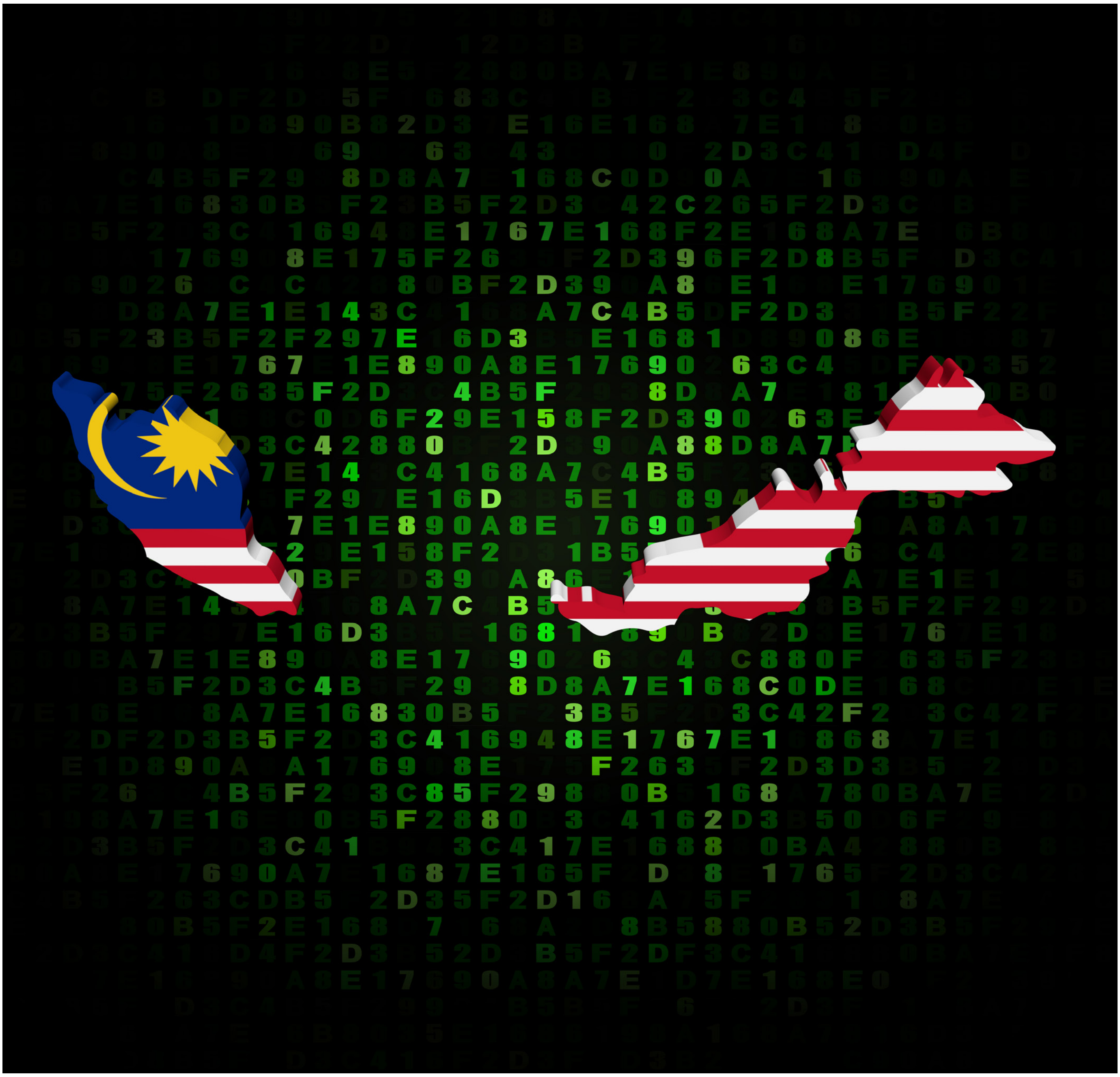
Digital development in Malaysia

An analysis of cyber threats and responses

A report from DAKA advisory



Commissioned by the British High Commission
in Kuala Lumpur

Contents

Cover photo: © Stephen Finn

About the report

Digital development in Malaysia: An analysis of cyber threats and responses is a report from DAKA advisory written by Kim Andreasson. It was commissioned by the British High Commission in Kuala Lumpur on behalf of the British Foreign & Commonwealth Office. The report does not necessarily reflect the views of the sponsor.

The aim of the report is to raise awareness of cyber security in Malaysia and to provide suggestions on which to build proactive policy measures. It also aims to serve as a reference point for those interested in digital development in the country. Although the report does not use a consulting framework per se, a SWOT (strengths, weaknesses, opportunities, threats) approach was used in deriving the recommendations.

To uncover cyber security threats and responses in Malaysia, and those that affect it from a global perspective, DAKA advisory conducted extensive desk research and interviews with a mix of international and local experts in the public and private sectors. We like to thank the following people and organisations for their contributions (listed in order of appearance):

- Stephen Ezell, Senior Analyst, Information Technology & Innovation Foundation
- Dr Amirudin Abdul Wahab, CEO, CyberSecurity Malaysia
- Chakib Abi-Saab, CIO, Bumi Armada Berhad
- Hood Abu Bakar, General Manager of ICT, Group Information & Communications Technology, MISC Berhad
- Mike Usher, Director of Information Risk, Prudential Asia
- Andy Tan, CIO, RHB Group
- Kashif Syed Haq, Chief Information Technology Officer, Celcom Axiata Berhad
- Marco Obiso, Cybersecurity Coordinator, International Telecommunication Union
- Datuk Mohd Noor Amin, Chairman, International Multilateral Partnership Against Cyber Threats
- Marsineh Jarmin, ICT Security Officer, Malaysian Administrative Modernisation and Management Planning Unit
- Mohamed Sharil Tarmizi, Chairman, Malaysian Communications and Multimedia Commission
- Mingu Jumaan, Director of State Computer Services Department, Sabah State Government
- Daniel V.C. Lee, CIO, Felda Global Ventures

Foreword

Simon Featherstone CMG

In two decades, use of cyberspace has grown exponentially; it is now fundamental to the global economy. Although the impact of this expansion may have varied across countries, in many ways it has been as profound in the developing world as in the developed.

Our global interdependence in cyberspace leads to a universal interest in all states having the skills and capacity to tackle cyber threats and increase the resilience of their networks. The UK has made this a particular priority as we aim to be one of the safest places to do business online and are developing leading-edge cyber capabilities.

The UK's 2010 National Security Strategy rated cyber attacks as a top threat and the 2011 UK Cyber Security Strategy sets out the importance of working with international partners in this area.

In my three years here, I have been struck by the high level of connectivity in Malaysia and the vibrancy of debate in the online space.

I am delighted that the British High Commission in Kuala Lumpur has been able to fund this report on digital development in Malaysia.

Its analysis and recommendations will help identify some of the challenges facing Malaysia. I am sure that this report will provide our two countries with further opportunities to work together on cyber, for the security and prosperity of the people of both our countries.

Simon Featherstone CMG
British High Commissioner to Malaysia
@HCSFeatherstone

Executive summary

Malaysia aims to become a developed country by 2020. Digital development – whether an increase in domestic supply and demand or international exports of information and communication technologies (ICT) products and services – plays a central role in this effort. Boosting supply of online public sector services, increasing broadband connectivity to stimulate demand, attracting foreign direct investment (FDI) into the ICT sector and developing niche products for export, are some of the key efforts indicative of this strategy.

Digital development creates efficiencies and enhances economic growth. However, a greater reliance on ICTs also means an increase in digital dependency which leads to exposure to cyber threats. Categorising threats into those that are financially-motivated or politically-motivated, reveals that emerging markets are typically subject to the former while their exposure to the latter rises as they either engage in more advanced military capabilities or develop higher-end corporate products.

Although Malaysia is currently not a target of sophisticated attacks, questions linger about its readiness to face the challenges ahead, particularly in regards to cyber threat awareness, digital divides, challenges in international ICT trade, overlapping domestic organisational interests, and a lack of collaboration between the public and private sectors.

To uncover cyber threats and responses in Malaysia, and those that affect it from a global perspective, this report is based on a combination of extensive desk research and interviews with international and local experts. Parts 1 and 2 introduce cyber opportunities and threats around the world from a Malaysian perspective. Parts 3 and 4 provide an overview of current initiatives and key stakeholders in Malaysia before evaluating challenges and proposing steps in order for the country to seize the full socio-economic potential of a digital society moving forward.

The key findings are as follows:

Opportunities: The ICT industry in Malaysia is growing at 10% a year and the Internet's contribution to GDP – a rough measure of domestic utilisation of ICTs – stands at 4%, which is on par with many developed countries. As such, the country is in a good position to further enhance and solidify the economic benefits of digital development. In particular, as Malaysia seeks to become a global hub for ICTs, it is moving into value-added services and niche products that are more profitable and also less prone to global economic fluctuations. Meanwhile, there are also opportunities to enhance supply of public sector services – the government aims to have 90% of them online by 2015 – and

provide the connectivity to match – the high speed broadband initiative seeks to have 75% of households connected by the same year. Combined, such efforts will further enhance domestic utilisation of ICTs for productive purposes.

Threats: Malaysia primarily faces financially-motivated cyber threats, such as malware and phishing attacks. Fraud is also the most common cyber security problem according to incident statistics tracked by the government. In part, this is due to its level of digital development in which there is a general lack of awareness of cyber attacks. Given their usage patterns, Malaysians are particularly vulnerable to mobile and social media threats. This is also an issue for the private sector as employees and customers increasingly use mobile devices without much knowledge of the risks. Lack of awareness also extends to senior management who are often unaware of the challenges that come with emerging technologies, such as cloud computing in which data fall under the jurisdiction where it is stored, not only where it is used. As the country's digital development continues, Malaysia is also likely to increasingly be exposed to politically-motivated attacks, such as cyber espionage and potential attacks on critical infrastructures, as illustrated by countries that are further ahead in digital development like South Korea.

Responses: Malaysia has a civilian cyber security strategy, which recognises CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI), as the technical experts and the Malaysian Communications and Multimedia Commission (MCMC) as the regulator. In addition, the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) is tasked with security compliance within public sector organisations. Malaysia is keenly supporting international initiatives such as the Organisation of The Islamic Cooperation - Computer Emergency Response Teams (OIC-CERT), the Asia Pacific Computer Emergency Response Team (APCERT), and the International Multilateral Partnership Against Cyber Threats (IMPACT), which is also supported by the International Telecommunication Union (ITU). In the private sector, banks and telecommunications companies are anecdotally relatively well-prepared and they take steps to mitigate common cyber threats. Yet corporate awareness more broadly remains low and a lack of formal public and private sector information-sharing leads to lost collaboration opportunities.

Ways forward: Greater digital dependency brings new cyber threats but also broader challenges related to cyber security, something which Malaysia will increasingly encounter. For instance, greater reliance on the digital domain will necessitate further investment in bridging digital divides, particularly outside of Kuala Lumpur, to tackle a lack of awareness regarding productive and safe usage of ICTs. Given stated ambitions to further enhance ICT exports, Malaysia is also likely to face geopolitical cyber security trade challenges as well as issues related to intellectual property rights (IPR). Further concerns also surround the potential liberalisation of government-linked companies

(GLCs), in which the government holds a controlling stake, in critical infrastructure industries and overlapping interests between domestic agencies, in particular CyberSecurity Malaysia and MCMC.[1]

Recommendations: Based on the key findings, this report concludes with five suggestions towards enhancing cyber security in Malaysia moving forward:

1. **Pursue digital by default, but don't neglect trust:** Enhanced electronic service delivery is efficient; however, there is a danger that supply outpaces useful usage – the extent to which people can take advantage of them. This is a digital divide but also a cyber security concern as attacks on public sector websites – and the people who use them – can undermine trust.

2. **Compete globally and move from international technical cooperation to policy engagement:** Malaysia is keenly aware of global ICT export competition. To create a competitive advantage, the country should consider leveraging its position in international technical forums such as APCERT and OIC-CERT, to engage further in global policy discussions surrounding geopolitical ICT trade concerns.

3. **Tackle the lack of awareness at all levels:** There is a need for greater cyber security education in schools, among society at large, as well as within organisations. The private sector also faces the dual task of educating external and internal users, including senior management. Although some efforts are under way, almost everyone agrees that more needs to be done in this regard.

4. **Prepare for politically-motivated attacks by establishing a foundation for collaboration between sectors:** If Malaysia liberalises the dominance of GLCs, as it intends to do, the country would do well by establishing the foundation for greater information-sharing between sectors, particularly as the lack of such is already cited as hindering enhanced cyber security in Malaysia.

5. **Clarify domestic roles and responsibilities:** It is not a situation unique to Malaysia but there are clear overlapping interests between domestic agencies, in particular CyberSecurity Malaysia and MCMC. Clearer definition of roles and responsibilities will help streamline future efforts to meet the challenges ahead, and hopefully improve collaboration among agencies in the process.

[1] The ten Critical National Information Infrastructures (CNII) in Malaysia are: National Defence and Security; Banking and Finance; Information and Communications; Energy; Transportation; Water; Health Services; Government; Emergency Services; and, Food and Agriculture. See http://nitc.mosti.gov.my/nitc_beta/index.php/national-ict-policies/national-cyber-security-policy-ncsp

1. Introduction

Governments around the world look to leverage ICTs to stimulate economic growth and enhance social outcomes either via exports or enhanced productivity through domestic supply and demand. “Greater use of ICT will not only support the growth of the sector but also boost productivity and raise the nation’s overall competitiveness,” says the 10th Malaysia Plan, which along with the Government Transformation Programme (GTP) and the Economic Transformation Programme (ETP) under the New Economic Model, figures prominently in Vision 2020 for Malaysia to become a developed country.[2]

Stephen Ezell, a Senior Analyst at the Information Technology & Innovation Foundation (ITIF), a Washington, D.C. think-tank, and co-author of *Innovation Economics: The Race for Global Advantage*, says there are two ways in which countries can enhance productivity.[3] They can either replace traditional industries with more advanced ones or use ICTs to increase productivity across all sectors.

To achieve the objective of high-income status by 2020 requires an average annual GDP growth rate of 6%.[4] Increased use of ICTs is therefore a key focus area. “The Government will aggressively promote the use of ICT in all industries in parallel with the development of the ICT sector,” says the 10th Malaysia Plan.

The numbers support this point. According to McKinsey, a consultancy, the Internet has accounted for 21% of GDP growth among developed countries over the last five years and 75% of this growth took place in traditional industries that benefitted from ICTs.[5]

To reach its targets, Malaysia also needs to become a net exporter of ICT instead of a net importer and in the process delve into niche products. To do so, the Multimedia Super Corridor (MSC) programme, a Special Economic Zone largely concentrated in Kuala Lumpur that was officially inaugurated by the 4th Malaysian Prime Minister, Mahathir Mohamad, on 12 February 1996, was established to attract international companies and investment.

Simultaneously, the removal of tariffs on eight types of ICT products by participating countries in the 1996 World Trade Organisation (WTO) Information Technology Agreement (ITA), led to a massive increase in trade

[2] Prime Minister’s Office of Malaysia: http://www.pmo.gov.my/?menu=page&page=1904

[3] For more information regarding the book, see http://www.globalinnovationrace.com

[4] Economic Planning Unit: http://www.epu.gov.my/en/tenth-malaysia-plan-10th-mp-

[5] McKinsey Global Institute, Internet matters: http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters

for developing countries, in particular in Asian markets. The continent now accounts for about two-thirds of the world's total exports of USD 1.8trn.[6]

In Malaysia, the ICT sector will also grow by 10% per year from 2013 to 2017 and total industry revenue will reach RM 95bn in 2017 from the base of RM 57bn in 2012, according to PIKOM, the national ICT association.[7] Incidentally, one of the more promising niche areas happens to be cyber security. Today, about 10% of local ICT revenue and 30% of export revenues are derived from cyber security products and services. By 2015, CyberSecurity Malaysia reckons that the local information security industry is expected to contribute about RM 3bn to Malaysia's Gross National Income (GNI) up from RM 1bn today.[8] MSC also has several capability development programmes in place to enhance cyber security products and services produced by its companies, according to an email statement for this report from the Multimedia Development Corporation (MDeC), which supervises MSC.

The global economic downturn has raised questions regarding the feasibility of the country's strategy as GDP growth slowed from 7.4% in 2010, according to the World Bank, to 4.7% in 2013, according to local sources.[9] However, as HSBC, the global bank, has noted, Malaysia is in a strong position in the global ICT sector and although the near-term prospects are poor, the longer-term outlook is still favourable.[10] According to the email statement, MDeC is also confident of continuing to attract FDI.

This report begins by explaining the tie between increased digital development and rising cyber dependency through a framework that combines the demand- and supply-side factors that give rise to cyber security concerns.[11]

The supply-side: ICT readiness

A thriving ICT sector can be important to economic development. But the potential readiness to use products and services domestically (supply) are equally crucial to reap the full benefits of a digital society. For instance, a country can be a large exporter of ICT products, such as China, but have lesser readiness to use them for productive domestic purposes. Conversely, a country can have low ICT exports, such as Denmark, but have a large digital economy, leading to greater efficiencies.

[6] UNCTAD: http://unctad.org/en/pages/InformationNoteDetails.aspx?OriginalVersionID=37&Sitemap_x0020_Taxonomy=1629;

[7] PIKOM: http://www.pikom.org.my/cms/General.asp?whichfile=Press+Releases&ProductID=23251&CatID=33

[8] The Borneo Post: http://www.theborneopost.com/2011/08/25/information-security-to-bring-rm3-bln-to-gni/

[9] World Bank: http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG;
New Straits Times: http://www.nst.com.my/top-news/gdp-grows-4-7pc-in-2013-exceeds-forecast-1.483016

[10] HSBC: https://globalconnections.hsbc.com/united-kingdom/en/tools-data/trade-forecasts/my

[11] Adapted from Kim Andreasson, editor, Cybersecurity: Public Sector Threats and Responses: http://www.crcpress.com/product/isbn/9781439846636

Malaysia consistently ranks in the top 30 in the Global Information Technology Reports from the World Economic Forum's (WEF) Networked Readiness Index, which "measures the extent to which 142 economies take advantage of ICT and other new technologies to increase their growth and well-being." Malaysia also consistently ranks in the top 45, out of 193 member states, in the biennial United Nations (UN) e-government survey, which is the primary source for tracking public sector supply-side efforts (see figure 1).

Figure 1: Malaysia's ICT readiness in an international context

	UN E-Government Development Index	WEF Networked Readiness Index
	Ranking	**Ranking**
2013	N/A	30
2012	40	29
2011	N/A	28
2010	32	27
2009	N/A	28
2008	34	26
2007	N/A	26
2006	N/A	N/A
2005	43	24
2004	42	26
2003	43	36

N/A – no update published in the year given
Sources: United Nations, World Economic Forum

Although Malaysia is doing relatively well, it also has some ways to go. The country is pushing hard to get there. On 16 September 2010, current Prime Minister Najib Tun Rasak called on government agencies and civil servants to improve efficiencies through the 1Malaysia: People First, Performance Now programme.[12] The Malaysian Public Sector ICT Strategic Plan (2011-2015) also provides a strategy to accelerate development of public sector ICT service delivery and usage.[13] Current policy targets are to have 90% of all government services available online and 90% of total transactions made via ICTs by 2015.

The demand-side: Connectivity and usage

The supply of services or the extent of their availability are unimportant if people do not use them. This has been a common problem facing online government services in which countries roll out great numbers of initiatives without much demand from users, leaving the promise of public sector

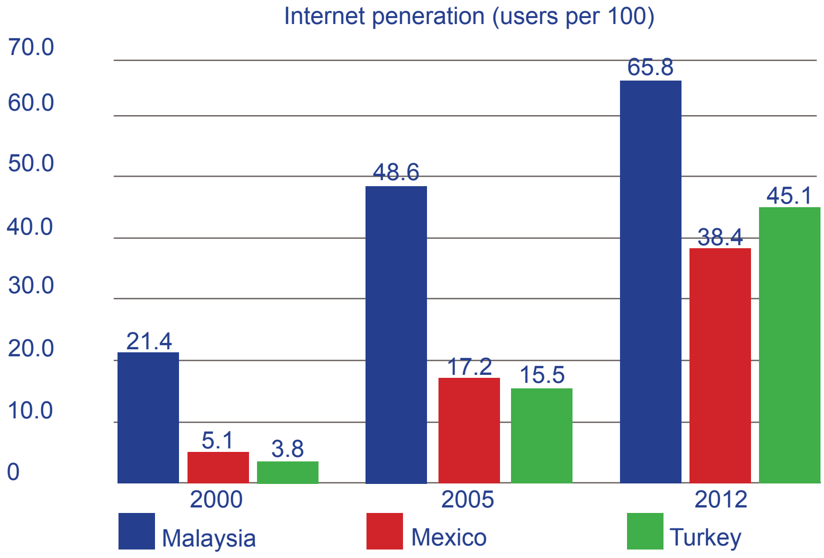
[12] 1Malaysia: http://www.1malaysia.com.my/en
[13] MAMPU: http://www.mampu.gov.my/web/en/ict-strategic-plan

transformation largely unfulfilled. A couple of years ago, South Korea led the world in e-government according to the UN survey and reports showed that although 73% of its citizens were aware of online public sector services, only 47% actually used them.[14]

Usage depends in part on access. Although there is an urban/rural digital divide in Malaysia, in particular between Kuala Lumpur and other areas (see section 4, challenges), the country fares relatively well overall from an international perspective. The latest data from MCMC in the 4th quarter of 2013 shows a broadband penetration rate of 67.1 out of 100 households and a cell phone penetration rate of 143.6 per 100 inhabitants.[15]

Given various definitions by different countries, it can be difficult to compare broadband development across borders. In the case of Malaysia, the broadband targets are based on speeds of 256Kbps with the aim to provide 10Mbps or greater to high economic impact areas, although target speeds also evolve over time. Suffice to say that the universal National Broadband Initiative (NBI) and the High Speed Broadband (HSBB) Project, conducted in collaboration with Telekom Malaysia Berhad, are both ambitious efforts that will serve the country well. Under the 10th Malaysia Plan, the government has set a target to increase the broadband penetration rate to 75% of households by 2015.[16] In regards to Internet usage, the country is also on par, or above, similarly developed countries, such as Mexico and Turkey (see figure 2).

Figure 2: Growth in Internet penetration – three similarly developed countries (by GDP per capita) over 12 years



Source: World Bank, World Development Indicators database

[14] The Korea Times: http://www.koreatimes.co.kr/www/news/nation/2010/02/117_61097.html

[15] MCMC: http://www.skmm.gov.my/Resources/Statistics/Communications-and-Multimedia-Pocket-Book-of-Stati.aspx

[16] Economic Planning Unit: http://www.epu.gov.my/en/tenth-malaysia-plan-10th-mp-

Malaysia is also doing well in regards to using ICTs productively. For instance, in 2011 the Internet contributed an average of 3.4% to GDP – a rough measure of domestic utilisation of ICTs – in the G8 countries plus South Korea, Sweden, Brazil, China and India, according to McKinsey, although there were significant differences between high-performing developed countries like Sweden (6.3%) and emerging markets like Russia (0.8%).[17] A subsequent report in 2012 shows that Malaysia is keeping pace with Internet contribution to GDP at 4.1%, almost on par with developed countries.[18]

From cyber dependency to cyber risk

An increase in supply and demand will further solidify Malaysia's digital and economic development. However, it also raises the importance of cyber security. "Cyber security is a prerequisite to economic growth," says Dr Amirudin Abdul Wahab, CEO of CyberSecurity Malaysia. "There is extensive use of ICT in Malaysia today and that can become a concern because it exposes us to cyber threats." The PIKOM ICT Strategic Review 2013/14, a joint publication with MOSTI, also notes that "Malaysia's increasing dependency on cyber space has become a significant risk, hence there is a need for a higher level of security and information assurance due to our increased interaction in cyber space."[19]

Combining ICT readiness (using GDP per capita as a proxy indicator since research shows a strong link between ICT progress and income) with the demand for them (using Internet usage as a proxy indicator), indicates the level of cyber dependency across countries (see figure 3).[20] This simple assessment reveals where a country stands today in its cyber development and also predicts where it is heading by looking at the potential threats facing those that are further ahead.

For instance, countries with higher GDP per capita are more prone to national security and corporate espionage, on average, as competitors seek information to gain an advantage. Hence, a rise in cyber dependency means an increase in risk. In particular, Malaysia's private sector is likely to come under increased attack while there will be a greater need for both higher levels of awareness and enhanced public-private collaboration as the country develops.

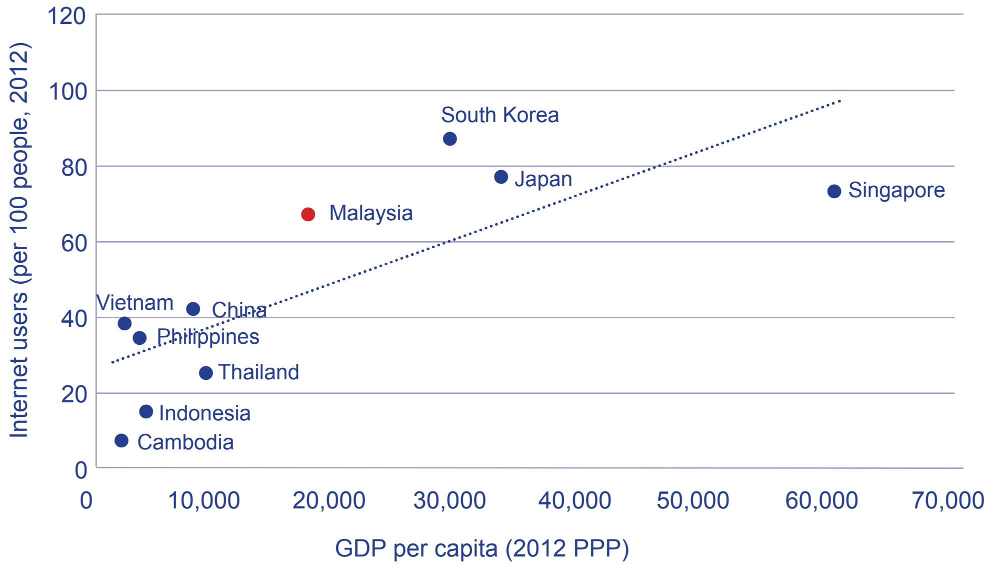
[17] McKinsey Global Institute, Internet matters: http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters

[18] McKinsey Global Institute, Online and upcoming: The Internet's impact on aspiring countries: http://www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries

[19] PIKOM: http://www.pikom.org.my/cms/General.asp?whichfile=ICT%20Strategic%20Review%202012/13&ProductID=23131&CatID=79

[20] ITU: http://www.itu.int/net/pressoffice/press_releases/2012/70.aspx#.UueBIbQxWM8; http://www.itu.int/net/pressoffice/press_releases/2013/67.aspx#.UueDMLQxWM9

Figure 3: Malaysia’s cyber dependency in an Asian context



Source: World Bank, World Development Indicators database

For instance, a distributed denial of service (DDoS) attack shutting down access to Internet banking in Cambodia and Indonesia is of less concern than when it happens to Japan and Singapore as their populations rely on the Internet to a greater extent. In South Korea, for example, a massive cyber attack in March, 2013, shut down more than 48,000 computers and servers and in the process limited ATM withdrawals and online banking for several days, leading to distress among the population.[21]

Malaysia is doing relatively well in both ICT readiness and usage, indicative of the number of people online, which is almost on par with countries that have higher GDP per capita. But as the country pushes its digital development agenda in the next few years, new threats and challenges also await, as exemplified by those that are further along in the digital development curve.

The next section discusses the current threats and challenges facing the country, followed by the public and private sector response to date. The concluding section examines Malaysia’s cyber security challenges in light of its digital development and provides suggestions on which to build proactive policy measures.

[21] Yahoo News: http://news.yahoo.com/skorea-says-nkorea-behind-computer-crash-march-054009443--finance.html

2. Cyber threats

Because they are borderless in nature, cyber threats affect all countries equally. However, preparedness for cyber security and levels of development play a role in either mitigating or attracting certain types of threat. The first half of this section focuses on categorising global cyber threats while the second half looks at those that are particularly relevant in Malaysia today.

Global cyber threats

A simple way to classify global cyber threats is by determining whether they are cyber crime-related or politically-motivated. This categorisation enables a better understanding of the changing threats that countries face as they develop.

Cyber crime and non-political threats

Financially-motivated threats include corporate espionage, intellectual property theft, identity theft, and various forms of fraud. At the simplest level, they are usually carried out through malware and phishing techniques in which users click on unknown links thereby either infecting their computers or being tricked into submitting information. More advanced methods are used to gain access to intellectual property (IP) and corporate information while remaining undetected.

Estimates vary but the cost of cyber crime is high by any count. Norton, a security company, reckons the global cost to be about USD 110bn based on a survey of thousands of people around the world.[22] In Malaysia, cyber crime victims lost RM 1.6bn in 18,386 cases in 2012, up from an estimated RM 1.1bn a year earlier.[23] Such figures do not include indirect costs, such as a loss of trust when data is compromised, which is a concern for both public sector services as well as e-commerce providers.[24]

Politically-motivated threats

Hacktivism, a combination of the words hacker and activism, is the simplest form of politically-motivated threats as it seeks to disrupt or deface websites to make a statement. Anonymous is the most high-profile group in this area and in 2011 it attacked numerous Malaysian government websites through DDoS attacks, making them inoperable for a short period of time.[25]

[22] Symantec: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02
[23] The Star: http://www.thestar.com.my/News/Nation/2013/03/27/Victims-lost-RM16bil-to-scam-artists-in-18386-cases-last-year-alone/
[24] The Economist: http://www.economist.com/node/21557817
[25] Examiner.com: http://www.examiner.com/article/operation-malaysia-anonymous-ddos-attacks-cripple-gov-websites

More sophisticated political threats usually involve government support and cyber espionage is commonplace as intelligence agencies do what they can to gather information. Although this is a concern – for instance during sensitive trade negotiations – a greater issue is whether they collude with the private sector in order to gain competitive business insights using national security capabilities. Such allegations are frequent, in particular against China, although there is little concrete evidence such collusion actually takes place.

Cyber attacks targeting critical infrastructures are of great concern to cyber security. For instance, the US has officially labelled cyber as the fifth domain (after air, land, sea, and space) and established offensive military capabilities in this area. In 2010, the Stuxnet malware also became the first attack with offline consequences to a critical infrastructure as it reportedly succeeded in disrupting Iran's nuclear power reactors. Given the sophistication needed, such attacks are rare, yet increasingly likely as countries invest in offensive cyber attack capabilities and consider these to be an alternative to diplomacy or traditional military action.

Cyber threats to Malaysia

Classifying cyber threats as either politically-motivated or non-political in nature, reveals that almost all global cyber security collaboration initiatives focus on the latter. The reason is that countries are generally in agreement that cyber crime needs to be prevented, as most are also victims thereof. Developed countries are targeted because of their wealth whereas less developed countries may face a proportionally greater risk to such crimes, given a lack of awareness on behalf of users. There is no such common denominator regarding politically-motived threats as they are usually an extension of national security, hence subject to geopolitics as usual.

Advanced economies are subject to politically-motivated cyber espionage attacks as they have entered a new dimension of ICT capabilities and are targeted for their corporate and national security secrets. Since Malaysia is still moving up the ICT value chain, it is unlikely to be subject to such activities. "Regardless of what many people think, sophisticated cyber attacks and corporate espionage isn't very common and we have seen very few such serious attacks to our organisation," says Chakib Abi-Saab, CIO at Bumi Armada Berhad, an international offshore oil and gas services provider headquartered in Malaysia. "Corporate espionage doesn't keep me awake at night," agrees Hood Abu Bakar, General Manager of ICT, Group Information & Communications Technology, at MISC Berhad, a government-linked transportation company.

Attacks on critical infrastructures are also rare and usually target countries that are highly dependent on ICTs or have developed a particular military dependence on them, such as the US, Europe, China, Iran and Russia. Malaysia is neither high on the development curve nor does it appear to have any particular military ambitions. Hence there is little reason to expect such attacks. “Malaysia occupies a middle tier position in terms of development, so it is not an obvious target,” agrees Mike Usher, Director of Information Risk at Prudential Asia in Malaysia, a global insurance company.

Therefore, although global threats apply equally in Malaysia, some aspects of the country’s digital development make it more vulnerable to certain types of attacks, and these are primarily financially-motivated. “The primary cyber security concern in Malaysia now would be cyber crime,” agrees Andy Tan, CIO, RHB Group, a financial-services organisation. In particular, cyber criminals are likely to seize on a lack of awareness and target mobile devices and social media networks.

A lack of awareness

Social engineering techniques in which users are tricked into providing information that is used for criminal purposes are sophisticated and constantly evolving, highlighting the difficulty in keeping pace with cyber criminals. “Cyber security is not just about technology but also about people. They are the weakest link,” says Dr Amirudin. This points to a digital divide in which people with insufficient knowledge of cyber threats are particularly prone to suffer from them. “Some people are easy targets because there is a lack of awareness and education,” elaborates Dr Amirudin.

Although CyberSecurity Malaysia is already running educational programmes, such as CyberSAFE, to raise awareness for everyone, it is insufficient. An academic paper analysing Malaysia’s cyber security weaknesses suggests that creating awareness is particularly important given its rapid technological development and concludes that some of the educational programmes have not reached their intended audience.[26]

This anecdotal evidence is reflected in statistics. The Malaysia Computer Emergency Response Team (MyCERT), which tracks cyber attacks, shows a majority of all reported incidents in 2013 were fraud related, 4,485 out of a total of 10,636. Intrusion attempts (2,770) and malicious codes (1,751) followed, both of which could be related to financially-motivated malware and phishing. Together, the three categories constituted 85% of all reported incidents.[27]

Research by Trend Micro, a security company, also shows that Malaysia has the fourth highest number of botnet-connected computers globally as of the first quarter of 2013.[28] Similarly, according to the threat exposure rate (TER) in the Security Threat Report 2013 from Sophos, a security firm, Malaysia had the fifth highest percentage of PCs that experienced a malware attack in the world over a three month period.[29]

[26] Lalitha Muniandy and Balakrishnan Muniandy, State of Cyber Security and the Factors Governing its Protection in Malaysia:
http://www.ijastnet.com/journals/Vol_2_No_4_April_2012/14.pdf

[27] MyCERT: http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html

[28] Trend Micro: http://www.trendmicro.com/us/security-intelligence/current-threat-activity/malicious-top-ten/

[29] Sophos: http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2013.pdf

Mobility and social media

According to a 2013 lecture by Dr Amirudin, the more users go online, the higher the risk that they are exposed to cyber threats. Statistics show that 79% of those who spend more than 49 hours a week online, fall victim to cyber crime.[30] Such development is in part driven by increased mobile connectivity which enables more frequent usage of ICTs.

Malaysia's high mobile penetration therefore makes it a prime target for cyber criminals, especially as user awareness of such threats is typically even less than on stationary devices. "The biggest challenge is mobility and the lack of security that comes with it, whether it is laptops, tablets, or any other mobile device," agrees Mr Abi-Saab.

In additional to mobile attacks, Norton reports that social media threats are a particular concern in Malaysia, especially given high usage rates.[31] Out of those online, 88% of Malaysians have a Facebook account.[32] This conflates several problems as people are increasingly connected and often use social media apps on their mobile devices. "With the proliferation in the development and usage of mobile apps and smart devices, a lot of the cyber security challenges include protection against mobile cyber crime, application scam, and social media exploits," says Kashif Syed Haq, Chief Information Technology Officer of Celcom Axiata Berhad, a government-linked mobile operator.

[30] The Borneo Post: http://www.theborneopost.com/2013/04/06/79-per-cent-of-social-media-users-victims-of-cyber-crime/

[31] Computerworld: http://www.computerworld.com.my/resource/security/cyber-criminals-switching-to-mobile-targets-norton-in-malaysia/

[32] Malaysia Asia: http://blog.malaysia-asia.my/2013/09/malaysia-social-media-statistics.html

3. The Malaysian response

Malaysia's cyber security efforts to date have been proactive, extensive and clearly documented to support the country's digital development. "Overall, Malaysia is well-positioned at the international level," says Marco Obiso, Cybersecurity Coordinator at the ITU. "In terms of vision, they have it correct," agrees Datuk Mohd Noor Amin, Chairman of the UN-backed IMPACT. "They have also had the foresight to correctly identify the challenges."

Malaysia's National Cyber Security Policy is based on a common framework that is comprised of five pillars (legislation and regulation, technology, public-private cooperation, institutional and international aspects) across eight thrusts.[33] For instance, it seeks to "address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors" and was explicitly designed to "facilitate Malaysia's move towards a knowledge-based economy (K-economy)."

As in most countries, cyber security in Malaysia is a multi-stakeholder effort in which defence and national security departments tackle military strategy whereas civilian efforts are dispersed among government agencies, the private sector, academia and civil society. The rest of this section provides an overview of civilian cyber security efforts in the private and public sectors.

Public sector approach and key actors

Although most government agencies deal with cyber security to some extent, the roles and responsibilities of a few actors stand out. MDeC, though MSC, is charged with promoting ICT sector development, part of which is developing a local cyber security industry. MAMPU is tasked with cyber security in public sector agencies, including for the country's website portal.[34] CyberSecurity Malaysia is responsible for the nation's "e-security" from a technical perspective, which cuts across all government agencies, including to some extent national security. MyCERT handles domestic and international incident reporting and is part of CyberSecurity Malaysia. MCMC is the regulating agency for cyber security and oversees related areas, such as broadband development and digital signatures. The Royal Malaysia Police (RMP) is in charge of law enforcement. A brief overview of each actor will be given in turn.

Multimedia Super Corridor (MSC), an initative under the Multimedia Development Corporation (MDeC)

MSC is Malaysia's national initiative designed to attract international technology companies while grooming the local ICT industry. It has grown rapidly. According to its most recent annual report, 2012 saw record growth

[33] For details, see http://cnii.cybersecurity.my/main/ncsp/tncsp.html

[34] The Government of Malaysia's Official Portal: https://www.malaysia.gov.my

and revenue of RM 33.53bn, up by 5.7% from 2011, while exports grew to RM 11.6bn, a 14% rise from the previous year.[35]

The establishment of MSC in the mid-1990s and the introduction of cyber laws was a new beginning for Malaysia. “Since the launch of the MSC, the use of ICT in the government was greatly enhanced, hence the importance of cyber security management in the public sector. ” says Marsineh Jarmin, ICT Security Officer at MAMPU about the potential unintended consequences brought by rapid ICT development in the country.

In order to compete better internationally, MSC has since delved into the development of niche areas, one of which is cyber security. As part of this effort, Mr Amin proposed the establishment of IMPACT, the international cyber security organisation headquartered in Cyberjaya, with the aspiration to make Malaysia a global cyber security hub. The initiative has attracted a large presence by many foreign providers who benefit from various incentives schemes by setting up operations in the MSC geographic zone, such as F-Secure, a Finnish security company. In turn, the Malaysian government and domestic businesses get access to first-rate products and can leverage foreign know-how.

Malaysian Communications and Multimedia Commission (MCMC)
Tasked with regulating and enforcing laws in regards to the communications and multimedia industry in Malaysia, MCMC was established on 1 November 1998 through the Communications and Multimedia Commission Act 1998 (MCMCA). It supervises seven sectors (broadcasting, postal & courier services, mobile services, fixed services, broadband development, digital signatures, and the strategic trade act), most of which relate directly to cyber security.[36]

Its role is also to implement and promote national policy objectives for the communications and multimedia sector. According to Mohamed Sharil Tarmizi, Chairman of MCMC, this means that the organisation is an industry developer as well as a regulator. “We have a mandate to ensure that investments come into the country, that services are provided while at the same time, we have the responsibility to ensure the development of local skills and talent,” he says.

For instance, MCMC offers educational opportunities through its Digital Lifestyle Malaysia initiative, as well as through various programmes specifically targeting cyber security awareness such as the “Klik Dengan Bijak” or Click Wisely Campaign. In practice, Mr Tarmizi continues, this means the MCMC is involved in infrastructure, applications and services, improving quality of service, and related security issues.

[35] MSC: http://www.mscmalaysia.my
[36] MCMC: http://www.skmm.gov.my/Home.aspx

Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)

"Most websites are hacked not because hackers are good but most likely because the websites are not secured," says Ms Jarmin. To tackle this challenge, the ICT Security Division at MAMPU developed an information security handbook and guidelines for the public sector in the year 2000 called the Malaysian Public Sector ICT Security Handbook. Today, MAMPU continues to provide ICT security consultancy services to the public sector through workshops, courses and seminars and offers a forum for discussion via the Government ICT Security Portal (GSWP).[37]

Their efforts particularly benefit local governments. Mingu Jumaan, Director of State Computer Services Department (SCSD) in Sabah State Government, says he received assistance from MAMPU to implement ISO 27001:2005, a technical cyber security standard. Sabah became the first State Government agency in Malaysia to be certified on 13 January 2012. Mr Jumaan says that SCSD is now in the process of upgrading to the recently released ISO 27001:2013 and targets certification by mid-2014.

The Malaysian Public Sector ICT Security Handbook is still in use but the work is never ending. Since the introduction of the 10th Malaysia Plan, MAMPU initiated the centralisation of government data center management and efforts to bring security to a level of international standards, according to Ms Jarmin. "MAMPU is responsible to coordinate the ICT development for the public sector" she says.

CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI)

Currently known as CyberSecurity Malaysia, the agency was established by regulation H609/2005 on 28 September 2005 as the National ICT Security and Emergency Response Centre (NISER), a national body to monitor the nation's e-security.[38] "Our role is as the cyber security national technical experts or specialist, and to become the reference point for cyber security in the country," says Dr Amirudin. "In simple English: we are the IT security department expert for the country."

As a provider of specialised services, CyberSecurity Malaysia has instituted a broad range programmes, such as CyberSAFE, an educational initiative to raise awareness of cyber threats, Cyber999, a helpline, Digital Forensics (Cyber CSI), as well as information security certifications, professional development and multilateral engagement, amongst other efforts.[39] CyberSecurity Malaysia also has an industry collaboration programme that works with both local and foreign actors, although it is largely focused on

[37] MAMPU: http://www.mampu.gov.my/web/en/ict-security
[38] CyberSecurity Malaysia: http://www.cybersecurity.my/data/content_files/46/1235.pdf?.diff=1392970989
[39] CyberSAFE: http://www.cybersafe.my/; for all services, see http://www.cybersecurity.my/en/our_services/mycert/main/detail/2328/index.html

finding new business opportunities rather than providing a platform for public and private information-sharing regarding cyber threats.[40]

Since 2013, CyberSecurity Malaysia is also asked to provide technical assistance and training services for national cyber crisis management, per Order No. 24 of the Dasar dan Mekanisme Pengurusan Krisis Siber Negara (Policy and Mechanism for National Cyber Crisis Management). In practice, this means the agency helps government ministries or other agencies that need technical cyber security assistance, including the National Security Council (NSC). “We are the national technical arm for the NSC by supporting them to work on long-term strategic policy and direction and on how to manage cyber security and monitor the state of health of e-security of the nation,” summarises Dr Amirudin.

Malaysia Computer Emergency Response Team (MyCERT)
A CERT is designated to handle computer security incidents from a technical perspective. The approach was established at Carnegie Mellon University in the US in 1988 and today most countries have a CERT, sometimes affiliated with the government and sometimes not.

MyCERT was formed on 13 January 1997 and operates out of the office of CyberSecurity Malaysia. Like other CERTs, it provides assistance in handling incidents, tracks data, and works closely with law enforcement agencies such as the Royal Malaysian Police (RMP), as well as with the Securities Commission, and Bank Negara Malaysia, and has close collaboration with Internet Service Providers (ISP) and global computer security incident response teams, such as OIC-CERT and APCERT.

Royal Malaysia Police (RMP)
Malaysia established its Computer Crime Act in 1997 and the RMP is in charge of enforcing it.[41] To do so, RMP has a commercial crime unit tasked with white collar crimes such as fraud, breach of trust, and cyber-crime, although by necessity it also has to work with multiple stakeholders in regards to enforcement given ever blurring lines between online and offline crimes. “All crimes can have a cyber component in them because that’s the environment we live in today,” says Mr Tarmizi. “It is a fallacy to think that any one agency can be the ultimate cyber cop.”

Another challenge facing RMP is the recent development of stiffer privacy laws. Initially passed in 2010, Malaysia’s new privacy regulations went into effect on November 15, 2013.[42] Companies had until February 15, 2014, to comply with them and failure to do so can result in fines and imprisonment.[43]

[40] CyberSecurity Malaysia: http://www.cybersecurity.my/en/our_services/industry_development/main/detail/2335/index.html
[41] Malaysian Computer Crime Act of 1997: http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf
[42] ZDNet: http://www.sdnet.com/my/malaysia-gasettes-data-protection-act-effective-immediately-7000023239/
[43] The Malaysian Bar: http://www.malaysianbar.org.my/notices_for_members/personal_data_protection_act_2010_partnerships_to_register_with_commissioner_by_15_feb_2014.html

Although Malaysia is moving in the right direction, questions linger regarding enforcement. “Privacy laws are just coming into force and we don’t expect them to be enforced to the same level as in Singapore and Hong Kong,” says Mr Usher.

International engagement

Malaysia’s commitment to cyber security goes beyond its borders. Besides ad-hoc collaborations with individual countries, Malaysia has played a role in establishing both the OIC-CERT as well as the internationally-recognised IMPACT, which is supporting ITU in delivering its mandate on building confidence and security in the use of ICTs. “Such initiatives show their engagement at the international level,” commends Mr Obiso at ITU.

Organisation of The Islamic Cooperation - Computer Emergency Response Teams (OIC-CERT)[44]

The formation of a CERT among OIC members was proposed in Malaysia in 2005 and task force meetings established its presence a year later. Malaysia, represented by CyberSecurity Malaysia, is one of six co-founders (along with representative agencies from Nigeria, Saudi Arabia, Tunisia, Pakistan, and the UAE). OIC-CERT provides a platform for collaboration and to explore lessons learned and best practices to strengthen cyber security.

In January, 2013, CyberSecurity Malaysia was appointed to chair the organisation (while also holding a Secretariat position). Today, OIC-CERT includes 22 CERTs and cyber security related agencies from 18 countries.

Asia Pacific Computer Emergency Response Team (APCERT)[45]

Malaysia is on the Steering Committee of APCERT, which provides a network of security experts in the Asia Pacific region to improve awareness and competency regarding computer security incidents.

This includes enhancing regional and international cooperation, joint measures to deal with security incidents, information-sharing, collaborative research and development, assistance, and help to address legal issues related to information security across boundaries. Today, APCERT consists of 26 member teams across 19 economies.

International Multilateral Partnership Against Cyber Threats (IMPACT)[46]

Supported by the Malaysian government, IMPACT, headquartered in Cyberjaya in Kuala Lumpur, was founded in 2008 with 30 member states and officially became affiliated with the ITU in 2011. Today, with 147 nations as members, it is the world’s largest cyber security alliance.

[44] OIC-CERT: http://www.oic-cert.net/v1/index.html
[45] APCERT: http://www.apcert.org/index.html
[46] IMPACT: http://www.impact-alliance.org/home/index.html

“The establishment of IMPACT speaks volume of Malaysia’s commitment to cyber security,” says Mr Amin, as the country provided seed funding for operations and extended a free 30-year lease for their headquarters.

A key aspect of its rapid development has been close collaboration with private sector partners who have provided IMPACT with threat information, which it has compiled to create a composite picture that is better than each individual player can see on their own. IMPACT also provides access to expertise and information through the Global Response Centre (GRC), NEWS (Network Early Warning System) and ESCAPE (Electronically Secure Collaboration Application Platform for Experts).

In addition to international collaboration through NEWS and ESCAPE, IMPACT provides training and skills development to cyber security initiatives in UN member states. In the last three years, it has conducted assessments in over 50 countries and has helped to establish six national CERTs.

The challenges of public-private collaboration

Information-sharing between sectors is often cited as key to better cyber security. Initiated in 1997 to assess threats and vulnerabilities by US President Bill Clinton, the Commission for Critical Infrastructure Protection recommended stronger public-private partnerships to enhance protection, a message that has been repeated since. Most international reports say public-private collaboration is important, yet the outcome of such initiatives have been uneven.

For instance, a December 2008 report from the Center for Strategic and International Studies (CSIS), a bi-partisan US non-governmental organisation (NGO) highlights gaps in collaboration. “Despite broad recognition of the need for partnership, government and the private sector have taken separate paths. Indeed, the so-called partnership as it now exists is marked by serious shortcomings. This includes the lack of agreements on roles and responsibilities, an obsession with information sharing for its own sake, and the creation of public-private groups each time a problem arises without any effort to eliminate redundancy.”[47]

Such deficiencies continue today, not only in America, but in most countries that engage in various forms of public-private collaboration, including in the United Kingdom. The theoretical benefits are simply trumped by practical reluctance to share sensitive information and the process for doing so is often inadequate. In light of potential liberalisation of critical infrastructures, Malaysia would do well to learn from previous mistakes in this area as it seeks to strengthen the relationship between

[47] CSIS: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

the public and private sectors. Perhaps the most crucial such lesson is to clarify roles and responsibilities, an area in which Malaysia also has some ways to go.

The private sector approach

In broad terms, there are two types of companies in Malaysia: GLCs in which the government holds a controlling stake or other private sector companies, including small and medium-sized enterprises (SMEs).[48]

A key question for cyber security is what happens if the country liberalises the role of GLCs in critical infrastructures, such as energy, transportation, banking and finance, or other "National Key Economic Areas."[49] For instance, the 10th Malaysia Plan calls for "rationalising the role of GLCs in the economy," including increased privatisation.

However, interviewees are unconcerned about such potential development as they do not see a difference regarding preparedness between GLCs and others in the private sector. "It doesn't matter if you are a GLC or not; cyber security is something we have to worry about regardless what kind of company we are," says Mr Bakar at MISC Berhad, a GLC. "It more depends on the industry you are in," says Daniel V.C. Lee, CIO at Felda Global Ventures, a GLC in the agricultural business, and cites banks and telecommunications companies as particularly vulnerable to cyber threats.

Collaboration, or the lack thereof

Relatively high cyber security awareness among banks and telecommunications companies has made formal private-public collaboration somewhat redundant (and virtually non-existent). Financial institutions such as Maybank and CIMB Bank, both GLCs, have full-page advertisements in The Star, a local English-speaking newspaper, which alert people against online banking scams as part of an ongoing industry campaign by the Association of Banks Malaysia (ABM) in co-operation with CyberSecurity Malaysia.[50] "We are very sure that this will not be a one-time-off activity but one which requires multiple repeats," says Mr Tan at RHB Group about the industry's efforts to educate the public about cyber security.

Being a top performing government-linked company, Celcom is expected to take the lead in protecting and maintaining the confidentiality and

[48] For a definition of GLCs, see http://www.khazanah.com.my/faq.htm#ques8

[49] According to the Malaysia 10th Plan, National Key Economic Areas are 1. Oil and gas; 2. Palm oil and related products; 3. Financial services; 4. Wholesale and retail; 5. Tourism; 6. Information and communications technology; 7. Education; 8. Electrical and electronics; 9. Business services; 10. Private healthcare; 11. Agriculture; and 12. Greater Kuala Lumpur [the geographic area].

[50] The Star: http://www.thestar.com.my/News/Nation/2012/05/27/Top-banks-join-forces-to-fight-fraud/

privacy of customer information," says Mr Haq, the company Chief Information Technology Officer, to illustrate the efforts also under way in the telecommunications industry. Last year, Celcom won the Cyber Security Organisation of the Year Award at the CSM-ACE 2013, the first and only telecommunications service provider to be recognised since the inception of the awards in 2009.[51]

Despite such efforts, the need for greater information-sharing between the public and private sectors is likely to rise, especially as the country privatises GLCs. For instance, at a recent event in Kuala Lumpur, Sazali Sukardi, Vice President of Research at CyberSecurity Malaysia, said that current lack of data sharing affects the ability to gather threat information from multiple sources.[52] Yet, the ability to compile greater amounts of data is a key aspect to enhance cyber security.

Greater collaboration can also benefit smaller players, which are likely to be a key aspect to future cyber security efforts in Malaysia as the country seeks to nurture the domestic ICT industry. "SMEs who are just embracing ICTs are getting hit by all sorts of attacks," warns Mr Tarmizi.

Yet, most private sector companies look to enhance cyber security internally or through industry collaboration. The overall security roadmap requires us to build the right organisation internally," says Mr Haq. "We have external partners as in vendors but no formal partnership with the government, no," says Mr Abi-Saab, while Mr Bakar agrees that government interaction is not really a priority. "The private sector in Malaysia tends to do things on their own," says Mr Amin. "In terms of sharing information, that is not happening."

Awareness, awareness, awareness

Reflecting the country's level of digital development generally, the private sector in Malaysia is similarly concerned with raising awareness, in particular across three key areas: employees, customers, and among senior executives.

As a company in a critical infrastructure, Celcom handles lots of customer related information, which also makes it a target. "This makes it all the more imperative to have increased controls to prevent cyber security attacks that are targeted towards our enterprise and the immense amount of customer data that we possess," says Mr Haq.

Anecdotally, Malaysian financial services institutions and telecommunications companies are said to be relatively doing well in their cyber security efforts, including in raising awareness among customers. "Banks and telecoms do a reasonable job," says Mr Usher, who as Director of Information Risk Asia oversees operations in more than a dozen countries and often compare policies across the region. "But in many corporates, there is also a lack of

[51] CSM-ACE: http://www.csm-ace.my/awards.html
[52] IQPC, 4th Annual Cybersecurity for Government Summit: http://www.cybersecurityasia.com

awareness," he continues, to illustrate that the private sector more broadly still has some ways to go. Corporate practices and awareness in general is not as much what it is compared to the developed countries," agrees Mr Haq. Mr Usher also sees a trend in that cyber attackers are using individual employee information to attack corporate entities.

The challenge of awareness also extends beyond employees and users as senior management and IT departments often do not communicate well in this area. "Senior management wants to know how to enable more business and to create a competitive advantage by having access to data safely," says Mr Abi-Saab. "But IT personnel don't know how to speak to management because they come from a technical background and to them it is all about servers, firewalls, and IP addresses, and if you mention this to senior management, they won't get it."

This disconnect is a global problem that is unfortunately also manifest in Malaysia, which leads to practical concerns. "Education is not just about staff but also the board of directors and senior management," says Mr Lee about the basic challenge at an agricultural company. "They carry a lot of confidential documents and that's the first thing I need to protect." At RHB Group, Mr Tan rates awareness among senior management as reasonably good. "We are making every effort to raise the level of cyber security awareness," he says.

At Prudential, Mr Usher developed an extensive cyber security dashboard to monitor progress in technical terms only to find that it didn't resonate with management. As a result, he has now simplified the dashboard and replaced technical lingo with terms that executives can understand. "Translating technical terms to business language is the only way to be successful," advises Mr Abi-Saab. "When speaking to the board you focus on efficiency gains and how to save money, and then they will adopt your ideas," he says about a recent effort to introduce cloud computing in the enterprise.

The Snowden impact on business

In 2013-14, the revelations by Edward Snowden, a former US government contractor who exposed extensive surveillance by the American National Security Agency (NSA), completely changed the international discourse on cyber security. Although many aspects have been politically sensitive and contentious it is also possible that the attention they have garnered may lead to improved cyber security as awareness and transparency rises. "Mutual dialogue among all countries is beneficial," says Mr Obiso, who is the Cybersecurity Coordinator at the ITU. "We need greater transparency to restore trust and to build global understanding."

One aspect that is particularly applicable to business is data privacy. As the online population continues to rise and companies seek the benefits of new technologies, such as cloud computing, this is also especially relevant in Malaysia. "Awareness of information security and our privacy in the cyber space has increased as a result of the revelations and there are concerns about the reliability of products and services from overseas," says Dr Amirudin.

For instance, the push towards cloud computing means that data fall under the jurisdiction where it is stored and used. Hence, data on a server in the US is subject to American privacy regulations even though the owner could be in another country – in fact, most users may not even be aware of where their information is located. American cloud providers

currently have an 85% global market share, although that may decrease as non-US customers discover that they are subject to American data regulations.[53]

The Snowden allegations show that the NSA uses legal, though sometimes controversial, ways to access such data without court orders in the name of national security. In response, several jurisdictions, such as the European Union, are keen to enhance their own cloud computing capabilities in order for the data to fall under their regulations. Such localisation strategy – geographically storing data where it is used – is a global trend. "We welcome foreign products but we don't want to be too dependent on them. We hope to be able to make Malaysia's CNII more secure, resilient and self-reliant," says Dr Amirudin.

The rise of sovereign clouds, or data localisation regulations, can enhance data privacy control and also benefit domestic cloud providers as they enter this growing market. Gartner, an IT consultancy, estimates the value of global cloud services in 2013 to be USD 131bn, up from USD 111bn a year earlier.[54] In response, American providers are therefore contemplating how to counterbalance this trend. Microsoft, for instance, recently announced that they would let their customers select where their data is stored in order to avoid potential domestic regulations.[55]

Effectiveness vs security
Companies often struggle to take full advantage of emerging technologies that promise to enhance productivity as they simultaneously bring new security

[53] The Independent: http://www.independent.co.uk/life-style/gadgets-and-tech/news/mps-call-for-government-to-consider-ending-use-of-cloud-amid-concerns-that-us-authorities-can-access-information-8473693.html
[54] Gartner: http://www.gartner.com/newsroom/id/2352816
[55] Network World: http://www.networkworld.com/news/2014/012314-microsoft-cloud-278034.html

challenges that need to be managed carefully. “We’re trying to address it in a manner that makes sense to us where it doesn’t slow down day-to-day operations,” says Mr Bakar.

A particular example is the rapid rise of cloud computing. MDeC, for instance, is pushing SMEs to adopt it, according to an email statement from the organisation. Although such efforts can theoretically enhance security by outsourcing data management to a specialist provider it also exposes companies to new challenges that they may be unaware of, such as differences in cross-border data regulations. “Organisations don’t want their data to be seen and potentially given to a competitor,” says Mr Abi-Saab. “The NSA revelations are a huge red flag.”

Beyond potential foreign data interference, mobile devices also present a key challenge to the private sector. Employees increasingly bring their own devices to the workplace and often work remotely creating new efficiencies but also exposing their organisation to new conundrums. “There are a lot of people with mobile devices in our industry who carry engineering documents that, if lost, could result in millions of dollars of lost contracts,” says Mr Abi-Saab. Hence companies must increasingly look to secure such devices in particular as mobile malware is rising rapidly and can either access information or compromise it.

In this effort, Data Loss Prevention (DLP) programmes to proactively monitor data, remote wiping capabilities of physically lost devices, and remote storage solutions, are all on the rise. Hence, in an ironic twist, private enterprises often come full circle as they look to cloud solutions to centralise data control and management. “In our view, a cloud environment is safer,” says Mr Abi-Saab about the company’s recent move to such a platform.

4. Tackling future challenges

The desire for greater digital development comes with unintended consequences. Some countries with high levels of Internet penetration are going digital by default, meaning that public sector services are delivered via ICT channels in the first instance and sometimes only so. Such efforts enhance efficiency but can also exclude the small portion of the population that remain offline or those who do not have the skills to conduct services on their own and therefore have to seek digital assistance.

Similarly, as countries engage in ICT trade, primarily exports, to reap the benefits of global opportunities, new challenges also await. Many buyers are increasingly voicing geopolitical concerns in which the country of origin and ICT supply chains are scrutinised, also leading to questions surrounding IPR.

To solidify cyber security moving forward, there also needs to be clear domestic roles and responsibilities as well as greater public and private information-sharing in order to counter increasingly sophisticated threats.

Although Malaysia has some ways to go before reaching the levels of digital development in Japan, South Korea and Singapore, now is the time to recognise such challenges resulting from the country’s promotion of ICTs and how they relate to cyber security.

Digital divides

Connectivity and usage are key to an efficient digital economy, yet countries around the world suffer from numerous digital divides. Malaysia is no different in this area and although broadband and mobile phone penetration rates are generally high, more than a quarter of the population remains offline and access is uneven. In particular, there is an urban/rural divide between Kuala Lumpur – which has almost twice the number of online users – and rural areas. The same essentially holds true for mobile phone penetration and access to laptop and tablet devices (see figure 4 on next page).

Initiatives such as the 1Malaysia Netbook, which provides a basic computer to underserved people in underserved areas, bode well but more needs to be done.[56] To reap the full benefits of a digital society, Malaysia must not only close the access gap but also improve useful usage -– whether people have the ability to use their access for productive purposes and can leverage the supply of services available to them. Denmark, for instance, reckons that the government will save an estimated EUR 160m a year once public service communication is completely digital.[57]

[56] 1Malaysia Netbook Official Portal: http://1malaysianetbook.com.my/

[57] Danish Agency for Digitisation, eGovernment strategy 2011 – 2015: http://www.digst.dk/Home/Digitaliseringsstrategi/Download%20strategien

Figure 4: Regional connectivity in Malaysia

	Percent of households with access to:				
	Broadband penetration rate	**Personal computer**	**Laptop**	**Tablet**	**Mobile phone penetration**
Johor	65.1	19.0	45.5	12.2	128.7
Kedah	53.3	16.0	38.6	8.6	118.8
Kelantan	41.9	14.8	29.4	4.9	107.8
Melaka	64.7	28.2	50.2	21.1	143.6
Negeri Sembilan	74.6	17.9	29.7	6.7	144.7
Pahang	60.1	19.3	47.4	9.6	134.8
Perak	51.7	19.6	34.7	9.3	114.6
Perlis	67.4	11.3	42.7	7.3	139.6
Pulau Pinang	80.3	24.0	45.6	10.7	142.3
Selangor	79.1	28.7	57.6	26.5	154.4
Terengganu	57.3	12.9	42.1	9.4	132.6
Sabah	53.8	16.3	45.3	10.7	87.6
Sarawak	53.5	16.7	41.8	9.5	105.7
WP Kuala Lumpur	111.7	28.2	64.7	37.4	203.5
WP Labuan	64.0	23.3	68.6	21.4	120.6
WP Putrajaya	81.9	20.2	72.4	42.3	87.0
Malaysia	**67.1**	**21.0**	**46.3**	**15.3**	**143.6**

Sources: MCMC, Communications & Multimedia Pocket Book of Statistics, Q4 2013; Department of Statistics Malaysia (DOSM), 2012.

The usage divide is important to cyber security. In Malaysia, a lack of awareness is often cited as a weakness and further efforts to improve knowledge will be key to enhancing cyber security more broadly. Useful usage will require a shift in focus from providing access towards greater education and Malaysia would do well by incorporating cyber security awareness into school curriculums.

The digital divide also extends to the lack of cyber security professionals in the country. According to CyberSecurity Malaysia, there are only about 800 security professionals in the country today.[58] Yet, in three years, the same agency reckons Malaysia will need 7,000 of them, a number likely to at least double by 2020 when it has reached developed country status.

[58] CyberSecurity Malaysia, Frequently Ask Questions: http://www.cybersecurity.my/en/media_centre/media_faqs/media_faqs/main/detail/1691/index.html

ICT trade

The 10th Malaysia Plan already acknowledges increased global competition in export-led manufacturing but remains firm in its commitment to increase trade, a decision that is likely to lead to new challenges as cyber security concerns loom large in ICT supply chains. Despite the economic benefits of global trade, policy-makers are sometimes concerned with foreign manufactured products. For instance, Huawei, the Chinese telecommunications maker, was deemed as a potential threat to US national security and is not able to provide the full range of its services in the country.

In an ironic twist, it recently surfaced that the NSA has installed listening components into Huawei equipment, essentially the same thing that US policy-makers believed that Huawei might do to them.[59] Such tampering creates global concerns, and increasingly so as ICT supply chains expand and cyber security becomes more important with rising levels of digital development.

Assuming Malaysia succeeds in keeping its current ICT export share – and perhaps even grow it – such geopolitical concerns are likely to increasingly face domestic manufacturers who will need to show their commitment to cyber security to skeptical buyers. This requires greater effort for Malaysia to build political trust at a global level.

To some extent this is already happening. The Association of Southeast Asian Nations (ASEAN) urges its members to improve cyber security, in part through enhanced regional cooperation with China, Japan and South Korea.[60] The Asia-Pacific Economic Cooperation (APEC) Strategic Plan for 2010-2015 also calls for a safe digital environment and improved regional cooperation.[61] Such efforts include a cyber security awareness programme with the OECD Working Party on Information Security and Privacy (WPISP) as well as collaboration with Computer Security Incident Response Teams (CSIRTs). Malaysia is also leading an ASEAN project on the security of mobile devices.

Yet, as Malaysia continues to push ICT exports, the need to further partake in the international discourse will rise accordingly. This means the country will have to supplement technical collaboration with policy engagement and complement regional forums with global ones.

Intellectual property rights

The protection of IPR is a global problem that is particularly relevant in an Asian context. This is reflected in current negotiations over the Trans-Pacific Partnership (TPP), a free trade agreement with 12 negotiating members,

[59] Bruce Schneier: https://www.schneier.com/blog/archives/2014/01/halluxwater_nsa.html

[60] ASEAN: http://www.asean.org/news/asean-statement-communiques/item/joint-media-statement-of-the-12th-asean-telecommunications-and-it-ministers-meeting-and-its-related-meetings-with-dialogue-partners

[61] APEC, Strategic Plan for 2010-2015:
http://www.apec.org/Home/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information

including Malaysia. TPP raises the bar as members agree that they will not only follow but also expand upon the legal rights and obligations described in the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).[62]

From a cyber security perspective, IPR theft, in the form of counterfeit products, poses two challenges.

First, a potential loss of revenue for businesses. This is a particularly relevant concern as Malaysia develops niche areas in ICT in accordance with the 10th Malaysia Plan and further expands its role in global ICT supply chains. Stronger IPR protection will ensure that domestic companies get the revenues they deserve.

Second, since pirated products can't be properly secured and are not eligible for automated updates, it leaves those using them with an increased exposure to cyber threats, such as malware. This is also particularly concerning for Malaysia as the country is anecdotally weak in enforcement and the country suffers from a disproportionally high number of infected computers. Stronger domestic action will likely decrease the use of pirated software and also lead to better cyber security.

Overlapping domestic interests

In theory, the roles and responsibilities of public sector agencies in Malaysia are clear while the private sector is largely absent from any collaborative efforts. But in practice there is concern in overlapping organisational interests. This is a common problem around the world – perhaps particularly illustrated in the US where there are numerous competing agencies – but the fact that it also applies in Malaysia should warrant domestic attention. “Like many other countries around the world, Malaysia too has a coordination issue between agencies,” agrees Mr Amin, something which is reinforced by multiple interviewees for this report.

Although to some extent this includes MSC and MAMPU, the primary overlapping interests involve MCMC and CyberSecurity Malaysia. “We think as long as we have responsibility to build and expand broadband, access and commerce, we also have the responsibility of expanding people's knowledge in using these things,” says Mr Tarmizi. “We also provide awareness and education,” counters Dr Amirudin. “This is not a specific mandate by the government to us, but it is part of the mandate to ensure the health of e-security of the nation.”

Besides overlapping educational efforts (which may ironically be a good thing, given low levels of awareness), there is also overlap in regards to the role of

[62] The New York Times: http://www.nytimes.com/2014/02/26/business/pacific-trade-talks-end-inconclusively.html?_r=1

providing assistance to other government entities with MAMPU, MCMC and CyberSecurity Malaysia all claiming to have such a remit, albeit in slightly different forms. Similarly, in terms of developing the ICT sector, MSC, MCMC, and CyberSecurity Malaysia all have their own initiatives, ranging from industry collaboration to efforts to build infrastructure and in attracting FDI.

Conclusion and recommendations

By most estimates, Malaysia is doing relatively well in cyber security. But to reap the full benefits of the information society as the country develops, Malaysian executives and policy-makers should consider the lessons learned elsewhere and develop appropriate measures to meet the cyber security challenge moving forward. Although it is acknowledged that a lot of this work is already under way, findings throughout this report indicate that the following measures can be enhanced further.

1: Pursue digital by default, but don’t neglect trust

“The extensive use of ICT and rapid changes in technology, bring new challenges,” says Dr Amirudin. For instance, as the public and private sectors expand their online services and move towards greater digital efficiency, the focus on whether users can take advantage of them will also increase. In this regard, greater efforts are needed to extend connectivity to the approximate one-third of the population that remains offline and to educate those who are already online about cyber threats. In addition, useful usage assumes a certain level of trust in online services, an area in which Malaysia needs to do more.

“ICT security in government today is more challenging because engagement can be abused by others,” says Ms Jarmin. “It’s a challenge to build trust and we have to create more awareness amongst ourselves.” To do so, MAMPU has initiated programmes to further enhance public electronic system service delivery. The latest being the introduction of “Malaysia Trust Mark” to certify certain online services.

In the private sector, RHB Group and other financial services institutions are enhancing their efforts to educate users. “Despite having an ongoing awareness programme, most of the customers are not able to differentiate between a genuine website and a phishing website,” says Mr Tan about the problem facing the industry; 40% of all RHB retail customers bank online today. “This is an industry wide issue,” he continues, indicative by the fact that financial services institutions have come together to raise trust and awareness. The country would do well by building on such initiatives to create a foundation for greater trust at all levels, including in the private sector more broadly, to stimulate productive and safe use of ICTs.

2: Compete globally and move from international technical cooperation to policy engagement

“This is not the time to withdraw but to accept and embrace the rules of the game in terms of global competition," says the 10th Malaysia Plan. Mr Ezell also agrees that an open and liberalised ICT sector is clearly beneficial to development. "It will require greater effort to ensure that Malaysia continues to be a beneficiary of globalisation," continues the 10th Malaysia Plan.

But the inability to move forward with a new ITA agreement to expand free ICT trade and the introduction of new data regulations around the world, are both indicative of an increasingly geopolitical environment.

Malaysia is already engaged in numerous technical and trade initiatives – such as OIC-CERT, APCERT, IMPACT, ASEAN, APEC, and TPP. But combined with its efforts to attract ICT companies and promote industry exports, the time is ripe to build on its aspiration and further enhance policy engagement.

Greater such efforts will enable Malaysia to build trust – and to trust others when it comes to IPR regulations and new technologies such as cloud computing. To do so will require Malaysia to elevate its international efforts beyond technical and trade cooperation to also address global ICT governance and cyber security collaboration from a policy perspective.

3: Tackle the lack of awareness at all levels

Cyber growth has outpaced awareness and several interviewees cite it as a fundamental problem to improve cyber security, also indicative by the number of malware and phishing incidents in the country. There are multiple levels of a lack of awareness, starting with those who come online for the first time and are targeted by financially-motivated social engineering techniques, in particular via mobile devices and on social media networks.

Creating a culture of cyber security," and "continue to raise industry awareness," are key initiatives to further improve cyber security in Malaysia, suggests Mr Haq. In this effort, the country would do well by introducing cyber security into school curriculums, in particular as it has begun to distribute computers to underserved people and areas.

Lack of awareness extends to the private sector, which is facing the dual challenge of educating both external customers and internal users. At the same time, senior management are pushing the use of new technologies to improve efficiency, yet lack a complete understanding of the associated challenges as they are typically presented to them in technical terms instead of in business language. "It is not good enough if the CIO knows about cyber security, the CEO must understand it too," says Mr Tarmizi.

4: Prepare for politically-motivated attacks by establishing a foundation for collaboration between sectors

As Malaysia develops niche industries in ICT and plays a central role in global supply chains, it is likely that politically-motivated threats such as espionage activities will increase over time. Yet, there is a lack of formal public and private sector collaboration. “A way to further improve cyber security in Malaysia is through collaboration,” says Mr Tan. Although the National Security Council organises an annual cyber crisis drill involving both the public and private sector actors in various critical infrastructures, there does not appear to be any ongoing efforts, despite its potential benefits. “With collaboration, we should be able to observe and anticipate cyber security trends and share useful information to prevent and respond effectively to cyber threats,” continues Mr Tan.

As the 10th Malaysian Plan calls for increasing privatisation and rationalising the role of GLCs, the time is ripe to consider the potential impact on cyber security. Calls to liberalise critical infrastructure sectors will result in the need to build a stronger foundation for information-sharing and formal interactions between the public and private sectors. This is both a challenge to implement new processes but also an opportunity to proactively put in place enhanced information-sharing to meet emerging threats.

This may or may not entail public-private cooperation as envisioned in the West. Although such attempts have been well-intended, they have largely failed. Malaysia would do well in evaluating the challenges such initiatives have faced, in particular overlapping interests between domestic organisations and to adapt those lessons to the local environment.

5: Clarify domestic roles and responsibilities
Malaysia suffers from two organisational deficiencies. In light of new data privacy laws, the first is an anecdotal lack of criminal enforcement. “We need a few test cases, we need people to get caught and make cyber security more visible,” suggests Mr Bakar. “That will raise awareness.” Hence, the country needs to strengthen not the regulatory environment but rather the enforcement thereof.

The second issue surrounds overlapping domestic organisational interests. MSC, MAMPU, CyberSecurity Malaysia and MCMC – all acknowledged to do well on their own – overlap to some degree and do not cooperate to the fullest extent possible. It is not a situation unique to Malaysia but it would behoove the country to better delineate their efforts.

For instance, the potential liberalisation of GLCs, in which greater assistance might be needed by the private sector, is also a good opportunity to improve collaboration between agencies and in the process establish formal information-sharing between the public and private sectors. “Everyone has a role to play,” concludes Mr Tarmizi, about enhancing cyber security in the country. To seize on this sentiment, Malaysia needs to clarify roles and responsibilities in order to avoid domestic turf battles and streamline the effective use of resources to meet the cyber security challenges moving forward.

About DAKA advisory

We provide strategic advisory and research services in cyber security, e-government, measurement of the information society and related topics primarily for the public sector or those interested in it. Our projects span the globe as we help clients improve their internal effectiveness through strategic reports and assist them in reaching an international audience via white papers, custom research, speaking engagements, and thought leadership distribution. Our independent analysis is paramount and our list of clients speaks for itself.

For more information, please contact Kim Andreasson, Managing Director, at kim@DAKAadvisory.com

Visit us at:
www.DAKAadvisory.com

Disclaimer

Our aim is always to provide accurate information from reliable sources. However, neither DAKA advisory, nor the sponsor, can accept any responsibility or liability for the data, information or statements contained within this report.