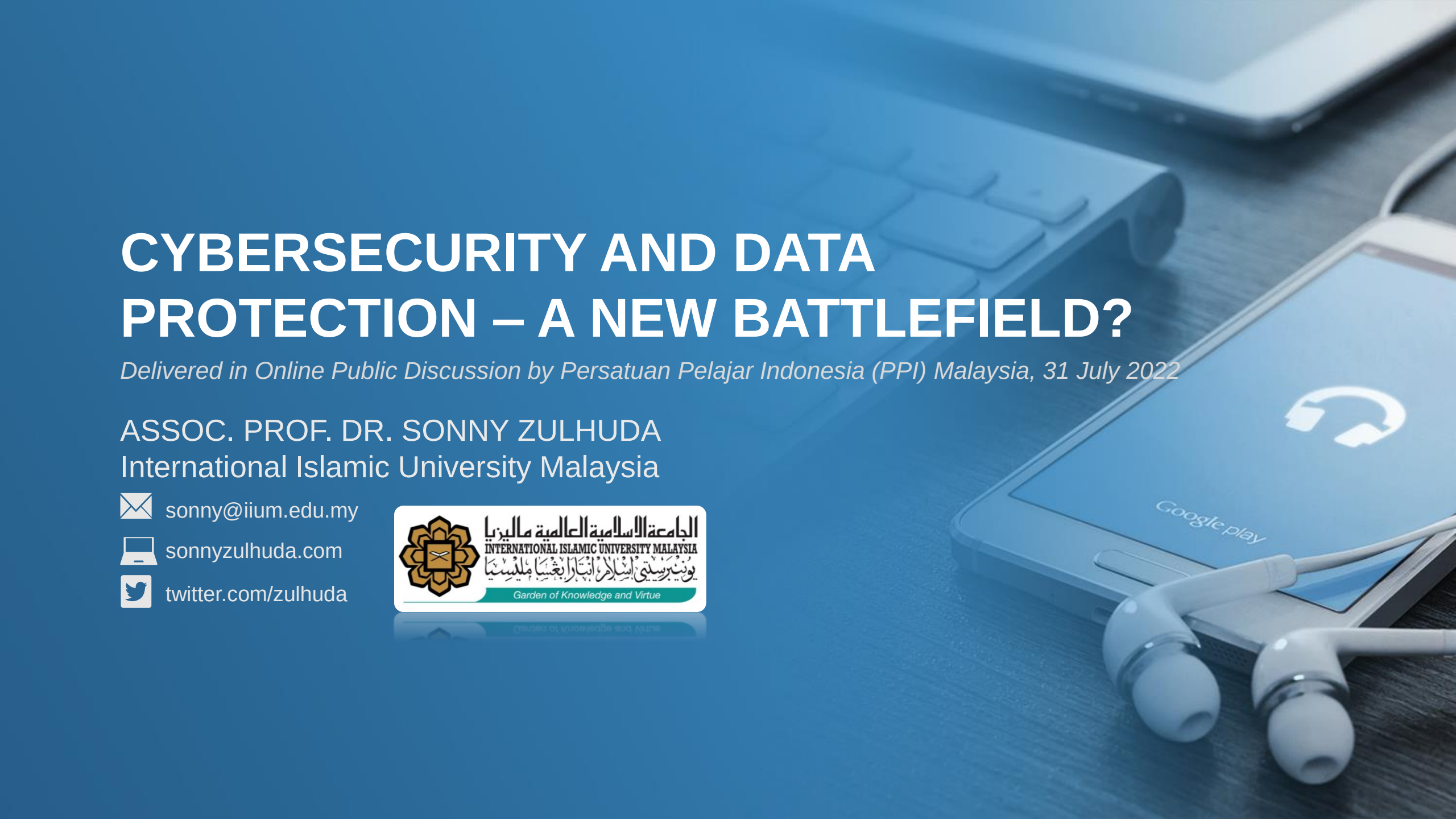
CYBERSECURITY AND DATA PROTECTION – A NEW BATTLEFIELD?

Delivered in Online Public Discussion by Persatuan Pelajar Indonesia (PPI) Malaysia, 31 July 2022

ASSOC. PROF. DR. SONNY ZULHUDA
International Islamic University Malaysia

sonny@iium.edu.my
sonnyzulhuda.com
twitter.com/zulhuda



Key Points

01 Cyberspace: Reality Check

02 Understanding Cyber Security & Data Protection

03 A New Battlefield?

04 Lessons Learned

CYBERSPACE

REALITY CHECK

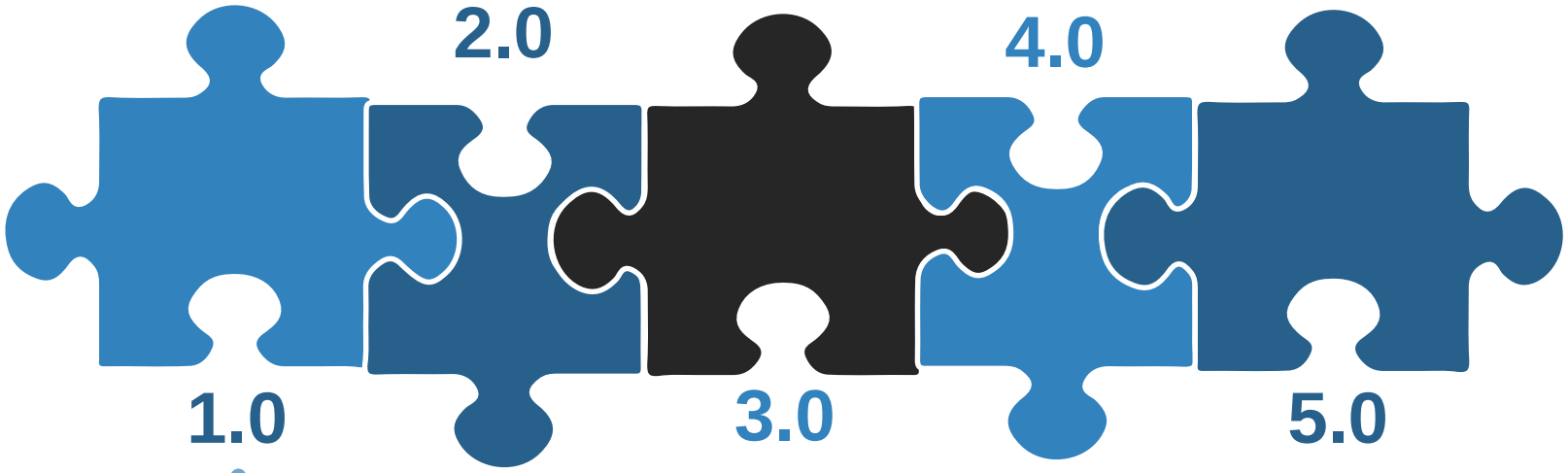
Society 5.0 >> Cyber Society

FARMING SOCIETY

Farming, planting tools
Agricultural product

INFORMATION SOCIETY

Computer, satellite
internet



HUNTING SOCIETY

Stone, metal weapons
Pure natural sources

INDUSTRIAL SOCIETY

Electricity, steam locomotive
Printing machine

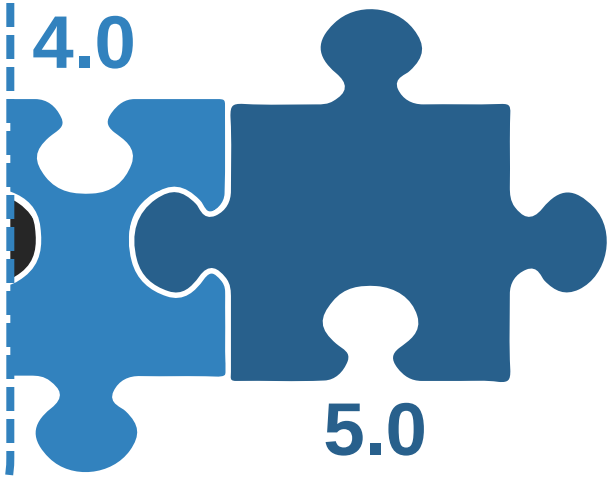
SUPERSMART SOCIETY

Big data, IOT, Artificial
Intelligence

Society 5.0 >> Cyber Society

The Characteristics of Cyber Society:

- ✓ Diminishing border
- ✓ Time-zone doesn't matter, but timeline does
- ✓ The illusion of lawlessness
- ✓ Abundance of information – confusion between data and noise.
- ✓ Gadgets change, but data stays
- ✓ Rise of digital assets
- ✓ Digital natives take over
- ✓ Traditional authority being challenged



INFORMATION SOCIETY

Computer, satellite
internet

HUNTING SOCIETY

Stone, metal weapons
Pure natural sources

INDUSTRIAL SOCIETY

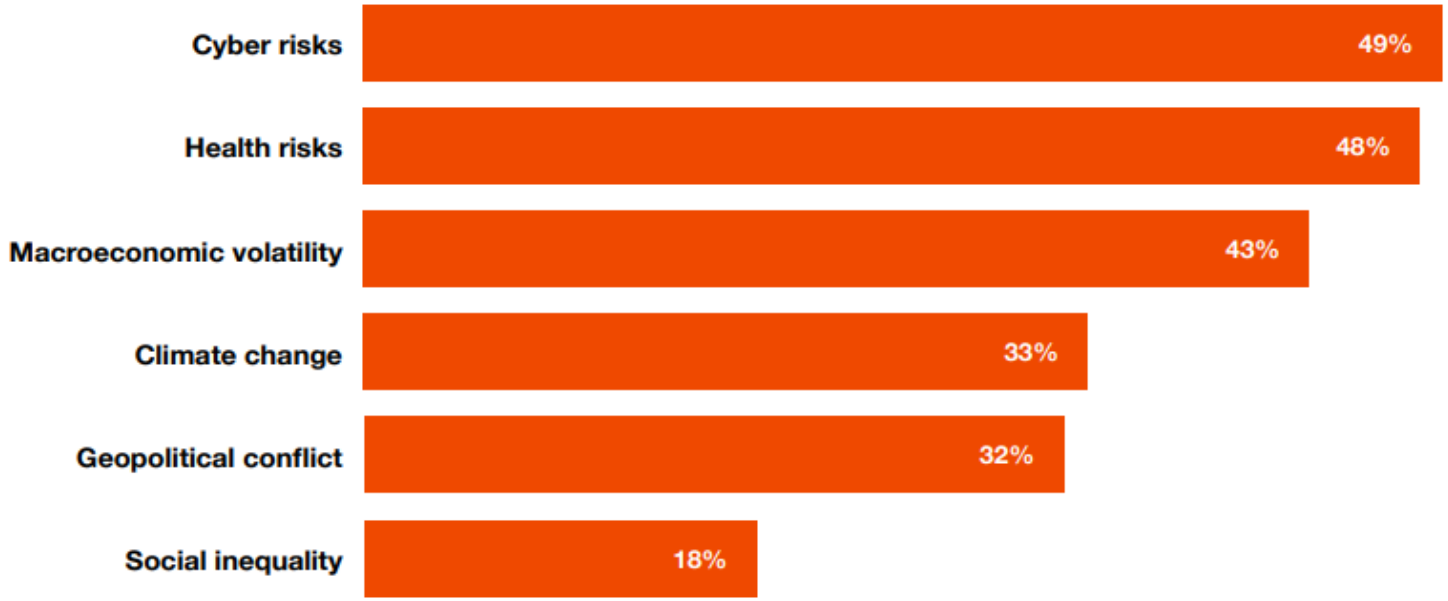
Electricity, steam locomotive
Printing machine

SUPERSMART SOCIETY

Big data, IOT, Artificial
Intelligence

The threats that global CEOs are most worried about…

CEOs rank cyber risks as the top threat to growth, with health risks close behind



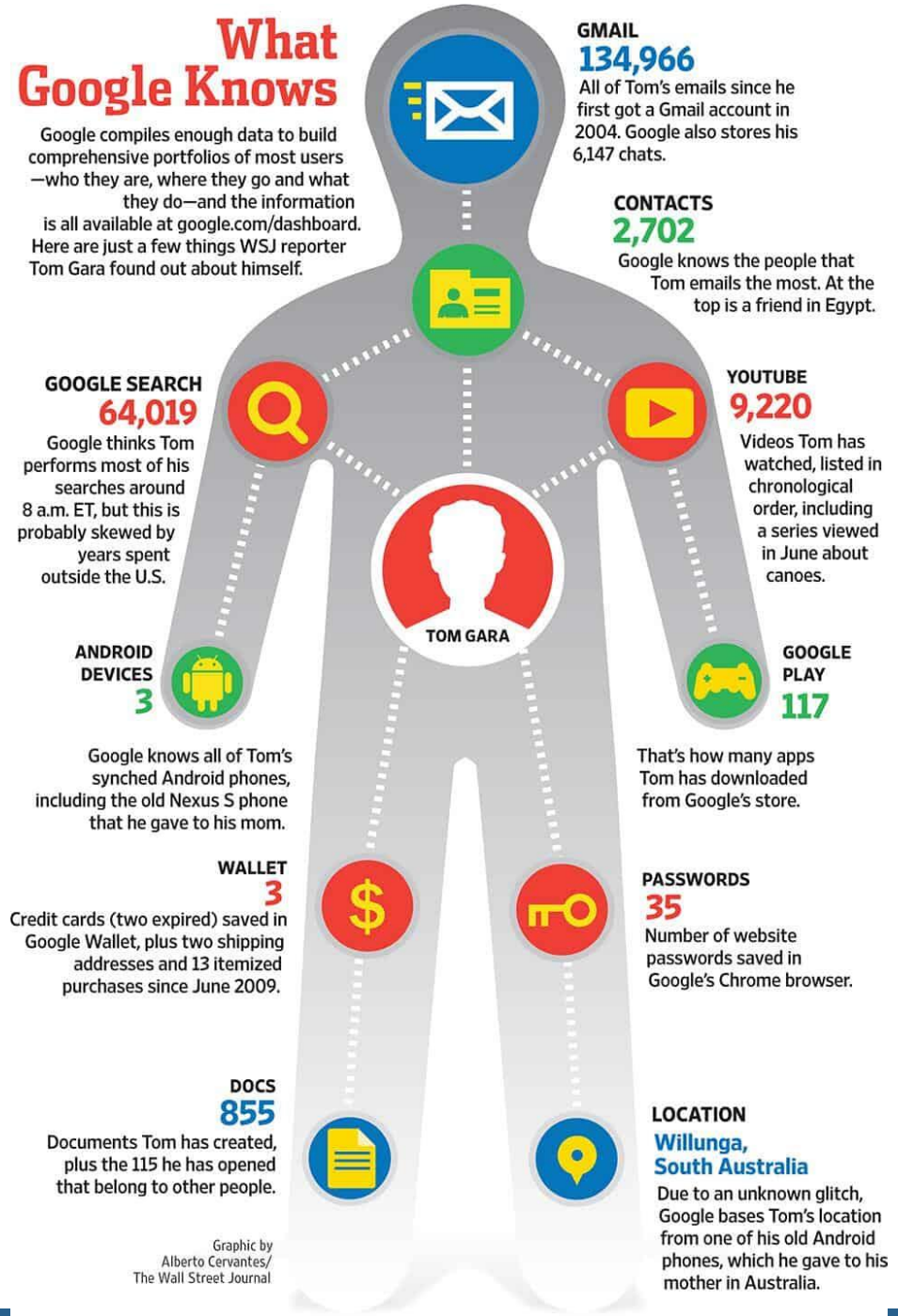
Source: PwC 25th Annual Global CEO Survey

Why Cyber Risks?

- **Industry 4.0 – Where informatisation embraces datafication and transforms into automatisation**
- **Post-pandemic World – Efficiency, Work from Anywhere, Cloud as Service**
- **Inter-dependence on public Information Infrastructure, e.g. telecom, data storage, health system, transport system, government**
- **Increasing threat of attack to the digital assets (Cybercrimes, cyberterrorism, etc.)**

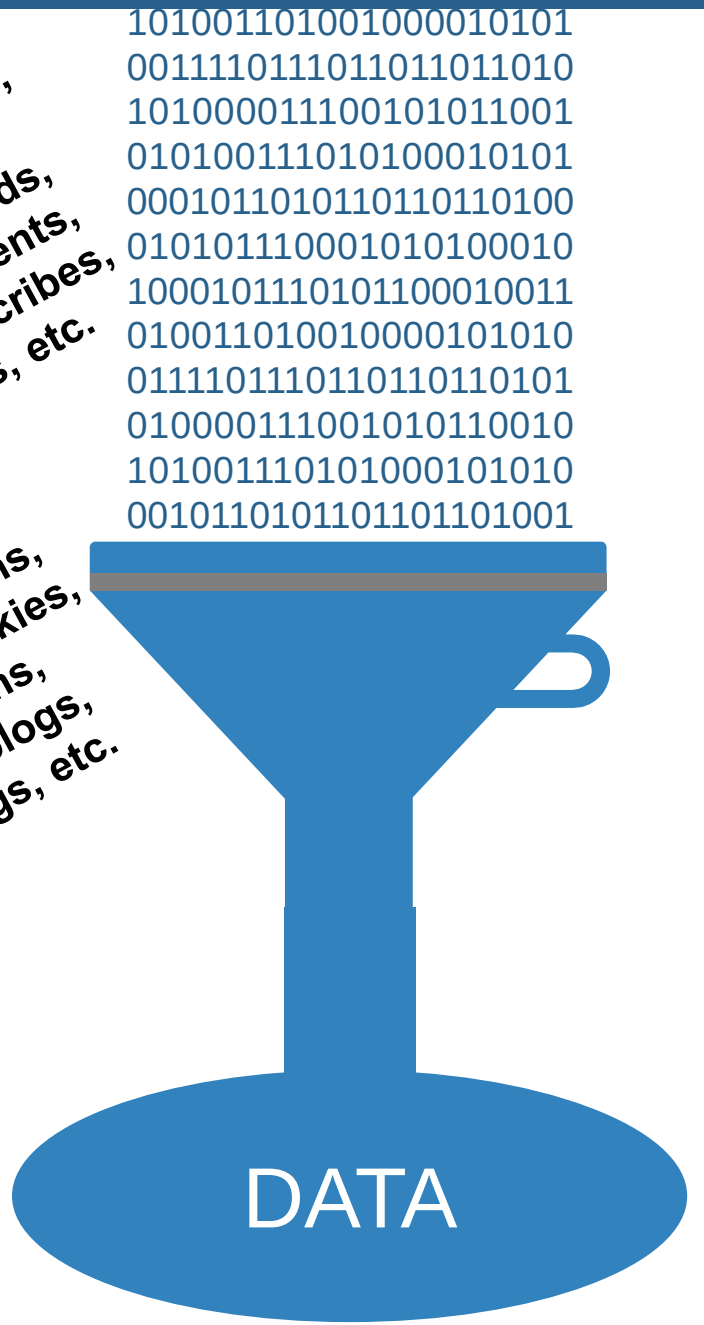
Informatisation –> Digitalisation –> Datafication!

DATAFICATION

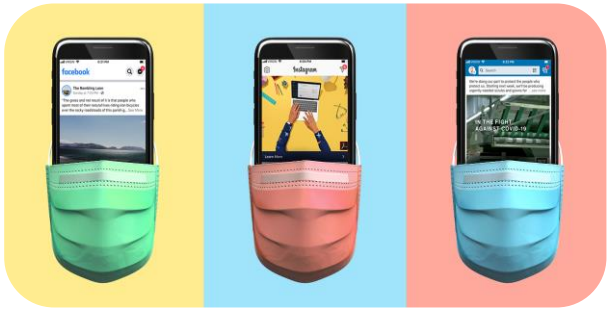


Social media posts, likes, loves, mentions, threads, shares, comments, follows, subscribes, emoticons, etc.

Travels, locations, wearables, cookies, transactions, pictures, blogs, vlogs, logs, etc.



Prominent Threats and Risks of Cyber Security



Personal data exploitation through **illicit collections** via online services (eg P2P lending), Apps, etc;

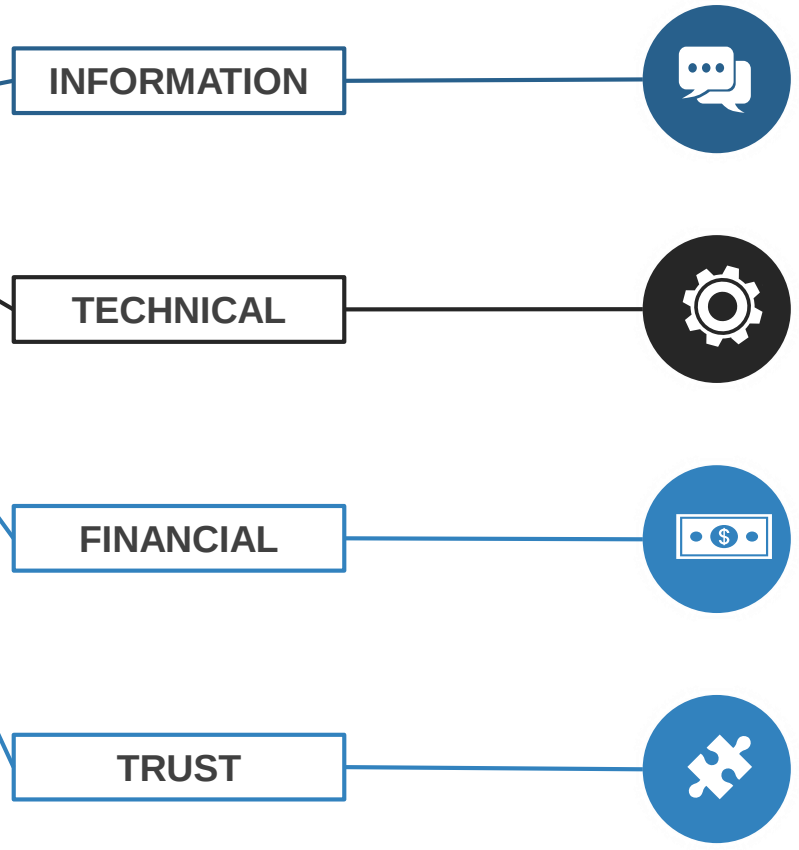
Scam via fake accounts begging for donation, fake charity drives, fake emergencies etc.

Misinformation: citizen journalism with unaccountable stories – a test-bed for phishing attacks.

Unsecured online platforms prone to personal data breaches (online shopping, online meeting, social media, etc).

The rise of public **surveillance** and Private data collection?

Post-Pandemic Cyber Vulnerabilities



People tend to **rush collecting** information about the Pandemic, click on links and web pages, spreading the information with **poor exercise of fact-checking**

People work on **official documents** using home-based computers, with **inadequate security protection** and support as they have in office.

Reduced mobility, **losing jobs**, scarcity of earning opportunities, etc. creates financially challenged society, who would **turn into shortcuts (crimes, etc)**.

Wide and fast **adoption of mobile Apps** for social networking, e-shopping, e-meeting, e-learning and cloud services, but with poor **security and privacy measures** or policies

Post-Pandemic Cyber Vulnerabilities

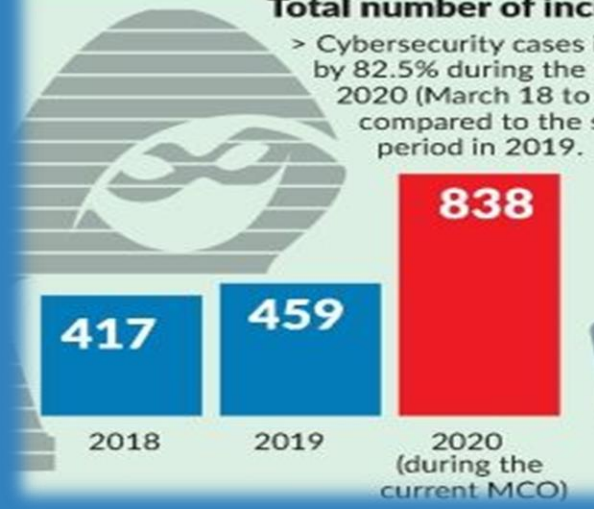
PANDEMIC

COVID-19

Beware of cyberattacks!

Total number of incidents

> Cybersecurity cases increased by 82.5% during the MCO 2020 (March 18 to April 7) compared to the same period in 2019.



Tips to stay safe online

Working from home

> Update all systems including Virtual Private Networks (VPN) and devices with the latest security patches
> Alert employees about phishing attempts.
> Avoid logging in to your work environment using public Internet Wi-Fi. Connect through your home or mobile network data.
> Enable Multi Factor tication

Covid-19 scams

> Always verify information from emails, text messages and social media posts about Covid-19.
> Do not share personal or financial information in emails
> Do not click on suspicious links provided to you on Covid-19, verify with the sender or agencies that can help.
> Use legitimate, government websites for up-to-date, fact-based information

Video teleconferencing apps

> Use the latest version of apps and security software
> Only download software from its official website or app store.
> Never share confidential information during a meeting
> Enable non-recordable videos and audio, and limit file sharing.
> If something is suspicious, log out.
> If you lose your computer or mobile phone, log out from all clients immediately and change your login password.
> Do not share or publish the confer
> Log out from the app after a meeting.

Source: CyberSecurity Malaysia

• Post-Pandemic Cyber Vulnerabilities

PERFORMANCE IMPROVEMENT PARTNERS
an ERIE STREET company

The United States declares its first case of COVID-19, cyber attacks go up **48%**

30TH JANUARY

Multiple states in the US declare a public emergency; cyber attacks go up **64%**

» 29TH FEBRUARY

The country of Italy goes into lockdown, attacks go up **28%**

» 8TH MARCH

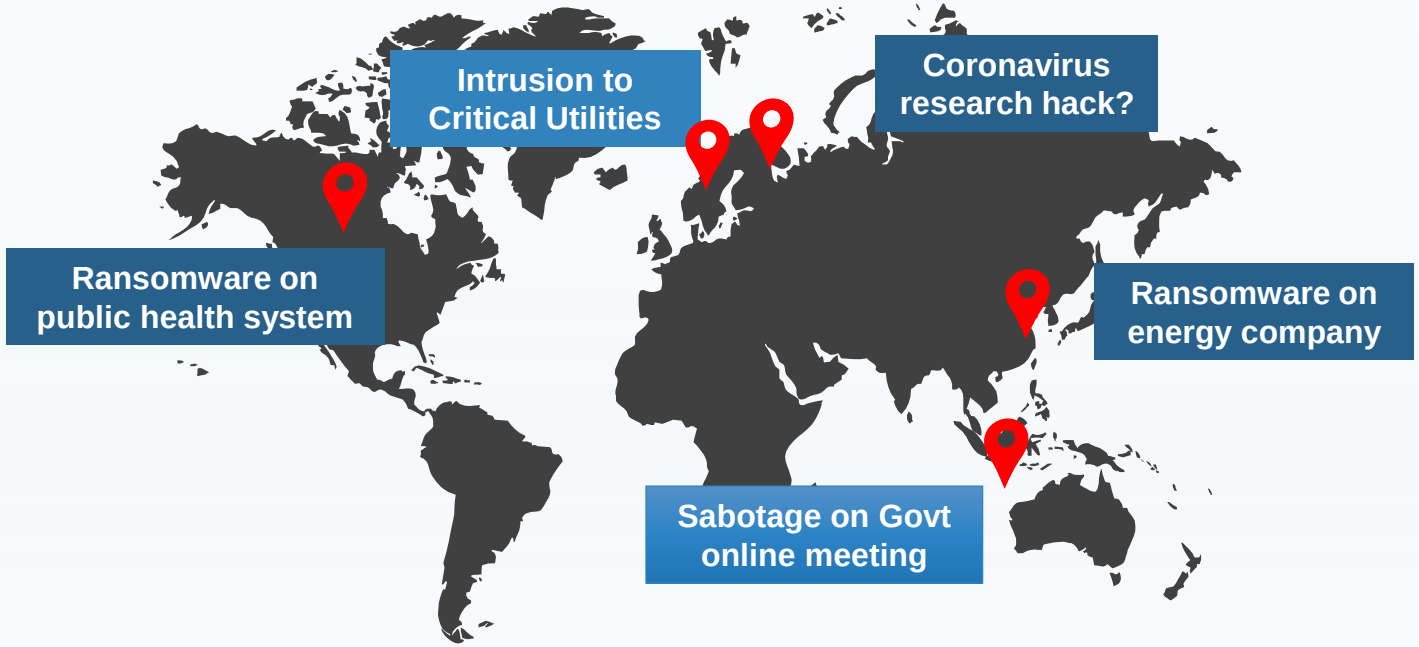
The World Health Organization declares COVID-19 a pandemic, cyber attacks go up **22%**

» 11TH MARCH

Data source: Computer Weekly via Carbon Black

Exploitation of Cyber Information Infrastructure (CIIP)

Post-Pandemic Cyber Vulnerabilities



Terrorists and cybercriminals are always interested to exploit cyberspace vulnerabilities. The activity of cyber terrorism does not relax during Covid-19. Several cyber attacks do target a critical information infrastructure (CII), a traditional target for cyber terrorism.

Cybersecurity A New Battlefield?

Russia-linked cyberattacks on Ukraine: A timeline

Cyber incidents are playing a central role in the Russia-Ukraine conflict. Here's how events are unfolding along with unanswered questions.

TECH POLICY

Dozens of Thai activists and supporters hacked by NSO Group's Pegasus

By Joseph Menn

July 17, 2022 at 11:00 p.m. EDT

REUTERS

U.S. Republicans worry China might use TikTok to meddle in election

Alexandra Alper

July 29, 2020 · 2 min read

Quote Lookup

HEALTH TECH

Healthcare data breach costs reach record high at $10M per attack: IBM report

By **Heather Landi** • Jul 27, 2022 10:27am

Cyber security experts raise alarm over possible data breach involving millions of Malaysians

By Adib Povera - June 12, 2022 @ 5:37pm

+ 48

Recent Global Data Breach Cases

The Highest EU-based Fines (2020-2021)

AMAZON

- $877 million
- Offence? Cookie consent

WHATSAPP

- $255 million
- Failed to properly explain its data processing practices in its privacy notice

GOOGLE

- $56.6 million
- Privacy notice & consent for personalized advertising, etc

H&M

- $41 million
- Monitoring of employees

TIM

- $31.5 million
- Series of violations accumulated over the last several years.

Recent Data Breach Incidents in Indonesia*

BPJS Kesehatan
Badan Penyelenggara Jaminan Sosial

komisi pemilihan umum

eHAC Indonesia
Health Quarantine MoH Indonesia

Lazada

facebook
Indonesia

BRIlife

tokopedia

bukalapak

BHINNEKA

RedDoorz

kreditplus
PT. KB FINANSIA MULTI FINANCE

https://nasional.kompas.com/read/2021/09/03/18445501/deretan-kasus-kebocoran-data-pribadi-dalam-dua-tahun-terakhir

Fintech-related Data Breach

CYBERSECURITY

ARE WE (LEGALLY) READY?

A New Battlefield for the Indonesian Authority

Pasal 40 UU No. 11/2008 Ttg ITE

Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan peraturan perundang-undangan.

Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundangundangan.

Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.

Dalam melakukan pencegahan s6lagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum.

Pemerintah menetapkan instansi atau institusi yang memiliki . data elektronik strategis yang wajib dilindungi.

Are We (Legally) Ready?

1999

- UU No. 36/1999 Ttg Telekomunikasi

2008

- UU No. 11/2008 Ttg ITE

2016

- UU No. 19/2016 Ttg Perubahan ITE

2019

- Perpres No. 39/2019 Ttg Satu Data indonesia

2021

- Perpres No. 28/2021 Ttg Badan Siber dan Sandi Negara

2022(?)

- RUU Ttg Pelindungan Data Pribadi

Meanwhile in Malaysia….

1997

- Computer Crimes Act 1997
- Digital Signature Act 1997

1998

- Communications and Multimedia Act 1998

2006

- Electronic Commerce Act 2006

2007

- Electronic Government Activities Act 2007

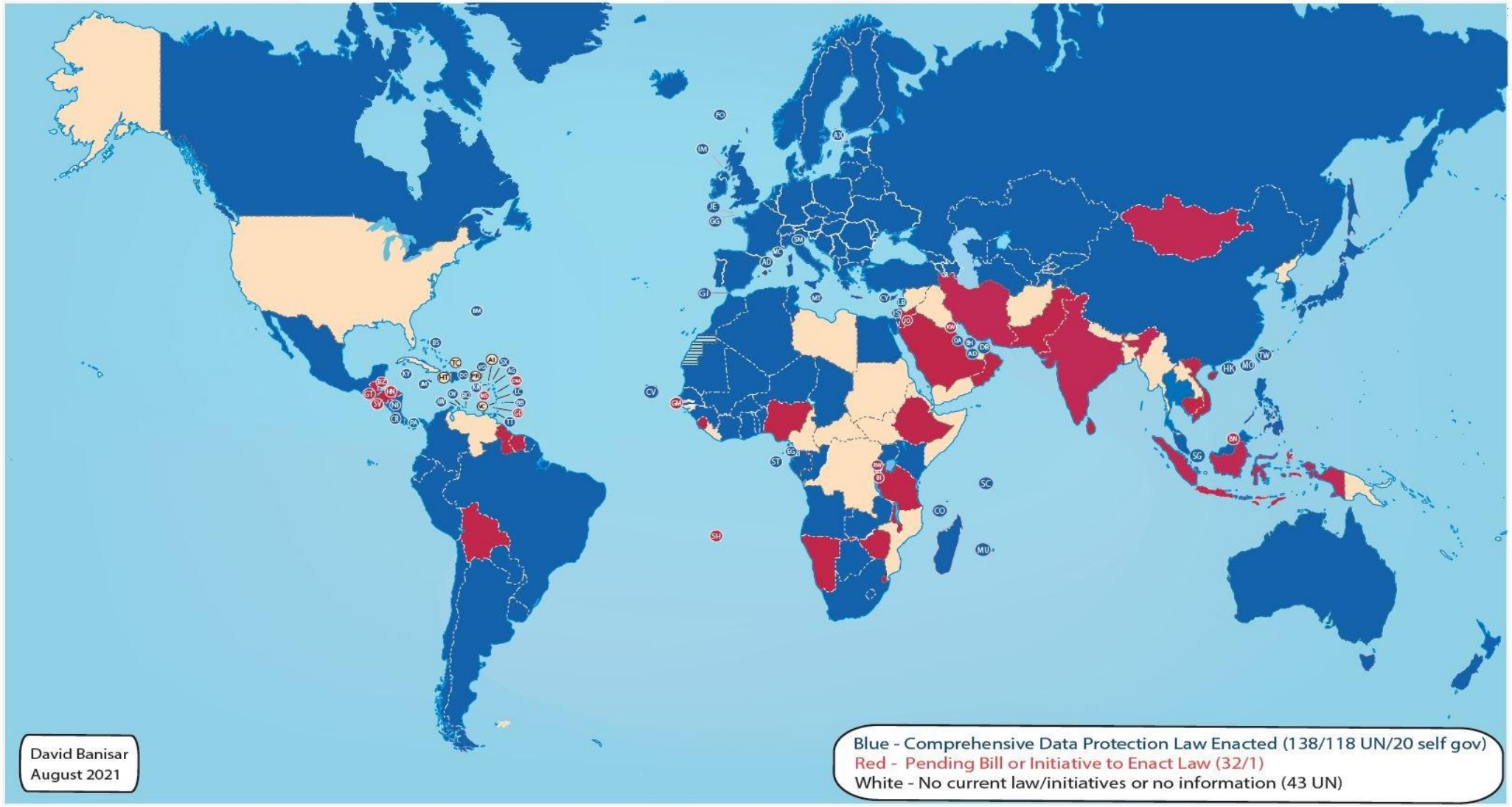
2010

- Personal Data Protection Act 2010

2022(?)

- Study on the Draft Law on the Cyber Security Act

National Comprehensive Data Protection/Privacy Laws and Bills 2021



A New Push for Indonesian Government

G-20 Summit 2019: Osaka Track on Data Free Flow with Trust (DFFT)

G-20 Summit 2022: What will the Host say about Data Protection?

The Future for Our Cyber Security and Data Protection

- Internationally accepted benchmark?
- 3C: Clarity, Comprehensive, Concerted Law?
- Regulate = Balance between carrot & stick?
- Effective Mechanism of Enforcement?

Past


Data Pribadi Dijual Bebas

Present

Future

- ✔Digital Sovereignty
- ✔Transparency (Good Governance)
- ✔Sustainable Business
- ✔Sustainable Innovation

LESSON LEARNED

KEY TAKEAWAYS

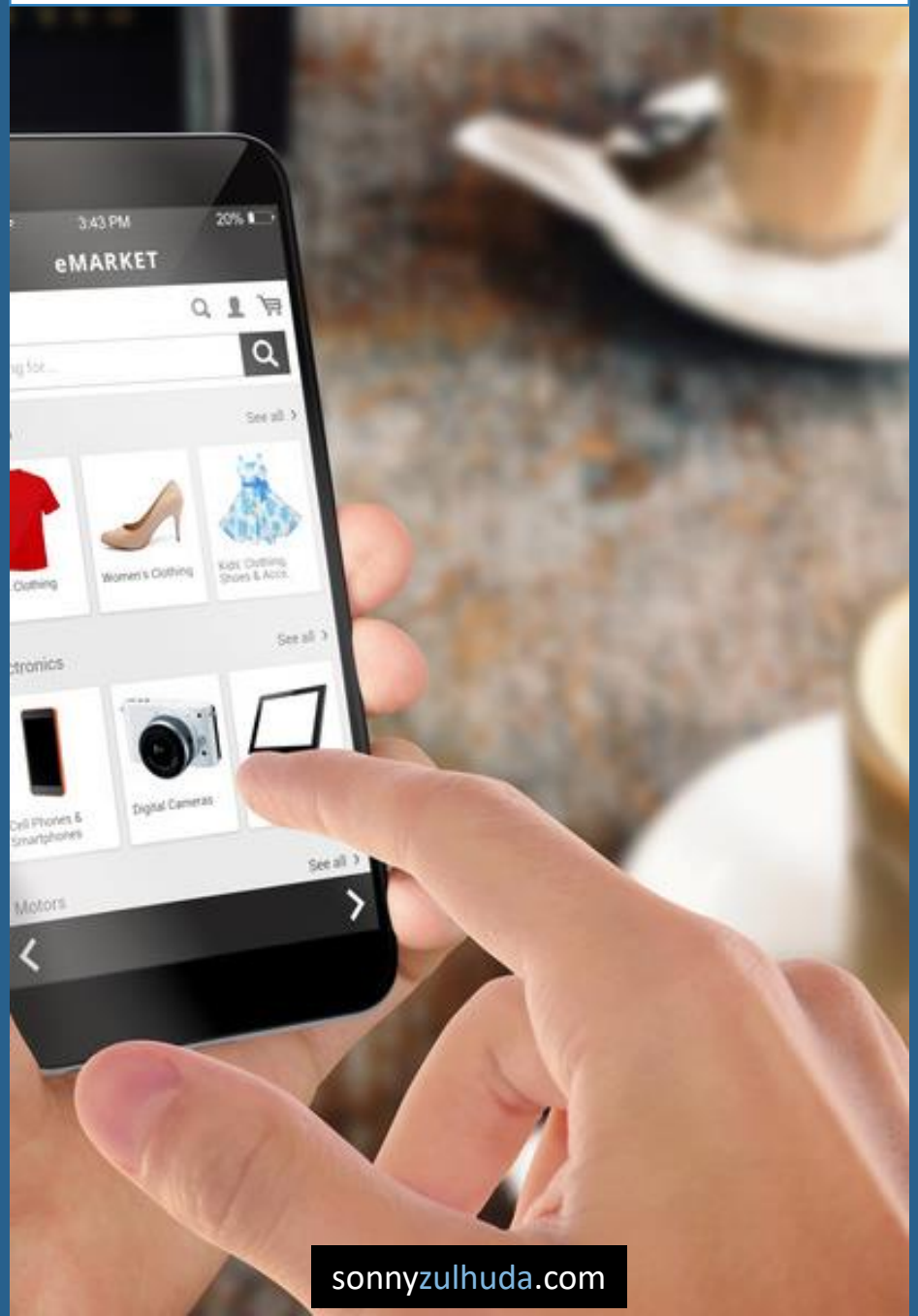
Lesson Learned

RESETTING CYBER SECURITY CULTURE

Cyber security is a process, not a product. It is a journey not a destination

CYBER SOCIETY: INTERDEPENDENCE

With the interdependence of information infrastructure, collective efforts to secure our cyberspace is necessary



NEW OFFENCES, NEW LAWS

Restrictions are introduced to reshape the new expected behaviour on data

CYBER SOCIETY NEEDS CYBER LEADERSHIP

No order without law, no law without enforcement, no enforcement without leadership

THANK YOU

DR SONNY ZULHUDA

Associate Professor at the International Islamic University Malaysia

sonny@iium.edu.my

sonnyzulhuda.com

twitter.com/zulhuda