CYBER RISK: WHY BOARDS SHOULD TAKE IT SERIOUSLY!

A presentation by:

MURUGASON R. THANGARATNAM
Chief Executive Officer

novem CS
Bespoke Cyber Security

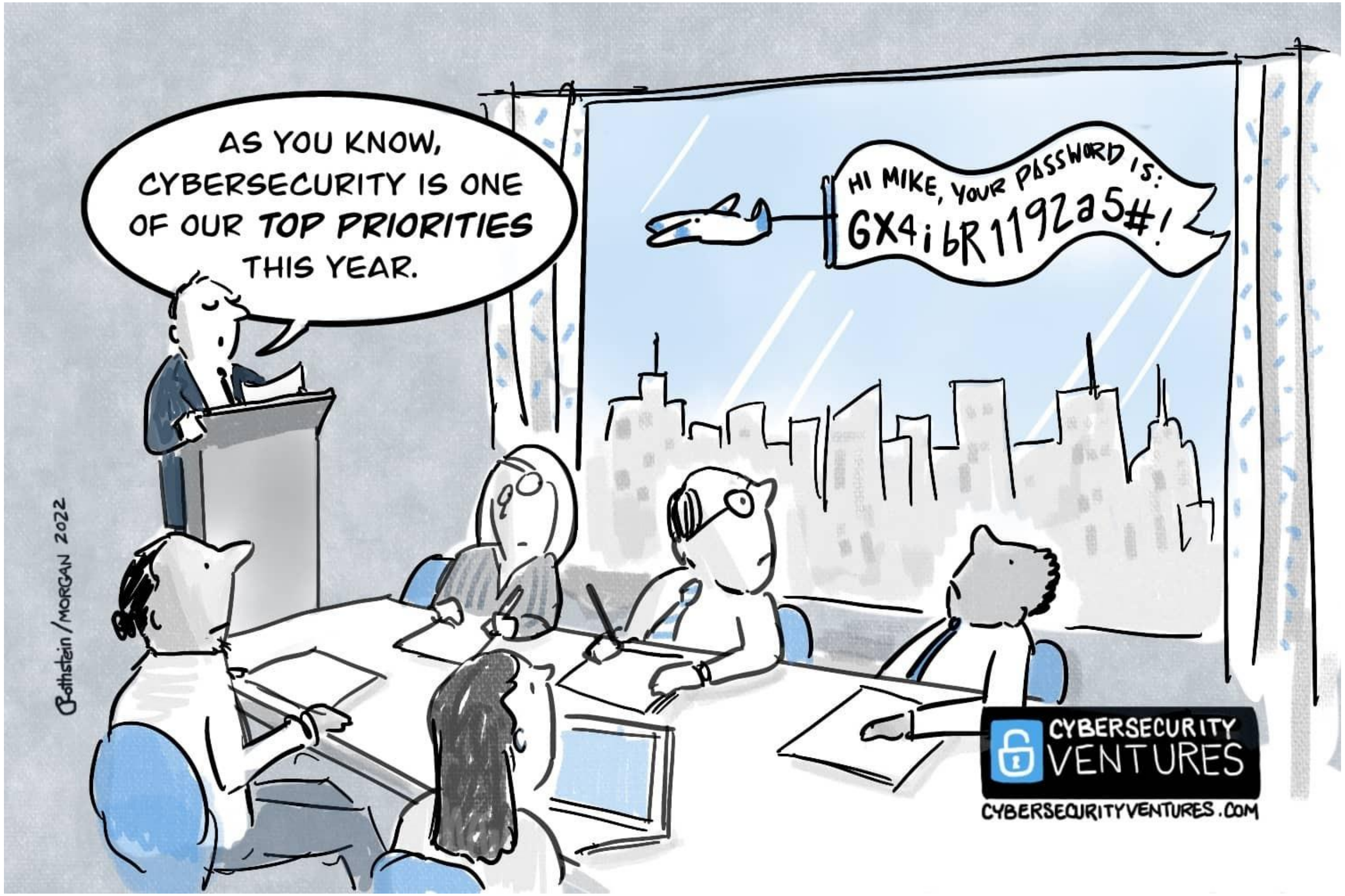
MDBC
Malaysian Dutch Business Council

MDEC™

CyberSecurity
MALAYSIA

About Novem CS

- **ESTABLISHED** NOVEM CS SDN BHD was established in 2019 focusing on bespoke cyber security solutions.
- **NOVEM CS** is a subsidiary of Advanced Security Network Sdn. Bhd., an established Ministry of Finance registered and Ministry of Home Affairs licenced company, since 1991.
- **FOCUS** is to provides clients with Managed Security Services, Incident Response Services, Threat Intelligence, Cloud Readiness, Business Continuity Planning and Security Awareness Training.
- **TEAM** of experienced subject matter experts in defence, telco network security, incident response, threat intelligence, cyber forensics, cyber security education and digital engineering.
- **CLIENTS** include leading healthcare group, government owned telco, international university, leading consulting firm, state agency, etc.
- **TRAINING PROVIDER** Novem CS is a registered training provider under HRDCorp.
- **AWARD WINNER** Novem CS was awarded the prestigious ‘Cyber Security Product (Innovation) of the Year’ at the CSM-ACE Malaysia Cyber Security Awards 2021.



AS YOU KNOW, CYBERSECURITY IS ONE OF OUR TOP PRIORITIES THIS YEAR.
HI MIKE, YOUR PASSWORD IS: GX4ibR1192a5#!
Rothstein/MORGAN 2022
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

CyberSecurity MALAYSIA MDEC™ MDBC Malaysian Dutch Business Council

Board NEEDS to know!

Cyber security is NO MORE about just protecting data!

Directors need a real picture of the cyber-physical and cyber-digital threats their organizations face. Digitized processes and operations, interconnected industrial control systems that enable remote management, supply chains with automated processes and increased usage of IoT, have exponentially increased the cyber threat landscape.

The BODs must be knowledgeable participants in cyber security OVERSIGHT!

The NIST framework has 5 areas: identify, protect, detect, respond, and recover. Document plans for each of these areas, share those plans with leaders, and practice the actions to be taken to build muscle memory for use in a breach situation.

Boards must FOCUS on risk, reputation, and business continuity!

The languages used to manage the business and manage cybersecurity are different, and this might obscure both the understanding of the real risk and the best approach to address the risk.

Approach to cyber security is DEFENSE-IN-DEPTH!

Layered protective measures safeguard valuable information and sensitive data because a failure in one of the defensive mechanisms can be backed up by another. This multi-layered approach is commonly referred to as the “castle approach”.

Cyber security is AN ORGANIZATIONAL PROBLEM, not just a technical problem!

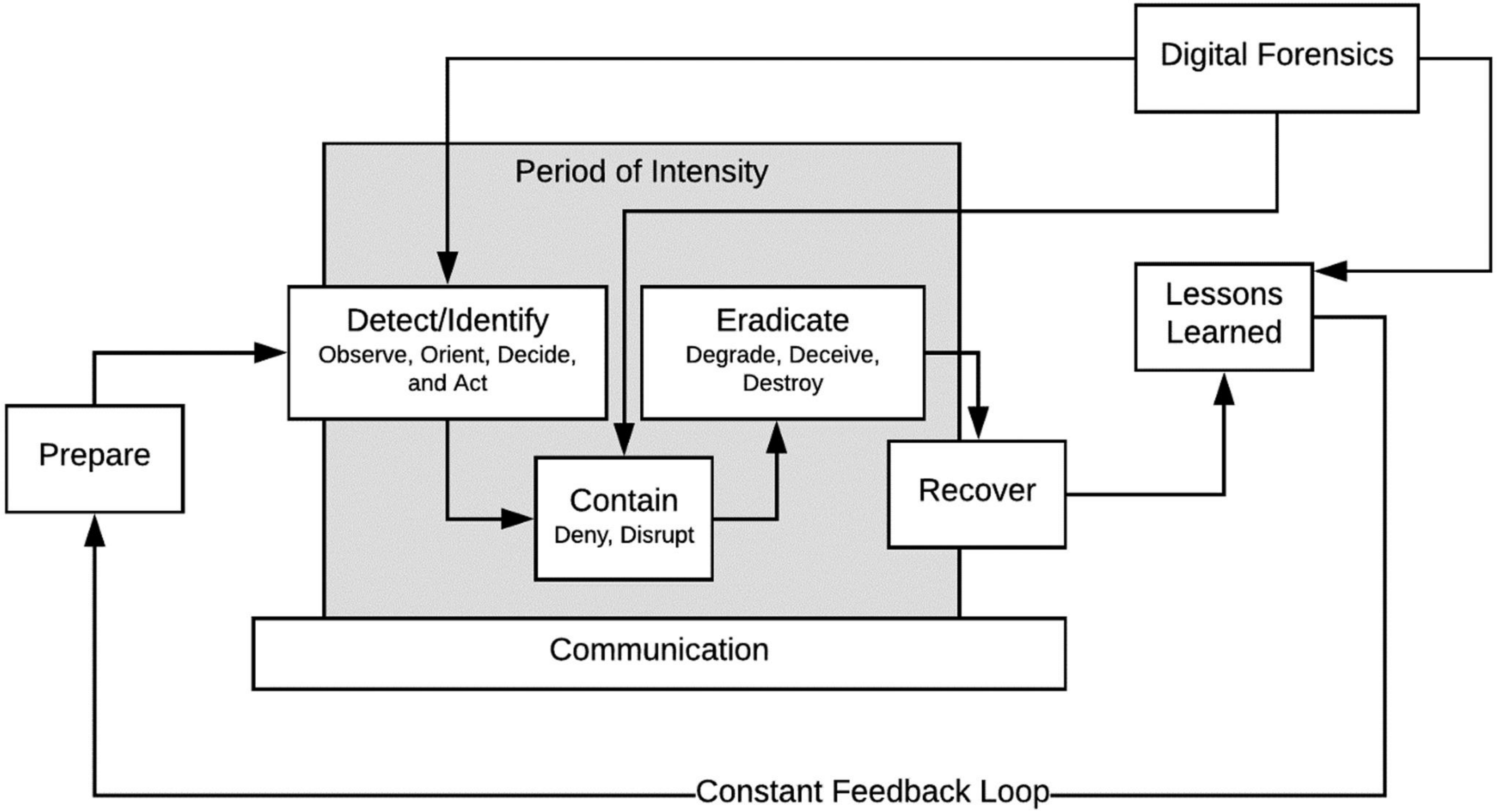
A study from Stanford University revealed that 88% of data breach incidents were caused by employee mistakes. Cyber security requires awareness and action from all members of the organization to recognize anomalies, alert leaders, and ultimately to mitigate risks. Organisation wide cyber culture has to be driven top down.

Questions for the Board!

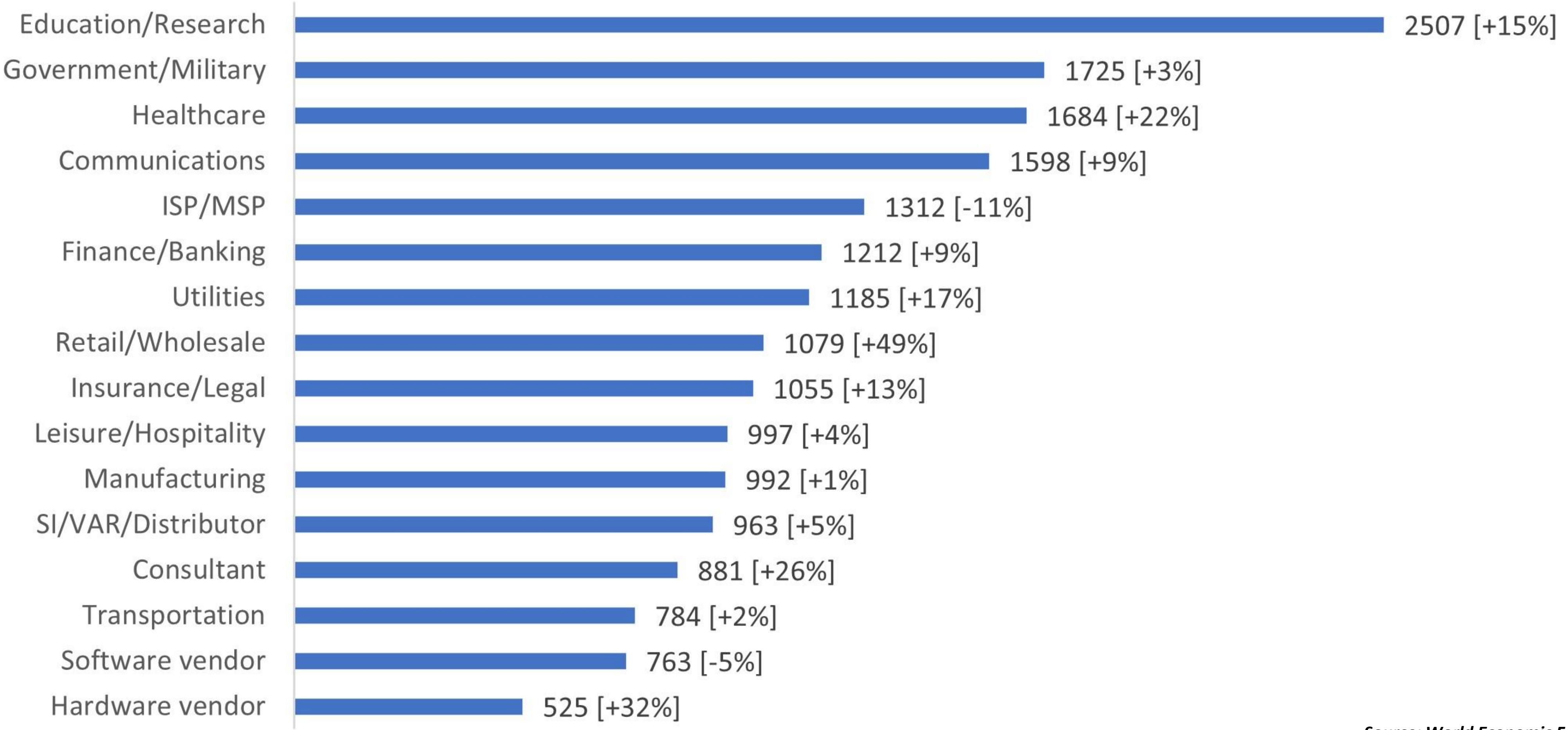
- What are our most important assets and how are we protecting them?
- What are the layers of protection we have put in place?
- How do we know if we’ve been breached? How do we detect a breach?
- What are our response plans in the event of an incident?
- What is the board’s role in the event of an incident?
- What are our business recovery plans in the event of a cyber incident?
- Is our cybersecurity investment enough?

DO YOU HAVE A CYBER SECURITY PLAYBOOK?

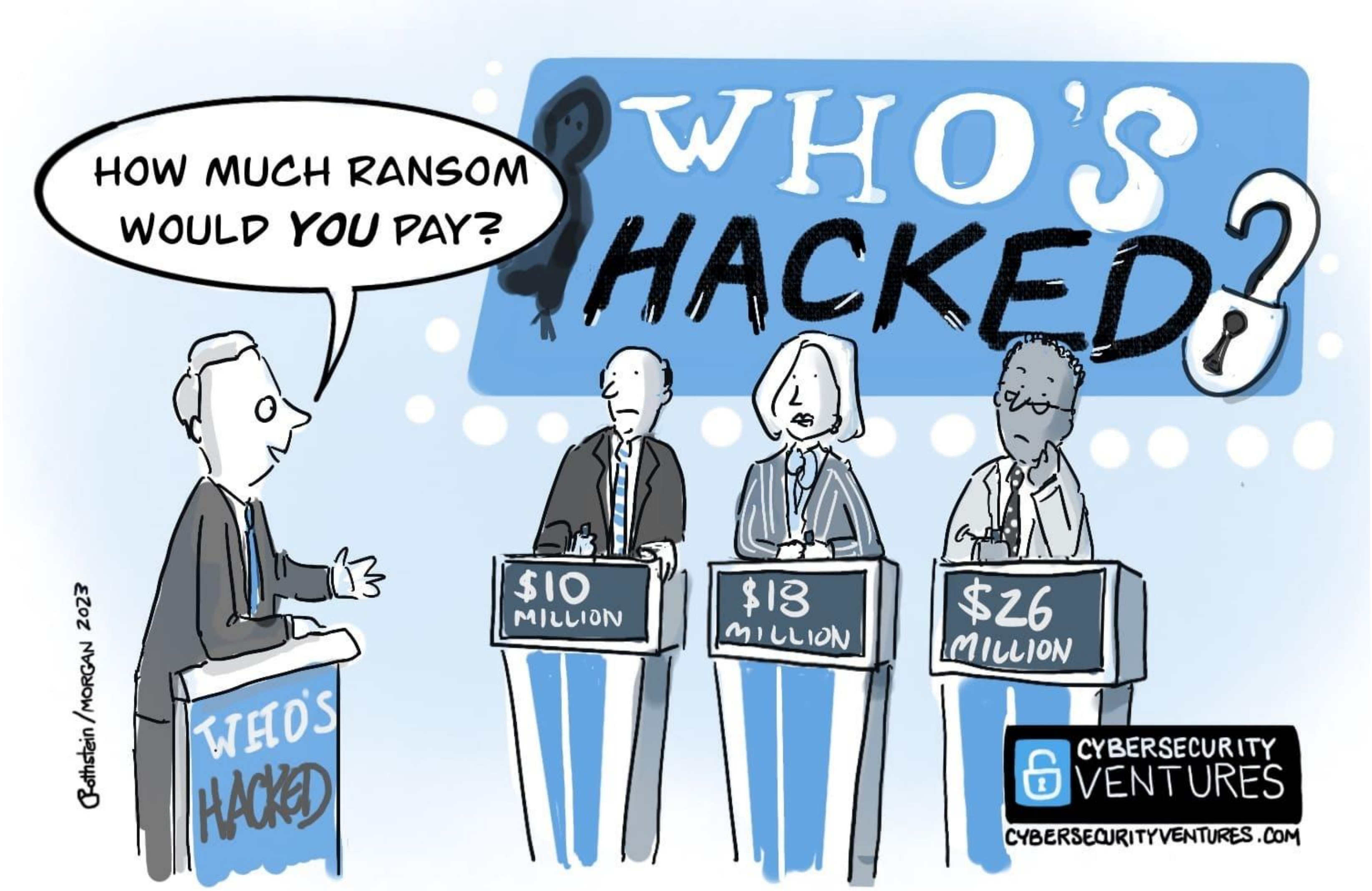
Modern Incident Response Life Cycle



Global Avg. Weekly Cyber Attacks Per Industry
(2022 Q1 Compare to 2023 Q1)



Source: World Economic Forum


WHO'S HACKED?
HOW MUCH RANSOM WOULD YOU PAY?
$10 MILLION
$18 MILLION
$26 MILLION
WHO'S HACKED
Rothstein/MORGAN 2023
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

Economic impact of Ransomware

66% of organisations reported significant revenue loss as a result of a ransomware attack. There is clearly an increase in ransom demands. 35% of businesses that paid the ransom demand shelled out between USD $350,000-$1.4 million, while 7% paid ransoms exceeding USD $1.4 million.

Companies spend millions of dollars on firewalls and secure access devices, and its money wasted because none of these measures address the weakest link in the security chain: the PEOPLE who use, administer and operate computer systems.

Kevin David Mitnick

CyberSecurity MALAYSIA MDEC MDBC Malaysian Dutch Business Council

MALAYSIA: COMING SOON!

- **CYBER SECURITY ACT** (expected December 2023)
- **AMENDED PERSONAL DATA PROTECTION ACT** (expected December 2023)
- **SC'S REGULATORY FRAMEWORK FOR TECHNOLOGY RISKS** (expected August 2023)

novem CS Bespoke Cyber Security

Cyber Hygiene – A Baseline

- Identify and prioritize key organisational services, products and their supporting assets.
- Identify, prioritize, and respond to risks to the organisation's key services and products.
- Establish an incident response plan and have a playbook.
- Regularly conduct cyber security education and awareness activities.
- Establish network security and monitoring.
- Control access based on least privileged and maintain the user access accounts.
- Manage technology changes and use standardized secure configurations.
- Implement controls to protect and recover data.
- Prevent and monitor malware exposures.
- Manage cyber risks associated with suppliers and external dependencies.
- Perform cyber threat and vulnerability monitoring and remediation.

In the world of cyber security,
the last thing you want is
to have a target painted on you!

Tim Cook

Security is not an expense.
It is an INVESTMENT AGAINST LOSS!

Thank You!

Murugason R Thangaratnam

☎ +6016 262 2224

✉ muru@novemcs.com