ICT LAW CENTER | ETDA สพธอ www.etda.or.th

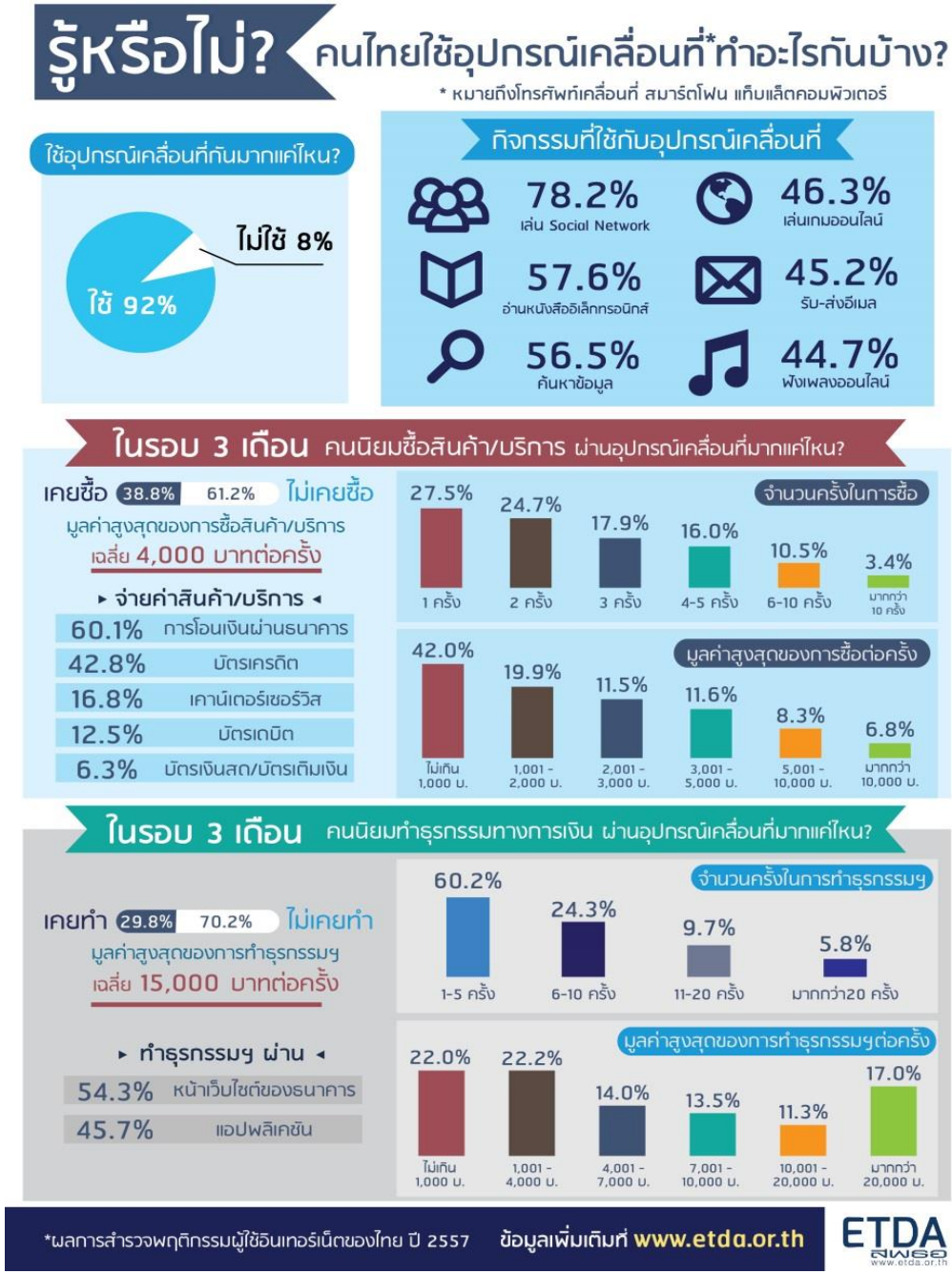
Open Forum : ICT Law Center, a member of ETDA

ร่วมปฏิรูปกฎหมาย ร่วมให้ความเห็น เพื่อเดินหน้าประเทศไทย

วันเสาร์ที่ 24 มกราคม 2558 เวลา 10.00 – 14.00 น.

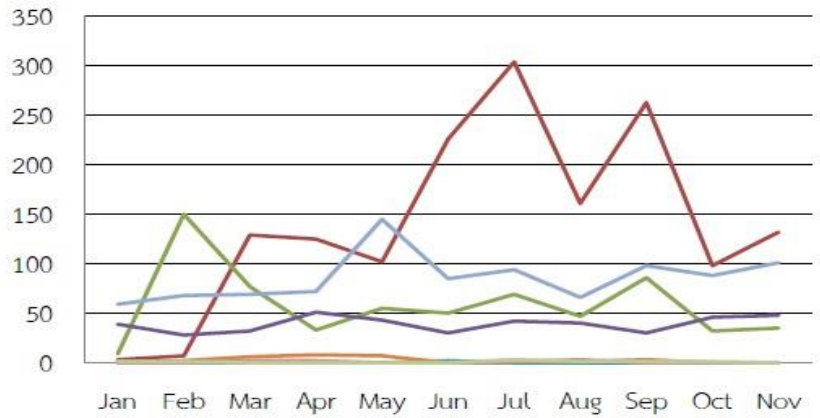
ณ ห้อง Open Forum สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
ชั้น 21 อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) กรุงเทพฯ

อินเทอร์เน็ตกับภัยคุกคามไซเบอร์



สถิติภัยคุกคามประจำปี พ.ศ. ๒๕๕๗

Directly Reported Incidents To ThaiCERT In 2014 Per Type



Number of reports: 3,616

1. Malicious Code: 1,550 reports (43%)
2. Fraud: 945 reports (26%)
3. Intrusion Attempts: 643 reports (18%)

ETDA

ThaiCERT

ETDA www.etda.or.th | ICT LAW CENTER

ทำไมต้อง “พัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม”

ทำอย่างไร ให้สอดคล้อง มีเอกภาพ

m-Commerce

e-Commerce

e-Payment

Digital Banking

Digital Contents

Embedded Software

iCloud

Telecom

Broadcasting

กฎหมาย & ข้อเสนอเกี่ยวกับมาตรการทางกฎหมายที่จำเป็น เพื่อรองรับ Digital Economy & Society

ช่วงที่ ๑

๑.กฎหมายลิขสิทธิ์
-การปกป้องมาตรการทางเทคโนโลยี (จำเป็นต้องมี Best Practices)
-การระงับการเผยแพร่ซึ่งมีมาตรการตรวจสอบโดยศาล

๒.กฎหมายอำนวยความสะดวก

ช่วงที่ ๒

ร่างกฎหมาย ๑๐ ฉบับ
๑.ปรับปรุงกระทรวง ICT
๒.กรรมการ DE
๓.กสทช. : กสช.& กทค.
๔.กองทุน Digital Economy
๕.Digital Economy Promotion
๖.ธุรกรรมทางอิเล็กทรอนิกส์ (e-Commerce)
๗.Data Protection (ตั้งแต่ปี ๒๕๔๑-๒๕๕๗ = ๑๖ ปีเต็ม)
๘.Cybersecurity
๙.Computer Crime
๑๐.จัดตั้งสพธอ.

ช่วงที่ ๓

๑.การจัดซื้อจัดจ้าง
๒.ระบบสารบรรณอิเล็กทรอนิกส์
๓.การรักษาความลับ
๔.การรักษาความปลอดภัย (เมื่อไม่มีมาตรการทำลายเอกสารที่เหมาะสม ก็ยังคงมีภาระในการมีและเก็บทั้งเอกสารกระดาษ & e-Document ควบคู่กัน ซึ่งเป็นต้นทุนทางเศรษฐกิจมหาศาล)
๕.กฎหมายข้อมูลข่าวสารของราชการ
๖.กฎหมาย e-Government ??
๗.การคุ้มครองผู้บริโภคทางออนไลน์ (Online Consumer Protection)

ช่วงที่ ๔

๑.การคุ้มครองทรัพย์สินทางปัญญาทั้งระบบ ??
การรับแจ้ง/ขึ้นทะเบียนลิขสิทธิ์และความจำเป็นในการเข้าเป็นภาคีอนุสัญญาสำคัญๆ
๒.มาตรการทางภาษี การเงิน & การคลัง
การร่วมลงทุนระหว่างรัฐและเอกชนในโครงสร้างพื้นฐานสำคัญ/ขนาดใหญ่
๓.e-Transferable Record
๔.การระงับข้อพิพาททางออนไลน์ (Online Disputes Resolution)
๕.Internet Governance - IGF

ประเด็น Hot

- Digital Economy คืออะไร

  ใครได้ประโยชน์ ???

- กฎหมาย 10 ฉบับ ทำไมประชาชนไม่เคยได้เห็น ??? ทำไมเร่งรัดกฎหมาย
- การปรับโครงสร้างการทำงานของรัฐจะช่วยในการพัฒนา Digital Economy ได้จริงหรือ ???
- ชุดกฎหมายเหล่านี้เป็นชุดกฎหมาย “เศรษฐกิจดิจิทัล” จริงหรือ ??? หรือเป็นชุดกฎหมายความมั่นคง ที่ให้อำนาจอย่างกว้างขวางกับหน่วยงานและพนักงานเจ้าหน้าที่ ???

- Cybersecurity เพื่อล้วงตับ ดักรับ โดยไม่มีขอบเขตและไม่มีกลไกการตรวจสอบ เสรีภาพประชาชนตกอยู่ในมือรัฐ
- สมควรแล้วหรือที่หน่วยงานที่ดูแล Data Protection อยู่ร่วมกับ Cybersecurity Agency ???

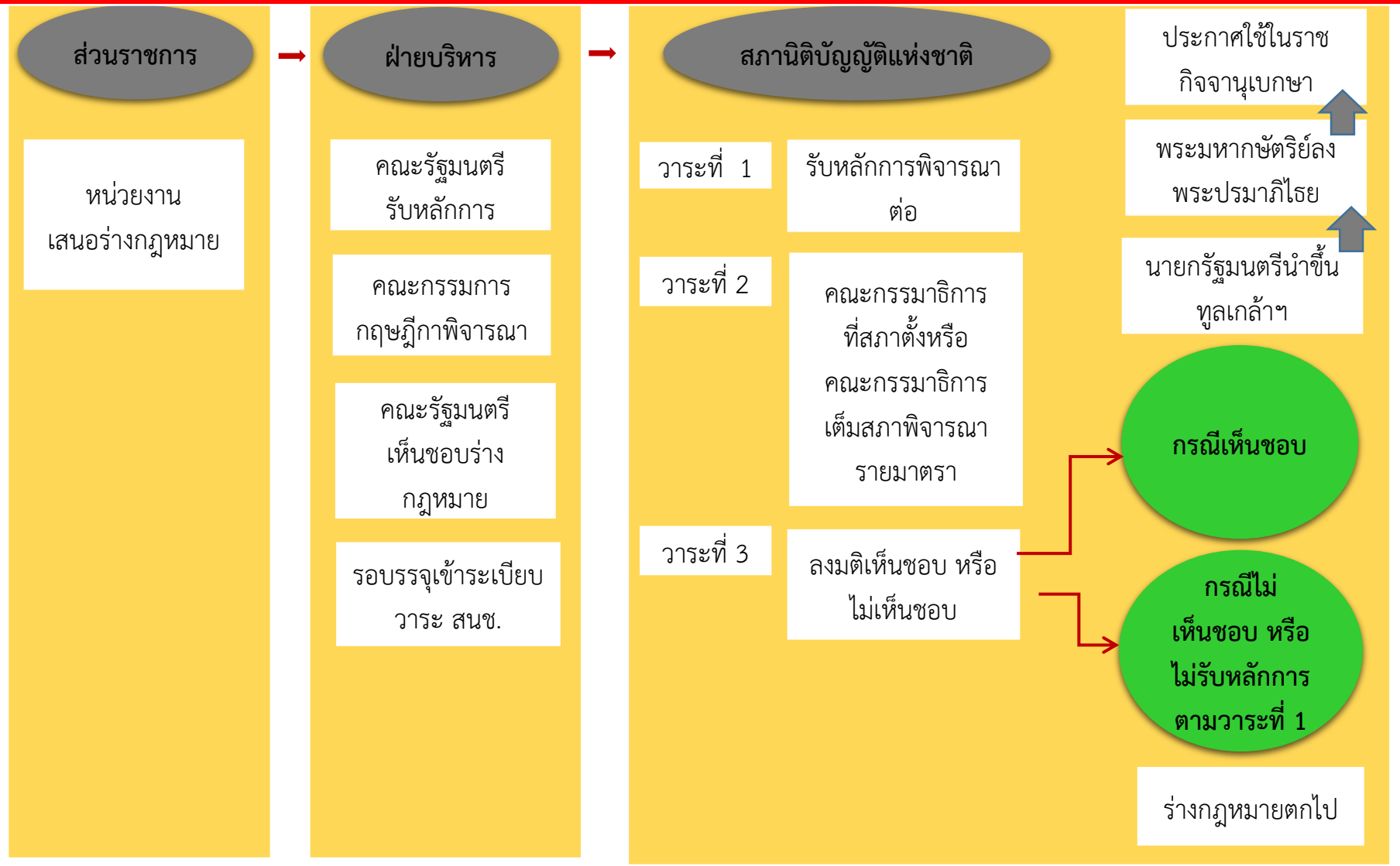
- กองทุน Digital Economy คือ แหล่งเงินกู้ที่สุดท้ายจะสูญเปล่า และประชาชนก็จะไม่ได้อะไร ???

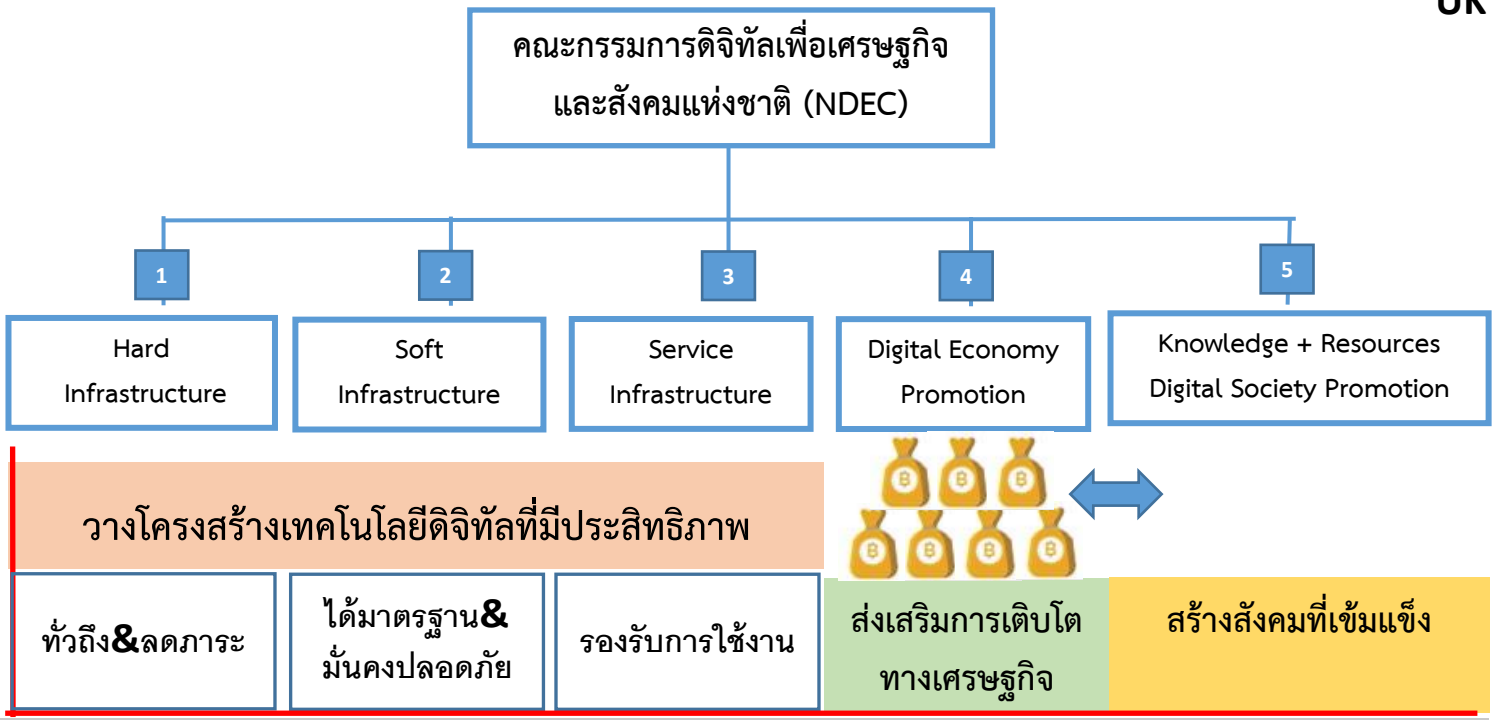
- คลื่นความถี่จะถูกรัฐควบคุมและล้วงลูก จนสื่อไม่มีอิสระ หรือไม่???
- คลื่นความถี่จะถูกจัดสรร โดยไม่ใช่การประมูล ???

  จะประกันความโปร่งใสได้อย่างไร ???

กระบวนการตรากฎหมายเพิ่งเริ่มต้น & ยังต้องการความเห็นตลอดทาง

๔ ก.ย. ครม.ประยุทธ์ ตั้งสนช. & สปช. คาดว่ารธน.จะแล้วเสร็จ ก.ย.๕๘ และมีการทำกฎหมายประกอบรธน. ก.พ.หรือพ.ค ๕๙ คาดว่าจะมีการเลือกตั้ง





UK Digital economy action plan 2014 to 2015

Hong Kong 2014 DIGITAL 21 STRATEGY

OECD Digital Economy Papers

Digital economy rankings and scores, 2010

2010 rank (of 70)	2009 rank	Country	2010 score (of 10)	2009 score	2010 rank (of 70)	2009 rank	Country	2010 score (of 10)	2009 score
1	2	Sweden	8.49	8.67	36	38	Malaysia	5.93	5.87
2	1	Denmark	8.41	8.87	37	37	Latvia	5.79	5.97
3	5	United States	8.41	8.60	38	36	Slovakia	5.78	6.02
4	10	Finland	8.36	8.30	39	39	Poland	5.70	5.80
5	3	Netherlands	8.36	8.64	40	41	South Africa	5.61	5.68
6	4	Norway	8.24	8.62	41	40	Mexico	5.53	5.73
7	8	Hong Kong	8.22	8.33	42	42	Brazil	5.27	5.42
8	7	Singapore	8.22	8.35	43	43	Turkey	5.24	5.34
9	6	Australia	8.21	8.45	44	44	Jamaica	5.21	5.33
10	11	New Zealand	8.07	8.21	45	47	Bulgaria	5.05	5.11
11	9	Canada	8.05	8.33	46	45	Argentina	5.04	5.25
12	16	Taiwan	7.99	7.86	47	48	Romania	5.04	5.07
13	19	South Korea	7.94	7.81	48	46	Trinidad & Tobago	4.98	5.14
14	13	United Kingdom	7.89	8.14	49	49	Thailand	4.86	5.00
15	14	Austria	7.88	8.02	50	52	Colombia	4.81	4.84
16	22	Japan	7.85	7.69	51	50	Jordan	4.76	4.92
17	18	Ireland	7.82	7.84	52	51	Saudi Arabia	4.75	4.88
18	17	Germany	7.80	7.85	53	53	Peru	4.66	4.75
19	12	Switzerland	7.72	8.15	54	54	Philippines	4.47	4.58

The economist : Digital Economy Ranking 2010 (49)

Legal Environment specific laws governing Internet use

Data Privacy

Data Protection

OECD Guidelines Governing the Protection of Privacy 2013

APEC Privacy Framework 2013

EU Directive 95/46/EC

Critical Infrastructures & Cyber Attack

Cyber Security

Japan Cyber Security Basic Act

US National Cybersecurity Protection Act 2014

Czech Republic Act on Cyber Security 2014

Hungary Act on the Electronic Information Security of Central and Local Government Agencies

E-transaction & E-Commerce

Facilitate & Legal Recognition

Uncitral Model law on electronic commerce

Uncitral Model law on electronic Signature

United Nations Convention on the Use of Electronic Communications in International Contracts

สร้างกลไกการทำงานร่วมกันระหว่างรัฐ เอกชน และประชาชน
ในการขับเคลื่อนงานทั้ง 5 ด้าน “ร่วมคิด & ร่วมทำ”

Law for Digital Economy

Policy | Resource | Operation

พ.ร.บ.การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ....

- มี คกก. NDEC กำหนดนโยบาย & Master Plan เป็นทิศทางการทำงานที่หน่วยงานนำไปปฏิบัติ
- คกก. NDEC ต้องประสานนโยบายกับ คกก. ตามกฎหมายอื่นเพื่อให้เป็นไปในทิศทางเดียวกัน
- ติดตามและประเมินผล

พ.ร.บ. กองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ....

- มีกองทุนรองรับการพัฒนาดิจิทัลทั้ง 5 ด้าน ครอบคลุมสังคม เศรษฐกิจ บริการภาครัฐ
- สำหรับหน่วยงานรัฐ เอกชน ผู้ประกอบการ ชุมชน และประชาชน
- การบริหารกองทุนโดย คกก. กองทุน ภายใต้หลักเกณฑ์ที่ คกก. NDEC กำหนด

มีการควบรวมกฎหมาย

พ.ร.บ.ปรับปรุงกระทรวง ทบวง กรม พ.ศ. ....

- ปรับบทบาทของกระทรวง MICT ให้รองรับการนำดิจิทัลเป็นฐานในการพัฒนาประเทศในด้านต่างๆ ด้วยการจัดตั้ง MoDE ที่มุ่งการทำงาน 5 ด้าน
- ปรับอำนาจหน้าที่ของส่วนราชการ ให้สอดรับการปรับโครงสร้างการทำงานระหว่างภาคราชการ / องค์การมหาชน / รัฐวิสาหกิจ / องค์กรอิสระ
- เพิ่มเติม สนง. ดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่เป็นฝ่ายเลขาฯ คกก. NDEC ด้วยการช่วยติดตาม/ดูแลงานทั้ง ๕ ด้าน และดูแลงานด้าน Digital Society

Hard Infra NBTC

พ.ร.บ. กสทช. (ฉบับที่ ..) พ.ศ. ....

ปรับปรุงให้การบริหารจัดการคลื่นความถี่ที่เป็นทรัพยากรสื่อสารของประเทศตอบโจทย์/เชื่อมโยงกับการพัฒนา DE ที่ต้องอาศัยคลื่นความถี่เป็นฐานรากด้านงาน Hard Infra

DE Promotion NDEP

พ.ร.บ. การส่งเสริมเศรษฐกิจดิจิทัล พ.ศ. ....

กำหนดให้มีหน่วยงานรัฐเพื่อส่งเสริม/ดูแลงานด้าน Promotion ที่เกี่ยวข้องกับภาคเศรษฐกิจ อุตสาหกรรม นวัตกรรม ด้านเทคโนโลยีดิจิทัลและ Digital Content

Service Infra NEGA

พ.ร.บ. รัฐบาลอิเล็กทรอนิกส์ พ.ศ. ....

(ความจำเป็นในการยกร่าง ?)

Soft Infra NETDA

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. ....

- บูรณาการหน่วยงานที่เกี่ยวข้องเข้าด้วยกันเพื่อผลักดันการใช้งานธุรกรรมทางอิเล็กทรอนิกส์ใน sector ต่าง ๆ
- เพิ่มเติมหลักเกณฑ์ให้สอดคล้องกับ e-communication Convention เพื่อเตรียมอนุวัติการ
- ปรับปรุงกฎเกณฑ์การทำธุรกรรมทางอิเล็กทรอนิกส์ และการกำกับดูแลธุรกิจบริการให้เหมาะสม

พ.ร.ฎ. สพธอ. (ฉบับที่ ..) พ.ศ. ....

ปรับปรุงให้เกิดการทำงานร่วมกันระหว่างรัฐและเอกชนในการพัฒนาระบบหรือบริการที่เป็น Critical Infra ให้มีมาตรฐาน เช่น e-Authentication (แก้กฎหมายช่วงเปลี่ยนผ่าน)

ยังคงมีกลไกการตรวจสอบการใช้อำนาจโดยศาล NCSA

พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

กำหนดให้มี สนง. เพื่อเป็น Command Center ในการดำเนินงานทางปฏิบัติด้าน Security ทั้งการป้องกัน รับมือ และจัดการกับ Incidents Response เพื่อลดความเสี่ยง ผลกระทบและความเสียหายจากภัยคุกคามไซเบอร์

พ.ร.บ. การกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ. ....

- ปรับปรุงให้กฎหมายมีความชัดเจน ป้องกันการปรับใช้ที่ผิดเจตนารมณ์
- ปรับปรุงฐานความผิดเพื่อห้ามปรามภัยร้ายออนไลน์ในรูปแบบใหม่
- ช่วยเหลือติดตามการทำความผิดอื่นที่ทำผ่าน Online เพื่อให้ได้พยานหลักฐานที่เชื่อถือได้ กระบวนการได้มาได้มาตรฐาน

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

- กำหนดหลักเกณฑ์ขั้นต่ำให้เกิด Standardization ในการดูแลข้อมูลส่วนบุคคล
- ผู้ควบคุมข้อมูลที่ถือครองข้อมูลส่วนบุคคลต้องดูแลมิให้มีการละเมิดสิทธิเจ้าของข้อมูล
- ส่งเสริมกลไกการกำกับดูแลตนเอง (Self-Regulation) ของผู้ประกอบการ/รัฐ
- มีกลไกติดตามเรื่อง Law Compliance

Digital Society สนง. ดิจิทัลเพื่อเศรษฐกิจและสังคมใน สปทก. ดูแล

ร่าง พ.ร.บ. กสทช. (ฉบับที่ ๒) พ.ศ. ....

Key Factors for Developing Digital Economy

Hard Infrastructure	Service Infrastructure	Soft Infrastructure	Digital Economy Promotion	Digital Society & Knowledge Resources

คลื่นความถี่

เป็นทรัพยากรสื่อสารของชาติ
ใช้เพื่อประโยชน์สาธารณะ

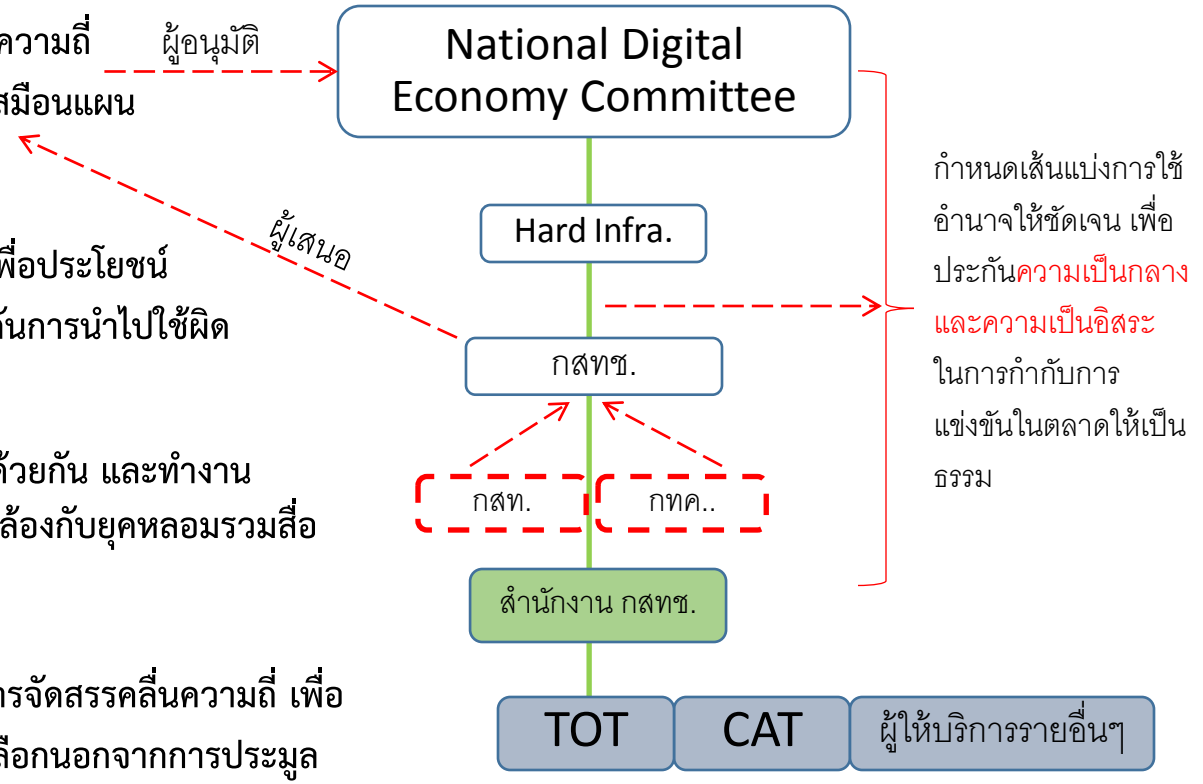
1 ทำให้ทิศทางการบริหารคลื่นความถี่ในระดับ Policy สอดคล้องกับการพัฒนา Digital Economy ตอบโจทย์การเป็นทรัพยากรสื่อสารของชาติ

2 การทำแผนแม่บทการบริหารคลื่นความถี่ ตารางกำหนดคลื่นความถี่ ที่เป็นเสมือนแผนชาติด้านคลื่นความถี่

3 คกก. จะดูแลสัดส่วนของการใช้คลื่นความถี่เพื่อประโยชน์สาธารณะและเชิงพาณิชย์ให้เหมาะสม ป้องกันการนำไปใช้ผิดวัตถุประสงค์

4 รวม กสท. และ กทค. เข้าด้วยกัน และทำงานเป็นชุดเดียว เพื่อให้สอดคล้องกับยุคหลอมรวมสื่อ

5 ปรับปรุงวิธีการจัดสรรคลื่นความถี่ เพื่อเพิ่มเติมทางเลือกนอกจากการประมูล



อำนาจหน้าที่คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม (NDEC) & กสทช. (NBTC)

NDEC

National Policy :

- แผนระดับชาติ เช่น National Broadband Plan
- แผนแม่บทการบริหารคลื่นความถี่ (Spectrum Master Plan)
- ตารางกำหนดคลื่นความถี่แห่งชาติ (National Frequency Allocation Table)

การจัดทำตารางกำหนดคลื่นความถี่แห่งชาติ ให้เป็นข้อเสนอของ NBTC แต่ให้เสนอ NDEC อนุมัติพร้อมแผนแม่บท เพื่อให้ตอบโจทย์การเป็น**ทรัพยากรสื่อสารของชาติ ประโยชน์ของประชาชน และภาระของผู้ประกอบการ**

NBTC

Sectoral Policy : (ต้องสอดคล้องกับแผนระดับชาติ)

- Broadcasting Master Plan
- Telecommunications Master Plan
- Frequency Plan (แผนความถี่วิทยุ)

เพื่อให้การทำงานของภาครัฐเดินไปในทิศทางเดียวกัน **ไม่เกิดภาวะต่างคนต่างทำไปคนละทิศ**

NDEC

Spectrum Assignment :

- จัดสรรการใช้คลื่นความถี่ในกิจการอื่นที่ไม่มีการแข่งขัน เช่น เพื่อการบรรเทาสาธารณภัย

Spectrum Assignment :

- จัดสรร (อนุญาต) การใช้คลื่นความถี่ในกิจการที่มีการแข่งขัน คือ กิจการโทรคมนาคม/กิจการโทรทัศน์

NBTC

ต้องมีการแบ่งสัดส่วนของย่านความถี่ว่าแข่งขัน/ไม่แข่งขันเท่าไหร่ เพื่อไม่ให้เกิดการแย่งกัน **และกำกับให้การใช้คลื่นความถี่เป็นไปตามวัตถุประสงค์ ยังคงมีอิสระในการกำกับดูแล**

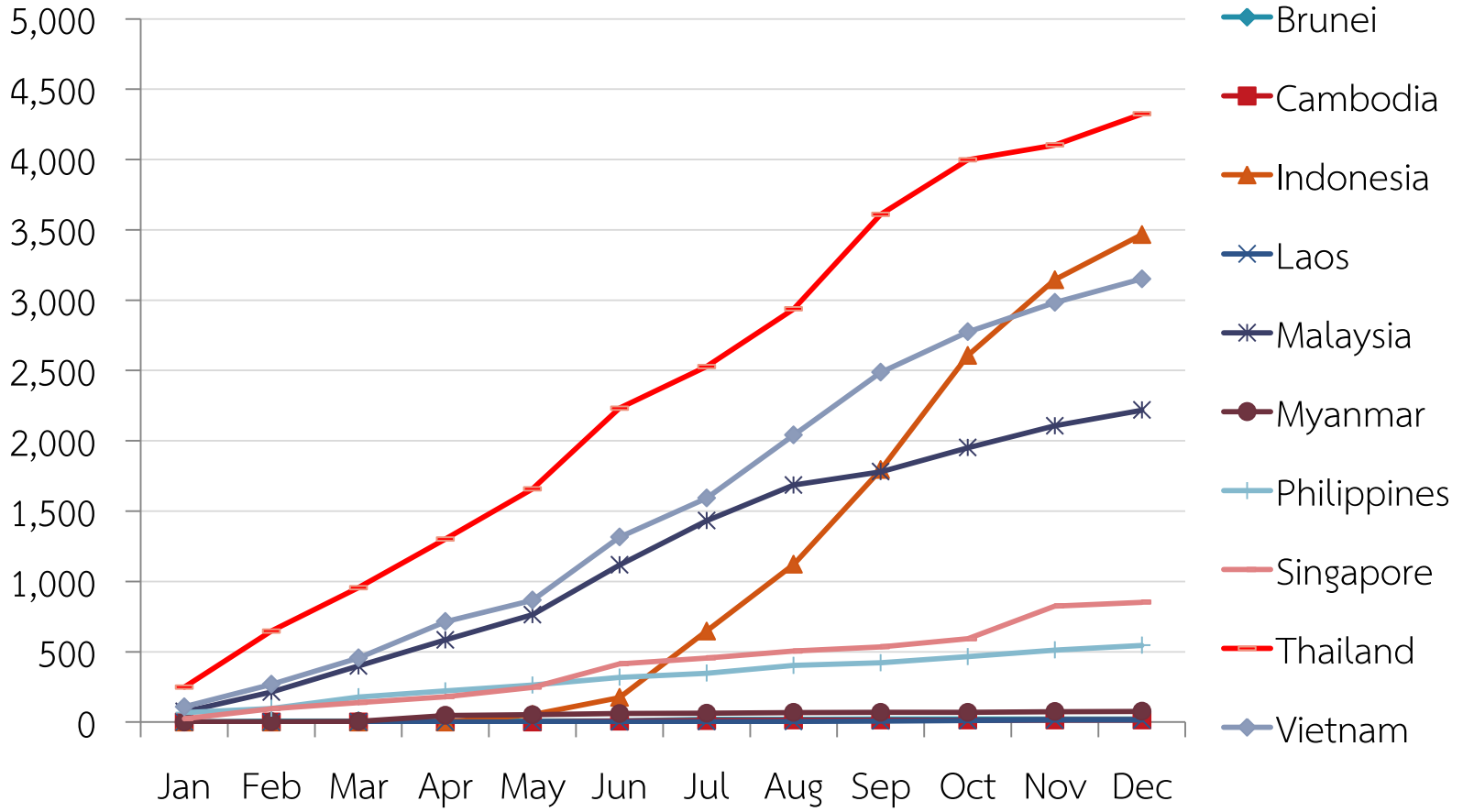
NBTC

Spectrum monitoring :

ติดตามตรวจสอบ/กำกับดูแลการใช้คลื่นให้ได้มาตรฐานการให้บริการ & ป้องกันคลื่นรบกวนกัน

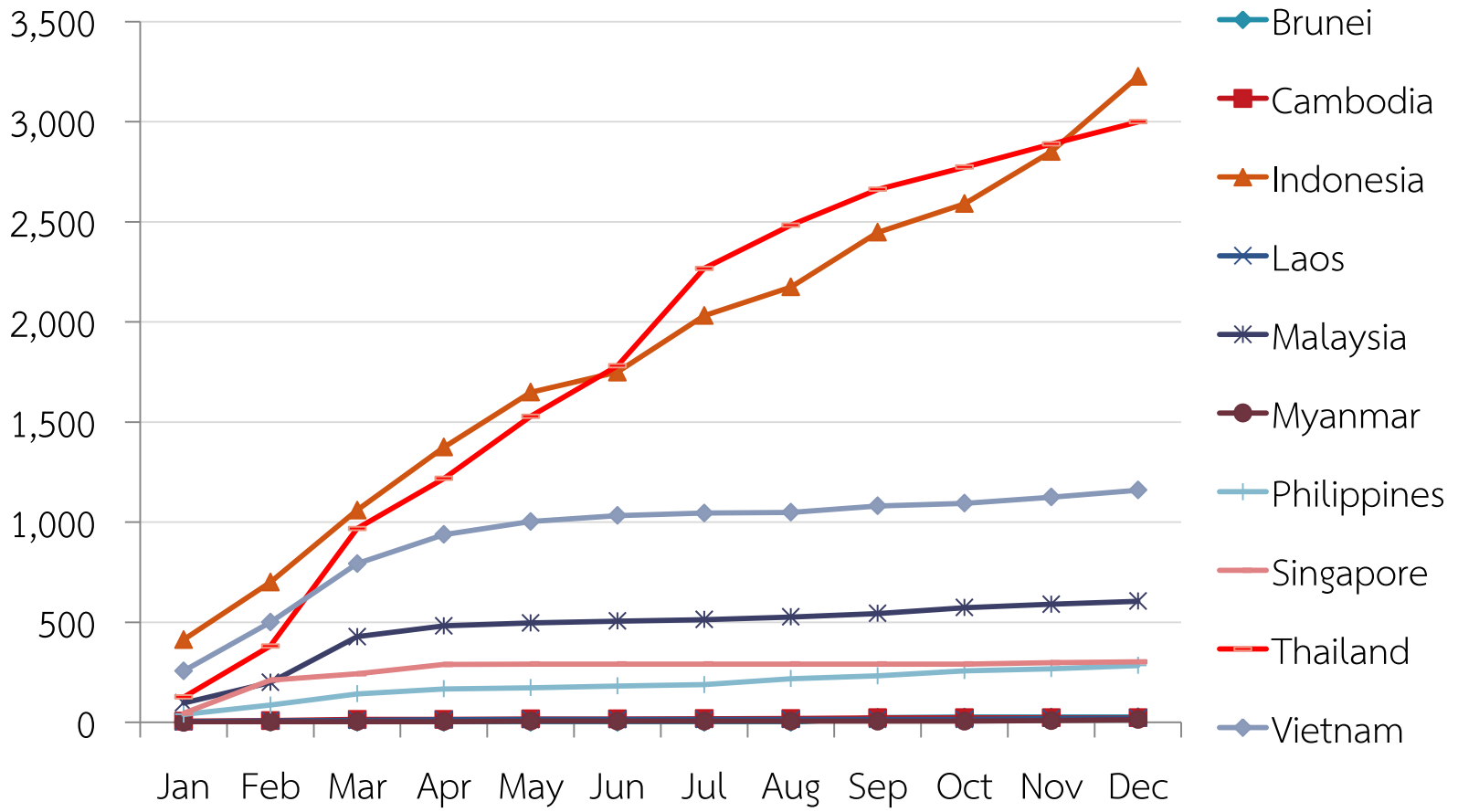
ประเทศไทย
กับความพร้อมด้าน Cybersecurity
กรอบความร่วมมือ AEC : 2015
& ITU Recommendation

สถิติภัยคุกคามประเภท Web Defacement ในภูมิภาค ASEAN ในปี 2556



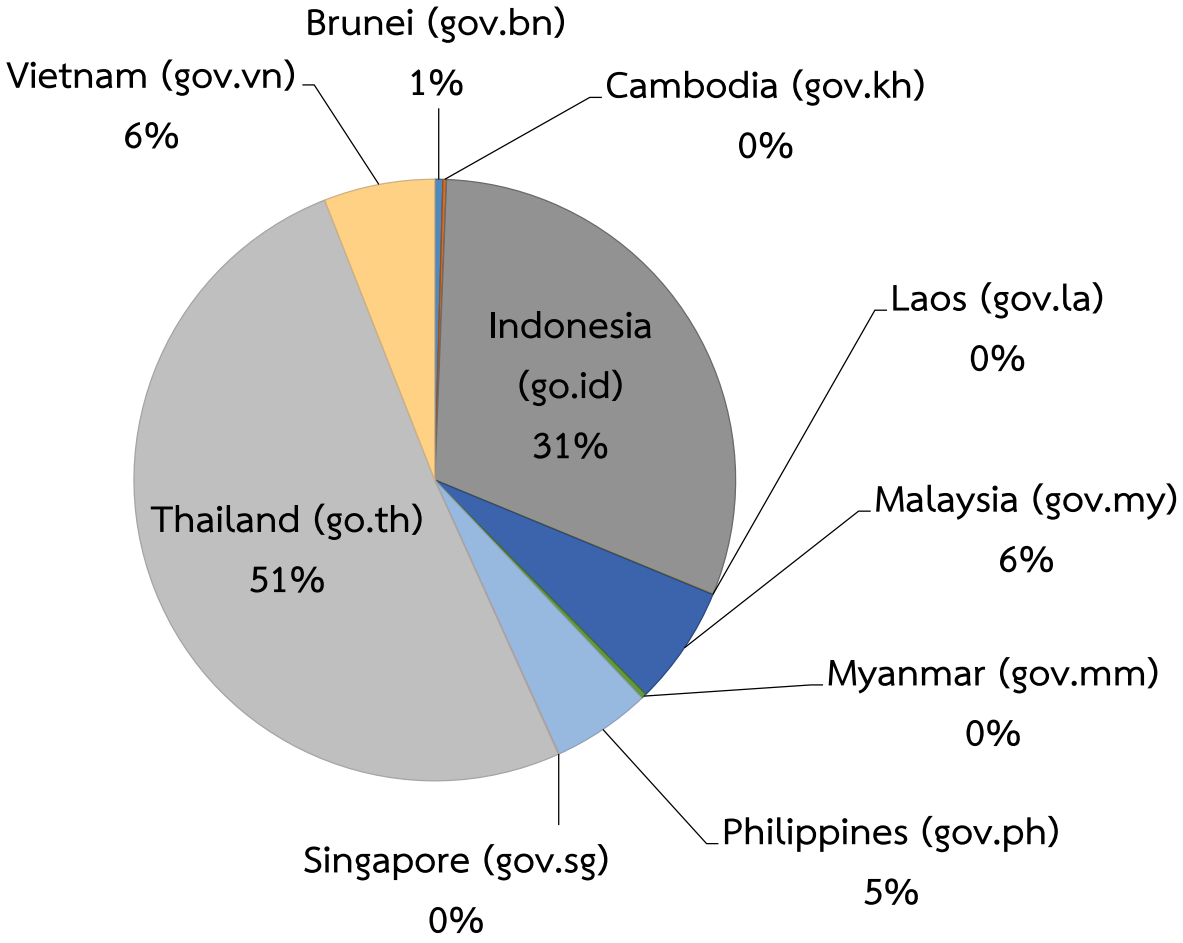
หมายเหตุ: ข้อมูลจากระบบ ThreatWatch ของไทยเซิร์ต ระหว่างเดือน ม.ค. – ธ.ค. 2556

สถิติภัยคุกคามประเภท Web Defacement ในภูมิภาค ASEAN ในปี 2557



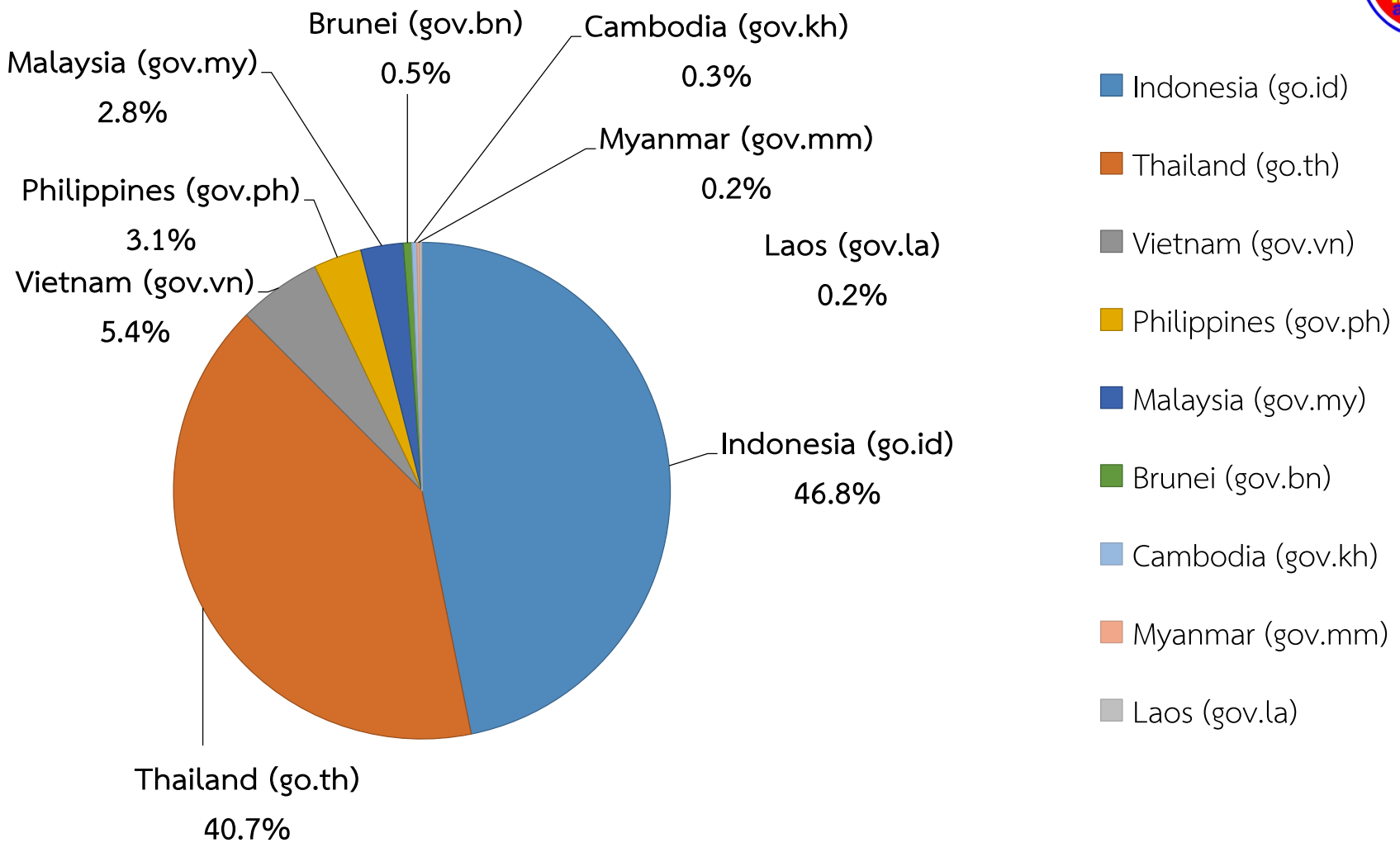
หมายเหตุ: ข้อมูลจากระบบ ThreatWatch ของไทยเซิร์ต ระหว่างเดือน ม.ค. – ธ.ค. 2557

สถิติภัยคุกคามประเภท Web Defacement
จำแนกเฉพาะหน่วยงานของรัฐในภูมิภาค ASEAN ในปี 2556



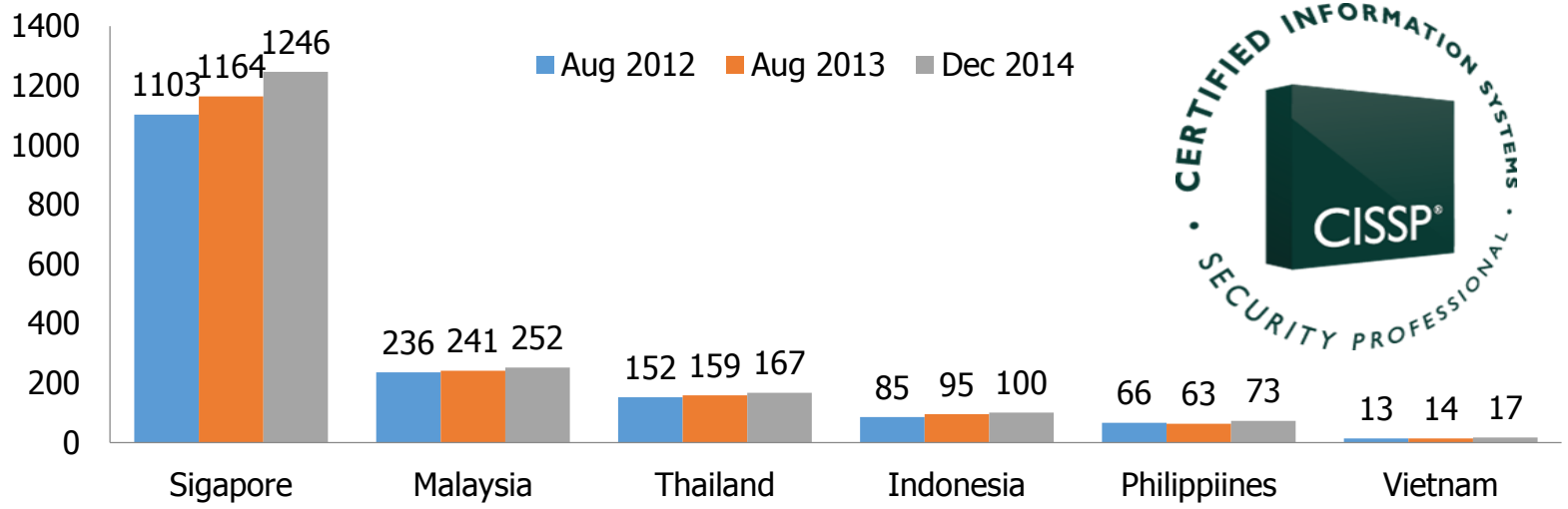
หมายเหตุ: ข้อมูลจากระบบ ThreatWatch ของไทยเซิร์ต ระหว่างเดือน ม.ค. – ธ.ค. 2556

สถิติภัยคุกคามประเภท Web Defacement
จำแนกเฉพาะหน่วยงานของรัฐในภูมิภาค ASEAN ในปี 2557



หมายเหตุ: ข้อมูลจากระบบ ThreatWatch ของไทยเซิร์ต ระหว่างเดือน ม.ค. – ธ.ค. 2557

สถานการณ์ความพร้อมของบุคลากรด้านความมั่นคงปลอดภัย



อ้างอิง ข้อมูล CISSP holders จาก www.isc2.org/member-counts.aspx (Aug 2012, Aug 2013, Dec 2014) **และ ข้อมูล** GIAC จาก The SANS Institute

Bloomberg

Photographer: Miquel Benitez/Getty Images

Seth Rogen during a photocall for his latest film 'The Interview' on June 18, 2014 in Barcelona, Spain.

Sony's Breach Stretched From Thai Hotel to Hollywood

By Jordan Robertson, Dune Lawrence and Chris Strohm
December 07, 2014 12:54 PM EST

The Hollywood Reporter BUSINESS

Sony Hackers Reportedly Worked From Thailand

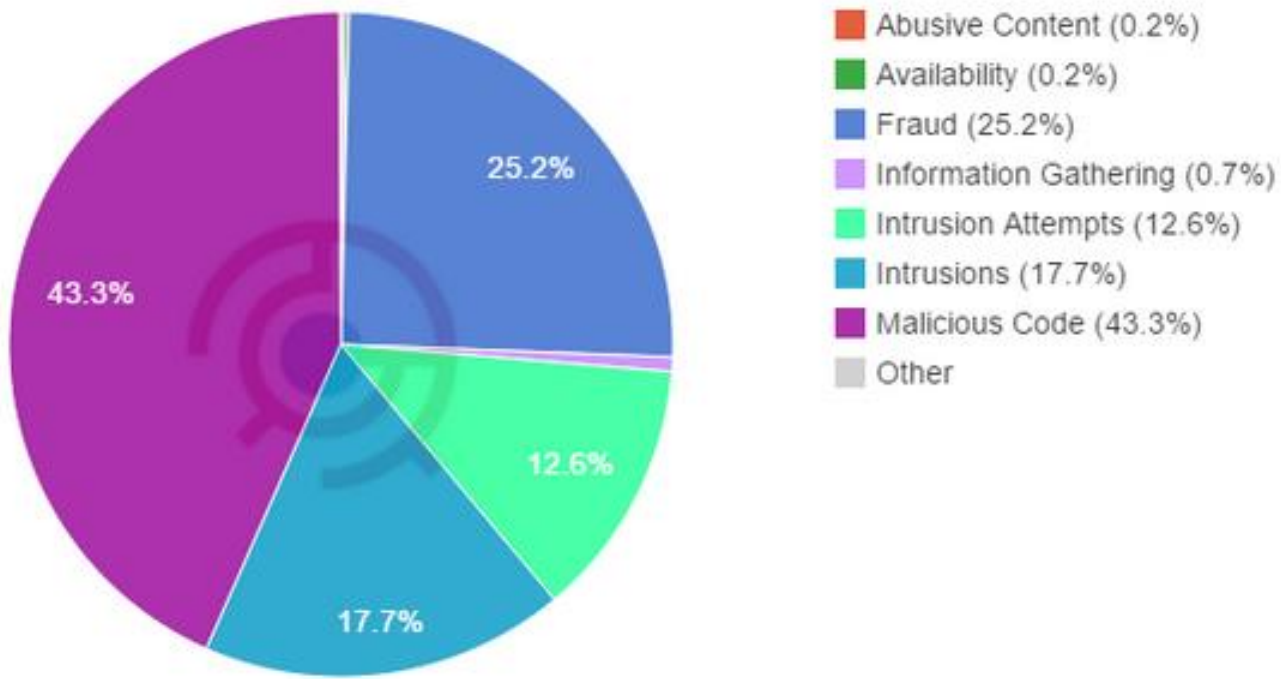
Courtesy of Sony Pictures Entertainment

NEXT UP
Kevin Hart: I Won't Play a Gay Character

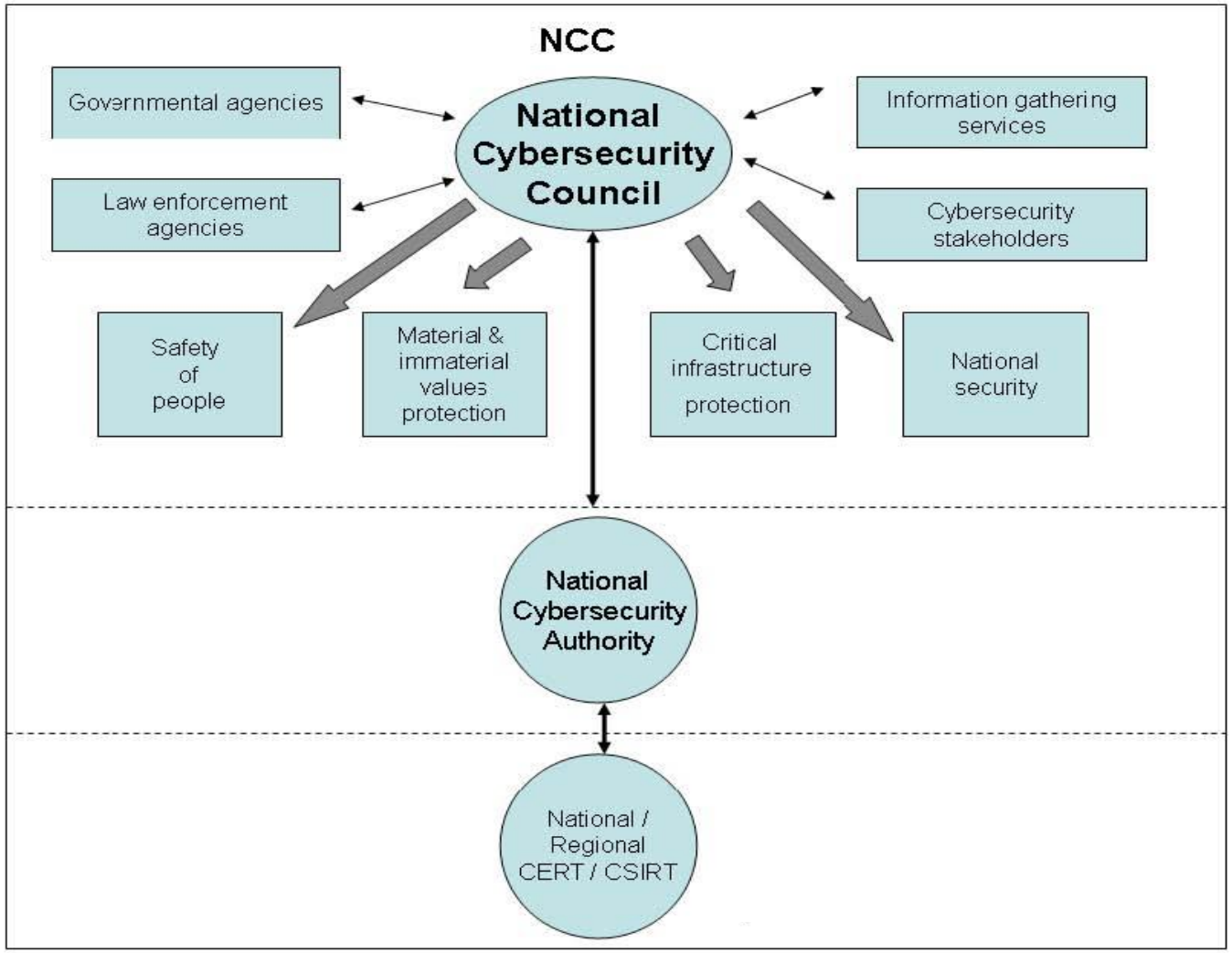
สถิติภัยคุกคาม ประจำปี พ.ศ. 2557

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	1	1	0	0	0	0	3	1	1	1	0	0	**8**
Availability	0	0	2	2	0	0	1	3	0	0	0	0	**8**
Fraud	59	68	69	72	145	85	94	66	98	88	101	65	**1010**
Information gathering	1	2	6	8	7	0	1	1	3	0	0	0	**29**
Information security	0	1	0	0	0	2	0	0	1	0	0	0	**4**
Intrusion Attempts	39	28	32	51	43	30	42	40	30	46	48	74	**503**
Intrusion	9	150	77	33	55	50	69	47	86	32	35	68	**711**
Malicious code	3	7	129	125	102	226	304	161	263	98	132	185	**1735**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**112**	**257**	**315**	**291**	**352**	**393**	**514**	**319**	**482**	**265**	**316**	**392**	**4008**

จำแนกตามประเภทภัยคุกคาม

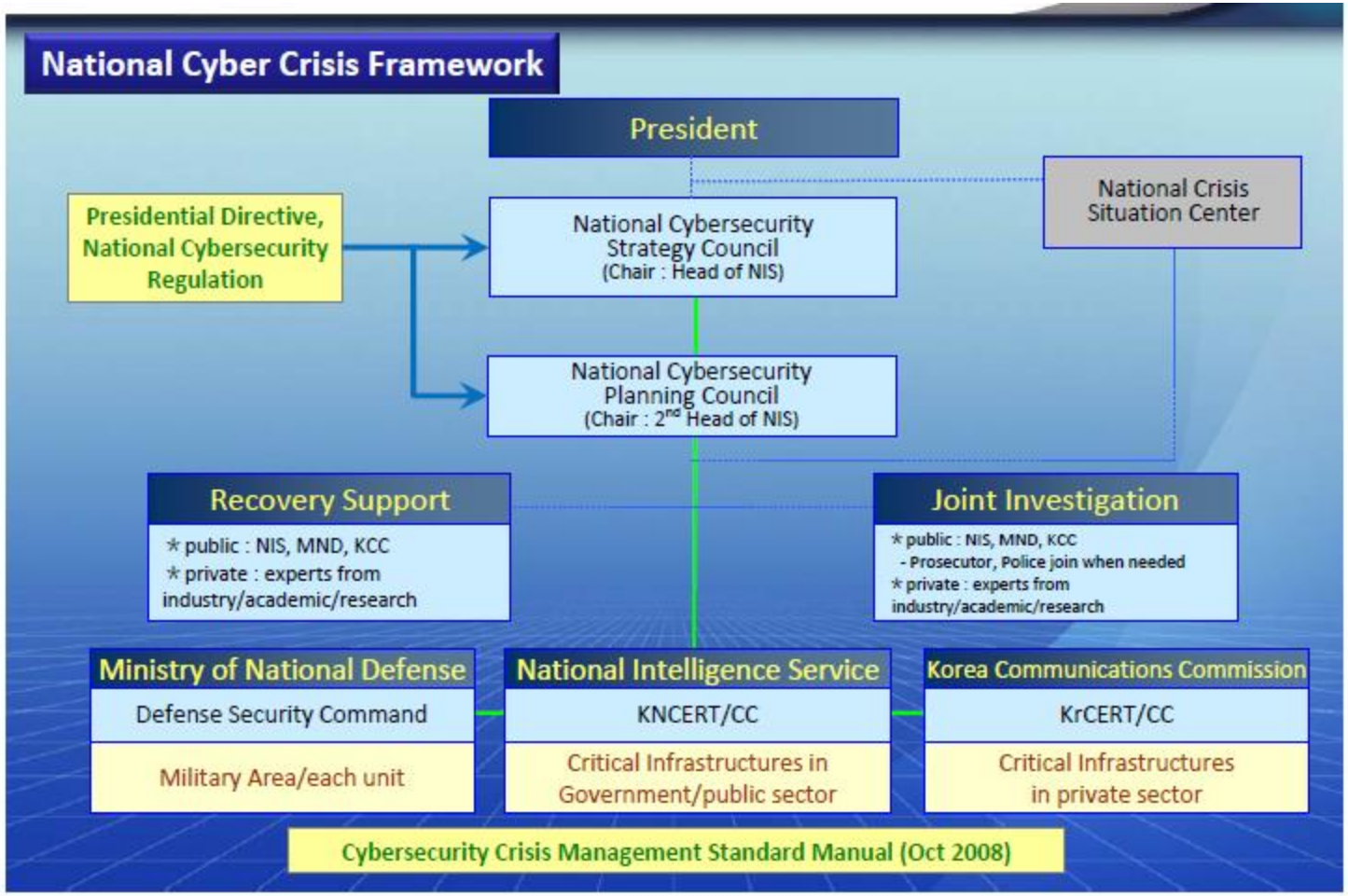


ITU Framework for National Cybersecurity

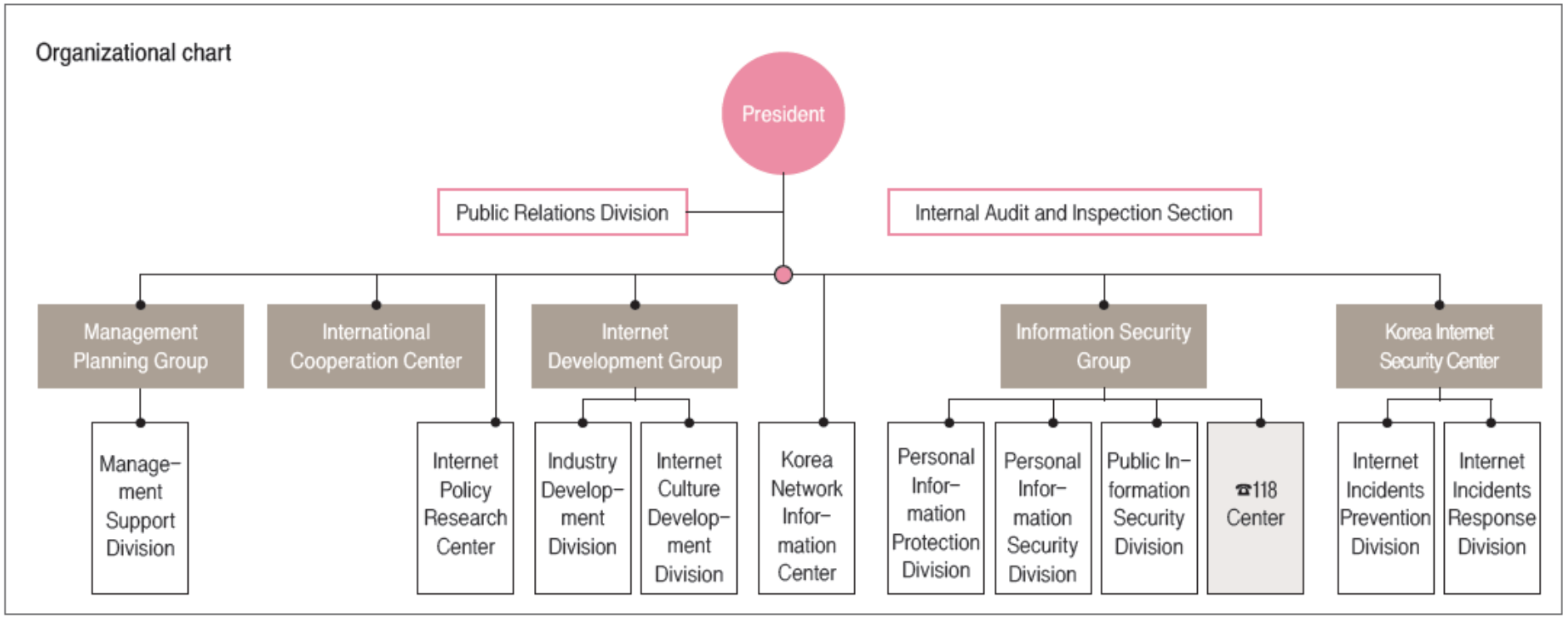


ITU Global Cybersecurity Agenda 2008http://www.cybersecurity-gateway.org/pdf/global_strategic_report.pdf

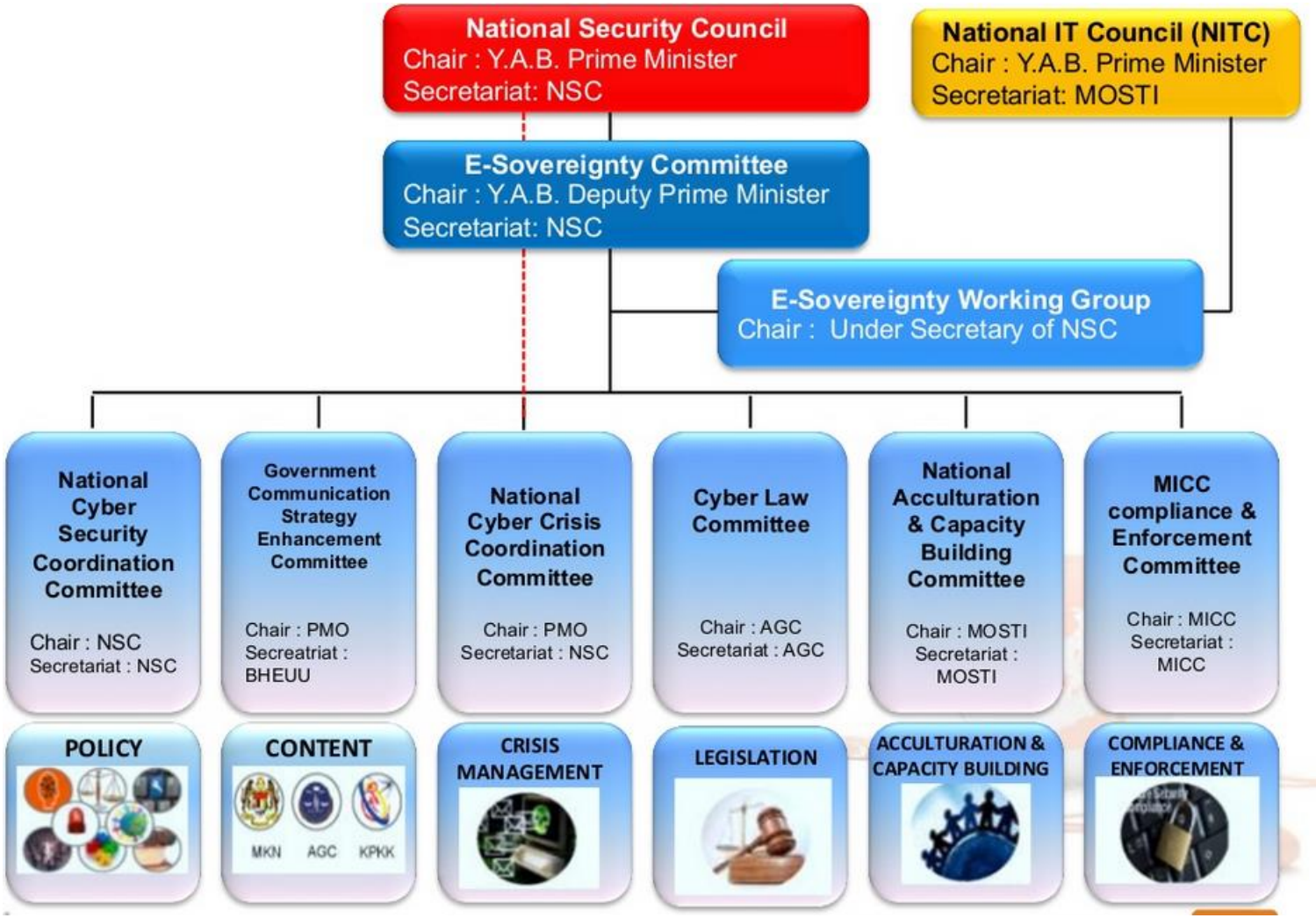
National Cybersecurity Framework (Kr)



KISA Organization



National Cybersecurity Framework (My)



คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
National Cybersecurity Committee

Measures

Risk management

Cybersecurity

Master plan

Reporting

Policy

ความเสี่ยง Cybersecurity

- ชื่อเสียง Reputation
- ความเสี่ยงด้าน Operational

Cyber Attacks Cyber Terrorism

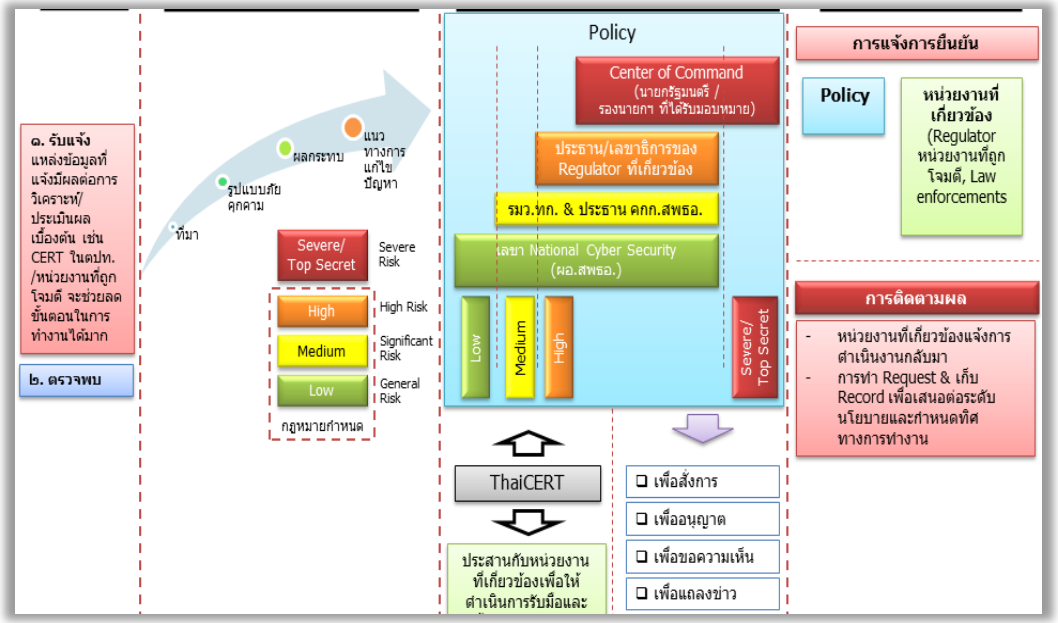
Cyber Warfare

ความท้าทาย Cybersecurity ของประเทศ

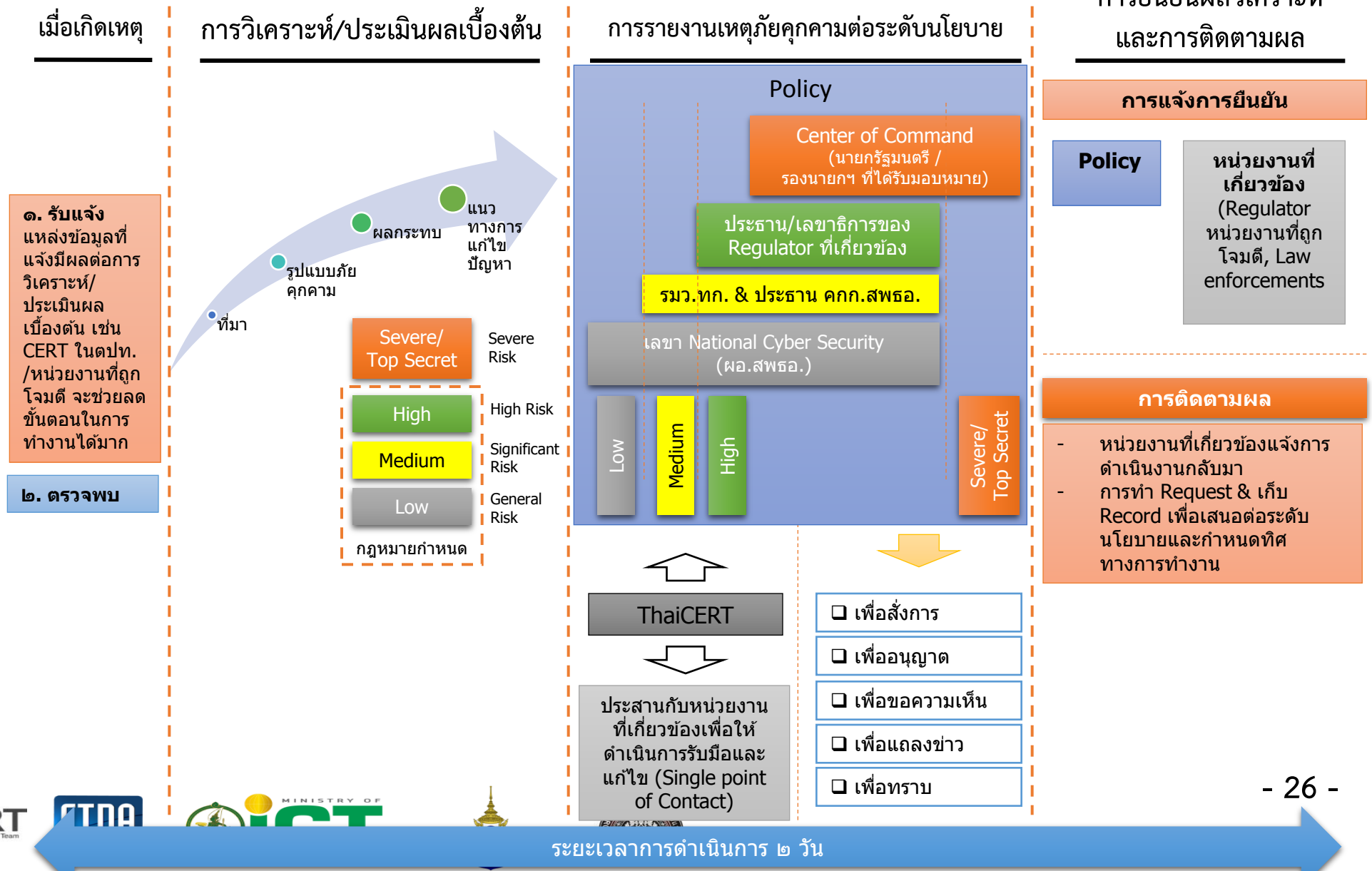
- การให้ความสำคัญในระดับผู้นำ
- Business Continuity ของบริการโครงสร้างพื้นฐาน
- บุคลากรด้าน Security ของประเทศ
- การสร้างความตระหนัก
- Collaboration

(ร่าง) กรอบนโยบายเกี่ยวกับ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(ร่าง) ขั้นตอนการแจ้ง/รับมือเหตุภัยคุกคามที่กระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศ



ขั้นตอนการแจ้ง/รับมือเหตุภัยคุกคามที่กระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศ



Executive Order – Improving Critical Infrastructure Cybersecurity

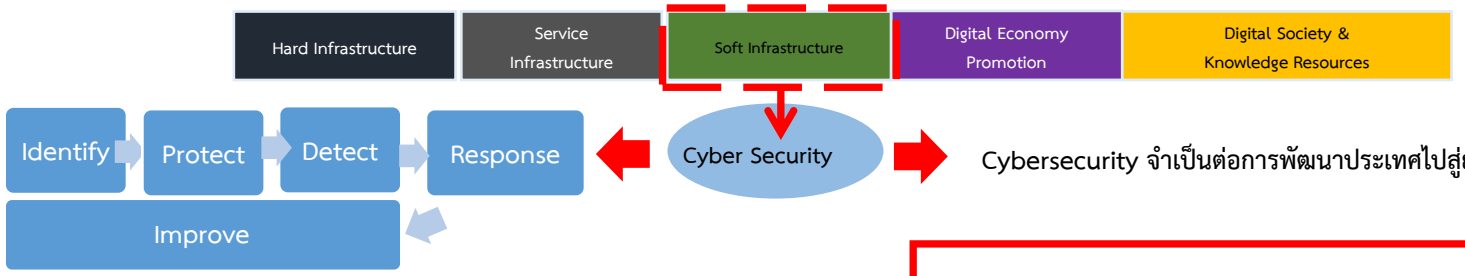
BARACK OBAMA

Policy

"...The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. ..."

ร่าง พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

Key Factors for Developing Digital Economy



Cybersecurity จำเป็นต่อการพัฒนาประเทศไปสู่ยุคสังคมดิจิทัล

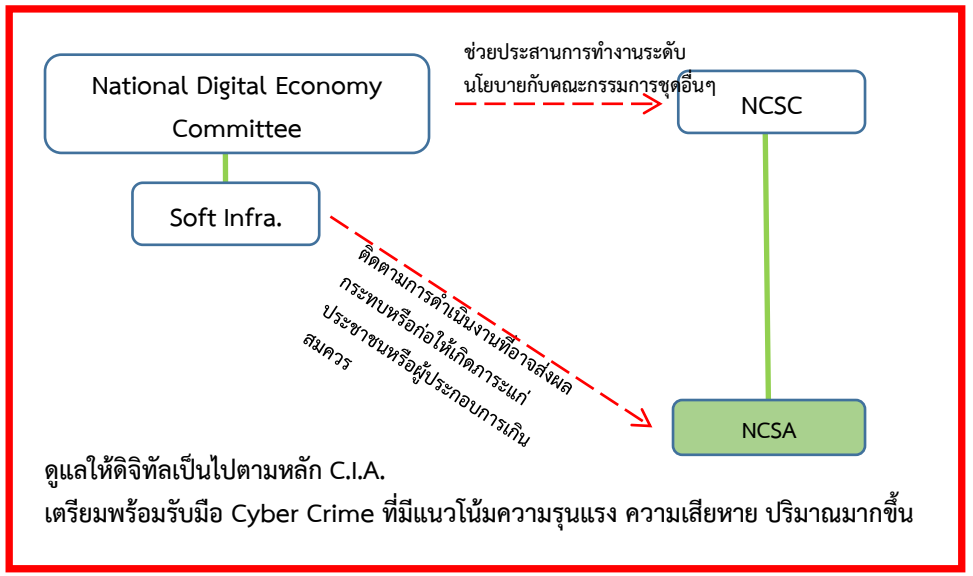
1 สนับสนุนให้การดูแล Cybersecurity ระดับนโยบายที่ภาคส่วนต่าง ๆ ต้องให้ความสำคัญในยุค Digital

2 คณะกรรมการทำหน้าที่ในการวางระบบ/มาตรฐาน/มาตรการในการดูแล Cybersecurity และประเมินความพร้อม

3 กำหนดกลไกการดูแล Cybersecurity ทั้งก่อนเกิดเหตุ ขณะเกิดเหตุ หลังเกิดเหตุ พร้อม level และ National Flow ในการรับมือ

4 NCSA จะเป็นหน่วยงานที่มีความเชี่ยวชาญ เพื่อสนับสนุนการดูแล Cybersecurity ของภาคส่วนต่าง ๆ และสร้างความพร้อมในการดูแลตนเองของแต่ Sector

5 ให้กลไกในการดูแล Critical Infrastructures ที่สำคัญกับการให้บริการสาธารณะ



ดูแลให้ดิจิทัลเป็นไปตามหลัก C.I.A.

เตรียมพร้อมรับมือ Cyber Crime ที่มีแนวโน้มความรุนแรง ความเสียหาย ปริมาณมากขึ้น

ขอบเขตของกฎหมาย

- นิยาม “ความมั่นคงปลอดภัยไซเบอร์”
- การดูแลความมั่นคงปลอดภัยไซเบอร์ กับความมั่นคงทางทหาร

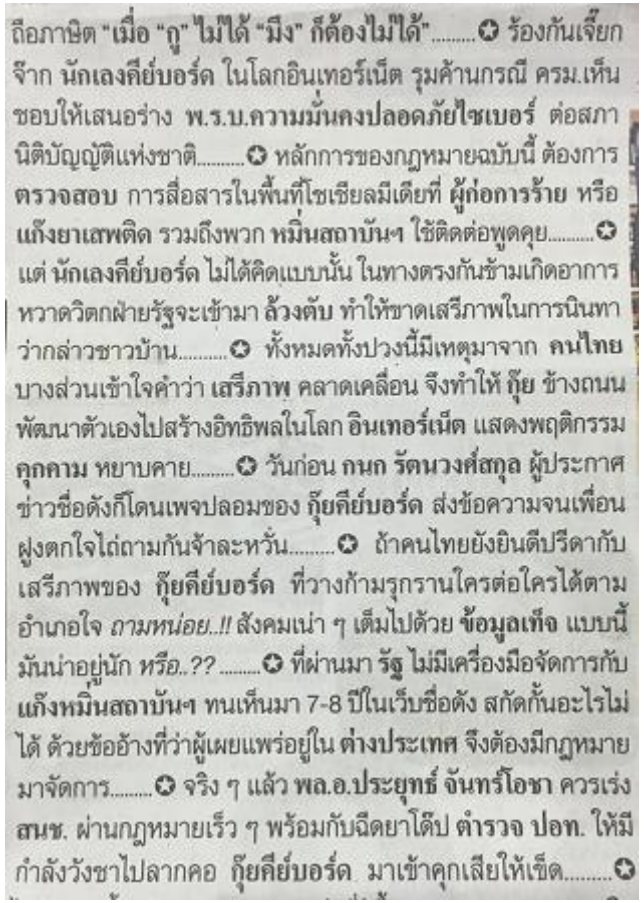
คณะกรรมการ & สำนักงาน

- องค์ประกอบคณะกรรมการที่เหมาะสม
- สำนักงาน Security & Policy

อำนาจพนักงานเจ้าหน้าที่

- การเข้าถึงข้อมูลการติดต่อสื่อสาร – ทำได้หรือไม่เพียงใด?
- มาตรการตรวจสอบถ่วงดุลการใช้อำนาจของพนักงานเจ้าหน้าที่ : Check & Balance

ทุกความเห็นและข้อเสนอแนะมีคุณค่าควรรับฟัง



ถือภาษิต "เมื่อ "กู" ไม่ได้ "มึง" ก็ต้องไม่ได้"..... ✪ ร้องกันเจี๊ยก จ๊าก นักเลงคีย์บอร์ด ในโลกอินเทอร์เน็ต รุมค้านกรณี ครม.เห็นชอบให้เสนอร่าง พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ ต่อสภานิติบัญญัติแห่งชาติ..... ✪ หลักการของกฎหมายฉบับนี้ ต้องการตรวจสอบ การสื่อสารในพื้นที่โซเชียลมีเดียที่ ผู้ก่อการร้าย หรือแก๊งยาเสพติด รวมถึงพวก หมิ่นสถาบันฯ ใช้ติดต่อพูดคุย..... ✪ แต่ นักเลงคีย์บอร์ด ไม่ได้คิดแบบนั้น ในทางตรงกันข้ามเกิดอาการหวาดวิตกฝ่ายรัฐจะเข้ามา ล้วงตับ ทำให้ขาดเสรีภาพในการนินทาว่ากล่าวชาวบ้าน..... ✪ ทั้งหมดทั้งปวงนี้มีเหตุมาจาก คนไทยบางส่วนเข้าใจคำว่า เสรีภาพ คลาดเคลื่อน จึงทำให้ กุ๊ย ข้างถนนพัฒนาตัวเองไปสร้างอิทธิพลในโลก อินเทอร์เน็ต แสดงพฤติกรรมคุกคาม หยาบคาย..... ✪ วันก่อน กนก รัตนวงศ์สกุล ผู้ประกาศข่าวชื่อดังก็โดนเพจปลอมของ กุ๊ยคีย์บอร์ด ส่งข้อความจนเพื่อนฝูงตกใจไล่ถามกันจ้าละหวั่น..... ✪ ถ้าคนไทยยังยินดีปรีดากับเสรีภาพของ กุ๊ยคีย์บอร์ด ที่วางก้ามรุกรานใครต่อใครได้ตามอำเภอใจ *ถามหน่อย..!!* สังคมเน่า ๆ เต็มไปด้วย ข้อมูลเท็จ แบบนี้มันน่าอยู่นัก *หรือ..??*..... ✪ ที่ผ่านมา รัฐ ไม่มีเครื่องมือจัดการกับแก๊งหมิ่นสถาบันฯ ทนเห็นมา 7-8 ปีในเว็บชื่อดัง สกัดกั้นอะไรไม่ได้ ด้วยข้ออ้างที่ว่าผู้เผยแพร่อยู่ใน ต่างประเทศ จึงต้องมีกฎหมายมาจัดการ..... ✪ จริง ๆ แล้ว พล.อ.ประยุทธ์ จันทร์โอชา ควรเร่ง สนช. ผ่านกฎหมายเร็ว ๆ พร้อมกับฉีดยาโด๊ป ตำรวจ ปอท. ให้มีกำลังวังชาไปลากคอ กุ๊ยคีย์บอร์ด มาเข้าคุกเสียให้เข็ด..... ✪

NGOล่าชื่อต้าน10กม.ดิจิทัล

ไทยโพสต์ ● "ประยุทธ์" ระบุเรื่องใดที่อยู่ในกระบวนการให้ผู้รับผิดชอบดำเนินการจนจบ ย้ำพร้อมรับฟังความเห็นประชาชน แต่ต้องฟังรัฐบาลด้วย เครือข่ายพลเมืองเน็ตรันแคมเปญรณรงค์ลงชื่อ "หยุดชุดกฎหมายความมั่นคงดิจิทัล" ชี้ละเมิดสิทธิเสรีภาพผูกาดการเข้าถึงทรัพยากร จี้หน่วยงานที่เกี่ยวองทบทวนและระงับร่างกฎหมาย

เมื่อวันศุกร์ พล.อ.ประยุทธ์ จันทร์ชา นายกรัฐมนตรีและหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) กล่าวในรายการคืนความสุขให้คนในชาติว่า เรื่องใดที่อยู่ในกระบวนการของผู้ที่รับผิดชอบอยู่แล้ว ไม่ว่าจะเป็นการบริหารราชการแผ่นดินของรัฐบาล ของคณะรักษาความสงบแห่งชาติ สภาปฏิรูปแห่งชาติ (สปช.) สภานิติบัญญัติแห่งชาติ (สนช.) และกระบวนการยุติธรรม นั้น อยากให้ผู้ที่มีหน้าที่และมีความรับผิดชอบโดยตรงนั้น ได้ดำเนินการไปจนกว่าจะจบกระบวนการ ประชาชนอย่างพวกเราก็เพียงแต่ติดตามอย่างมีสติ มีเหตุ มีผล สติปัญญาความรู้ ใคร่ครวญให้ถูกต้อง ให้ทุกอย่างต้องเป็นอุปสรรคกับการแก้ปัญหาเศรษฐกิจ ทั้งในภาคใหญ่ของประและปัญหาของประชาชนในส่วนของการเกษตร และอื่นๆ ด้วย ก็มีประเดือดร้อนอยู่หลายส่วนด้วยกัน

"สำหรับการมีส่วนร่วมของประภาคประชาสังคม และอื่นๆ นั้น

อ่านต่อหน้

NCSC

ขอบเขตอำนาจหน้าที่ของคณะกรรมการชุดนี้จะให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในมิติทางความมั่นคงทางการทหาร การทำความร่วมมือระหว่างประเทศเพื่อปกป้องภัยคุกคามไซเบอร์ การรักษาความสงบเรียบร้อยภายในประเทศและการสร้างความมั่นคงทางเศรษฐกิจ ดังนั้น **อำนาจหน้าที่ของคณะกรรมการจึงไม่ครอบคลุมถึงการกระทำความผิดที่เกี่ยวข้องกับเนื้อหา (content)** ในรูปของการกระทำความผิดฐานหมิ่นประมาท การหลอกลวงหรือฉ้อโกงประชาชน ที่เผยแพร่ผ่านสื่อเทคโนโลยีสารสนเทศและการสื่อสารในรูปแบบต่าง ๆ อันเป็นฐานความผิดที่อยู่ภายใต้ขอบเขตของกฎหมายที่มีโทษทางอาญาหรือกฎหมายอื่นที่เกี่ยวข้องและอยู่ภายใต้การดำเนินการของหน่วยงานในสายกระบวนการยุติธรรมตามปกติ **ทั้งนี้ เพื่อมิให้มีผลเป็นการลดบทบาทและความสำคัญในภารกิจหลักของคณะกรรมการที่มุ่งหวังให้เป็นคณะกรรมการที่ทำหน้าที่ในการกำหนดนโยบายในการรับมือกับความเสี่ยงหรือภัยคุกคามทางไซเบอร์เป็นสำคัญ**

คำสั่งสำนักนายกรัฐมนตรี

ที่ ๓๖๖ /๒๕๕๕

เรื่อง แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee)

โดยที่ปัจจุบันพัฒนาการทางเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงอย่างรวดเร็ว มีการใช้เทคโนโลยีการติดต่อสื่อสารความเร็วสูงแบบมีสายและเทคโนโลยีแบบไร้สาย ประกอบกับจำนวนการใช้คอมพิวเตอร์ โทรศัพท์เคลื่อนที่ อินเทอร์เน็ตที่ใช้ในการติดต่อสื่อสาร หรือใช้ในการทำธุรกรรมต่างๆ มีแนวโน้มเพิ่มจำนวนสูงขึ้น จึงก่อให้เกิดสภาพแวดล้อมที่เอื้อต่อการกระทำความผิดที่อาศัยกลไกความก้าวหน้าทางเทคโนโลยีสารสนเทศในการสร้างความเสียหายจนนำมาซึ่งปัญหาอาชญากรรมหรือปัญหาสังคมในหลายรูปแบบ

NCSC ม. 35 ตรวจสอบโดยศาล

มาตรา ๓๕ เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการ มีอำนาจดังต่อไปนี้

(๑) มีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการปฏิบัติการตามพระราชบัญญัตินี้

(๒) มีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช.

(๓) เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

การดำเนินการตาม (๓) ให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่คณะรัฐมนตรีกำหนด

ร่าง พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- **เหตุผลในการเสนอแก้ไขเพิ่มเติมกฎหมาย**

๑. การบังคับใช้กฎหมายและการตีความยังไม่สอดคล้องตามเจตนารมณ์ของกฎหมาย ซึ่งส่งผลกระทบโดยตรงต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๒. ปัญหาการบังคับใช้กฎหมายในทางปฏิบัติซึ่งจำกัดการใช้อำนาจไว้เฉพาะพนักงานเจ้าหน้าที่ในการใช้อำนาจเฉพาะกรณีที่เป็นความผิดตามพระราชบัญญัตินี้เท่านั้น

๓. การสร้างมาตรการและทางปฏิบัติให้สอดรับกับการรักษาความมั่นคงปลอดภัยเพื่อการขับเคลื่อนระบบเศรษฐกิจดิจิทัลอย่างมีประสิทธิภาพ

ปัญหา / อุปสรรค และข้อเสนอในการแก้ไขปรับปรุงกฎหมาย

ข้อพิจารณา		ข้อเสนอแก้ไขเพิ่มเติม
ขอบเขตการบังคับใช้	Computer Crime or Computer Related Crime	การกำหนดขอบเขตการบังคับใช้ เนื่องจากควรเป็นกฎหมายที่จำกัดเฉพาะการกระทำความผิดต่อคอมพิวเตอร์โดยแท้เท่านั้น
ฐานความผิดในกฎหมาย	ถ้อยคำที่ไม่ชัดเจน ส่งผลต่อการบังคับใช้ที่ผิดไปจากเจตนารมณ์	กฎหมายมาตรา ๑๔ ที่นำไปปรับใช้กับการหมิ่นประมาททางอินเทอร์เน็ต เป็นการบังคับใช้ที่ผิดไปจากเจตนารมณ์ของกฎหมาย
	ช่องว่างที่กฎหมายไม่สามารถจัดการกับการกระทำบางอย่างที่ก่อให้เกิดความเสียหายได้	หลักการเรื่อง spam ซึ่งยังมีข้อจำกัดเรื่องการปกปิดผู้ส่งข้อมูลหรือแหล่งที่มาของข้อมูล
หน้าที่และความรับผิดของผู้ให้บริการ	การกำหนดความรับผิดตามกฎหมายของผู้ให้บริการ	ข้อพิจารณาในการนำหลัก Notice & Takedown มาปรับใช้เพื่อกำหนดมาตรการสำหรับผู้ให้บริการในการพิสูจน์เจตนาในเบื้องต้น
	ปัญหาระยะเวลาและรูปแบบการเก็บ Log file ที่เหมาะสมและมีคุณภาพ	การปรับปรุงหลักเกณฑ์การจัดเก็บ log file ทั้งด้านระยะเวลาการจัดเก็บ และการกำหนดข้อมูลที่จำเป็นต้องจัดเก็บ ให้สอดคล้องกับทางปฏิบัติและความสามารถในการดำเนินการของทุกฝ่ายที่เกี่ยวข้อง

ข้อพิจารณา		ข้อเสนอแก้ไขเพิ่มเติม
การระงับการเผยแพร่ข้อมูล	ข้อโต้แย้งกระบวนการตรวจสอบการใช้อำนาจรัฐว่า กระบวนการตามที่กฎหมายกำหนดเป็นการตรวจสอบอย่างแท้จริงหรือไม่	การทบทวนกระบวนการตรวจสอบการใช้อำนาจ ผู้มีอำนาจพิจารณา และกระบวนการต่อเนื่องภายหลังจากมีคำสั่งระงับการเข้าถึง รวมถึงการพิจารณายกเลิกคำสั่ง
หลักกฎหมายที่สอดคล้องกับสากล	ฐานความผิดที่ยังไม่ครอบคลุมหรือสอดคล้องกับมาตรฐานสากล ซึ่งส่งผลต่อการส่งตัวผู้ร้ายข้ามแดน และการเข้ามาในประเทศเพื่อเป็นแหล่งพักอาศัยในการกระทำความผิด	การพิจารณาเพิ่มเติมฐานความผิดเรื่อง child pornography

ข้อพิจารณา		ข้อเสนอแก้ไขเพิ่มเติม
หน่วยงานบังคับใช้กฎหมาย และพนักงานเจ้าหน้าที่	ขาดหน่วยงานรับผิดชอบซึ่งเป็นศูนย์กลางการปฏิบัติงานอย่างแท้จริง	พิจารณาหน่วยงานซึ่งมีความพร้อมในการปฏิบัติให้เป็นไปตามกฎหมาย เพื่อให้มีศูนย์ปฏิบัติงานอย่างแท้จริง
	พนักงานเจ้าหน้าที่ขาดความรู้ความสามารถในเชิงเทคนิค และขาดความเข้าใจในการบังคับใช้กฎหมาย	การทบทวนคุณสมบัติและการแต่งตั้งพนักงานเจ้าหน้าที่ เพื่อให้ได้บุคลากรที่มีความรู้ความเชี่ยวชาญ และความเข้าใจในการปฏิบัติหน้าที่อย่างเหมาะสม
		การพิจารณากำหนดค่าตอบแทน หรือการสร้างแรงจูงใจให้กับบุคลากรที่มีศักยภาพให้เข้ามาทำงานในภาครัฐ
พยานหลักฐาน	การแชร์พยานหลักฐานสำหรับกรณีที่เป็นการกระทำความผิดตามกฎหมายอื่นยังถูกจำกัด	การปรับปรุงให้เอื้อต่อการช่วยเหลือพนักงานเจ้าหน้าที่ตามกฎหมายอื่นในการรวบรวม จัดเก็บ หรือวิเคราะห์พยานหลักฐาน หรือให้พยานหลักฐานที่ได้จากการดำเนินการตามกฎหมายนี้สามารถนำไปใช้ประกอบการดำเนินคดีตามกฎหมายอื่นได้
	หน่วยงานสนับสนุนด้านการจัดเก็บ รวบรวม และวิเคราะห์พยานหลักฐานดิจิทัล	ควรมีหน่วยงานซึ่งทำหน้าที่สนับสนุนงานด้านการตรวจพิสูจน์และวิเคราะห์พยานหลักฐานดิจิทัล ซึ่งมีความเป็นอิสระและเป็นกลาง ไม่มีส่วนเกี่ยวข้องกับการดำเนินคดี

OECD Guideline 2013

- Privacy management program: ส่งเสริมให้มีแผนการบริหารจัดการกระบวนการคุ้มครอง
- Data security breach notification: การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูล/หน่วยงานที่เกี่ยวข้อง
- Privacy enforcement authorities: ส่งเสริมให้มีหน่วยงานบังคับใช้กฎหมายที่มีความรู้ความเชี่ยวชาญ
- Transborder flows of personal data: สร้างกลไกการโอนข้อมูลที่เอื้ออำนวยต่อการไหลเวียนของข้อมูลระหว่างประเทศ“adequacy model”
- National implementation: พัฒนาความรู้ สร้างความตระหนัก และส่งเสริมมาตรการคุ้มครองแก่เอกชน
- International co-operation and interoperability: ประสานความร่วมมือกับหน่วยงานระหว่างประเทศในการแลกเปลี่ยนข้อมูลเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

Data Controller

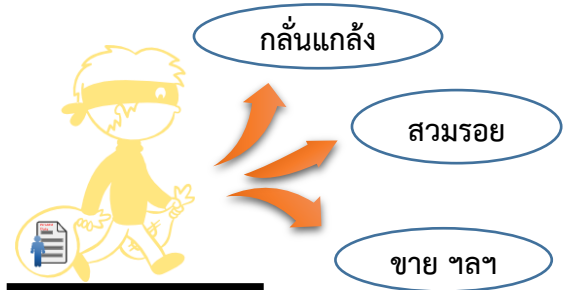
Personal Data

ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

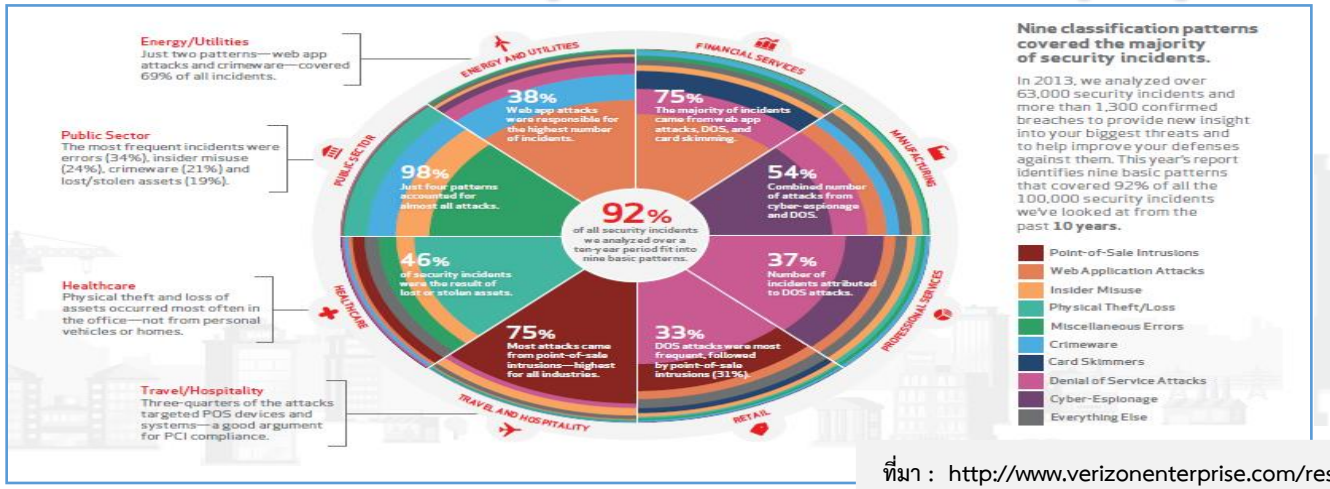
ข้อมูลส่วนบุคคล

- ชื่อ หมายเลข รหัส สิ่งบอกลักษณะตัว
- ข้อมูลสุขภาพ
- ฐานะการเงิน
- ลายพิมพ์นิ้วมือ
- ประวัติอาชญากรรม ฯลฯ

ผู้ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคล ซึ่งรวมถึงการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคล

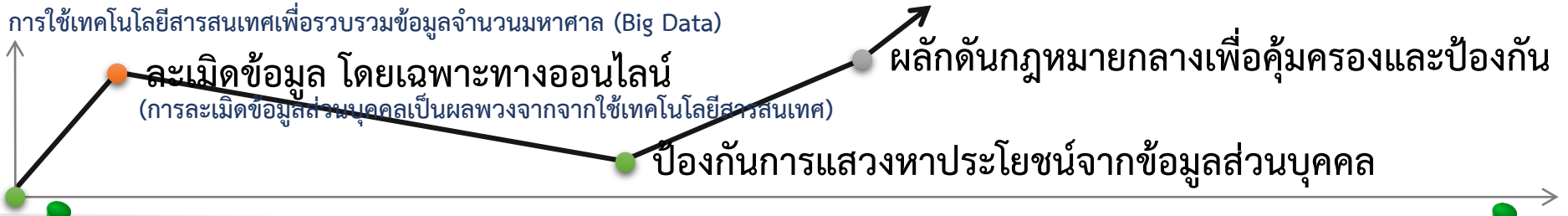


Nine classification patterns covered the majority of security incidents.



ที่มา : http://www.verizonenterprise.com/resources/infographics/ig_Verizon-DBIR-2014_en_xg.pdf

Data Protection Bill



คุ้มครองและป้องกันการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคล

สร้างความพร้อมของภาครัฐในยุคดิจิทัล

ผู้มีความรู้ความเชี่ยวชาญด้าน CyberSecurity กำกับดูแล

สร้างกลไกการดูแลข้อมูลส่วนบุคคลที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์เป็นส่วนใหญ่อย่างเหมาะสม

การบังคับใช้กฎหมาย

- กำหนดมาตรฐานขั้นต่ำสำหรับการคุ้มครอง
- คุ้มครองทั้งบุคคลธรรมดา และนิติบุคคล
- ผู้ควบคุมทั้งรัฐ และเอกชน
- ผู้ควบคุมทั้งบุคคลธรรมดา และนิติบุคคล

คณะกรรมการ

- มี “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งชาติ”
- ช่วยเหลือ/เยียวยาจากการละเมิด
- ส่งเสริม/สร้างความตระหนัก
- พิจารณาข้อพิพาท/การร้องเรียน

มาตรการคุ้มครองข้อมูลส่วนบุคคล

กลไกการคุ้มครองที่ยืดหยุ่นเหมาะสม และสอดคล้องกับสากล

- “แจ้ง” เมื่อเก็บรวบรวม
- “ขอความยินยอม” เมื่อใช้และการเปิดเผย
- สิทธิ “ขอเข้าถึงข้อมูล” ของเจ้าของข้อมูล
- กำหนดหน้าที่ของผู้ควบคุมข้อมูล เพื่อการคุ้มครองที่เหมาะสม
- มาตรการส่งเสริม “เครื่องหมายรับรองข้อปฏิบัติการคุ้มครอง”

หน่วยงานกำกับดูแล

- หน่วยงานเฉพาะทำหน้าที่กำกับดูแลตามที่ คกก. DP มอบหมาย
- หน่วยงานที่มีความรู้ความเชี่ยวชาญด้าน CyberSecurity
- “สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” กำกับดูแล (เช่น KISA ของประเทศเกาหลี)

Data Protection Bill

การคุ้มครอง Standardization

- เฉพาะ “บุคคลธรรมดา” หรือควรรวม “นิติบุคคล” ?
- ข้อมูลส่วนบุคคล “คนตาย” ควรได้รับความคุ้มครอง ?
- ผู้ควบคุมข้อมูล เฉพาะ “ผู้มีอำนาจตัดสินใจในการดำเนินการเกี่ยวกับข้อมูล” หรือเพียงแค่ “ผู้ที่ถือครองข้อมูล” ?
- ใครคือผู้ได้รับการยกเว้นไม่ต้องทำตามกฎหมายนี้ ?

การบังคับใช้

- มาตรฐานขั้นต่ำ หรือ overrule กฎหมายเฉพาะแบบ automatic ?
- Committee ใหญ่เพื่อ Think Tank หรือคล่องตัวเพื่อ operate ?
- จะสร้างแรงจูงใจอย่างไรให้คนไม่รู้สึกว่ากฎหมายเป็นภาระ ?

หลักเกณฑ์คุ้มครอง

- “ข้อมูลส่วนบุคคล” ระบุให้ชัด หรือเปิดให้กว้าง ?
- Definition “Sensitive Data” ควรกำหนดหรือไม่ ?
  (ในร่างกฎหมาย กฎหมายลำดับรอง หรือในกฎหมายเฉพาะ)
- การเก็บรวบรวม เพียง “แจ้ง” หรือควร “ขอความยินยอม”

“การ Balance การใช้อำนาจ ต้องมีการตรวจสอบ
เพื่อประกันสิทธิประชาชน”

“การ communicate และ Public Hearing
จะมีการทำตลอดเส้นทาง”

พัฒนาเศรษฐกิจดิจิทัล
เอกชนดำเนินการ รัฐอำนวยการ