

JENAYAH SIBER: KESELAMATAN TRANSAKSI SECARA DALAM TALIAN

RAFIDAH ABDUL HAMID
CYBERSECURITY MALAYSIA
16/8/2016



Agenda

- Cyber Threat Landscape
- Online Transaction Security Issues
- How to Govern and Assure Cyber Security in Organisations?
- Mode of Incident Referrals



Cyber Threat Landscape



The World Today is **HIGHLY CONNECTED**



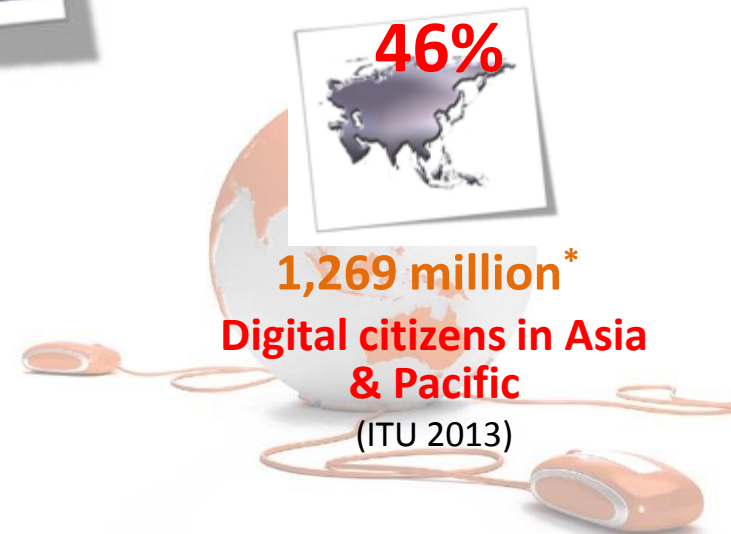
19.2 mil

Digital citizens in Malaysia

(Malaysia Communication and Multimedia Commission 2013)

2,749 million*
Digital citizens worldwide
(ITU 2013)

5 billion in 2015
(Nokia Siemen)



The World Today is HIGHLY CONNECTED



**JAN
2015**

DIGITAL IN MALAYSIA

A SNAPSHOT OF THE COUNTRY'S KEY DIGITAL STATISTICAL INDICATORS

TOTAL
POPULATION



we
are
social

**30.5
MILLION**

URBANISATION: 73%

FIGURE REPRESENTS TOTAL NATIONAL
POPULATION, INCLUDING CHILDREN

ACTIVE
INTERNET USERS



we
are
social

**20.1
MILLION**

PENETRATION: 66%

FIGURE INCLUDES ACCESS VIA
FIXED AND MOBILE CONNECTIONS

ACTIVE SOCIAL
MEDIA ACCOUNTS



we
are
social

**16.8
MILLION**

PENETRATION: 55%

FIGURE REPRESENTS ACTIVE USER
ACCOUNTS, NOT UNIQUE USERS

MOBILE
CONNECTIONS



we
are
social

**41.8
MILLION**

vs. POPULATION: 137%

FIGURE REPRESENTS MOBILE
SUBSCRIPTIONS, NOT UNIQUE USERS

ACTIVE MOBILE
SOCIAL ACCOUNTS



we
are
social

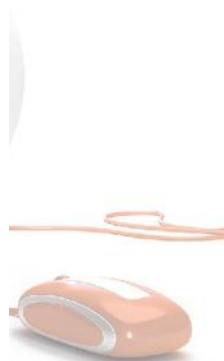
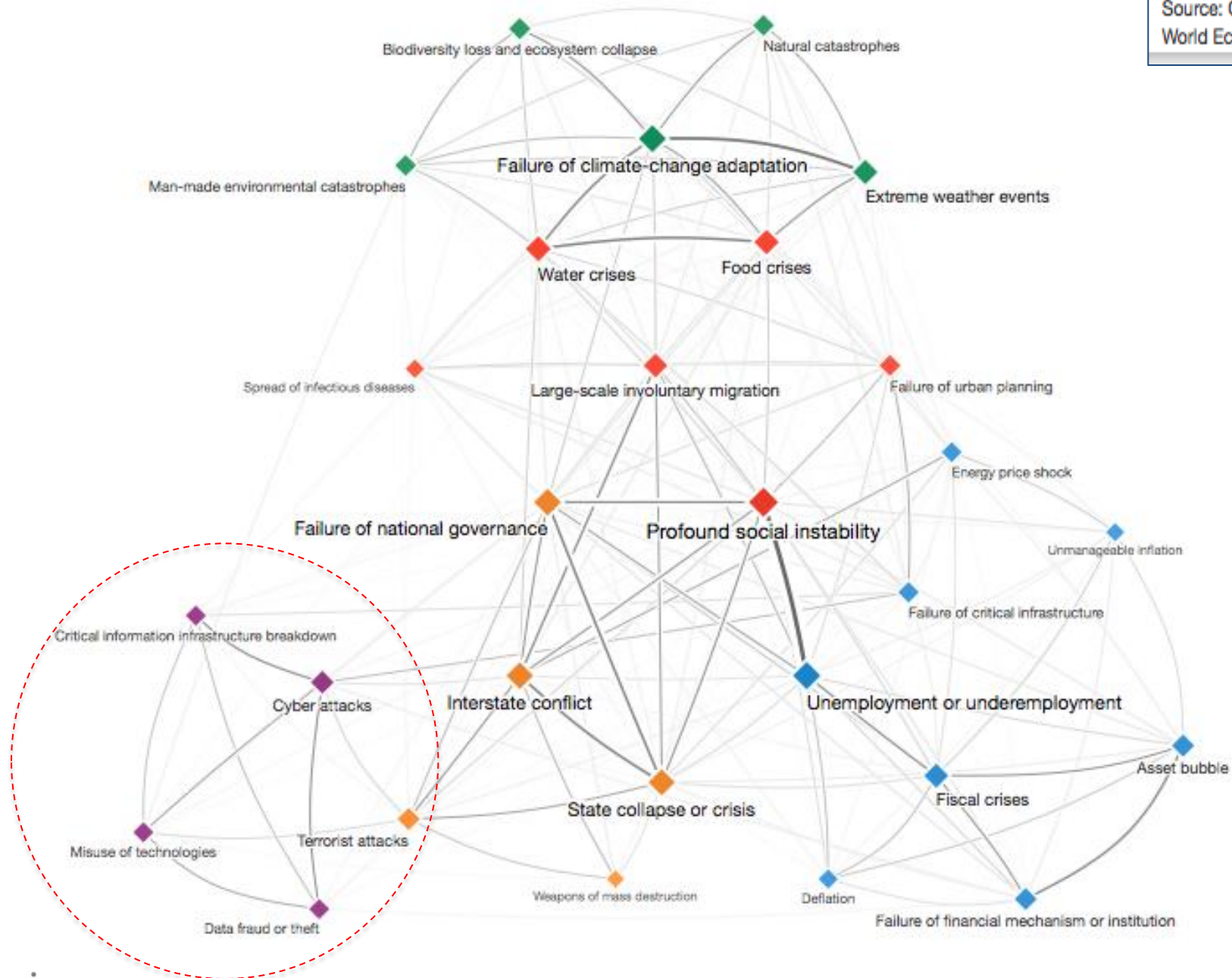
**15.0
MILLION**

PENETRATION: 49%

FIGURE REPRESENTS ACTIVE USER
ACCOUNTS, NOT UNIQUE USERS

Survey respondents were asked to identify between three and six pairs of global risks they believe to be most interconnected.

Source: Global Risks 2015 Report,
World Economic Forum



Trends of Computing

Technology Is Double-Edged Weapon

Mobile Devices



**Free
WiFi
Hacking Tools**

Big Data

VOLUME
Large amounts of data.
VELOCITY
Needs to be analyzed quickly.
VARIETY
Different types of structured and unstructured data.

Internet of Everything
(people, process, data, things)



New Technologies Introduce New Security Issues



ICT as Business Enabler vs Escalation of Cyber Threats



Cloud Services: Trade-off between security and efficiency

** Data can be unencrypted*

** Is the Cloud secured?*



Internet of Things: Everything is connected

** Spread various kinds of malicious software i.e. Adware, bots, bugs, rootkits, spyware, trojan horses, viruses and worms*



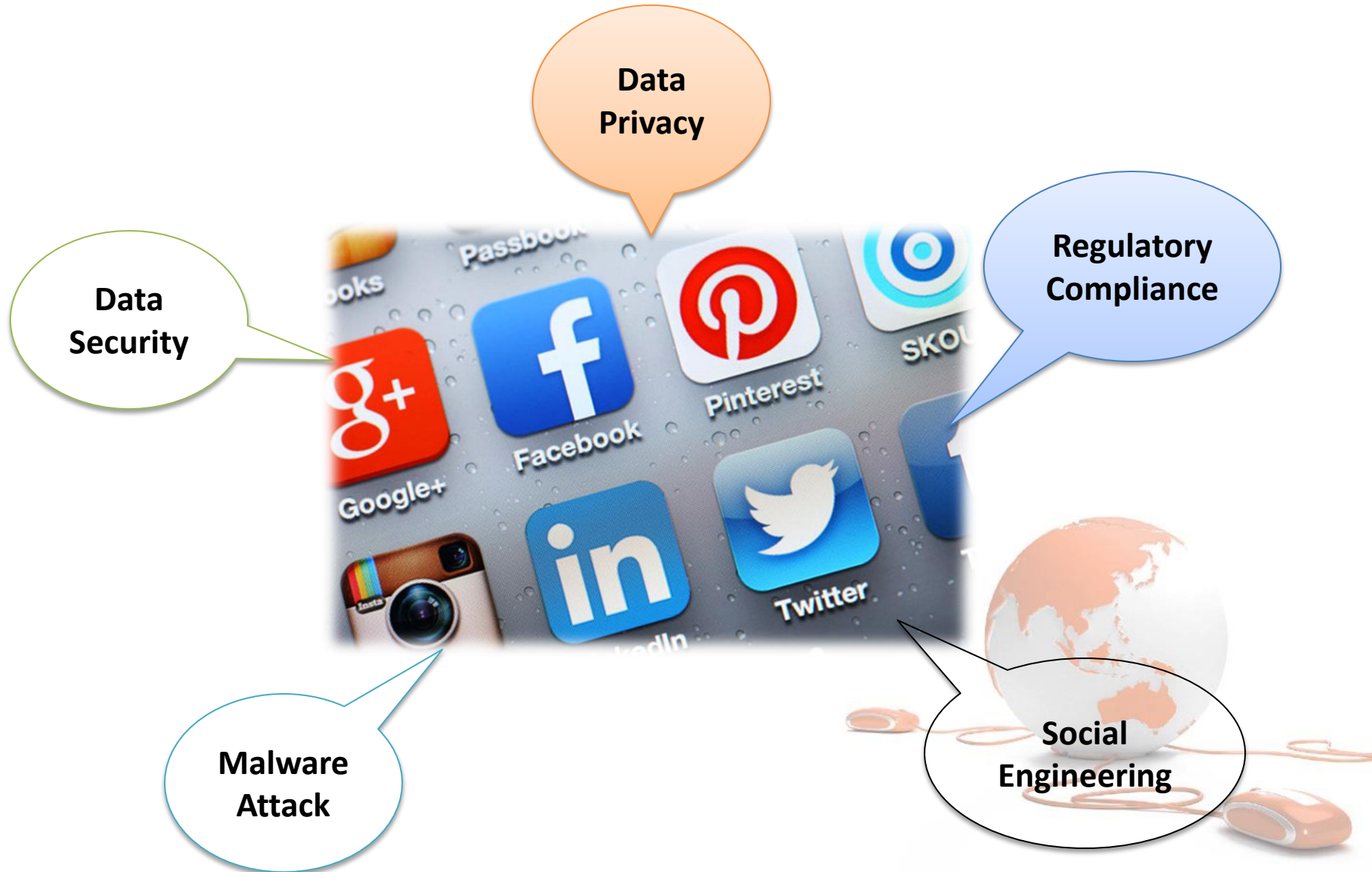
Mobile Devices: They are part of ecosystem, but organisations do not control

** Data loss/leakage * Devices maybe insecure*

** Abuse functions or unauthorised access as a result of malicious software*

The Use of Social Media:

Reduced the cost of content creation, distribution and discovery methods BUT



Easy access to Hacking tools

- Hacking tools can be downloaded from the Internet and applied with limited system knowledge
- Manual and training videos on attacking control systems (SCADA/DCS) are publicly available (Tutorial, Youtube, etc)

Ads by Google

SCADA Training Classes and Programs

Automation Courses

[home](#) : [Automation](#) : [SCADA](#) [go up..]

[Ads by Google](#) [SCADA Database](#) [SCADA Data Collection](#) [SCADA Controller](#) [SCADA Hardware](#)

SCADA Training Classes

SCADA stands for Supervisory Control And Data Acquisition. As the name indicates, it is not a full control system, but rather focuses on the supervisory level. As such, it is a purely software package that is positioned on top of hardware to which it is interfaced, in general via Programmable Logic Controllers (PLCs), or other commercial hardware modules.

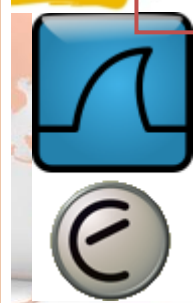
Are you a SCADA training provider?
You could be on this page today - for FREE!

Search for Training
What do you want to learn about?

Some important terms: automation,scada,plcs,control modules plcs,plc,cnc,scada,automation,industrial automation

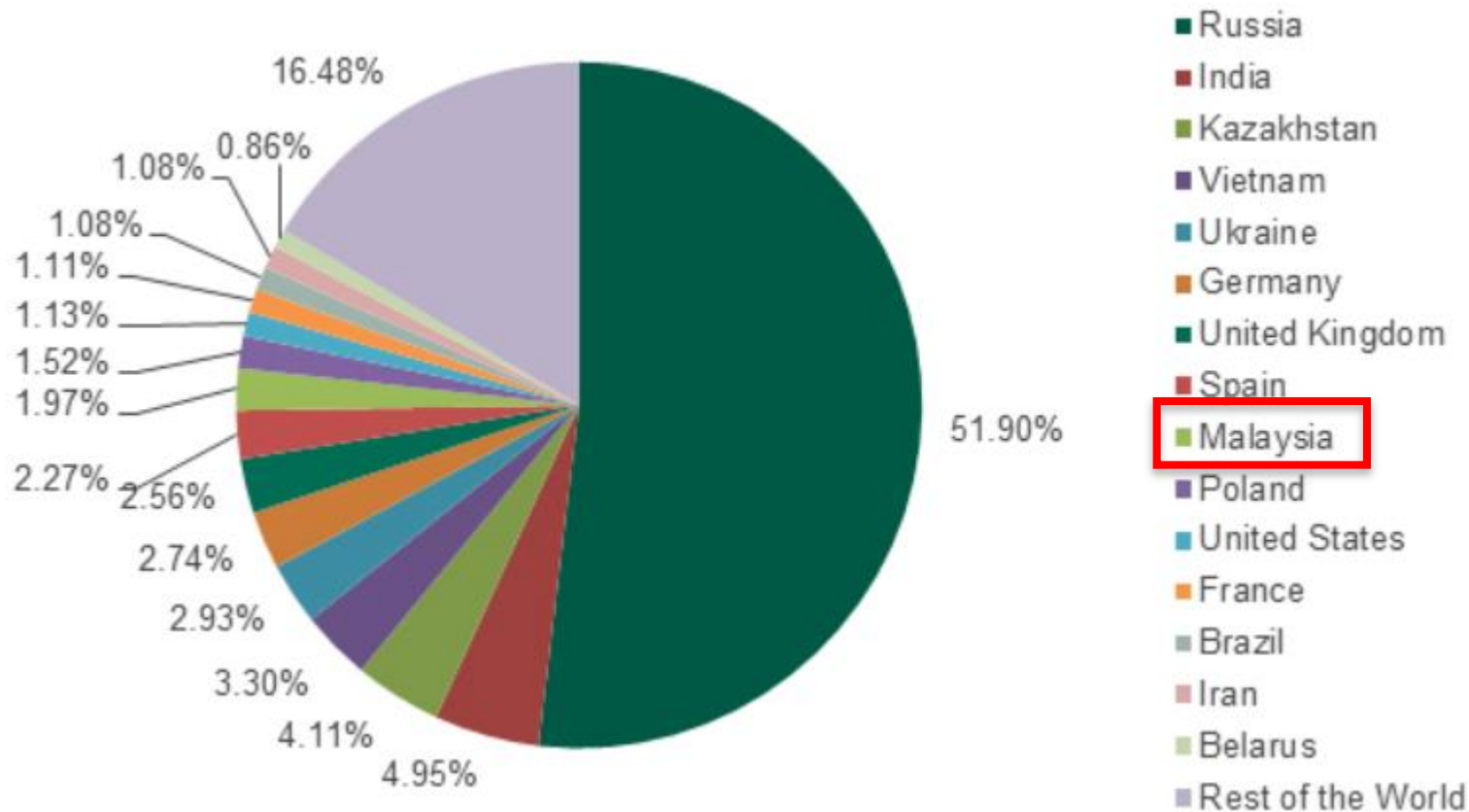
Related Keywords: [automation](#) [scada](#) [plcs](#) [control modules](#)

online course instructor led class learn at home group study self directed training cd based training DVD based training printed book e-book digital book workshop seminar train the trainer computer based learning on sale discounted pricing



ISSUES & CHALLENGES

- Malaysia Ranked 9th In Malware Attacks



Top 15 countries with highest numbers of users attacked between April 2013 and July 2014. Malaysia: 1.97% out of 3,408,112 malware attacks

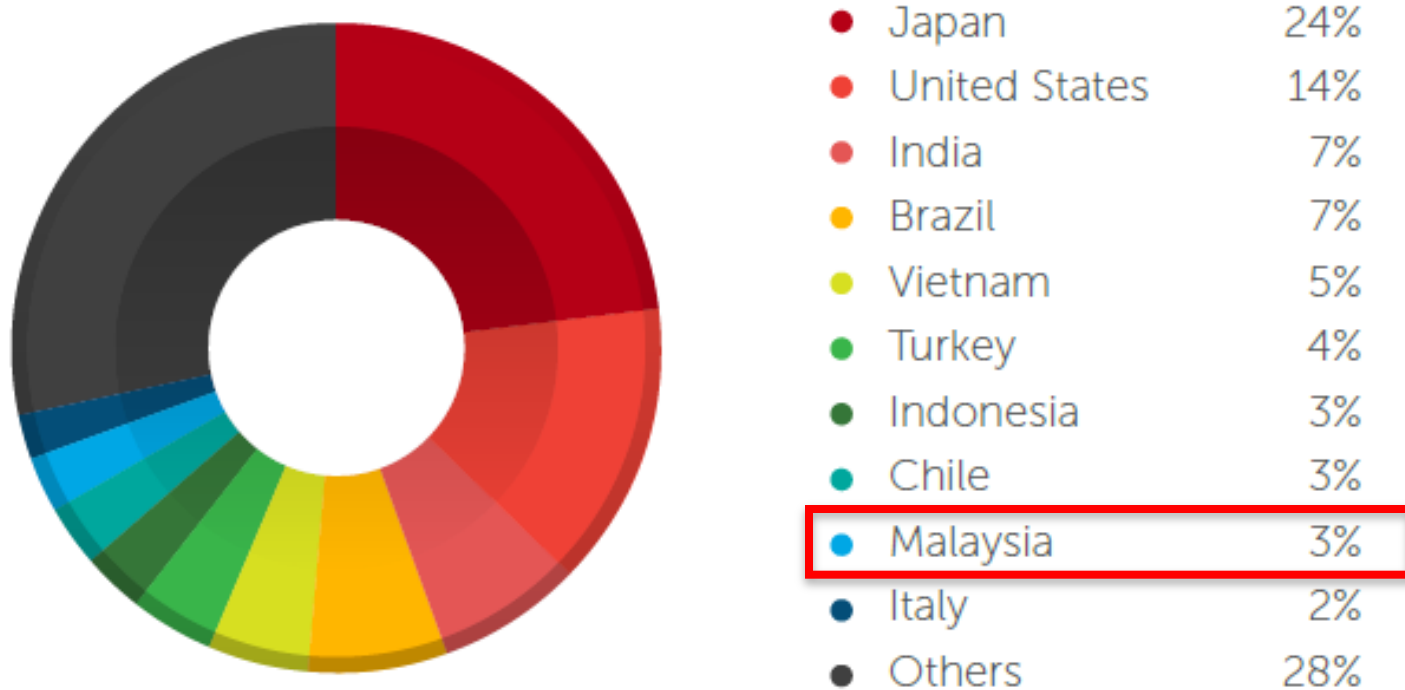
Source: Mobile Cyber Threats. Kaspersky Lab & INTERPOL Joint Report, October 2014

Copyright © 2016 CyberSecurity Malaysia

ISSUES & CHALLENGES

- Online Banking Malware Attacks

Countries Most Affected by Online Banking Malware, 2Q 2014



Source: TREND MICRO – TrendLabs 2Q 2014 Security Roundup

Online Transaction Security Issues



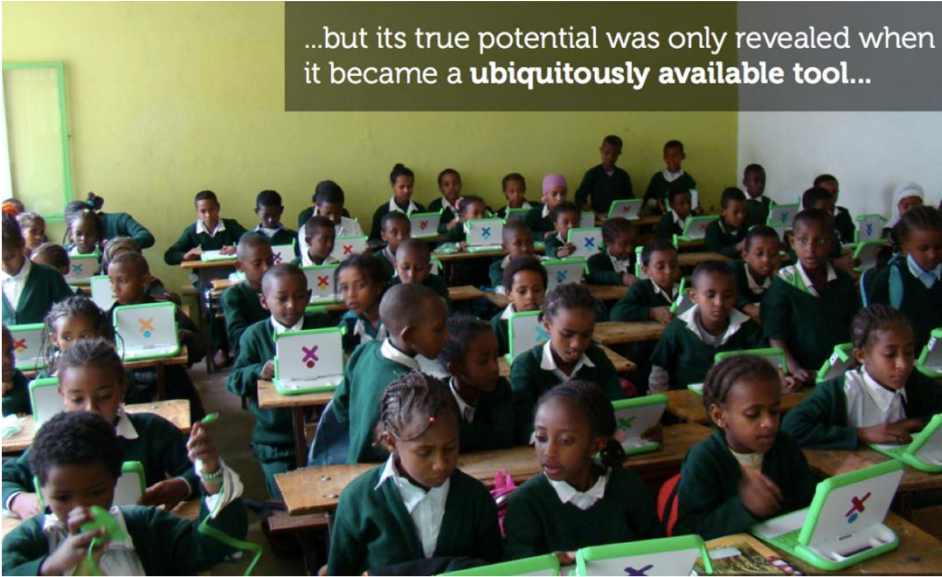
Harvesting Opportunities



“All one needs is a computer, a network connection, and a bright spark of initiative and creativity to join the economy”

Don Tapscott & Anthony D. Williams, Wikinomics

...but its true potential was only revealed when it became a **ubiquitously available tool...**



A Sizeable & Growing Market

- Globally, Digital Economy contributed **35%** to Global Trade (US\$17 trillion) in 2009
- Total Worldwide ICT Spending was expected to grow 3% to **US\$4.1 trillion** in 2011
- Global e-Commerce revenues will hit **US\$3.8 trillion** by 2020
- Malaysia e-commerce transaction (2011) **RM824 million**
- Malaysia e-commerce expected to surpass **RM1.9 Billion in 2016**

Source:
ITIF March 2010
Digital Planet WITSA, 2010
TMX News, Oct 2010
Euromonitor



Reasons: Users not doing Online Shopping

- 56.35% : Safety Issues
- 50.79%: Unreliable

(Source : IDC research)



thestar
online  **7/10** online users
are willing to spend/ spend
more online if the internet
safety measure are improved

79%
Of People Who Spend
49+hrs/Week Online
Have Been Victims Of
Cybercrime



Kes tipu dalam talian babit kerugian RM15j

» 4,792 laporan diterima sejak Januari 2011 hingga Julai lalu

Oleh Nor Fazlina Abdul Rahim
 nfazlina@bharian.com.my

► Kuala Lumpur

Mangsa penipuan e-dagang mencatatkan kerugian terkumpul sehingga RM15 juta dalam tempoh antara Januari 2011 hingga Julai lalu.

Jumlah kerugian itu menerusi 4,792 kes dalam tempoh sama yang dilaporkan kepada Jabatan Siasatan Jenayah Komersial (JSJK) Polis Diraja Malaysia, semuanya membabit-

kan barang yang dipesan melalui dalam talian tidak diterima pembeli walaupun pembayaran sudah dibuat.

Pengarah JSJK, Datuk Syed Ismail Syed Azizan, berkata jumlah kes bagi tahun ini dijangka bertambah apabila sehingga Julai saja, jumlah kes penipuan e-dagang direkodkan ialah 1,201 membabitkan kerugian RM5.2 juta.

Sepanjang 2011, jumlah kes

direkodkan ialah 1,854 dengan kerugian RM5.8 juta dan 2012 pula 1,737 membabitkan kerugian RM5.1 juta.

Penipuan e-dagang

Katanya, antara Januari hingga Julai lalu, polis menerima 593 aduan pengguna yang teripu selepas menggunakan sebuah portal e-dagang terkemuka dengan kerugian RM1.3 juta manakala sebanyak RM660,000 pula lesap dalam urus niaga Facebook.

Syed Ismail berkata siasatan mendapati kumpulan penjenayah siber itu bergerak dalam kumpulan kecil, maksimum tiga orang, dengan mewujudkan laman web e-dagang.

"Mereka memilih barang yang mampu menarik minat pembeli dengan menawarkan harga lebih murah berbanding harga pasaran dan ber-



Syed Ismail Syed Azizan

kualiti," katanya kepada BH semalam.

Antara barang yang ditawarkan termasuk telefon bimbit berjenama terkenal, alat ganti kereta, barang elektronik dan jam.

Pembayaran pula dilakukan menerusi kad kredit, wang tunai yang dimasukkan ke dalam akaun tertentu dan pemindahan wang menerusi perbankan internet.

Beliau berkata, antara cara mudah untuk mengenali urus niaga e-dagang yang mencurigakan ialah penjual tidak mendedahkan kaedah untuk dihubungi seperti nombor telefon atau alamat pejabat kecuali hanya berinteraksi menerusi e-mel.

FAKTA NOMBOR

RM5.1 juta

Jumlah kerugian yang ditanggung bagi kes e-dagang dilaporkan pada 2012

Website Scam

***myMetro** Versi Mobile RSS 1klclassifieds iMetro Akhbar Digital Team Metro

UTAMA BERITA EKSTRA METROPLUS GIGS HATI RAP VARIASI TANYA PAKAR BIMBINGAN KOLUMNIS ARKIB SEMINGGU VIDEO

myMetro Berita Utama

'Aduh! Galaxy lesung batu'

Klik sini! Ingin merasa kehebatan Coway Bidet? Perub Perub

Oleh Mohamad Fahd Rahmat
metrojb@yahoo.com



KESAL...Hazirul menunjukkan lesung batu yang diterima selepas membeli telefon bimbit secara dalam talian.

JOHOR BAHRU: Seorang kakitangan swasta yang membeli tiga telefon bimbit dengan harga RM3,250 se terkejut apabila hanya menerima lesung batu berharga RM14.50, sehan selepas melunaskan pembayaran. Lebih menyakitkan hati, tulisan RM14.50 berkenaan masih ada pada lesung batu berkenaan dan mangsa...

thestar online

FLIGHT REDEMPTIONS AT 50% LESS WITH ENRICH MILES
Redeem now

Redemption Period : 1 Nov - 31 Dec 12 Travel Period : 1 Feb - 30 Jun 13
1 Feb - 30 Apr 13 (India destinations)

News Business Sports Multimedia Lifestyle Entertainment Tech Education MyStar Classifieds Motoring Property Jobs mStar Subscribe

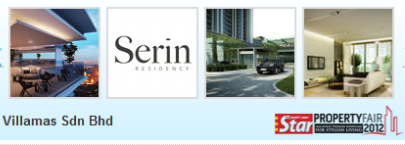
News Home > News > Nation

Classifieds SEARCH Property Search for Property Property Motoring Jobs Others

Thursday November 22, 2012

Bogus hospital website uses RM27,000 bait to lure expats

By AUDREY EDWARDS
audee@thestar.com.my



Villamas Sdn Bhd

Non-existent facility: A screen grab of the Dutamas Hospital website which has since been taken down.
Non-existent facility: A screen grab of the Dutamas Hospital website which has since been taken down.

PETALING JAYA: A "virtual hospital" is the latest scam targeting prospective expatriates into parting with their money by getting them to pay for Malaysian visas upfront.

The fake Dutamas Hospital offered salaries of more than US\$9,000 (RM27,000) per month for executive jobs, in addition to holidays, accommodation and other perks to lure victims.

If they take the bait, they would be asked to pay thousands of ringgit upfront as visa and contract fees.

Its website, created early this month, displayed detailed information

Add latest news feeds to your website with StarWidget

Latest Nation Business World Sports

- Low: Target to reduce new HIV cases may be achieved before 2015
- MB Khalid: Selangor state assembly will be dissolved in March
- RapidKuantan bus service to commence Saturday
- DID issues flood alert for Hulu Selangor, Gemas and Batu Pahat residents
- Two cops acquitted of using criminal force on press photographer at Bersih rally
- Man rushes into burning house in Kota Baru to save daughter
- Duo jailed for robbing Malaysian student during London riots freed after convictions quashed
- Felda to sue Harakah, Suara Keadilan over allegations palm oil sold to Israel



MALAYSIA'S
MOST ADVANCED
PROPERTY SEARCH WEBSITE!

www.propwall.com
We're Different!

**NEWS****BUSINESS****SPORT****TECH****LIFESTYLE****TRAVEL****OPINION****MORE**

Latest

Nation

Regional

World

Community

Environment

Education

Nation

[Home](#) > [News](#) > [Nation](#)

Published: Monday February 18, 2013 MYT 12:00:00 AM

Updated: Wednesday April 17, 2013 MYT 12:02:04 PM

Fomca: There is a need for better monitoring of online purchasing

A+ A- [Printer Icon] [Email Icon] [Share Icon] 0 [Facebook Icon] 0 [Tweet Icon] 0

PETALING JAYA: There has to be a more secure and established mechanism to oversee the process of online purchasing as more people turn to e-shopping for their needs, said Federation of Malaysian Consumers Association (Fomca) president Datuk Paul Selvaraj.

With the growing popularity of e-shopping and deal sites, he said the mechanism would need to be put in place to ensure the authenticity of these dealers.



Career Comeback.

Know of a woman on a career break who is keen to make a comeback?

>> click here

ADVERTISEMENT

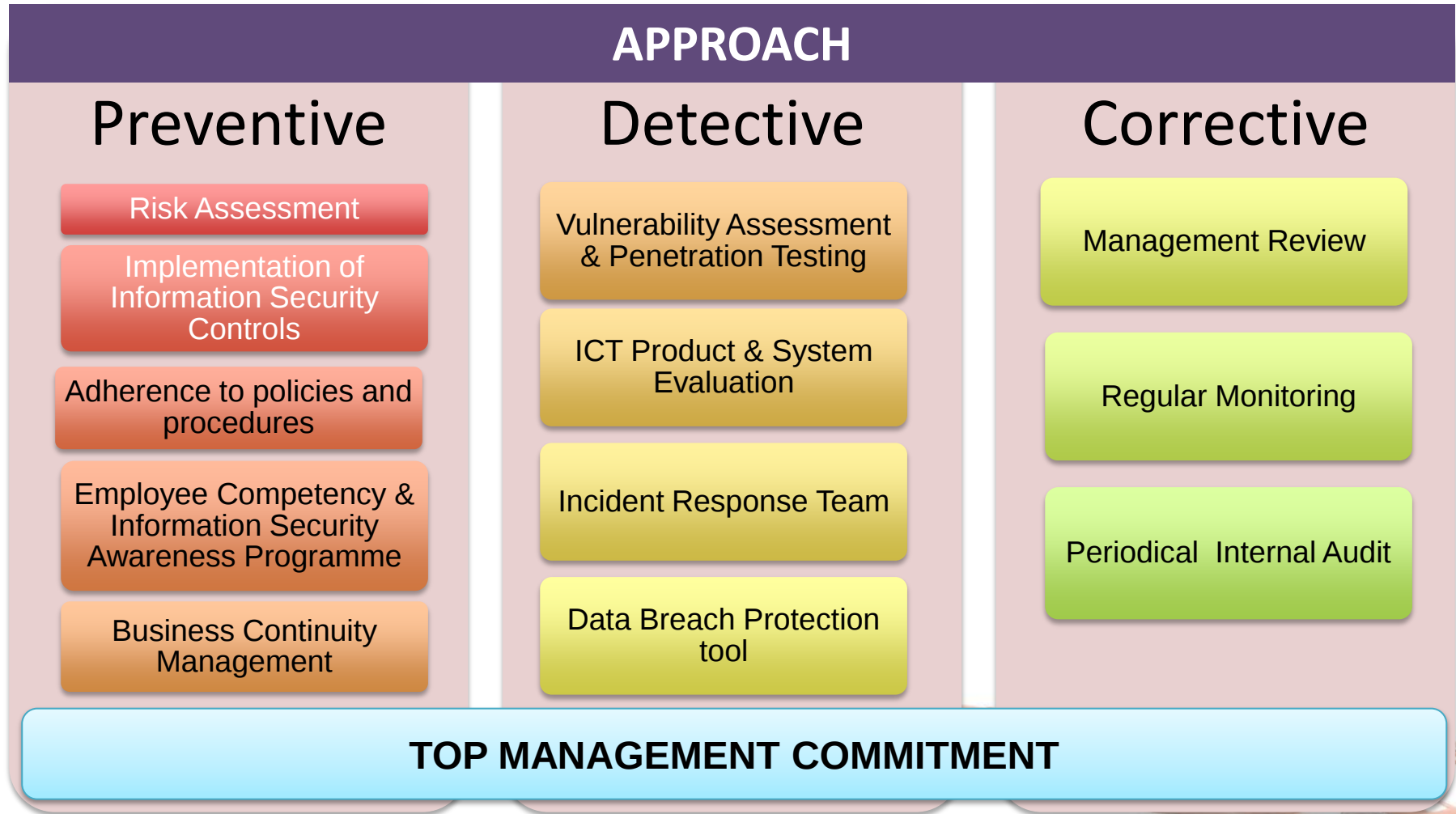
Most Viewed**Most Shared**

1. [Businesses to set thermostats higher to cope with electricity tariff hike](#)
2. [Planned demo at Dataran Merdeka](#)

How to Govern and Assure Cyber Security in Organisations?



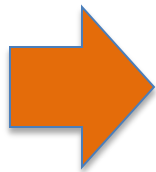
What Drive Cyber Security Preparedness



Objectives of Information Security Governance

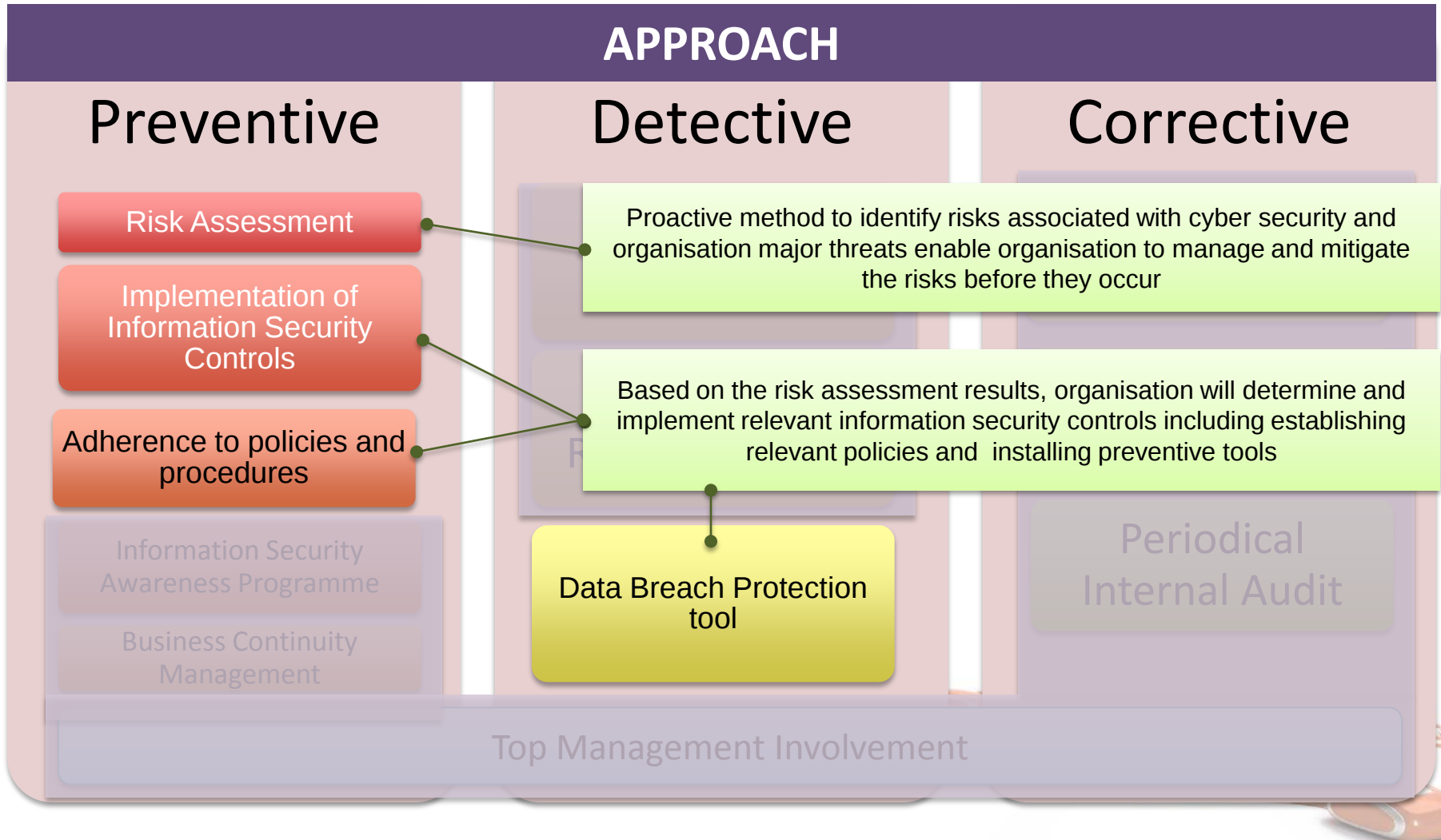
- Strategic Alignment - to align the information security strategy with business strategy /objectives (strategic alignment)
- Value delivery – to deliver value to the governing body and to stakeholders
- Provides accountability – to ensure that information risk is being adequately addressed

Source: ISO/IEC 27014:2013 Governance of information security

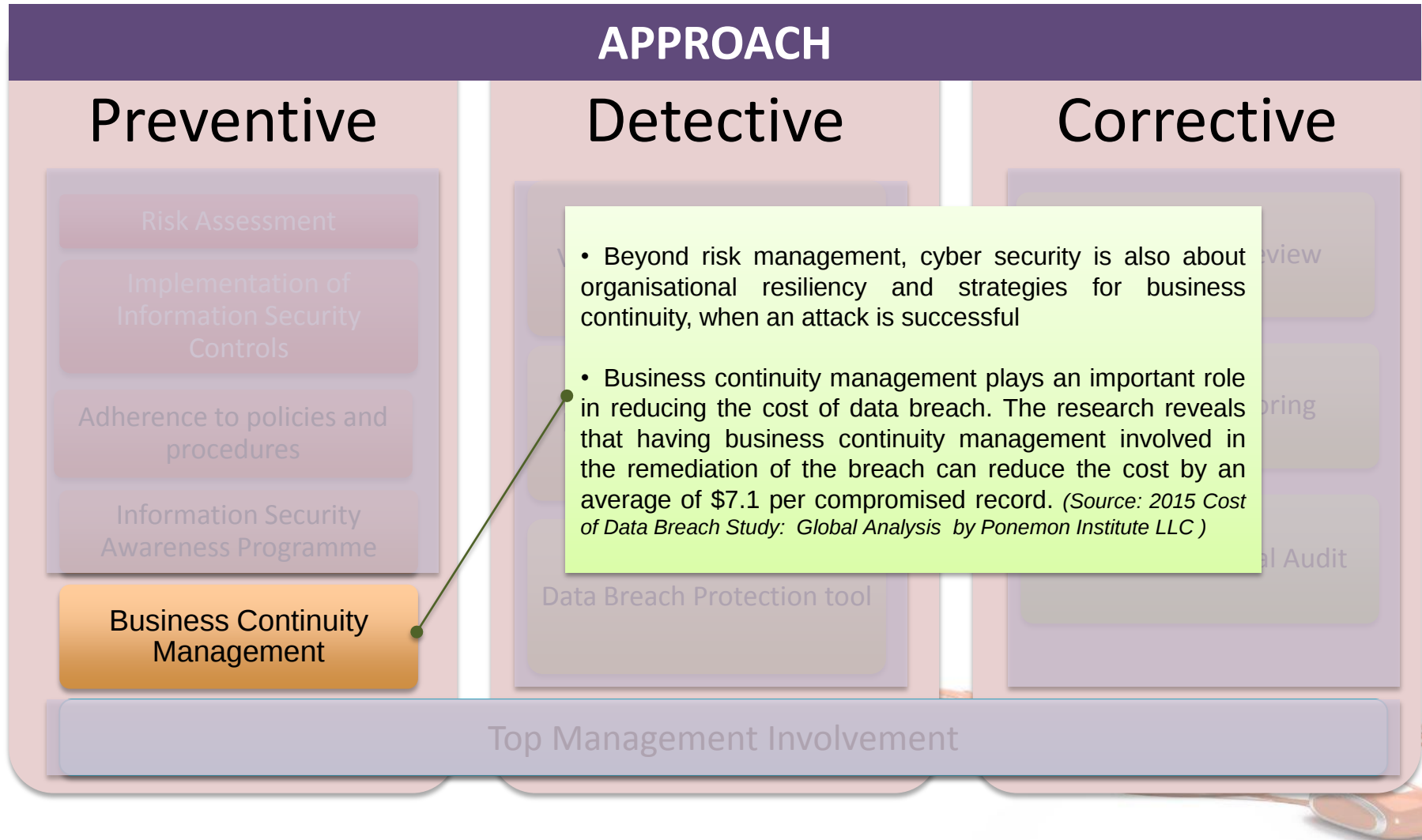


Can be achieved by having a set of principles and processes by which an organisation provides direction and oversight of information security-related activities

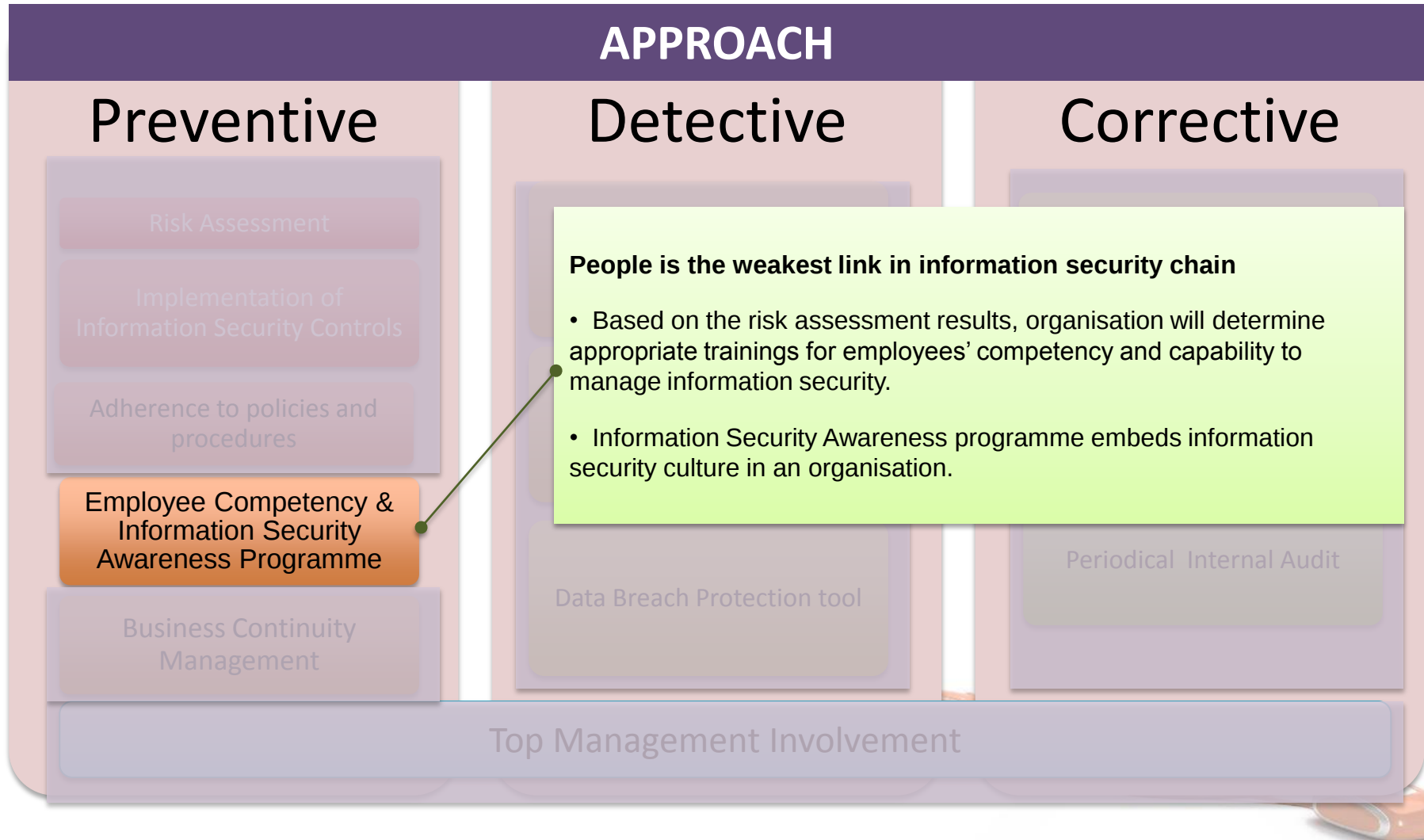
What Drive Cyber Security Preparedness (cont...)



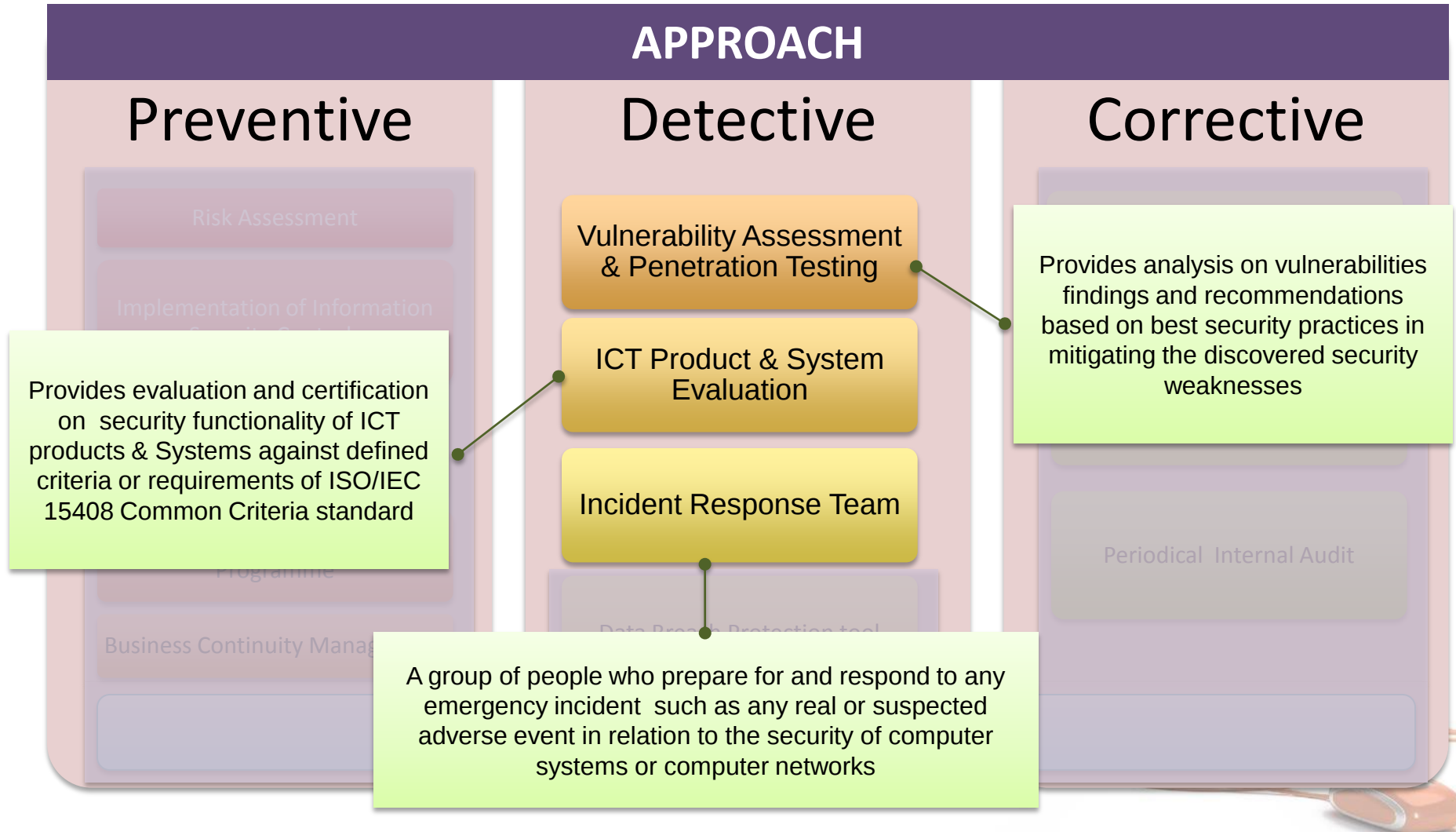
What Drive Cyber Security Preparedness (cont...)



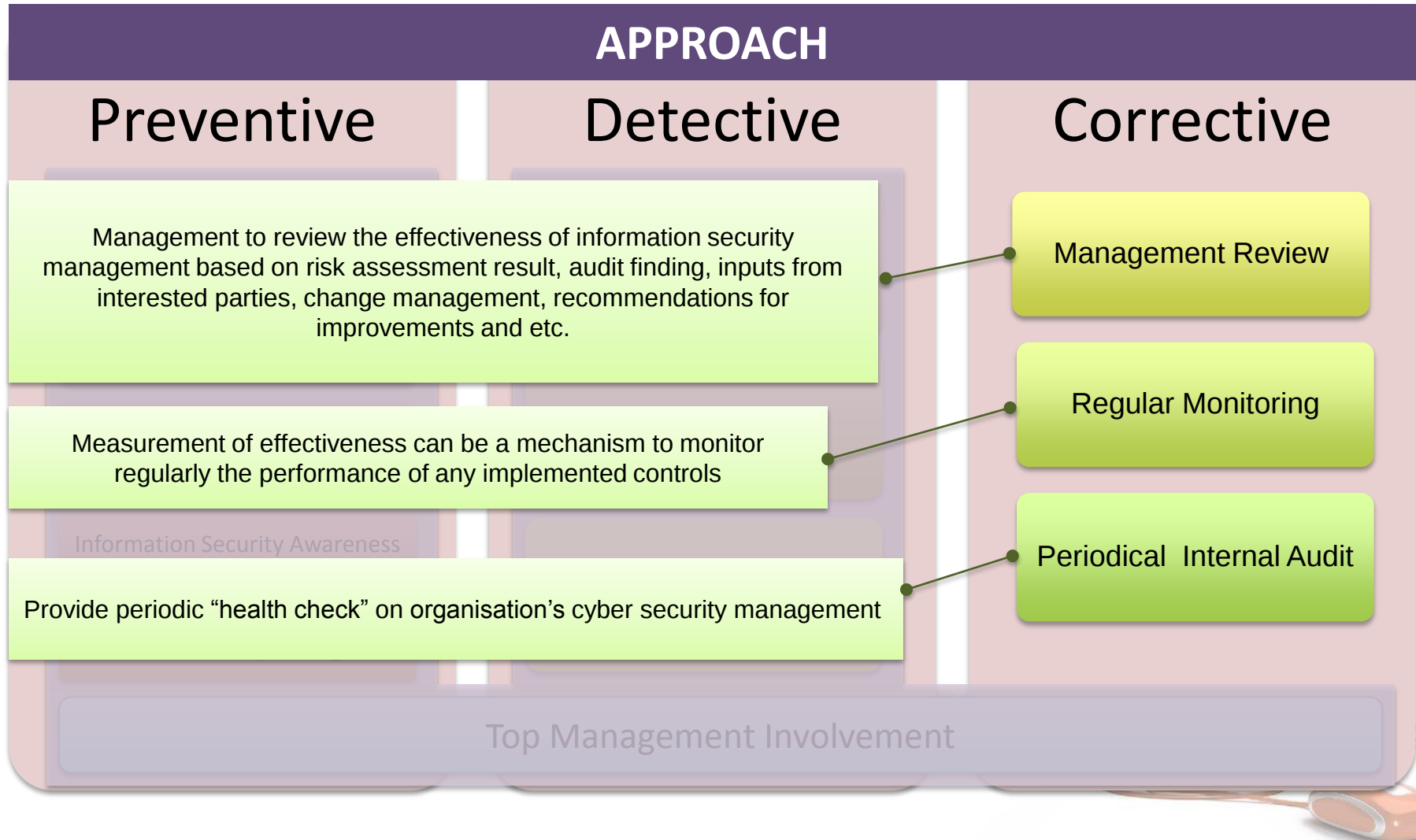
What Drive Cyber Security Preparedness (cont...)



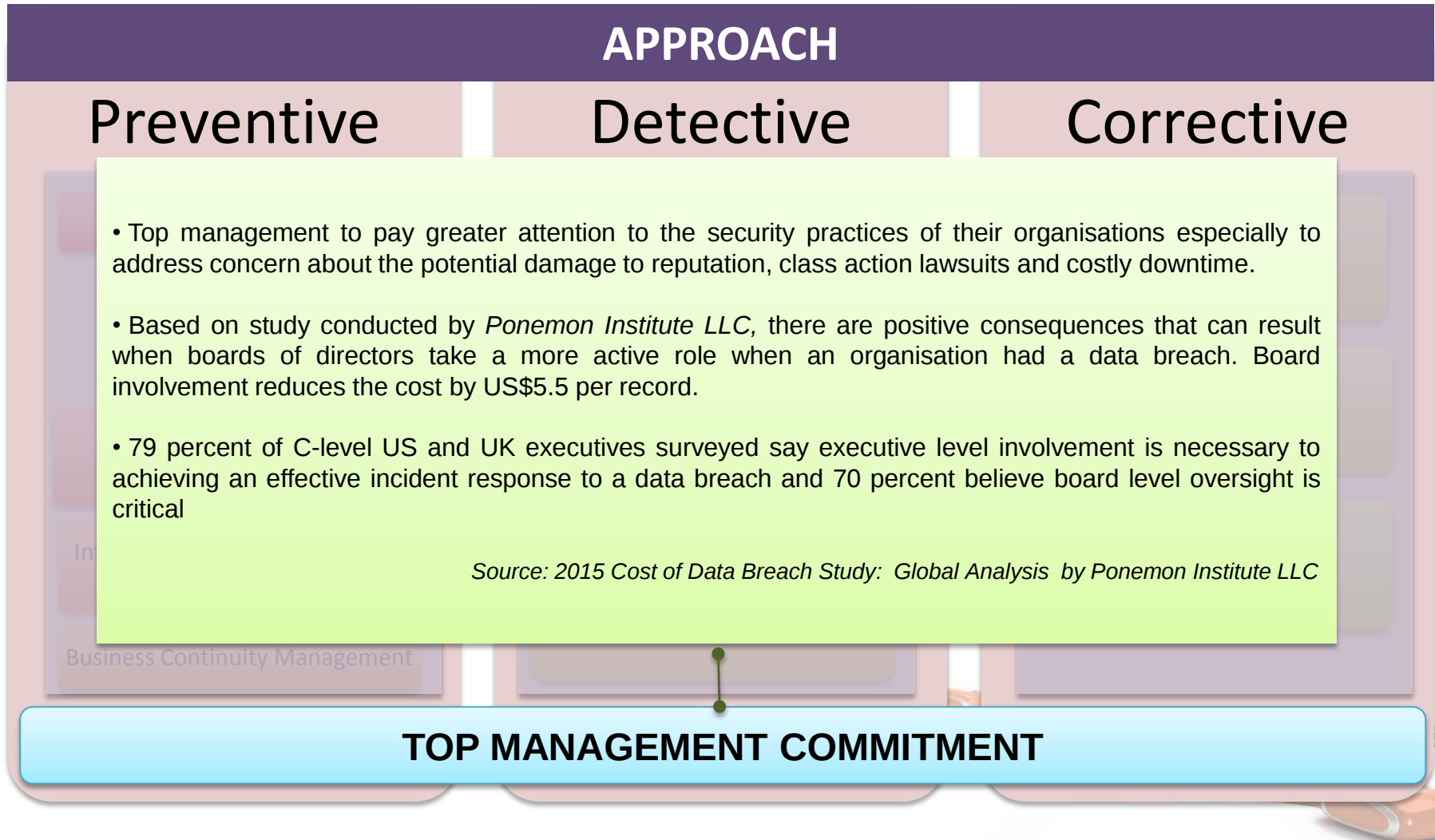
What Drive Cyber Security Preparedness (cont...)



What Drive Cyber Security Preparedness (cont...)

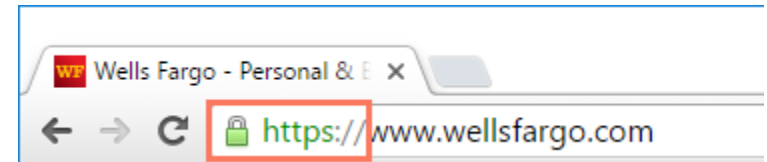


What Drive Cyber Security Preparedness (cont...)



Safe online transaction tips

- Update your browser
- Look at HTTPS
- Secure password
- Two-factor authentication
- User secure payment methods



Increase Trust Rating with

 ***Malaysia Trustmark***[®]



Overview of Malaysia Trustmark

- ➔ Malaysia Trustmark is a **government initiative** to ensure the **safety of e-business over the Internet**. By having a mean of audit and validation, consumers are able to trust the e-business websites that it browses and proceed with the online transaction if applicable.
- ➔ **Ministry of International Trade and Industry (MITI)** is mandated to drive the development of Malaysia Trustmark development.
- ➔ **CyberSecurity Malaysia** is entrusted with **Malaysia Trustmark for Private Sector**, while Malaysia Administrative Modernization and Management Planning Unit (MAMPU) are responsible for Malaysia Trustmark for Public Sector



What is an e-Commerce Trustmark?

A badge, image or logo found on an electronic commerce Web site that indicates the Web site is a member of a professional organization or that the Web site has passed security tests. The trustmark shows approval branding of a known third company.



Your Reputable and Reliable Trustmark for e-merchants



Why Malaysia Trustmark?

- ✓ Compliance with the national regulatory requirements
 - Personal Data Protection Act 2010
 - Digital Signature Act 1997
 - Digital Signature Regulation 1998
 - Consumer Protection Act 1999
 - Companies Act 1965
 - Registration of Business Act 1956
- ✓ Recognised and proven e-commerce code of conduct by WTA
- ✓ Services provided is based on national and international requirements
- ✓ PCI DSS and Security Posture Assessment, can be included as additional services



Benefits of Malaysia Trustmark

- ✓ Gain consumers' **trust and confident** in Malaysian e-business
- ✓ Improve the **competitiveness** of Malaysian merchants in global market
- ✓ Enhance **Malaysia's reputation** as a country operating in conformance to high levels of security assurance that monitors e-business activities - to prevent fraud and other online shopping scams



Mode of Incident Referrals

- Email
 - cyber999@cybersecurity.my
- Phone/Hotline
 - +603 8992 6888
 - 1 300 88 2999
- Fax
 - +603 8945 3442
- SMS
 - 15888 “Cyber999 Report”
- Mobile (24x7)
 - +6019 266 5850
- Online – <http://www.mycert.org.my>
- Walk In - Office Hours: MYT 0900 – 1800
- Mobile application (iOS and Android)

The screenshot displays the MyCyberSecurity Clinic website. At the top, the logo 'MyCSC' is shown next to the text 'MyCyberSecurity Clinic'. To the right, the address is listed: 'My CyberSecurity Clinic, E-R2, Ground Floor, Block E, The Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia.' Below this, a red banner contains the contact number '+603-8946 0811'. The main content area features a header for 'Cyber999 Malaysia Computer Emergency Response Team' with a globe icon. Below the header, there are sections for 'About Us', 'Contact Us', and 'MyCERT Statistic'. The 'Contact Us' section lists various communication methods: Cyber999 Hotline (1-300-88-2999), Handphone (+6019-2665850), SMS (CYBER999 REPORT), Fax (+603-89453442), Email (cyber999[at]cybersecurity.my), Web (http://www.mycert.org.my), and Twitter (http://www.twitter.com/mycert). It also includes office hours: 'Day: Monday - Friday, Time: 09:00 AM - 18:00 PM, MYT+0800'. The 'MyCERT Statistic' section shows a bar chart of reported incidents. The footer includes logos for member organizations like APCERT, FIRST, APWG, The Honeynet Project, and OIC-CERT, along with a disclaimer: 'Disclaimer | Copyright © 2010 - CyberSecurity Malaysia'.

Thank you

Corporate Office

CyberSecurity Malaysia,
Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.

T : +603 8992 6888

F : +603 8992 6841

H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

Northern Regional Office

CyberSecurity Malaysia,
Level 19, Perak Techno-Trade Centre
Bandar Meru Raya, Off Jalan Jelapang
30020 Ipoh, Perak Darul Ridzuan, Malaysia

T: +605 528 2088

F: +605 528 1905

 www.facebook.com/CyberSecurityMalaysia

 twitter.com/cybersecuritymy

 www.youtube.com/cybersecuritymy

