Managing the Chaos: Effective Response to Cyber Incidents

9 DECEMBER 2025

From Technical Firefighting to Strategic Command.

Part 1: Facts, Financials & Legislation

The Cost

- Financial Services sector has the highest average breach cost of any industry—USD 5.57 million (approx. RM 24.7 million) per incident.*

- Organizations that detect and contain a breach in <200 days save an average of $1.39 million (approx. RM 6.1m) **.

**Business World Online, 8 August 2024*
***IBM's 2024 Cybersecurity Report*

Speed isn't just for IT; it's a direct hit to the balance sheet.

The Cost

In 2024, Malaysia experience a significant surge in cyber threats.

Over 19.6 million web-based attacks in the first half of the year.

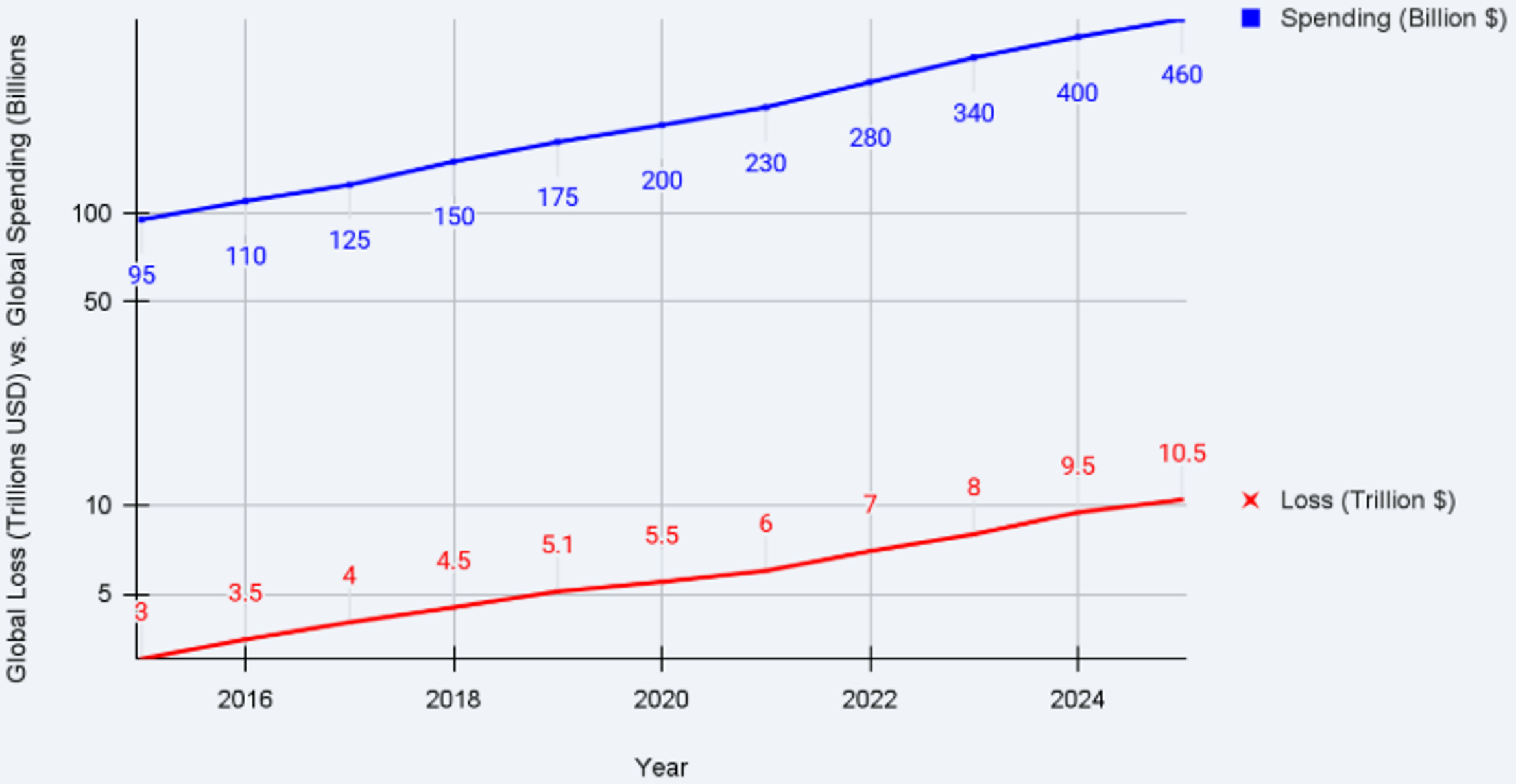
153% increase in ransomware incidents compared to the previous year.

Cyber Incident Statistics Reported to Cybersecurity Malaysia (Q1-Q4 2024)

Category	Q1 2024	Q2 2024	Q3 2024	Q4 2024	Total Reported
Data Breach	142	162	168	151	623
Fraud	1,025	1,114	1,139	1,108	4,386
Intrusion	48	65	71	75	259
Intrusion Attempt	38	58	140	97	333
Malicious Codes	111	91	57	42	301
Other Categories	191	(not specified)	(not specified)	(not specified)	317
TOTAL	1,555	1,481	1,623	1,550	6,219

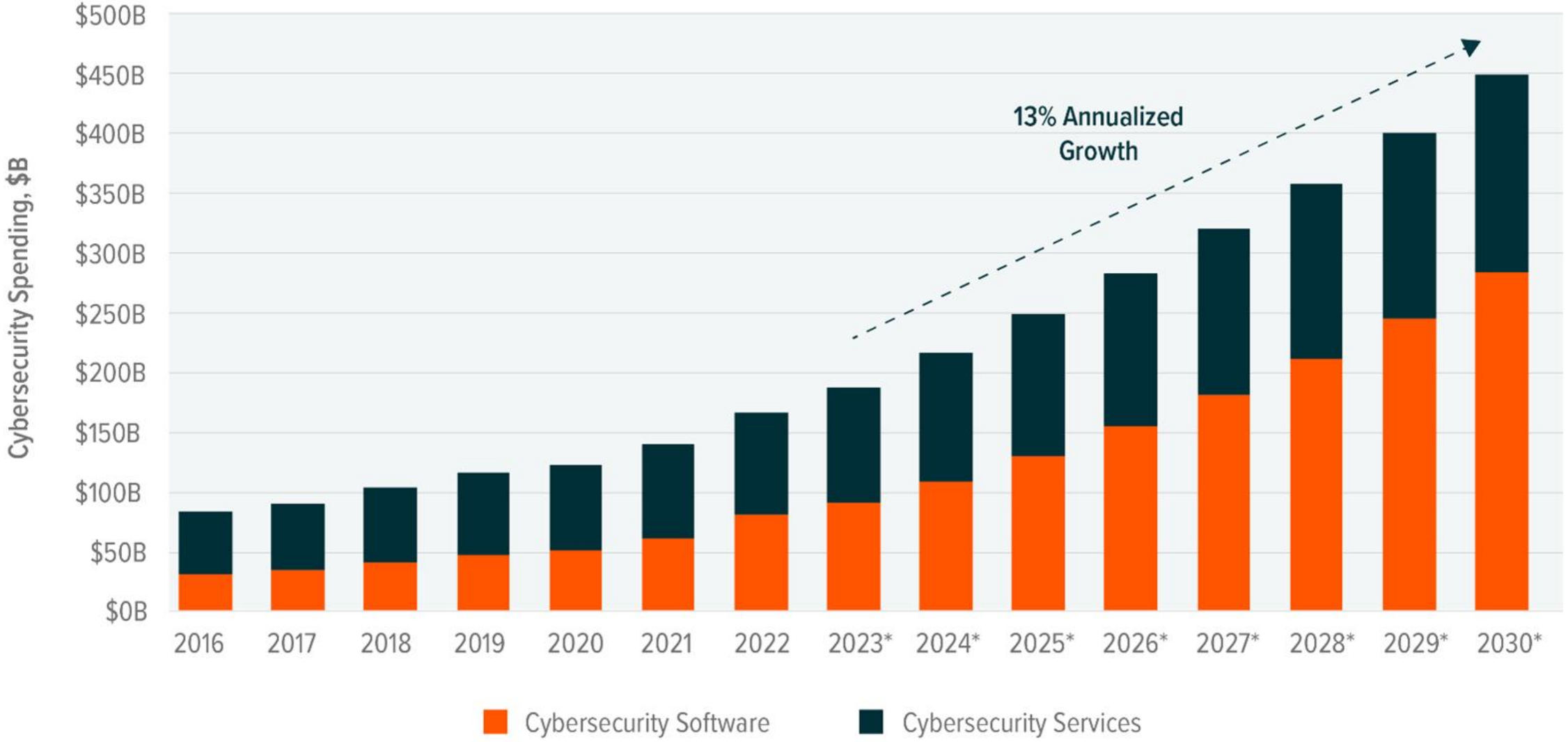
Note: The numbers in the table represent incidents reported to MyCERT and only reflect the total handled by their centre, not all incidents nationwide.

Global Cybercrime Loss vs. Cybersecurity Spending Over Time



GLOBAL CYBERSECURITY SPENDING FORECASTED TO GROW TO $450 BILLION BY 2030

Sources: Global X estimates with data from Gartner (2023, Sep 28) Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.



*Indicates Forecast

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)

As of Sep. 2023. Data shown is using current exchange rates.

Source: Statista Market Insights

THE GAME CHANGER - MALAYSIA CYBERSECURITY ACT 2024 (ACT 854)

Key sections for Risk Managers:

- **Section 21: Duty to Implement Code of Practice**
- **Section 22: Mandatory Risk Assessments & Audits**
- **Section 23: Duty to Notify**

THE "6-HOUR" GUN TO YOUR HEAD

The Risk: Failure to notify = RM 500,000 Fine + up to 10 Years Jail

21.Duty to Implement Code of Practice

Core Message

"Good enough" is dead. You must meet the specific technical Code of Practice for your sector.

The Duty

An NCII entity shall implement the measures, standards, and processes specified in the Code of Practice.

The Flexibility (Limited)

You can use alternative measures, but only if you prove they offer equal or higher protection.

The Penalty: Non-compliance = RM 500,000 Fine + Up to 10 Years Jail.

21.Duty to Implement Code of Practice

For Banking & Financial Institutions (BNM)

- **The Code:** Policy Document on Risk Management in Technology (RMiT).
- **Status:** This is the primary directive. BNM regulates cybersecurity through the RMiT framework.
- **Key Requirement:** The Act makes adherence to RMiT not just a regulatory expectation but a matter of national security law.

  Note: BNM also enforces the **Management of Customer Information and Permitted Disclosures (MCIPD)** for data protection aspects.

The Penalty: Non-compliance = RM 500,000 Fine + Up to 10 Years Jail.

21.Duty to Implement Code of Practice

For Capital Market Entities (Securities Commission)

- **The Code:** Guidelines on Technology Risk Management (GTRM).
- **Status:** Recently revised (August 2024) specifically to align with the Cyber Security Act 2024.
- **Key Requirement:** Paragraphs within these Guidelines regarding cyber risk management, access control, and data protection are now legally enforceable under the Cyber Security Act 2024.

The Penalty: Non-compliance = RM 500,000 Fine + Up to 10 Years Jail.

22.Mandatory Risk Assessment & Audit

The Duty

You must conduct a Cyber Security Risk Assessment and an Audit within the prescribed periods.

The Deadline

Reports must be submitted to the Chief Executive (NACSA) within 30 days of completion.

The Power

The Chief Executive can reject your report and order a re-evaluation if deemed unsatisfactory.

The Penalty: Failure to conduct or submit = RM 200,000 Fine + Up to 3 Years Jail.

22.Mandatory Risk Assessment & Audit

Requirement	The "Standard" under Section 22	Mapping to BNM/SC Standards
Cyber Risk Assessment	**Frequency**: At least once every 1 year.	**BNM RMiT:** Paragraph 10.5 requires regular risk assessments. **SC GTRM:** Mandates regular Threat & Risk Assessments (TRA). ***Note**: The Act solidifies this to a strict annual cycle.*
Cyber Security Audit	**Frequency**: At least once every 2 years.	**BNM RMiT:** Requires independent assurance. The Act sets the 2-year hard limit. ***Note:** The auditor must be an approved auditor registered with NACSA.*

The Penalty: Failure to conduct or submit = RM 200,000 Fine + Up to 3 Years Jail.

23.Duty to Notify

The Trigger

Notification is mandatory if an incident "has or might have occurred". It does not require full confirmation, just the knowledge that it might have happened.

The Recipients

Must notify NACSA (Chief Executive) AND the Sector Lead.

The Deadline

Immediate notification followed by a detailed report (The "6-Hour Rule" via NC4S).

The Penalty: Non-compliance = RM 500,000 Fine + Up to 10 Years Jail.

23.Duty to Notify

You are likely used to reporting to BNM via **ORION** (formerly TRiS) or to the SC. You must now ensure your incident response plan covers **both**:

1. **The Regulator (Sector Lead):**
   - **BNM:** Report via **ORION** (Operational Risk Integrated Online Network).
   - **SC:** Report via the **Common Reporting Platform (CRP)** or direct email as per GTRM.

2. **The National Agency (NACSA):**
   - **New Requirement:** You must effectively report to the **National Cyber Coordination and Command Centre (NC4)** system simultaneously.

The "Risk Manager" Warning:
Previously, under RMiT, you might have interpreted "promptly" as "once we know the root cause" . Under Section 23 and the new Regulations, "discovery" triggers the 6-hour timer. Waiting 24 hours to confirm the source of the hack before reporting could technically put the company in breach of the Cybersecurity Act 2024.

The Penalty: Non-compliance = RM 500,000 Fine + Up to 10 Years Jail.

Am I affected?

1. The "Impact Test" (Legal Definition)

NCII is defined by the **consequence of failure**.

A Financial Institution is an NCII Entity if its computer systems meet this definition (Section 4):

*"A computer or computer system which the disruption to or destruction of... would have a **detrimental impact** on the delivery of any service essential to the **security, defense, foreign relations, economy, public health, public safety or public order** of Malaysia."*

The "Risk Manager" Translation:

- "If our system goes down, does it just hurt *our* profits? Or does it hurt the *country*?"
- If a small money changer goes offline, it hurts the owner. **(Likely Not NCII)**
- If Maybank2u or the chaotic interbank payment switch (RPP) goes offline, it hurts the economy. **(Definitely NCII)**

Am I affected?

2. The Designation Process (How you know for sure)
Being a "bank" or "insurer" makes you a *candidate*, but it doesn't make you an *entity* under the Act until you receive the Designation.

The Authority: The **Sector Lead** (Bank Negara Malaysia or Securities Commission) is responsible for identifying which specific FIs meet the definition above.

The Notification: You will receive a written **Notice of Designation** from BNM or SC.

The Register: NACSA maintains a register of these entities, but for security reasons, this list is generally not broadcast to the public to avoid creating a "Target List" for hackers.

Am I affected?

3. **Likely Candidates (Who is in the crosshairs?)**

- **Domestic Systemically Important Banks (D-SIBs):** (e.g., Maybank, CIMB, Public Bank). Their failure would crash the economy.
- **Major Payment System Operators:** (e.g., PayNet, major e-wallet providers like TNG Digital).
- **Large Insurers & Takaful Operators:** Particularly those with massive market share where a collapse would leave millions uninsured or unable to claim.
- **Capital Market Infrastructure:** (e.g., Bursa Malaysia).

Am I affected?

4. The "Grey Area" Trap (Crucial for Risk Managers)

The Trap: "We haven't received a letter from BNM yet, so we don't need to worry about the Cyber Security Act.“

The Reality: Even if a smaller FI hasn't been designated as "NCII" yet, **BNM’s RMiT (Risk Management in Technology)** policy applies to *all* licensed financial institutions.

The Catch: BNM has aligned the RMiT with the Cyber Security Act.

The Result: Even if you aren't legally an "NCII Entity" under the Act, BNM will likely enforce the *same standards* (Section 21 equivalent) and *reporting timelines* (Section 23 equivalent) through their own regulatory powers.

Summary

Section	Key Keyword	The "Risk Manager" Takeaway
S. 21	Implementation	"Best effort" is gone. We must strictly follow the Sector Lead's Code of Practice.
S. 22	Assessment	Mandatory Annual Risk Assessments & Bi-annual Audits. No skipping.
S. 23	Notification	6 Hours to report. Silence is now a crime.

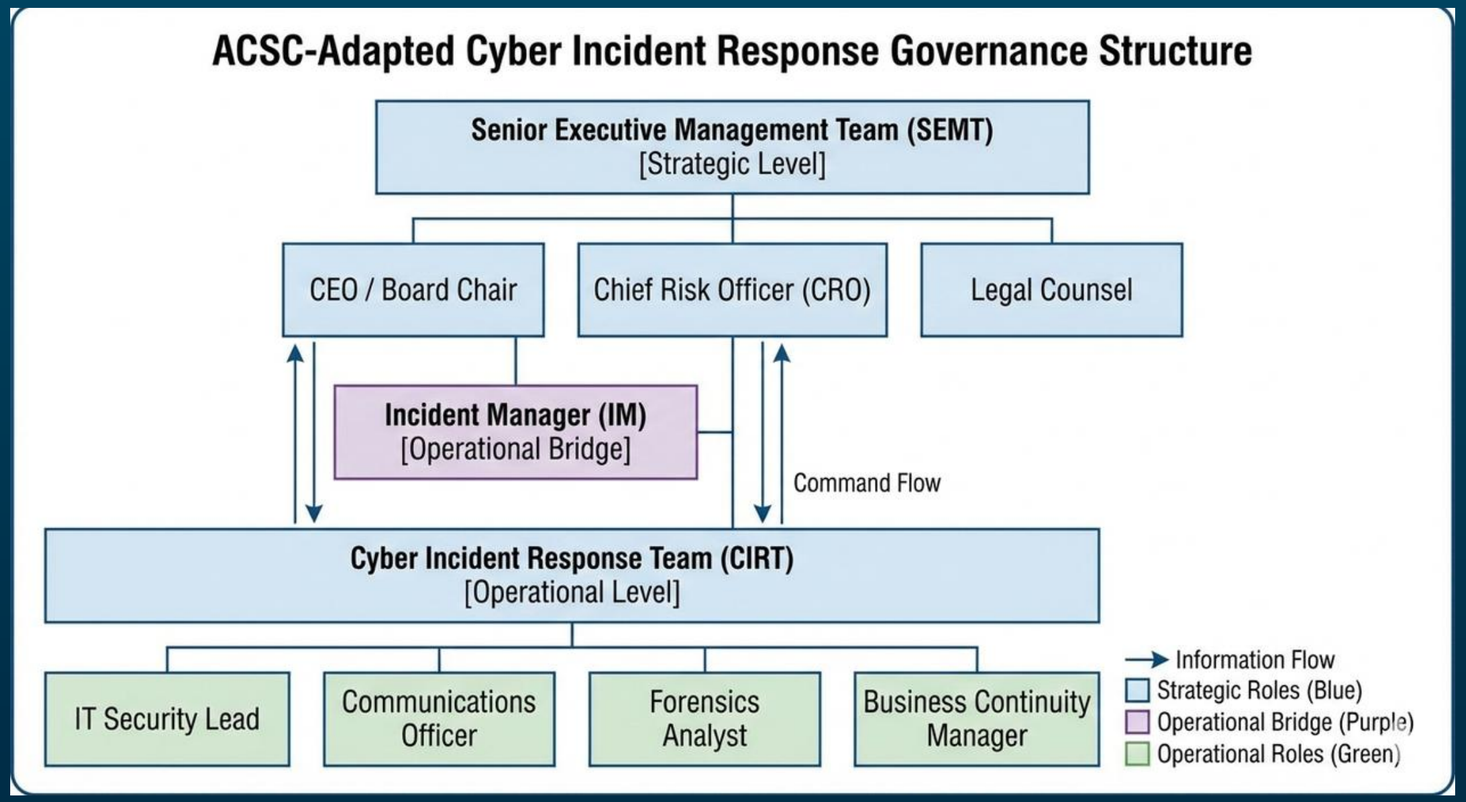
Summary

Offence	Maximum Financial Penalty	Maximum Imprisonment
Failure to report a cybersecurity incident	RM 500,000	10 years (or both)
Failure to implement the Code of Practice	RM 500,000	10 years (or both)
Failure to conduct risk assessments or audits	RM 200,000	3 years (or both)
Failure to provide info on NCII assets	RM 100,000	2 years (or both)
Providing cybersecurity services without a license*	RM 500,000	10 years (or both)

Part 2: Framework

Roles & Communication

Who is Flying the Plane? (CIRT vs. SEMT)



Note: ACSC - Australian Cyber Security Council

CIRT (Operational)

IT, Forensics. Focus: Containment & Eradication.

SEMT (Strategic):

Risk, Legal, Comms, HR. Focus: Reputation, Liability, & Regulatory Compliance.

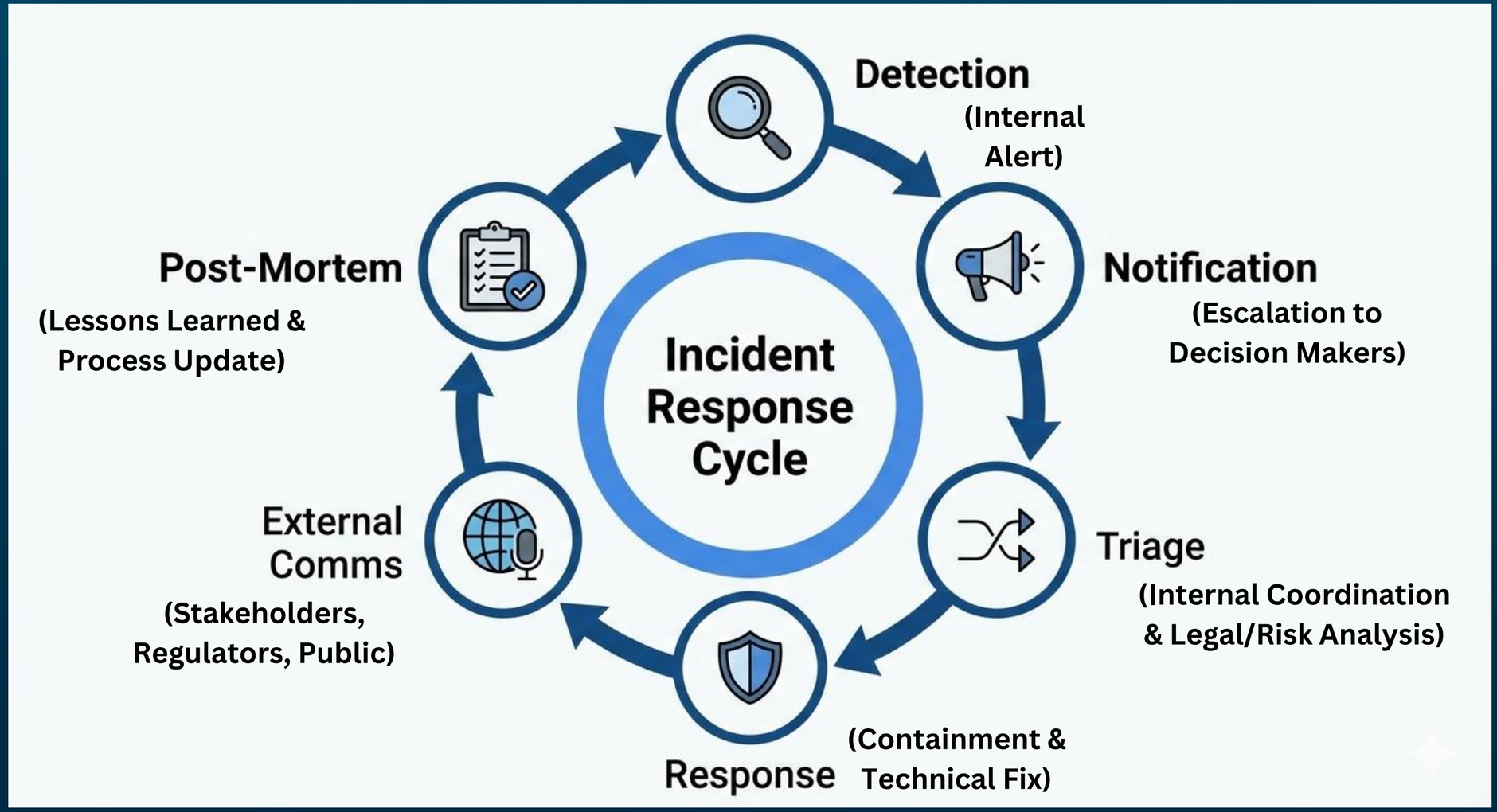
The Gap:

Most companies have a CIRT (IT fix) but lack an activated SEMT (Crisis Command).

Action:

Risk Managers must chair or advise the SEMT (Senior Executive Management Team).

Unified Communication Model



Unified Communication Model

The Core Principle: Communication is an operational pillar, not an afterthought.

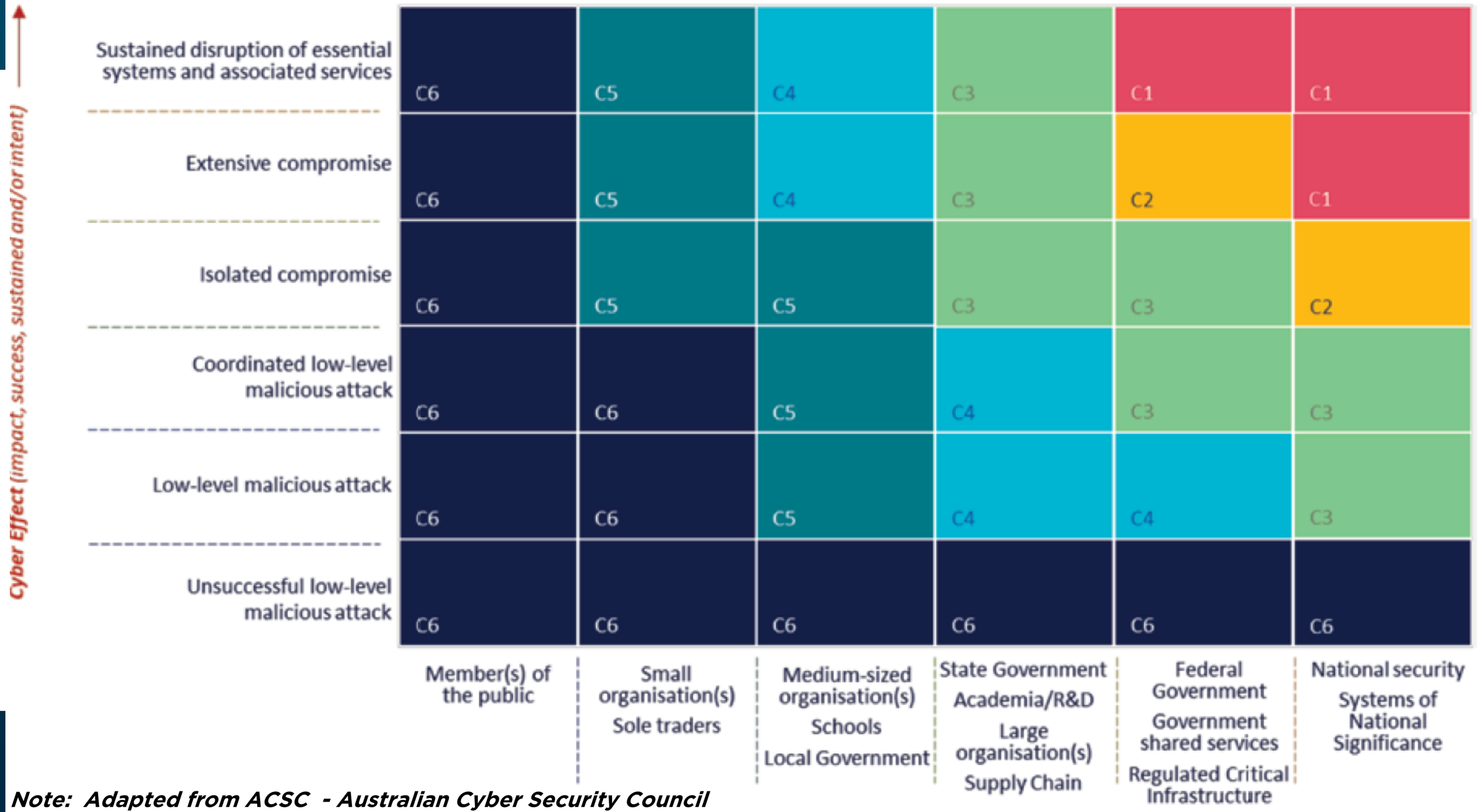
The Golden Rule: "Silence is not a strategy."

- **Reactive (Uber 2016):** Concealed breach, paid ransom to hide it.
  - **Result:** $148M settlement, criminal charges, massive reputational loss.

- **Proactive (CrowdStrike 2024):** Immediate, transparent disclosure.
  - **Result:** Trust maintained despite global outage.

Key Takeaway: Integrated communication reduces uncertainty and regulatory backlash.

Decision Matrix



Note: Adapted from ACSC - Australian Cyber Security Council

The Decision Matrix

Is there a definition of the criticality (C1,C2,C3 etc.) of the incident based on depth and width of the cyber attack in the Cybersecurity Act 2024?

No, the Cybersecurity Act 2024 itself does not explicitly define "C1, C2, C3" (or any specific alphanumeric matrix) in the primary text of the Act or its Regulations.

However, the Act **delegates** this definition to the **Code of Practice (Sector Leads)** and the **National Cyber Security Agency (NACSA)**.

The Decision Matrix

Here is how we can breakdown the "Criticality" and define “legal” vs. “operational”

1. **The Legal "Severity" Requirement**
The *Cyber Security Act 2024 (23. Notification of Cyber Security Incident)* requires you to report the **"Severity"** of the incident.

The Problem: The Regulation does not print a table saying "Level 1 = x".

The Solution: You must use the classification provided by your **Sector Lead (BNM)** or the **National Cyber Coordination and Command Centre (NC4)**.

The Decision Matrix

2. The "C1, C2, C3" Equivalent: The NCCMP Levels

When Malaysian government bodies (and NCII Sector Leads) discuss "Criticality" based on "depth and width," they are referencing the National Cyber Crisis Management Plan (NCCMP).

Level	Criticality Definition (Depth & Width)	Who Manages It?
Level 1 (Low)	**Agency/Entity Level Incident:** The impact is contained within your specific organization. It does not spread to other banks or the national grid. **Example:** A generic malware infection on 5 staff laptops.	You (The Entity).You handle it internally but must notify the Sector Lead.
Level 2 (Medium)	**Sectoral Crisis:** The attack has the "width" to affect multiple entities in the same sector OR the "depth" to cripple a critical sectoral function. **Example:** A ransomware attack that takes down the interbank payment switch (RPP/DuitNow).	Sector Lead (BNM)BNM activates its crisis team to coordinate across banks.
Level 3 (High)	**National Crisis:** The attack spreads across multiple sectors (e.g., Energy AND Finance) or threatens national security/public safety. **Example:** A state-sponsored attack wiping data from both TNB and Maybank simultaneously.	National Cyber Security Committee (Prime Minister)National Security Council (MKN) takes command.

The Decision Matrix

3. The BNM Context

- We need to be familiar with BNM's ORION (Operational Risk Integrated Online Network) reporting.
- When reporting under the Act, we should not invent a new "C1-C3" matrix
- We should align with the BNM RMiT impact classifications that we already use, which BNM then maps to the National Levels.

The Decision Matrix

3. The "Risk Manager" context:

"The Act requires us to report 'Severity.' We do not need to invent a new metric. We will continue to use our **Impact Rating (Minor, Significant, Critical)** as defined in our internal Cyber Incident Response Plan (CIRP), which aligns with BNM's RMiT.

However, under the new Act, if our internal rating hits **'Critical'**, it likely triggers a **Level 2 (Sectoral)** or **Level 3 (National)** response from the government, which invites immediate NACSA intervention into our operations."

The Decision Matrix

4. Mapping of BNM/RMiT Impact Ratings (what you already use) to the National Crisis Levels (what the government uses)

Internal Impact (BNM RMiT View)	Description (Depth & Width)	National Crisis Level (NACSA View)	Action Required under Section 23
LOW / MINOR	**Isolated Incident** • Affects single user/device (e.g., malware on 1 laptop). • No data loss or financial impact. • Operations continue normally.	N/A (Routine)	**Internal Log Only**(Generally not reportable unless it reveals a new systemic threat pattern).
MEDIUM / SIGNIFICANT	**Localized System Failure** • Critical internal system down (e.g., HR portal, internal email). • Customer-facing services slow but functional. • Non-sensitive data exposed.	Level 1 (Entity Crisis)	**REPORTABLE (6 Hours)** Notify Sector Lead (BNM) + NACSA. Why? It jeopardizes the security of the NCII system.
HIGH / CRITICAL	**Service Disruption** • Customer-facing channels down (e.g., Mobile Banking, ATM switch). • Confirmed data leak (Customer PII/Financials). • Financial loss expected.	Level 2 (Sectoral Crisis)	**MANDATORY REPORT** (Immediate)Activate Crisis Management Team (CMT). Prepare for BNM Intervention.
SYSTEMIC / CATASTROPHIC	**National Threat** • Attack spreads to other banks/insurers (Supply Chain). • Threatens financial stability (e.g., RPP/Payment Switch down). • State-sponsored actor suspected.	Level 3 (National Crisis)	**NATIONAL EMERGENCY** National Security Council (MKN) takes command. Board of Directors must be notified immediately.

The Decision Matrix

1. The "Reportable" Threshold (The Trap)
Many risk managers ask: "Do I have to report a phishing email?“

The Rule: If it was blocked, NO.

The Exception: If it was clicked and "jeopardized" the system (even if you contained it quickly), YES.

"Under the Cybersecurity Act 2024, the trigger isn't 'Loss of Money,' it is 'Jeopardy of Security.' If a hacker got in—even if they stole nothing—you must report it within 6 hours. Do not confuse 'No Loss' with 'No Incident'."

The Decision Matrix

2. The "Severity" Definition (Regulation 4)
The Cyber Security (Notification of Cyber Security Incident) Regulations 2024 requires you to state the "Severity" in your report.

Recommendation: Do not invent a new scale. Use the terms "Significant" or "Critical" from the matrix above. These align with BNM's language and signal to NACSA that you are treating this seriously.

3. The "6-Hour" Timer Logic
Use this simple flowchart for your audience:

Discovery of "Jeopardy" ➔ Start Timer ➔ Notify BNM (ORION) & NACSA (NC4) ➔ < 6 Hours Elapsed

CYBERARMOUR

Part 3: Case Studies

CASE STUDY 1 – THE "SILENT" BREACH (IPAY88)

Detection

May 31, 2022

Internal red flag raised when the internal IT team discovered the breach and classified it as an incident and not a glitch.

Containment

July 20, 2022

Green Checkmark - Technically Fixed. The IT team marked the case as internally resolved.

Notification

August 11, 2022

"Public Informed"

73 DAYS OF SILENCE

CASE STUDY 1 – THE "SILENT" BREACH (IPAY88)

The Scenario: A payment gateway breach compromising card data.

- **Technical Response**: Successful. The breach was contained by July 20.
- **Strategic Response**: Delayed. Public/Regulators notified ~2.5 months after detection.

The "Act 854" Reality Check (If this happened today):

- **Violation**: Section 23 mandates notification when an incident "might have" occurred.
- **The Gap**: 73 Days vs. 6 Hours (Regulatory Deadline).

The Consequence (If this happened today):

- **Regulatory:** RM 500k Fine + Up to 10 Years Jail (Section 23).
- **Liability:** Directors are personally liable under Section 58.
- **Insurance:** Likely denial of coverage due to "Late Reporting" breach.

CASE STUDY 2 – RANSOMWARE HOSTAGE (AIRASIA)

Detection

Nov 2022

Daixin Team Ransomware.

The Impact

5 Million Passenger & Staff records leaked. Hackers publicly stated they stopped the attack not because of AirAsia's defences, but because the network was so chaotic and disorganised that they got annoyed sifting through it.

The Tactic

"Double Extortion" (Encryption + Exfiltration). AirAsia refused to pay. From a 'Business Continuity' view, that is brave. But the hackers then published the data.

CASE STUDY 2 – RANSOMWARE HOSTAGE (AIRASIA)

The Incident: Nov 2022. Daixin Team Ransomware.

- **The Impact:** 5 Million Passenger & Staff records leaked.
- **The Tactic:** "Double Extortion" (Encryption + Exfiltration).

The Dilemma:

- **Option A:** Restore from backup (Ignores the data leak).
- **Option B:** Pay the ransom (Illegal? Unreliable? Stops the leak?).

Act 854 Reality:

- **Duty to Protect (Section 21):** The attackers mocked the "chaotic" security. Under Act 854, "chaotic security" is now evidence of negligence, punishable by up to RM 500k fine.

THE RISK MANAGER'S INCIDENT BATTLE PLAN

THE "6-HOUR" BATTLE PLAN

Time	Action	Owner	Act 854 ref.
T +00:00	Discovery & Triage is it critical? Activate SEMT immediately.	SOC/IT	S. 23 (1)
T +00:30	Legal privilege: Engage counsel before writing reports to protect discovery	Legal/Risk	-
T +01:00	The "Kill Switch" Decision: Disconnect the Network? (Stop spread vs. Business Loss)	SEMT	-
T +02:00	Draft Notification: Do not wait for perfect facts. Draft "Initial Notice" based on suspicion.	Comms/Risk	S. 23
T +04:00	Board/Insurer Alert: Notify insurer (Hotline) & Board. Do not breach "Late Notice" Clause.	Risk Manager	Policy
T +06:00	SUBMIT TO NACSA - Mandatory reporting via NC4S portal.	CISO/Risk	S. 23

THE "PPOSTTE" MODEL FOR REVIEW (POSTMORTEM)

- **Objective**: Move beyond "human error" to systemic resilience.

- **The Model (ACSC Framework):**

1. **People:** Did we have the right skills and fatigue management?
2. **Process:** Did the playbook actually work, or did we improvise?
3. **Organization:** Did Legal, Comms, and IT speak the same language?
4. **Support:** Did vendors (forensics/PR) deliver on their SLAs?
5. **Technology:** Did the tools (backups/EDR) fail or succeed?
6. **Training:** Was the team prepared for this specific scenario?
7. **Exercise:** Had we tested this decision path before?

Note: Adapted from ACSC - Australian Cyber Security Council

Q & A

THANK YOU