الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
Garden of Knowledge and Virtue

LAW, POLICY, AND DATA GOVERNANCE: PRINCIPLES IN SETTING UP THE STANDARDS OF CYBERSECURITY

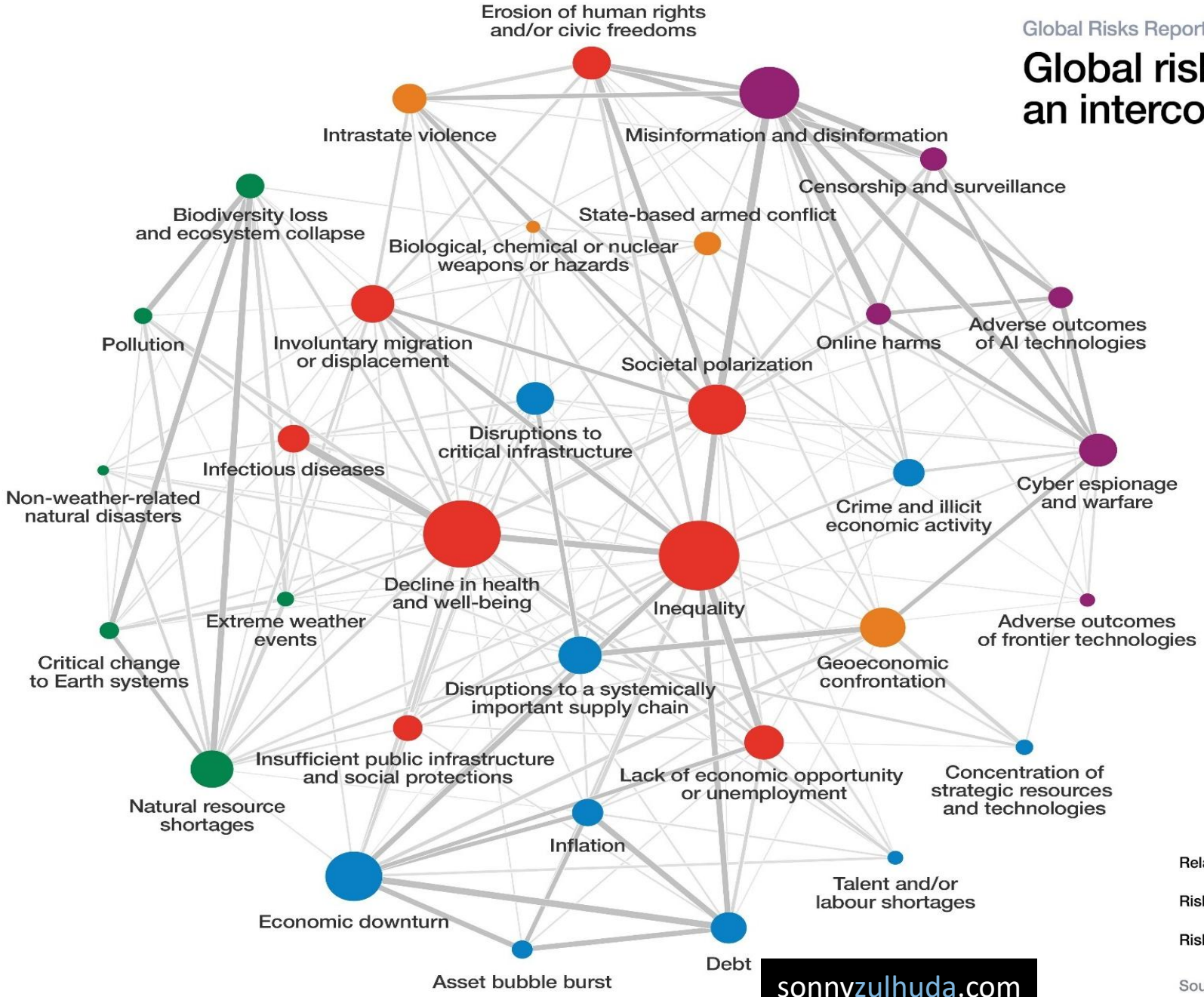
ASSOC. PROF. DR. SONNY ZULHUDA
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

ASEAN CYBER SECURITY SCHOOL 2026
18th November 2026

Global Risks Report 2025

Global risks landscape: an interconnections map

WORLD ECONOMIC FORUM



Relative influence, Edges — High — Medium — Low

Risk influence, Nodes ○ High ○ Medium ○ Low

Risk categories Economic · Environmental · Geopolitical · Societal · Technological

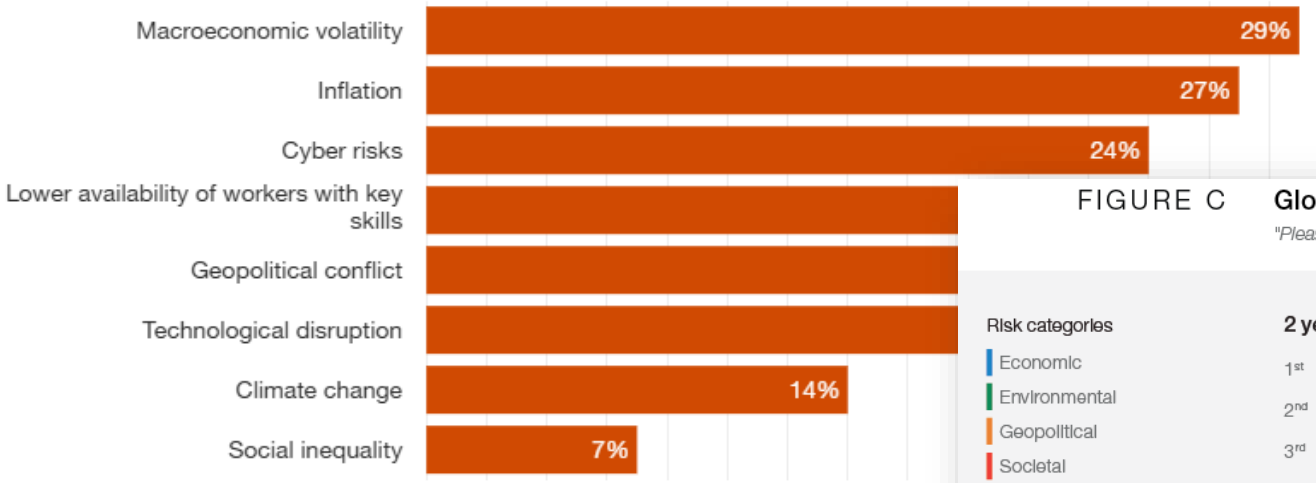
Source: World Economic Forum, Global Risks Perception Survey 2024-2025

sonnyzulhuda.com

Cyber Risks Today: Top 3 Global Threats (PwC 2025)

Q. How exposed do you believe your company will be to the following key threats in the next 12 months?

(Showing % that answered 'Extremely exposed' and 'Highly exposed')



Note: Exposure is the probability of significant financial loss.
Source: PwC's 28th Annual Global CEO Survey

Global Risks Severity: Cyber-related Risks Top 5 (World Economic Forum 2025)



Learning from the Recent Data Breaches….

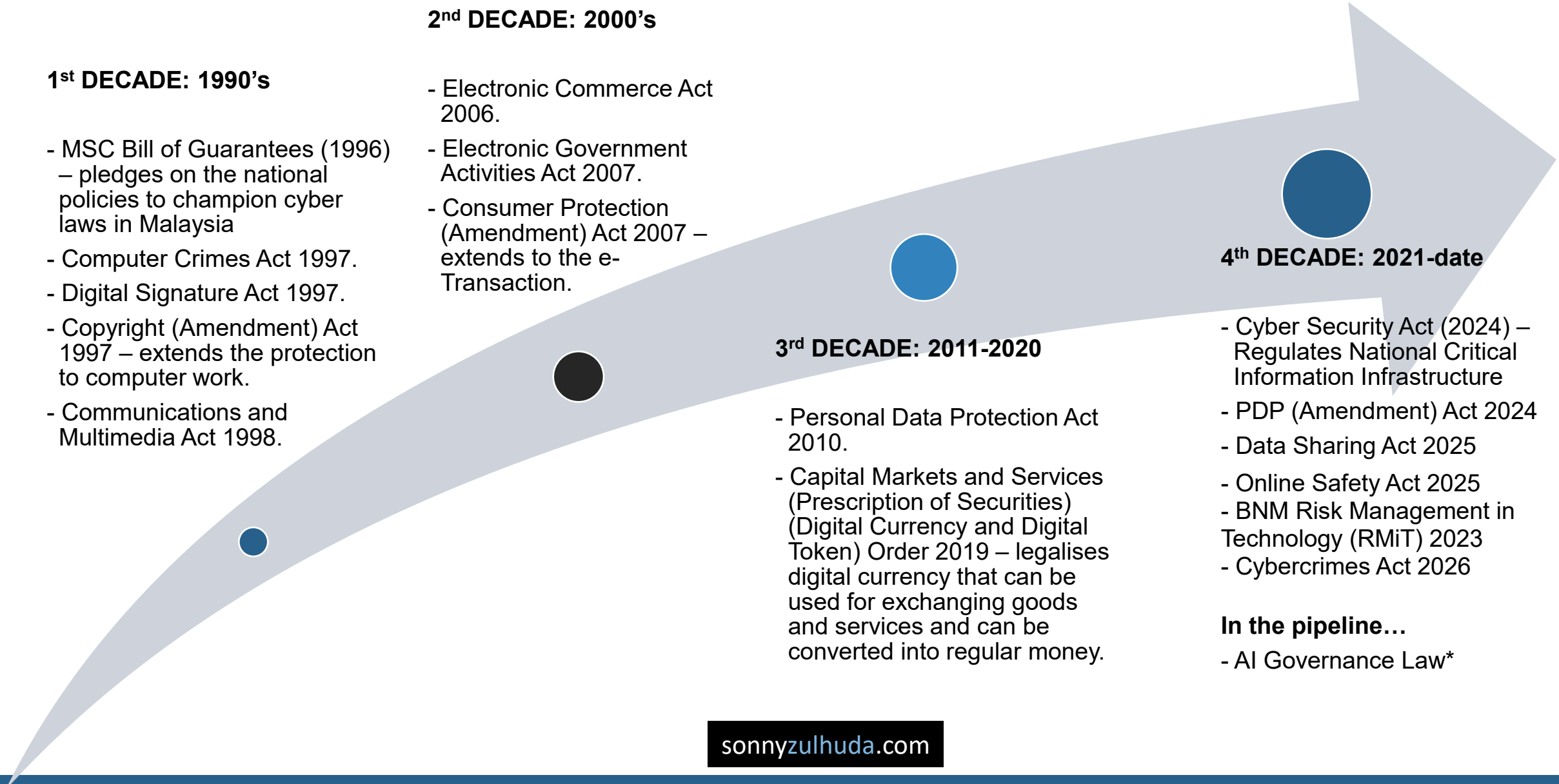




- In 2025, critical infrastructure organizations around the world have faced a wave of cyber threats driven by **espionage**- or **sabotage**-motivated threat actors, financially motivated ransomware groups, and **ideologically driven hacktivists**.
- The cyber operations are often connected to real-world geopolitical and ideological conflicts.
- Adversaries increasingly **“log in”** rather than **“break in,”** so they exploit legitimate accounts and authentication processes to gain access.

Morgan Adamski, PwC US (2025)

Digital Governance in Malaysia: A Work in Progress



1st DECADE: 1990's

- MSC Bill of Guarantees (1996) – pledges on the national policies to champion cyber laws in Malaysia
- Computer Crimes Act 1997.
- Digital Signature Act 1997.
- Copyright (Amendment) Act 1997 – extends the protection to computer work.
- Communications and Multimedia Act 1998.

2nd DECADE: 2000's

- Electronic Commerce Act 2006.
- Electronic Government Activities Act 2007.
- Consumer Protection (Amendment) Act 2007 – extends to the e-Transaction.

3rd DECADE: 2011-2020

- Personal Data Protection Act 2010.
- Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 – legalises digital currency that can be used for exchanging goods and services and can be converted into regular money.

4th DECADE: 2021-date

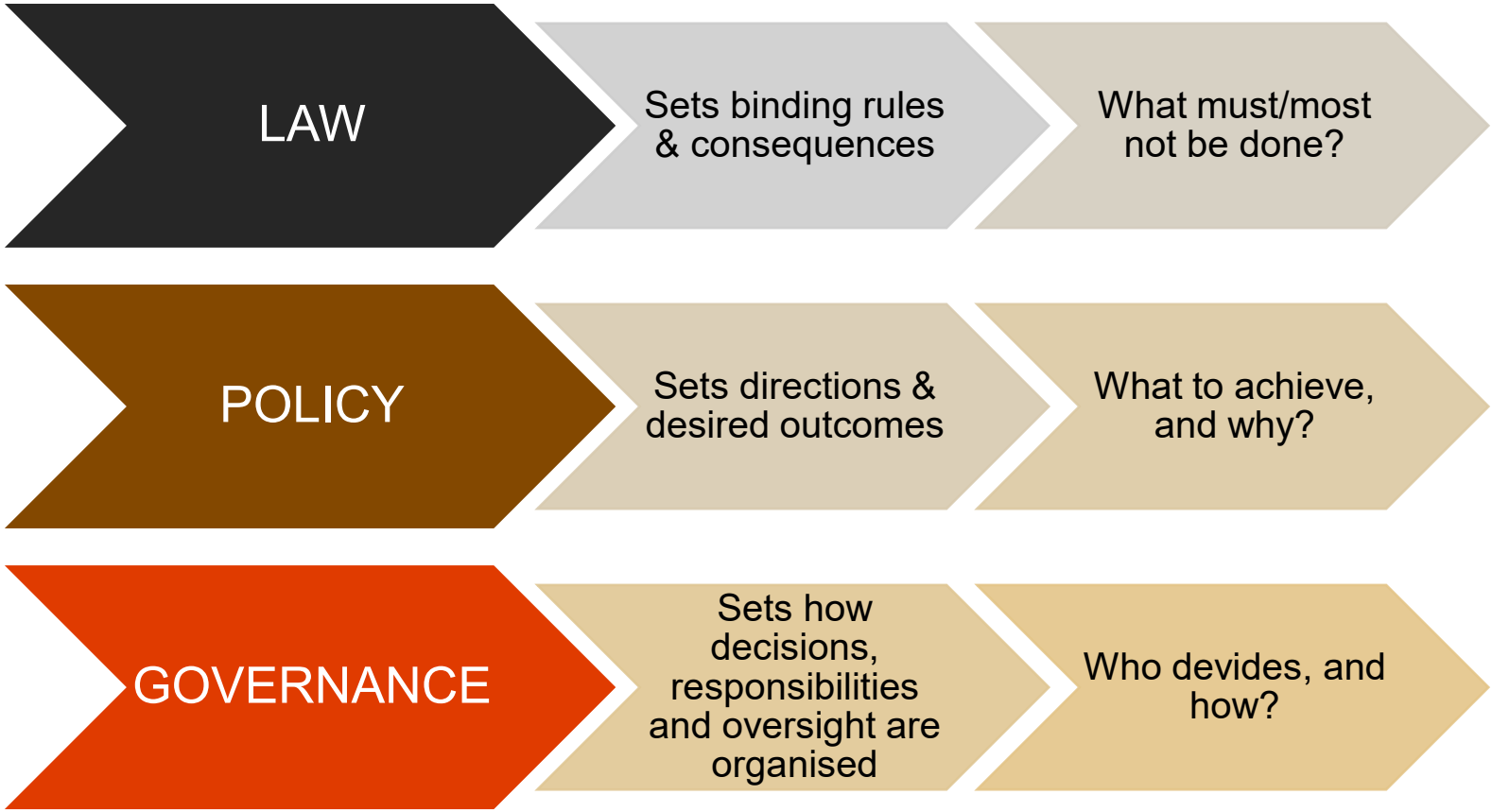
- Cyber Security Act (2024) – Regulates National Critical Information Infrastructure
- PDP (Amendment) Act 2024
- Data Sharing Act 2025
- Online Safety Act 2025
- BNM Risk Management in Technology (RMiT) 2023
- Cybercrimes Act 2026

In the pipeline…

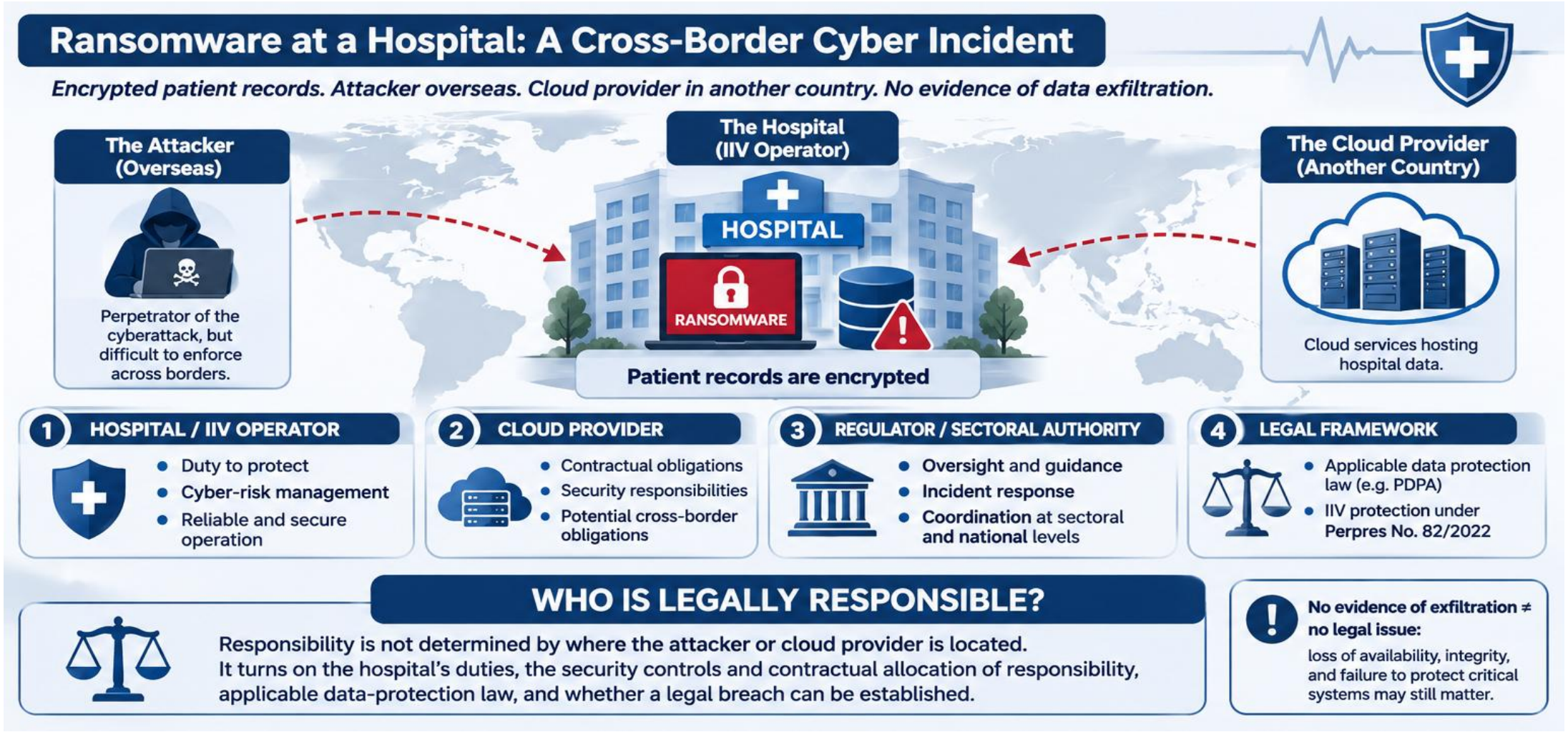
- AI Governance Law*

CYBERSECURITY:
From Law to Policy to Governance

The Basics

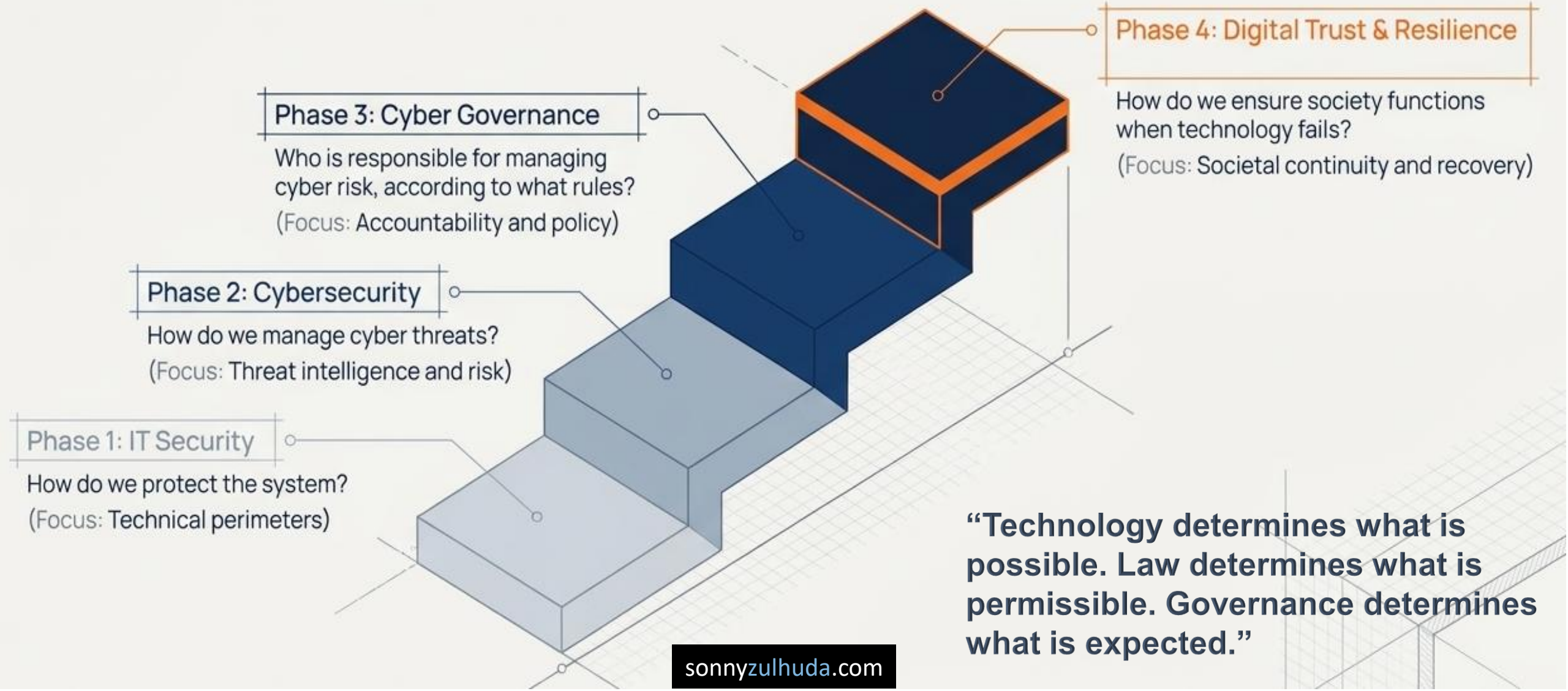

LAW
Sets binding rules & consequences
What must/most not be done?
POLICY
Sets directions & desired outcomes
What to achieve, and why?
GOVERNANCE
Sets how decisions, responsibilities and oversight are organised
Who devides, and how?

When a security attack takes place...



Cybersecurity is simultaneously: Technology → Law → Risk Management → Governance

The Evolution of Cyber Governance



"Technology determines what is possible. Law determines what is permissible. Governance determines what is expected."

The “Distributed Security” Approach



DISTRIBUTED SECURITY: A NEW MODEL OF LAW ENFORCEMENT

By

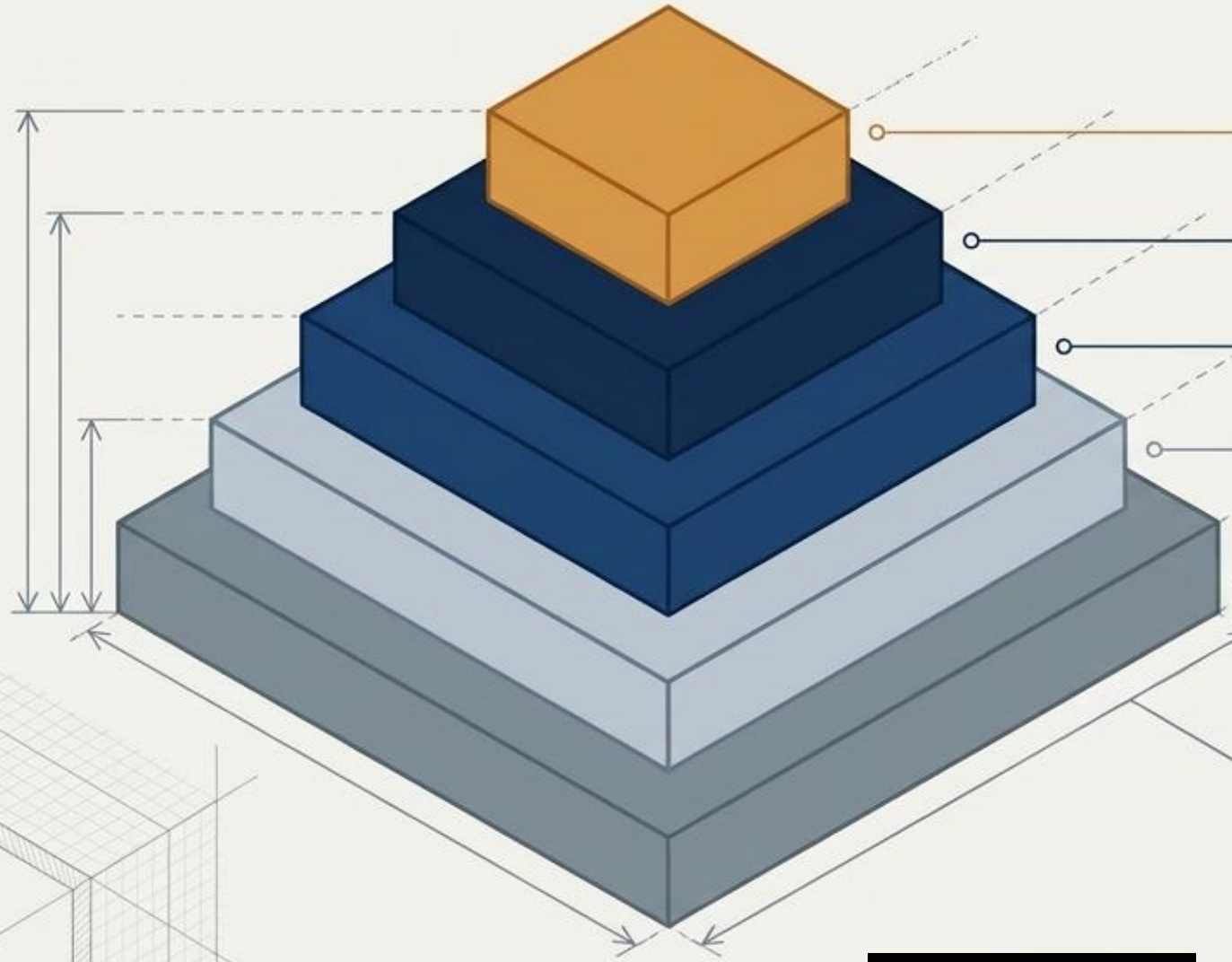
Susan W. Brenner
NCR Distinguished Professor of Law & Technology
University of Dayton School of Law
300 College Park
Dayton, OH 45469-2772
Email: Susan.Brenner@notes.udayton.edu
Phone: 937.229.2929
Fax: 937.229.2469

Leo L. Clarke
Associate Professor
Thomas M. Cooley Law School
111 Commerce Avenue SW
Grand Rapids, MI 49503
Email: clarkele@cooley.edu
Phone: 616.301.6800 ext. 6955

The “Distributed Security” Approach

Traditional Approach		Future Paradigm
From **reactive**	→	to **prevention**
From **locality**	→	to **globalisation**
From **defensive**	→	to **Strike-back strategy**
From **human-reliant**	→	to **automated detection**
From **incident-oriented**	→	to **risk-based approach**
From **top-down,** authority-centred	→	to **co-regulatory community** empowered
From **industry default-based** approach	→	to **industry insurance initiative**

The 5-Layer Legal Architecture



Governance & Accountability

Defines the top-of-chain responsibility (Board, CISO, Regulators).

Critical Infrastructure

Safeguards national economic survival and vital societal services.

Data Protection Law

Protects the human interests and rights attached to the information.

Cybersecurity Regulation

Establishes organizational security obligations and baselines.

Cybercrime Law

Protects systems against unlawful conduct (interference, fraud, unauthorized access).

Cybercrime Law

- To define the **illegal conduct**
  - Cyber-enabled and cyber-dependent crimes
  - Indirect actor: service providers
  - Corporate liability
- To determine the **punitive sanctions**
- To determine the **procedural requirements**
  - Investigation
  - Evidentiary issues
  - International collaboration
  - Preventive actions

International Cybercrime Treaties

United Nations Convention against Cybercrime;

Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

A new Convention adopted by the UN General Assembly in New York on 24th December 2024 by Resolution 79/243.

Article 7: Illegal access
Article 8: Illegal interception
Article 9: Interference with electronic data
Article 10: Interference with an information and communications technology system
Article 11: Misuse of devices
Article 12: ICT technology system-related forgery
Article 13: ICT system-related theft or fraud
Article 14: Offences related to online child sexual abuse or child sexual exploitation material
Article 15: Solicitation or grooming for the purpose of committing a sexual offence against a child
Article 16: Non-consensual dissemination of intimate images
Article 17: Laundering of proceeds of crime



Budapest Convention on Cybercrime 2001

Adopted in Budapest in 2001 as a European Treaty, and was further expanded to be opened to the rest of the World.

Article 2. Illegal access
Article 3. Illegal interception
Article 4. Data interference
Article 5. System interference
Article 6. Misuse of devices
Article 7. Computer- related forgery
Article 8. Computer- related fraud
Article 9. Offences related to child pornography
Article 10. Offences related to infringements of copyright and related right

sonnyzulhuda.com

Cybersecurity Regulations

- To determine:
  - The parameter of cybersecurity (CIA Objectives)
  - The object being secured (computer & computer system)
  - The critical infrastructure
  - The parameter of threats
  - The desired security practices: Prevent, Detect, Respond, Recover
  - The national and sectoral command in both peace and crisis
- To determine the **illegal conduct & sanctions**
  - Failure to conduct cyber-governance measures
  - Failure to comply with standards

Spotlight: Cyber Security Act 2024 (NCII Duties)



1

Implement Codes of Practice

Adopt specified measures, standards, and processes to ensure infrastructure security.

2

Risk Assessments & Audits

Conduct regular cyber security risk assessments and compliance audits via approved auditors.

3

Incident Notification

Mandatory reporting of cybersecurity incidents to the Chief Executive within a strict 6-hour window.

4

Cyber Exercises

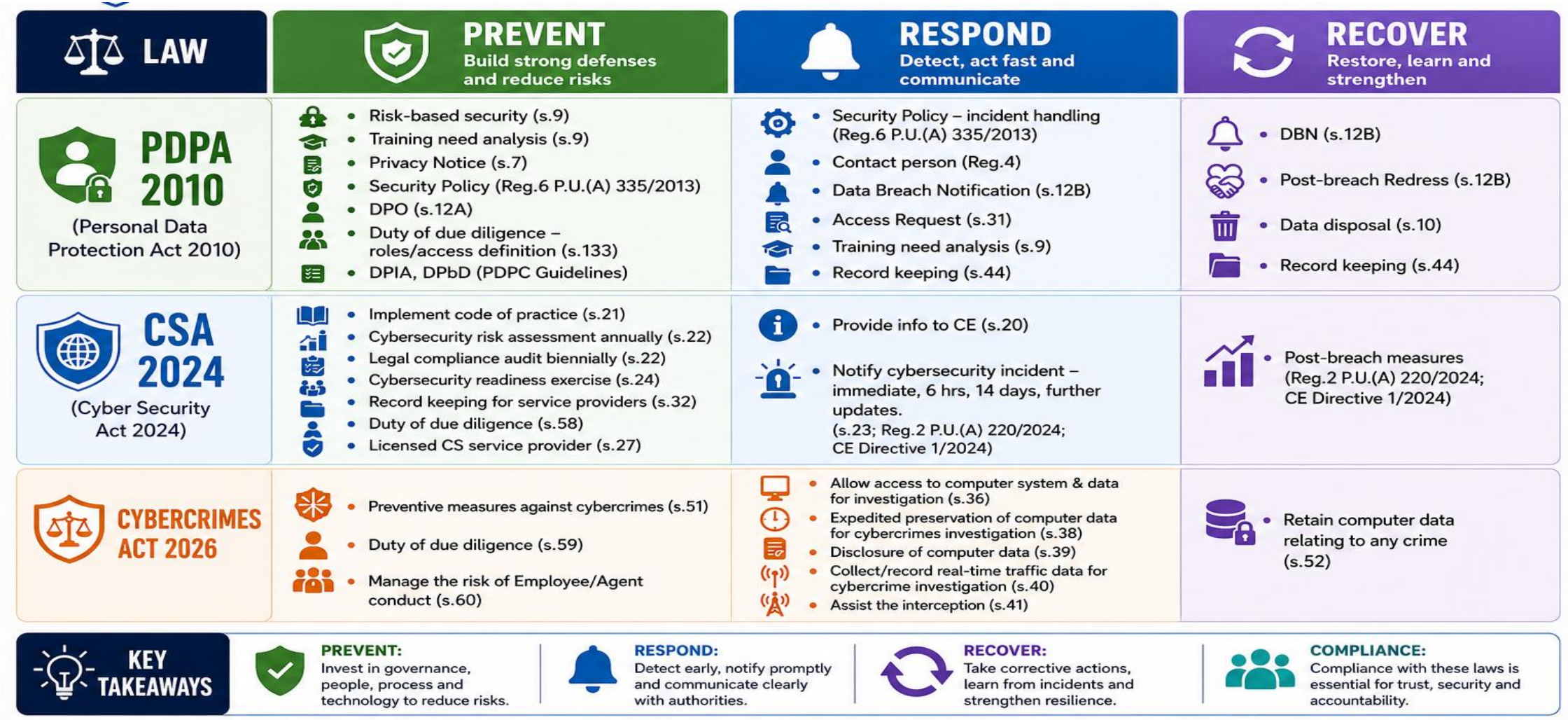
Active participation held by the Chief Executive to assess readiness and response to threats.

5

Service Provider Transparency

Clear designation, registration, and management of third-party cybersecurity service providers.

Cybersecurity Legal Framework (Malaysian Experience)



Personal Data Protection Law

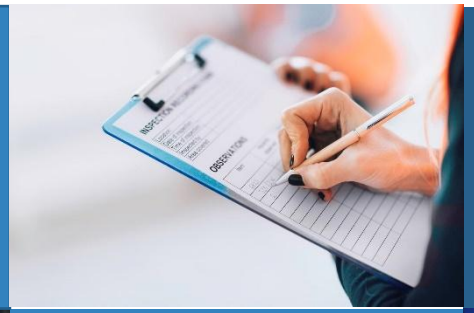
- To determine:
  - The nature and scope of protected **personal data**
  - The parameter of **threats** to personal data
  - The desired data privacy practices: A full data lifecycle
- To determine the **obligations** of data controller, data processor and the power of supervisory authority
- To determine the **rights of individuals** in term of data privacy
- To determine the **illegal conduct & sanctions**
  - Offences related to data breach & failures
  - Offences by body corporate


“The collection of data by any organisation or government without an expressly stated objective leaves said data highly vulnerable to abuse and represents a clear and dangerous dereliction of duty on the part of the collectors.”
Datuk Seri Anwar Ibrahim
sonnyzulhuda.com
Anwar Ibrahim FB

Common Privacy & Security Breach Incidents



1. Excessive collection of staff's or customers' data



2. Giving away control of data to third parties: processors, service providers. etc.



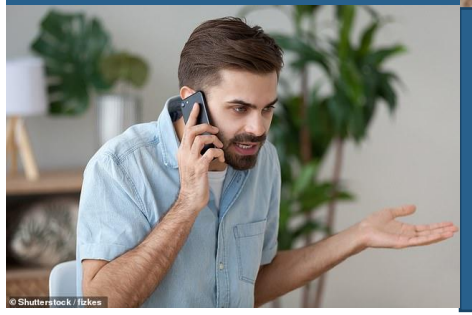
3. Unauthorised or Excessive access to internal system



4. Unsecured devices (WiFi, Commonly used computers)



5. Loss of unencrypted disc/drives, ID cards, private docs etc.



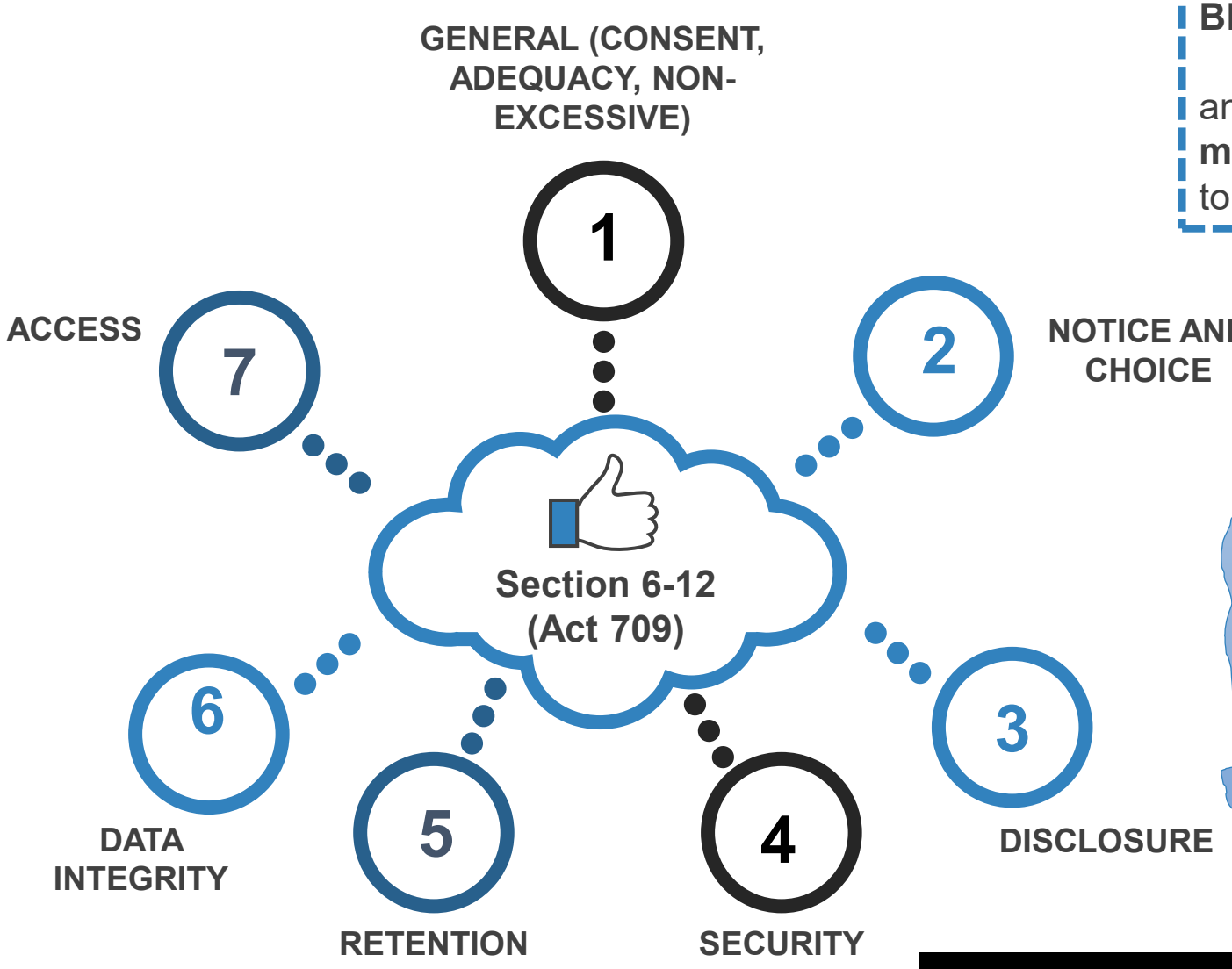
6. Use of unsecured AI or Apps for internal meetings/process.



7. Communications (Discussion, Gossip, etc.) over Social Media

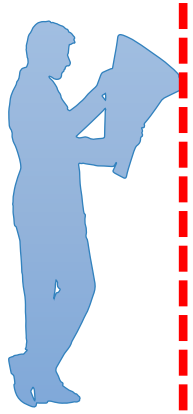


Seven Data Protection Principles



BREACH OF ANY PRINCIPLE?

an offence that triggers a potential fine up to **one million ringgit** or an imprisonment up to **three years** or to both [sec. 5 PDPA].



IF COMMITTED IN A BODY CORPORATE, WHO MAY BE IMPLICATED?

"…any person who at the time of the commission of the offence was a **director, chief executive officer, chief operating officer, manager, secretary or other similar officer of the body corporate** or was purporting to act in any such capacity or was in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management…" [section 133 PDPA]

Critical Information Infrastructure Protection

- To determine:
  - The scope of nation's critical information infrastructure (CII)
  - The roles and obligations of each CII owner and sector lead
  - The desired CII protection practices
- To determine the **obligations** of CII owner, CII service providers and CII sector Lead
- To determine the **illegal conduct & sanctions**
  - Damage to the CII system
  - Breach of CII-related licences
  - Offences by body corporate

The National Critical Information Infrastructure (NCII) Sectors under Cyber Security Act 2024

1. Government;
2. Banking and finance;
3. Transportation;
4. Defence and national security;
5. Information; communication and digital;
6. Healthcare services;
7. Water, sewerage and waste management;
8. Energy;
9. Agriculture and plantation;
10. Trade, industry and economy; and
11. Science, technology and innovation

Section 4, Schedule, Act 854



sonnyzulhuda.com

Presidential Regulation No. 82 of 2022
on the Protection of Vital Information Infrastructure (IIV)

Strengthening Indonesia's Digital Security for National Resilience

1 What is IIV?

IIV refers to Electronic Systems that use information technology and/or operational technology, which, if disrupted, could seriously impact **public interest, public services, national defence** and **security**, or the **national economy**.

2 8 Strategic Sectors

- Government Administration
- Energy & Mineral Resources
- Transport
- Finance
- Healthcare
- ICT
- Food
- Defence

3 Identification as the First Step

Electronic System Operators in IIV sectors must conduct identification of IIV **at least once a year**, and report the results to the relevant Ministry/Agency for verification.

IIV
Vital Information Infrastructure

Objective:
Keep, Prevent, and Ensure Recovery

4 Protection Lifecycle

Achieve a fully resilient cycle:

Identify → Protect → Respond → Recover

5 Shared Responsibility

- **BSSN:** national coordinator
- **MoF/Ministries:** sectoral responsibility
- **IIV Operators:** protect their systems
- **Cyber Incident Response Teams:** national, sectoral and organisational

6 Cyber Incident Response Mechanism

A 3-tier structure:

National → Sectoral → Organisational

7 BSSN as National Coordinator

BSSN

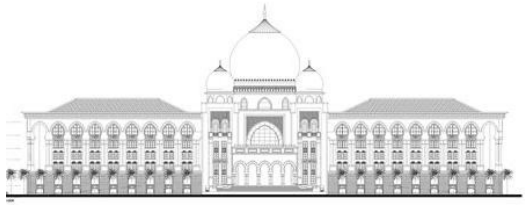
BSSN leads and coordinates the implementation of IIV protection and reports to the President.

Key Insight

Presidential Regulation No. 82/2022 turns digital infrastructure security from a technical issue into a matter of national resilience, with shared responsibility across the State and its operators.

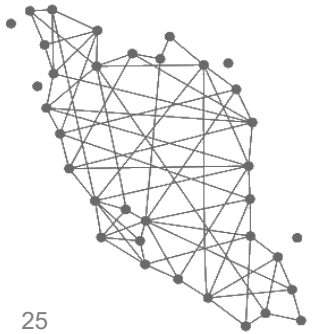
sonnyzulhuda.com

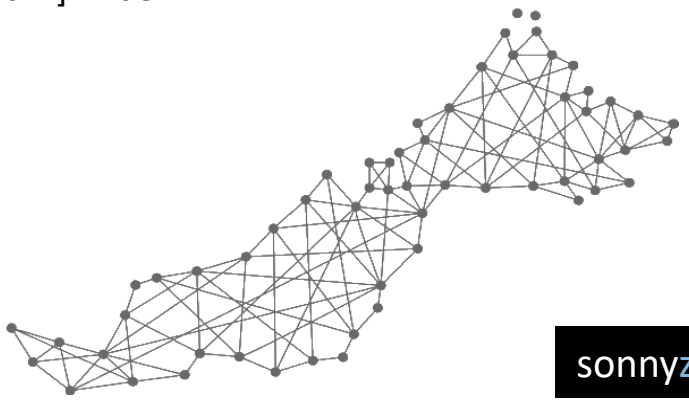
Breach to Critical Information Infrastructure



> The offense committed (against the banking sector) **challenges national dignity and integrity**… Emphasis must be given to issues of **Public Interest**… it involves the loss of public confidence in the banking institution… Computer crime is a serious offense. The offense committed is very disgusting and the community strongly condemns this behavior.

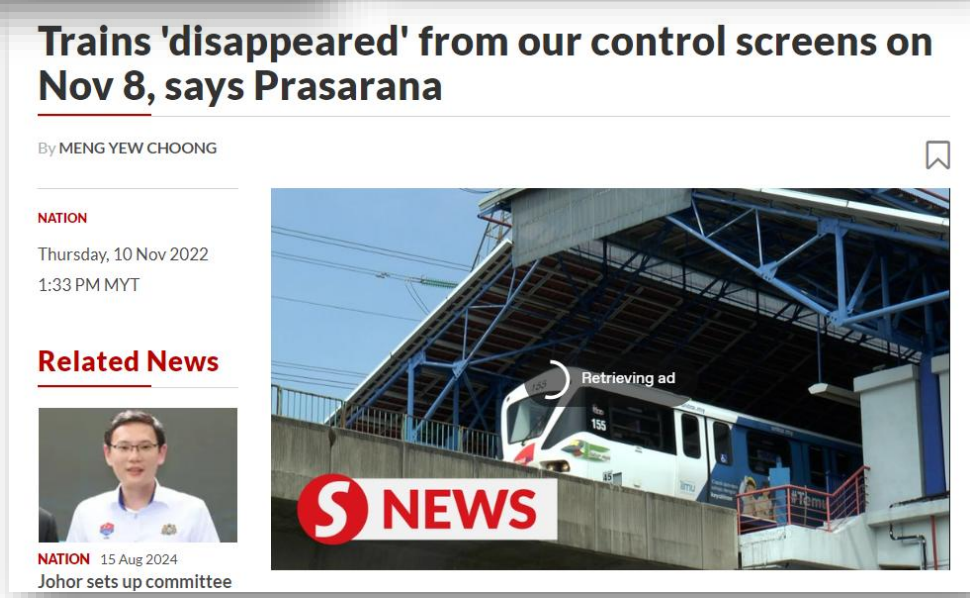
Mohamad Shariff Abu Samah, JC (High Court KL) in *Rose Hanida bt Long Iwn Pendakwa Raya* [2017] MLJU 1212.











sonnyzulhuda.com

Breach to Critical Information Infrastructure

NEW STRAITS TIMES | BUSINESS TIMES

Experts warn of cyber risks following KLIA cyberattack

By Mohamad Al As - March 26, 2025 @ 8:25pm



Cybersecurity experts have warned of evolving threats targeting critical infrastructure and called for strengthened defences across aviation systems. REUTERS FILE PIC

malaymail

HOME MALAYSIA SINGAPORE MONEY WORLD LIFE EAT/DRINK SHOWBIZ OPINION SPORTS TECH/GADGE

MALAYSIA

Personal Data Protection Dept chief discloses 3,699 reports on breaches since 2017, commonest through online purchases

Data breaches still haunt Indonesia as BSI becomes latest victim

The hacker group, which uses malicious software LockBit 3.0 that blocks user access to computer systems, claimed to hold BSI's data, including its customers' and employees' contact details, financial documents, card details and passwords of the customers.

Nur Janti (The Jakarta Post)

Tue, May 16, 2023

The Star

StarPlus | News | Asean+ | Business | Sport | Metro | Lifestyle | Food | Tech | Education

TOPICS : StarExtra | Flood Alert | StarESG | Urban Biodiversity | True or Not | SOBA 2023

Potential data breach at iPay88 still under probe, says Bank Negara

TEMPO.CO ENGLISH VERSION

Search News | TEMPO EXCLUSIVE

Home | Popular News | News | Asean & Beyond | Sport | Environment

Police Arrest EDCCash CEO over Cryptocurrency Fraud

Translator: Ricky Mohammad Nugraha

Editor: Laila Afifa

20 April 2021 23:09 WIB

THE STRAITS TIMES

8,500 phishing cases in Singapore in 2022; more than 80% spoofed a bank or financial service

Maybank warns of new fake banking website created to steal customer details

By ANGELIN YEOH

Singapore bank faces regulatory action over 'unacceptable' digital service outage

Hours-long disruption to DBS' online banking services is the second such incident in just over a year, notes Singapore's industry regulator, which says the bank has "fallen short" in ensuring system availability and quick recovery.

The ASEAN Context: Digital Masterplan 2030



VISION

Moving beyond initial connectivity toward a deeply integrated, secure, trusted, and resilient cross-border digital ecosystem.

Key Objectives

- Strengthen Digital Government & Infrastructure
- Empower Citizens with Safe Digital Public Services
- Digitally Transform Economies (Boost productivity & SMEs)
- Build Trustworthy & Secure Cyber Cooperation
- Align Technology with Sustainable Development

Key Principles of Cybersecurity Standards

1. Objective & national leadership (Cyber Resilience)
2. Role-playing: Government, Industry, Market, Educators, Community
3. Standardisation & innovation
4. Transparency & trust – Data governance by-design
5. International compliance and interoperability
6. Inclusion, public-private partnership
7. Risk-based Accountability

Cybersecurity Governance Self-Test

Whever you encounter a cyber problem, ask:

1	What must be protected? (Data? System? Infrastructure? National Security?)
2	From what risk? (Crime? AI? Insider threat? State actor?)
3	Who has the duty? (Board? Vendor? CISO? Government?)
4	What standard applies? (Law? Contract? International framework?)
5	What happens when it fails? (Penalty? Notification? Remediation?)

Challenges on Putting Cybersecurity Standards

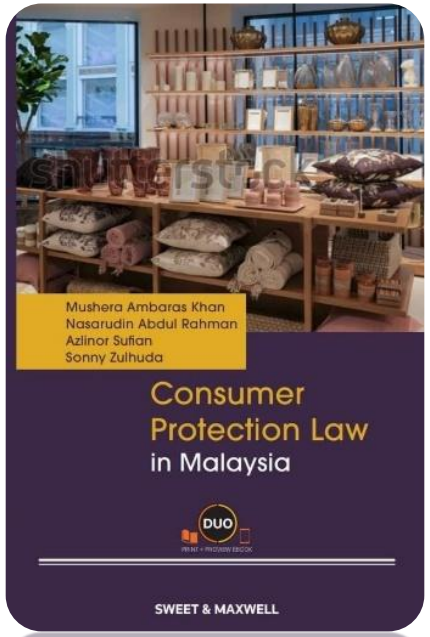
1. Involvement of multiple agencies – Who lead?
2. Reliance on industry makes negotiation harder
3. Maintaining the technology neutrality
4. Rapid changes on legal framework – pushed by frontier technology
5. Connectivity disparity

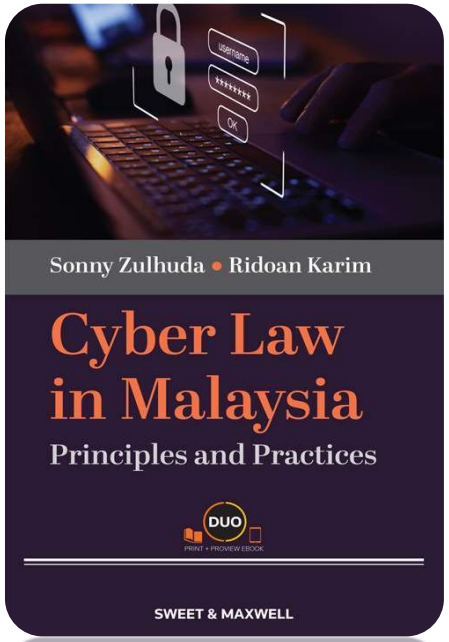
Final Remarks



THANK YOU

DR SONNY ZULHUDA





sonny@iium.edu.my
sonnyzulhuda.com

SCOPUS ID: 35782606500
ORCID ID: 0000-0003-0192-1971
GOOGLE SCHOLAR ID: B99CpLkAAAAJ&hl
IREP IIUM PAGE: http://irep.iium.edu.my/

