Cybersecurity: the 21st century challenge … and opportunity
Content

- ACCA’s focus on Cyber risk
- Cyber risk – intensifying in Asia
- Cyber attack – types and impact
- Key Insights for Boards
- Questions that Boards need to ask Management on cybersecurity
- VIOD’s advocacy on cyber security
ACCA survey: Perceived risk of cybercrime

- **North America**: 88%
- **Caribbean**: 73%
- **Western Europe**: 91%
- **Central & Eastern Eur.**: 74%
- **South Asia**: 91%
- **Middle East**: 79%
- **Africa**: 86%
- **Asia Pacific**: 85%
- **Global**: 85%
- **South America**: 50%

**Think Ahead**
Cyber risk

- Intensifying in Asia
Cyber risk – intensifying in Asia

Hackers are 80% more likely to attack organizations in Asia

Total economic loss: $1.75 trillion
→ 7% of Asia Pacific’s GDP

Source: Cyber risk in Asia-Pacific: The case for greater transparency; Marsh & McLennan 2017
Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World; Frost & Sullivan and Microsoft, 2018
Cyber risk – intensifying in Asia (2)

Ranked 5th among Asian top risks

Asian organizations take 1.7 times longer to discover a breach

78% of internet users in Asia – not received cybersecurity education

Source: Cyber risk in Asia-Pacific: The case for greater transparency; Marsh & McLennan 2017
Cyber risk – intensifying in Asia: recent examples

2016

Bangladesh Central Bank

$81 million fraudulent wire transfers
Cyber risk – intensifying in Asia: recent examples

2018

Singapore - 1.5 million people's personal health information breached, including its Prime Minister
Cyber risk – intensifying in Asia: recent examples

2016

The Philippines - 68 government websites simultaneously hacked
Cyber risk – intensifying in Asia: recent examples

2015

Hong Kong - 6.4 million children’s data stolen from digital toymaker
Cyber risk – intensifying in Asia: recent examples

2014

Malaysia - 46.2 Million mobile phone subscribers details leaked
Cyber risk – intensifying in Asia: recent examples

2017

Damage caused by computer viruses:

VND 12.3 trillion equivalent to USD 540 million (2016: VND 10.4 trillion)

Source: BKAV

Increasing digital appetite

Highest # registered domains in Asean (www.AAA.vn)

Mobile penetration rate – 144%, 50% smartphone

E-commerce growing at 35% p.a.
World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 4th July 2018)

Source: informationisbeautiful.net
Cyber attacks – Type and Impact
Cyber-attacks – type

A cyberattack.. by any other name.. is still bad!

Trojan
botnet
Malware
Spyware
Phishing
Ransonware
DDoS
Advanced Persistent Threats (nation states, cyber-terrorism)

... an on and on
Cyber-attacks – impact

Real nature (e.g.):
- Financial fraud
- Online sales channels unavailable
- Online brand impersonation
- Data exfiltration or corruption

What Boards should be most concerned about – highest impact and slowest recovery time

Impact:
- Data privacy breaches
- Loss of confidential information to competitors
- Loss of reputation and customer trust
- Loss of revenue
- Loss of jobs
- Lowers trust in eco-system – decreased consumer and enterprise spending
- Directors’ personal reputation

Think Ahead
Key Insights for Boards
Key Insights for Boards

1. Cyber-security should be boardroom topic
   - M&A
   - New product launches
   - New projects
   - Strategy and annual budgets

Digital transformation journey -
   - develop a cybersecurity strategy
2. Address your cyber defensive frailties
   - Make a C-level executive responsible for information security
   - Integrated, not silo-based approach
   - Information security training – employees, key suppliers (?)

Chart 1: Top five information security challenges
3. Go beyond prevention – speed of detection and recovery!

Chart 2: Do you know the average time required for your organisation to resolve a security breach or incident?
Key Insights for Boards (3) – lessons learnt

What they did right

1. Discovered the breach themselves – not hackers or media (reputation risk management)

2. Immediately advised federal authorities. Hired reputable cyber consultants to deal with immediate damage control (internal preparedness)

3. Although regulations allowed for 60-day reporting window, Anthem announced publicly within days of discovery (restoring trust and loyalty)

4. Clear and coherent messaging of what happened

5. CEO letter – addressed concerns of key stakeholders, apologised, showed empathy, provided immediate resources
4. Investments in information security must keep pace with technology adoption

Chart 4: Has your organisation allocated any budget for information security in the coming three years?

Address Board and Management bias towards investments on emerging technologies – ‘adopt first, manage later’ (71%)
Key Insights for Boards (4)

4. Invest in “basic” best practices

- Strong passwords
- Multi-factor authentication
- Keep devices operating system, software and anti-malware protection genuine and up to date
- Invest in Assessments and Reviews – regularly
- Data encryption of sensitive data
- Leverage on AI
Questions for Boards to ask Management on cyber-security

- Who at the C-level is responsible for cyber-security? Does this person have the right skills and experience?

- How much of our business is digital/tech driven or enabled? Which areas are most vulnerable to cyber-attacks?

- How much are we spending on cyber-security? How does it compare with competitors/peers?

- How do we measure effectiveness of our cyber-security programmes?
Questions for Boards to ask Management on cyber-security (2)

• Penetration test or independent external assessment of our cyber-defences – *when was the last time? Key findings and how are we addressing them?*

• External auditor raised any cybersecurity related deficiencies in internal controls over financial reporting?
VIOD - Advocacy

• Collective voice – strategic.
• Business-led improvements in cyber-security governance ahead of regulatory interventions
• Evidence-based local research on cyber matters. Critical to inform policy-making by government, Boards
• Changes in eco-system – e.g. cyber risk insurance, quality and availability of cyber security professionals
Questions?
For more ACCA Resources on Cyber: https://www.accaglobal.com/gb/en/professional-insights/technology.html
Contact ACCA Speaker – Sharath Martin: Sharath.Martin@accaglobal.com