



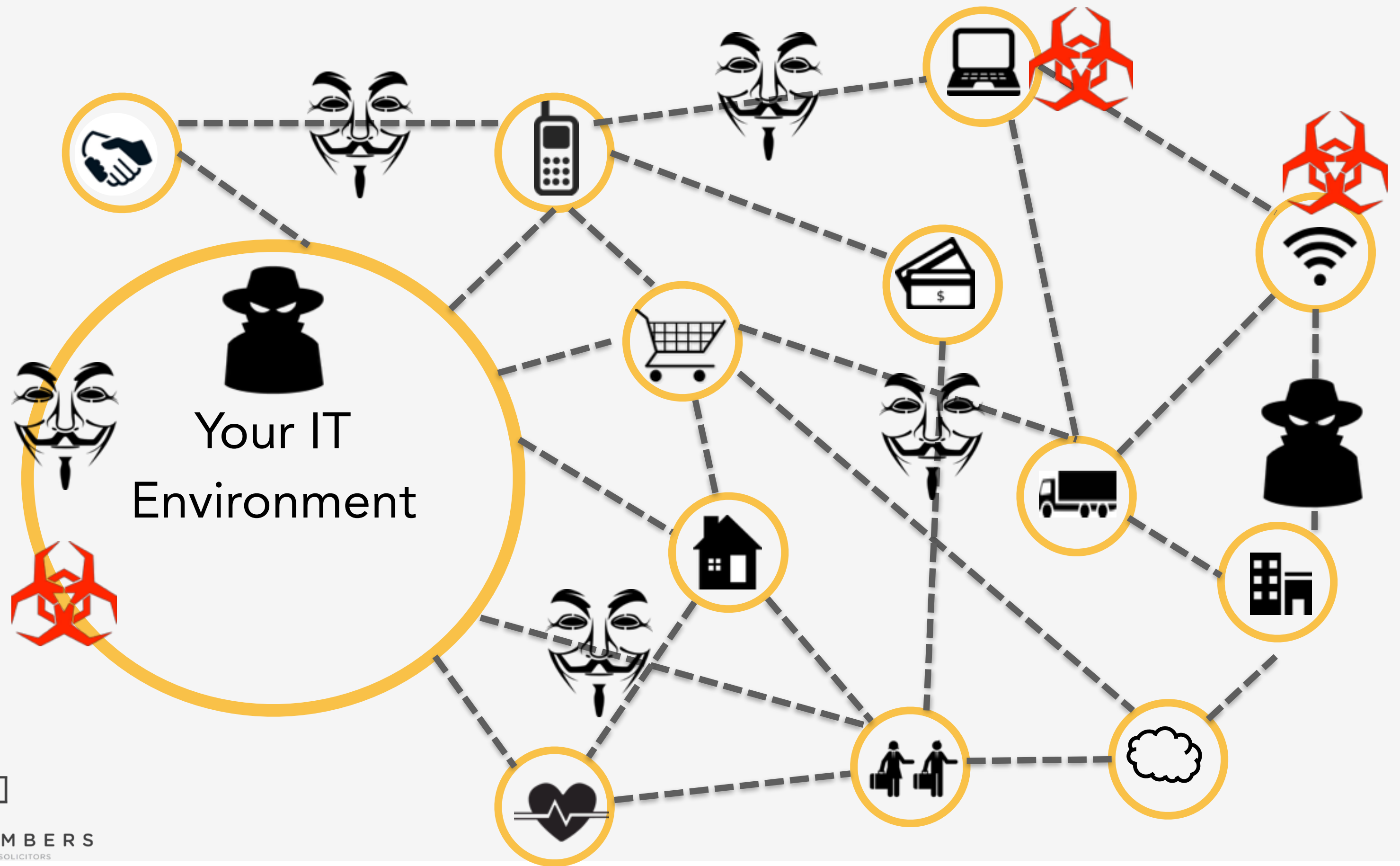
SK Chambers Lunch Talk Series 03

Cybersecurity: Corporations
and the Cloud



Your IT Environment





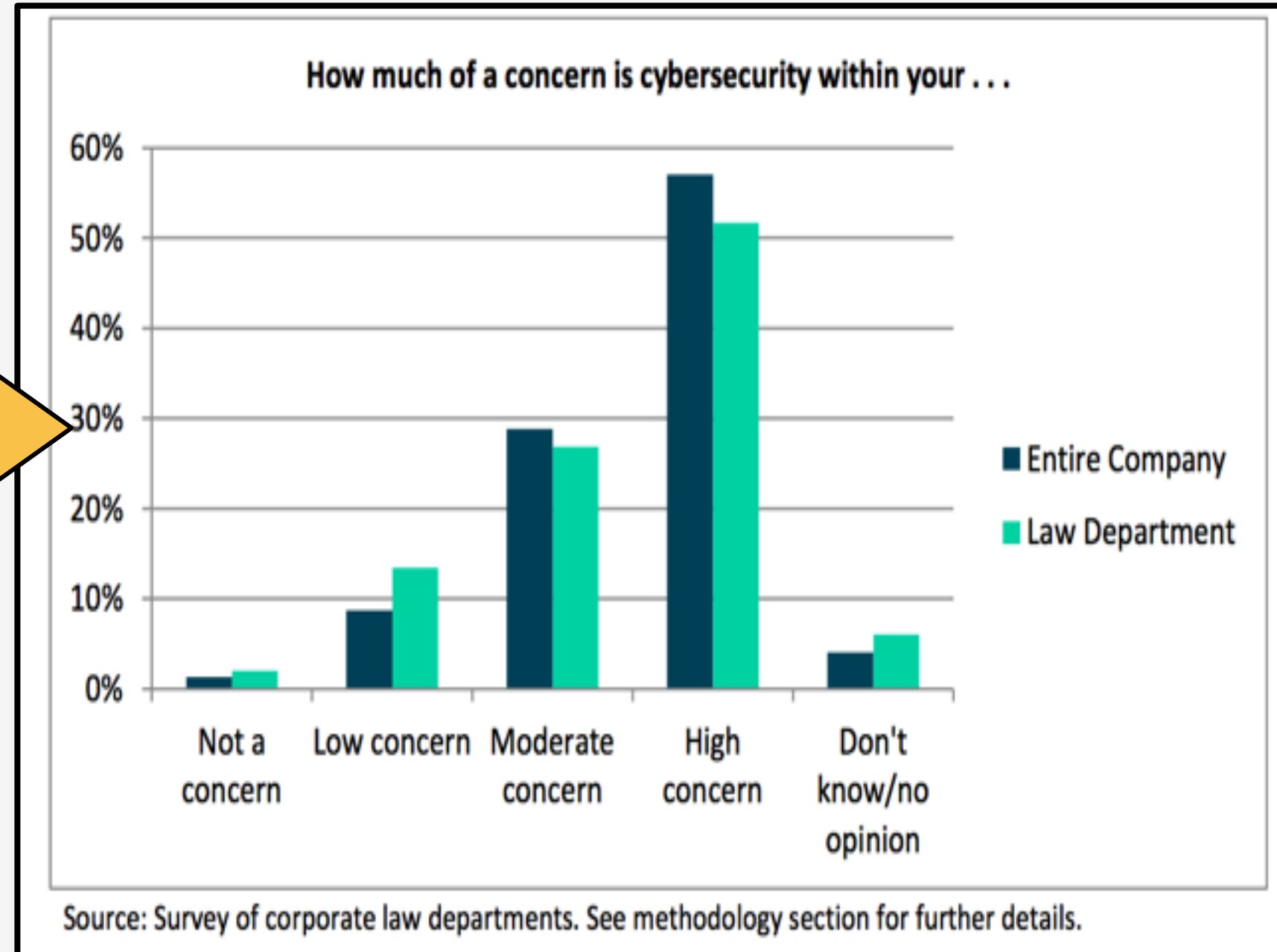
Cybersecurity: Challenge

The Cyber Scene is evolving...are you?



Level of concern about Cybersecurity Among Corporate Counsel

Cybersecurity is a major concern for companies including their Law Departments



Corporate Counsel's Top Concerns for Cybersecurity



Highest levels of concern relate to reputation damage With Customers & Loss of Intellectual Property



Cybersecurity : Some home-truths

They will get in.

- Cyber attacks are inevitable
- Defences lag Attackers



Cybersecurity : Some home-truths

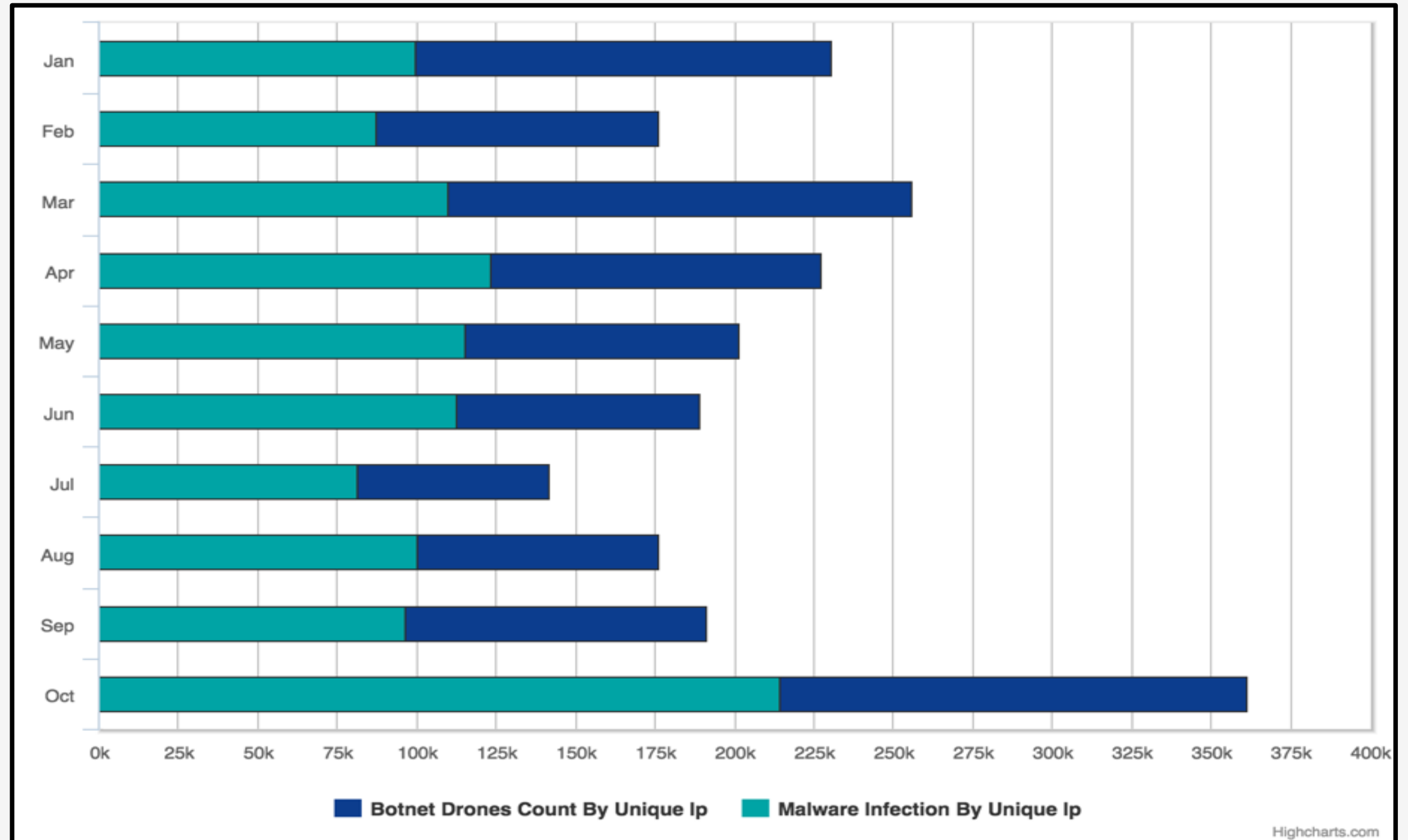
Malaysia is not immune!

- Not just a US problem



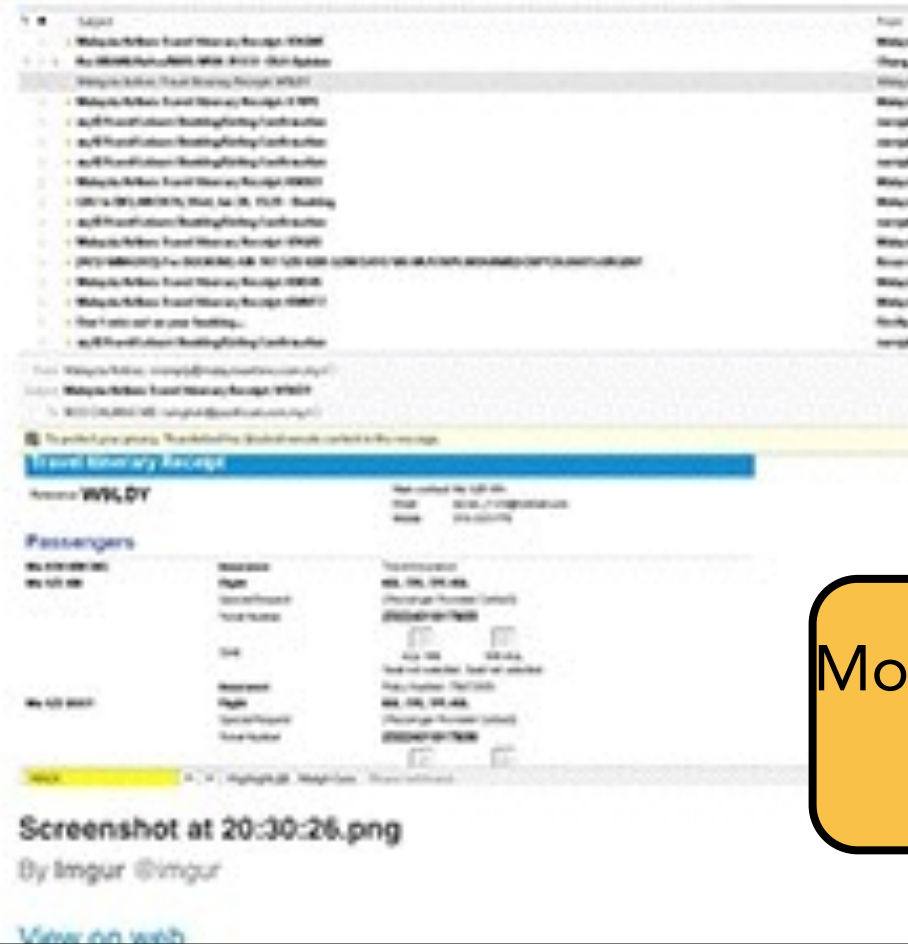
Malaysia Botnet Drones And Malware Infection 2015

According to MyCert* in October alone, 214,387 cases of Malware infection & 146,924 cases of Botnet Drones traced





lololol imgur.com/7j4BsdU



Police: ATM heist syndicate used computer virus to steal money

50 3 0 2 1
Share Tweet Share Email G+

TOOLS INCREASE TEXT DECREASE TEXT RESET TEXT PRINT
ARTICLE



Money stolen from ATM
through virus

A tweet by LizardSquad
of leaked screenshots
of bookings made by Ministers

IRCANONOPS.LI
#OPMALAYSIA
PORT: 6667

WEDNESDAY,
JUNE 15
7:30 PM
GMT



TARGET: HTTP://WWW.MALAYSIA.GOV.MY
OPERATION MALAYSIA

IRCANONOPS.LI
#opMalaysia
Port:6667

Date:04/07/11
Time:13:37GMT

Target: WWW.PMO.GOV.MY



**YOUR GOVERNMENT
HAS FAILED YOU.**

Democrats and Republicans also sit atop Capitol hill and abuse their power. They are deaf to the will of the people; they pass bills that strip away your rights and your dignity. They laugh as they use their influence to gather personal wealth, uncaring as they crush the average citizen in the process. The system is broken.

But we can fix that.

A Vote For Anonymous is a Vote For the People.

ANONYMOUS 2012.

NEVER FORGET - NEVER FORGIVE - VOTE LEGION

Defaced Government's
websites
by Anonymous

Singapore's Straits Time's website defaced and hacked by Anonymous.

IDA warns users about SingPass phishing email

POSTED: 25 Jun 2015 12:52 UPDATED: 25 Jun 2015 14:03



SINGAPORE: Users of SingPass, the gateway to e-Government services, were warned by the Infocomm Development Authority of Singapore (IDA) on Thursday (Jun 25) not to fall for a phishing email making the rounds.

ST's Home Ground

Anonymous: Message to straitstime, you just got hacked.

"ST is tempting fate" - newstation.sg Greetings Irene Tham & Straitstimes.com, I am The Messiah from the Anonymous Collective. We are a decentralized non-violent resistance movement, which seeks to restore the rule of law and fight back against the organized criminal class. We oppose any form of internet censorship among other things. Allow [...]

Email

Print

0

Tweet

0

Share

Published on November 1st, 2013



By Irene Tham
Correspondent
itham@sph.com.sg

IT'S GREAT TO BE
SINGAPOREAN TODAY



A's Facebook post, some SingPass users have received an email titled "Account security info verification" from "SingPass Government Support Center". The email contains a link to a Singpass-security.com website and a suspension notice.

at this is a
ot click on
sonlogic.c

iminally fr
e persona
asswords,

The phishing emails purported to be from support@gebiz.gov.sg. GeBIZ is a government-to-business (G2B) public e-procurement business center where suppliers can conduct electronic commerce with the Singapore government.

The fraudulent email advised GeBIZ trading partners to complete a one-time account update following the roll-out of the enhanced SingPass system. User credentials were stolen when users entered their username and password on the phishing page.




Cybersecurity : Some home-truths

**What you do and how
you manage data security
is driven most
significantly by the law.**

•  Not just an issue for tech.

Cybersecurity : The Basic Question for Boards



*Are we doing enough to protect our assets
and minimise risk?*

Falls upon legal counsel guide Boards &
CTOs, CIOs answer this question



In legal speak, this translates to the following legal questions...

Are we discharging our duty of care (D.O.C)?

What is the standard of care (S.O.C) by which we will
be assessed?

Are our measures reasonable?



What is the applicable S.O.C?

Compliance

- A Cybersecurity compliance program is a good start
- Not much direct law now so compliance alone may not be enough
- Legislation & Sectors specific rules exist
-

Emerging

Laws

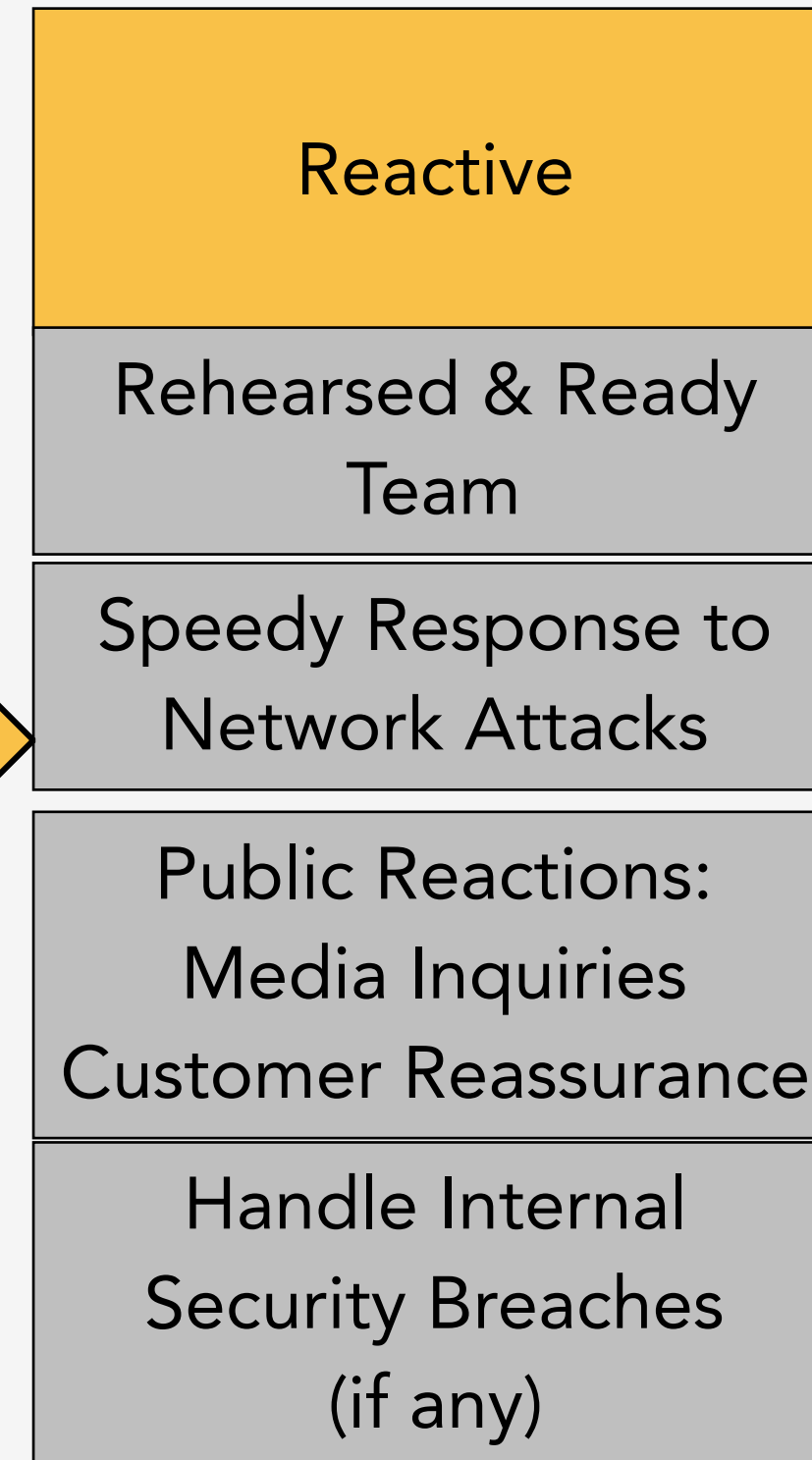
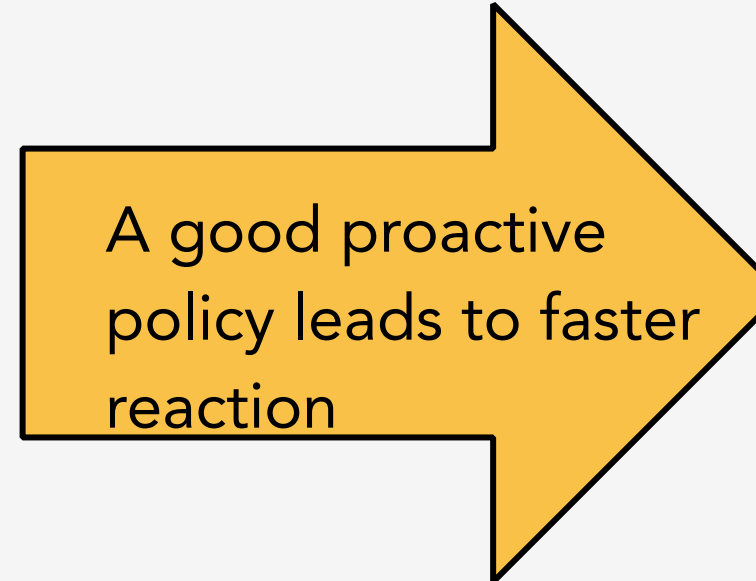
- Track evolving sources of standards
- Case law, statements by the exchange or securities regulator
- Widely accepted industry standards

• Periodic

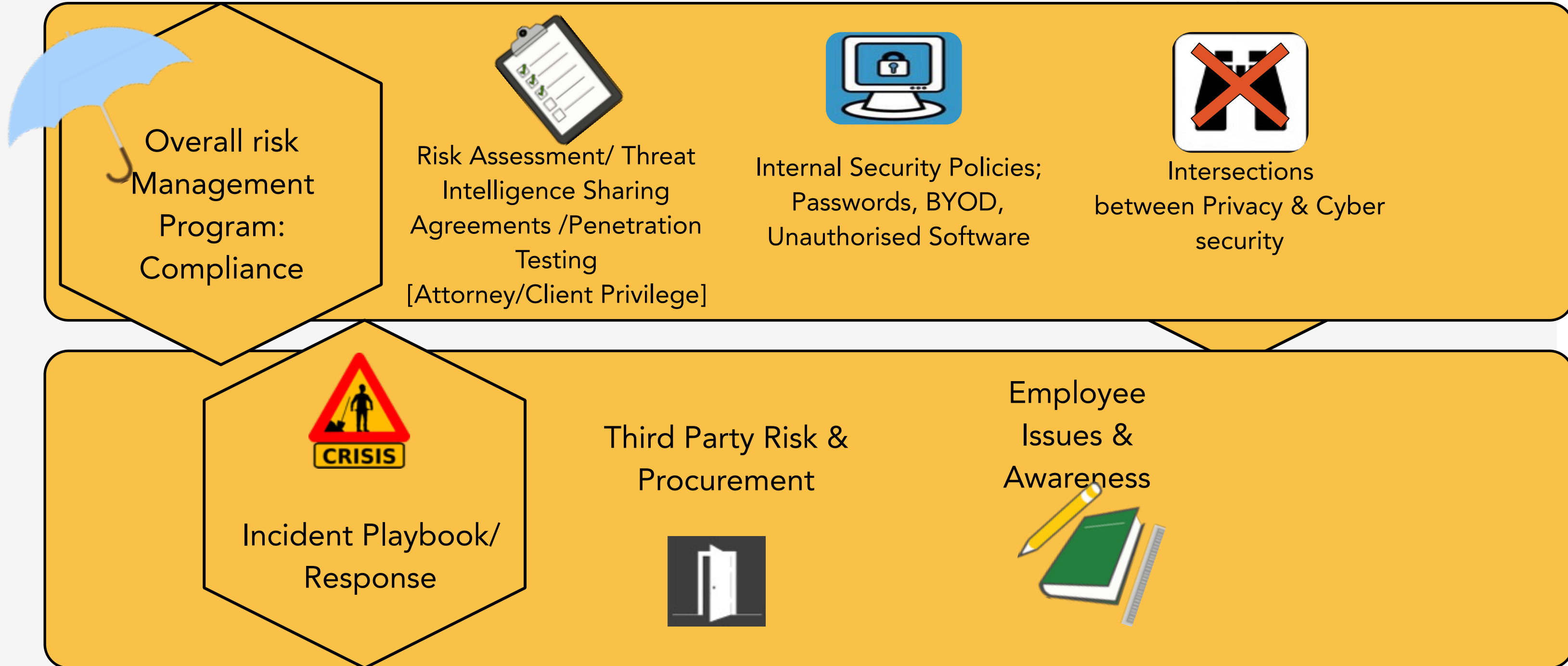
review of



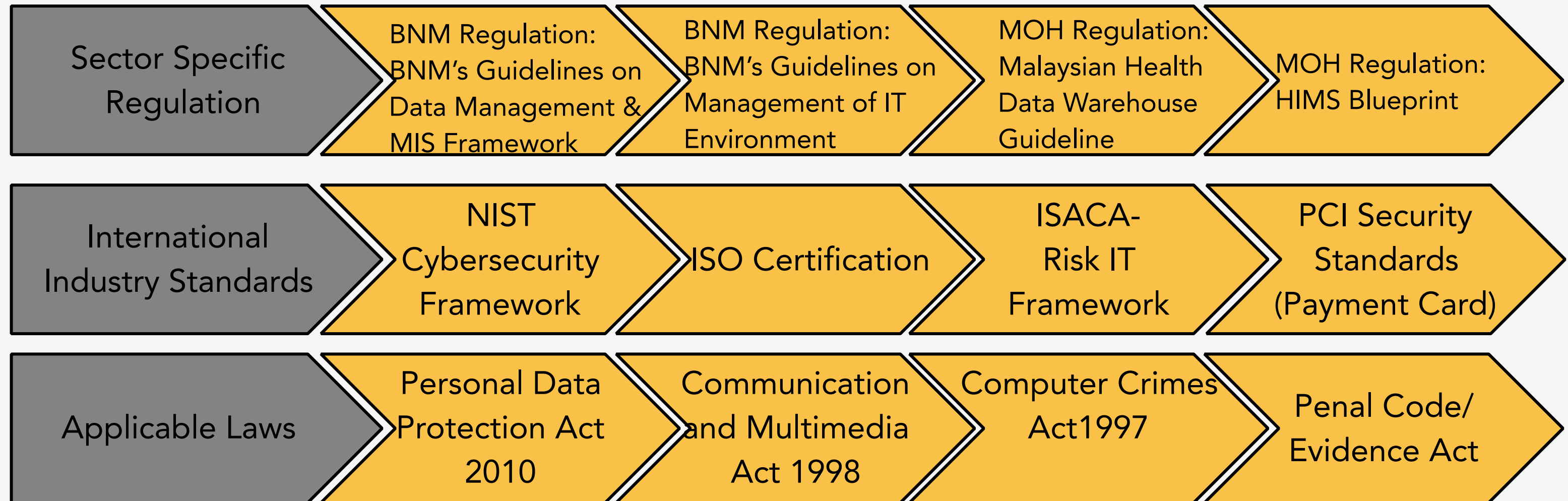
Block and Tackle Approach to action the S.O.C



Critical Legal Input: Cybersecurity Issues



Cybersecurity Law: Complex & Multi Disciplinary



...and the list is growing!



Internal Security & Privacy Policies



Security

Internal security policies

Threat intelligence-sharing arrangements

Check for gaps in security policies, attorney client privilege



Privacy

Workforce monitoring to detect "Insider Threats"

Cross-border/domestic privacy restrictions

Information sharing with Govt & other companies



Contract Review: Third Party Risk & Procurement

Third Party Risk
& Procurement



The Cloud brings new
Challenges – Govt.
access

Contract Checklist

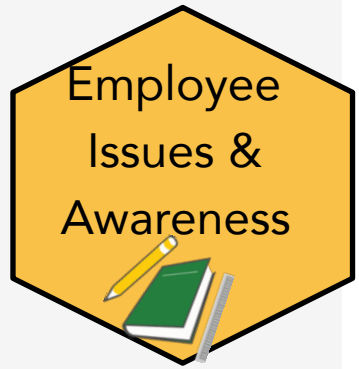
- ☒ Properly Secure Information
- ☒ Notify immediately if information is lost or compromised
- ☒ Indemnify you for costs associated failure to secure/
third party's misuse
- ☒ Rights of audit /Full cooperation in the event of breach

Customer Contract Mitigation

- ☒ Disclaimers for cyber breaches from confidentiality provisions



Employee Issues & Awareness



Issues

Labor & Privacy Laws

Communicate
Risk

Management
Oversight

Policy on violations

Protocol for
suspected
employees

Education &
Training

Actions

Revise Policies &
Document Revision

Be Creative
& Catchy

Get management
on board

Use Actual Examples

Have Clear Policies

Promote education
& awareness



The Incident Playbook



- ☒ Identify key players
(Communications, CISO,
Corporate Security, Business)
- ☒ Assign clear roles &
responsibilities
- ☒ Close alignment with legal
- ☒ Have a shortlist of external
counsels & IT forensic specialists

- ☒ Highly visible incident reporting
process & education
- ☒ Internal and External
Communications
- ☒ Test and plan for both crisis
& more routine incidents;
table top incident role play
sessions



Handling an Incident - Realtime



- Priority: Stop the Bleed, Identify the Source of Attack
- Structure response: Establish central "command" to coordinate interactions
- Protect attorney-client privilege (ACP)
- Preserve Evidence
- Interact with law enforcement – Coping with Info demands
- Comply with data breach notification laws both in Malaysia and abroad
- Assess potential liability as well as court orders to stop the bleed or seek info
- Payment cards industry investigator – not acting for you
- Be prepared to handle the media – what to say, how much.



Cybersecurity Issues: Your Critical Legal Needs

- 1 Compliance with laws and standards – Review security policies
- 2 Assessing Risk – Threat intelligence sharing agmt /Gap testing (ACP)
- 3 3rd party providers / customer contracts – Policies & Contract review
- 4 Employee Issues & Training
- 5 Advising on privacy laws – data transfers, govt. access, employee
- 6 Developing and reviewing incident playbook
- 7 Handling an incident



Thank you