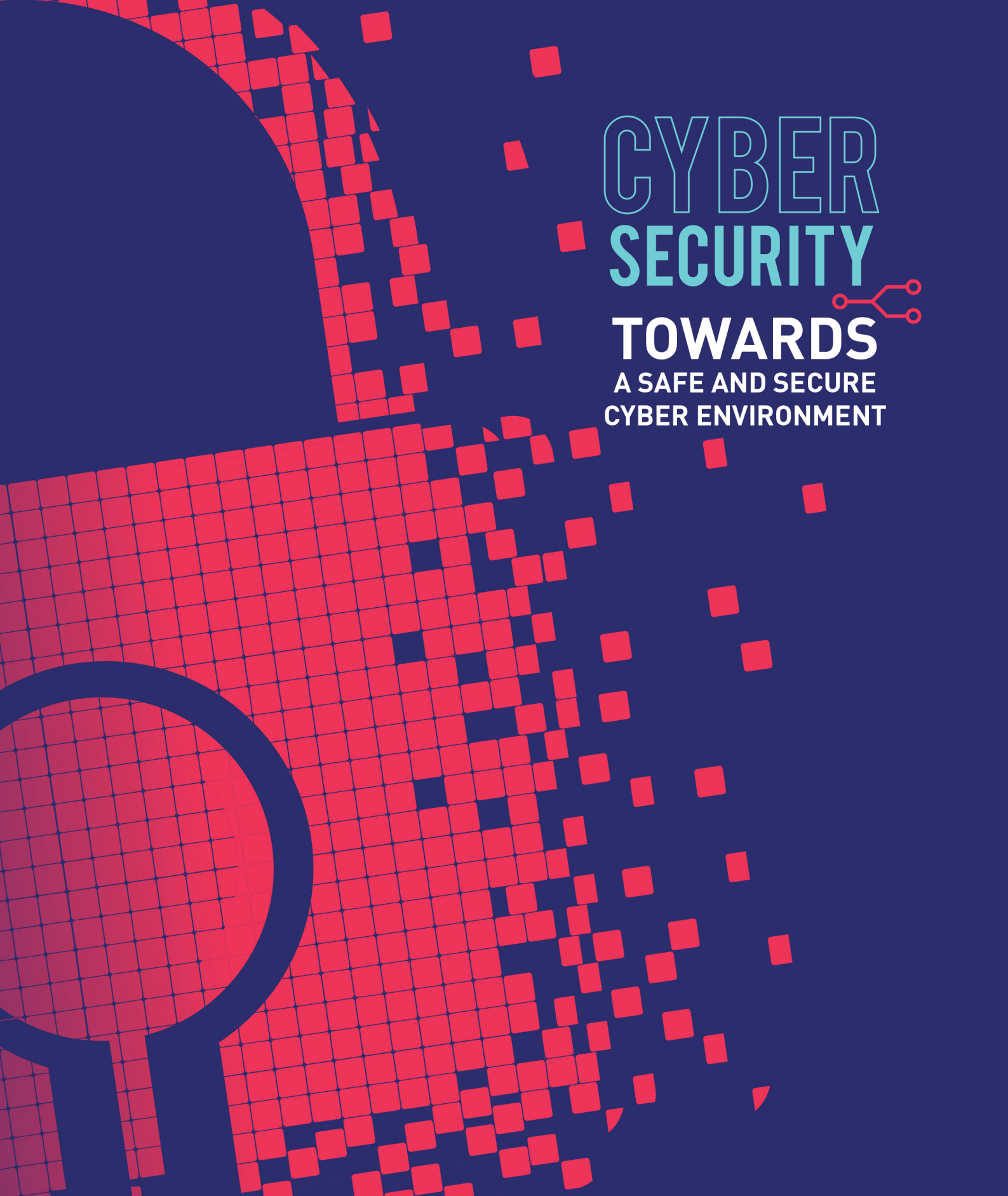

CYBER
SECURITY
TOWARDS
A SAFE AND SECURE
CYBER ENVIRONMENT

CYBER SECURITY

Towards A Safe and Secure Cyber Environment

2018

Cyber Security
Towards a Safe and Secure Cyber Environment

Academy of Sciences Malaysia
Level 20, West Wing, MATRADE Tower
Jalan Sultan Haji Ahmad Shah off Jalan Tuanku Abdul Halim
50480 Kuala Lumpur, Malaysia

Perpustakaan Negara Malaysia Cataloguing-In-Publication Data
Cyber Security
Towards a Safe and Secure Environment

ISBN 978-983-2915-38-6
1. Cyberspace--Safety measures
2. Computer networks--Safety measures
3. Internet--Safety measures
005.8

CONTENTS

Foreword

The Academy of Sciences Malaysia (ASM) has been entrusted with the mandate to be a "Thought Leader" in the science, technology and innovation (STI) arena and we consider this an immense responsibility to our society and nation. The Academy translates this mission into action by undertaking strategic STI studies and delivering programmes that mobilise a wide spectrum of expertise not only within the Academy but also its network of prominent international and local linkages. ASM is committed to providing the highest quality of scientific, intellectual and strategic input concerning global challenges and national priorities.

Cyber Security is a key reflection of a nation's socio-economic development. It is also a key consideration to boost the level of confidence of investors. As the world becomes more connected and collaborative, exposure to cyber threats and attacks also escalate. The Global Risks Report 2017 by the World Economic Forum (WEF) stated that massive data fraud / theft are among the top five global risks. The Fourth Industrial Revolution that heralds an era of unprecedented technological disruption also ushers a new level of cyber threats that are becoming increasingly sophisticated. Conventional protection of security and privacy are inadequate in addressing the threat to safety in the age of the Internet of Things (IoT), Artificial Intelligence (AI) and Cyber Physical Systems (CPS). Innovative solutions and mitigating measures made possible by advanced science and technology are critically needed.

Today, the acquisition and deployment of new technologies feature greater integration across sectors and at multiple levels from the government to businesses to the citizen at large. This expanding interconnectedness is often facilitated by devices with limited security thus creating additional points of vulnerability to cyber attacks and makes assessing the risk factors more difficult. This report provides timely and relevant recommendations on tackling threats through the adoption of a risk-based cyber security ecosystem.

In developing this advisory report, ASM has engaged various experts and stakeholders from the public and private sectors. I would like to congratulate the ASM Task Force on Cyber Security under the leadership of Dr Mohamed bin Awang Lah FASc on this timely advisory report. I hope the highlighted issues and recommendations in this advisory report would benefit policy makers, implementing agencies, academics as well as industry players towards sustainable strategies and solutions for a more secure and safer cyber environment in Malaysia.

Professor Datuk Dr Asma Ismail FASc
President
Academy of Sciences Malaysia

Preface

This advisory report by the Academy of Sciences Malaysia (ASM) aims to provide independent input in the form of a reality check, relevant strategies and specific recommendations towards ensuring a safe and secure national cyber environment. This report addresses cyber security issues that affect national infrastructure, businesses and the well-being of citizens. The focus is not only on the security aspects related to data and systems but also the safety aspects related to people at large that are often ignored in the cyber security discourse.

The exponential expansion of cyberspace and the value of using it have triggered escalating exposure to cyber threats. The growth and pervasiveness of network ready technologies such as Internet of Things (IoT) and Artificial Intelligence (AI) are poised to fuel disruption at an accelerated pace globally. The fabric of society, data, devices and analytics have created an ecosystem rich in information, mechanisms and tools that have widely impacted the way people live and work. This new ecosystem has, at the same time widened and deepened the risks of security and privacy, demanding the need to strengthen cyber security and safety.

Malaysia started early in cyber security initiatives and we have obtained a commendable third place ranking in the Global Cyber Security Index 2017 for commitment to cyber security. However, this index did not measure effectiveness of cyber security initiatives. The key issue is translating comprehensive plans into action through robust governance, competent and sufficient talent as well as STI proficiency.

Having considered the global scenario and reality of cyber security in Malaysia, this report provides insights on security governance strategies, legislation and regulatory framework that present challenges to enforcement, technology and infrastructure resiliency issues, talent development and effective international cooperation. There is a critical need for cyber security, privacy and safety elements to be an integral part of any science, technology an innovation (STI) initiatives. The overarching recommendation is to adopt a risk-based cyber security ecosystem to address threats to security, privacy and safety that will benefit the nation an its citizens.

This report was developed with extensive stakeholder consultations as well as strategic technical discussions involving government agencies, institutions of higher learning, industry practitioners as well as STI professional bodies and non-governmental organisations.

On behalf of ASM, I would like to thank the Task Force members for their valuable input and commitment towards making this report possible. It is hoped that this report would catalyse concerted efforts and synergistic action towards a safe and secure cyber environment for everyone.

Dr Mohamed bin Awang Lah FASc
Chairman
ASM Task Force on Cyber Security

Cyber Security Strategy Team

The Academy of Sciences Malaysia wishes to thank all members of the Task Force on Cyber Security for their participation and contributions in support of the academy in completing this Advisory Report.

ADVISOR

Professor Datuk Dr Asma Ismail FASc
President, ASM

CHAIR

Dr Mohamed bin Awang Lah FASc

WRITERS

Raja Azrina Raja Othman (Co-founder of MyCERT)

International Islamic University of Malaysia (IIUM)
Dr Normaziah Abdul Aziz (Assoc. Prof, Kuliyyah of ICT)

Microsoft Malaysia
Dr Dzaharudin Mansor (National Technology Officer)

TASK FORCE MEMBERS

Attorney General Chambers of Malaysia (AGC)
Lailawati Ali (Deputy Public Prosecutor)

Bank Negara Malaysia (BNM)
Zainal Abidin Maarif (Risk Specialist (Technology))

CyberSecurity Malaysia
Dato' Dr. Haji Amirudin bin Abdul Wahab (Chief Executive Officer)
Dr Solahuddin bin Shamsuddin (Chief Technology Officer)
Sazali bin Sukardi (Vice-President of Strategic Research)
Mohamed Anwer bin Mohamed Yusoff (Head of Industry and Business)

Majlis Keselamatan Negara
Ir. Md Shah Nuri bin Md Zain (Chief Executive, National Cyber Security Agency)
Shariffah Rashidah Syed Othman (Principal Assistant Director, National Cyber Security Agency)

Malaysian Administrative Modernisation and Management Planning Unit (MAMPU)
Dr Suhazimah binti Dzazali (Deputy Director General (ICT))

Malaysian Communications and Multimedia Commission (MCMC)
Harme Mohamed (Head of Division, Digital Surveillance)

Malaysian Society for Cryptology Research
Associate Professor Dr Muhammad Rezal bin Dato' Dr Kamel Ariffin (President)

MIMOS
Ng Kang Siong (Principal Researcher, Information Security Lab)

Multimedia Development Corporation (MDeC)
Victor Lo (Head of Information Security)

Polis Diraja Malaysia (PDRM)
SAC Mohd Kamarudin bin Md Din (Deputy Director, Cyber Crime & Multimedia Investigation)

Universiti Malaya (UM)
Dr Nor Badrul Anuar bin Jumaat (Lecturer, Department of Computer System & Technology)

Universiti Malaysia Perlis (UNIMAP)
Suhizaz Sudin (Senior Lecturer, School of Computer and Communication Engineering)

Universiti Malaysia Sarawak (UNIMAS)
Dr Johari Abdullah (Dean, Faculty of Computer Science & IT)

Universiti Malaysia Terengganu (UMT)
Tn. Hj. Al Muzmi Abd. Hamid (ICT Security Officer)

Universiti Putra Malaysia (UPM)
Professor Dr Abu Bakar Md Sultan (Dean, Faculty of Computer Science and Information Technology)

Universiti Sains Malaysia (USM)
Associate Professor Dr Aman bin Jantan (Lecturer, School of Computer Sciences)

Universiti Teknologi Malaysia (UTM)
Associate Professor Dr Shukor Razak (Lecturer, Department of Computer Science)

Universiti Teknologi MARA (UiTM)
Dr Fakariah Hani Hj Mohd Ali (Senior Lecturer, Faculty of Computer Science and Mathematic)

ASM MANAGEMENT

Chief Executive Officer
Hazami Habib

Principal Analyst
Nitia Samuel

Analysts
Mohd Ikhwan Abdullah
Muhammad Syazwan Alauddin
Nurfathehah Idris

Designer
Dharshene Rajayah

Editor
Syazwani Abu Bakar

Administrative Support
Norehan Kadir

List of Figures

List of Tables

List of Acronyms

AGC	Attorney General's Chambers
AI	Artificial Intelligence
APAC	Asian Pacific
APCERT	Asia Pacific Computer Emergency Response Team
APECTEL	Asia-Pacific Economic Cooperation Telecommunications
APT	Advanced Persistent Threat
ARF	ASEAN Regional Forum
ASEAN CERT	ASEAN Computer Emergency Response Team
ASEAN TELMIN	ASEAN Telecommunications and IT Ministers Meeting
ATRC	ASEAN Telecommunications Regulators Council
BNM	Bank Negara Malaysia
CCA	Computer Crime Act
CCTV	Closed-Circuit Television
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CGSO	Chief Government Security Officer Office
CII	Critical Infocomm Infrastructure
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMA	Communications and Multimedia Act 1998
CNII	Critical National Information Infrastructure
CPS	Cyber Physical System
CRM	Customer relationship management
CSM	CyberSecurity Malaysia
CTO	Chief Technology Officer
DDoS	Distributed Denial-of-Service
DNS	Domain Name Server DNS
DNS	Domain Name System
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning
EU	European Union
FIRST	Forum of Incident Response and Security Team
GDP	Gross Domestic Product
HMI	Human Machine Interface
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISGRC	Information Security Governance, Risk, Compliance

ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
JPN	Jabatan Pendaftaran Negara (National Registration Department)
KKMM	Kementerian Komunikasi dan Multimedia Malaysia (Ministry of Communication and Multimedia Malaysia)
KPDNKK	Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan (Ministry of Domestic Trade, Co-operatives and Consumerism)
LHDN	Lembaga Hasil Dalam Negeri (Inland Revenue Board of Malaysia)
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit
MCMC	Malaysian Communications and Multimedia Commission
MDeC	Multimedia Development Corporation
MLAT	Mutual Legal Assistance Treaty
MOSTI	Ministry of Science, Technology and Innovation
MyCC	Malaysian Common Criteria Evaluation and Certification
MyCERT	Malaysian Computer Emergency Response Team
MyNIC	Malaysian Network Information Centre Berhad
NCSP	National Cyber Security Policy
NCSS	National Cyber Security Strategies
NEO	New Economic Opportunities
NFA	No Further Action
NISER	National ICT Security & Emergency Response Center
NIST	National Institute of Standards and Technology
NSC PMD	National Security Council Prime Minister's Department
OIC	Organization of Islamic Cooperation
OIC CERT	OIC Computer Emergency Response Team
PDPA	Personal Data Protection Act
PDRM	Polis DiRaja Malaysia (Royal Malaysia Police)
PII	Personally identifiable information
PKI	Public Key Infrastructure
PTG	Pejabat Tanah dan Galian (Lands and Mines Office)
RFID	Radio Frequency Identification
RMK11	Rancangan Malaysia Ke-11 (11th Malaysia Plan)
SIEM	Security Information and Event Management
SSDLC	Secured System Development Life Cycle
STI	Science, Technology and Innovation
TELSOM	Telecommunications Senior Officials Meeting
TPM	Trusted Platform Module
UN GGE	United Nations Group of Governmental Experts
USA	United States of America
USCERT	United States of America Computer Emergency Response Team
V&V	Verification and Validation

Keywords

4th Platform technologie Connected fabric of people, data, devices and intelligence within an ecosystem that turns data into knowledge, with high fluidity and accessibility.

Advanced persistent threat (APT) A network attack in which an unauthorised person gains access to a network and stays there undetected for a long period of time, targeting organisations in sectors with high-value information, such as national defence, manufacturing and the financial industry.

Artificial Intelligence (AI) An area of computer science that imitates and automates the intelligence behaviour of human and nature into a computing environment.

Backdoor variants A technique in which a system security mechanism is bypassed undetectably to access a computer or its data.

Big Data A process that is used when traditional data mining and handling techniques cannot uncover the insights and meaning of the underlying data. Data that is unstructured or time sensitive or simply very large cannot be processed by relational database engines. This type of data requires a different processing approach called big data, which uses massive parallelism on readily-available hardware.

Botnet A group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks. A botnet may also be known as a zombie army.

Closed-circuit television (CCTV) A TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

Cloud computing The use of various services, such as software development platforms, servers, storage, and software, over the Internet, often referred to as the "cloud". It is common to categorise cloud computing services as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS).

Computer emergency response team (CERT) A group of experts who respond to cybersecurity incidents. This team deal with the evolution of malware, viruses and other cyber-attacks.

Crypto-malware Ransomware that encrypts files until a ransom is paid – every compromised device, whether company or personally owned, can be quickly monetised.

Cyber-attack A cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attack is also known as a computer network attack (CNA).

Cyber drills Role-playing or planned exercises, across teams handling different threat scenarios. Through testing and repetition, one can evaluate their team's response and learn from mistakes. Same concept of a fire drill.

Cyber Security Preventative methods used to protect information from being stolen, compromised or attacked in the cyber world.

Cyber Physical System Mechanism controlled or monitored by computer-based algorithms, tightly integrated with the internet and its users, interacting with each other in a myriad of ways that change with context. Similar to the Internet of Things (IoT) sharing the same basic architecture, nevertheless, CPS presents a higher combination and coordination between physical and computational elements.

Cyber threats Any malicious act that attempts to gain access to a computer network without authorisation or permission from the owners.

Distributed Denial-of-Service (DDoS) A type of computer attack that uses a number of hosts to overwhelm a server, causing a website to experience a complete system crash. DDoS differs from a denial-of-service (DOS) attack in that it uses several hosts to bombard a server, whereas in a DoS attack, a single host is used.

DDoS-for-hire A service offered by cyber criminals that provides paying customers with distributed denial of service (DDoS) attack capabilities on demand.

Digital disruption The change that occurs when new digital technologies and business models affect the value proposition of existing goods and services.

Domain Name Server (DNS) It provides domain name resolution services that translates IP Address, which is machine readable to domain names, that is human readable.

FinTech Financial technologies, i.e technologies used and applied in the financial services sector, chiefly used by financial institutions themselves on the back end of their businesses.

Hacking Unauthorised intrusion into a computer or a network.

HyperText Transfer Protocol (HTTP) An application-layer protocol used primarily on the World Wide Web.

Hypertext Transfer Protocol Secure (HTTPS) Additional layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection. HTTPS enables encrypted communication and secure connection between a remote user and the primary web server.

Industry 4.0 The current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things and cloud computing.

** **Industry 4.0, 4th Industrial Revolution** - In this document is equivalent*

Internet of Things (IoT) A computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices.

IP Address An Internet Protocol address is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network. It binds the World Wide Web together.

Malware Malicious software is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.

Machine Learning A method of data analysis that automates analytical model building. Using algorithms that iteratively learn from data, machine learning allows computers to find hidden insights without being explicitly programmed where to look.

Network ready Devices that has built-in networking or connection capability.

Net use command Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.

Phishing Fraudulent act of acquiring private and sensitive information, such as credit card numbers, personal identification and account usernames and passwords.

Ransomware A type of malware program that infects locks or takes control of a system and demands ransom to undo it. Ransomware attacks and infects a computer with the intention of extorting money from its owner.

Reverse shell access Remote computer sending its command shell to a specific user, to enable remote (unauthorised) access.

Risk-based approach Priorities are established and decisions are made through a proper process of evaluation such as evaluating the vulnerability of the network hosting environment, data storage, transmission and processing, systems and applications functionality and safety, and the likelihood of threats.

Sleeper malware Malware that are designed to catch their victims unaware, or “sleeping”.

Secure Shell (SSH) A cryptographic protocol and interface for executing network services, shell services and secure network communication with a remote computer. Secure Shell enables two remotely connected users to perform network communication and other services on top of an unsecured network.

Trojan A Trojan horse is a seemingly benign program that when activated, causes harm to a computer system. Also known as a Trojan virus or Trojan.

VPN Subversion Method of unauthorised access to network by exploiting VPN gateways, such as via weak authentication.

Executive Summary

This document aims to propose strategies in dealing with cyber security issues that affect the national infrastructure, business environment and wellbeing of citizens.

The Internet has changed the way people live by enabling economic growth and providing alternative platforms for people to communicate and cooperate. We are starting to see the impact of new 4th Platform technologies (refer to Annex B) such as Internet of Things (IoT) and Artificial Intelligence (AI) poised to fuel digital disruption at an accelerated pace globally (Leonhard, 2015). This will further expand cyberspace as well as the value of using it.

> **Our vision for Malaysia is to create a safe and secure cyber environment for the well-being of citizens and wealth creation, in addition to establishing resilient and secure critical national information infrastructure, which is guided by core values of integrity, equitable and prosperous society for social and business activities.**

To achieve this vision we want:

Objective 1
Malaysia to align cyber security policy and synergise initiatives across authoritative bodies in Malaysia to provide clear guidelines that enable a greater level of security in day–to-day services rendered by the national critical agencies and businesses.

Objective 2
Malaysia to tackle advanced and organised cybercrime in order to create a secure environment to conduct business in cyberspace.

Objective 3
Malaysia to take a risk- based approach in development and acquisition of network ready products and solutions to create a secure and safer cyber environment for the public at large.

Objective 4
Malaysians to have the awareness, knowledge, skills and capabilities to handle cyber threats.

Objective 5
Malaysian Government to collaborate and engage other trusted international entities in global efforts to combat cyber threats.

Objective 6
Malaysia to spearhead innovation in cyber security, privacy and safety through science and technology R&D.

Chapter 1
Chapter 1 describes the growth of the pervasiveness of technology and the impact on people in general. The expansion of the networked world has brought new opportunities in social and business aspects, yet at the same time has resulted in dependencies on technologies that make people and businesses become vulnerable to threats of security, safety and privacy. There is a need to address security in a comprehensive manner through protection, detection and response.

Chapter 2
Chapter 2 provides a background for the information security governance approach in Malaysia; where we are today, and where we want to be. The chapter discusses the cyber security roles of various entities in the country as well as the approach to create alignment and synergy in implementation of cyber security policies.

Chapter 3
Chapter 3 discusses the various legislation and regulatory framework that present challenges to enforcement. It requires recognising and leveraging core strengths of enforcement entities and technical experts within multi discipline to investigate cybercrime.

Chapter 4
Insights on the technology and infrastructure resiliency challenges and needs are deliberated in Chapter 4. The chapter also provides an approach to establish a risk-based ecosystem to address security and privacy threats that will benefit citizens at large.

Chapter 5
Addressing the appropriate human capital requirements is one of the key underlying factor that will contribute largely to the success of the cyber security strategy as discussed in Chapter 5. The need to develop information security awareness, knowledge and skills across multidiscipline such as engineering, law, finance and health, is imperative in order to embrace the digital disruption. Citizens at large require knowledge to avoid abuse, fraud and crime that are embedded in the networked world.

Chapter 6
Chapter 6 discusses how international cooperation can be made more effective in addressing cyber security challenges that require rapid response and trusted information exchange in order to disrupt the modus operandi of organised crime.

Chapter 7
Chapter 7 describes an outlook on how the conventional protection of security and privacy are inadequate in addressing the threat to safety in the age of IoT. The chapter deliberates on the need for innovation to ensure cyber security, privacy and safety are seamlessly integrated through science and technology research, development and education.

Chapter 8
Recommendation and conclusion.

01
Reality of Cyber Security

1.0 Reality of Cyber Security

The landscape - pervasiveness of technology and threats

The growth and pervasiveness of network ready technologies have created a society that is exposed to a multitude of information and capabilities that impact on how people live. The fabric of society, data, devices and analytics have created an ecosystem rich in information, mechanism and tools that impact day to day activities, decision making and life in general. This new ecosystem has, at the same time, widened and deepened the risks of security and privacy.

Exploitation and penetration of back end systems has now shifted to threats that target and leverage on endpoint devices, primarily the smartphones and Internet of Things (IoT) such as smart home system, wearables, and tracking devices. The IoT has contributed to the complexity of the threat and exploit.

We are living in an age where IoT devices such as CCTV are being infected and "weaponised" to launch large scale DDoS attacks. Recent arrests of suspects from 13 countries in an international DDoS-for-hire service proved how real and extensive this type of offence could become. From merely nuisance and disturbance to online users, it has now come to a point of disabling critical internet services such as the domain name server (DNS) (Kan, 2016).

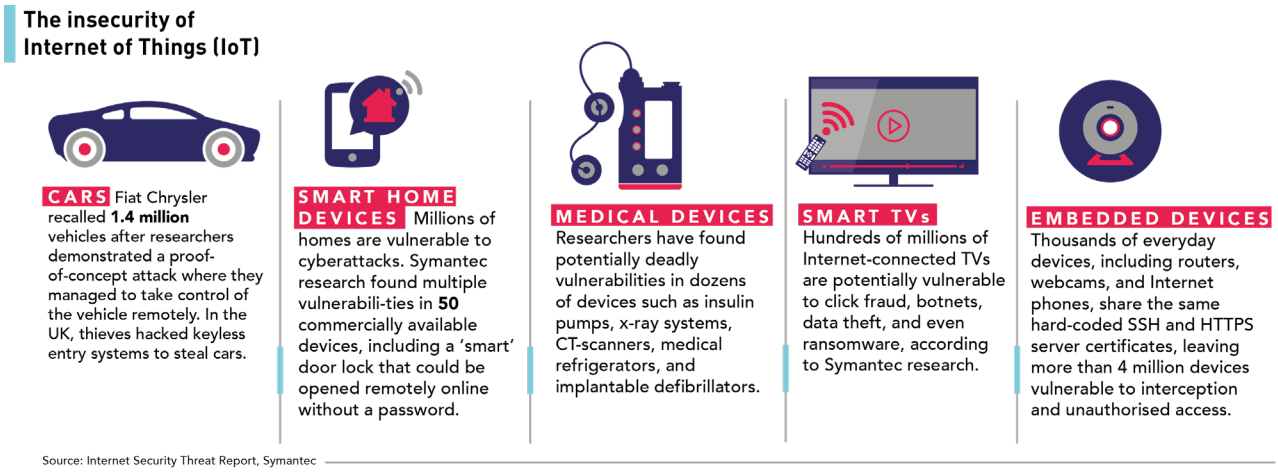


Figure 1.1: The insecurity of Internet of Things (IoT)
[Source: Internet Security Threat Report, Symantec]

In a hospital scenario, a malicious user can connect to the hospital's wifi network and sniff the network traffic. The fact that the network for users and hospital administrators are not normally separated, lack of network access control and applications are using non-secure protocols to transmit data, patient records can be captured in clear text. In the absence of authentication of data received by the back end system, malicious users can also tamper and modify patients' data that can result in wrong diagnosis and mistreatment. This has direct safety implications to patients.

The threat to cyber security is becoming a real life, physical threat as driverless cars are deployed on the roads, network based pacemakers, smart homes, various automations and eventually robotic functions become a norm. The common underlying infrastructure used to develop and operate these systems is plagued with vulnerabilities. There are increased occurrences of attacks on core infrastructure that makes the Internet, implying efforts by carefully planned, not ruling out, nation state initiatives.

With regard to data protection, data and applications are no longer residing in on-premise devices, but are located in multi locations and cloud computing. In such distributed systems, there are interdependencies and vulnerabilities at every layer, and securing the key components closest to the data/information is paramount. While network perimeter security remains critical, security in the time of cloud computing, driverless cars and IoT requires a new approach as we start to see an emergence of hybrid security infrastructures. The challenge is to have security policy and management that can be controlled centrally, regardless of the location of the application or data.

An illustration of how a cyber-attack takes place is explained in Figure 1.2, which describes an attack lifecycle model with classic attacker techniques. Anyone who has been using the Internet or networked-based devices would have experienced some level of these attacks, attempts or successful attacks, at some point in their life, with or without their realisation.

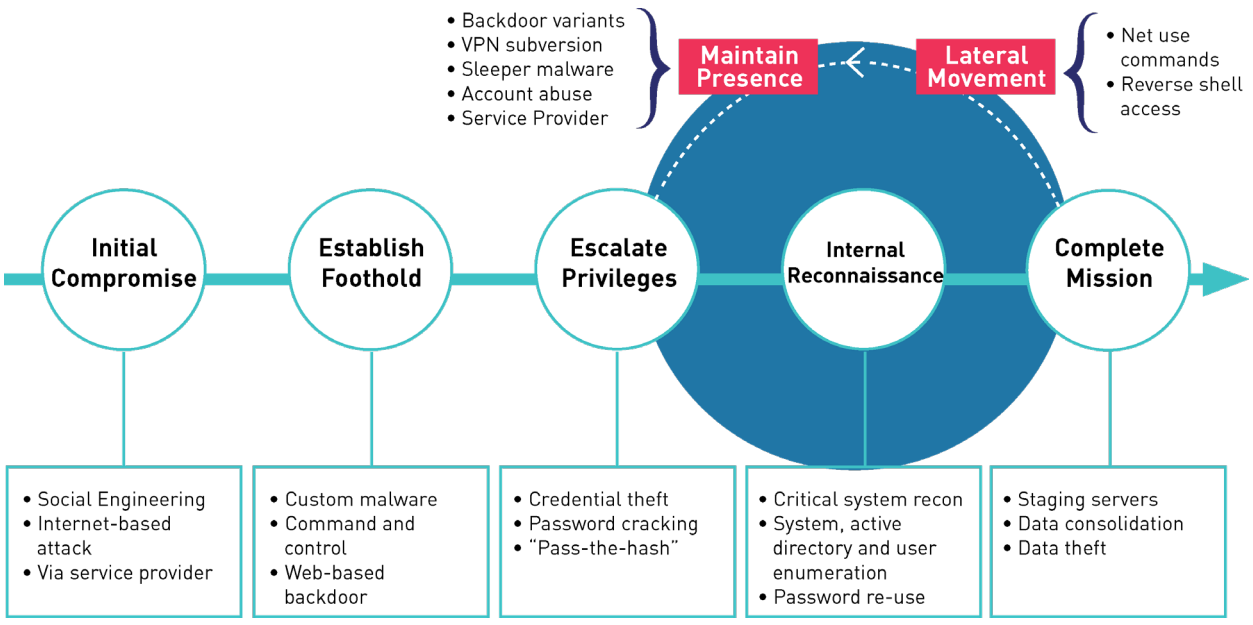


Figure 1.2: Cyber-attack Lifecycle Model
[Source: FireEye M trends 2016 APAC Edition]

In the Global State of Information Security Survey 2015 by PWC, CIO and CSO, 15% of survey respondents cited organised crime as a source of incidents, up from 12% the year before. By region, theft by organised criminals was particularly high in Malaysia (35%), India (22%) and Brazil (18%). This data is further supported by the report by FireEye on targeted attacks in Asia Pacific region. Investigation by FireEye shows an average of 3.7GB data exfiltrated (leaked) from breached organisation per incident in APAC in 2015. However, most organisation lack visibility, as such it is likely that the total average volume data stolen per breach was significantly more than that. The type of information gathered primarily consists of emails, sensitive documents, personally identifiable information, and infrastructure documents, as shown in Figure 1.3.

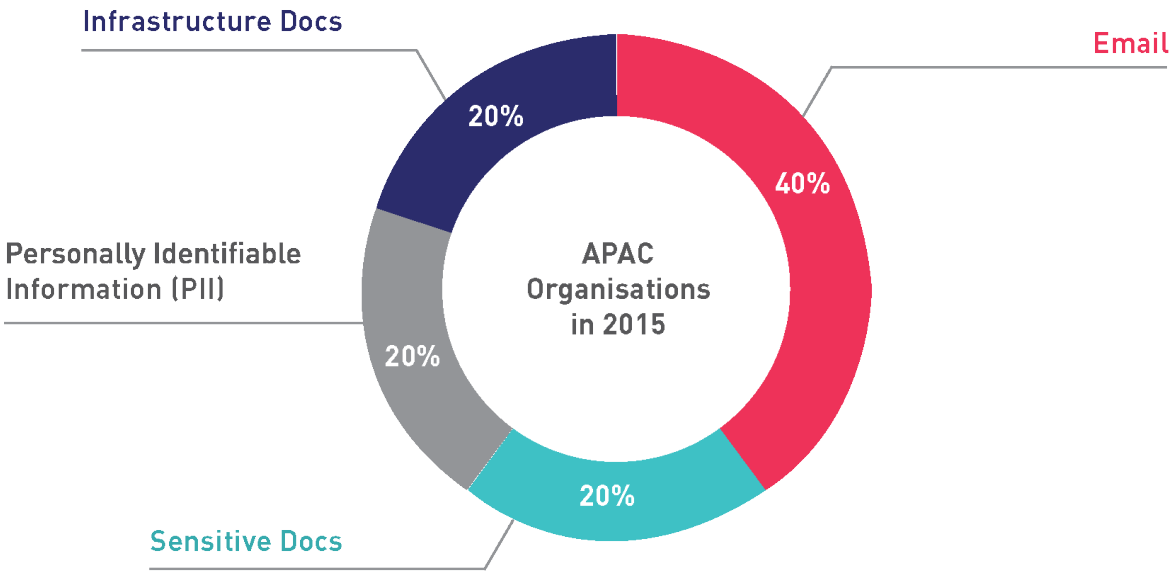


Figure 1.3: Classification of Information Stolen from APAC Organisation in 2015
[Source: FireEye M-Trends 2016 Asia Pacific Edition]

One of the indicators for cyber threats is malware propagation and evolution. In 2016, according to Symantec Corporation, Malaysia ranks 47th globally, and 12th in the Asia Pacific and Japan region, in terms of ransomware attacks. In 2015, Malaysians experienced around 5,000 ransomware attacks or 14 attacks per day (Regent Risk Advsory, 2016). The economic incentive of cybercrime is attractive as the cost of doing cybercrime and the probability of being apprehended and successfully being prosecuted is low. With such lucrative returns as well as the involvement of state-sponsored activities, cyber threats are becoming dynamic and sophisticated. As depicted in Figure 1.4, the risk to business is increasing due to the stealthiness of the attacks and the financial impact of a data breach. At the same time attacks are becoming fast, efficient and easier to propagate.

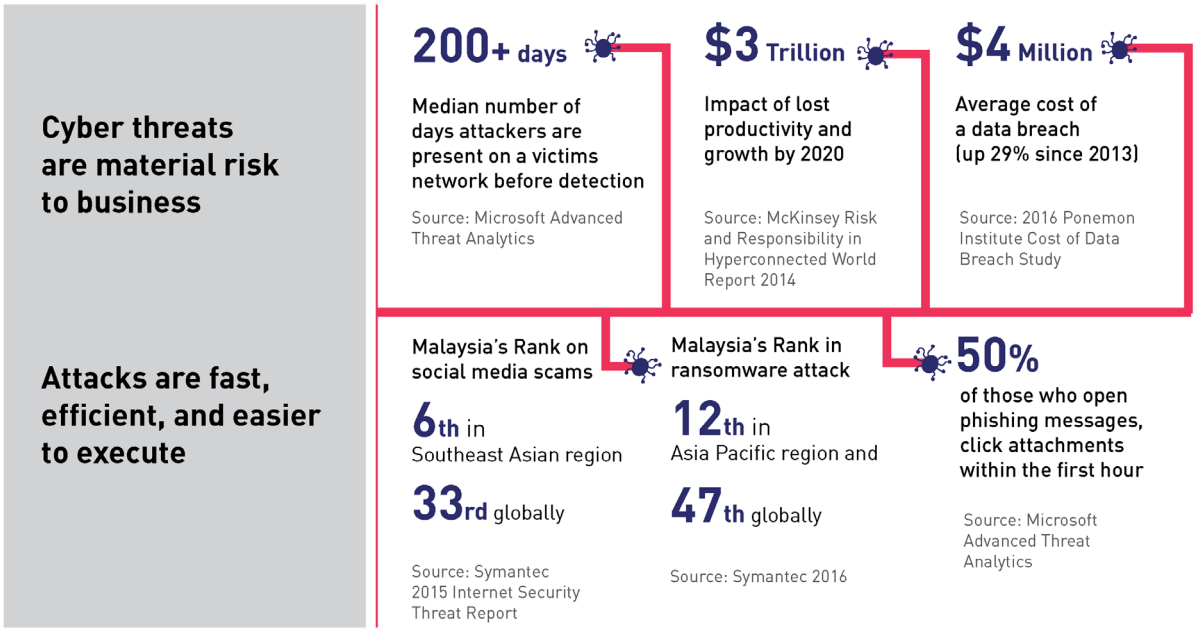


Figure 1.4 : Malware and Vulnerability Trends

In illustrating the Malaysian landscape with regard to cyber threats, the trend indicates increase in fraud a nd intrusion reported incidents as shown in Figure 1.5. This is consistent with the global studies which show Malaysia in the top 10 in terms of online scam.

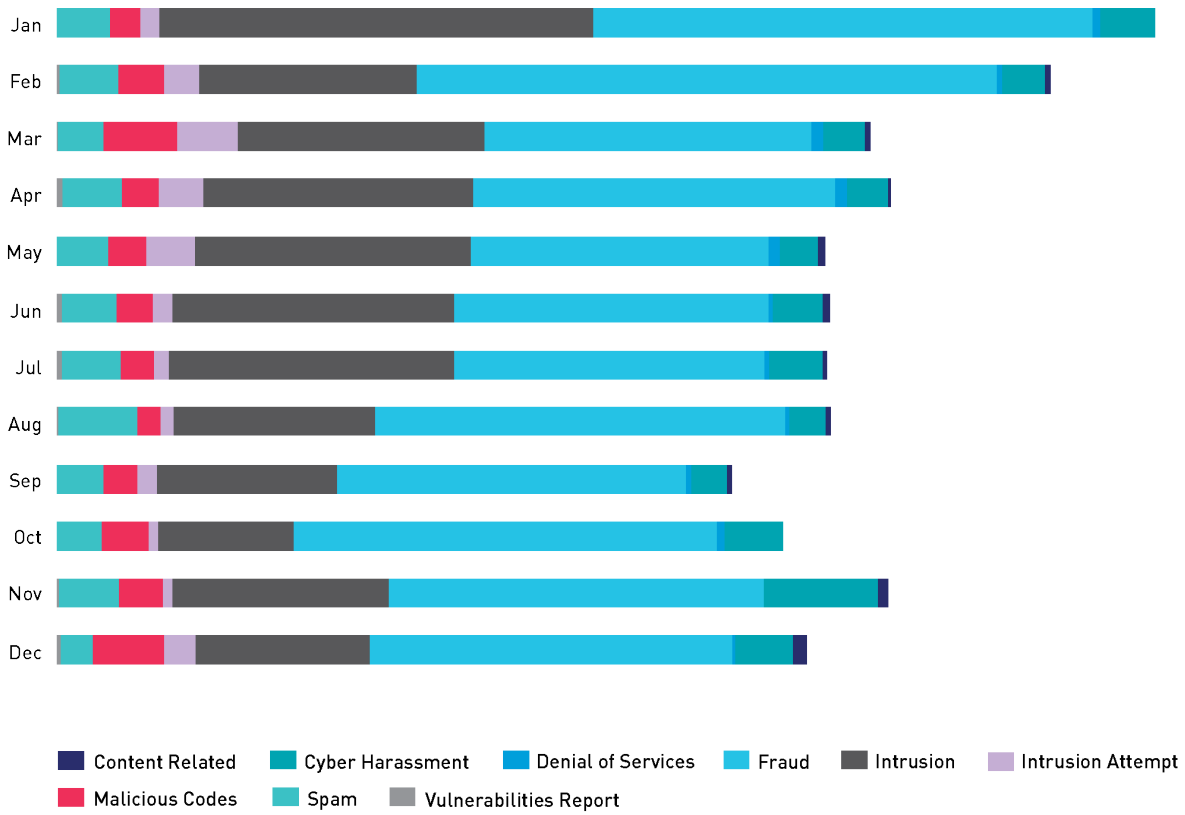


Figure 1.5: Malaysian Reported Incidents to MyCERT in 2016

In terms of financial impact, according to Polis DiRaja Malaysia (PDRM), in the year of 2014, the amount of losses due to cyber related crime were over RM162 million. The losses increased by 22% in 2015 to over RM179 million and by November 2016, the amount of losses reported were over RM206 million.

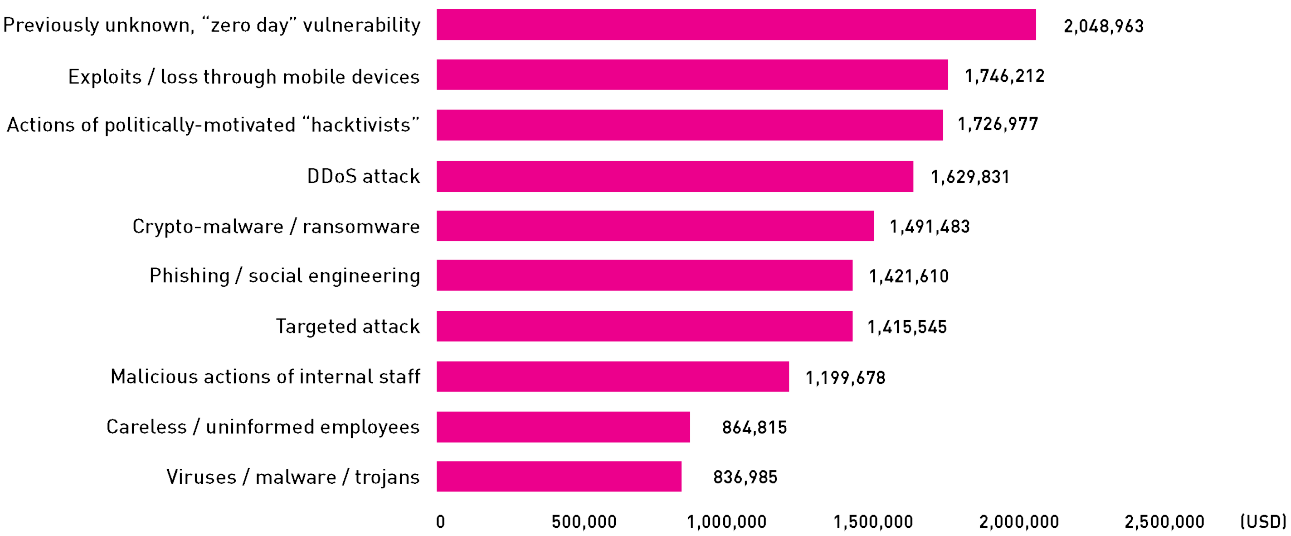


Figure 1.6: Top 10 most costly security incidents.
[Source: Kaspersky Lab IT Security Risk Report 2016]

Several reports measure the financial impact of various security incidents as well as the impact of data breaches. One report by Kaspersky, as shown in Figures 1.6 and 1.7 respectively, demonstrates the amount of cost incurred based on the type of incident experienced.

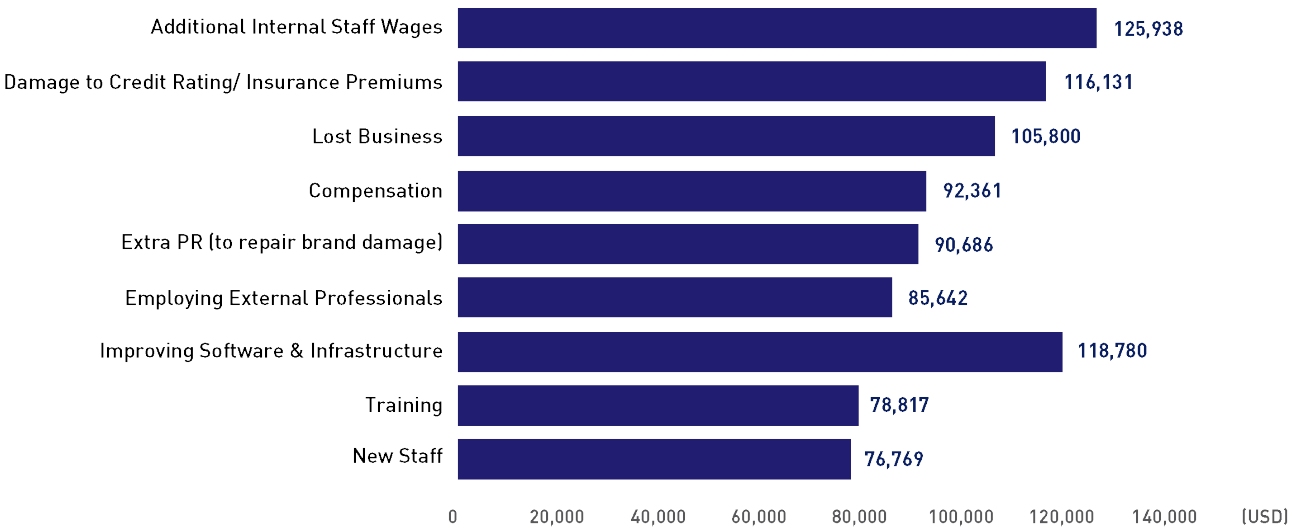
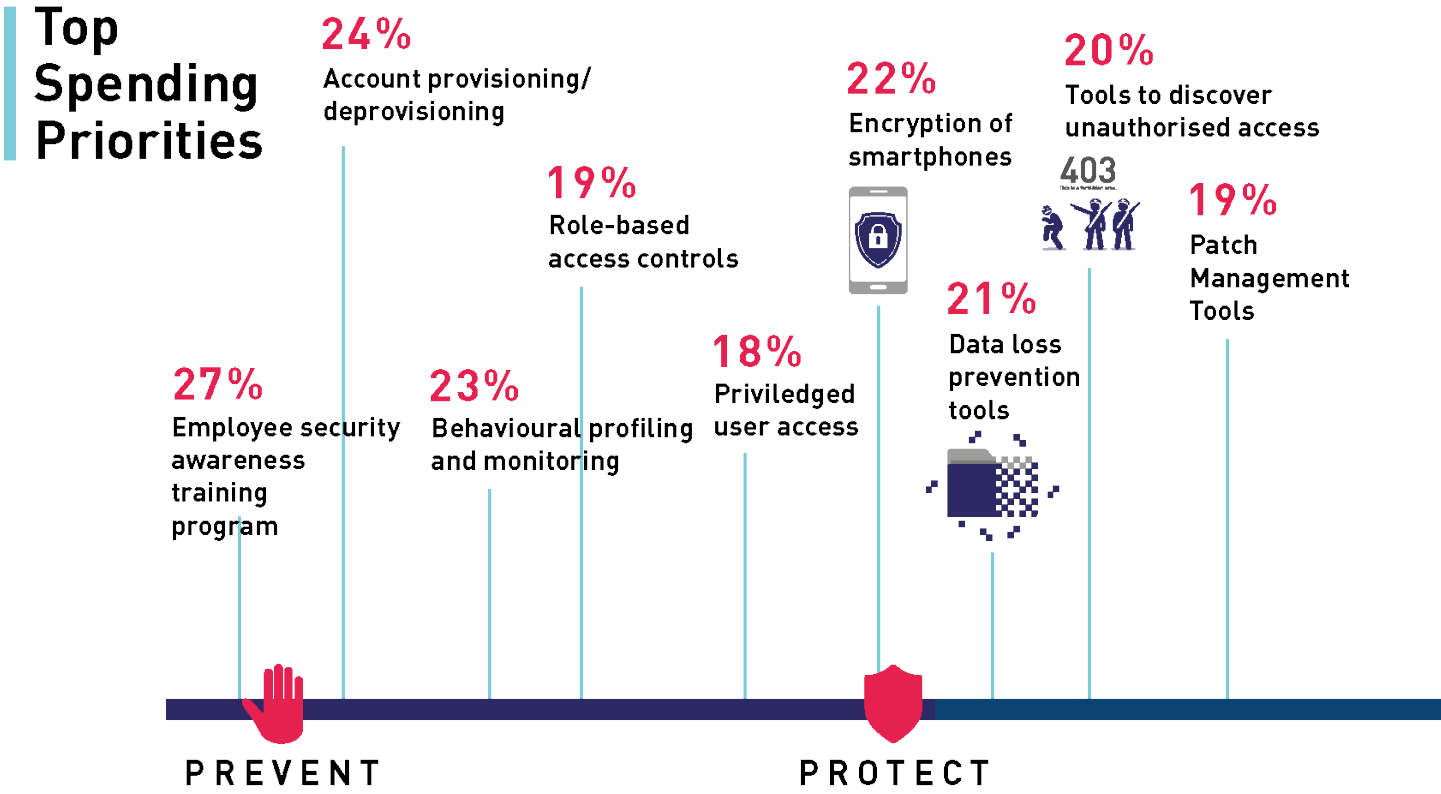


Figure 1.7: Breakdown of an average financial impact of data breach
[Source: Kaspersky Lab IT Security Risk Report 2016]

The protection, detection and response efforts and strategies

Security becomes the underlying factor that ensures the resiliency of the components within the infrastructure and information, towards attacks that threatens information security and privacy as well as physical safety. A risk-based approach that is relevant and aligned to business objectives needs to be taken in identifying and implementing information security control at every level of protection, detection and response. Protective measures need to balance with the ease of use, while monitoring and detection measures need to preserve privacy. The mechanisms and approach to detection is not based on pre-determined signature alone, but require machine learning, dynamic and intelligence as well as profiling of devices and applications based on the perceived level of risk. Incident response needs to ensure preservation of evidence for analysis, while at the same time allow businesses to recover, implement corrective measures and resume operations.



Source: Global State of Information Security Survey 2015, PWC, CSO

According to a report, (Kaspersky Lab IT, 2016) businesses only allocate about 17% of IT budget to IT security. However, the fraction is even smaller in Malaysia. The investment of IT Security is shown in Figure 1.8. Although it appears to indicate substantial investment in monitoring and detection, the majority of these technologies are not integrated and require their own set of management and monitoring console.

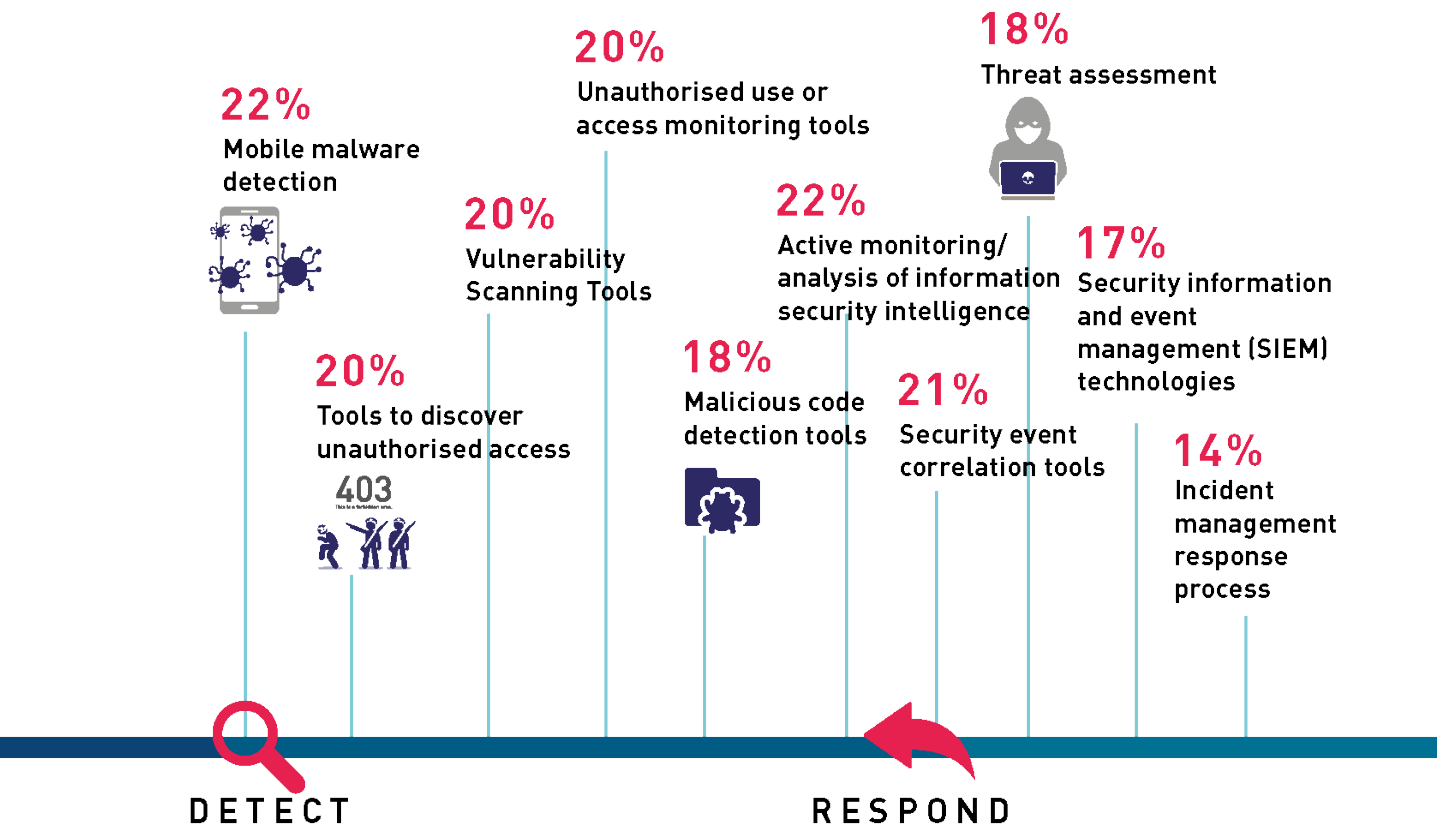


Figure 1.8: Top Spending Priorities
[Source: (PWC, 2014)]

In achieving a safer cyber space, careful design, development and implementation needs to take place at every layer of any interconnected network device, regardless how miniaturised or large scale the solution is. The strategy needs to come from the top, which then relies heavily on the governance and enforcement at national level to facilitate a concerted effort in creating and maintaining a healthy cyber ecosystem.

Malaysia embarked on cyber security policy formulation and implementation from year 2005 via the National Cyber Security Policy. The ultimate goal has been is to establish a secure, resilient and self-reliant Critical National Information Infrastructure (CNII). The policy has resulted in a clear identification of 10 critical sectors and has since developed to varying levels of impact in terms of information security readiness.

Singapore however has taken a different approach by staggering focus areas. The Infocomm Security Masterplan started by addressing the government in 2005. The Infocomm Security Masterplan 2 expanded its coverage to Critical Infocomm Infrastructure (CII) in 2008 and finally include businesses and individuals in their National Cyber Security Masterplan 2018. (Infocomm Development Authority of Singapore, 2016)

In Europe, the European Union (EU) Agency for Network and Information Security (ENISA) has taken a step further in developing a mechanism to measure the implementation of the national strategies in cyber security of the EU members. The evaluation framework for National Cyber Security Strategies (NCSS) was developed to identify useful key indicators that could be chosen by the stakeholders to evaluate the NCSS.

The national level strategies in cyber security for Malaysia, Singapore and the EU member countries have shown that there are different levels of concern and stakeholders. The approach by EU shows a maturity level of cyber security strategy development that provides the a framework for Key Performance Indicator and outcome-based evaluation of implementation as essential means for determining whether the objectives are met or otherwise. (European Union Agency for Network and Information Security, 2014)

02

Cyber Security Governance in Malaysia

2.0 Cyber Security Governance in Malaysia

Malaysia had started addressing computer incidents and threats by establishing the Malaysian Computer Emergency Response Team (MyCERT)[1] in 1997. Other initiatives followed suit at research and law enforcement agencies with the establishment of Digital Forensics Lab facilities and government CERT. Cyber Laws were enacted and implemented with challenges at various levels and magnitude.

Malaysia had learned over the years that Information Security needs to be a top-down agenda primarily in creating a safer and conducive environment for consumers and businesses alike. The Malaysia National Cyber Security Policy (2005) initiated a coordinated approach to secure Malaysia's critical national information infrastructure.

National Cyber Security Policy (NCSP) has the following vision:
Malaysian's Critical National Information Infrastructure will be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well-being and wealth creation.

The Policy recognises the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets. This was spearheaded through the eight policy thrusts working committees covering 10 sectors of the Critical National Information Infrastructure (CNII).

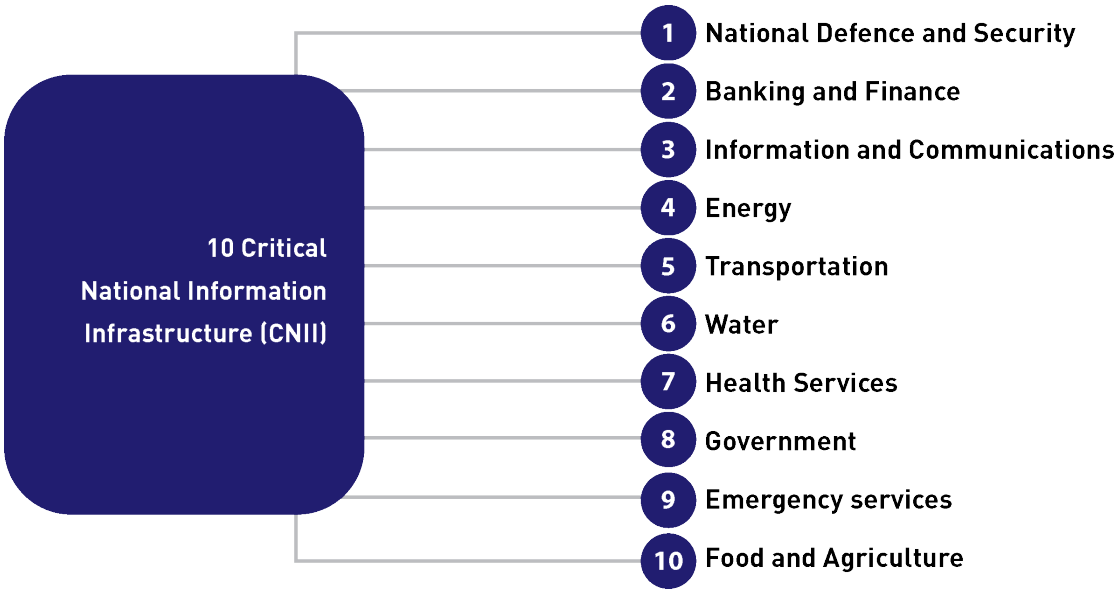


Figure 2.1: 10 Critical National Information Infrastructure (CNII)

[1] This unit had then developed into an agency under MIMOS called National ICT Security and Emergency Response Center NISER), which was later spun off as a Company Limited by Guarantee and rebranded to CyberSecurity Malaysia.

Eight Policy Thrust areas under the NCSP, as shown in Figure 2.2, were established more than a decade ago and have undergone progress at various levels. In ensuring resiliency and reliability of the cyber infrastructure and services for the economy at large, the following areas require focus and impetus primarily in enabling:

- Greater engagement on initiatives under Legislative & Regulatory Framework and Compliance and Enforcement; and
- Alignment of Cyber Security Technology Framework and Research & Development with measurability of impact and effectiveness.

Malaysia currently has a centralised cyber security governance structure both at national and sector level. At the national level, the e-Sovereignty Committee is chaired by the Deputy Prime Minister that reports matters concerning cyber security of national interest to the National Security Council, chaired by the Prime Minister. As a secretariat to e-Sovereignty Committee, the National Security Council Prime Minister's Department leads the national cyber security initiatives as well as the cross-sector communication through the e-Sovereignty Working Group and various national cyber committees in coordination with the Sector Leads.

Thrust 1: Effective Governance
- Centralise coordination of national cyber security initiatives
- Promotes effective cooperation between public and private sectors
- Establish formal and encourage informal information sharing exchanges

Thrust 2: Legislative & Regulatory Framework
- Review and enhance Malaysia's cyber laws to address the dynamic nature of cyber security threats
- Establish progressive capacity building programmes for national law enforcement agencies
- Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions.

Thrust 3: Cyber Security Technology Framework
- Develop a national cyber security technology framework that specifies cyber security requirement controls and baselines for CNII elements
- Implement an evaluation/certification programme for cyber security product and systems

Thrust 4: Culture of security and Capacity Building
- Develop, foster and maintain a national culture of security
- Standardise and coordinate cyber security awareness and education programmes across all elements of the CNII
- Establish an effective mechanism for cyber security knowledge dissemination at the national level
- Identify minimum requirements and qualifications for information security professionals

Thrust 5: Research & Development towards Self-Reliance
- Formalise the coordination and prioritization of cyber security research and development activities
- Enlarge and strengthen the cyber security research community
- Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development
- Nurture the growth of cyber security research

Thrust 6: Compliance and Enforcement
- Standardise cyber security systems across all elements of the CNII
- Strengthen the monitoring and enforcement of standards
- Develop a standard cyber security risk assessment framework

Thrust 7: Cyber Security Emergency Readiness
- Strengthen the national computer emergency response teams (CERTs)
- Develop effective cyber security incident reporting mechanisms
- Encourage all elements of the CNII to monitor cyber security events
- Develop a standard business continuity management framework
- Disseminate vulnerability advisories and threat warnings in a timely manner
- Encourage all elements of the CNII to perform periodic vulnerability assessment programmes

Thrust 8: International Cooperation
- Encourage active participation in all relevant international cyber security bodies, panels and multi-national agencies
- Promote active participation in all relevant international cyber security by hosting an annual international cyber security conference

Figure 2.2: Policy Thrusts under the NCSP

2.1 Cyber Security Roles in Malaysia

The NCSP was planned to be implemented through a coordinated and focused approach. A one-stop centre was to be established to fulfil this vision. Many initiatives were observed by various entities in delivering cyber security roles since the implementation of the NCSP. However, the lack of central coordination had some impact in the realisation of the NCSP vision. But some strides towards the alignment of authority and governance has been made.

Based on the entities' source of authority, each entities' roles and responsibilities as well as the existing institutional arrangements at the national level has been mapped against their functions. Table 2.1 describes the respective cyber security-related roles and responsibilities of these entities at the national level based on their respective mandate under the Ministers of the Federal Government Order 2013 under Ministerial Functions Act 1969.

Table 2.1: Matrix on Organisations' Key Roles in Cyber Security

Entities	Cyber Security-related Roles and Responsibilities	Functions in Cyber Security Governance Value Chain
Attorney General's Chambers (AGC) *Jabatan Peguam Negara Malaysia*	AGC's responsibilities include the following, but not limited to : • Providing advice to the Malaysian Government on cyber security-related legal matters including the drafting of all cyber security-related legislations; and • Providing prosecution instructions to all related law enforcement agencies for cyber security-related criminal cases.	Policy Development
Chief Government Security Officer Office (CGSO) *Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia*	CGSO's functions are stated as: • Management of protective security for Ministries, departments and Government agencies at the Federal and State levels. • Protective security for Key Points Installations, Protected Areas and Protected places; and • Security for protection of government official secrets.	• Conformance & Compliance ; and • Education & Awareness.

CyberSecurity Malaysia (CSM)	CSM's function is to : • Provide specialised cyber security services and continuously identifies possible areas that may be detrimental to national security and public safety.	• Monitoring; • Response & Recovery; • Education & Awareness; and • Research.
Ministry of Communication and Multimedia Malaysia *Kementerian Komunikasi dan Multimedia Malaysia (KKMM)*	KKMM's functions are : • Formulating and implementing national policy objectives on communications and industry; • Formulating and implementing national policy on safety, security protection, integrity and reliability of network and application services; and • Regulating the operation, management and financial aspects of the MCMC under the Communications and Multimedia Act 1998 and the Malaysian Communications and Multimedia Commission Act 1998. As of September 2013, the ministry "...has taken over the Multimedia Development Corporation (MDeC) and the Malaysian Network Information Centre Berhad (MyNIC) , along with their functions and roles, from MOSTI."	• Policy Development; and • Conformance and Compliance.
Ministry of Domestic Trade, Co-operatives & Consumerism *Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan (KPDNKK)*	KPDNKK's function is : • Enhancing development and supervision of domestic trade activities, including transactions by electronic commerce and consumerism.	•Conformance and Compliance.
Malaysian Administrative Modernisation and Management Planning Unit *Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)*	MAMPU's functions are : • Leading the change in modernising the administration of the public service; and • Intensifying usage of ICT to enhance the efficiency of the public service delivery system	•Conformance and Compliance.

Entities	Cyber Security-related Roles and Responsibilities	Functions in Cyber Security Governance Value Chain
Malaysian Communications and Multimedia Commission *Suruhanjaya Komunikasi dan Multimedia Malaysia (MCMC)*	MCMC's function is stated as: • Enforcement, supervision and regulation of communications and multimedia activities under the Malaysian Communications and Multimedia Commission Act 1998, Communications and Multimedia Act 1998, Postal Services Act 1991 and Digital Signature Act 1997.	• Conformance and Compliance; • Monitoring; • Response & Recovery; and • Education & Awareness.
MIMOS Berhad (MIMOS)	MIMOS's function is stated as: • Spearheads applied research and technology transfer via seeding new technology ventures in ICT and microelectronics towards enhancing domestic industry competitiveness.	• Research & Development
National Security Council – Prime Minister's Department *Majlis Keselamatan Negara (NSC PMD)*	NSC PMD's functions are: • Formulation of national security policies and co-ordination of national security measures; • Secretariat for the NSC and all committees and working groups established under the NSC at the Federal level and the State Executive Committees on Security at State level that deal with matters of national security, public order and crisis and disaster management placed under the jurisdiction of the NSC; • Co-ordinating and monitoring the implementation of policies on national cyber and space security that threatens national security; and • Monitoring and formulating strategies to address issues that affect public order, national security and the integrity of the Government.	• Policy Development; • Monitoring; • Response & Recovery; and • Education & Awareness.

	NSC, PMD has a division specifically looking into matters of cyber security, namely the Space and Cyber Security Division. It issued the NSC Directive No.24 that outlines the national cyber crisis management mechanism and policy and the given responsibilities to CNII agencies with regard to cyber security.	
Ministry of Science, Technology and Innovation (MOSTI)	MOSTI's functions are: • Formulation of national policies for the development of science, technology and innovation (STI); • Promotion of on-going effort towards research and development in STI; and • Promotion of the understanding awareness and appreciation of STI.	• Policy Development; and • Education and Awareness.
Royal Malaysia Police (RMP) *Polis Diraja Malaysia (PDRM)*	PDRM's function is: • Performing functions and responsibilities according to Police Act 1967 and other powers given to the police. PDRM is part of the security forces in Malaysia. Under the Commercial Crime Investigation Department, a Technology Crime Unit has been established. The Unit is responsible for investigating and taking preventive actions against commercial crime that involves computers, as well as internet-related crimes. In addition, the PDRM has also established a forensics computer laboratory for the purpose of investigating computer related crimes.	• Conformance & Compliance; and • Response & Recovery.
Standards Malaysia	Standard Malaysia's functions are : • Provides accreditation to certification bodies; and • Provides accreditation for lab testing of ICT products.	• Conformance & Compliance;

2.2 Challenges

Despite many entities and committees tasked with cyber security roles, challenges in terms of having the right mandate, roles, and regulatory/enforcement authority, remain in managing multi sectors within the CNII, business entities and public at large.

Coordination of the cyber security roles is required not only during crisis but most importantly during day to day operations to ensure effective and efficient response in the event of a cyber incident. The separation of policy enforcement for public and private sectors has posed a challenge in ensuring overall compliance. As an example, in the event that a network security of a business entity is compromised, if the business does not fall within any of the regulated sectors or the CNII sectors, the business owner might opt not to report the incident. Similarly, the same action could be taken by individuals or organisations, which may have no interest or awareness on the importance of reporting an incident.

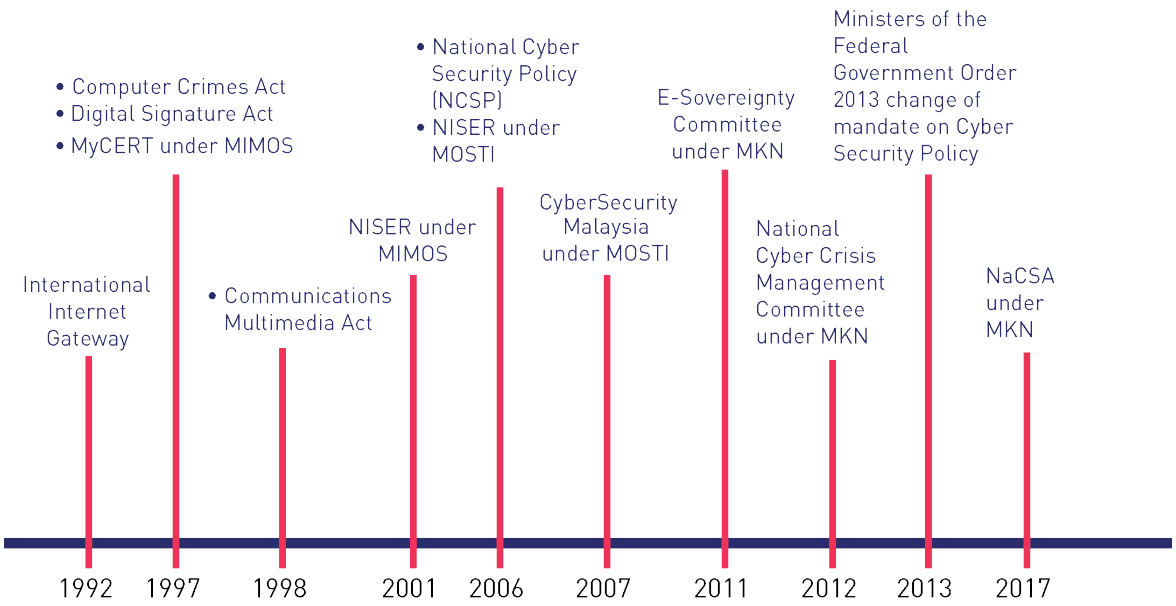


Figure 2.3: Timeline of National Cyber Security Development

Corporate Governance

Cyber security is now front and center on organisations' boardroom agendas, but most chief information security officers (CISOs) have yet to earn a seat at the table. According to a 2016 study by ISACA and RSA Conference, 82 percent of cyber security and information security professionals polled in the survey report that their board of directors is concerned or very concerned about cyber security, but only 1 in 7 (14 percent) CISOs are reporting to CEOs.

Awareness

The survey also highlighted a marked lack of situational awareness for professionals who report that cyber security or information security is their primary role:

- 24 percent did not know if any user credentials were stolen in 2015
- 24 percent did not know which threat actors exploited their organisations
- 23 percent did not know whether their organisation had experienced an advanced persistent threat (APT) attack
- 20 percent did not know whether any corporate assets were hijacked for botnet use

Source: (ISACA, 2016)

Ransomware attacks are among 2017's biggest cyber incidents (WIRED, 2017). These attacks involved malicious software compromise on devices, which resulted in locked files and software applications, forcing extortion onto victims, in order to recover access to their information. With the lack of accountability on cyber security in the Boardroom, organisations struggle to deal with advanced and sophisticated attacks such as Ransomware attack, Distributed Denial of Service ((DDoS) attacks and Advanced Persistent Threat (APT).

2.3 Way Forward

Alignment of information security policy requirements at strategic and policy level from authoritative bodies responsible for CNII and businesses is key in getting the message across to board level of these organisations.

The consolidation of authority and roles in cyber security amongst various government agencies that develop strategy as well as create policies, guidelines and compliance requirements will reduce confusion in information security controls requirements. It is imperative that coordination of cyber security issues is done across CNII, business entities in order to enable effective detection and response.

Greater coordination will enable effective information exchange and opportunity in leveraging expertise, primarily in addressing advanced and sophisticated attacks that often require multi discipline and cross sector engagement. This is feasible given the clear reporting process required for CNII, businesses and public at large.

Globally, there are nation states that have consolidated their cyber security mandate. Examples include establishment of Department of Homeland Security in the US, which currently hosts the USCERT and the establishment of the Cyber Security Agency Singapore, which is part of the Prime Minister's Office and hosting SingCERT.

The establishment of a National Cyber Security Agency in the country as a central entity, with the mandate to provide formulation, monitoring, coordination and synchronisation of implementation of cyber security policy and framework in peace time as well as to provide national security cyber crisis management, is essential to leverage the resources and capabilities across organisations.

03

Legislative, Regulatory Framework and Enforcement

3.0 Legislative, Regulatory Framework and Enforcement

3.1 Current Laws

Malaysia was one of the earliest countries in Asia to enact the Computer Crime Act in 1997. Subsequent to that, several other cyber laws were enacted. However, based on our findings, most of the cybercrime and cyber related crime had been tried under other Acts as identified in Table 3.1.

Table 3.1: Present Laws and challenges in relation to cybercrime cases

Act, Clauses and Penalties	Present Issues and Challenges
Computer Crime Act 1997 (CCA) Sec 10(1)(a) CCA 1997 Analysing Evidence Sec 10(1)(b) CCA 1997 Power To Compel Assistance In Analysing The Evidence Note: Maximum RM150k and/or 10 years	The CCA covers the following offences: • Unauthorised access to computer materials • Unauthorised access to computer with intent to commit/facilitate further offence • Unauthorised modification of content • Wrongful communication of access credentials And the underlying challenges are in identifying the identity behind the cybercrime.
Evidence Act 1993 Subsection 90A(2) and 90A(6) of the Evidence Act 1950 (Amendment 2012) - admissibility of documents produced by computers.	• Challenges in handling exhibits in electronic evidences and digital formats, which includes preserving and presenting the evidence in a form that is acceptable by the court. • Compliance to international standards such as the ISO/IEC 27037 that provides guidelines in handling digital evidence.
Communications and Multimedia Act 1998 (CMA) Consumer Protection • 5th National Policy Objectives – Consumer Confidence Forum, Content Code & Consumer (Sections 94 – 103) Cyber Criminals • Offensive content (Sections 211 & 233) • Fraud and related activities (Section 236) • Provisions for the powers of entry, investigations into offence and prosecution (Sections 245 – 262) Information Infrastructure • 10th National Policy Objectives – Network Security • Technical Standards (Sections 183 & 184) • General duty of Licensee (Section 263) • Special Powers in Emergency (Section 266) • Disaster Plan (Section 267)	• Require additional provisions to address data retention and data preservation requirements to assist investigations • Need to continue to address data accuracy and integrity of subscribers of telecommunications services through regulatory measures (BERNAMA, 2016) • The use of social media and the Internet to spread false contents that could destabilise the country.

Personal Data Protection Act 2010 (PDPA) Note: Max RM500K, and/or 3 years	Most syndication crimes committed involving fraud, identity theft, and document forgery related to government services are not subject to PDPA, e.g. scam involving land grant, immigration and IC modification.
Penal Code Section 411 - Dishonestly receiving stolen property. Note: Max 5 years and/or with fine.	Challenges in investigating and presenting stolen properties that were acquired in networked environment and are exist in virtual form and that had occurred across borders.
Penal Code Section 411A - Receiving benefit derived from criminal activities of organised criminal group Note: Max 6 years and/or with fine.	Challenges in investigating, acquiring evidence and presenting the benefits derived from criminal activities conducted in networked environment and that the crime had occurred across borders.
Penal Code Section 420 - Cheating and dishonestly inducing delivery of property Note: Max 10 years and whipping, with fine.	Challenges in investigating, acquiring evidence and presenting the crime associated to cheating and dishonestly inducing delivery of property when the crime was committed and the property exist in networked environment and that the crime had occurred across borders.

The Attorney General's Chamber heads the review of the laws of Malaysia with a view to enhancing the existing legislative and regulatory framework with respect to cyber security. This exercise represents not only a national agenda but also part of an international undertaking where the review examines the European Convention as well as laws of other countries on curbing common threats to the global community.

Based on cyber related cases as shown in Table 3.2, the majority of the No Further Action (NFA) cases were due to insufficient evidence to support the case, and this includes inability to identify and locate offender, and cross border jurisdiction issues.

Table 3.2 Statistics of cyber related cases reported[2]

Owner of Records	Year	No. of Cases
PDRM cases	2014 – June 2016	21207
AGC, Putrajaya (cases referred to HQ)	2013 – 2016	179 41 Prosecuted 36 Closed (NFA) 102 Further investigation

In terms of classification of cyber related cases, the Royal Malaysian Police and Attorney General's Office classify these cases as shown in Table 3.3. Further alignment of the classification would benefit the nation to allow a more structured method of measuring effectiveness of the laws against these threats.

Table 3.3: Classification of Cyber related cases

PDRM Cases	AGC Cases
E-commerce 419 scam Telecommunication Fraud E-Financial Fraud Harta Intelek S233 CMA 1998	CMA 1998 CCA 1997 Sedition Act Penal Code

Based on the current statistics, most computer related crimes are charged under the Penal Code and Sedition Act.

[2] Different classifications of cyber cases are being used by the AGC and PDRM.

3.1.1 Cyber Court

A cyber court has been established to streamline the hearing and disposal of cyber-related cases. The first phase of its implementation started on the 1st of September 2016 at the Kuala Lumpur Sessions Courts (The Star, 2016). One Criminal Sessions Court has been designated as Cyber Court (Criminal) to handle all cyber related criminal cases and one Civil Sessions Court has been designated as Cyber Court (Civil) to handle all cyber related civil cases. Fifteen Acts have been registered by the chief registrar and ten judicial officers (session judges) with sufficient knowledge in IT have been identified to handle cases in this special court. The Acts registered are:

- Computer Crime Act 1997
- Communications and Multimedia Act 1998
- Malaysians Communications and Multimedia Act 1998
- Digital Signature Act 1997
- Copyright Act 1987
- Telemedicine Act 1997
- Optical Disc Act 1987
- Electronic Commerce Act 2006
- Electronic Government Activities Act 2007
- Penal Code (Act 574)
- Prevention of Crime Act 1959
- National Security Council Act 2016
- Security Offences (Special Measures) Act 2012
- Sedition Act 1948

Other Act that is being considered to be included in the Cyber Court is the Financial Services Act 2013. The second phase would be to implement this court throughout Malaysia. However, there is no specific date provided by the judiciary for the implementation of cyber court in other states.

3.2 Challenges

The prevalence of cloud-based applications results in the need to improve the cross border coordination of law enforcement and service providers (including cloud service providers) to enable digital forensics processes to be carried out in ways that comply with international standards and the laws of the country. This includes maintaining integrity and chain of custody of digital evidence in the acquisition, preservation, analysis and presentation as exhibits in court.

There are great challenges in identifying and locating the offender due to the distributed nature of the "crime scene", in which relevant evidences may reside within cloud-based application and networked based devices such as IoT, mobile computers as well as enterprise servers and firewalls.

The sophistication involved in organised crime requires laws to address attacks that affect online services, but do not physically destroy the infrastructure (e.g. Distributed Denial of Service Attack). At the same time, activities such as selling of email addresses that financially fuels spammers and recruitment of crime actors need to be effectively addressed by the law and require understanding of the anatomy of organised crime.

Malaysia has its share of prosecution involving cybercrime as shown in Case Study 1 and 2, which is only the tip of the iceberg. The underlying threat of cybercrime goes beyond apprehending compromised personnel, but also an understanding of the larger syndication activities that are well financed to support the marketing and counterfeit of information that constantly evolves to subvert detection.

Case Study 1 :
Unauthorised Modification of Land Title

Several cases have been identified involving compromise of internal staffs handling information system, as well as forged signatures and counterfeit of documents resulting in change of land ownership. There are public statements issued by police that Sistem Pendaftaran Tanah Berkomputer Pejabat Tanah dan Galian (PTG) was illegally used for land title transfer by internal staff.

Source : (Institut Tanah dan Ukur Negara, 2009)

Case Study 2 :
Unauthorised Modification of Records

A government personnel had been charged for unauthorised modification of nationality status of 19 individuals via the National Information System Records at the Department Office of Nationality, Marriage and Divorce, Department of National Registration (JPN) Melaka between 24 December 2014 and 27 March 2016. A total of 20 charges were made for hacking and accepting bribes totalling RM44,000.

Charges were made under Act 563 Computer Crimes Act 1997 (Section 5: Unauthorized modification of the contents of any computer (a fine not exceeding one hundred thousand ringgit or imprisonment for a term not exceeding 7 years or both)) as well as Act 574 PENAL CODE (Section 161: Public servant taking a gratification, other than legal remuneration, in respect of an official act (a fine or imprisonment for a term not exceeding three years or both)).

Source: Berita Harian, 21 Sept 2016

3.3 Way Forward

Prosecution of cyber-related cases have and will likely depend heavily on digital evidence. As presented in the statistics and case studies above, some key areas to be addressed is the approach in recording unconventional evidence (non-printed) presented to the court and providing sufficient clarity for judges to comprehend prior to passing judgement. Addressing requirement for certain level of competency amongst the people involved in the handling of digital evidence, maintaining the chain of custody, comprehensive processes and appropriate infrastructure, could improve the level of evidence admissibility in court. Technical competency among those involved in the handling of digital evidence is essential to avoid compromise and contamination of evidence. For example, in identification and acquisition of smart phone, it is important to ensure that the information within the device cannot be tampered remotely. Thus the use of Faraday box or equivalent is essential.

In ensuring admissibility of digital evidence, it is pertinent that organisations first responders and law enforcement officers adopt international standards such as ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence.

Due to the rapid advancement of technology and scarcity of resources, it is strategic for law enforcement computer forensics labs to have focus areas of specialisation, depending on the nature of cases often encountered by the respective digital forensic lab. This will enable development of Malaysian experts in various technologies to address the growing level of complexity demanded in investigating organised crime and more recent technology such as IoT and Big Data. Greater collaboration and information exchange between law enforcement agencies and technical agencies, such as PDRM, BNM, MCMC, KPDNKK, LHDN, AGC and CyberSecurity Malaysia, can further prepare them to address the advancement of organised crime. In addition, there is a need for law enforcement to work closely with a team of specialists from multidisciplines, to assist in investigations.

To address the shortage of competent resources across the nation as well as logistic challenges, there may be a need to consider virtual court hearings, but only when there is sufficient information security controls and resiliency in the network services.

04
Technology and Infrastructure towards Resiliency

4.0 Technology and Infrastructure towards Resiliency

4.1 Current Technology and Infrastructure

The IoT and Big Data are expected to transform businesses in various sectors. Network ready devices are already becoming ubiquitous in many aspects of day-to-day life, from fitness trackers, pacemakers, cars to control systems for homes and offices. Among these technologies, most devices are Internet-connected. IoT use cases (ISACA, 2015) include, but are not limited to, the following:

a. Manufacturing and logistics

i. Machine-to-machine communication
ii. Machine-to-infrastructure communication
iii. Asset tracking of goods on the move

b. Health care and life sciences

i. Remote monitoring of patient health
ii. Cardiac pacemaker

c. Industrial and home automation

i. Smart city, smart homes and automation
ii. Industrial building automation
iii. Livestock farming – tagging and devices to monitor activities

d. Retail

i. Replacement of bar coding and radio frequency identification (RFID) with devices that feed more data to monitoring systems, thereby improving supply chain efficiency
ii. Easier product learnability and discoverability through product and smart phone communication

Based on various studies, the IoT installed base is predicted to grow to multiple 10s of billion units by 2020. IoT further creates dependency on cloud computing service providers. Gartner predicts there will be dependency on cloud-based security in realizing the strength of presence and scale of IoT (Gartner, 2016). To further improve services, big data analytics will be widely incorporated to further exceed user's expectation. Cyber security is essential in all these services, primarily as an enabler for businesses.

As shown in the case of St Jude heart implants, vulnerabilities were discovered that could lead to a compromise of a medical device with possible life threatening impact to the user. It is worth noting that one of the manufacturing plang is in Malaysia.

Implanted Device Vulnerable to life-threatening Hacks

Abbott Laboratories (ABT.N)'s move to protect patients with its St. Jude heart implants against possible cyber-attacks, releasing a software patch on Monday that the firm said will reduce the *extremely low* chance of them being hacked.

The company disclosed the move some five months after the U.S. government launched a probe into claims the devices were vulnerable to potentially life-threatening hacks that could cause implanted devices to pace at potentially dangerous rates or cause them to fail by draining their batteries.

Source: (Reuters, 2017)

St. Jude 'looking' to expand production and services operations in Malaysia

St. Jude, which has invested about $625 million in Penang since 2011, is investigating whether it will increase its product offerings and develop a local vendor ecosystem in the country. The company currently produces cardiac pacemakers, leads and defibrillators in Malaysia, and recently added neuromodulation products to the line. The country is one of St. Jude's leading manufacturers of pacemakers.

Source: (Emmanuel, 2014)

Another aspect of security in various technology deployed in the market have dependencies on the strength of cryptographic algorithms. It is a fact that selected technologies are subject to cryptographic key strength export restrictions by their country of origin. As a national strategic measure to increase aspects of confidentiality, integrity, authenticity and non-repudiation as well as national self-reliance in the use of cryptography, Malaysia initiated and established the National Cryptography Policy in 2013. The key objective is to increase the level of information security protection within the government and national critical agencies based on the use of Trusted Cryptographic Products. The aim of the National Cryptography Policy is to increase the capacity in development of human capital.

4.2 Challenges

In embracing a more complex interconnected and integrated technology in IoT and Big Data, there are pertinent cyber security challenges that need to be addressed.

According to a report of an analysis of a DDoS conducted by an international security operations team (Sucuri Inc.), the DDoS attack in June 2016 generated over 50,000 HTTP requests per second which lasted for a few days, and the source was traced to CCTV devices. What was alarming is that, the top fifth highest number of contributor to the attack was CCTV originating from Malaysia (Cid, 2016) as shown in Figure 4.1.

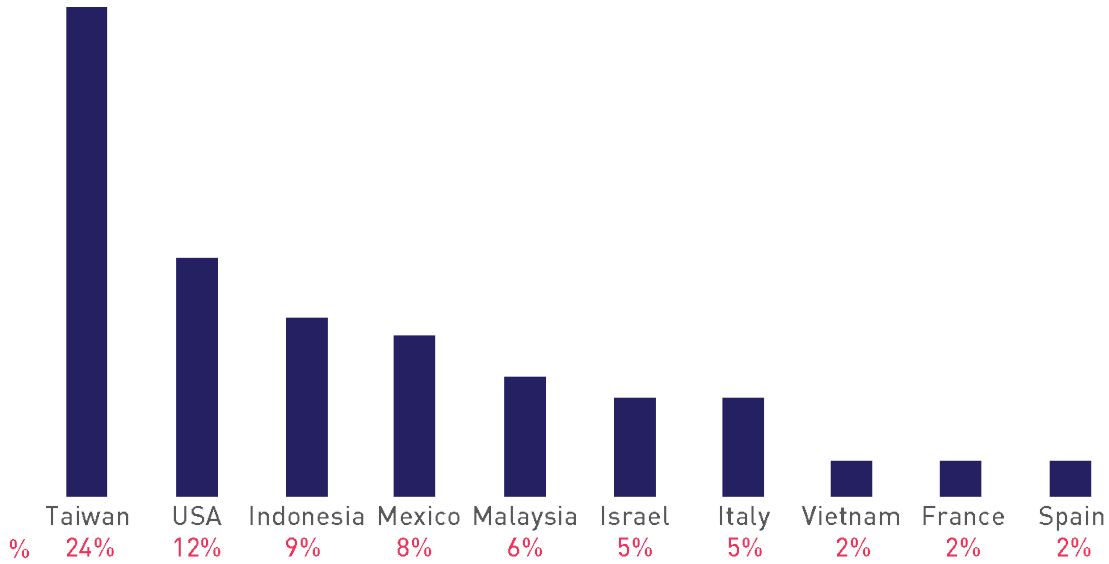


Figure 4.1: CCTV DDoS Botnet Geographic Distribution
[Source: Sucuri Inc.]

Key cyber security challenges faced by these IoT devices are due to underlying issues in technology architecture and configuration such as:

a. Insufficient access control in authentication and authorisation.
b. The use of manufacturer default credentials.
c. Lack of transport and/or network encryption, resulting in credentials being transmitted in clear text.
d. Insecure web or mobile users interface that contained known and common vulnerabilities.
e. Lack of secure code practices in the design and development of the application.
f. Weak security of personally identifiable information and credentials.

In addition, there has been an increased number of targeted attacks on Domain Name System (DNS) service providers, which shows interest in learning the capability of DNS service sustainability. Failure of key DNS providers in the world can impair the use of Internet.

On 30 November 2015, the Internet Domain Name System (DNS) Root name servers were hit with DDoS attack (Root Server Operators , 2015). DNS registrars typically provide authoritative DNS services for thousands or tens of thousands of domain names, and if there is a service-impacting event, the collateral damage footprint can be very large (WIRED, 2016). Later on 21st October 2016, a DNS service provider called Dyn, was hit by Mirai bot DDoS attack from 10s of millions IP Addresses, impacting several major cloud service providers. Security expert Bruce Schneier suggested these DDoS attacks take the form of precisely calibrated attacks designed to determine exactly how well these companies can defend themselves, and what would be required to take them down (Schneier on Security, 2016).

4.3 Way Forward

In the wake of recent targeted large-scale attacks, developed countries such as the US have issued IoT security guidelines. There is also a call for regulatory establishment to mitigate these vulnerabilities as well as a proposal on a Cyber Hygiene Bill. Cyber security experts in US are calling for government intervention in tackling IoT security. The aim is to create and deploy safer technologies for the public at large, critical services and for safer online business environment.

In Malaysia, businesses that largely consist of manufacturing and services contribute to the export economy shall be subject to these developed countries import requirements. At the same time, local home grown products that aim to gain the international market share and for foreign products reaching Malaysian shores shall be a need to comply with a certain level of security standards or guidelines as part of a risk-based approach to technology implementation. Defining the level of security standards desired of technology brought into the country and establishing effective control measures for compliance will be imperative.

To begin with, the Trusted Cryptographic Products under Malaysia's National Cryptography Policy provides a mechanism for evaluation in one aspect of security. There are other areas that require compliance to security guidelines, such as access control, internet services and default configurations of devices that are network ready. Common Criteria and Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme are approaches to distinguish the level of security evaluation undergone by a product. However, baseline requirements are necessary to define an acceptable level of security for the consumer as well as level for mission critical.

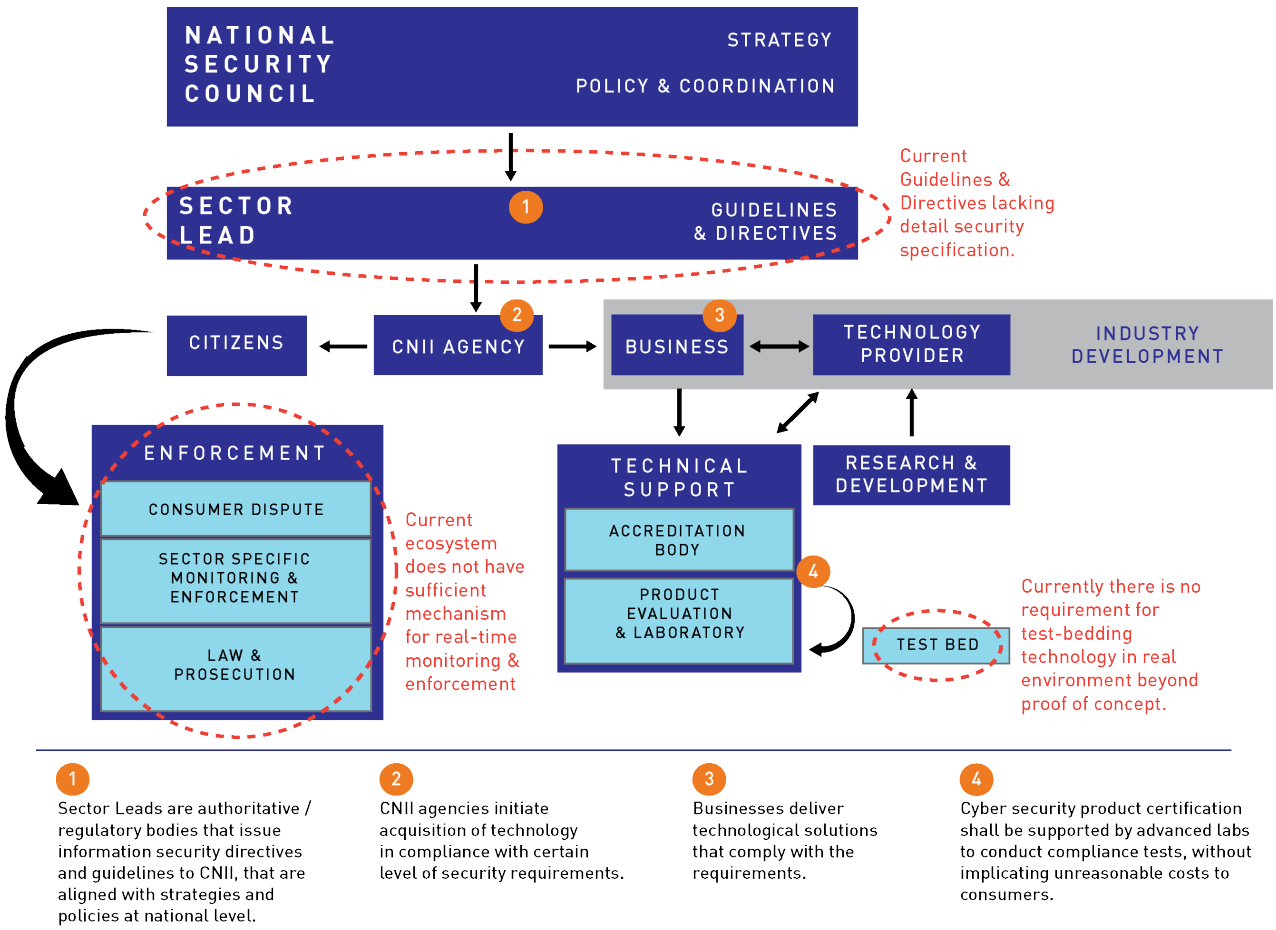


Figure 4.2: Cyber Security Risk-based ecosystem towards technology resiliency

It is desirable to establish a Risk-based Ecosystem, as illustrated in Figure 4.2, which is guided by policy at the national level, followed by directives and guidelines of authoritative bodies, and supported by advanced labs to conduct compliance tests, without implicating unreasonable costs to the consumer. The risk-based ecosystem is aimed at achieving technology and infrastructure resiliency.

In addition, to counter periodic targeted DDoS attack on large DNS service providers, there is a need to ensure resiliency of the .my domain.

National policies need to balance the benefits of technology and how to reduce cyber-risks (e.g. to provide incentives and regulations for businesses to implement cyber security in their product). There is also a need for the enforcement of technology compliance with information security guidelines and/or International Standards in procurement processes. In realising this, there is a high demand for security specialist in the respective security domain to address issues pertaining to the network, system, application and hardware to ensures cyber security needs are being addressed at design, development and implementation stages.

05
Cyber Security Readiness

5.0 Cyber Security Readiness

Cyber Incidents will occur and the recovery of services will be dependent on the level of readiness of the personnel, technology and processes in place, to ensure a minimal disruption of services in response to the incident.

Continuous cyber security awareness is a must for the public at large, who are the end-users of technology services, in order to create a new norm. Ultimately a cyber security conscious society will be able to reap benefits of information technology in its true sense for a developed nation and knowledge-based economy.

A cyber security readiness agenda needs to be inculcated at organisational and national level with greater commitment. Executing cyber drills and cyber security playbook at organisation level serves as a platform for developing relevant expertise. Such exposure will greatly contribute to preempt appropriate cyber security incident response at both the organisation and national levels.

5.1 Current Level of Readiness

In addressing the need for cyber security readiness at the organisation level, there have been national cyber drills conducted over the last 10 years at critical national information infrastructure agencies and sector leads.

However, the readiness level of each agency and sector is varied at multiple levels. Appropriate corrective and preventive actions need to be in place by the participating agencies based on risk-based outcomes. There is a need to ensure the sector leads and regulators of the respective sectors provide incentives and/or enforcement to ensure compliance and continuity of such initiatives.

The pervasiveness of connectivity of devices and information allows on-going attacks to be carried out relentlessly. This increases the likelihood of successful penetration, given sufficient resources to carry out the attacks. As such, organisations need to ensure visibility of threats, vulnerabilities monitoring and automation within applications and network environments in order to develop appropriate mitigation strategies, to deal with noise and advanced threats in the network environment.

Several studies have shown a disparity in fulfilling the market demand for cyber security professionals. Based on a study by Information Systems Audit and Control Association (ISACA) (ISACA, 2017) as shown in Figure 5.1, there is shortage globally of qualified cyber security professionals to fill the gaps across sectors within the industries. Not having skilled employees certainly impacts upon an enterprise's ability to identify, contain and mitigate complex security incidents, which could then result in an increased cost to organisations.

32%
Organisations take more than 6 months **to fill cyber security positions**

22%
Companies in Asia are unable **to fill open cyber security positions**

55%
Practical and hands on experience is **most important for cyber security candidates**

69%
Organisations require **security certificates for open positions**

Figure 5.1: Shortage of qualified cyber security professionals across the globe
[Source: ISACA 2017]

The same scenario exists in Malaysia. Both industries and higher learning institutions are making efforts to address the shortage of competent cyber security professionals. There are various offerings of cyber security modules at local universities, however, the number trained and experienced personnel remains low. This is due to the expectation that security know-how needs to be developed through on-the-job experience and certification. For example, businesses have a tough time finding talent with skills in areas of secure software development, intrusion detection, and attack mitigation. Organisations plan to address the skill shortage through outsourcing and deploying security technology, but primarily this is only feasible for areas that are easily automated. In the US alone, about 209,000 cyber security jobs were unfilled in 2015 (Center for Strategic and International Studies, Intel, 2016).

5.2 Challenges

There is a need to improve response towards targeted and complex attacks. This requires competent cyber security personnel who understand the broader threat and business landscape, as well as able to drill down to identify gaps in business implementation and the root cause of the attack.

Within the Malaysian government sector, there is a challenge in retaining information security professionals within their domain of expertise due to the lack of career growth opportunities. Presently, the career development of qualified information security professionals leads them to positions within government agencies that may further dilute their own expertise and know how in information security domains.

In terms of areas of skills required, several recent employment studies reveal that the largest gap exists in intrusion detection, secure software development and attack mitigation. Other areas desirable among information security practitioners is the ability to understand the business and to have strong communication skills in addressing these issues at the management level.

The cyber security awareness initiatives in Malaysia are currently undertaken by relevant agencies or organisations through various approaches and target groups. To name a few, CyberSecurity Malaysia conducts the CyberSAFE campaign, while MCMC conducts the Klik Dengan Bijak. BNM has collaborated with KPDNKK to produce a booklet on guidelines for conducting electronic transactions and PDRM through its collaboration with Lim Kok Wing University implemented the 'Be Smart' programme that targeted children, youth and adults. These commendable initiatives at the same time are experiencing challenges in terms of resources, coverage, approaches and target groups that have hindered the effectiveness of the implementation.

The annual trend of an increasing number of reported fraud incidents to MyCERT indicates lack of awareness among citizens in detecting and avoiding abuse, fraud and crime that are prevalent online. There is a need to educate citizens with knowledge and the ability to detect and avoid abuse, fraud and crime online, as well as to nurture accountable behaviour in creating well-informed and responsible cyber citizens.

5.3 Way Forward

The ability to strategise and deliver solutions that are able to mitigate complex attacks requires experience and exposure primarily by learning from others. As such, the ability to collaborate and share information across C-levels (CEO, CISO, CIO, CTO) within respective sectors should be strongly encouraged for a mutual benefit.

Within the Public Service Department, there is a need to establish cyber security as a vertical (grade) in the government sector to enable specialisation in the various domains under information security and to enable retention of these trained personnel within their expertise by providing sufficient opportunities for career growth.

In academia, there is a need to embed cyber security across taught courses under ICT and Computer Engineering programs. As an example, cyber security requirements need to be taught in Software Programming (secure coding), Software and System Development Cycle (Secure SDLC), Database, Operating Systems, Network, IT Administration and Management, as well as cross platform application development. This effort is in addition to the present dedicated cyber security related courses being taught in colleges and universities.

The same effort of introducing cyber security related issues across non-ICT or non-Engineering disciplines such as covering Cyber law in Law, FinTech in Finance, security risk management of network ready medical devices in Health, among others, is necessary to enable graduates to stay relevant and to be able to grasp the impact of new technological developments.

Organisations need to invest in security certification programmes that add value and complement the skills required besides on-the-job guidance. Other forms of incentives such as matching grants can be offered by higher learning institutions and the government to new graduates to pursue good quality and established security professional certifications primarily in areas of cyber security that are lacking in the country.

Risk-based outcomes of cyber drills need to reach the highest leadership within the organisation and need to be accounted for in meeting business objectives. The identified gaps need to be translated to improved and reformed processes within organisations to ensure resiliency and security of the critical national information services.

The National Cyber Security Awareness Master Plan led by the National Security Council Prime Minister's Department has identified roles and responsibilities of stakeholders based on core competencies within the private and public sectors to conduct targeted and continuous cyber security awareness initiatives. The Master Plan, which is pending implementation, provides an implementation model that identifies the governance platform, the program execution for an identified target audience and the content development approach to enable shared resources and collaboration in program execution. The plan outlines integrated initiatives on public-private driven collaboration and coordination, mobilising resources to enable a wider outreach of programmes to kids, youth, adults/parents and organisations.

06
International Cooperation

6.0 International Cooperation

The world is transitioning into Industry 4.0 where the technologies driving these inevitable global social economic disruptions are enabled by the global internet. Small and agile entities are rapidly innovating to drive a big impact globally in a short period of time, while consumers benefit by having better and cheaper services. In short, the world will become more internet dependant in this era of digital transformation.

While the socio-economic benefits brought about by the internet is real, there is a dark side. The economic and strategic benefits of cyber-attacks have also increased significantly. Given the global nature of the internet, the security threats and vulnerabilities are also international. Hence, addressing these threats require global collaboration and an exchange of information with international partners to be able to have insights and to respond to this dynamic threat landscape that inherently cuts across national boundaries.

In recent days, we have seen the rise of cyber-conflict and even cyber-war between rival nations. This has led to an increased frequency of highly sophisticated cyber-attacks initiated by some nations for various political motivations and interest. There are serious unintended consequences to this aside from the international political tensions. Firstly, this will hinder the abilities for many nations and societies ability to benefit from the disruptive technologies. Secondly, this will further equip cyber criminals with more sophisticated tools and techniques that increase cyber threat risks globally.

Hence, the global community today have started to come together to discuss cyber security norms not only to increase the security of cyber-space, but also to preserve the utility of a globally connected society. As a nation, we need to be involved not only to enhance cyber-safety, but also to have a say in ensuring national interests are addressed in these evolving cyber security norms.

6.1 Current initiatives

To date, Malaysia has contributed and participated actively in various platforms at a regional and global level in addressing cyber security. Its primary involvements are in:

- Asia Pacific Computer Emergency Response Team (APCERT)
- G8 24/7[3]
- Forum of Incident Response Team (FIRST)
- APECTEL - Asia-Pacific Economic Cooperation Telecommunications
- ASEAN Computer Emergency Response Team (ASEAN CERT)
- Internet Corporation for Assigned Names and Numbers (ICANN)
- ASEAN Regional Forum (ARF)
- United Nations Group of Governmental Experts (UN GGE) on Cyber security
- OIC Computer Emergency Response Team (OICCERT)
- ASEAN TELMIN/TELSOM - ASEAN Telecommunications and IT Ministers Meeting/ Telecommunications Senior Officials Meeting
- ASEAN Telecommunications Regulators Council (ATRC)
- Asia Pacific Telecommunity
- International Telecommunication Union (ITU)
- ISO/IEC SC 27

[3] A 24- hour point of contact amongst participating state committed to act expeditiously to secure evidence and release information via Mutual Legal Assistance Treaty (MLAT) or Letters of Request procedure.

These engagements have provided access to relevant point of contacts, primarily in addressing cross border information sharing and cyber security incident response.

At the same time, the Malaysian mirror committees of the ISO (International Organization for Standardization) and IEC (the International Electrotechnical Commission) SC27 is also actively participating in projects on ISO standards development, which allows Malaysia to actively contribute to information security standards development in ensuring adaptability of standards to benefit the nation.

6.2 Challenges

The initiatives on both global and regional platforms provide exposure to technology, lessons learnt and to build liaison that would enable greater coordination in dealing with cyber security incidents, in particular, is time dependent.

There is a limit to fully leveraging on the investments made in our participation in international platforms due to lack of continuity and the participation of competent personnel from relevant ministries, commissioners and security agencies, on the regional and global platform which then restricts networking and cross border collaboration.

Lack of urgency and determination to leverage on the potential of this global community can often limit our ability in addressing incidents involving targeted attacks and international organised crime effectively. For example, a lack of urgency and information sharing amongst critical national information infrastructure agencies and sector leads in addressing incidents involving targeted attacks and organised crime reduces the likelihood of traceability of the offender.

Increase state-sponsored cyber warfare has triggered international initiatives on new norms, and yet the relevant organisations are not deeply involved to present and defend our interests.

The increase in subversive and resilient organised international crime requires computer emergency response teams (CERTs) to establish greater collaboration with law enforcement bodies across the globe.

6.1 Way Forward

There is a need to enhance national strategy with clear goals, activities and associated measures to assess the effectiveness of investments made in participating in international platforms and collaborations. It is critical to consider approaches that can disrupt the business model and infrastructure of organised crime through greater cross-border collaboration.

Learning from the successes and failures of others in policing and enforcing cyber security and curbing infringements of copyright, computer-related fraud, child pornography, online gambling and violations of network security will help in continuous improvements in cyber safety.

Responding promptly to intelligence from trusted international partners on issues that have implications to our country (e.g. cyber terrorism and IoT) can reduce malicious cyber-threats especially those that threaten our critical national infrastructure.

The engagement at international platforms primarily in international standards development and ratification of treaties contributes will ensure that any new international cyber security norms being developed do not contradict national interests.

07

Science, Technology and Innovation in Cyber Security

7.0 Science, Technology and Innovation in Cyber Security

7.1 Current Initiatives

Applied research and development in public key infrastructure (PKI) started in Malaysia in the late 90s under MIMOS initiatives, when web technology was at its infancy. Prior to that, locally developed antivirus solution was also in the market.

As of now, the science, technology and innovation (STI) initiatives in cyber security are mainly concentrated in higher learning institution with some engagement with industry primarily to acquire tools and technology to aid in the research work. Some selected organisations such as MIMOS and CyberSecurity Malaysia also contribute to cyber security research. More recent commercial local solutions include access control solutions, data protection (cryptographic solution), Security Information and Event Management (SIEM) and biometric systems that have undergone various levels of Common Criteria Evaluation. Several innovative solutions have not been commercialised yet, such as toolkits for digital forensics, intrusion detection, web application firewall and digital watermarking, while research that is exploratory include quantum key distribution and operating system security.

MDEC initiatives are in support of cyber security as a strategic initiative based on projections to attain a fraction of the global market share, with the aim to fuel and enable the Digital Economy. The local cyber security companies are primarily in security consulting services.

On the other hand, MIMOS which has previously conducted applied research in Trusted Platform Module (TPM) is now initiating new areas of research in IoT gateway security, Digital ID, Blockchain and maintaining applied research and commercialisation of access control solution using the method of adaptive authentication.

CyberSecurity Malaysia conducts applied research under RMK11, in several areas including Cryptography, Cyber Threats Profiling, Malware Eradication & Remediation, Digital Forensics tools development, Cloud Security Auditing, IoT Security evaluation of medical devices and smart city, Smart Card Security evaluation, SCADA Security simulation for energy sector, Secured System Development Life Cycle (SSDLC) involving source code review, and Information Security Governance, Risk, Compliance (ISGRC) and Privacy. Analytics in security involve the development of solutions in detecting scam and fraud websites.

7.2 Challenges

The cyber security needs spans across sectors at multitude levels to enable successful implementation of technological solutions. Taking cognizance of the New Economic Opportunities (NEO) in STI-based Industries to serve Emerging Markets Report (Academy of Sciences Malaysia, 2017), there are significant opportunities in future digital transformation and disruptive innovation. These disruptive innovations and new business model involve technologies that have an impact on the economy and on safety. The NEO Report emphasizes on pursuing innovation strategically in order to create real value and to meet market demand. However, it is imperative that these strategies include security risk based approaches.

There are initiatives made under US NIST Cybersecurity for IoT Program (National Institute of Standards and Technology, 2017), which addresses fundamental and applied research targeting industry to enable technology advances and innovation. Their initiatives include standards and guidance, which address security for IoT in areas such as Lightweight Encryption, RFID and Bluetooth Security, BIOS Integrity, Industrial Control Systems Security, Blockchain and Verifiable Time. Applied research for IoT security focuses on work to address market-focused application of research through partnering with industry verticals such as Health Information Technology, Vehicle/Transportation, Smart Home and Manufacturing.

MIMOS's National IoT Strategic Roadmap initiated in 2015 portrays gaps in cyber security initiatives and risk assessment. The current observation reveals that there is a lack of research in security and safety in cyber physical systems. In general, at the national level, there is absence of an understanding of security requirements among consumers and industries in the wake of adopting emerging technologies.

Despite the various initiatives by higher learning institutions and organisations conducting research in cyber security, there are inadequate collaboration and synergy across these research organisations as well as insufficient prioritisation of research.

7.3 Way Forward

Malaysia's direction towards developing science, technology and innovation (STI)-based industries requires sustainable and resilient technologies. Taking cognizance of fluidity and continuous evolution of technology as described in chapter 4, it is recognised that currently, one of the common underlying technology requirements across industry sectors is primarily the IoT technology. In meeting these needs, the cross domain functions of security, safety, resilience, trust, privacy, connectivity, interoperability, and dynamic composition are essential.

Mapping the IoT architecture with security requirements is relevant considering that the conventional computing environment is a subset of the IoT ecosystem. As shown in Figure 7.1, the IoT architecture includes a platform that hosts Operations Support System (e.g. provisioning, monitoring, reporting) and Business Support Systems (e.g. accounts, billing), Application Services that includes Basic Service System for data services and Business Service System (e.g. ERP, CRM, asset management, human resource), Interchange System, Access Management and the IoT gateway. The IoT gateway interacts with actuators and sensors to enable and operate the cyber physical system (CPS). The IoT gateway also interacts with user interface devices that provide human machine interface (HMI) and digital user.

The entities within each component are very general and optional depending on specific applications. Figure 7.1 further illustrates the security assurance requirements of each entity. There are also four different types of networking (proximity network, access network, user network and service network), that require secure network protocols and secure connectivity.

Security assurance involves a multi layered approach to security control. This requirement includes securing and strengthening of operating systems, firmware and configurations of systems that host the application. Data stored, transacted and processed require anonymisation and encryption, while application using the data requires protection, such as input validation, to prevent application layer attacks. Entities that require access shall undergo strong authentication and authorisation. In addition, the cyber physical system that interacts with actuators and sensors require safety measures to protect against hazards, for example, under failure mode, while security measures is essential in protecting against intentional attacks.

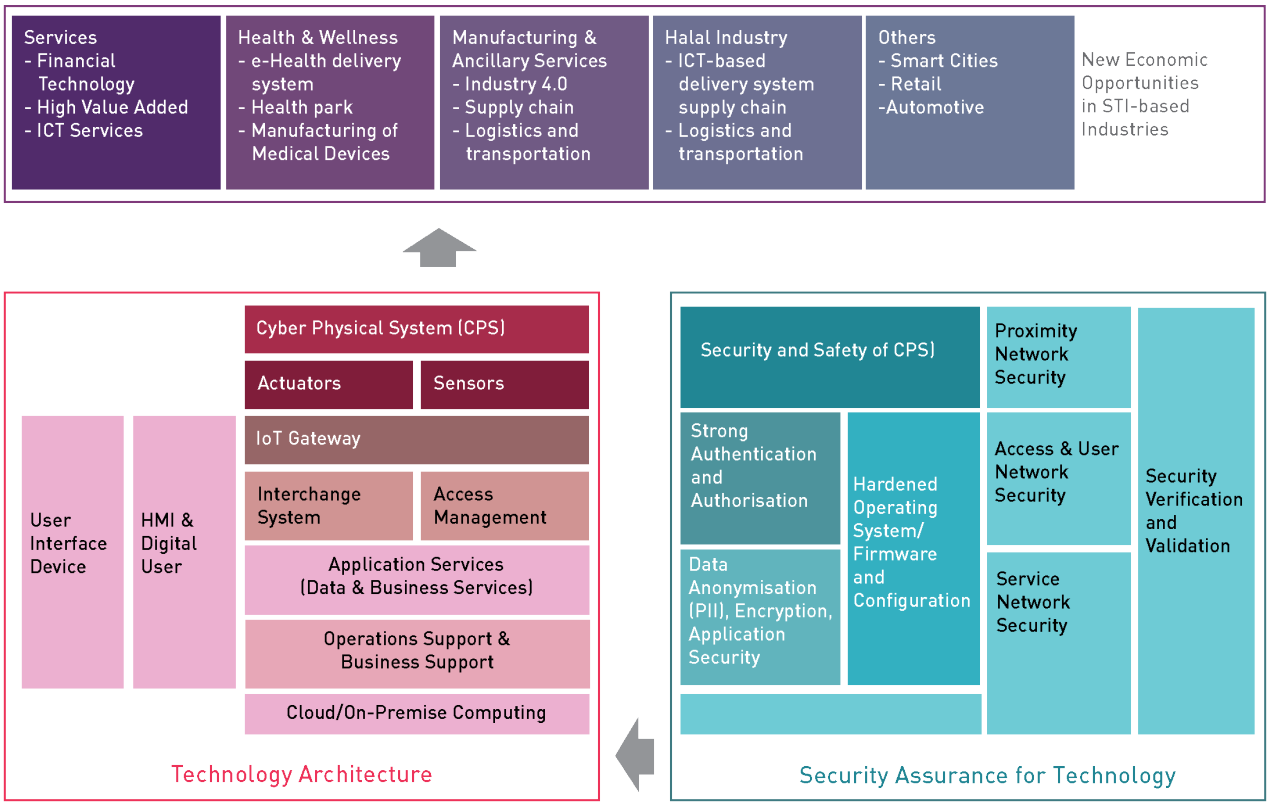


Figure 7.1: Security, safety and privacy requirements in IoT applicable across sector

Understanding IoT safety and security requires risk assessment by subject matter experts in security, safety and the industry involved. In many operational environments, approval to operate or to connect devices will not be granted if safety requirements are not met.

Initiatives in Industry 4.0, Smart Cities, Retail, Automotive Transportation and Connected Healthcare that are highlighted in the NEO Report require a risk-based approach in aspects of cyber security to ensure resiliency of the adopted and developed technologies primarily for applications that have an impact on public safety and mission critical implementation. A commendable approach taken by Germany was to conduct risk assessment prior to investment in Industry 4.0. As early adopters of Industry 4.0, they clearly identified that their biggest obstacles for implementing Industry 4.0 were data and network security (McKinsey Digital, 2015). Their concern in particular was on data security and safeguarding systems, as well as a lack of uniform standards for data transfers and end-to-end connectivity via wireless networks. Malaysia also needs to foresight similar challenges.

Taking into context the current technology evolution, STI-based development requires innovation in areas of cyber security to preserve safety, security and privacy. As such, based on the defence-in-depth methodology, further enhancement to the security approach is visualised as depicted in Figure 7.2. The core of the diagram illustrates:

- the key information assets to be protected within the inner shell, that exists in forms and format of application, which includes multiple components such as databases, web services, intelligence, analytics and rules engine;

- the embodiment of data requires anonymisation for PII when used across systems for analytics, as well as encryption of various types of data in storage and transmission;

- application requires further protection at the code development level, which includes controls such as input validation to protect against injection attacks;

- the operating systems or firmwares that host the data and application require strengthening due to the prevailing vulnerabilities on operating systems and firmwares that are common targets of compromise. For example, buffer overflow attacks; and
- the next layer of technology that is commonly exploited is the network, which requires control such as surveillance, access control, secure protocol and encryption to prevent attacks such as man-in-the-middle attacks and spoofing.

At the system back end, there are further controls required, primarily on cloud-based systems, which involve secure virtual platforms, regardless whether for single or multi-tenancy. These security controls include not only software, but may require hardware controls at hypervisor level, for example. The security verification and validation (V&V) is a process and requires security, safety and privacy principles to be incorporated at the design stage in order to enable effective evaluation at various levels of implementation.

The fronting elements that use the data and outcome of processing are either human users or machineries that are part of a larger cyber physical system (CPS), that requires protection in terms of safety, security and privacy. As such, access by human users or machineries alike, need forcible controls that are able to enforce strong yet adaptive authentication and authorisation to curb unauthorised access, modification and usage of resources. At the CPS level, the requirement for safety is of utmost priority, and this can be achieved by incorporating measures such as fail-safe mechanisms to mitigate unsafe consequences of system's failure, at physical endpoint devices and user interfacing components.

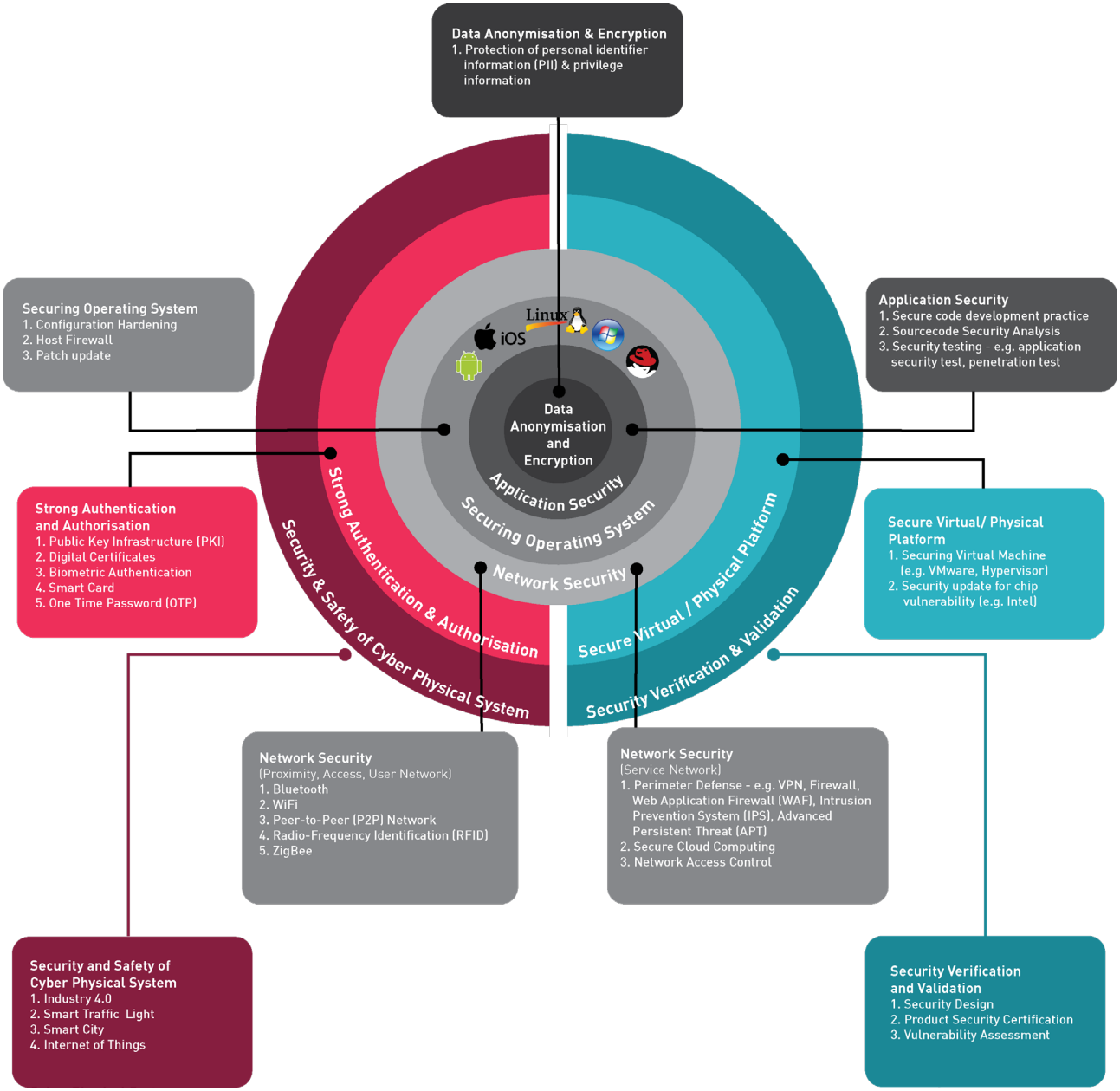


Figure 7.2: Areas for STI in cyber security

Behind every driving force towards technology development or adoption, a fundamental understanding of impact towards security and safety is crucial. As the physical world becomes more dependent on controls exerted by cyber system, the security controls are vital in protecting against intentional attacks that may or may not impact national security, while safety requirements protect against failure that threatens life.

In addition to the growing need for security and safety, there is a valid increase of concern on privacy. As we move forwards, what is slated as Web 3.0, there will be pervasive use of machine learning and artificial intelligence in optimising internet services that allows greater accuracy in information search, to compare and contrast, or recommendations based on personal preference and more. The fast paced development of voice assistants such as Apple's Siri, Microsoft's Cortana, Amazon's Alexa, Google assistant and Facebook's Jarvis that thrives on artificial intelligence will create a need to ensure privacy, public identity concealment or pseudonymity.

The balancing of security and privacy without impeding usability, while at the same time, not compromising safety, requires participation from experts of cross disciplines in applied research. It is highly recommended that these areas in cyber security be part of the future STI Masterplan. There is a need to have a central body staffed with the right talents and also empowered to improve collaboration and synergy across research organisations and to prioritise areas of cyber security research.

Despite the reduction in research and development allocation for 2017, the country still needs to expand in STI-based industries, particularly in Manufacturing (Industry 4.0), Services, Health, Halal Industry and Smart Cities, that requires sustainable and resilient technology. In realisation of the rapid and pervasive adoption of technology, it is strongly recommended that Malaysia allocates 1% of GDP for research and development, primarily in technologies that have a direct impact on multi sectors such as cyber security, privacy and safety.

Malaysia should aspire to become a global player in cyber security and secure a significant fraction of the projected global market share in cyber security products and services. Towards this end, there is a need to create a conducive environment for test-bedding of innovations in developing, attracting and retaining talent and technology players that can create a sustainable and resilient digital economy.

08

Recommendation and Conclusion

8.0 Recommendation and Conclusion

The key recommendation of this report is the need to have a risk-based approach in re-prioritising the cyber security initiatives to enable a safe, secure and resilient cyber environment for the well-being of citizens and wealth creation. As shown in Figure 8.1, this approach begins with the identification of security areas for enhancement and new initiatives, followed by identification of leaders of the initiatives. It is important to ensure that leaders have the mandate to coordinate initiatives to avoid disintegration and redundant initiatives that do not bring about benefits to the nation. Due to the pressing issues of limited resources, a risk-based approach is desirable in prioritising initiatives. Besides the need to be realistic and frugal in funding of the initiatives, it is also important to evaluate and measure initiatives not merely by measuring success, but also by identifying gaps to further form the impetus for better and improved cyber solutions.

Figure 8.1: Risk-based approach in re-prioritising initiatives

The following recommendations have been brought to attention of the Prime Minister of Malaysia through the 3/2017 National Science Council meeting:

1. Cyber Security Strategy

- **Adopt a risk-based cyber security ecosystem** (consisting of risk assessment and prioritisation of control mechanism to meet specific security objectives) thus strengthening the existing committee-based structure

2. Governance

- **Empower central entity**, with the mandate to provide formulation, monitoring, coordination and synchronisation of implementation of cyber security policy, framework and strategy to safeguarding the government, critical national information infrastructure (CNII), businesses and the public large, talent development, as well as coordination of issues on legislation and enforcement in collaboration with all relevant entities.

- **Cyber security shall be mandatory requirement for acquisition** of critical technologies related to networks, systems and applications guided by national policy, directives and guidelines of authoritative bodies.

3. Science, Technology and Innovation

- Ensure R&D and innovation of ICT solutions **comply with cyber security standards or guidelines** supported by accredited advanced **labs and field tests (test-bedding)** to achieve technology and infrastructure resiliency

4. Talent

- Nurture competent and sustainable cyber security talent by:
  i. **Investing** in quality and established security **certification** programs that promote skills development in technical areas of cyber security.
  ii. **Establishing** cyber security as a **vertical in public service** to allow specialization with career progression
  iii. **Embedding cyber security** in ICT & engineering courses and introducing cyber security in non-technical courses (eg. Law, Banking).

The full summary of the approach and action items are provided in Annex A.

References

Academy of Sciences Malaysia. (2017). New Economic Opportunities in STI-based Industries to serve Emerging Market. Kuala Lumpur: Academy of Sciences Malaysia.

BERNAMA. (2016, December 6). BERNAMA : 09 DEC 2016 : MCMC: 94 COMPOUNDS WORTH RM3.45 MILLION ISSUED AS AT NOVEMBER. Retrieved 7 31, 2017, from Ministry of Communications and Multimedia Malaysia: http://www.kkmm.gov.my/index.php?option=com_content&view=article&id=11420:&catid=233:&Itemid=541&lang=en

Center for Strategic and International Studies, Intel. (2016). Hacking the Skills Shortage - A study of the international shortage in cybersecurity skills. Center for Strategic and International Studies, Intel.

Cid, D. (2016, June 27). Large CCTV Botnet Leveraged in DDoS Attacks. Retrieved February 20, 2017, from Sucuri Blog: https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html

Cyber Security Market worth 202.36 Billion USD by 2021. (n.d.). Retrieved February 20, 2017, from Markets and Markets: http://www.marketsandmarkets.com/PressReleases/cyber-security.asp

Emmanuel, M. (2014, November 13). St Jude Medical to expand production, services here. Retrieved February 20, 2017, from News Straits Times: https://www.nst.com.my/news/2015/09/st-jude-medical-expand-production-services-here

European Union Agency for Network and Information Security. (2014). An evaluation Framework for National Cyber Security Strategies. European Union Agency for Network and Information Security.

Gartner. (2016, April 25). Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016. Retrieved August 24, 2017, from Gartner: http://www.gartner.com/newsroom/id/3291817

Infocomm Development Authority of Singapore. (2016). National Cyber Security Masterplan 2018. Singapore: Infocomm Development Authority of Singapore.

Institut Tanah dan Ukur Negara. (2009, November 10). PENIPUAN DALAM URUSAN TANAH : ISU DAN PENYELESAIAN. Retrieved February 20, 2017, from Institut Tanah dan Ukur Negara: https://www.instun.gov.my/index.php/ms/muat-turun-2/muat-turun-pengkalan-ilmu/artikel-1/tanah-3/189-penipuan-dalam-urusan-tanah-isu-dan-penyelesaian-1/file

ISACA. (2015). Security and Privacy Challenges of IoT-enabled Solutions . ISACA JOURNAL VOLUME 4, 1 - 4.

ISACA. (2016). State of Cybersecurity Implications for 2016. ISACA.

ISACA. (2017). State of Cyber Security 2017. ISACA.

Kan, M. (2016, December 12). Dozens arrested in international DDoS-for-hire crackdown. Retrieved February 20, 2017, from PC World: http://www.pcworld.com/article/3149543/security/dozens-arrested-in-international-ddos-for-hire-crackdown.html

Kaspersky Lab IT. (2016). Kaspersky Lab IT Security Risk Report2016 – Measuring Financial Impact on IT Security on Businesses. Kaspersky.

Leonhard, G. (2015, May 11). What is the 4th Platform? Retrieved March 2, 2017, from the futures agency: http://thefuturesagency.com/2015/05/11/what-is-the-4th-platform/

McKinsey Digital. (2015). Industry 4.0: How to navigate digitization of the manufacturing sector. McKinsey & Company.

National Institute of Standards and Technology. (2017, June 27). NIST Cybersecurity for IoT Program. Retrieved July 7, 2017, from NIST: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

NEWMAN, L. H. (2016, October 21). What We Know About Friday's Massive East Coast Internet Outage. Retrieved February 20, 2017, from Wired: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

PWC. (2014). Global State of Information Security Survey 2015. PWC.

Ransomware attacks surge in Malaysia. (2016, September 6). Retrieved February 20, 2017, from Regent Risk Advisory: http://regentsriskadvisory.com/ransomware-attacks-surge-in-malaysia/

Regent Risk Advsory. (2016, September 6). Ransomware attacks surge in Malaysia. Retrieved July 27, 2017, from Regent Risk Advsory: http://regentsriskadvisory.com/ransomware-attacks-surge

Reuters. (2017, January 9). St. Jude releases cyber updates for heart devices after U.S. probe. Retrieved February 2017, 2017, from Reuters: http://www.reuters.com/article/us-abbott-stjude-heart-idUSKBN14T1WT

Root Server Operators . (2015, December 4). Events of 2015-11-30. Retrieved February 20, 2017, from root-servers.org: http://root-servers.org/news/events-of-20151130.txt

Schneier on Security. (2016, September 13). Retrieved February 20, 2017, from Schneier : https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

The Star. (2016, September 1). Special court to handle cyber crime cases ready for use. Retrieved July 27, 2017, from The Star Online: http://www.thestar.com.my/news/nation /2016/09/01/first-cyber-court-in-jalan-duta-activated/

WIRED. (2016, October 21). WHAT WE KNOW ABOUT FRIDAY'S MASSIVE EAST COAST INTERNET OUTAGE. Retrieved July 27, 2017, from WIRED: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

WIRED. (2017, July 1). THE BIGGEST CYBERSECURITY DISASTERS OF 2017 SO FAR. Retrieved July 27, 2017, from WIRED: https://www.wired.com/story/2017-biggest-hacks-so-far?mbid=social_fb

MIMOS, (2015) National IoT Roadmap. MIMOS

Annex A : Summary of Approach and Action Items

Objective 1:
Malaysia to align cyber security policy and synergise initiatives across authoritative bodies in Malaysia to provide clear guidelines that enable greater level of security in day-to-day services rendered by the national critical agencies and businesses. (Refer to Chapter 2)

Approach	Actions
National coordination of cyber security roles during crisis and peace time.	a. Alignment of information security policy requirements at strategic and policy level from authoritative bodies responsible for CNII and businesses are key in getting the message across to board level of these organisations. b. Consolidation of authority and roles in cyber security amongst various government agencies that develop strategy is essential. c. Given clear reporting process for CNII, businesses and public at large, and coordination will enable effective information exchange. d. Greater coordination in leveraging expertise primarily in addressing advanced and sophisticated attacks. e. Establishment of the National Cyber Security Agency as a central entity, with the mandate to provide formulation, monitoring, coordination and synchronisation of implementation of cyber security policy and framework as well national security cyber crisis management. (Refer to Section 2.3)

Objective 2:
Malaysia to tackle advanced and organised cybercrime in order to create secure environment to conduct business in cyberspace. (Refer to Chapter 3)

Approach	Actions
Enable specialisation and multidisciplinary involvement to assist investigations in dealing with advanced threat and organised cybercrime.	a. Addressing requirements of competent personnel involved in the handling of digital evidence for evidence admissibility in court. b. Organisations first responders and law enforcement officers to adopt international standards such as ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence. c. Law enforcement computer forensics labs to have focus areas for specialisation, to enable development of experts in Malaysia in various technology in addressing the growing level of

	complexity demanded in investigating organised crime and more recent technology such as IoT and Big Data . d. There is a need for the law enforcement to work closely with specialist of multidisciplinary, to assist investigations. e. The shortage of competent resources across the nation as well as logistic challenges may require consideration on the need for virtual court hearings. (Refer to Section 3.3)

Objective 3:
Malaysia to take a risk- based approach in development and acquisition of network ready products and solutions to create a secure and safer environment for the public at large. (Refer to Chapter 4)

Approach	Actions
Help to shape a safer and more resilient cyberspace for public and businesses at large by creating greater resiliency within the critical services.	a. Establish a risk-based ecosystem for technology implementation. b. Baseline requirements are necessary to define an acceptable level of security for consumer as well as another level of requirement for mission critical. c. There is a need to ensure resiliency of the ".my" domain. d. National policies need to balance the benefits of technology and reducing cyber-risks. e. There is a high demand for security specialist in the respective security domain within network, system, application and appliance in ensuring cyber security needs is being addressed at design, development and implementation stages. (Refer to Section 4.3)

Objective 4:
Malaysians to have the awareness, knowledge, skills and capabilities to handle cyber threats. (Refer to Chapter 5)

Approach	Actions
Building coherent cross sector collaboration in strategic information sharing and security awareness initiatives Deepening understanding of advanced threats. Developing a culture that understands security risks in context of business resiliency. Expanding capability to develop safer and more resilient technology as well as ability to respond to advanced threats.	a. Improve our ability to collaborate and share information across C-levels (CEO, CISO, CIO, CTO) and within respective sector is critical. b. Establish cyber security as a vertical in public service. c. In academia, there is a need to embed cyber security across taught courses under ICT and Computer Engineering programmes. d. Introduce cyber security related issues across non-ICT or non-Engineering disciplines in particular in Law, Finance and Health.

e. Invest in quality and established security certification programmes that promote skills development in technical areas of cyber security.
f. Risk-based outcomes of cyber drills need to reach the highest leadership within the organisation and translate to improved and reformed processes within organisations.
g. Aggressively implement the National Cyber Security Awareness Master Plan to provide public awareness and education to identified target groups. (Refer to Section 5.3)

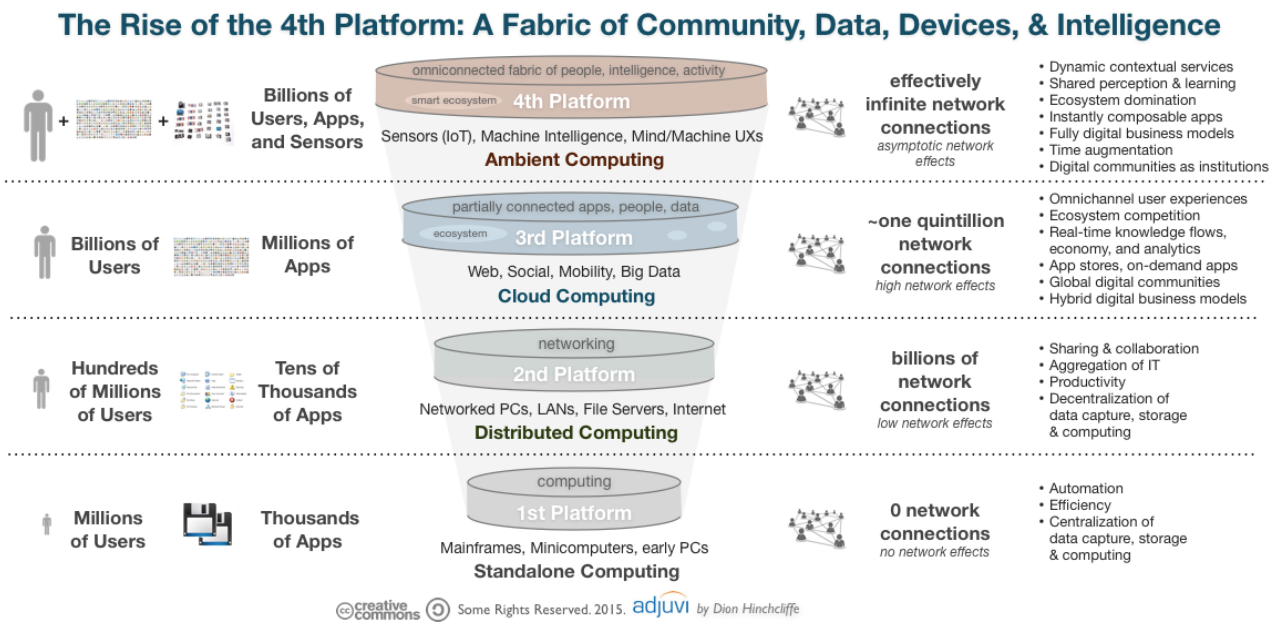
Objective 5:
Malaysian Government to collaborate and engage other trusted international entities for global efforts in combating cyber threats. (Refer to Chapter 6)

Approach	Actions
Enhance the national strategy with clear goals, activities and associated measures to assess the effectiveness of investments made in participating in international collaboration.	a. Disrupting the business model and infrastructure of the organised crime through greater cross-border collaboration. b. Learning from successes and failures of others in policing and enforcing cyber security and curbing infringements of copyright, computer-related fraud, child pornography, online gambling and violations of network security will help in continuous improvement in cyber safety. c. Responding promptly to intelligence from trusted international partners on issues that have implication to our country (e.g. Cyber terrorism and IoT) especially those threatening our critical national infrastructure. d. Ensuring that any new international cyber security norms being developed do not contradict national interests. (Refer to Section 6.3)

Objective 6:
Malaysia to spearhead innovation in cyber security, privacy and safety through science and technology R&D. (Refer to Chapter 7)

Approach	Actions
Stimulate and encourage cross discipline research and collaboration in achieving security, privacy and safety in technology development and adoption.	a. Need for cross domain functions of security, safety, resilience, trust, privacy, connectivity, interoperability, and dynamic composition are essential. b. Security assurance involve a multi layered approach to security control. c. Understanding IoT safety and security requires risk assessment by subject matter experts in security, safety and the industry involved. d. Balancing of security and privacy without impeding usability, while at the same time, not compromising safety, are areas of interest to be part of the STI Masterplan. e. Central body to improve collaboration and synergy across research organisations and prioritizatize areas of cyber security research. f. Malaysia allocate 1% of GDP for research and development, primarily in technologies that have direct impact to multi sector in terms of cyber security, privacy and safety. g. Create a condusive environment for test bedding of innovations in developing, attracting and retaining talents and technology players that can create sustainable and resilient digital economy. (Refer to Section 7.3)

Annex B : The Rise of the 4th Platform



Academy of Sciences Malaysia
Level 20, West Wing, MATRADE Tower
Jalan Sultan Haji Ahmad Shah off
Jalan Tuanku Abdul Halim
50480 Kuala Lumpur, Malaysia

Phone : +60 3 6203 0633
Fax : +60 3 6203 0634

www.akademisains.gov.my

ISBN 978-983-2915-38-6