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

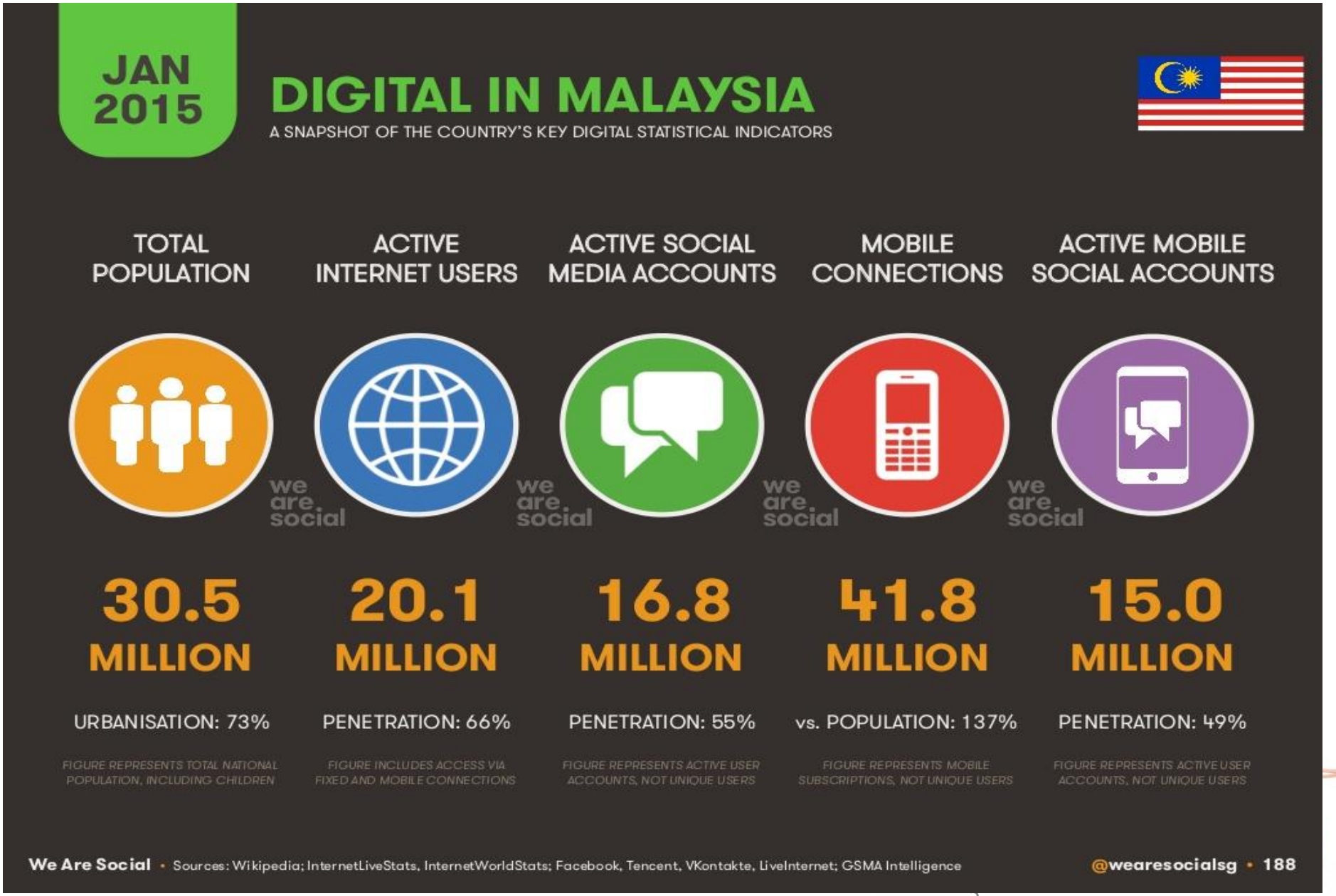
Digital citizens in Malaysia
(Malaysia Communication and Multimedia Commission 2013)

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

5 billion in 2015
(Nokia Siemen)

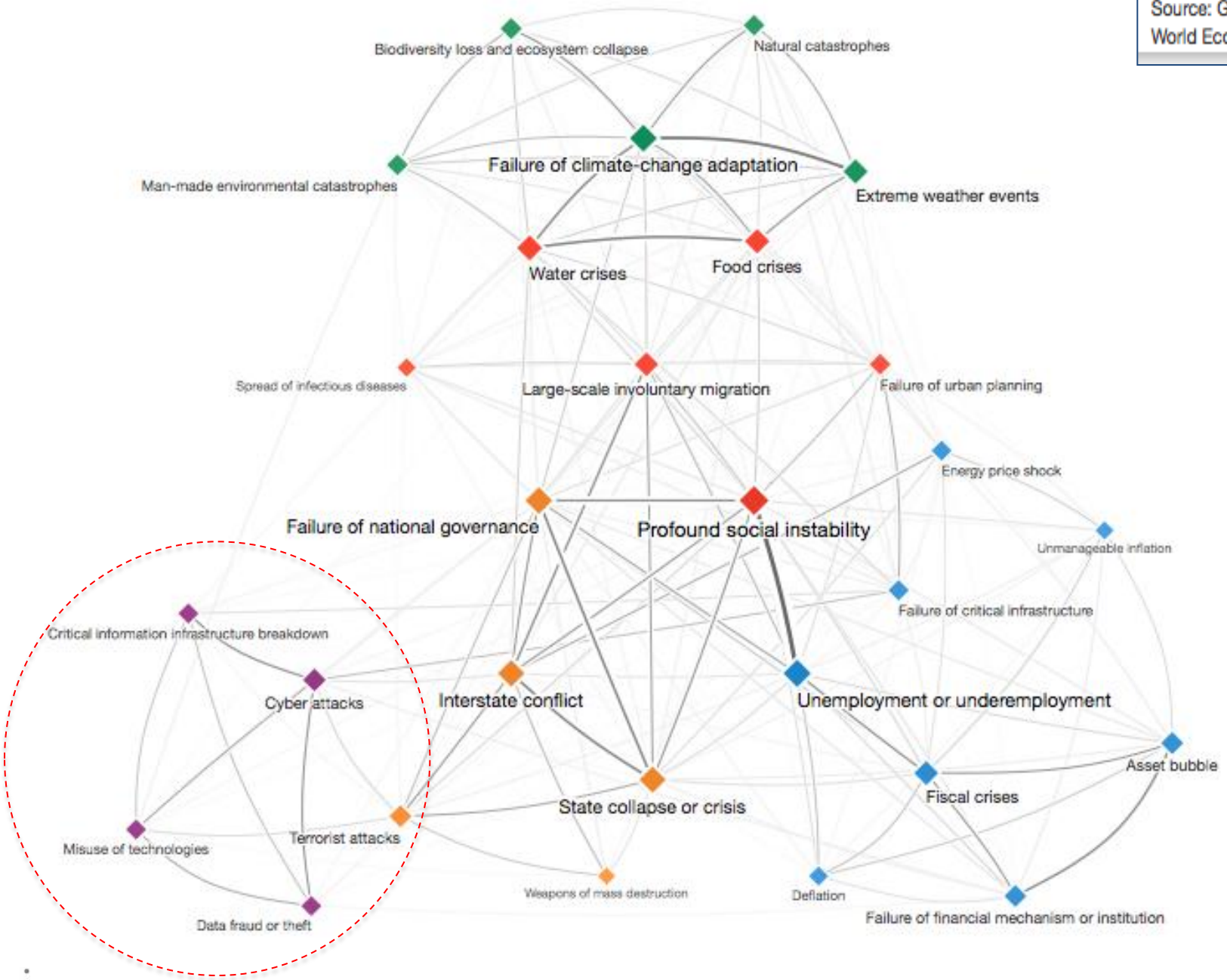
1,269 million*
Digital citizens in Asia & Pacific
(ITU 2013)

The World Today is HIGHLY CONNECTED



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

Big Data

VOLUME
Large amounts of data.

VELOCITY
Needs to be analyzed quickly.

VARIETY
Different types of structured and unstructured data.

Internet of Things

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

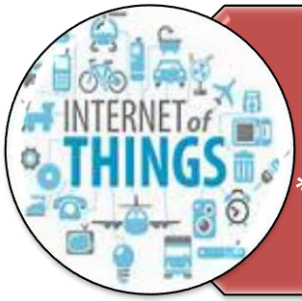
New Technologies Introduce New Security Issues

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 …..

Data Privacy

Data Security

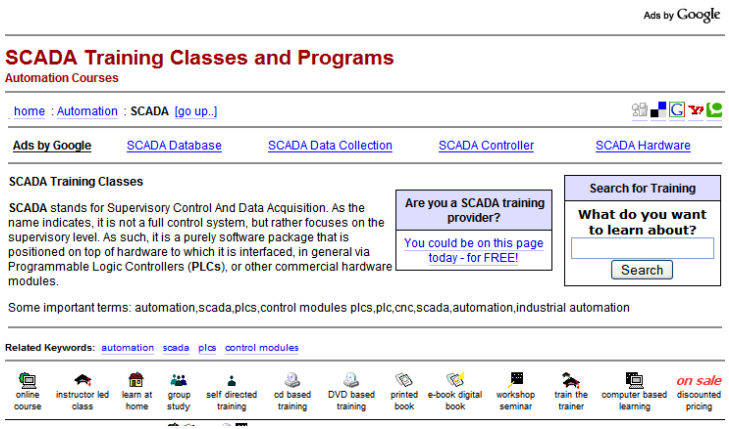
Regulatory Compliance

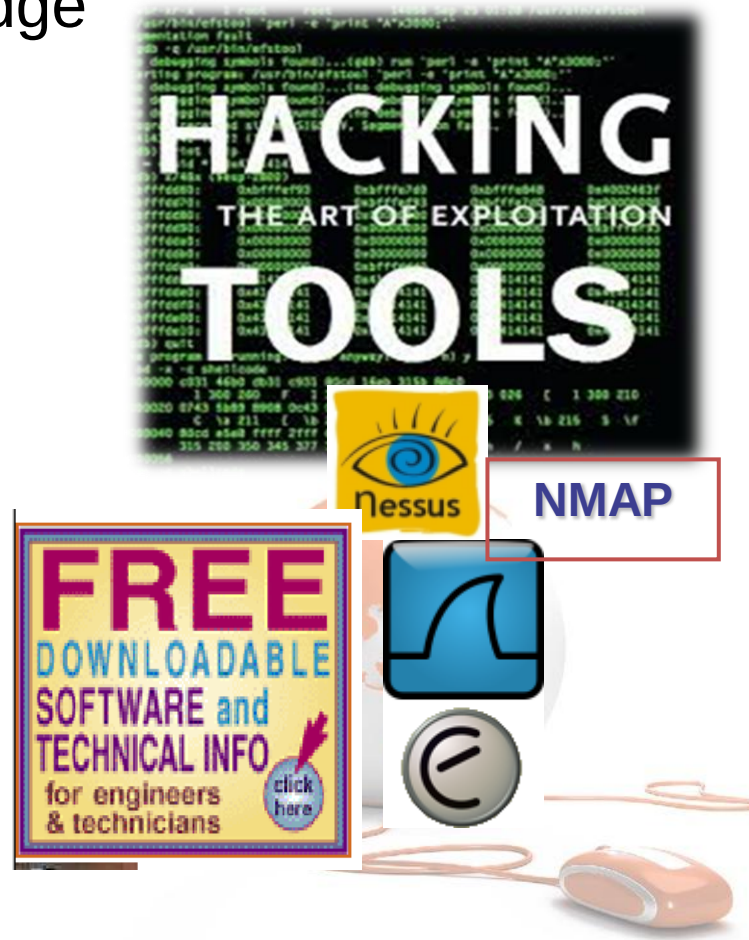
Malware Attack

Social Engineering

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)





TREND OF MALAYSIA CYBER SECURITY THREATS IN 2015

4,581 Reported Case on General Incident Classification

CONTENT RELATED

889,469

Reported Case of Malware & Botnet Drones Infection

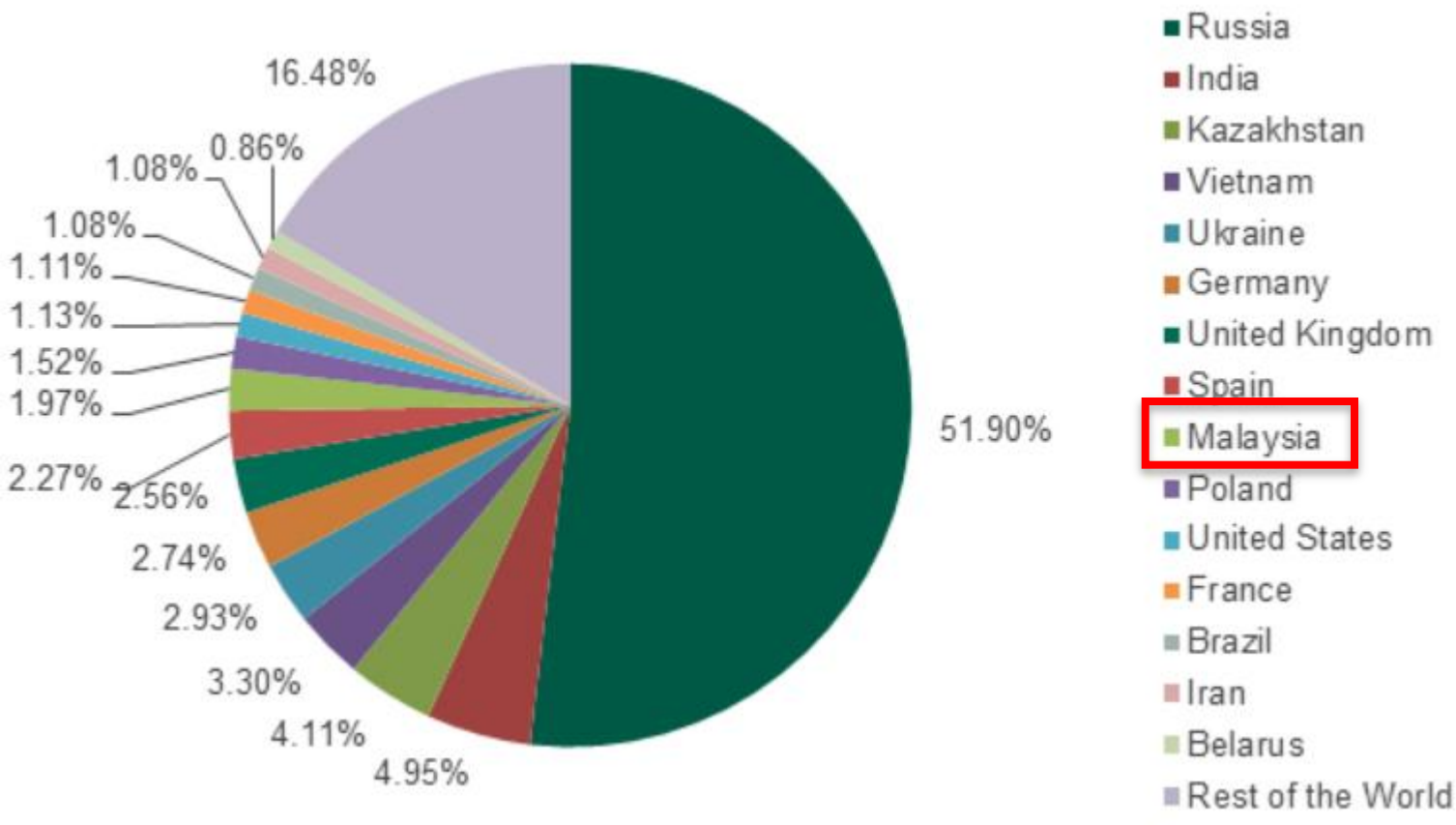
156,357

Reported Spam Emails

INTRUSION & INTRUSION ATTEMPT

FRAUD!

ISSUES & CHALLENGES
- Malaysia Ranked 9th In Malware Attacks

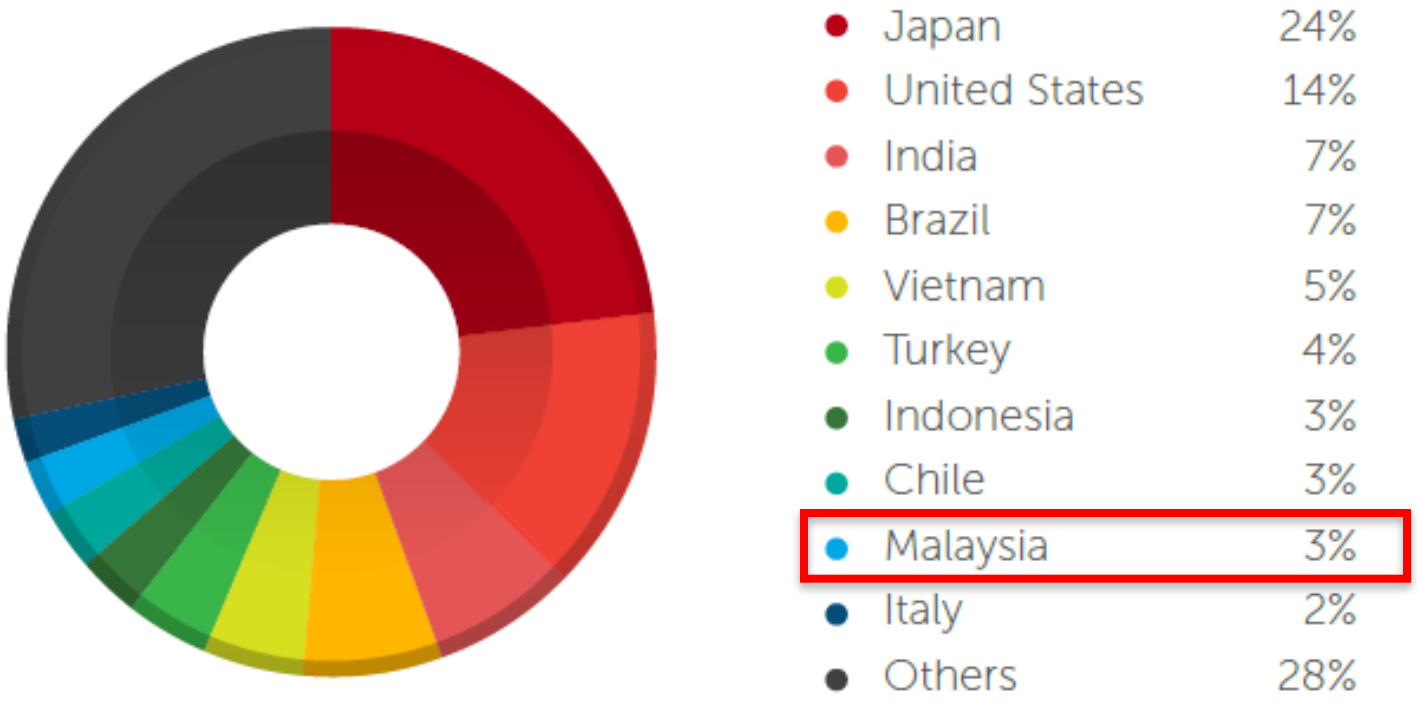


Top 15 countries with highest numbers of users attacked between April 2013 and July 2014. Malaysia: 1.97% out of 3,408,112 malware attacks

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

ISSUES & CHALLENGES
- Online Banking Malware Attacks

Countries Most Affected by Online Banking Malware, 2Q 2014



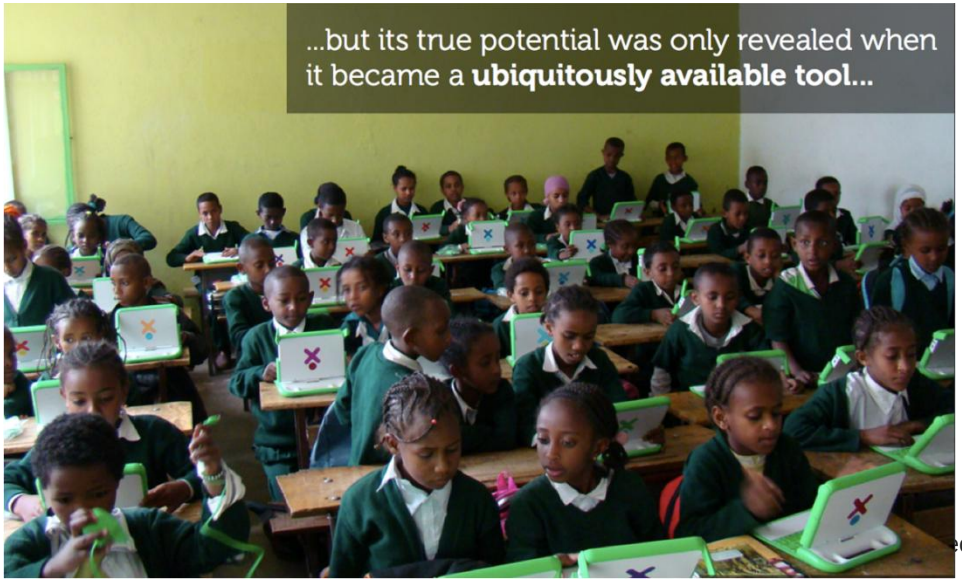
Source: TREND MICRO – TrendLabs 2Q 2014 Security Roundup

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



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

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 membabitkan 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.

FAKTA NOMBOR

RM5.1 juta

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

Syed Ismail Syed Azizan

Penipuan e-dagang

Katanya, antara Januari hingga Julai lalu, polis menerima 593 aduan pengguna yang tertipu 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 berkualiti," 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.

Website Scam

Nation

Published: Monday February 18, 2013 MYT 12:00:00 AM
Updated: Wednesday April 17, 2013 MYT 12:02:04 PM

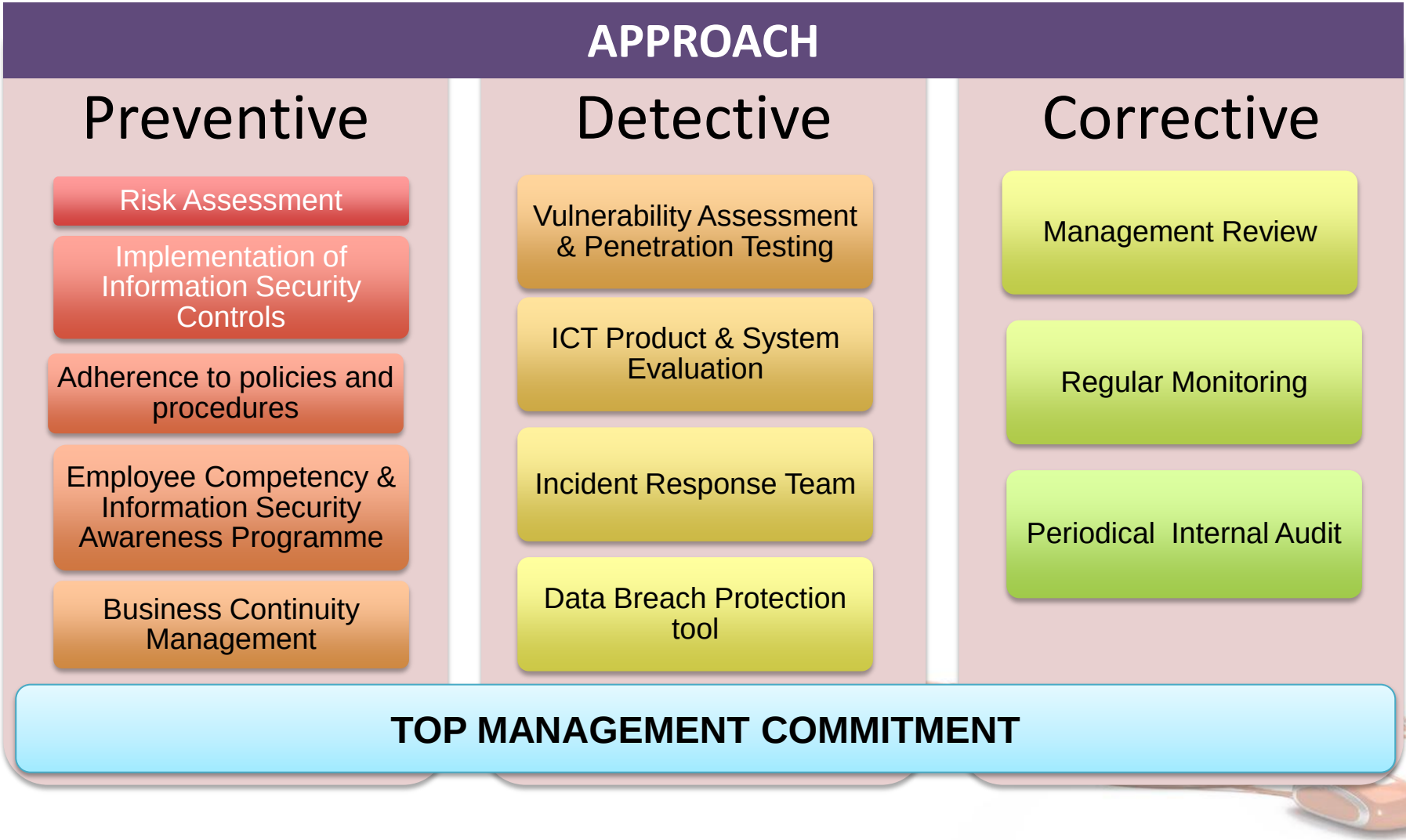
Fomca: There is a need for better monitoring of online purchasing

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.

How to Govern and Assure Cyber Security in Organisations?

What Drive Cyber Security Preparedness



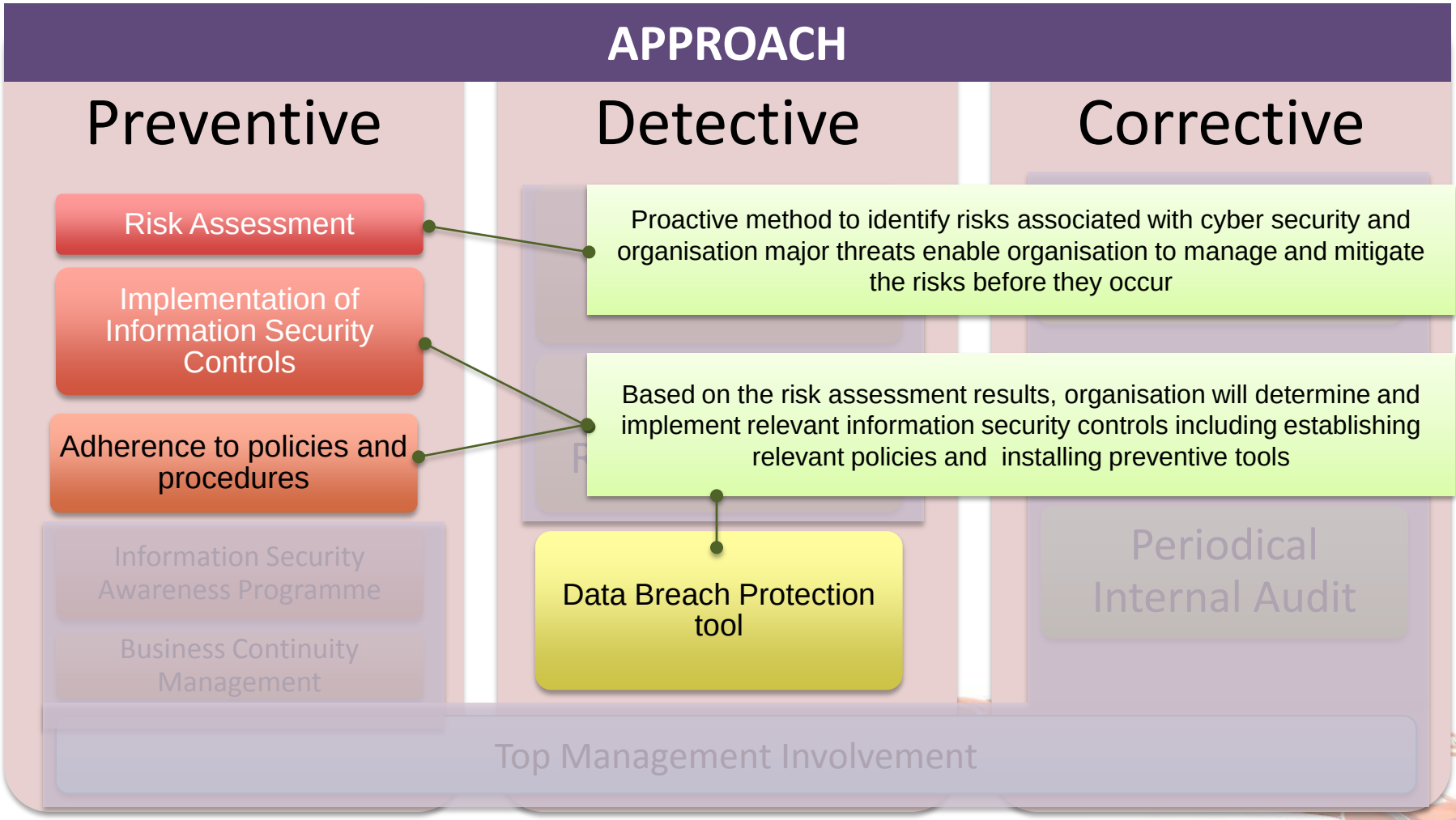
Objectives of Information Security Governance

- 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

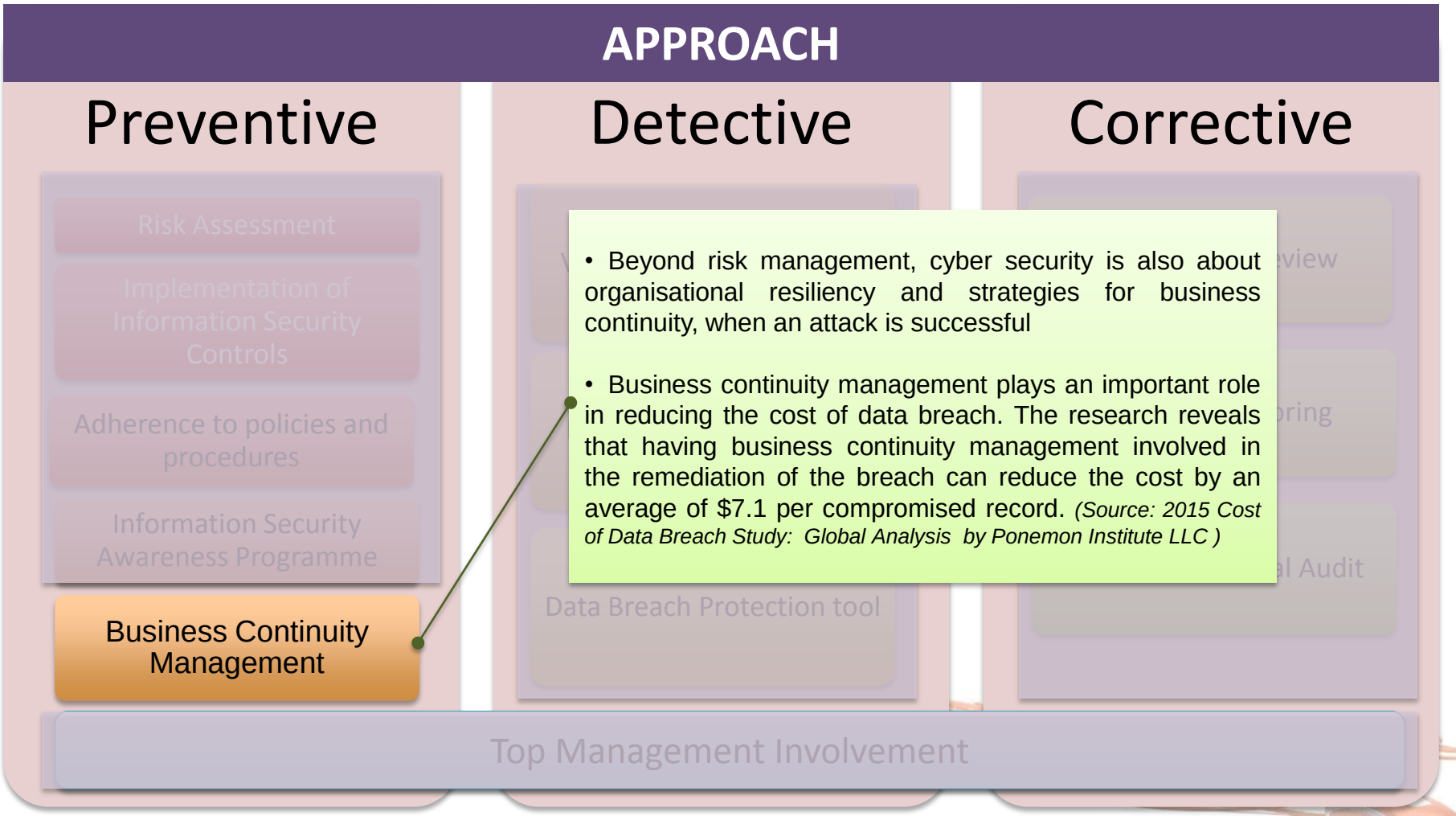
Source: ISO/IEC 27014:2013 Governance of information security

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

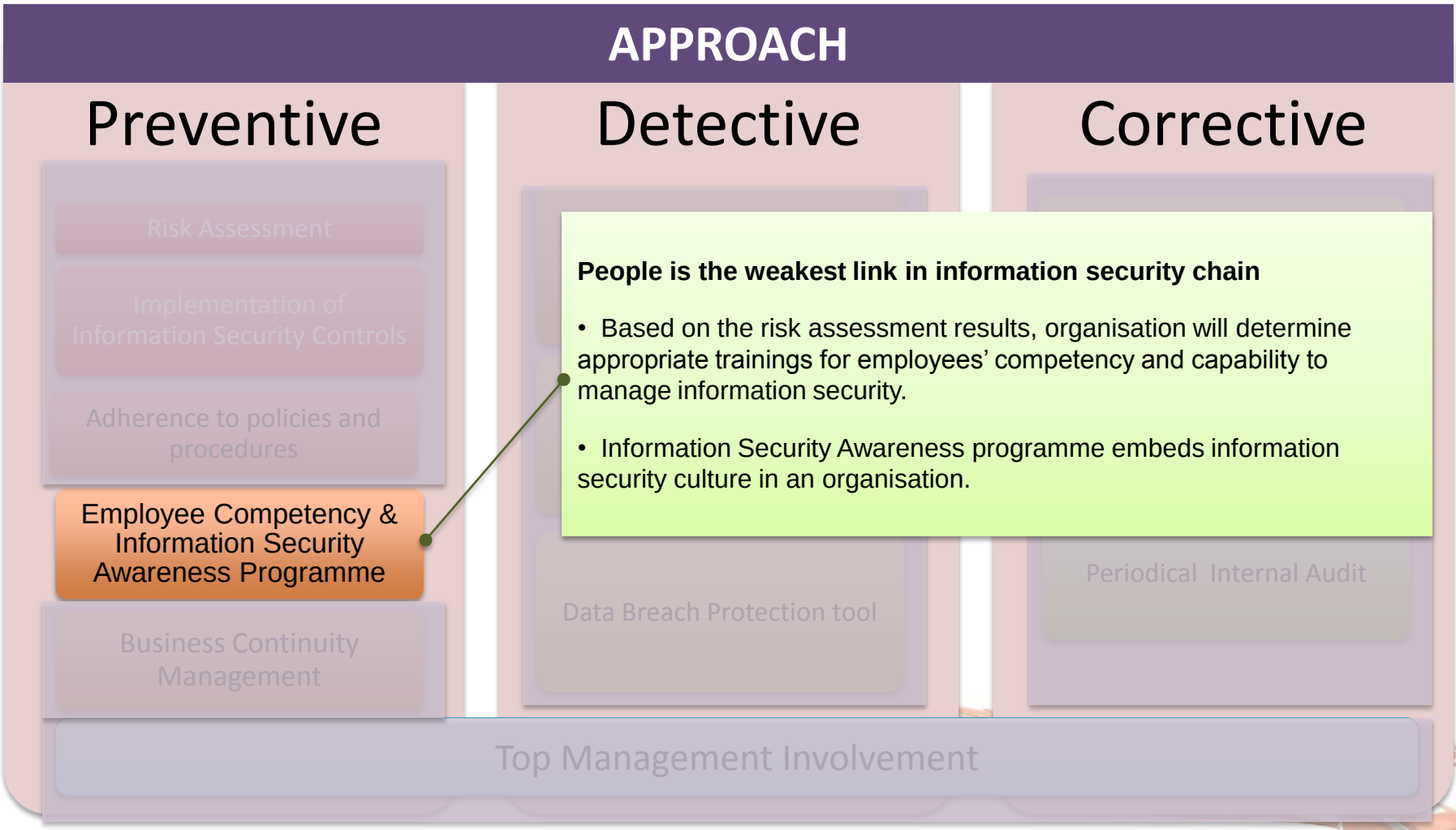
What Drive Cyber Security Preparedness (cont…)



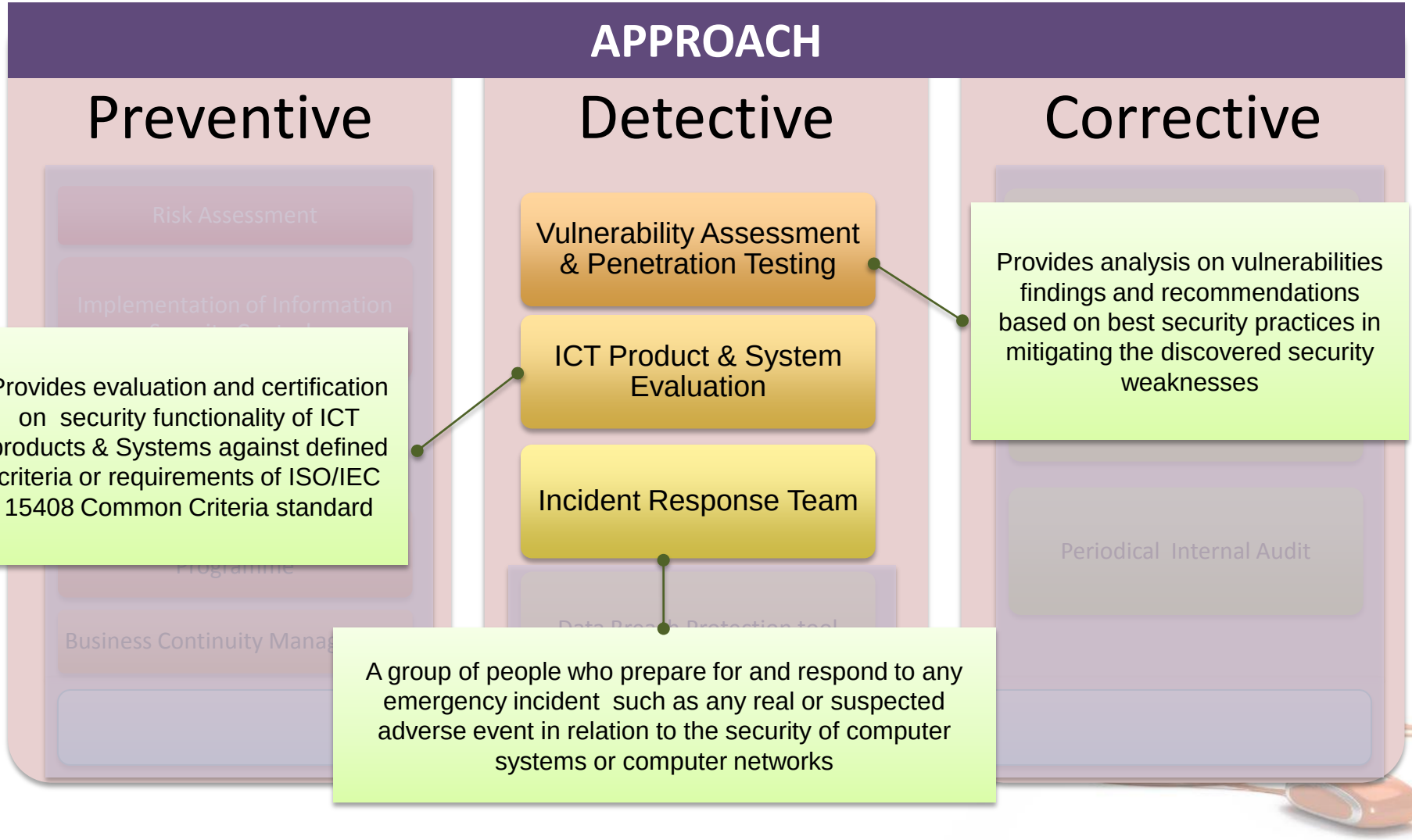
What Drive Cyber Security Preparedness (cont…)



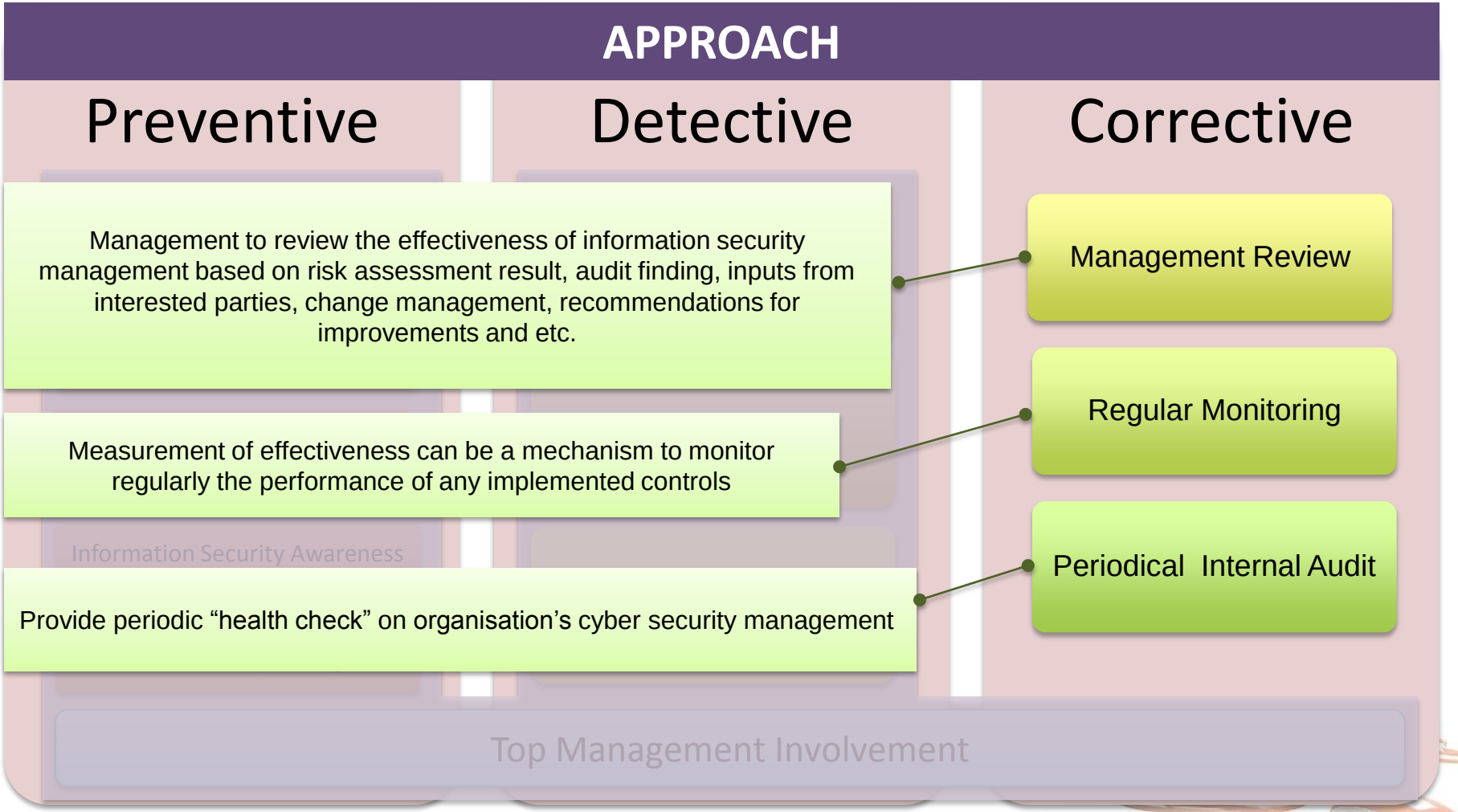
What Drive Cyber Security Preparedness (cont…)



What Drive Cyber Security Preparedness (cont…)



What Drive Cyber Security Preparedness (cont…)



What Drive Cyber Security Preparedness (cont…)

APPROACH

Preventive | Detective | Corrective

• Top management to pay greater attention to the security practices of their organisations especially to address concern about the potential damage to reputation, class action lawsuits and costly downtime.

• Based on study conducted by *Ponemon Institute LLC,* there are positive consequences that can result when boards of directors take a more active role when an organisation had a data breach. Board involvement reduces the cost by US$5.5 per record.

• 79 percent of C-level US and UK executives surveyed say executive level involvement is necessary to achieving an effective incident response to a data breach and 70 percent believe board level oversight is critical

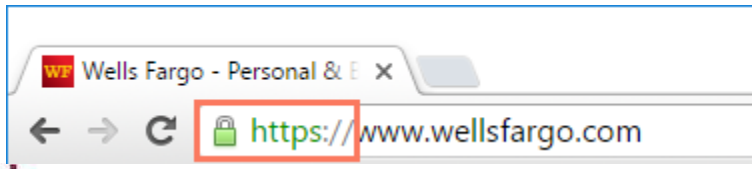
Source: 2015 Cost of Data Breach Study: Global Analysis by Ponemon Institute LLC

Business Continuity Management

TOP MANAGEMENT COMMITMENT

Safe online transaction tips

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



VeriSign®

Malaysia Trustmark®

CyberSecurity MALAYSIA

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

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.

Malaysia Trustmark®

BBB ACCREDITED BUSINESS

VeriSign®

trustsg
Your Reputable and Reliable Trustmark for e-merchants

TRUSTe CERTIFIED PRIVACY

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)

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

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

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : AR 4656

MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MyBEF LABORATORY)

MSC MALAYSIA
Status Company

Best Child Online Protection Website