PUBLIC DATA AT RISK:

CYBER THREATS TO THE NETWORKED GOVERNMENT

APRIL 2015

TRPC

http://www.trpc.biz

CONTENTS

EXECUTIVE SUMMARY

Being a networked government can offer tremendous opportunity for governments globally to connect with their citizens, productively collect and use information, as well as streamline and enhance the efficiency of internal work streams and processes. However, this can open up the Government to severe threats to national security, infrastructure, data, and international diplomacy. Addressing and mitigating these threats are essential to constructing a robust and resilient cyber security strategy.

In most cases, it is the government Chief Technology/Information Officer (CTO/CIO)'s responsibility to understand and manage the issues. However, a more holistic approach towards cyber security must be undertaken if a country is to be cyber ready – from the setting up of technical computer emergency response teams (CERTs), to educating both civil servants and the public at large, to protecting the procurement and purchasing process, which is often a gateway for malware and viruses to enter a system through unhygienic procurement practices.

This paper aims to provide a non-technical explanatory framework by which public officers *other than the technically-trained officers* can understand and discuss the issues together. These should include (but not be limited to) public officials from the communications, procurement, finance departments etc. This paper should also be used as a tool by the CTO/CIO to garner more broad-based support across the various government agencies for a whole-of-government approach to cyber security.

This report begins by reviewing the high government dependence on IT, the key information stored and managed by governments, and where government IT spend goes to. It then outlines the types of cyber threats governments are facing today, and concludes with a roadmap to creating a cyber security policy, offering a practical checklist by which governments can assess their institutional cyber security robustness. These chapters are outlined in brief below.

Chapter 1: Government IT Systems and infrastructure

- Development of e-government infrastructure and online services has had a significant positive impact on interaction and engagement with citizens through e-governance infrastructure. The USA, South Korea and Singapore are regularly being ranked as leaders in this field.
- The provision of public utilities and national defence services has also increasingly also been networked and channelled through IT systems.
- While tremendously useful, if not managed properly, this could expose governments and citizens to severe breaches of privacy, data theft and compromise in the provision of key public services.

Chapter 2: Types of information stored by governments

- Large amounts of public and private data are now stored and made accessible through government IT systems. This includes public information and documents that are now accessible online, sensitive data such as national ID numbers or tax information, internal government communications such as email and classified security information.
- Different levels of security and protection are required for the different levels of data and it is essential that governments take the right steps to ensure the integrity of the types of information that are stored and accessed on their systems.

- Major cyber attacks in recent years have targeted information and data stored by governments that have compromised citizen security and resulted in enormous cost to and loss of confidence in government.

Chapter 3: Public Sector IT Spending

- North America, Western Europe and Australia lead in committing money and resources to cyber security efforts. Several Gulf and Asian countries have stepped up commitment in recent years following attacks.
- Public Sector spending on cyber security is generally focused on rapid detection and response to a threat, remedial work necessitated by data breaches, and ongoing maintenance of websites and online services.

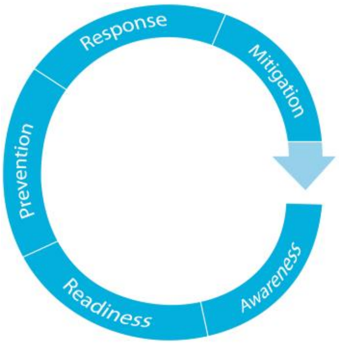
Chapter 4: Types of Cyber Security Threats to Government

- The types of cyber security threats posed to governments are numerous with as many levels of severity of impact. Common attacks include: cyber terrorism and threats to critical infrastructure, theft of confidential or sovereign data, denial of service attacks on e-government infrastructure, cyber espionage and advanced persistent threats.
- Counterfeit software, lack of maintenance and lax procurement supply chains pose a significant security risk by providing doorways to malware entering and abusing government networks and systems.

Chapter 5: A Roadmap to Constructing a Resilient Cyber Security Strategy

- A resilient cyber security strategy must be holistic and address different stages of an attack, including prevention, response and mitigation.
- An effective roadmap towards constructing a resilient strategy should include steps taken to;
  - ✓ Raise awareness and the level of understanding among the general population, by educating business owners, students and government agencies on the threats that exist as well as how to protect their networks from attack.
  - ✓ Ensure Readiness through the creation of Computer Response Emergency Teams (CERTs) that coordinate capabilities and share knowledge.
  - ✓ Prevention of attacks through building and maintaining a safe and secure network infrastructure and supply chain through good maintenance and procurement practices.
  - ✓ Responding effectively to attack through empowering legislators, regulators and policy makers with good regulation and using cyber hygiene tools that can fight attack.
  - ✓ Mitigate damage by rebuilding trust with citizens and other stakeholders through effective communication, established review processes and building partnerships with industry, other governments and international organisations.

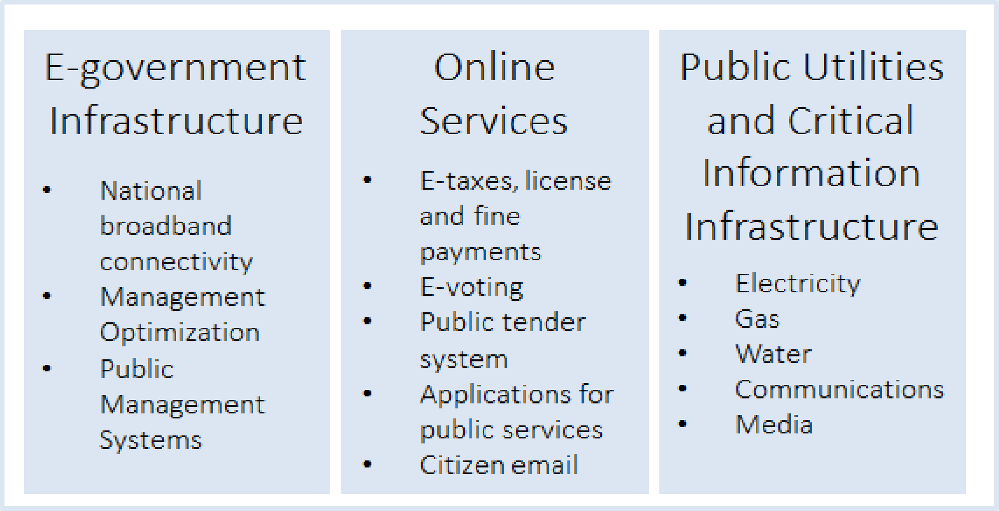
Figure 1: Roadmap to building a robust cyber security strategy



CHAPTER 1: GOVERNMENT DEPENDENCE ON IT SYSTEMS

Governments today are responsible for more information than at any other point in time. A vast array of different types of information are being stored across a variety of IT systems that in some cases are quickly evolving, while in other cases are proving dated and vulnerable. Information storage has grown in volume and significance in the last decade as public sector responsibilities around service delivery expand in the digital age.

Figure 2: Government Dependence on IT Systems



E-government Infrastructure

- National broadband connectivity
- Management Optimization
- Public Management Systems

Online Services

- E-taxes, license and fine payments
- E-voting
- Public tender system
- Applications for public services
- Citizen email

Public Utilities and Critical Information Infrastructure

- Electricity
- Gas
- Water
- Communications
- Media

To put a figure on the volume of data governments are now dealing with, in 2013, it was estimated that US federal agencies alone store around 1.6 petabytes of data, and this is expected to grow to 2.6 petabytes by 2016[1]. A data centre that is currently being built by the National Security Agency of the USA is estimated to have the capacity to store between an Exabyte and a Yottabyte of data.

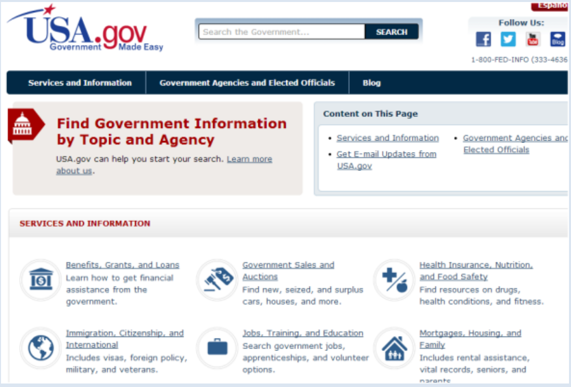
> *Two trends shaping the management of public documents and information across the public sector in recent years are "open government" policies and next-generation cloud initiatives. Among the many implications of these initiatives is the higher level of security risk for government.*

All levels of government are becoming ever more reliant on the quality of their information to coordinate across government and successfully deliver services. As a result, governments are becoming increasingly dependent on the software that powers their information systems and processes, and enables access and communications.

E-Government Infrastructure

Since the late-nineties, most countries have released e-government strategies or defined an approach to e-government resulting in significant progress at all levels of public administration. The underlying principle of e-government, according to the United Nations Department of Economic and Social Affairs[2], is to improve the internal workings of the public sector by reducing financial costs and transaction times so as to integrate work flows and processes and enable effective resource utilization – in other words, to promote coordination and connectivity between ecosystems and development outcomes. In this context, reflecting the importance and universality of these developments, a number of e-government readiness surveys have been established to assess relevant infrastructure development. In addition to broadband connectivity, personnel, and promotion programmes, typical indicators also include 'Management Optimization' (e.g. system optimization, integrated network system, administration and budgetary systems, public management reform by ICT, etc.) and 'Required Interface Functioning Applications' (e.g. e-tender systems, e-tax system, e-voting system, etc.).[3] The United States, Singapore and South Korea have consistently been at the top of annual rankings of e-government development (see Box 1).

Box 1: United States: 2014 World Leader in e-Government Development



Find Government Information by Topic and Agency

USA.gov can help you start your search. Learn more about us.

Content on This Page

- Services and Information
- Get E-mail Updates from USA.gov
- Government Agencies and Elected Officials

SERVICES AND INFORMATION

Benefits, Grants, and Loans
Learn how to get financial assistance from the government.

Government Sales and Auctions
Find new, seized, and surplus cars, houses, and more.

Health Insurance, Nutrition, and Food Safety
Find resources on drugs, health conditions, and fitness.

Immigration, Citizenship, and International
Includes visas, foreign policy, military, and veterans.

Jobs, Training, and Education
Search government jobs, apprenticeships, and volunteer options.

Mortgages, Housing, and Family
Includes rental assistance, vital records, seniors, and parents

The US e-Government portal (www.USA.gov) quickly directs citizens to information or services that they seek. This portal links to every agency, as well as state, local and tribal government. Since 2010, it has been available through mobile applications. Value-added features includes content alerts that visitors can sign-up for, as well as a live-chat capability with a government representative.

The US government also owns a Spanish language portal (www.GobiernoUSA.gov), which pulls together all the Spanish language government websites and makes them easily accessible.

Online Services

Building an e-government infrastructure to improve efficiency and effectiveness of public service delivery is one facet of being a networked government. Another area that has progressed in many countries is online service delivery. Many countries are moving from a decentralized organization model, to an integrated whole-of-government model that aims to centralize the entry point of service delivery to a single portal where citizens can access all government-supplied services, regardless of the government authority providing them. In some countries, the whole-of-government approach helps build a transparent government system with interconnected departments and divisions, further developing government efficiency and effectiveness.

Open platforms, interconnection, and interoperability have become some of the most important development issues facing government information technology officers.

As governments move to online activities and look for ways to innovate service provision and citizen engagement, they are confronted with issues around creating new service offerings, bundling of services, and opening data systems. Different information systems now need to talk to each other and public organizations must link their systems to others. Open platforms, interconnection, and interoperability have thus become some of the most important development issues facing government information technology officers. This is gaining ever more critical importance with the advent of open data movements.

Two trends shaping the management of public documents and information across the public sector in recent years are “open government” policies and next-generation cloud initiatives. The US government claims that its open government initiative has allowed “public access to over 390,000 high value agency data sets on such diverse subjects as auto safety, air travel, air quality, workplace safety, drug safety, nutrition, crime, obesity, employment, and health care.”[4] The US has also embarked on a cloud initiative requiring government agencies to move low- and moderate-impact systems to the cloud by 2015. Among the many implications of these initiatives is the higher level of security risk for government.

Public Utilities and National Defence Services

The provision of public utilities such as electricity, natural gas, water, and telecommunications – otherwise known as Critical Infrastructure, or Critical Information Infrastructure or CII – are essential services that are increasingly networked through transmission systems.

The communications and utilities sectors are also increasingly dependent on the IT sector, due to the software behind the operating systems, management software, billing software, and any number of other software packages being used. This also includes the Supervisory Control and Data Acquisition (SCADA) systems providing real time control for most power and utility facilities.

This in turn, has raised a variety of security concerns. To begin to address the risks that come with connection and collaboration, governments have been investing in secure networks such as GSI (Government Secure Intranet) and GCmail (Government Connect Mail). However, these tend to offer only limited capability to communicate securely with external third parties and suppliers.[5]

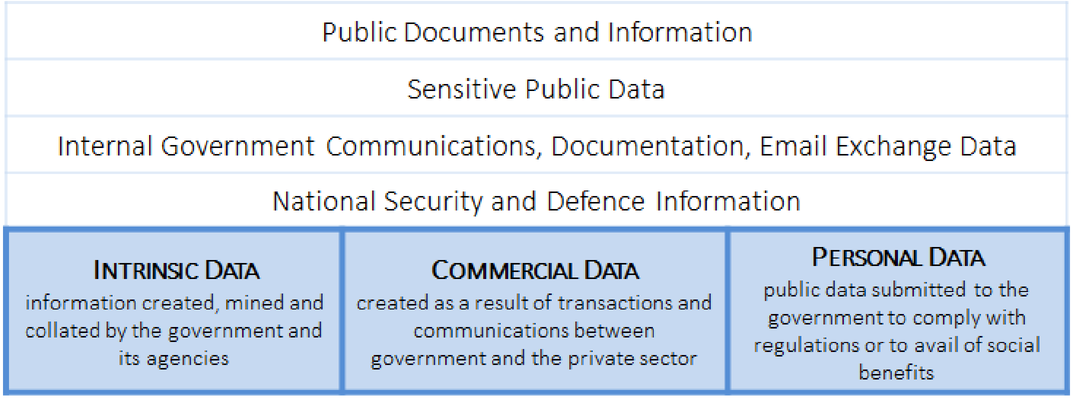
CHAPTER 2: TYPES OF INFORMATION STORED BY GOVERNMENTS ON IT SYSTEMS

Governments collect a variety of data:

1. **intrinsic data** – information created, mined and collated by the government and its agencies;
2. **commercial data** – created as a result of transactions and communications between government and the private sector;
3. **personal data** – public data submitted to the government to comply with regulations or to avail of social benefits.

Most data is now processed and stored by governments in a variety of electronic systems. Depending on the security classification of the information, the data is stored with limited or restricted access, put on an open network, or into the cloud for sharing. Access to data that does not need to be secured and can be shared, is either provided for a fee or for free.

Figure 3: Types of Data Stored on Government Systems



Public Documents and Information

Sensitive Public Data

Internal Government Communications, Documentation, Email Exchange Data

National Security and Defence Information

INTRINSIC DATA	COMMERCIAL DATA	PERSONAL DATA
information created, mined and collated by the government and its agencies	created as a result of transactions and communications between government and the private sector	public data submitted to the government to comply with regulations or to avail of social benefits

Public Documents and Information

Government servers hold and control a large repository of digitized information about their citizenry, and country operations. Large swathes of data previously held in physical file cabinets have been digitized thanks to concerted moves into e-government in the 1990s and 2000s. However, the type of data, levels of access, and accuracy of the information differs from country to country.

Governments have increasingly made large amounts of this information available to the public at no (or nominal) cost. Such information is often classified as a public good, and information is made available as a matter of public record. Examples include databases for:

- National Acts, Bills and other legislation – e.g. New Zealand Legislation (www.legislation.govt.nz)
- Public library books and documents – e.g. Singapore's National Library Board (www.nlb.gov.sg)
- Crime statistics – e.g. USA's FBI Crime Statistics Database (www.fbi.gov/about-us/cjis/ucr/ucr)

- Government online procurement systems – e.g. Singapore's GeBiz system (www.gebiz.gov.sg)

However, the increasing connectedness of government agencies and the huge volume of document production have made them targets for attack and information theft. In 2012, a number of government entities from the Ukraine, Belgium, Portugal, Romania, the Czech Republic and Ireland were compromised by the 'MiniDuke' attacks that used exploited PDF documents.[6] The PDFs, of "highly relevant-looking government documents" and including "well-crafted content" fabricating human rights and foreign policy information, would deposit a small piece of malware on the owner's computer that could later be activated by outside attackers, when opened. Similarly, a cyber-attack that compromised more than 3,000 official documents from Japan's ministries used a malware program to acquire and transmit the information by targeting PDFs.[7]

Box 2: WikiLeaks and the Snowden Revelations

WikiLeaks.org is a website registered by Australian Julian Assange in 1999. It begun to be actively run in 2006 as an "uncensorable system for untraceable mass document leaking and public analysis." Through partnership with several media agencies, – most notably the Guardian newspaper – highly confidential government documents were reported on and published. This included documents that the government considered highly damaging to national security.

The first major classified document leak to WikiLeaks was by Chelsea Manning (formerly known as Bradley Manning), a US Army soldier assigned to an Army unit in Iraq as an intelligence analyst. She has been sentenced to 35 years in prison for these offences.

In June 2013, Edward Snowden, a computer professional that had worked with the Central Intelligence Agency (CIA), the Defence Intelligence Agency (DIA) and the National Security Agency (NSA) released thousands of classified documents. His primary revelation was around global surveillance programs that were run by the NSA which included surveillance of phone, Internet and location records of private citizens. Several policymakers have called this the greatest setback to intelligence since World War 2.

Sensitive Public Data

Much of the public data held by government is sensitive. This can include names, birthdates, telephone numbers, tax numbers, national ID numbers, passport numbers, health/medical details, immigration records and the like.

Examples of e-government services which collate such information include:

1. National registration or voter registration records – e.g. Bangladesh's National Identity Card and Voter Registration (www.nidw.gov.bd)
2. Immigration, visa and travel applications – e.g. China's visa application for Hong Kong citizens (www.fmcoprc.gov.hk/eng/zgqz/)
3. E-Tax systems – e.g. Australia's e-Tax online (www.ato.gov.au)
4. Business licensing – e.g. USA's Washington State Business License online (www.bls.dor.wa.gov)

One of the key issues is that government data, which on its own can look fairly innocuous, can be pieced together across multiple databases to become deterministic, and to build identify profiles. The most common examples of sensitive data are those that are sensitive to individuals and corporations such as taxpayer information, social security information, medical records and even genetic information[8]. A government's list of sensitive data can also include information related to criminal investigations, financial resources and emergency preparedness.[9] This was brought into stark reality in April 2014 when the Heartbleed Bug was discovered. While it is not possible to trace the number of times that this bug was exploited for access to personal data, a few incidents demonstrate the severity of the situation. In Canada, for example, 900 Social Insurance Numbers were stolen from the Canada Revenue Agency during a 6-hour period by individual(s) exploiting the Heartbleed Bug vulnerability[10].

In Singapore, citizens use an online platform called SingPass to access about 340 government e-services. In another instance of unauthorised access of personal data, it was discovered, that over 1,500 SingPass accounts had been accessed fraudulently in 2014, and in some cases to forge government applications for work permits[11].

The level of security in processing and storing public sensitive data varies from country to country – and even within countries. Canada's Alberta province, for instance, requires all sensitive information to have authorized and authenticated access,[12] while North Carolina, in the US, states that sensitive data cannot be restricted unless legally declared closed.[13]

Internal Government Communication, Documentation and Email Exchange Data

Modern government communication channels have moved online, resulting in significant amounts of government internal communications now being stored in the form of email and messaging exchange data. A significant amount of government correspondence is confidential, restricted classified, or sometimes, simply embarrassing. In addition, Governments are in possession of vast amounts of documents such as slide decks, spreadsheets and others that contain sensitive internal data.

The amount of information collated and stored is growing exponentially and so too is the potential damage that can be wrought. When large amounts of private government correspondence are released by unauthorized sources – such as in the case of WikiLeaks or the Snowden NSA revelations – the repercussions can be highly damaging to governments involved.

> *When large amounts of private government correspondence are released by unauthorized sources – such as in the case of WikiLeaks or the Snowden NSA revelations – the repercussions can be highly damaging to governments involved.*

Such risks are being further compounded as more organisations, including governments, move into a Bring Your Own Device (BYOD) era along with a proliferation of devices that are used to access sensitive information including phones, tablets and increasingly other smart gadgets including watches and glasses. For a time, Blackberry was the most widely-used communication device for restricted information among governments. In 2012, the United Kingdom's Communications-Electronics Security Group (CESG) – its security arm – approved the use of iPhones to send and receive sensitive e-mails.[14]

However, following revelations that the NSA tried to spy on German Chancellor Angela Merkel's phone, security standards for mobile phones and tablets are increasing again. Blackberry currently produces the most secure phones, which are encrypted and sold only to government officials. To further complicate this situation, in the developing world, and particularly across Asia, a large number of government officials also use public e-mail addresses in official communication. At a 2012 conference of the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) in Bangkok, for example, officials from 20 of 33 Asian countries represented included Gmail, Hotmail or Yahoo addresses on their contact forms.[15]

One of the risks seen in the increasing adoption of governments of smartphones, tablets and other devices, involves application downloads. Juniper Research, for example, has warned: "App downloads are becoming an increasing security risk for corporate and government networks, as uncertified third-party applications can carry malware or spyware that can retrieve emails, messages, call history, client lists and other corporate data. Applications carrying malware can transform the device into a gateway for Trojans and viruses to enter the enterprise network or may cause data leakage or exposure."[16]

Box 3: Prominent cyber-attacks targeting high-level national security information in recent years

January 2011 – The Canadian government reported a major cyber-attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the Internet.

September 2012 – In the Philippines, prominent commercial entities, civil society organisations, and government websites were attacked in a widespread retaliatory protest against the contentious Cybercrime Act.

October 2012 - The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007. The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.

Jan 2013 – Hacker Group "Anonymous" defaced over 12 government websites.

April 2013 – The Pentagon in the US reported to Congress that the Chinese military had been mounting cyber-attacks on the US government and various defense contractors. This was deemed to be sufficient to draw a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited during a crisis. In July 2014 Chinese hackers accessed U.S. Office of Personnel Management networks and collected information on thousands of applicants for top secret clearances.

October 2013 – Hacker group "Anonymous," breached the websites of the PAP Community Foundation and the Ang Mo Kio Town Council in Singapore to express unhappiness about various incidents in the country. Later that month, two hackers hacked into the website of the Istana – the official residence and office of the President of Singapore – by exploiting a security vulnerability and injecting a malicious script into a web application.

National Security and Defence Information

"That's where the bad guys will go, there are no safe neighborhoods. All of us are neighbors [online][17]*.* James B. Comey, Head of the FBI in testimony to Congress on cyber-attacks, Capitol Hill, Washington November 14, 2013

The most sensitive government data is that which pertains to national security. This encompasses issues ranging from military intelligence, to civil defence and emergency/disaster preparedness, to the protection of critical infrastructure and troop deployment plans and movements.

To make matters more complex, much government information is shared with defence contractors, and other external parties. In more than one incident, cyber-attacks have been mounted against these external parties in order to access critical national security information.

Without exception, every government in Asia has now been subject to both strategic attacks and security breaches. This presents a critical security challenge to governments.

The private sector has not been immune either, and has had to deal with its own share of serious cyber-attacks. Target,[18] a major American retail store and Home Depot,[19] a Home Improvement store, have both been the victims of massive cyber-attacks that have compromised a combined estimated 100 million credit cards and debit cards.[20]

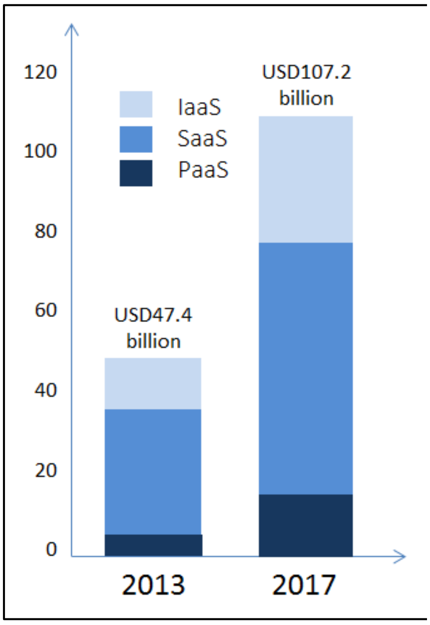
The more complicated the global supply chain of IT software becomes, the greater the potential for threats to emerge in the IT ecosystem and for vulnerabilities to become weak spots for cyber criminals to exploit. Cyber security measures taken by governments should focus on the cyber protection of the IT supply chain, and seek to include and engage public officers involved in the process of IT software procurement, in cyber security resilience measures.

CHAPTER 3: IT SPENDING BY GOVERNMENTS

According to IT research and advisory firm Gartner, government organizations worldwide will spend some USD449.5 billion on IT projects in 2013, down 0.1 percent from the previous year.[21] However, this projected slowdown has to be taken in context of previous spending: while the US, perennially the biggest spender, *has* slowed government IT expenditure in 2013, between 2001 and 2012 government IT spending by the US increased from USD46 billion to USD81 billion, almost doubling in the decade.[22]

Additionally, not all governments are slowing their IT spending. Australia's public sector IT spending, is expected to post a year-on-year growth of 2.2 percent, to reach AUD10.7 billion by 2017.[23] Most of these investments will be on software.[24] Neighbouring New Zealand is also expected to grow its spending by 1.4 percent to reach more than NZD1.6 billion.[25] The trending growth areas in public sector IT spending are seen in mobile technologies, IT modernisation and cloud computing.[26] Globally, spending on public cloud infrastructure is expected to reach nearly 108 billion by 2017.[27]

Figure 5: Worldwide Public IT Cloud Spending by Segment[28]



With government spending coming under increasing scrutiny, closer attention is being paid to where resources are being spent, especially multi-billion dollar IT budgets. Government recognition of the importance of cyber security efforts is reflected in the budgets that have been allocated in this area, with developed countries leading the way. In 2014, the US government Department of Defense budget included an unprecedented USD447 million for the US Cyber Command with an additional USD792 million for the Department of Homeland Security Cyber security team[29]. The UK government is spending GBP650 million between 2011 and 2015 on cyber security[30]. In comparison however, the Indian government budgeted just USD7.76 million for cyber security in 2013[31].

There is a growing understanding that some of these resources must be focused on cyber security issues, especially since state-sponsored and state-targeted cyber attacks have been projected to rise.[32] Thailand, for one, has sounded the alert, acknowledging that its cyber security state was in "crisis".[33] Similarly, cyber attacks on critical installations in Saudi Arabia and Qatar in 2012/2013 have been a wake-up call for the region. The UAE, Saudi Arabia and others in the region are moving towards investing significantly in cyber security.[34]

However, current government efforts to address cyber security to date seem to be piecemeal at best:

1. Singapore announced the set up of the Cyber Security Agency in April 2015. (http://www.channelnewsasia.com/news/singapore/government-to-set-up/1618658.html)

2. Indonesia officials were in discussions in Dec 2014 to set up a national body to fight cyber attacks on the country (http://www.futuregov.asia/articles/5924-indonesia-plans-to-set-up-national-cyber-security-agency)
3. Thailand is ratifying a controversial National Cyber Security Bill in Jan 2015 (http://tech.thaivisa.com/gen-prayut-defends-controversial-new-cyber-laws-thailand/3438/)
4. India published its first ever National Cyber Security Policy in July 2013 (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf)
5. Australian Prime Minister announced cyber security plans within a larger National Security Strategy in Jan 2013: (www.abc.net.au/unleashed/4484508.html)

Beyond specific spending on cyber security protection measures, the hygiene of government procurement is an overlooked factor in developing a robust cyber secure government. The components of cyber security spend - IT infrastructure and procurement, IT administration and support, website and online services maintenance – are often vulnerable to cyber security bypass and loopholes, such as using unlicensed or lapsed-license software, purchasing from questionable vendors, and using outdated software - quite often without knowing. These security loopholes can be addressed by ensuring that best practices guidelines are enforced for the purchase, maintenance, and upgrading of IT infrastructure and services.

Two problems arise for procurement professionals in Asia – the rise of infected computers and the lack of experience in dealing with actual threats… (and) most organisations… are not taking enough precautions against the threat of an Advanced Persistent Threat (APT) attack.

IT Infrastructure and Procurement

Productivity, sustainability and cost-efficiency are the three key components of IT infrastructure procurement, particularly in countries with large IT projects.[35] However, preparedness is becoming increasingly important for IT security. By 2020, 75 percent of IT budgets are projected to be set aside for rapid detection and response approaches – up from less than 10 percent in 2012.[36] Two problems arise for procurement professionals in Asia – the rise of infected computers and the lack of experience in dealing with actual threats.

More disturbingly, a global survey by security firm ISACA found that most security professionals have not yet had to deal with an actual Advanced Persistent Threat (APT) attack, with only 21.6 percent of respondents having been subject to an APT attack.[37] Most organisations, however, are not taking enough precautions against the threat of an APT. Up to 81.8 percent of respondents have not updated their agreements with vendors who provide protection against APT, and some 67.3 percent of respondents have not held any APT awareness training programmes for employees.

Box 4: Cloud and Security

A number of governments have made the decision to move into cloud, such as the USA, UK, and Australia -- three countries which have an articulated "Cloud First" policy, where cloud computing products will be considered first where purchases of IT products and services are required by the government.

Cloud has been deemed more secure than on-premise computing solutions for a number of reasons:

1. Identity and Access Management - this allows better management of who has access to what data, and allows for contact tracing as well, in case of a security breach.
2. Physical security - going on cloud provides better data protection and recovery controls put in place by cloud vendors, instead of having to do it by yourself.
3. Up-to-date security and maintenance - moving onto cloud also means that security experts will be performing regular maintenance and security hygiene tasks as part of the service.

IT Administration and Support

Some USD400 billion will be spent globally on remedial IT work and losses from data breaches – money that could be better spent far more productively if channelled into constructive development. To business and government the technical cost of malware is vast. With attacks against small businesses in the UK up by 10 percent in 2013, the costs are estimated to be up to 6 percent of their turnover.[38] Almost 60 percent of small businesses experienced staff-related security breaches. Overall, security breaches cost between USD54 million and USD100 million to small business in the UK. It is estimated that over 800 million individuals were impacted by data theft and cyber espionage in 2013.[39]

Website and Online Services Maintenance

In any jurisdiction, the government is likely to have the most number of citizen-facing websites. Upgrades and the need to constantly check for security lapses entail considerable expense. One solution is to consolidate many such sites and services into a single portal. The UK government, for example, claims to have saved some £42 million, having moved various sites to the single portal Gov.uk. Prior to this initiative, a Digital Britain report showed that the country had about 4,000 citizen-facing websites.[40]

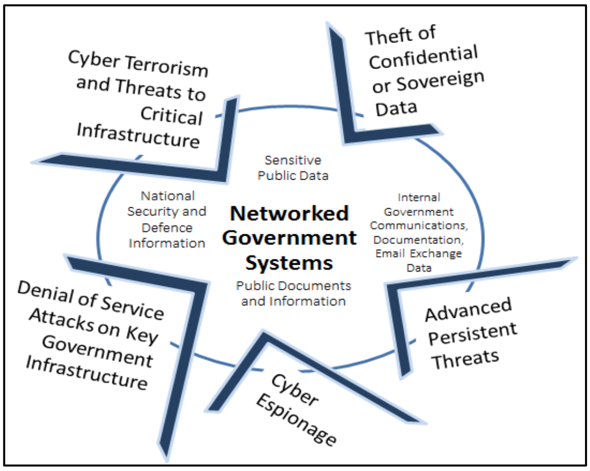
In India, where there are more than 303 million government websites, an overwhelming number are hacked every year and the hacking incidents have been increasing each year since 2010, according to the government. The preventive action imposed by the government is to have a “proper audit of all new government websites and applications in respect of cyber security prior to their hosting.”[41] Updating software and using known providers will mitigate security problems, but the scale and cost of dealing with breaches will grow by the year.

CHAPTER 4: TYPES OF CYBER SECURITY THREATS TO GOVERNMENT

The numerous and different types of data and interconnected data systems are bringing forth an increasing array of security threats lurking in malicious code, malware and unwanted software such as viruses, Trojans, keystroke-capturing software, authentication backdoors, and spyware contained in pirated software, websites and peer-to-peer (P2P) networks.

For most people, the repercussions of such infections or intrusions are a slower computer, annoying pop-up ads and, potentially, identity theft. For governments and enterprises, however, the consequences can be far more serious. The use of pirated or counterfeit software exposes government agencies to hacking, cyber espionage, and cyber terrorism. Using malware, hackers can take control of critical infrastructure and sensitive data.

Figure 6: Cyber Security Threats to Government



Cyber Terrorism and Threats to Critical Infrastructure
Theft of Confidential or Sovereign Data
Sensitive Public Data
National Security and Defence Information
Networked Government Systems
Internal Government Communications, Documentation, Email Exchange Data
Public Documents and Information
Denial of Service Attacks on Key Government Infrastructure
Advanced Persistent Threats
Cyber Espionage

Cyber Terrorism and Threats to Critical Infrastructure

Cyber terrorism includes attacks and threats of attack against computer networks with the intent to cause damage to critical infrastructure such as defence and aviation infrastructure, electricity and other public utility networks or the energy sector such as nuclear or oil and gas infrastructure amongst others. It can also include attacks and threats of attack against computer networks that target the population at large, causing widespread panic, financial loss or compromised safety.

Software and malware used in cyber terrorism is growing increasingly sophisticated (See Box 3), and most governments are bracing themselves for the next high-impact attack. A Californian water provider, for example, found that a computer hacker group was able to seize control of the water provider's systems and add chemical treatment to the state's water supply.

It is within this context that the Stuxnet worm designed to attack electromechanical processes was widely seen to be a game changer in cyber-attacks. Discovered in 2010, Kaspersky Labs labelled it as "a working and fearsome prototype of a cyber weapon that will lead to the creation of a new arms race in the world."[42] The Stuxnet worm is reported to have destroyed a fifth of Iran's nuclear centrifuges by causing them to spin out of control[43].

Theft of Confidential or Sovereign Data

The objectives of most cyber-attacks are to obtain confidential information, steal trade secrets or gain competitive advantages of one sort or another over companies, organizations, or state governments. Over recent years the incidence of data theft has grown enormously and few organisations are now able to comprehensively protect themselves from its reach.[44] A small sampling of some of the more high profile cases in 2011-14 shows the breadth of hacker access: retailers (Amazon's Zappos), marketing firms (Epsilon), online gaming (Sony), banks (Citigroup), government departments.

(Pentagon, Canadian government), defense contractors (Lockheed Martin), social networking sites (RockYou), cloud providers (Google's Gmail) and even sophisticated security firms (EMC's RSA, Stratfor, Symantec). In a recent case, a single malicious email sent to workers at the South Carolina Department of Revenue, led to the theft of 1.9 million Social Security numbers, 3.8 million tax returns and bank account details for 3.3 million people across the state.[45]

A cyber-attack on e-Commerce giant, eBay in 2014 resulted in information such as email addresses, encrypted passwords, birth dates and mailing addresses being stolen. eBay asked its 145 million users around the world to change their passwords following this attack[46]. In September of the same year Home Depot, a home improvement retailer reported a cyber-attack on the company's payment systems that put over 56 million customer credit and debit cards at risk.

The number and type of information security breaches that are affecting businesses of all types was shown in 2012 to be so extensive that small and mid-sized organisations are now experiencing the kinds of security breaches that were previously experienced only by larger organisations, with 87 percent of UK small businesses, for example, experiencing a security breach in 2012.[47]

Denial of Service Attacks on Key Government Infrastructure

A Denial of Service (DoS) attack is an attempt to make a service or machine inaccessible. Stealing information and using it to gain access to various computers or hacking into a network system are the first steps in a DoS attack. Using the computers accessed to then target a potential site and overwhelm it through repeated requests or by swamping its bandwidth, either crashes the system or keeps other users from being able to access the target.

This can be automated and scaled through distributed DoS (DDoS) attacks, which make use of botnets, software used to take control of many computers at once. Such botnets do not require any advanced computer skills, as they can be purchased for as little as USD100–200 per 1000 computers infected. DoS attacks are on the rise with government and financial IT systems being the favoured targets. One study reported an eight-fold increase in 2013 alone as compared to the previous year[48].

These attacks took on a whole new relevance with the assaults launched in 2007 and 2008 against Estonia and Georgia respectively. The attack on Estonia in April 2007 brought down Parliamentary websites and stalled government and banking services, with networks taken offline, and media and government disrupted by several waves of DoS attacks.[49] In a country where 90 percent of all financial transactions are conducted over the internet, and 70 percent of tax returns are filed electronically, the effect was crippling. Another example was the DoS counter attacks at the height of the tension between the Philippines and Taiwan in early 2013. Following the killing of a Taiwanese fisherman, Taiwanese "hacktivists" launched massive DoS attacks, imperilling Philippine government web sites and directly damaging the economy.[50]

Among the growing threats by DoS attacks are the potential applications with smarter technology and the arrival of the "internet of things" where more IP-enabled devices could be turned into botnets or other platforms used for distributed attacks.[51] A new threat is probes that look for ways to seize control of processing systems.[52]

Of particular concern these days are attacks on Supervisory Control and Data Acquisition (SCADA) systems, popular tools for controlling government equipment, facilities and infrastructure. A SCADA in Queensland, Australia, for example, fell victim to hacking, resulting in "sewage flooding a park and flowing hundreds of metres to a tidal canal."[53]

Box 5: Cyber Security Masterplans and Laws in Asia

A number of countries in Asia have existing cybersecurity plans in place, or have cyber security laws in place, with some in review:

Indonesia is establishing an agency to lead campaign against cyber attacks. The project was mooted by Communications and Information Minister Rudiantara and Coordinating Political, Legal and Security Affairs Minister Tedjo Edhy Purdijatno on Jan 2015. Relevant laws: the Electronic Information and Transaction Act.[54]

Malaysia has its National Cyber Security Policy, formulated in 2005 and coordinated through the Ministry of Science, Technology and Innovation (MOSTI). CyberSecurity Malaysia was launched in Aug 2007. GCERT MAMPU was also founded in 2001 by the Government ICT Security Policy framework to ensure continuity of government ICT arrangements, and has relationships with 55 other CERT agencies. Relevant laws: The Communications and Multimedia Act 1998, the Personal Data Protection Act 2010, the Computer Crimes Act 1997[55]

Myanmar's Computer Emergency Response Team (MMCERT) and the Myanmar Computer Federation (MCF) are working to reform Myanmar's CERT, to improve the country's cybersecurity. A US-Myanmar ICT Council in collaboration with USAID has also been created, and is working on a National Plan for Myanmar.[56]

In the Philippines, the National Cyber Security Office oversees the implementation of the Cyber Security Plan 2008. Relevant laws: the Cybercrime Prevention Act of 2012 (RA 10175 - repealed until further notice), the Data Privacy Act of 2012 (RA 10173), Electronic Commerce Act of 2000 (RA 8792).[57]

Singapore has a long history of cyber security masterplans: the Infocomm Security Masterplan I (2005-2007), II (2008-2012), National Cybersecurity Masterplan 2018 (NCSM2018). Relevant laws: the Computer Misuse and Cybersecurity Act, the Electronic Transactions Act, the Personal Data Protection Act. Cyber security is being coordinated by the National Security Coordination Secretariat under the Prime Minister's Office. [58]

As Thailand's political situation is still in flux, work reviewing its Computer Related Crime Act BE 2550 of 2007 has stalled for the moment. Relevant laws: The Consumer Protection Act 2002, the Penal Code of Thailand Section 269/1-7, The electronic transaction Act 2001, The Civil and Commercial Code, the Credit Information Business Act, and the Personal Information Protection Act (draft).

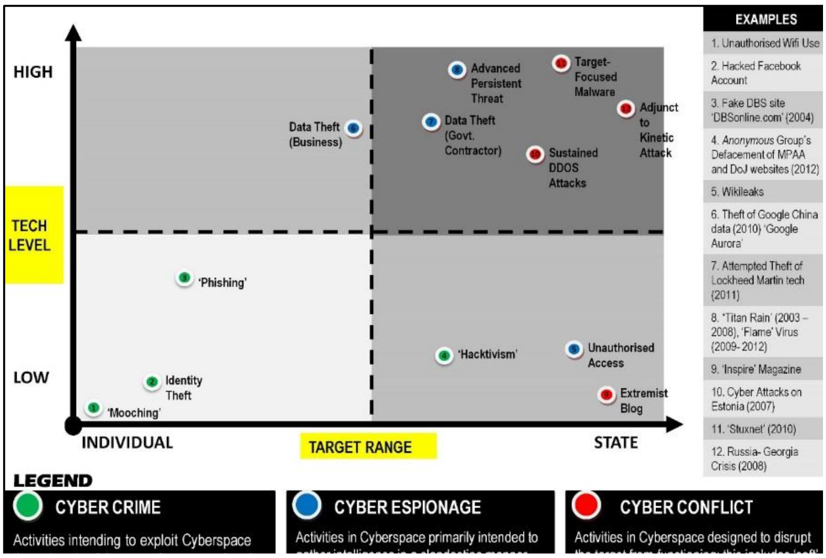
Vietnam is currently setting up a National Centre for Network Technology, and has three relevant laws to cybersecurity: the Law on Telecommunications, Law of Information Technology, Law on Electronic Transactions.

Cyber Espionage

Cyber Espionage or cyber spying is the stealing of secrets stored in digital formats or on computers or networks[59]. Cyber espionage attacks employ both low-tech and sophisticated means, and include a range of information stealing from individuals' data, to state-level secrets (Fig. 2). In 2013, a California-based cyber security firm said Chinese hackers had launched cyber-attacks on 141 organisations across 20 industries. Targets included a range of government departments, private companies, from the Pentagon to the New York Times. This led to an indictment in the US against five Chinese military hackers believed to be behind the theft of commercial secrets.

In another example of cyber espionage, the government of Finland reported that they were a victim of a long cyber espionage campaign that gained access to foreign policy documents. These documents are believed to have compromised Finland's position in international negotiations[60].

Figure 7: Cyber security and Espionage Threats to Individuals and Governments


HIGH
TECH LEVEL
LOW
INDIVIDUAL
TARGET RANGE
STATE
Data Theft (Business)
Advanced Persistent Threat
Target-Focused Malware
Data Theft (Govt. Contractor)
Adjunct to Kinetic Attack
Sustained DDOS Attacks
'Phishing'
'Hacktivism'
Unauthorised Access
Identity Theft
Extremist Blog
'Mooching'
EXAMPLES
1. Unauthorised Wifi Use
2. Hacked Facebook Account
3. Fake DBS site 'DBSonline.com' (2004)
4. Anonymous Group's Defacement of MPAA and DoJ websites (2012)
5. Wikileaks
6. Theft of Google China data (2010) 'Google Aurora'
7. Attempted Theft of Lockheed Martin tech (2011)
8. 'Titan Rain' (2003 – 2008), 'Flame' Virus (2009-2012)
9. 'Inspire' Magazine
10. Cyber Attacks on Estonia (2007)
11. 'Stuxnet' (2010)
12. Russia- Georgia Crisis (2008)
LEGEND
CYBER CRIME
Activities intending to exploit Cyberspace
CYBER ESPIONAGE
Activities in Cyberspace primarily intended to
CYBER CONFLICT
Activities in Cyberspace designed to disrupt

Advanced Persistent Threats

Advanced Persistent Threats (APT) are a new class of threat, that is often focused on the theft of intellectual property. As its name suggests, APTs are targeted, persistent, evasive and advanced[61].

A survey by IT Governance NGO, ISACA, found that 67.6 percent of security professionals surveyed were familiar with what APTs were and saw them as a serious threat to national security and economic stability, but 53.4 percent believed them to be similar to traditional threats.62 The malicious NetTraveler family of surveillance programs had been active since 2004, but its highest volume of activity wasn't until 2010-13. At that time, NetTraveler was used by APT actors to successfully compromise more than 350 high-profile computer systems across 40 countries. In 2010, Google reported that it, along with a few dozen other companies had been the victim of an APT attack. This attack which originated in China had resulted in the theft of intellectual property from Google.

Box 6: Malware

Malware is software intended to damage or disable computers and computer systems often found on counterfeit or pirated software. These programs create opportunities for hackers by loading malicious code onto computers to gain information and sometimes take control over computers. Common malware types include:

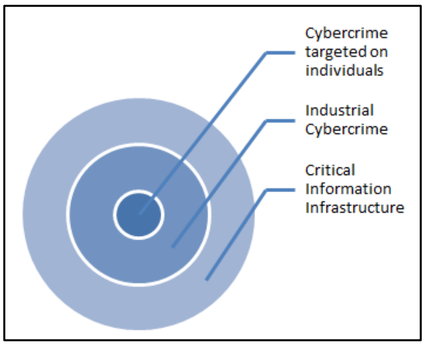
- Spyware: software that self-installs on a computer, enabling information to be gathered covertly about a person's Internet use, passwords, etc. The iBryte spyware program, for example, can track Web browsing habits, gather personal information, and transmit the information to remote attackers.
- Tracking Cookies: text files that a Web browser stores on a user’s machine and that is used to track a user’s activity online.
- Adware: any software package which automatically renders advertisements in order to generate revenue for its author.
- Trojan: a program in which malicious or harmful code is contained inside apparently harmless programming or data.
- Virus: a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer
- Keylogger: a program that records the keystrokes on a computer. That information can include passwords and written reports to be stored and received at a later date. Key logging doesn’t require specialized computer knowledge; a decent keylogging program can cost as little as $25, and can easily be included in unlicensed software packages.

Malware production is now reaching industrial levels with about 250,000 new pieces of malware created and 30,000 websites infected every day. The US government now ranks cyber security risks higher than terrorist attacks; such is the heightened vigilance against co-ordinated and organised cyber threats.

CHAPTER 5: ROADMAP TO CREATING A CYBER SECURITY STRATEGY

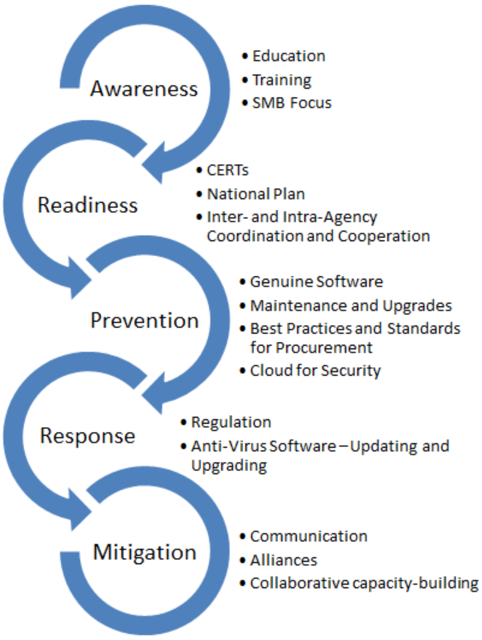
All societies – and governments – are vulnerable to attack in the cyberspace due to the growing interconnectedness of networks, 'internet of things' such as machines, sensors, e-commerce, and explosion of data through multitude of internet connected devices.

Figure 8: Cyber Threat Targets


Cybercrime targeted on individuals
Industrial Cybercrime
Critical Information Infrastructure

Vulnerabilities exist at all levels. For analysis it is useful to think of three levels: (i) high-level attacks on critical information infrastructure which can bring parts of a country to a standstill and are likely to come from terrorist assault or political cyber warfare; (ii) cybercrime which can range from industrial scale espionage, to commercial theft and fraud; and, (iii) attacks against individuals such as financial fraud and identity theft.

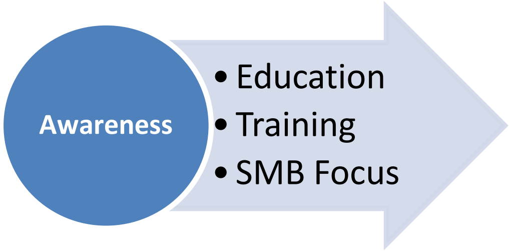
Figure 9: Components of a Robust Cyber Security Policy


Awareness
• Education
• Training
• SMB Focus
Readiness
• CERTs
• National Plan
• Inter- and Intra-Agency Coordination and Cooperation
Prevention
• Genuine Software
• Maintenance and Upgrades
• Best Practices and Standards for Procurement
• Cloud for Security
Response
• Regulation
• Anti-Virus Software – Updating and Upgrading
Mitigation
• Communication
• Alliances
• Collaborative capacity-building

Solutions and responses to cyber threats need to be holistic and should address different scenarios in developing a robust cybersecurity strategy. This section outlines a five-step roadmap to strengthen the preparedness, vigilance, responsiveness and recovery when faced with the inevitability of cyber threats and attacks. Much of existing cyber security planning has been focused on the areas of preparing for and responding to a cyber-attack. This paper advocates for adopting a strong "before, during and after" strategy, as it is important for all levels of governments – from the IT supply procurement, to software maintenance and upgrading, to the CERT teams etc – to be aware and well-positioned to defend their infrastructure and populations against one of the most dangerous threats in the modern world.

Proportionality, the paper aims to provide a good guide to addressing such issues: i.e. identifying the vulnerabilities and assigning levels of significance and levels of risk. Higher significance means more likely to be targeted (risk type 1) but not necessarily easier to attack (risk type 2). Lower level priority targets may be the most attacked because they are easier to attack. Strategy also needs to consider the range of cybercrimes committed by different set of criminal organizations: industrial espionage has its own priorities and methods; terrorists and states will go for high-value (infrastructure) or high-publicity (e-government) targets where the critical infrastructure targets are a key priority for any national security effort.

Awareness and Public Education



The responsibility of maintaining safe and secure Internet and networks rests with all segments of society, and it is important that all users of ICT play their part in the defence against cyber threats and cyber-attacks. It is through cooperation between government, consumers, small- and medium-sized businesses (SMBs), enterprises, contractors, security vendors, IT industry and the cybersecurity research community that networks and devices can be resilient enough against threats and attacks.

While cybercrime involves the use of ICT, many of the real issues concern the vulnerabilities of organizations, IT systems and the human factor, including Internet usage practices, IT/software procurement, BYOD programs, and IT preferences. Cybersecurity solutions/frameworks that do not embrace these issues comprehensively will struggle to successfully reduce the cybercrime risk vectors.

In order to do this, governments should launch and fund programs to raise awareness among all stakeholders on cyber-security, IT practices and risk management, particularly within government organization across the nation, to the state and district levels. Particular focus should be on raising awareness around the use of legal, genuine, up-to-date & current software products & applications, safer internet practices, and added malware protection through anti-virus solutions. In particular SMBs are easy victims of cybercrime due to lack of focus on cybersecurity and poor IT hygiene.

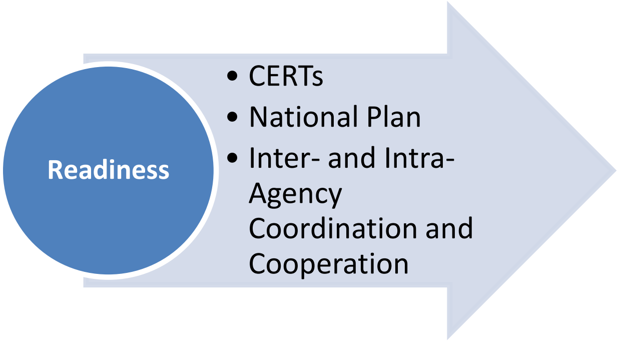
Government IT procurement officers and contractors that work with government agencies should also be strictly regulated, audited and sensitized towards the standards of security and safety, that will mitigate the likelihood of malware and other security threats entering through IT supply chain and compromising government networks and the public data. Best practices for procuring, maintaining and upgrading genuine software should also be put in place and regularly audited to reduce the security risk arising from an unclean and non-genuine IT procurement supply chain.

Recommendations:

- ✓ Have a cyber-wellness programme in place for citizens, larger businesses, and SMBs.
- ✓ Provide regular training on cyber-hygiene to government departments and usage of anti-virus solutions.
- ✓ Have a strong IT vendor audit practices to ensure reliable and clean IT supply chain involvement of procurement of genuine and upgraded software
- ✓ Review Government cybersecurity awareness programs regularly to refresh and provide periodic trainings
- ✓ Review and input to school & college curriculum, ensuring a basic level of cyber literacy and cyber-protection of the students online.

Schools and universities should develop curriculums that integrate ICT use and cyber security into courses as an important step in educating children and young adults in using ICT responsibly and safely. Alongside this, individuals operating ICT systems both in the public and private sector should be given expert training on managing the risks associated with their jobs. The Austrian cyber security strategy of 2013, for example, includes the “Human Sensor Programme,” which calls for the training of ICT system administrators to enable them to recognise cyber incidents’, to detect anomalies in their ICT systems and to report them to their security officers.

Readiness – Crisis Management Plan



Readiness

- CERTs
- National Plan
- Inter- and Intra-Agency Coordination and Cooperation

It is important for government agencies to work in close collaboration and exchange information, first at the national level, and second at the regional and international levels. Ministries and regulators need to be part of a national cyber strategy planning process. For example, the Ministry of Information and Communications in Mauritius with support from the African Development Bank has developed a holistic approach to cyber security with a National Strategic Plan that was created for 2007-2011 and has been revised for 2011-2014.[63] This follows the creation of Police Cybercrime Unit in 2000 and a Computer Emergency Response Team (CERT) in 2008. The Plan transparently identifies areas of cyber security that need strengthening, which is the first step towards reducing risk. It also outlines the coordinating mechanisms required between agencies.

The creation of CERTs is an important step and follows best practice for many countries. It is important that these teams integrate knowledge and expertise from different agencies and branches of government. Key elements include ensuring effective sharing of information/intelligence and coordinated response capabilities. For example, US-CERT is the 24x7 operational arm of the Department of Homeland Security.[64] In East Africa, the Cyber security Taskforce of the East African Communications Organizations (EACO) covering Burundi, Kenya, Rwanda, Tanzania and Uganda was formed in 2008. It is tasked with setting up national CERTS in each member state.

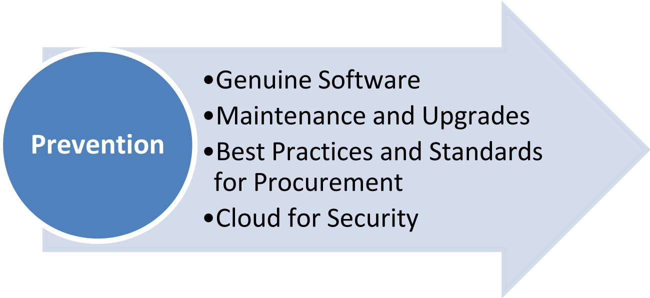
Recommendations:

- ✓ Have a national plan for cyber security in place aligning all government stakeholders.
- ✓ Have an agency responsible for coordinating cyber security preparedness and prevention protocols.
- ✓ Have a single agency responsible for coordinating cyber security responses in the event of a state-targeted attack.
- ✓ Establish a Computer Emergency Response Team (CERT).
- ✓ Create or join a network of CERT partners to share information/intelligence, and to work with in mobilisation and mock attack exercises.
- ✓ Identify, meet with and connect critical infrastructure providers (utilities such as power, water, networks) with each other, so as to enable smooth communications and quick responses during a cyber-attack.

National expertise in cybercrime issues may reside in several different departments and law enforcement agencies and in private IT, security firms, and telecom companies. It is therefore important that national strategic plans optimize ways to share information and cyber-threat intelligence on a timely basis.

Prevention – Safe and Protected Network Infrastructure

Many attacks can be prevented by following practices such as installing firewalls, being attentive to security updates, monitoring enterprise end-user software installations, using up-to-date anti-malware tools, and adhering to good security practices and IT policies. Techniques such as application whitelisting, where only trusted programs are enabled, and browser security can also help. But the best prevention is simply to use genuine, current and up-to-date software. This means procuring computers and software from trusted sources, ensure legal software usage, and following activation and registration protocols to benefit from IT support.



Prevention

- Genuine Software
- Maintenance and Upgrades
- Best Practices and Standards for Procurement
- Cloud for Security

Poor procurement practices can bring unsolicited malware or outdated software into the system which can in turn lead to security breaches. For governments pirated and unsolicited software can be unwittingly sourced through suppliers or distributors, given how complex global supply chains have become, causing network, website, or computer outages – or worse. One way of dealing with this is through establishing minimum standards of security that contractors and other businesses that work with the government need to adhere to. The UK government has instituted a "cyber kite mark" security standard based on the ISO27001:2005 certification that businesses need to attain in order to bid for government contracts. The National Cyber security Strategy of India includes the encouragement of us of valid and certified IT products, and mandates secure application and software development that is based on global best practices.

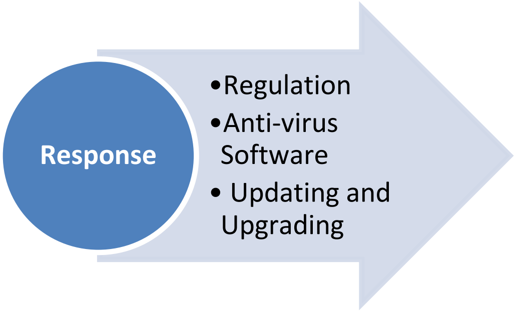
According to BSA, if counterfeit software is used, then malware will be encountered a third of the time on average. Given piracy rates, that means that installing one in nine PC software packages within government entails an encounter with malware. Once again, however, much of this can be addressed through simple yet rigorous processes: research has shown that only 5 percent of PCs running Windows do so with all updates installed, that at least 40 percent of users don't always update their systems, even when prompted, and 25 percent skip the updates altogether. Government agencies are not doing themselves any favours when it can be shown that 10 percent of IT managers and CIOs have disabled the programs that provide automatic updates, and that some 33 percent don't audit end-user PCs for user-installed software.

Recommendations:

- ✓ Have a procurement policy (e.g. whitelisting) for authentic software and malware protection in place for government procurement.
- ✓ Develop best practices for procurement in place for the private sector, for ISPs, larger businesses and SMEs.
- ✓ Develop, implement and enforce cybersecurity standards for IT vendors and suppliers for all public sector and sensitive national projects.
- ✓ Consider the use of cloud computing for best cyber security.

There are significant economic advantages in licensed software. Increasing the amount of licensed software used in the Asia Pacific by 1 percent would add USD18.7 billion to the regional economy, compared to USD6 billion from pirated software, a not insignificant $12.7 billion difference. Increasing licensed software use globally by 1 percent would inject an estimated USD73 billion into the world economy, compared to $20 billion from pirated software — a difference of USD53 billion.

Response – Regulation and Defence



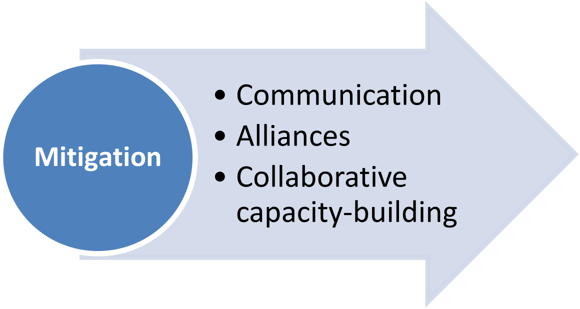
In spite of having the best preventions in place, the vulnerability to cyber-attacks remain a reality. CERTs in particular are the frontline force with the capacity to react and defend networks and infrastructure against damage. In order to ensure a high capability for response, the various defence actors should be subject to regular drills, joint exercises and simulations that test their ability to respond to the latest global threats.

Correspondingly, a legal platform should be established to empower the government and other actors to prosecute and seek redress from cyber security attacks. Regulation should ensure a balance between incentives and sanctions in order to adequately respond to and deal with attacks and threats when they happen.

Finally, software that is capable of fighting viruses and other security breaches should be used, installed and updated. The UK Government's Cyber security Strategy, for example, identified that most common cyber incidents could be prevented by simple 'cyber hygiene', estimating that more than 80 percent of currently successful attacks could be defeated by simple best practice, such as updating anti-virus software regularly.

Recommendations:
- ✓ Establish domestic, regional and international legal avenues for pursuing redress following a cyber-attack.
- ✓ Develop best practices for recommended timeframes and standards for constant upgrading and updating software used in the public sector.

Mitigation – Controlling the effects of a Security Breach



The economic and social impact that a successful cyber-attack could have is potentially devastating. In such an event, it is important that decisive measures are taken to restore confidence and re-build a secure infrastructure so as to mitigate the medium to long-term fall out of an attack. For example, an attack on a national airline carrier could erode public trust in the use of the airline for years which could severely cripple the industry. An effective crisis management and crisis communication strategy focused on rebuilding trust and giving assurance of redress measures is a critical component of this.

Internally, governments should have established procedures for investigation, evaluation and consultation in order to identify and investigate systemic weaknesses and restore confidence. Feedback should be sought, both from the general public as well as partners to determine if the procedures in place are sufficient and improve the overall management of cyber threats and attacks.

Recommendations:

- ✓ Establish a cyberforensics team in place which can work alongside the CERT, private industry & police to investigate security breaches.
- ✓ Develop or join a cybersecurity network of other government or international organisations for information, intelligence, and alliance-building purposes.

Given the global nature of cyber threats and attacks, partnerships with other governments and international organisations can be a valuable channel for sharing of information and building alliances to defend against occurrences in the future. Dialogue platforms such as the Japan-US Cyber Dialogue are very valuable for sharing best practices, case studies and guidelines that benefit from shared experiences and expertise.

Cyber Security Checklist for Governments

What should governments consider or focus on when building a cybersecurity plan?

✓*Awareness and Public Education*

- Have a cyber-wellness programme in place for consumers, enterprises and SMBs. Review Government cybersecurity awareness programs regularly to refresh and provide periodic trainings
- Provide regular training on cyber hygiene to government officers and staff and mandate usage of genuine & current software products, safer internet practices, and added malware protection through anti-virus solutions.
- Government IT procurement officers and government contractors and agencies should be strictly regulated, audited and sensitized towards the standards of security and safety of public data and national security
- Review and input to school & college curriculums about online safety, ensuring a basic level of cyber literacy and cyber protection for students.

✓*Readiness – Crisis Management Plan*

- Have an agency responsible for coordinating cybersecurity preparedness and prevention protocols.
- Have a single agency responsible for coordinating cyber security responses in the event of a state-targeted attack.
- Establish a strong and empowered Computer Emergency Response Team (CERT) and create or join a network of trusted CERT partners to share information and cyber-threat intelligence and mock attack exercises.
- Have a national plan in place for cybersecurity, aligning all government stakeholders – ICT, Law, Police, Science & Technology & Industry.
- Identify, meet with and connect critical infrastructure providers (utilities such as power, water, transportation, networks) with each other, so as to enable smooth communications and quick responses during a cyber-attack.

✓*Prevention – Safe and Protected Network Infrastructure*

- Have a secure government IT procurement policy for genuine and current software and trusted anti-virus solutions for malware protection.
- Develop best practices for procurement in place for the private sector, for ISPs, larger businesses and SMBs.
- Develop, implement and enforce cybersecurity standards for IT vendors and suppliers for all public sector and sensitive national projects.
- Consider the use of cloud computing for best cyber security.

✓*Response – Regulation and Defence*

- Establish domestic, regional and international legal avenues for pursuing redress following a cyber-attack.
- Develop best practices for recommended timeframes and standards for constant upgrading and updating software used in the public sector.

✓*Mitigation – Controlling the effects of a Security Breach*

- Establish a cyberforensics team in place which can work alongside the CERT, private industry and police to investigate security breaches.
- Develop or join a cyber-security network of other government or international organisations for information, intelligence and alliance-building purposes.

Conclusion

Despite the severity of cyber security attacks and the tremendous potential for damage to governments, critical infrastructure and governments, the resources that countries commit to building resilient cyber security architecture remains far behind what is spent on basic military or traditional defence. Hesitancy to ramp up spending and commitment of resources to this area will have a detrimental effect on a country's security and be a source of weakness within the larger defence strategy. This is further compounded by the fact that effective recovery from a cyber-attack will cost a country considerably more than putting the right measures in place to prevent one from happening in this first place. Further, this does not begin to take into account the non-quantifiable effects such as the erosion of trust in government and long terms impacts to society and industry.

Even within countries that are allocating increased levels of funding to cyber security, commitment levels still form only a fraction of very basic military and defence spending. As the online and networked world becomes a primary medium for government operation, industry and social interaction, there needs to be a convergence between policies and measures with the physical world.

Globally, Western industrialised countries currently lead the way in having a strategic cyber security strategy and even within this group, this has largely only emerged in the last 2-3 years[65]. Yet due to the global nature of cyber threats, Asian governments cannot afford to look to the West for solutions.

Addressing and mitigating government cyber threats are an imperative, and a robust cyber security policy must take a whole-of-government approach towards capacity-building. With the background provided by this white paper, government officials from all areas of the ICT supply chain will have a common understanding of the key threats the networked government faces. The paper also provides a cybersecurity roadmap and checklist by which public official can assess their institutional cyber security robustness, in order to identify which risk areas require attention and more resources.

REFERENCES

[1] www.dc.tw.ubm-us.com/i/149381/1

[2] United Nations E-Government Survey 2012, “E-Government for the People”, unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

[3] WASEDA – IAC 10th International E-Government Ranking 2014

[4] www.whitehouse.gov/sites/default/files/us_national_action_plan_final_2.pdf

[5] www.egress.com/local-central-government/

[6] http://bit.ly/1ovVd96

[7] http://japandailypress.com/malware-identified-in-hacking-incident-over-government-documents-0420850

[8] http://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information

[9] http://www.secureit.com/resources/WP_Data_Class_and_Protect.pdf

[10] http://globalnews.ca/news/1269168/900-sin-numbers-stolen-due-to-heartbleed-bug-canada-revenue-agency

[11] www.straitstimes.com/news/singapore/more-singapore-stories/story/three-breached-singpass-accounts-used-apply-fraudulent-w

[12] www.rimp.gov.ab.ca/publications/pdf/infosecurityclassification.pdf

[13] www.records.ncdcr.gov/erecords/faq.html

[14] www.computerweekly.com/news/2240170360/Departments-given-go-ahead-to-use-iPhones-for-sensitive-data

[15] www.thejakartaglobe.com/international/across-asia-officials-e-mails-may-be-vulnerable/

[16] www.computerweekly.com/news/2240170360/Departments-given-go-ahead-to-use-iPhones-for-sensitive-data

[17] www.rt.com/usa/fbi-cyber-attack-threat-739/

[18] http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219

[19] http://www.ft.com/intl/cms/s/0/7f9a2b26-3f74-11e4-984b-00144feabdc0.html#axzz3E2b6V9lG

[20] http://www.reuters.com/article/2014/09/18/us-home-depot-dataprotection-idUSKBN0HD2J420140918

[21] www.computerweekly.com/news/2240186339/Worldwide-government-IT-spending-to-remain-flat-in-2013-says-Gartner

[22] www.oversight.house.gov/release/video-why-the-waste-in-it-spending/

[23] www.itnews.com.au/News/347092,govt-it-spending-to-outrank-world-average.aspx

[24] http://www.computerweekly.com/news/2240186339/Worldwide-government-IT-spending-to-remain-flat-in-2013-says-Gartner

[25] http://cio.co.nz/cio.nsf/news/new-zealand-bucks-flat-government-it-spending-trend

[26] http://www.bloomberg.com/news/2013-06-18/gartner-revises-2013-government-it-spending-outlook-to-0-1-drop.html

[27] http://www.idc.com/getdoc.jsp?containerId=prUS24298013

[28] http://www.idc.com/getdoc.jsp?containerId=prUS24298013

[29] http://www.informationweek.com/government/cyber-security/budget-bill-boosts-cyber-security-spending/d/d-id/1113494

[30] http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

[31] http://thediplomat.com/2014/06/india-scrambles-on-cyber-security/

[32] http://www.govtech.com/security/Seven-Cyber-security-Predictions-for-2013.html

[33] http://www.zdnet.com/th/thailand-cyber-security-state-in-crisis-7000008126/

[34] http://www.defensenews.com/article/20140224/DEFREG04/302240015/UAE-Double-Security-Budget-Focus-Cyber

[35] http://ovum.com/2012/02/28/the-shape-of-uk-public-sector-procurement-in-2012/

[36] http://gcn.com/blogs/pulse/2013/06/gartner-mobile-big-data-advanced-targeted-attacks-shape-threat-landscape.aspx?admgarea=TC_SecCybersSec

[37] http://www.futuregov.asia/articles/2013/may/02/global-study-shows-low-understanding-new-security-/

[38] http://www.guardian.co.uk/media-network/media-network-blog/2013/jun/06/cost-security-breach-business

[39] http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html

[40] http://www.v3.co.uk/v3-uk/news/2272215/government-touts-gbp10bn-savings-as-it-spending-streamlined

[41] http://articles.timesofindia.indiatimes.com/2013-05-07/security/39089484_1_government-websites-cyber-security-nic

[42] www.kaspersky.com/news?id=207576183

[43] www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0

[44] www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/network-risk-insurance-privacy-security-exposures-and-solutions-for-law-firms.html

[45] http://investigations.nbcnews.com/_news/2012/11/20/15313720-one-email-exposes-millions-of-people-to-data-theft-in-south-carolina-cyberattack

[46] http://bgr.com/2014/05/27/ebay-hack-145-million-accounts-compromised/

[47] http://data.gov.uk/dataset/information-security-breaches-survey

[48] http://www.zdnet.com/ddos-attacks-rise-as-companies-fail-to-address-dns-security-7000025712/

[49] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[50] http://www.rappler.com/nation/29045-hackers-deface-philippine-government-sites-taiwan

[51] http://gcn.com/blogs/cybereye/2013/05/how-hackers-turn-internet-of-things-into-weapon.aspx

[52] http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all&_r=0

[53] http://www.theaustralian.com.au/australian-it/it-business/hackers-tap-into-local-essential-services/story-e6frganx-1226444141880

[54] http://www.thejakartapost.com/news/2015/01/07/govt-set-national-cyber-agency.html#sthash.f9OifJ51.dpuf

[55] http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp and http://asia.marsh.com/Portals/59/Documents/Cybercrime%20in%20Asia%20A%20Changing%20Regulatory%20Environment.pdf

[56] http://elevenmyanmar.com/index.php?option=com_content&view=article&id=3539:myanmar-to-reform-national-cyber-security-team&catid=44&Itemid=384 and http://photos.state.gov/libraries/burma/895/pdf/20141219USMyanmarICTCouncil.pdf

[57] https://www.itu.int/ITU-D/asp/CMS/Events/2010/NGN-Philippines/S5-Philippines_cybersecurity.pdf

[58] http://www.ida.gov.sg/Collaboration-and-Initiatives/Initiatives/Store/National-Cyber-Security-Masterplan-2018

[59] http://lexicon.ft.com/Term?term=cyber-espionage

[60] http://online.wsj.com/articles/finland-victim-of-long-term-cyberespionage-1404309676

[61] http://www.zdnet.com/microsoft-us-government-is-an-advanced-persistent-threat-7000024019/

[62] http://www.futuregov.asia/articles/2013/may/02/global-study-shows-low-understanding-new-security-/

[63] www.gov.mu/portal/goc/telecomit/file/ICTplan.pdf

[64] www.us-cert.gov/

[65] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

TRPC is a boutique consulting and research firm with over 25 years of experience in the telecommunications and ICT industries in the Asia-Pacific. We offer specialised advisory, research, and training services, with a focus on regulatory and strategic business issues, and possess an extensive network of industry experts and professionals throughout the region.

Our research focuses on the economics of telecommunications and information technology, and the policy and regulatory issues associated with national information infrastructure development, with an emphasis on the South-East and East Asian region. Our expertise encompasses both countries at with more developed ICT infrastructure (e.g. South Korea, Japan, and Hong Kong) to those with fast-growing and emerging ICT industries (e.g. Indonesia, Vietnam).

http://www.trpc.biz

TRPC wishes to thank Microsoft for funding support for the research necessary to conduct this study. Nevertheless, TRPC alone remains responsible for the accuracy of information and views expressed in this report, which do not necessarily represent the views of Microsoft.