Cybersecurity: Thailand’s and ASEAN’s priorities

Soranun Jiwasurat
www.etda.or.th
Cyber Threat Landscape Overview
Cyber threat

“a hostile act using computers, electronic information and/or digital networks to manipulate, steal, disrupt, deny, degrade or destroy systems, assets, information or functions”

Target

- Individual
- Critical Infrastructure
- Military System
- Government
Modern military systems are highly networked

Could degrade the effectiveness of fighting forces

GPS location could be manipulated or disrupted by expert hacker

In 2011, CIA multi-million dollar stealth drone was hijacked by hacking into GPS navigation and lost while flying on IRAN territory
In 2010, Sophisticated malware named Stuxnet infected Iran nuclear facility system, causing damage to centrifuges.

In October 2013, Cyberattack on Israel’s highway traffic control system, causing 8 hours shut down on a major tunnel.

Attack on critical infrastructure such as electrical power grid, financial systems, or transportation networks.

The attack could cause large parts of the country to lose power by overpowering transmission systems.

It may even include train derailments, bridge malfunctions, water supply contamination, etc…
DDoS

Important websites and internet-connected systems will be shut down.

Government, political, banks and major news papers' websites affected.

Attackers use computers to send tons of requests to the sites, thus overloading the server.

Attack originates from all across the globe.

Your infected computer with malware may be part of the attack.

In 2013, DDoS attack on Spamhaus, known as the world biggest cyber attack, caused the Spamhaus spam blacklist services became unreachable and congestion on Tier 1 Internet core.
Attack on Smartphone

Data in smartphones that keep large amount of your personal information are highly targeted.

User can be tricked to install application that may look normal but silently steal data.

Sensory capabilities that are built in devices such as GPS can give out user location, enabling more sophisticated attacks.

In December 2012, a banking Trojan attack campaign named Eurograbber that stole more than 36 million euro from more 30,000 customers of banks across Europe was discovered.
Trend and Preparation

Trend of Cyber Threats

- Cyber threats targeting country are already here
- It is increasing among countries and/or organizations over the past decade
- Nations are preparing against cyber threats which may come from terrorist, adversary country with different motivations
- Smaller countries with no military presence can resolve to this type of attacks to defeat its enemies

How We Can Prepare for Cyber Threats

- Develop state policies and actions against cyber threats
- Establish international agency for cybersecurity
- Support promotion of security awareness/training to the public
- Collaborate and exchange information with domestic and international bodies including private sector such as ISPs
- Create laws that support in fighting against various types of cyber threats
Cyber Threats & Cybersecurity in ASEAN and Thailand
ASEAN Economic Integration

- Over 600 M people
- Large young worker pool
- Rich in natural resources
- Steady GDP growth
- GDP 2.5 trillion USD in 2013

Source: IMF, Alaska Business Monthly Feb 2013
What Are the Challenges for ASEAN in 2015 and Beyond?

“Globalization and regional integration will introduce additional complexity and difficulties in consumer protection to be managed by all ASEAN Member States. There are, in particular, the increasing volumes and value of domestic and cross-border trade as well as the constant and rapid progress in the technologies in communications, production and e-commerce”

How to ensure the trust and confidence in business activities?

How do we preserve individual’s basic rights? (accessibility, privacy, etc.)

How do we encourage efficiency of cross-border transactions?

& security
ASEAN ICT Masterplan 2015

- Initiative 2.4 Build trust
  - Promote secure transactions within ASEAN
  - Promote awareness of cyber security

- Initiative 4.2 Promote network integrity, information security, data protection and CERT cooperation
Thailand Internet User Profile

Population
64.457 Mpeople (2012, dopa.go.th)

Internet users
24 Musers (2012, NECTEC)

International Bandwidth
507.084 Gbps (May 2013, NECTEC)

Domestic Exchange Bandwidth
1.223 Tbps (May 2013, NECTEC)

Mobile phone subscribers
87.446 Msubs (Apr 2013, NBTC)

.th domain names
64,316 domains (March 2013, all.in.th)

All domain names
246,274 domains (May 2013, webhosting.info, all.in.th)

Facebook users
18.766 Musers (June 2013, CheckFacebook)

Twitter users
2 Musers (Apr 2013, blog.zocialinc.com)
Survey on Thai people’s use of Internet: number of hours/week

Current Situation

Use of Social Media

- Facebook: 92.2
- Google+: 63.7
- Twitter: 8.2
- Instagram: 12.0
- WhatsApp: 8.4
- Line: 61.1

The devices most used for internet connection:

- Computer: 45%
- Notebook: 25.3%
- Smart Phone: 22.7%
- Tablet: 6.8%
- ETC: 0.2%

Yearly Change:

Year
- 2013: 35.7 Less than 10h, 25.8 11-20h, 38.5 More than 20h
- 2010: 37.4 Less than 10h, 23.4 11-20h, 39.2 More than 20h
- 2007: 49.8 Less than 10h, 21.2 11-20h, 29.1 More than 20h
- 2004: 48.5 Less than 10h, 25.7 11-20h, 25.8 More than 20h
- 2001: 53.6 Less than 10h, 27.7 11-20h, 18.7 More than 20h

Note: The percentage values are approximate and the figure may be subject to rounding.

Notebook: 25.3%
Computer: 45%
Smart Phone: 22.7%
Tablet: 6.8%
ETC: 0.2%
Smart & Secure Thailand

**Stronger Economy**

**Social Equality**

**Environmental Friendly**

**MICT**
SMART THAILAND 2015

**SMART NETWORKS**

- to connect (all rural) communities

**SMART GOVERNMENT**

- to optimize government services / investment

**SMART PEOPLE**

- to support people using ICT in smart manner

**SMART BUSINESS**

- to promote > citizens & ict-biz opportunities

Security is a part of Sustainability.
Cybercrime in Thailand

Phishing - Thailand still continues to rank highly in APWG top 10 countries, as it has for several years.

Watering hole – New trend of malware designed to target Thai e-banking platforms, capable of stealing both user credential and OTP.

Call center scam – Fraudulent call center always locates outside Thailand using a fake caller IP over VoIP services.
Overview of Threat Landscape in Thailand

![Threat Landscape Chart]

- No. of unique IPs
- Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep

Legends:
- Botnet
- Brute Force
- DDoS
- Malware URL
- Open DNS Resolver
- Open Proxy Server
- Phishing
- Scanning
- Spam
- Web Defacement

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
Electronic Transactions Development Agency (Public Organization)
Thai Cabinet approved IT2000 Master Plan

IT Law Initiative
- Electronic Commerce
- Electronic Signature
- Computer Crime
- Electronic Funds Transfer
- Data Protection
- Universal Access

Electronic Transactions Act 2001

Computer Crime Act 2007

Electronic Transactions Act 2008 (Amendment)

Royal Decrees:
- Rules and Procedures of the Public Sector’s Electronic Transactions 2006
- Security Techniques in Performing Electronic Transactions 2010

Notifications:
- Criteria on Collection of Computer Traffic Data from Service Providers 2007
- ...

Regulations
- Computer System Seizure Form 2008
- Arresting, Confining, Searching, Investigating, and instituting Criminal Prosecution Against Offenders 2007
- ...

### Electronic Transaction Act 2001 and 2008

<table>
<thead>
<tr>
<th>Section 25: Security Measures</th>
<th>Section 35: e-Transaction in Public Sector</th>
</tr>
</thead>
</table>

Notification: Policy and Practice in the Information Security of a State Agency 2010
The observed common and important policies are

1. Based on security principles: Availability, Integrity and Confidentiality; and comply with existing cyber laws
2. Establish a national CERT to be a country focal point of contact
3. Cover people, public and private sectors and some include national security and military
4. Promote the information exchange between interested parties in order to effectively handle the cyber incidents
5. Define Critical Information Infrastructure organization
6. Enhance the capability and capacity and public awareness raising
7. Support Cybersecurity R&D

Cyber Security Strategy by Australian Government and CSOC (CERT Australia and the Cyber Security Operations Center)


National Cyber Security Policy by Ministry of Science, Technology and Innovation

Infocomm Security Masterplan 2 (MP2) under iN2015 proposed by Info-communications Development Authority of Singapore (IDA)
Cybersecurity Challenges

- Build a single command center
- Not enough cybersecurity workforce and certified professionals
- Law enforcement capacity to fight cybercrime
- Language barrier and digital divide
- Building sector-based CSIRT/CERT

Cybersecurity Policy Framework

3 Main Strategies
1. Cybersecurity Governance
2. Cybersecurity Emergency Readiness
3. National Critical Information Infrastructure Readiness

5 Supporting Strategies
4. Public-Private Partnership
5. Capacity & Capability Building
6. Legal Measures
7. Research and Development
8. International Cooperation

National Incident Handling Flow

Cybersecurity-related risk mitigation

- Reputational risk
- Operational risk

National Cybersecurity Committee (NCSC)
Approaches to cope with Cyber Threats

- Encourage public and private organizations to have security and privacy policies that are in line with international standards and best practices.

- Raise awareness to ensure that individuals are equipped with sufficient knowledge and skills to protect themselves against cyber attacks.

- Bring together national CERTs to create the incident handling flow, allowing cybersecurity incident to be handled effectively.