy requiring most or all employees to work from home



Source: Privacy in the Wake of COVID-19, EY and International Association of Privacy Professionals (IAPP) 2020

WFH Overview

- Education/academia has been one of the biggest new adopters of WFH technologies



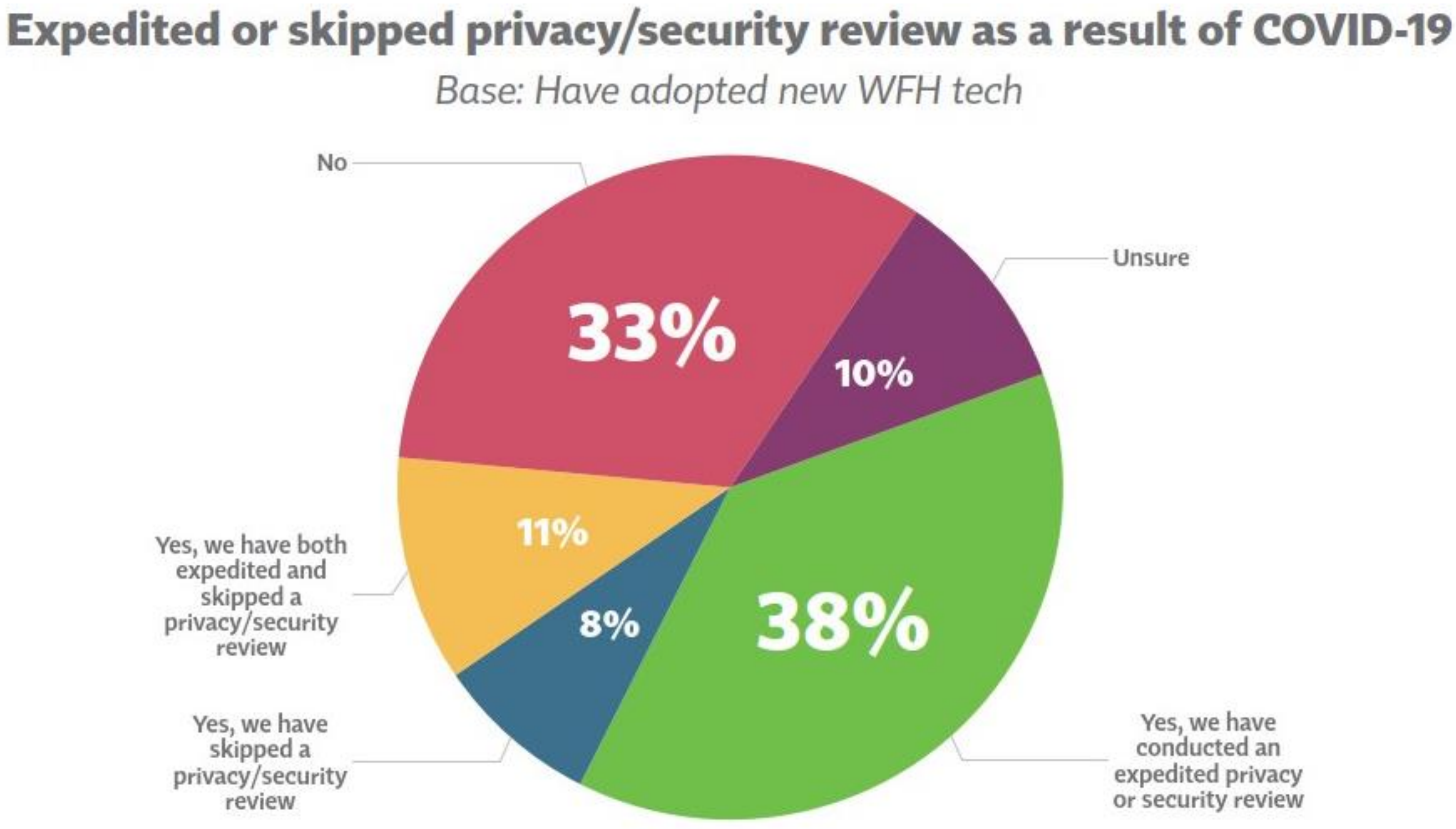
New tech adoption to enable remote work as a result of COVID-19

	Yes	No	Unsure
Legal Services	**68%**	**24%**	8%
Education/Academia	**67%**	**22%**	11%
Health care	**60%**	**32%**	8%
Government	**60%**	**28%**	13%
Banking	54%	34%	12%
Insurance	40%	46%	13%
Software and services	**32%**	**59%**	9%
Tech hardware/equipment	**22%**	**66%**	13%
Marketing	**22%**	**72%**	6%
Materials	**0%**	**60%**	**40%**
OVERALL	**45%**	**46%**	**9%**

Source: Privacy in the Wake of COVID-19, EY and International Association of Privacy Professionals (IAPP) 2020

WFH Overview (Cont'd)

- Of the organizations that have adopted new WFH tech, nearly 60% have accelerated or bypassed privacy/security review



Source: Privacy in the Wake of COVID-19, EY and International Association of Privacy Professionals (IAPP) 2020

Difference between WFH and office

Enterprise Network

- Logical Network Segmentation
- Secure System Configurations & Networ Deployment
- Advanced Network Monitoring Technologies
- Centralized Computer & Device Management

Home Network

- Unprotected Network
- Unsecured System Configurations
- Lack of Network Monitoring & Defense Mechanism
- Unprotected Endpoints & Devices

Major Risks Arising from Work From Home Arrangement

- More likely to be infected by malware due to relatively unsecured system configurations
- Higher chance of being compromised by external cyber-attackers due to insufficient network protection and the lack of the network monitoring
- Higher likelihood of accidental data leakage due to less secure endpoint protection in home network

Bring Your Own Device & Video Conferencing

- **Bring Your own Device (BYOD)**
  - Employees use their personal devices to access work-related systems and the organization’s information, potentially personal or confidential data.

- **Video Conferencing**
  - A technology that allows users in different locations to hold face-to-face meetings without having to move to a single location together.

Company Meeting

Seminar

Remote classroom

zoom

Webex Meetings

BYOD Security Risks

- **BYOD**
  - A lot of personal devices are already infected with **malware**
  - **Security configurations** and **hardening controls** might not be aligned with the organization’s standards
  - Storing the **organization’s information and data** on personal devices without proper guidelines and controls might lead to various **privacy issue** (i.e. data retention)

  - **Unsecured** and **uncontrolled** BYOD devices might create huge security loopholes in the organization’s security posture

BYOD Security Tips

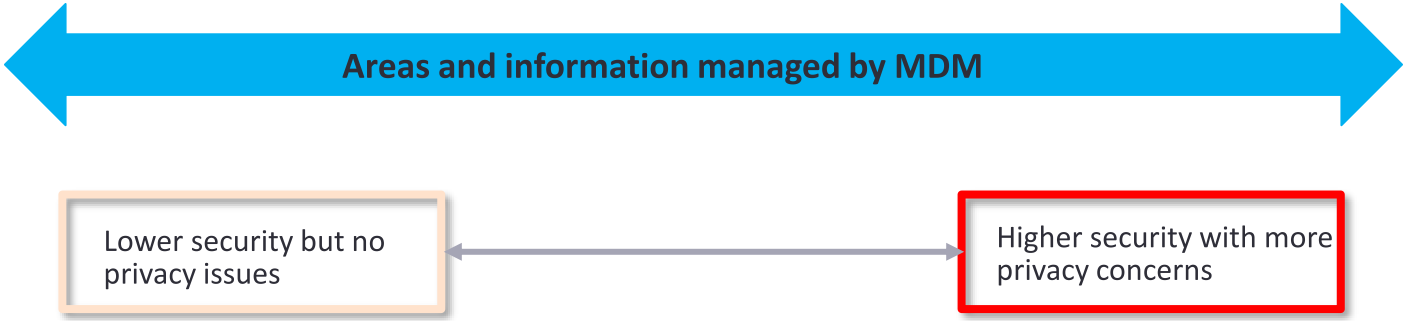
- Establish a **BYOD Policy** outlining critical security considerations such as:
  - Onboarding procedures
  - Type of devices that are sanctioned by the organization
  - Employees who can leverage BYOD
  - Data that can be accessed from these devices

- Use **Mobile Device Management (MDM)** solutions to control and monitor the devices:
  - Monitor the applications and updates being installed on the device
  - Deploy update patches
  - Monitor the usage of devices in the MDM server
  - Configure security settings on the device
  - Track the device's location
  - Remote wipe the device

- It's very important for the organization to ascertain if personal/sensitive data should be retained in BYOD devices and how its **retention** and **erasure policy** can be applied equally and effectively

BYOD Security Tips (Cont’d)

- Whilst a certain level of monitoring and control should be maintained over the BYOD devices, **both the organization and the users** should be aware of **what** and **how** the device is being managed



Areas and information managed by MDM

Lower security but no privacy issues

Higher security with more privacy concerns

Video Conferencing Security Risks

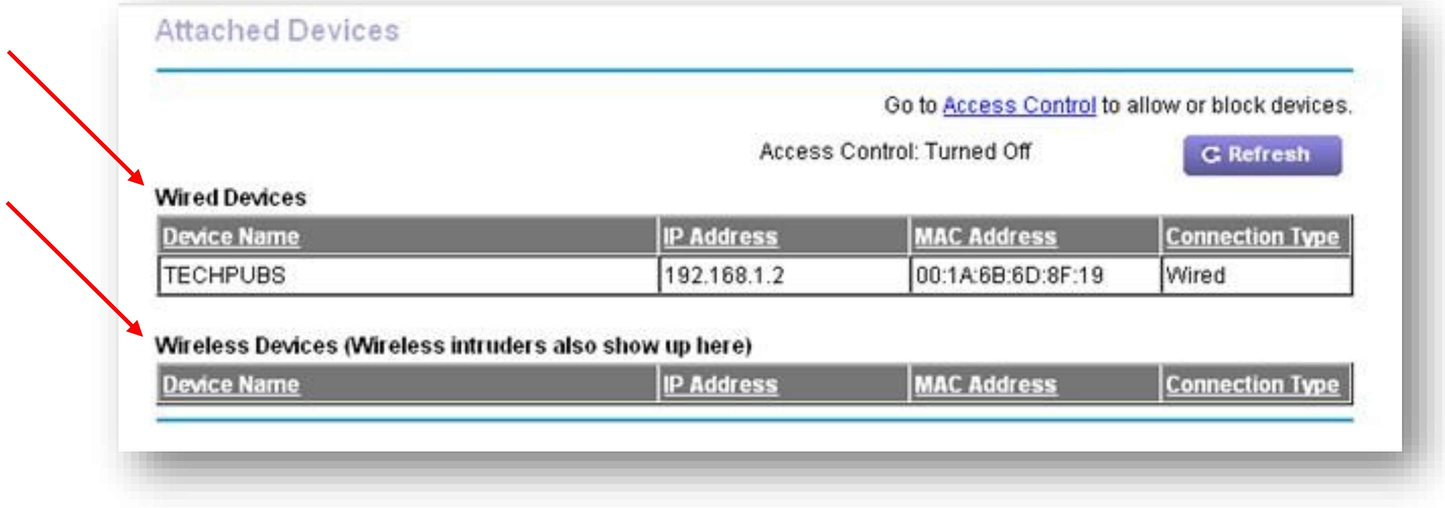
- Unauthorized access to private meetings
- Data transmission that isn't secure
- Users spreading malicious links or files on the chatroom
- Hackers potentially uploading video conferencing credentials on the dark web, putting a company's sensitive and business critical information at risk of exposure.
- Accidental sharing of sensitive footage or information

Video Conferencing Security Tips

- **Passwords** should be used for proper access control
- “**Waiting room**” feature should be leveraged such that the host can **admit or remove** attendees attempting to access the video conference
- Only use video conferencing tools that support **end-to-end encryption**
- Perform **routine updates** of all video conferencing tools to **patch vulnerabilities**
- Use **properly licensed** video conferencing tools
- Pay **extra attention** when you are **sharing** your screen
- **Mute** the microphone / **turnoff the video** when necessary

Other WFH Security Tips

Check if your home's network has been **hijacked** by unauthorized users. Start by checking if there is any unknown wired or wireless devices connected to the network



Attached Devices

Go to Access Control to allow or block devices.

Access Control: Turned Off

Wired Devices

Device Name	IP Address	MAC Address	Connection Type
TECHPUBS	192.168.1.2	00:1A:6B:6D:8F:19	Wired

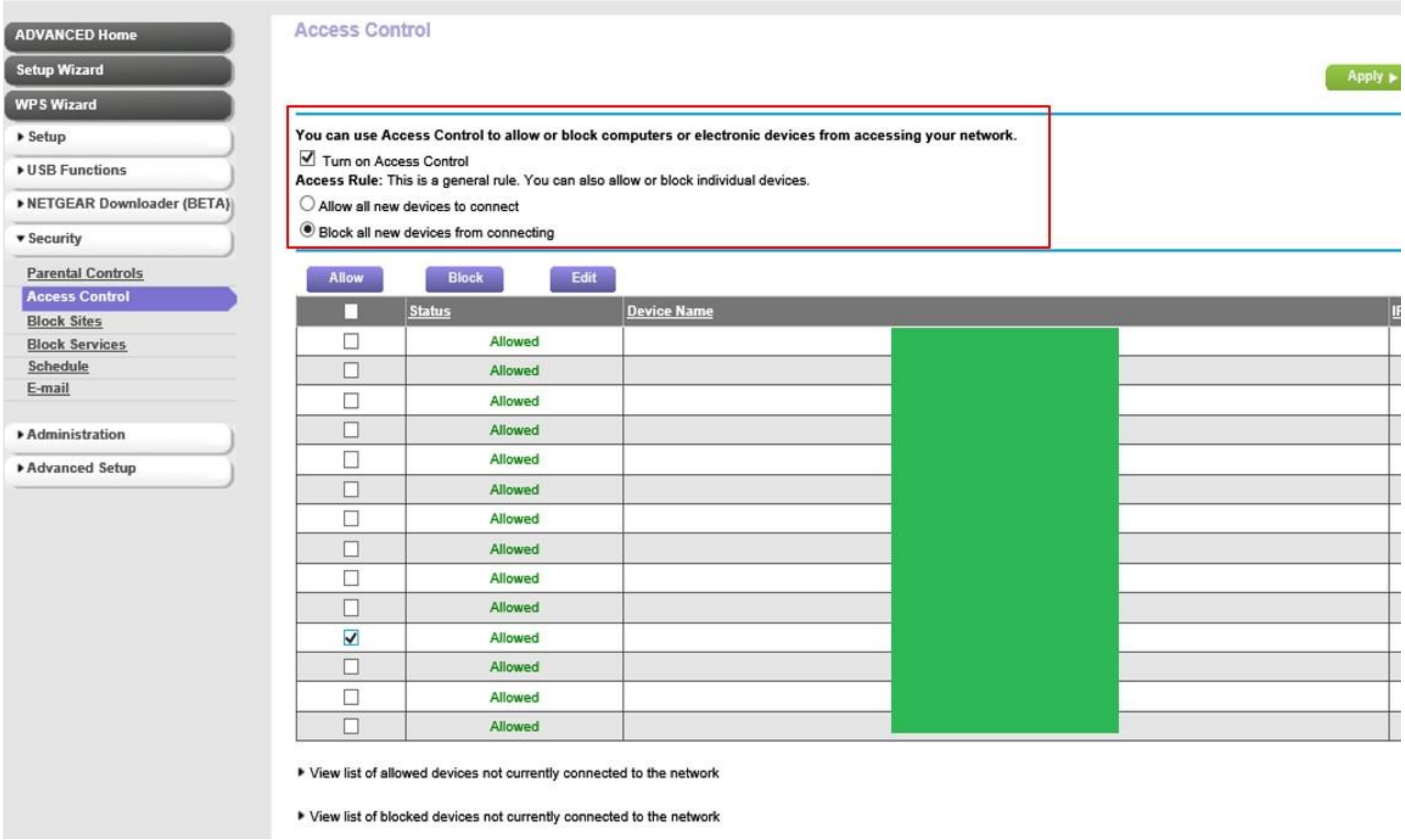
Wireless Devices (Wireless intruders also show up here)

Device Name	IP Address	MAC Address	Connection Type

Secure your router – change the **Wi-Fi password** and **network name (SSID)**

Other WFH Security Tips (Cont’d)

Use **MAC address filtering** or other **access control** to define a list of trusted devices and only allow these devices to connect to your Wi-Fi network



Access Control

You can use Access Control to allow or block computers or electronic devices from accessing your network.

☑ Turn on Access Control

Access Rule: This is a general rule. You can also allow or block individual devices.

○ Allow all new devices to connect

● Block all new devices from connecting

■	Status	Device Name	IF
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☑	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	
☐	Allowed	[redacted]	

▸ View list of allowed devices not currently connected to the network

▸ View list of blocked devices not currently connected to the network

Source: netgear – Access Control or MAC-Filtering

Other WFH Security Tips (Cont'd)

Secure your device

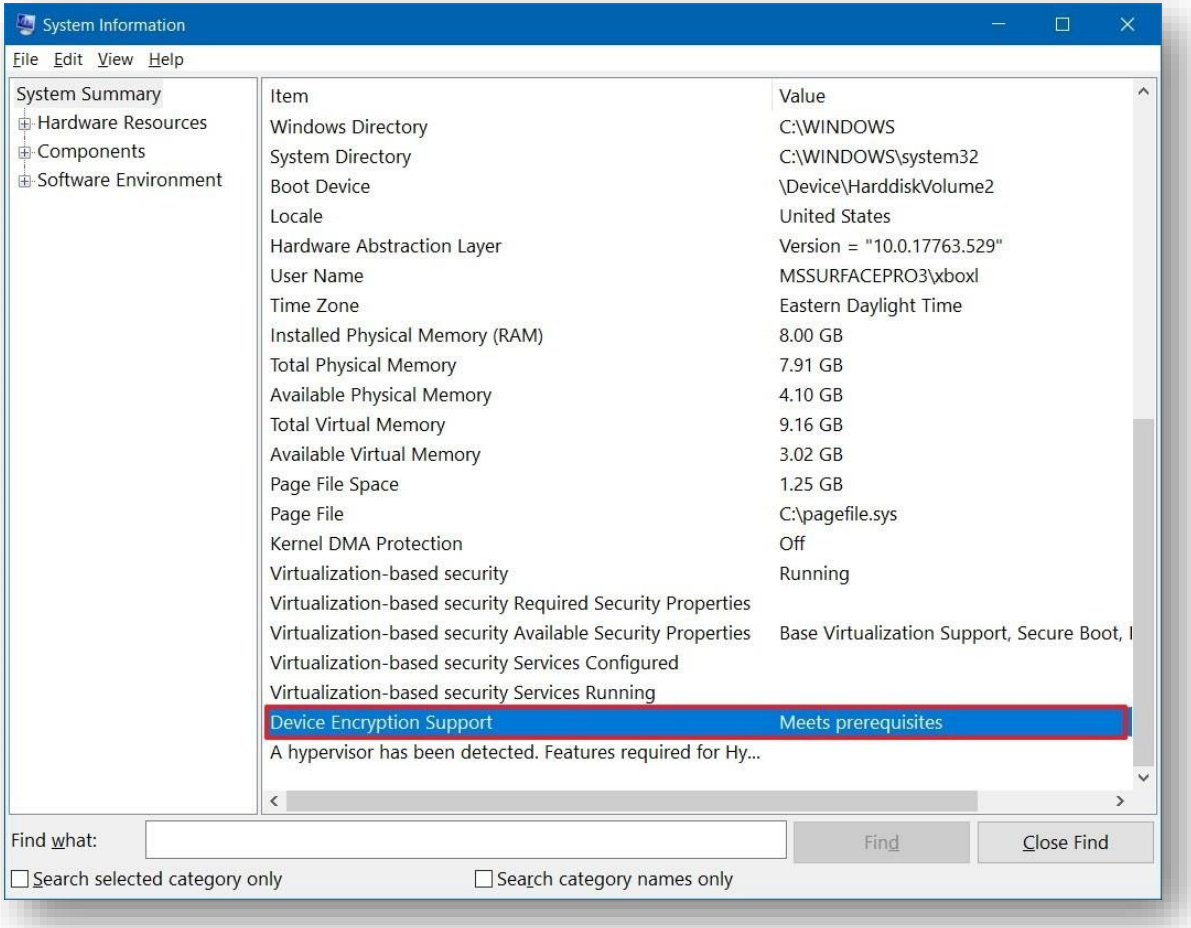
Device encryption protects your data from unauthorized access in case your device is lost or stolen.

The entire system drive will be **scrambled** upon the activation of this feature and the data can only be accessed with the correct password

Other WFH Security Tips (Cont’d)

Check whether your device meets the hardware requirements for device encryption

- Check the item “Device Encryption Support”
- If it displays “Meets prerequisites”, then your Windows devices support file encryption



Item	Value
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume2
Locale	United States
Hardware Abstraction Layer	Version = "10.0.17763.529"
User Name	MSSURFACEPRO3\xboxl
Time Zone	Eastern Daylight Time
Installed Physical Memory (RAM)	8.00 GB
Total Physical Memory	7.91 GB
Available Physical Memory	4.10 GB
Total Virtual Memory	9.16 GB
Available Virtual Memory	3.02 GB
Page File Space	1.25 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Running
Virtualization-based security Required Security Properties	
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, I
Virtualization-based security Services Configured	
Virtualization-based security Services Running	
Device Encryption Support	Meets prerequisites
A hypervisor has been detected. Features required for Hy...	

Other WFH Security Tips (Cont’d)

Use a **strong password** for your laptop or workstation

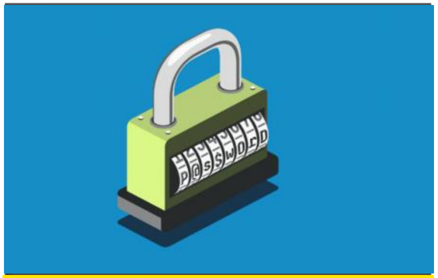
- Minimum length of **10** characters
- Alphanumeric
- Non-sequential
- Do not use default password

Lock your computer when leaving it unattended

Account lockout Policy

- Duration: **30 minutes**
- Threshold: **3 invalid attempts**

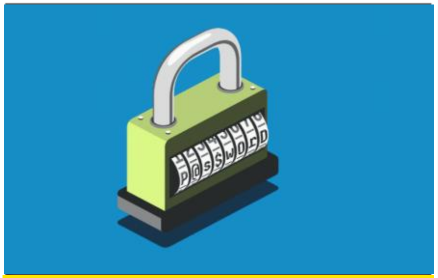
Other WFH Security Tips (Cont'd)



hacked

6 lowercase letters

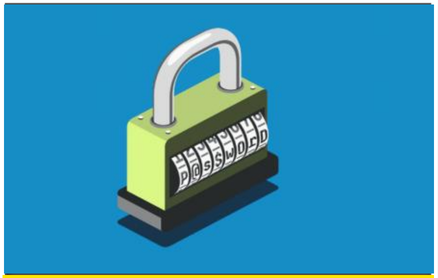
10 MINUTES



HaCKingG

7 lowercase & uppercase letters

23 DAYS



$eCureD1

8 lowercase, uppercase numbers and symbols

463 YEARS

P@ssw0rd

1234567890

12345678

Your name along with your birthday

Starwars

whatever

Letmein

123123

Unlock

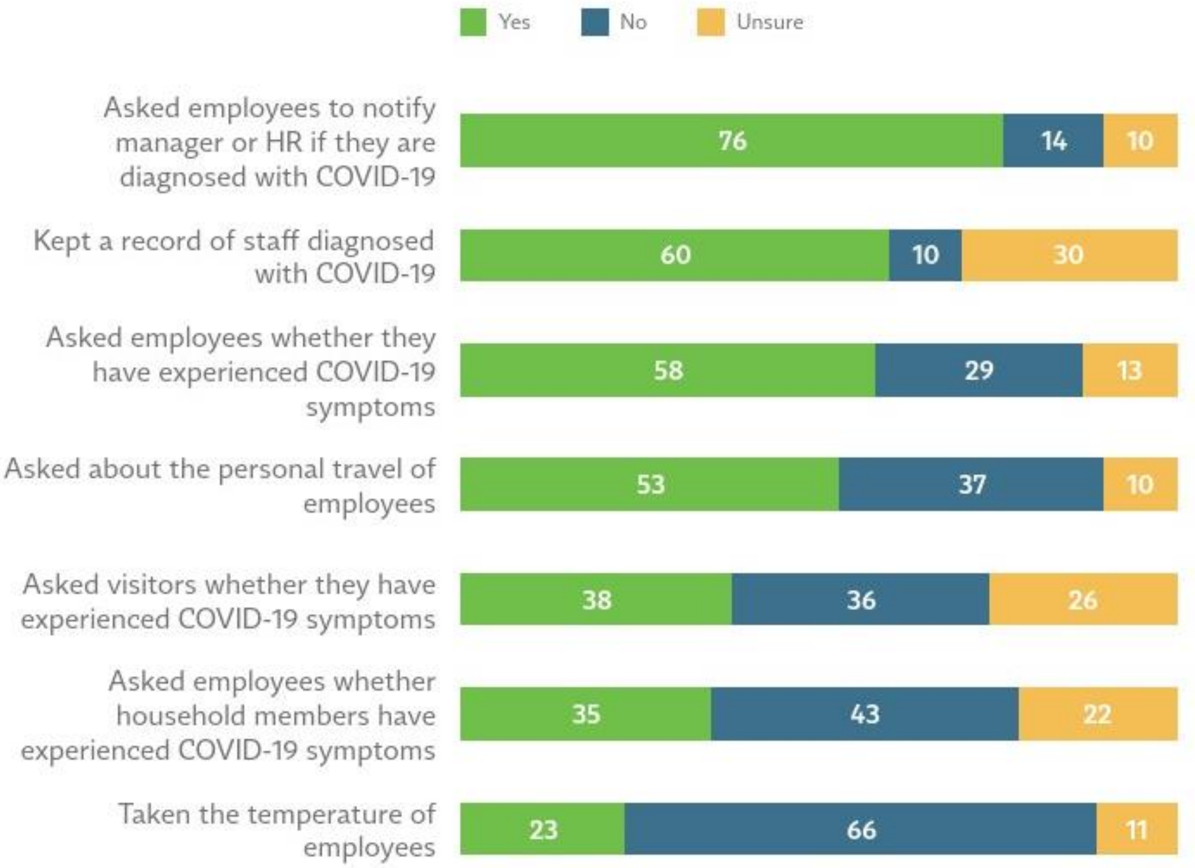
football

Other Remote Working Security Tips

- Enable Anti-virus protection on the devices
- Pay attention to the OS End-Of-Life
- Delete and manage cookies
- Disable web browser’s automatic password saving
- Disable plug-ins
- Update the web browser regularly
- VPN
- Keep work data on work computers
- Block the sight lines / install privacy filters
- Keep your device close to you
- Don’t use random thumb drives

Data Privacy – Employee Health Data

- Most organizations have collected data from employees about COVID-19 symptoms and kept diagnostic records



Source: Privacy in the Wake of COVID-19, EY and International Association of Privacy Professionals (IAPP) 2020

Data Privacy – Employee Health Data (Cont'd)

- During times like this, organizations would inevitably collect, use, process and retain additional personal data (i.e. health data) to protect the community from serious threats to public health.

Best Practice

- Avoid asking for excessive medical data
- Inform employees of the purposes of collection and class of person to whom the data may be transferred
- Ensure that the use of data remains within the scope of the intended purpose or purposes under Section 59 of the Personal Data (Privacy) Ordinance
- Conduct privacy and security reviews and data protection impact assessment
- Provide data privacy guideline to relevant personnel

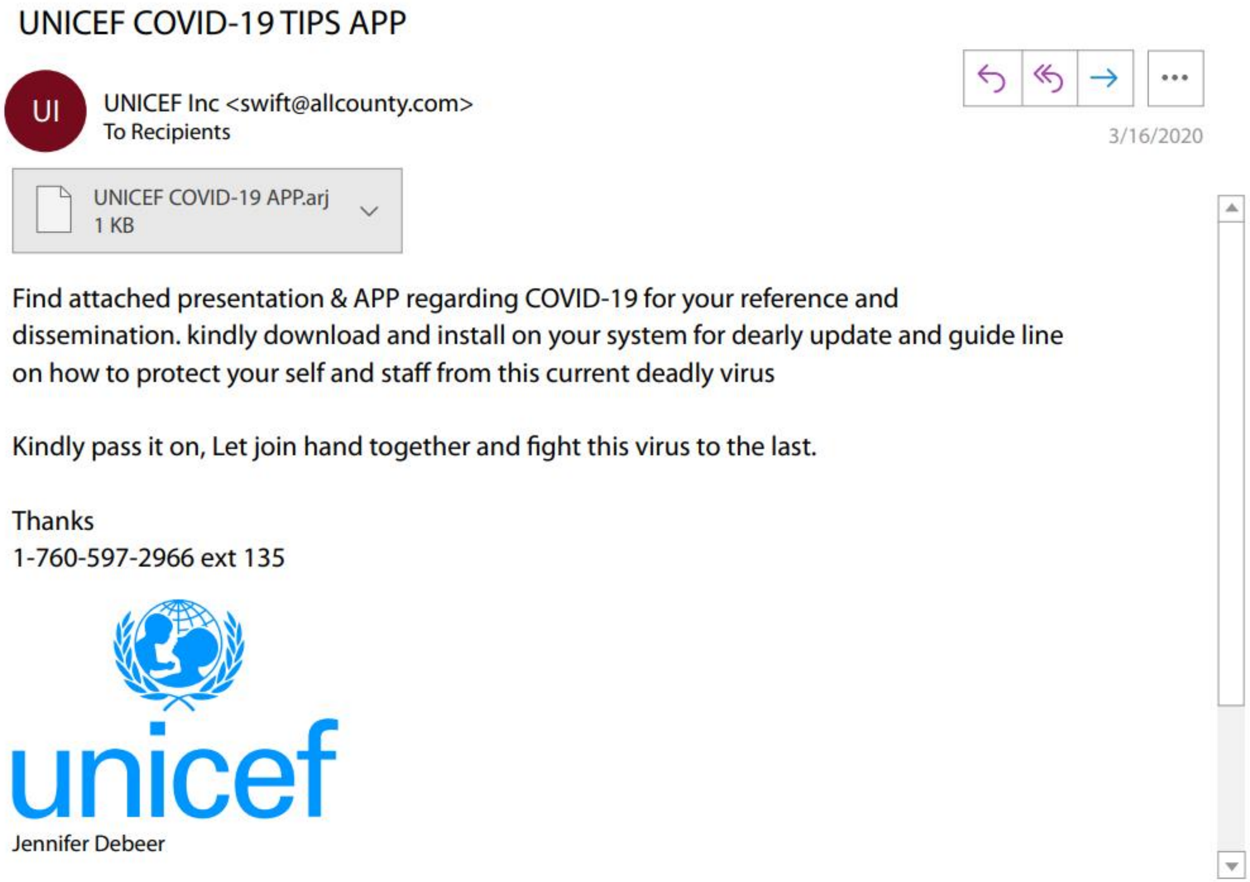
Social Engineering

- Dispersed workforce during WFH → Increased telecommunication → More exposed to phishing attacks

- Using the fear of COVID-19 as the theme for their malicious activities and spread various malware through phishing emails

- Malwares provide attackers with access to infected systems:
  - Remote desktop access
  - Remote webcam control
  - Password stealer
  - Keylogger
  - Remote shell
  - Privilege escalation
  - System manipulation

Social Engineering (Cont'd)



UNICEF COVID-19 TIPS APP

UI

UNICEF Inc <swift@allcounty.com>
To Recipients

3/16/2020

UNICEF COVID-19 APP.arj
1 KB

Find attached presentation & APP regarding COVID-19 for your reference and dissemination. kindly download and install on your system for dearly update and guide line on how to protect your self and staff from this current deadly virus

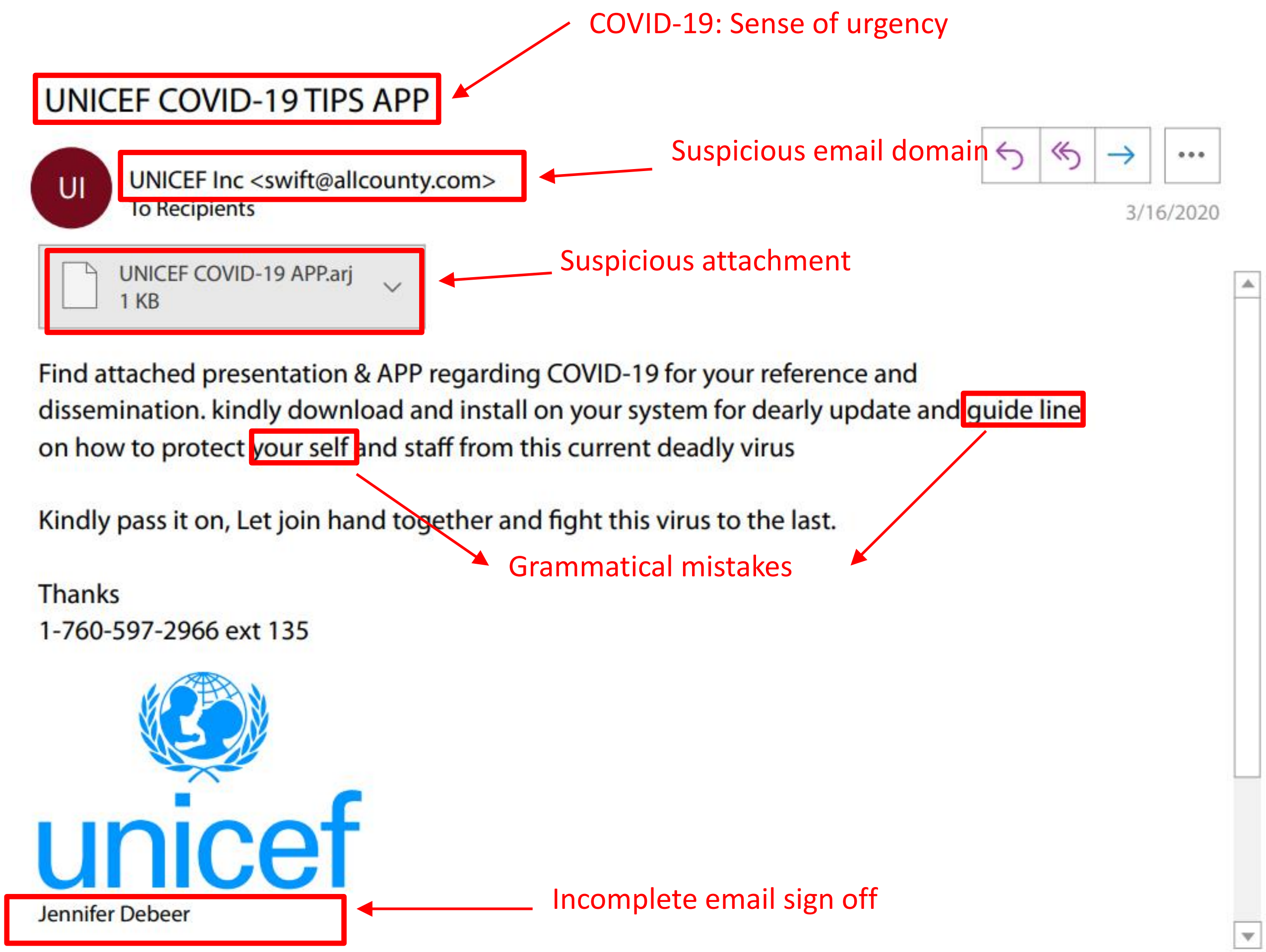
Kindly pass it on, Let join hand together and fight this virus to the last.

Thanks
1-760-597-2966 ext 135

unicef
Jennifer Debeer

Source: Enduring from home: COVID-19's impact on business security, Malwarebytes 2020

Social Engineering (Cont'd)



UNICEF COVID-19 TIPS APP

UNICEF Inc <swift@allcounty.com>
To Recipients

3/16/2020

UNICEF COVID-19 APP.arj
1 KB

Find attached presentation & APP regarding COVID-19 for your reference and dissemination. kindly download and install on your system for dearly update and guide line on how to protect your self and staff from this current deadly virus

Kindly pass it on, Let join hand together and fight this virus to the last.

Thanks
1-760-597-2966 ext 135

unicef
Jennifer Debeer

COVID-19: Sense of urgency

Suspicious email domain

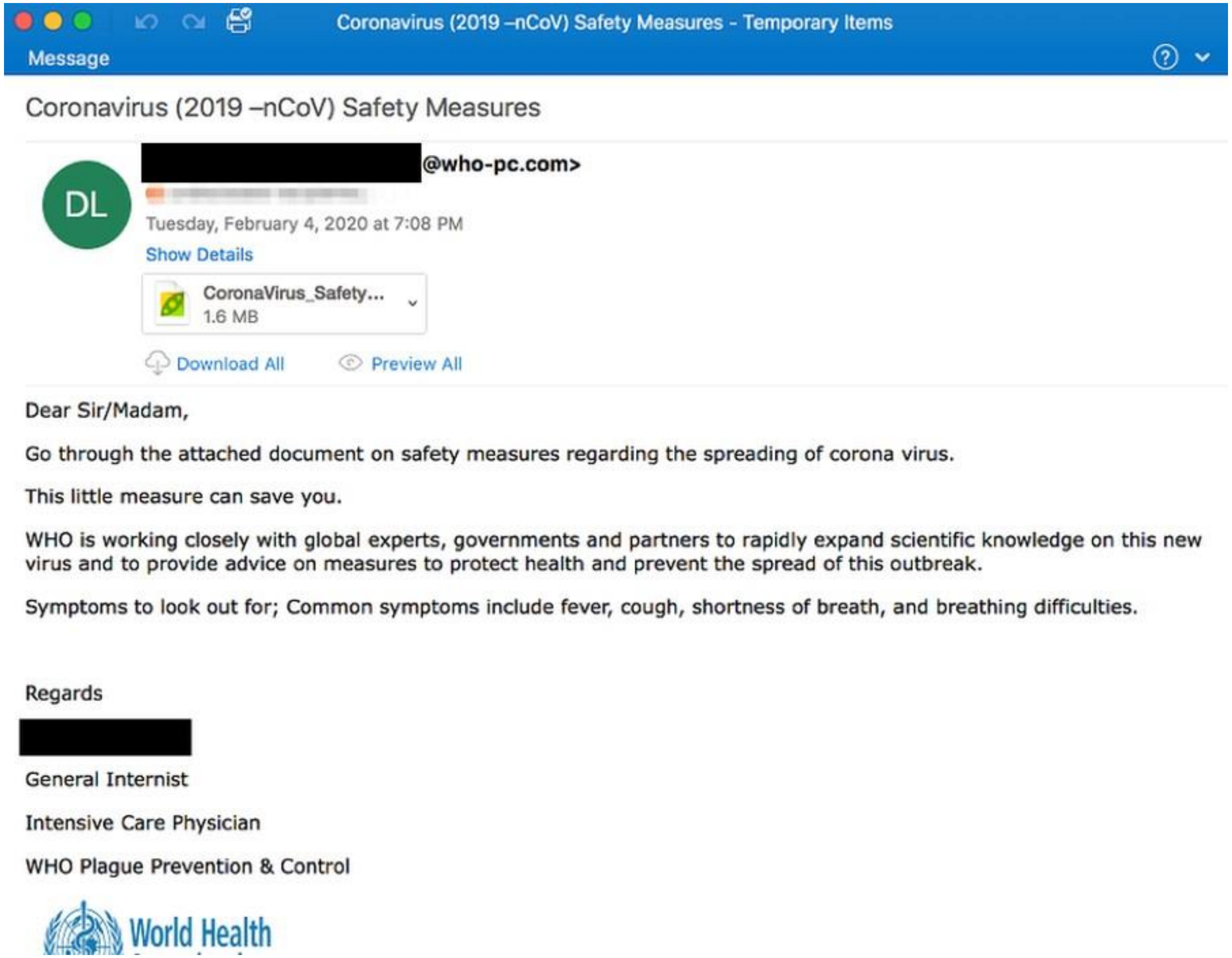
Suspicious attachment

Grammatical mistakes

Incomplete email sign off

Source: Enduring from home: COVID-19's impact on business security, Malwarebytes 2020

Social Engineering (Cont'd)



Coronavirus (2019 –nCoV) Safety Measures

DL [redacted]@who-pc.com>

[redacted]

Tuesday, February 4, 2020 at 7:08 PM

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

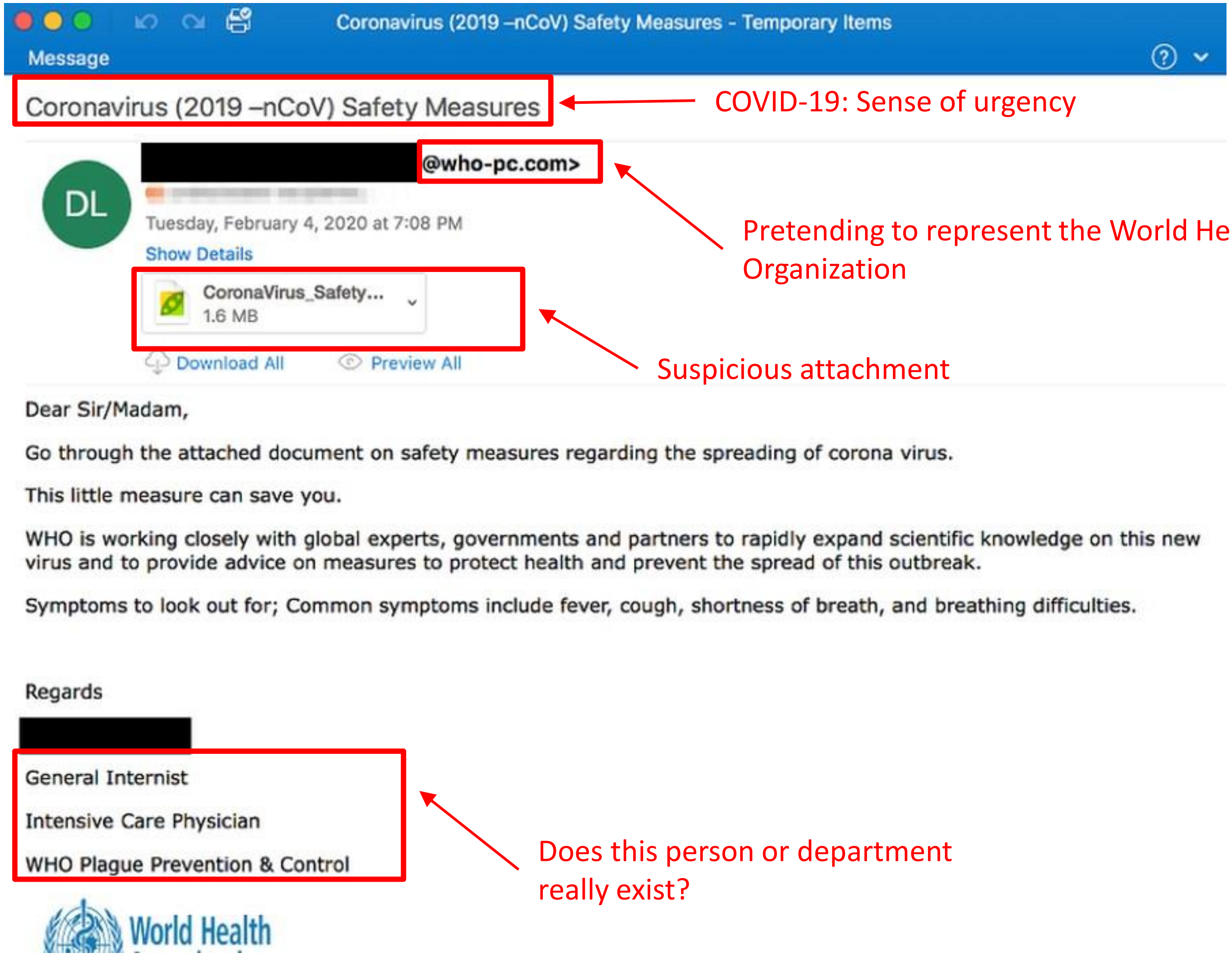
General Internist

Intensive Care Physician

WHO Plague Prevention & Control

Source: https://www.bbc.com/news/technology-51838468

Social Engineering (Cont'd)



Coronavirus (2019 –nCoV) Safety Measures

[redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

General Internist

Intensive Care Physician

WHO Plague Prevention & Control

COVID-19: Sense of urgency

Pretending to represent the World Health Organization

Suspicious attachment

Does this person or department really exist?

Source: https://www.bbc.com/news/technology-51838468

Social Engineering (Cont'd)

- **Spelling errors** (e.g. "pessward"), lack of punctuation or poor grammar.
- **Hyperlinked URL** differs from the title name displayed, the link is shortened.
- **Sense of urgency.** Phishing emails will usually use a language that demands for immediate actions.
- **Personally Identifiable Information.** Requests for personal information like user credential, financial transactions.
- **Suspicious attachment.** Request to open attachments to check and verify data.
- **Forged sender identity.** The email address domain and email sign off do not match with the claimed identity.

Crisis Management

C.A.R.E

- **C**ontaining the data breach to prevent further compromise of personal data
- **A**ssessing the data breach by gathering the facts and evaluating the risks, including the harm to affected individuals. Where assessed to be necessary, continuing efforts should be made to prevent further harm even as the organization proceeds to implement full remedial action.
- **R**eporting the data breach to all affected individuals and the PCPD, if necessary.
- **E**valuating the organization's response to the data breach incident and consider the actions which can be taken to prevent future data breaches. Remediation efforts may continue to take place at this stage.

A chain is only as strong as its weakest link

Thomas Reid, 1786

4 The System and Practices in the University

The System and Practices in the University

- Information Security and Data Management Policy: https://isdm.hku.hk/

- The Privacy Policy Statement: http://www.hku.hk/privacy_policy/

- Code of Practice (revised version 2019): https://intraweb.hku.hk/reserved_1/gsabc/pdpo_cop.pdf (portable storage devices, incident handling / reporting and other guidelines)

The System and Practices in the University

- Data Collection Statement
- Statutory Data Access / Correction Request Process
- Central Compliance Team (compliance/monitoring)
- University Data Protection Officer and Personal Data Protection Coordinators
- Information Technology Services (advice / security measures / guidelines / training information): http://www.its.hku.hk/services/training/infosec/personal-data-protection

The University of Hong Kong

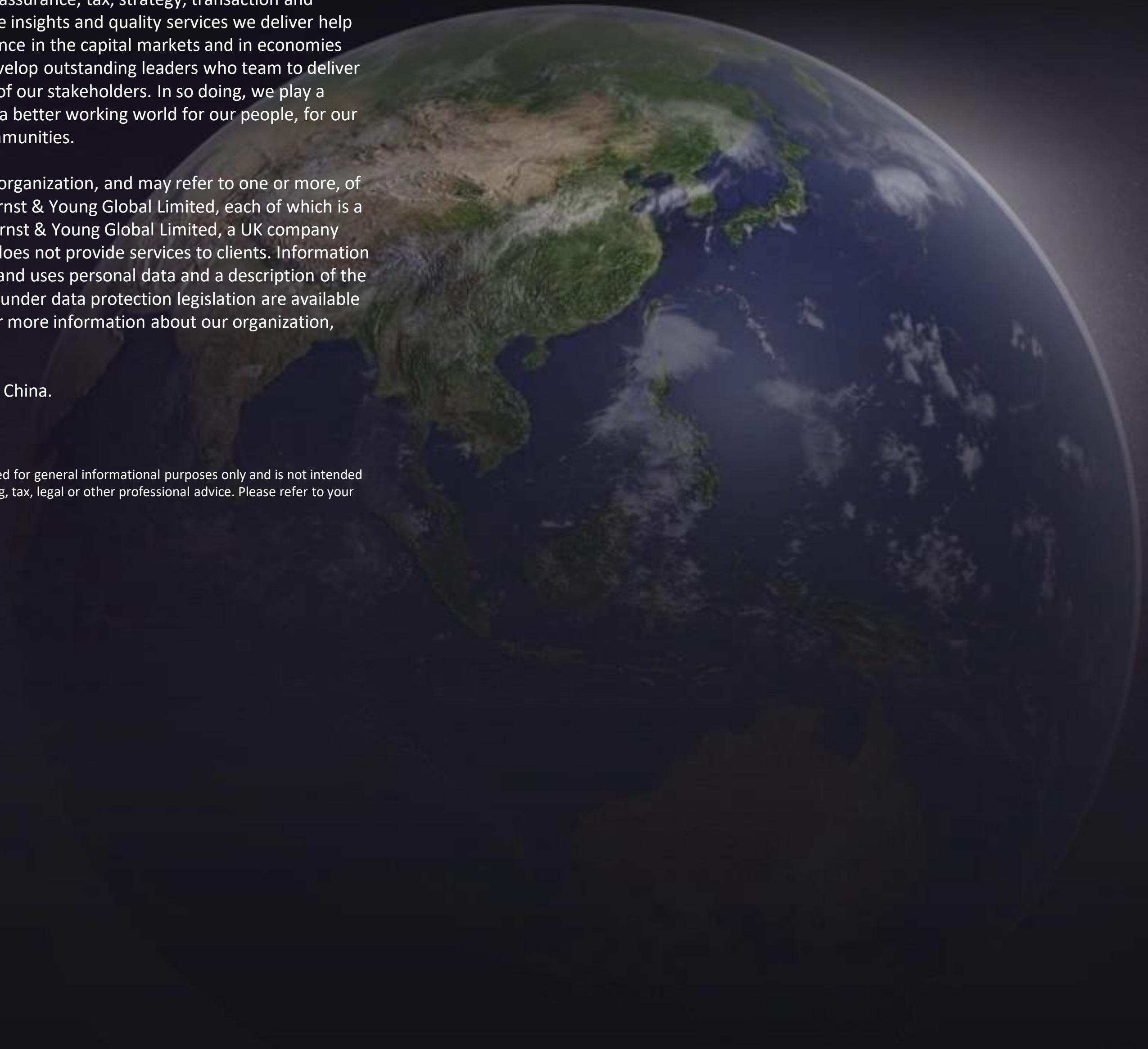
The System and Practices in the University

The Public Expectation

Awareness and Education

GOOD PRACTICE

The University of Hong Kong



EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/china