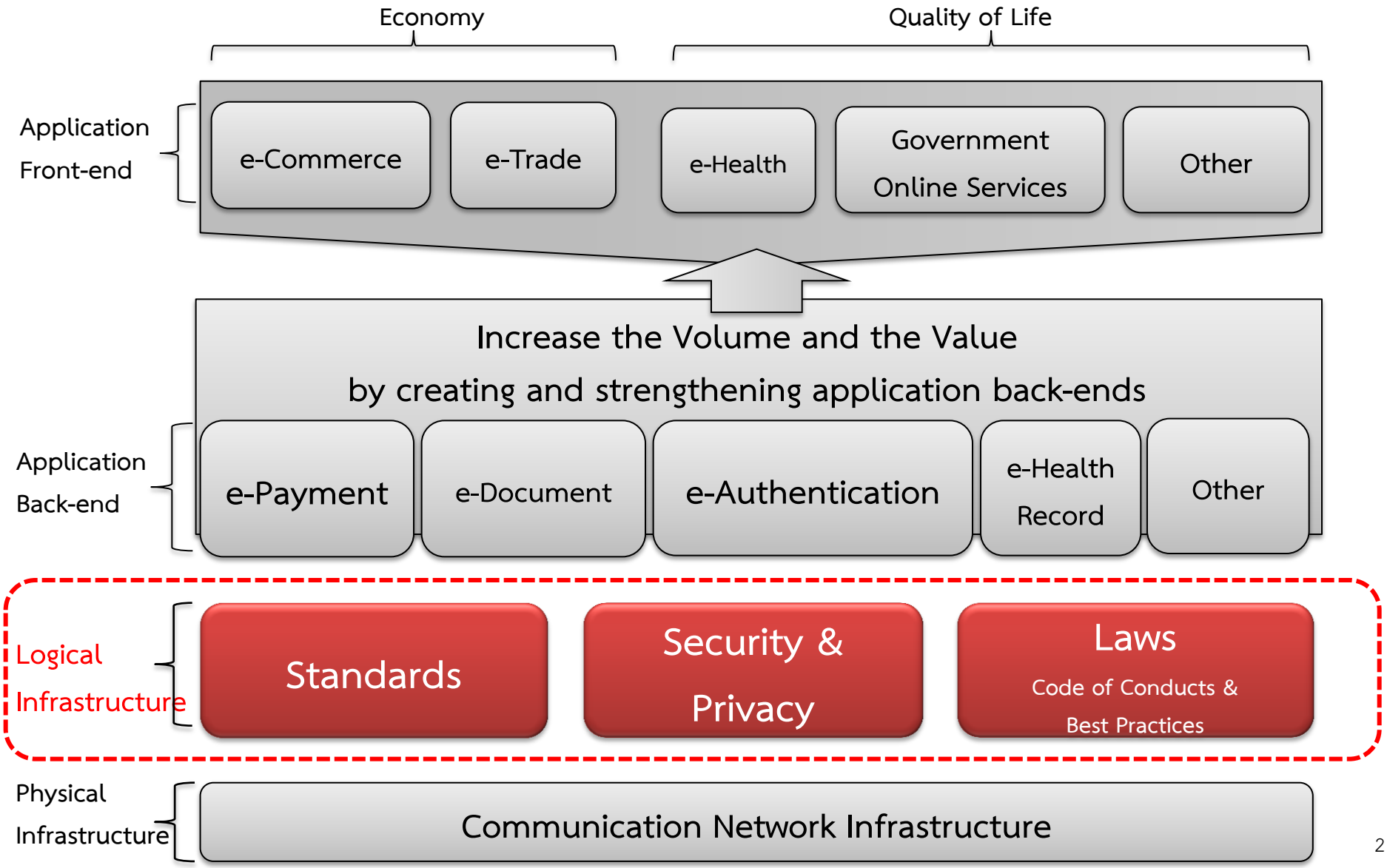
นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐ

สุรางคณา วายุภาพ
ผู้อำนวยการ สพธอ.

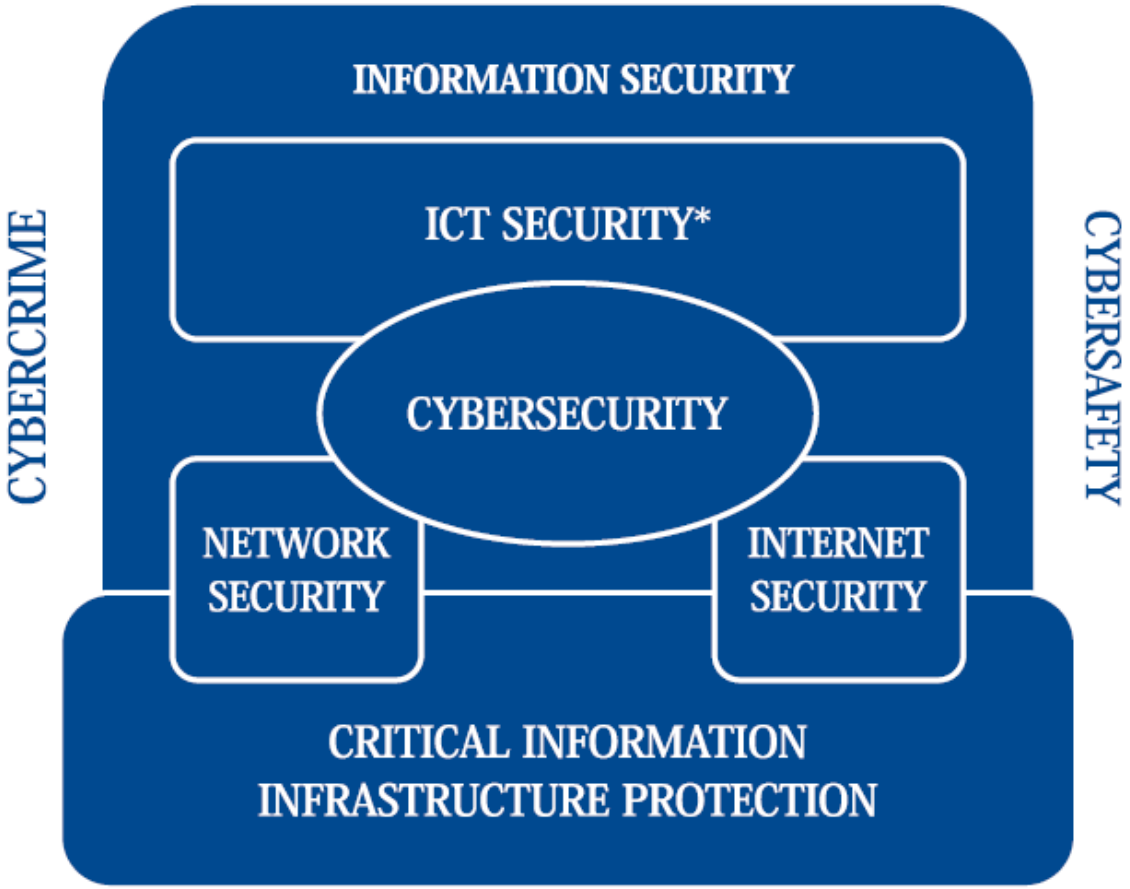
ETDA สพธอ
www.etda.or.th
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
Electronic Transactions Development Agency (Public Organization)

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

“Secure Logical Infrastructure”
เพื่อให้การทำธุรกรรมอิเล็กทรอนิกส์มั่นคงปลอดภัย



ความมั่นคงปลอดภัยไซเบอร์
กับความมั่นคงของ Critical Infrastructure



C.I.A.

- **Confidentiality**
  ความลับ
- **Integrity**
  ความถูกต้องครบถ้วน
- **Availability**
  สภาพพร้อมใช้งาน

*อ้างอิงจาก National Cyber Security Framework Manual. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence และ ISO/IEC 27032:2012 'Information Technology- Security Techniques – Guidelines for Cybersecurity'

Global Challenges

Terminology

Scope

Complexity

Non Boundary

Capacity

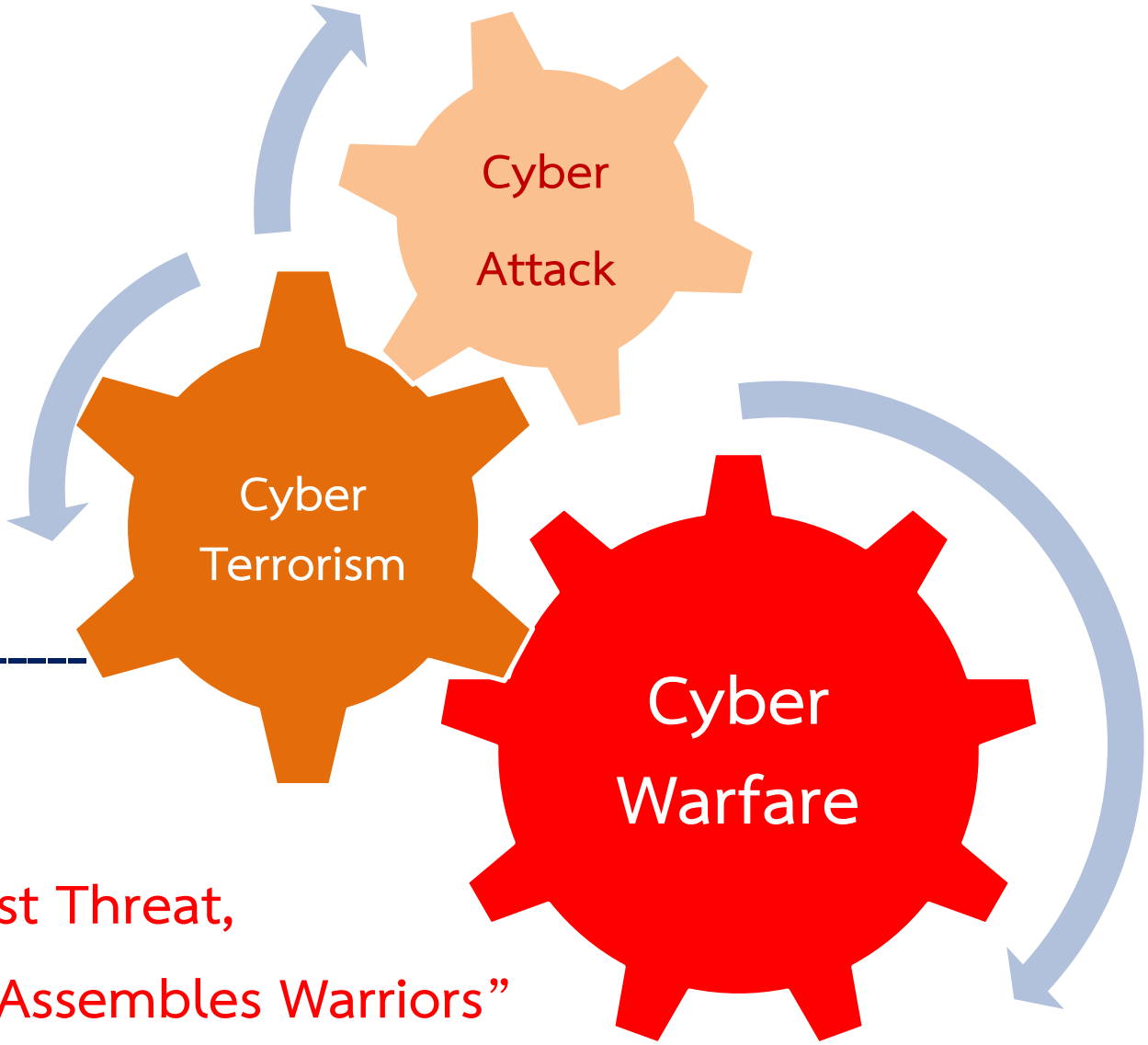
Collaboration

Obama Says

Cyberterrorism

Is Country's Biggest Threat,

U.S. Government Assembles Warriors"



RSA Conference 2014

เวทีระดับโลกด้าน Cybersecurity คาดการณ์อะไร

- *Arthur Coviello, Executive Chairman, RSA Security*

  Cyber conflicts: national security vs. civil liberty and privacy right

- *Scott Charney, Corporate Vice President, Microsoft*

  Microsoft protects Privacy, operates Security and provides Transparency

- *Art Gilliland, HP Senior Vice President*

  In 2013 Global security spending $46B, information breaches increased 20% and individual breaches increased 30%

- Chris Young, Senior Vice President, *Cisco*

  Internet of Things (IoT) 1 billion Internet-connected devices (2013), and there will be 50 billion devices (2020) i.e., a new way for attackers to steal data and threaten business from the vulnerability of these billion devices

Information breaches

Government Surveillance

Advance malware and DDoS

RSA CONFERENCE | Where The World Talks Security

Government Surveillance หรือ Industrial Spy

"If there's information at Siemens that's beneficial to US national interests - even if it doesn't have anything to do with national security - then they'll take that information nevertheless." Edward Snowden, สัมภาษณ์ทาง ARD TV (สหพันธ์สาธารณรัฐเยอรมนี), มกราคม 2014

10 Safest Countries			
Countries	TER	Countries	TER
1. Norway	1.81%	6. U.S.	3.82%
2. Sweden	2.59%	7. Slovenia	4.21%
3. Japan	2.63%	8. Canada	4.28%
4. UK	3.51%	9. Austria	4.27%
5. Switzerland	3.81%	10. Netherlands	4.28%

10 Riskiest Countries			
Countries	TER	Countries	TER
1. Indonesia	23.54%	6. India	15.88%
2. China	21.26%	7. Mexico	15.66%
3. Thailand	20.78%	8. UAE	13.67%
4. Philippines	19.81%	9. Taiwan	12.66%
5. Malaysia	17.44%	10. Hong Kong	11.47%

Threat exposure rate (TER) : Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period – Source : Security Threat Report 2013 - SophosLabs

Cybersecurity Ranking 2013

ETDA สพธอ www.etda.or.th

Ranking		
1	ISRAEL	8.04
2	UAE	7.84
3	SWEDEN	7.54
4	LUXEMBOURG	7.47
5	AUSTRIA	7.30
6	DENMARK	7.30
7	FINLAND	7.26
8	LITHUANIA	7.23
9	MALAYSIA	7.21
10	TAIWAN	7.18
11	FRANCE	7.18
12	SWITZERLAND	7.14
13	SINGAPORE	7.08
14	QATAR	7.05
15	CANADA	6.92
16	POLAND	6.87
17	GERMANY	6.85
18	ESTONIA	6.84
19	BELGIUM	6.67
20	NORWAY	6.57
21	IRELAND	6.55
22	HONG KONG	6.50
23	LATVIA	6.31
24	NETHERLANDS	6.21
25	AUSTRALIA	6.18
30	UNITED KINGDOM	5.77
31	USA	5.62
32	SPAIN	5.58
33	NEW ZEALAND	5.56
34	SLOVAK REPUBLIC	5.55
35	CROATIA	5.53
36	PORTUGAL	5.50
37	SOUTH AFRICA	5.40
38	KOREA	5.39
39	JORDAN	5.37
40	JAPAN	5.37
41	GREECE	5.36
42	CHINA MAINLAND	5.23
43	TURKEY	5.21
44	CHILE	5.19
45	MEXICO	5.18
46	INDONESIA	5.10
47	ITALY	5.08
48	THAILAND	4.93
49	INDIA	4.78
50	PHILIPPINES	4.77

ประเทศไทยอยู่ในอันดับที่ 48 จาก 60 ประเทศ

IMD World Competitiveness Rankings จัด Ranking ด้าน Cybersecurity โดยประเมินจากการให้ความสำคัญด้าน Cybersecurity ขององค์กรในแต่ละประเทศ

http://www.imd.org/wcc/news-wcy-ranking/

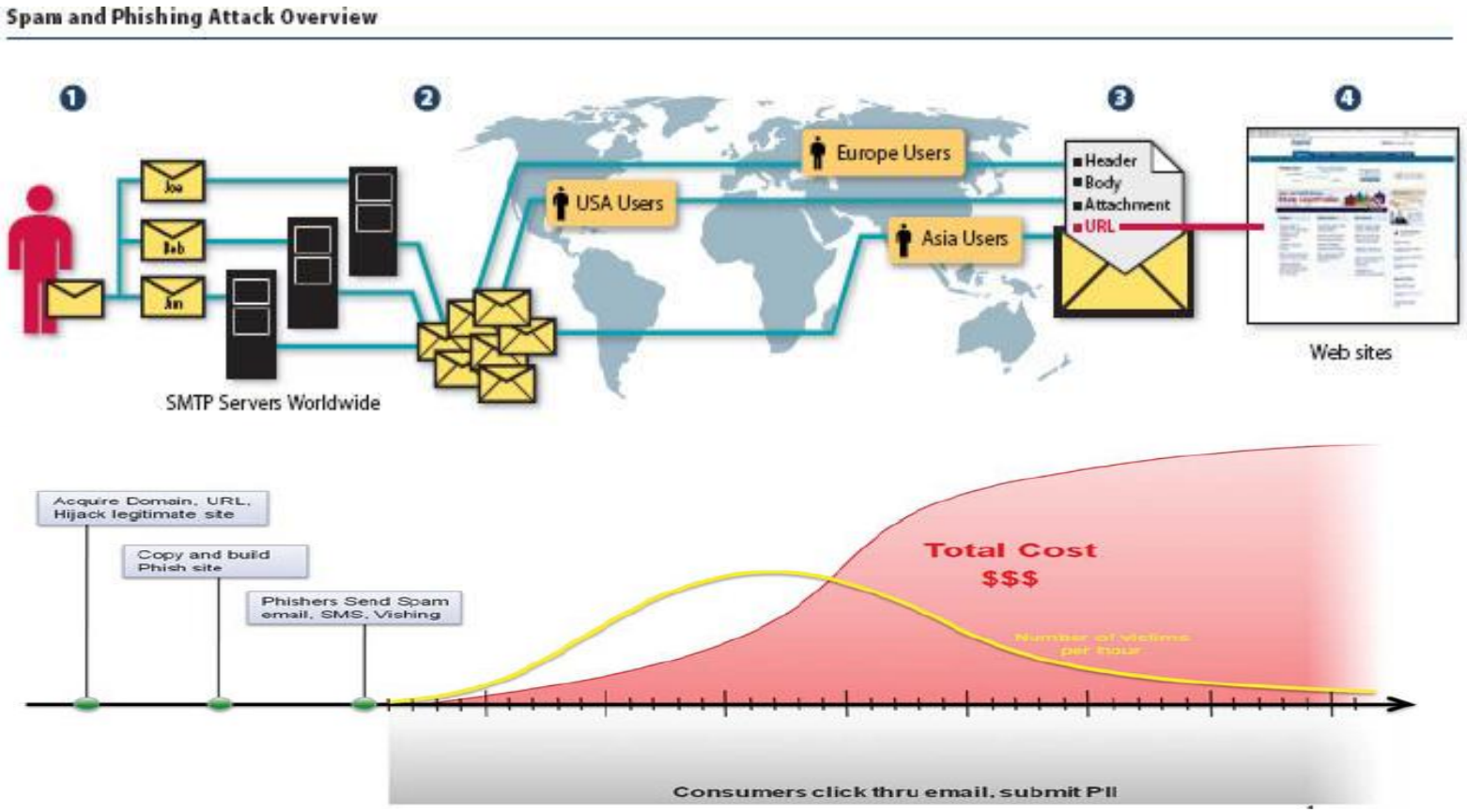
ประเทศที่มีสัดส่วน Phishing ต่อโดเมนเนม ของประเทศ สูงสุด 10 อันดับแรก

อันดับ	1H 2553	2H 2553	1H 2554	2H 2554	1H 2555	2H 2555	1H 2556	2H 2556
1	ไทย (62)	ไทย (65)	โมรอคโค (182)	โทเคลาอู (.tk) (7316)	ชิลี (831)	ไทย (136)	ปาเลา (109)	เนปาล (88)
2	เกาหลีใต้ (989)	อิหร่าน (169)	ไทย (89)	อินเดีย (1314)	เปรู (115)	ฮังการี (1192)	เนปาล (97)	ปาเลา (924)
3	ไอร์แลนด์ (79)	โมรอคโค (34)	โทเคลาอู (.tk) (6214)	ไทย (69)	อินโดนีเซีย (95)	ชิลี (731)	ไทย (125)	ไทย (155)
4	โปแลนด์ (744)	ไอร์แลนด์ (96)	โครเอเซีย (90)	มาเลเซีย (125)	ไทย (77)	เปรู (93)	สโลเวเนีย (196)	ชิลี (807)
5	ชิลี (111)	คาซัคสถาน (2429)	อิหร่าน (201)	เซอร์เบีย (51)	บราซิล (3201)	เอกวาดอร์ (38)	เอกวาดอร์ (48)	เปรู (100)
6	มาเลเซีย (39)	โทเคลาอู (.tk) (28)	เปรู (49)	ชิลี (260)	เอกวาดอร์ (31)	เนปาล (32)	เปรู (107)	กรีซ (407)
7	กรีซ (93)	หมู่เกาะโคโคส (55)	อินเดีย (781)	เปรู (38)	โรมาเนีย (533)	สิงคโปร์ (120)	ซาอุดิอาระเบีย (33)	อินโดนีเซีย (104)
8	โรมาเนีย (156)	อินเดีย (421)	เซอร์เบีย (51)	ฟิลิปปินส์ (20)	อเมริกาใต้ (644)	บราซิล (2435)	ชิลี (357)	เอกวาดอร์ (31)
9	เวียดนาม (48)	มาเลเซีย (55)	นิวซีแลนด์ (351)	บราซิล (1691)	อินเดีย (1351)	อินเดีย (1352)	บราซิล (2669)	บราซิล (3,023)
10	สาธารณรัฐเช็ค (207)	ฮังการี (255)	มาเลเซีย (90)	โครเอเซีย (53)	อุรุกวัย (29)	โมรอคโค (33)	โมรอคโค (33)	โมรอคโค (33)

9

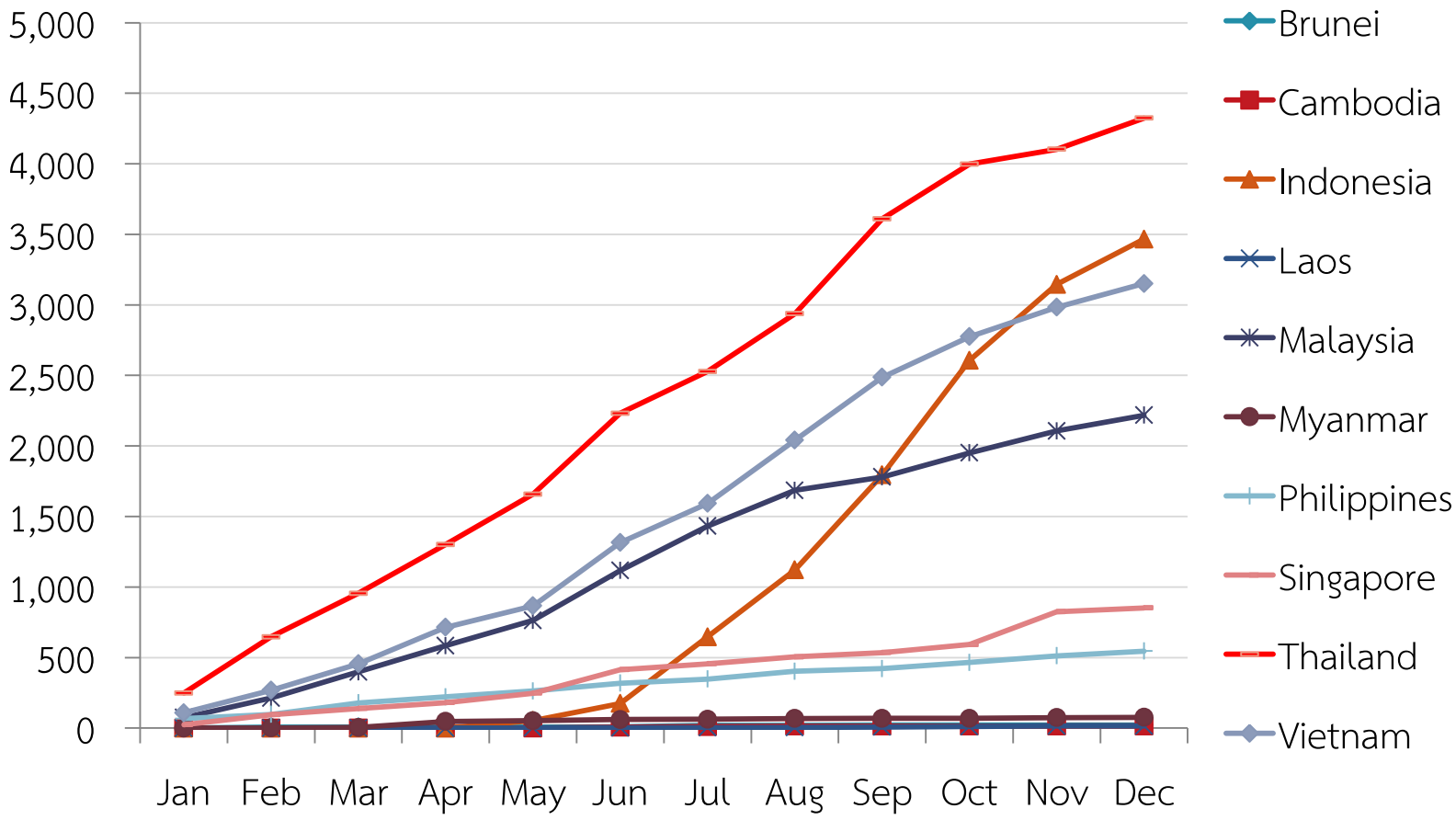
ที่มา: Global Phishing Survey: Trends and Domain Name Use in 1H2010 - 2H2013 โดย An Anti-Phishing Working Group Industry Advisory website: http://apwg.org/resources.html

สถิติภัยคุกคามประเภท Phishing



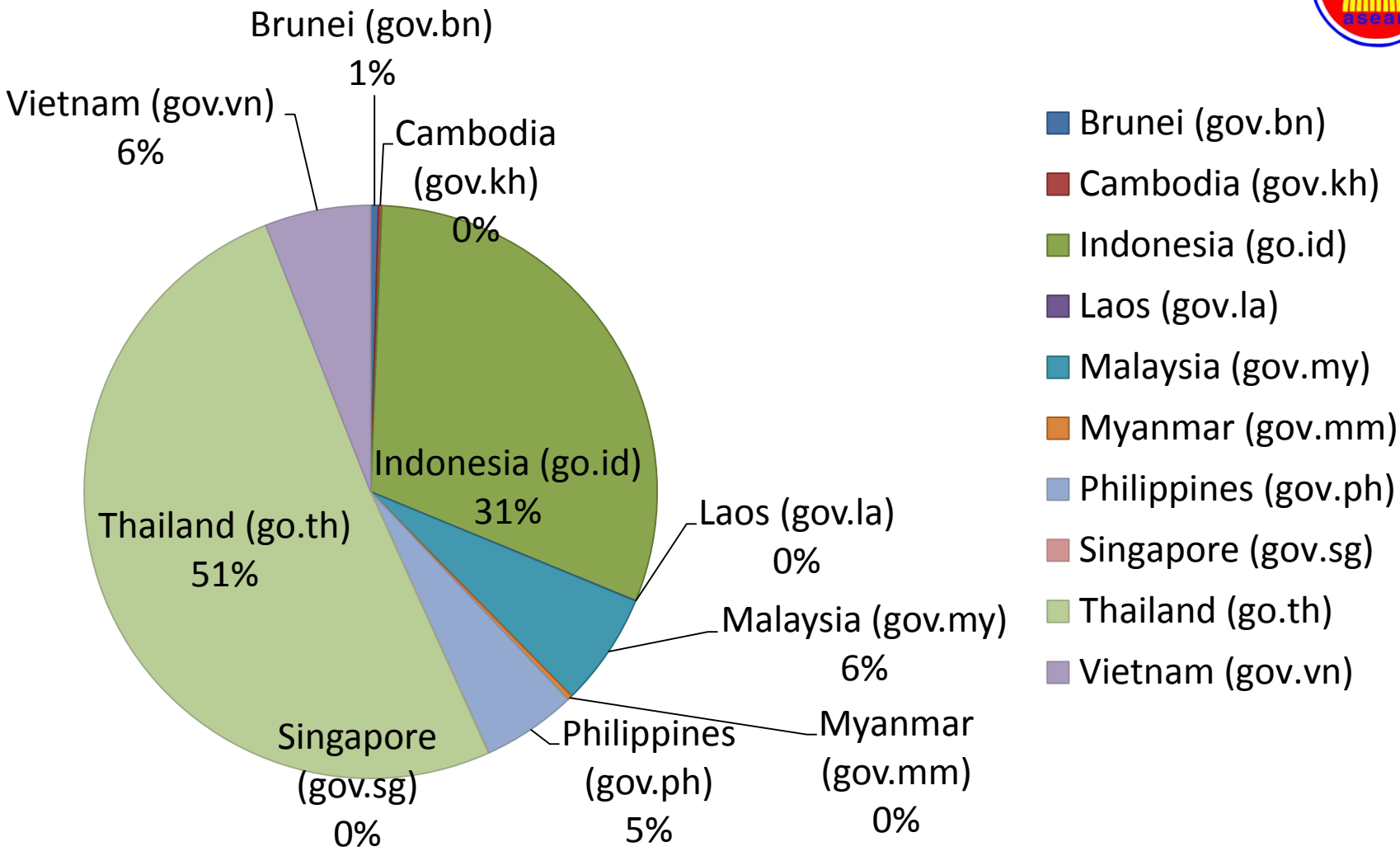
Phishing ที่พบในประเทศไทย เป็นภัยคุกคามที่ส่วนใหญ่เครื่องบริการเว็บหรือเครื่องคอมพิวเตอร์ในประเทศไทยถูกเจาะระบบและใช้เป็น website ฉ้อโกงหลอกลวงต่างๆ

สถิติภัยคุกคามประเภท Web Defacement ในภูมิภาค ASEAN ในปี 2556



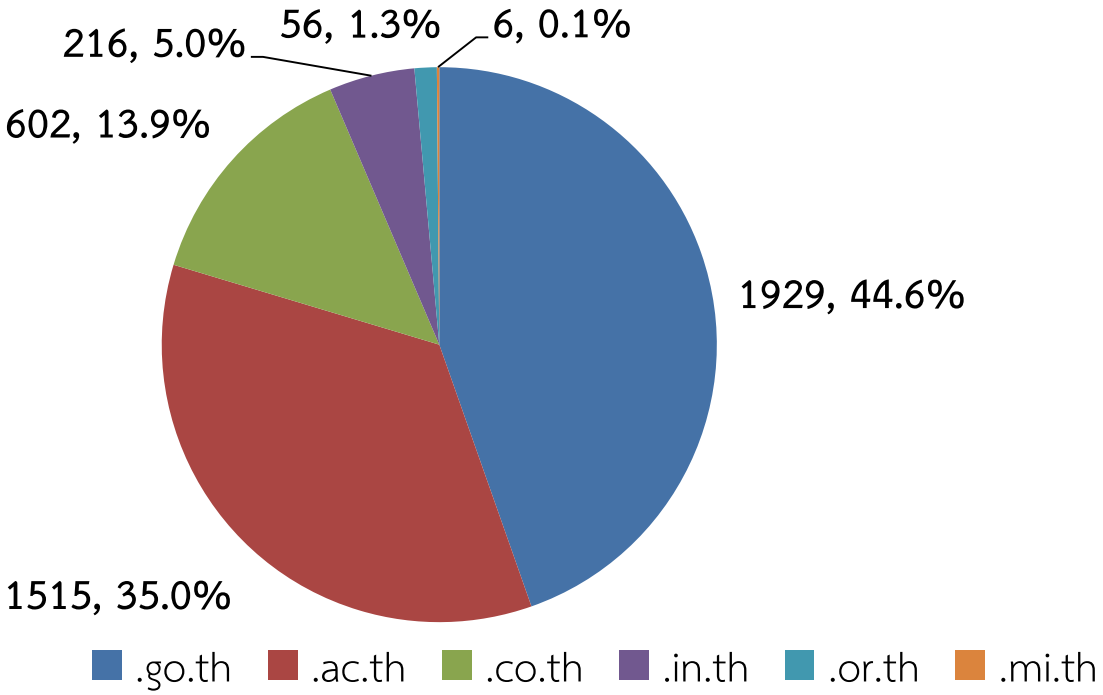
หมายเหตุ: ข้อมูลจากระบบ ThreatWatch ของไทยเซิร์ต ระหว่างเดือน ม.ค. – ธ.ค. 2556

สถิติภัยคุกคามประเภท Web Defacement จำแนกเฉพาะหน่วยงานของรัฐในภูมิภาค ASEAN ในปี 2556



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

สถิติภัยคุกคามประเภท Web Defacement ปี 2556 จำแนกตามประเภทหน่วยงาน (เฉพาะ .th)



จำนวนรายงานที่รับแจ้ง/ตรวจพบทั้งหมด : **4,324** รายการ

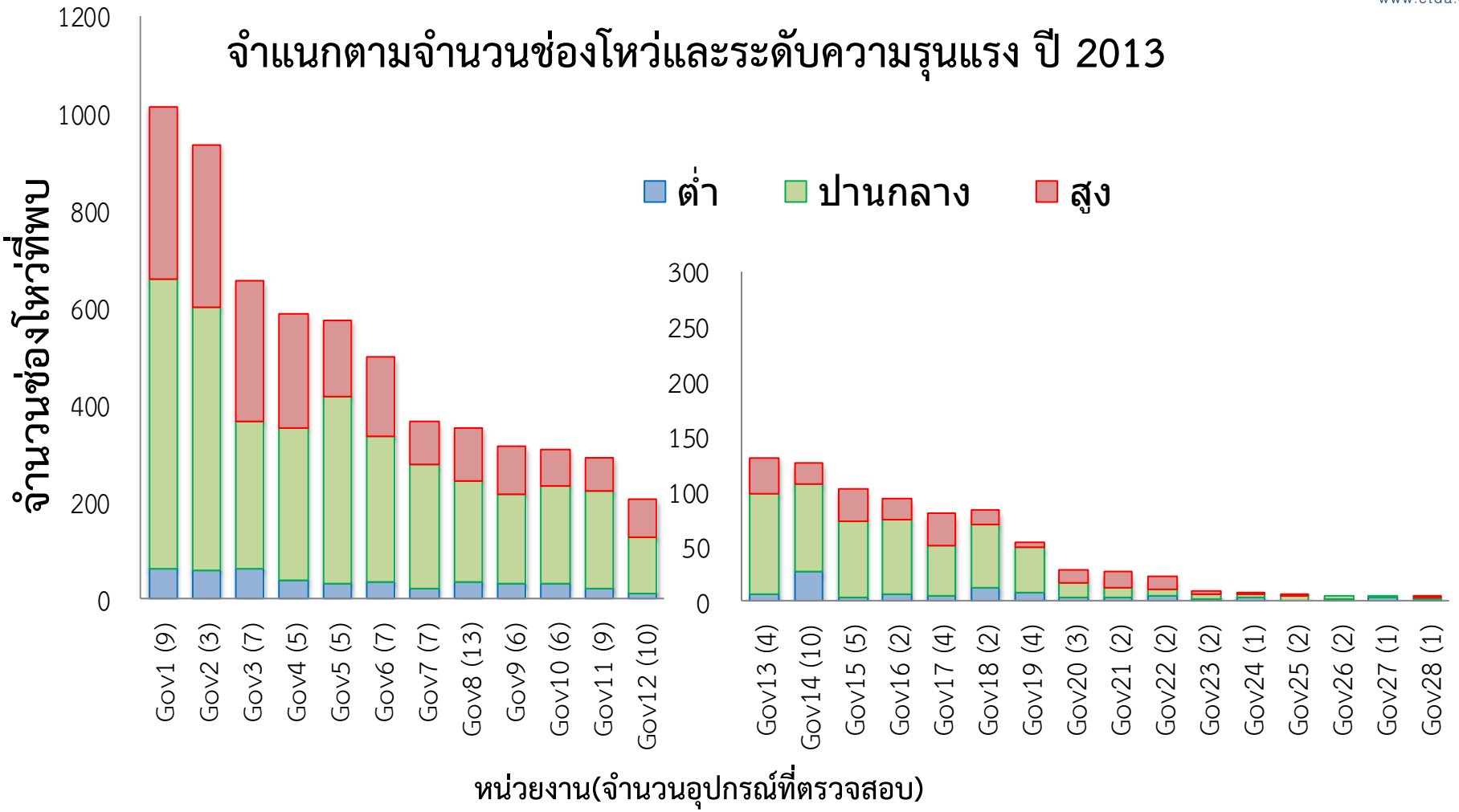
ปี 2556 เว็บไซต์ในประเทศไทย ที่ถูกเจาะระบบและเปลี่ยนแปลงข้อมูล (Web Defacement) มีจำนวน **4,324** รายการ

- หน่วยงานของรัฐ (go.th) มีจำนวนสูงสุด1,929 รายการ (คิดเป็นร้อยละ 44.6)
- สถาบันการศึกษา (ac.th) มีจำนวน 1,515 รายการ (คิดเป็นร้อยละ 35)

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

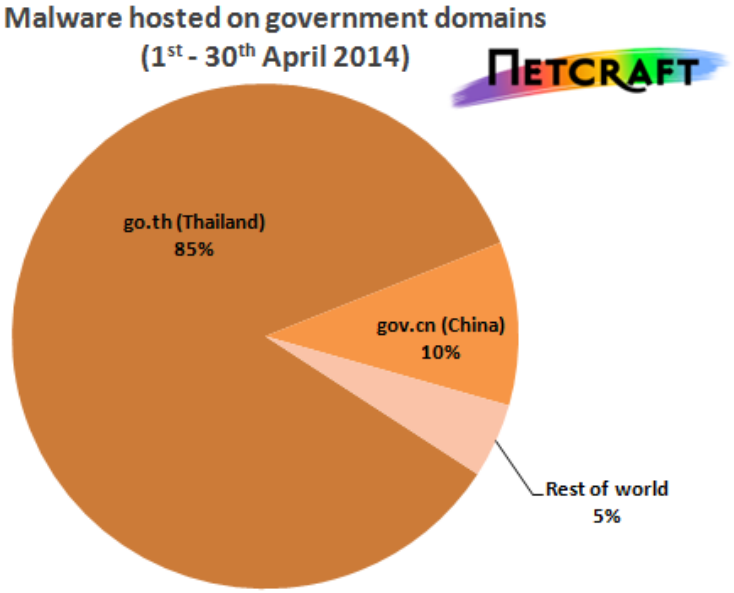
ผลการตรวจสอบช่องโหว่ในระบบสารสนเทศของหน่วยงานภาครัฐ

จำแนกตามจำนวนช่องโหว่และระดับความรุนแรง ปี 2013



- พบช่องโหว่ระดับความรุนแรงสูงในหน่วยงานของรัฐ 26 จากทั้งหมด 28 หน่วยงาน
- ค่าเฉลี่ยจำนวนช่องโหว่ระดับความรุนแรงสูงเป็นจำนวน 15 ช่องโหว่ต่อระบบสารสนเทศ

สถิติภัยคุกคามประเภท Malware บนเว็บไซต์ของรัฐ เดือนเมษายน 2557




Bangkok Post LEARNING ENGLISH

Thai govt websites infested with malware

Published: 7 May 2014 at 19.51 | Viewed: 1,370 | Comments: 0
Online news: Learning From News
Writer: Jon Fernquest
Level switch: Advanced

Thai govt websites have 85% of all government-host malware in world. Malware on Thai Navy computers defraud Visa credit card holders.

เดือนเมษายน 2557 เว็บไซต์ของหน่วยงานของรัฐในประเทศไทยถูกเจาะระบบและใช้เป็นช่องทางในการเผยแพร่มัลแวร์ (Malware URL) สูงสุดเมื่อเทียบกับประเทศอื่นๆ เป็นจำนวนร้อยละ 85

"Government sites typically confer a greater level of trust than other types of websites can, but in Thailand, many are evidently used to host phishing sites and conduct drive-by malware attacks" – NetCraft พ.ค. 2014

http://news.netcraft.com/archives/2014/05/06/thai-government-websites-infested-with-malware.html

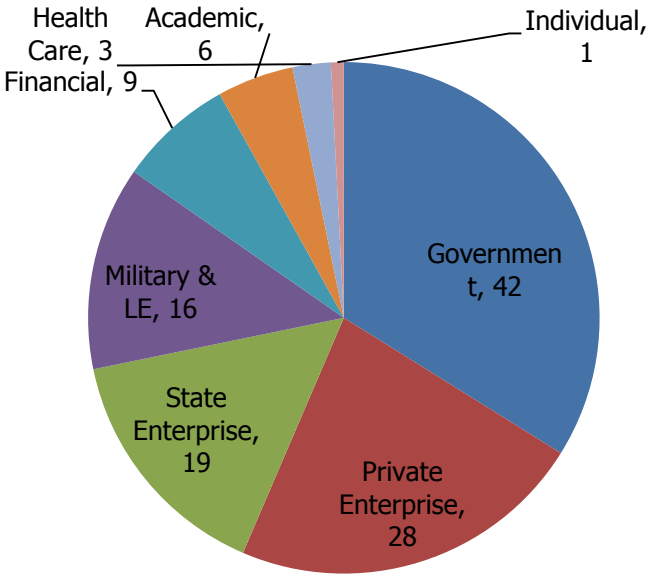
ความพร้อมของผู้เชี่ยวชาญ ด้านความมั่นคงปลอดภัยไซเบอร์

มิถุนายน 2556 สพธอ. และ TISA ร่วมพัฒนาหลักสูตรการรับรองสมรรถนะ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Expert Certification - iSEC) อ้างอิงตามเนื้อหา "IT Essential Body of Knowledge 2008" ซึ่งจัดทำโดย กระทรวงความมั่นคงแห่งมาตุภูมิ สหรัฐอเมริกา เทียบได้กับ Certification ในระดับสากล ซึ่งมี 2 ประเภท ประกอบด้วย

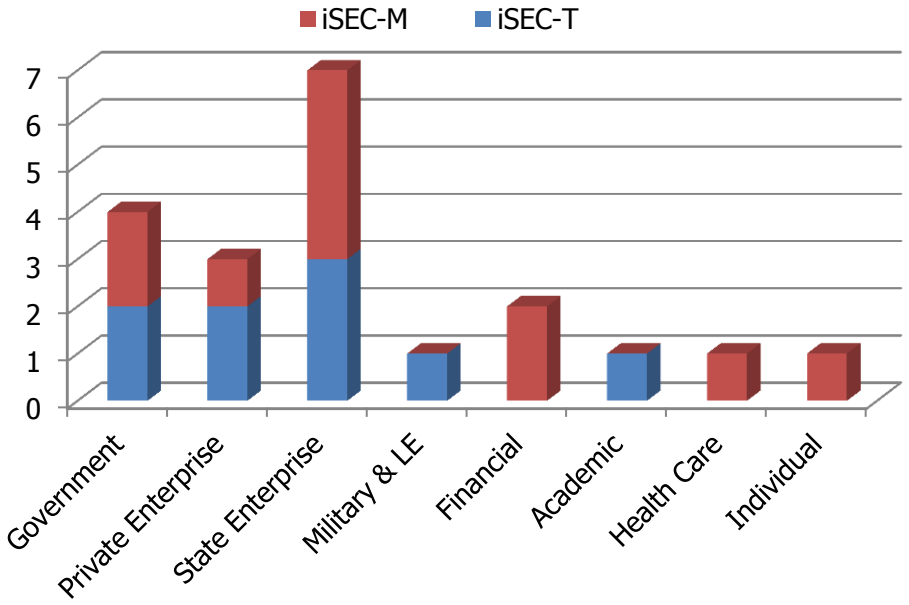
iSEC- Management (iSEC-M) วัดสมรรถนะด้านบริหารจัดการ การมองภาพรวมของแผนงานหรือเทคนิคในการรักษาความมั่นคงปลอดภัย ตอบสนองต่อความเสี่ยงและสภาพภัยคุกคามที่เปลี่ยนไปได้อย่างเท่าทัน

iSEC- Technical (iSEC-T) วัดสมรรถนะด้านดำเนินการเชิงเทคนิค กำหนดกรอบของแผนงานหรือพัฒนาขั้นตอน กระบวนการ และสถาปัตยกรรม เพื่อให้สามารถนำไปสู่การปฏิบัติให้เกิดผลลัพธ์อย่างมีประสิทธิภาพ

จำนวนผู้เชี่ยวชาญที่เข้ารับการอบรมมากกว่า 100 ท่าน และขอเข้ารับการวัดสมรรถนะ 124 ท่าน



จำนวนผู้เชี่ยวชาญที่ผ่านการรับรอง 20 ท่าน



Law Compliance to Minimize Risks & Ensure Reliability

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เพื่อลดความเสี่ยง & สร้างความน่าเชื่อถือ

พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ ๒๕๔๔

Computer Crime Law & Laws of Regulators

มาตรา ๓๕ ธุรกรรมอิเล็กทรอนิกส์ภาครัฐ

พ.ร.ฎ. การกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ๒๕๔๙

ประกาศ คกก. เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ ๒๕๕๓

หน่วยงานของรัฐ

มาตรา ๓๕ ข้อกำหนดพื้นฐาน

มาตรา ๒๕ Critical Infra-structure

มาตรา ๒๕ วิธีการแบบปลอดภัย

พ.ร.ฎ. ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ ๒๕๔๙

ISO/IEC 27001:2005 (2013) มาตรฐานความมั่นคงปลอดภัย : C.I.A

National CERT – Center of Command

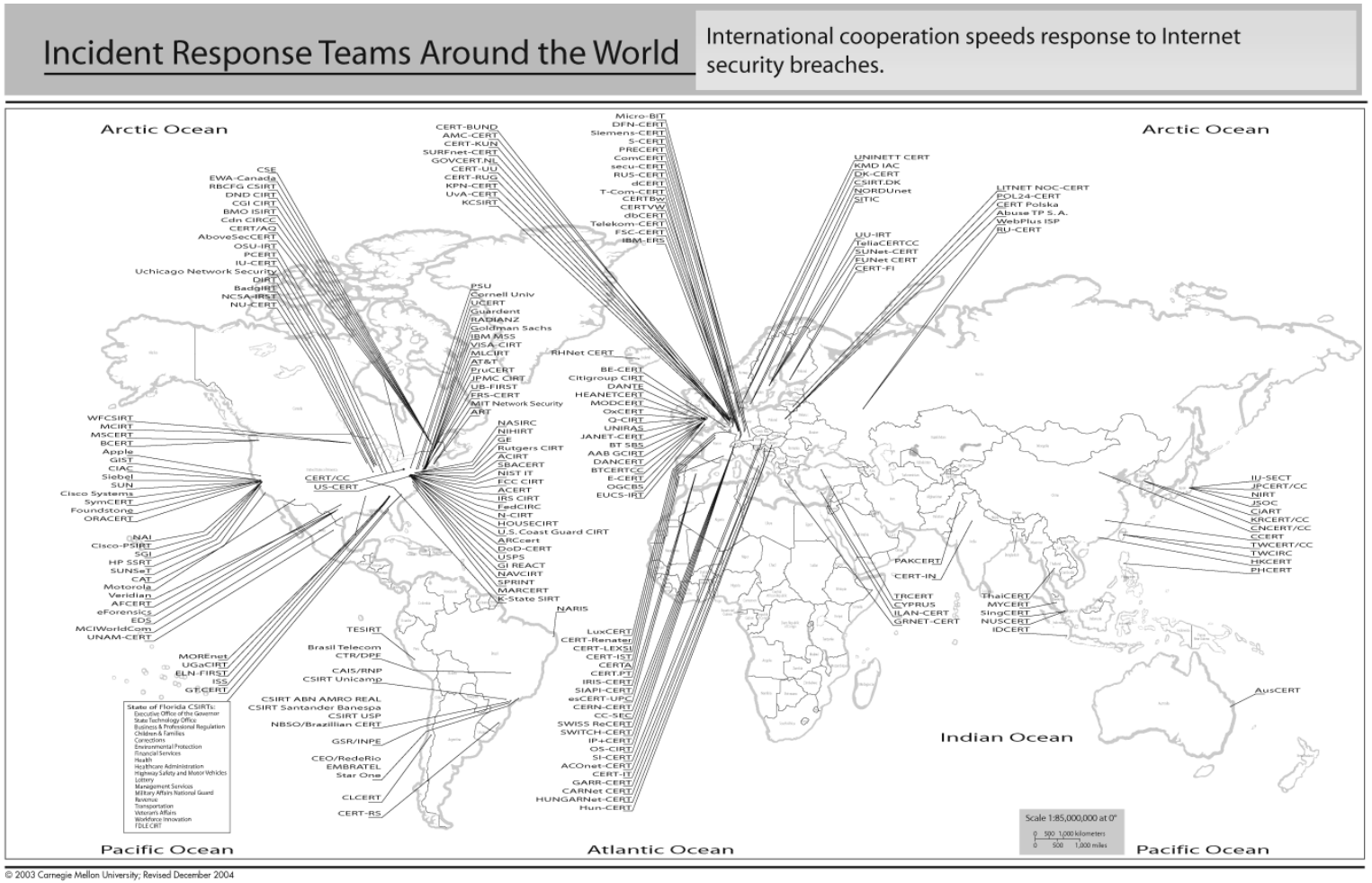
คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
National Cybersecurity Committee

ThaiCERT
Thai Computer Emergency Response Team

- Analyze & recommend แก้ปัญหา Cyber Threats & Digital Forensic
- Response Cyber Attack
- Evaluate cybersecurity readiness
- Warning the vulnerability
- สร้าง culture และ Cybersecurity Public Awareness
- Incidents Drill ซ้อมรับมือ & Capacity Building
- สนับสนุนการจัดตั้ง CERT ใน sectors ต่างๆ เพื่อประสานการทำงานกับ National CERT
- Global Collaboration & Coordination
- เป็น Contact points ทั้งในและต่างประเทศ

National Computer Security Incident Response Teams (CSIRT) CENTRAL REGION INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) WEBINAR, SEI, Carnegie Mellon University

เครือข่าย CERT หรือ CSIRT



เครือข่าย CERT มากกว่า 270 หน่วยงาน และ

มี National CERT จำนวน 50 หน่วยงาน

* National Computer Security Response Teams (CSIRT) CENTRAL REGION INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) WEBINAR, SEI, Carnegie Mellon University

Collaboration
ในสายงานด้านความมั่นคงปลอดภัยไซเบอร์

ETDA สพธอ www.etda.or.th

ความสงบสุขของสังคม

ความมั่นคงทางเศรษฐกิจ

- งานกำกับดูแล
- งานด้านกระบวนการยุติธรรม

ความมั่นคงทางการทหาร

- งานป้องกันประเทศ
- งานด้านข่าวกรอง
- งานตั้งรับ & ตอบโต้

Urgent Need

- Center of Command
- ThaiCERT & Sector based CERTs
- Strengthening Capacity & Raising Public Awareness

* นำเสนอในการประชุม คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ มิ.ย. 56

คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

อำนาจหน้าที่ จัดทำนโยบาย/ จัดทำแนวทาง มาตรการ หรือแผนงาน/ ติดตามและประเมินผลการปฏิบัติการตามแนวทาง มาตรการ หรือแผนงาน/ รายงานผลต่อคณะรัฐมนตรี

คณะกรรมการทั้งหมด 27 คน
กรรมการโดยตำแหน่ง 22 และกรรมการผู้ทรงคุณวุฒิ 5 คน

สายงานด้านความมั่นคงและกลาโหม

สายงานด้านเศรษฐกิจและคุณภาพชีวิต

สายงานป้องกันและปราบปรามการกระทำความผิด
สตช.

แผน/นโยบายความมั่นคงปลอดภัยไซเบอร์ประเทศต่างๆ

ETDA สพธอ www.etda.or.th

แนวทางการกำหนดแผน/นโยบายที่สำคัญของแต่ละประเทศ คือ

๑. การกำหนดแผนบนพื้นฐานของ Availability, Integrity และ Confidentiality ที่เชื่อมโยงกับกฎหมาย/การบังคับใช้กฎหมาย

๒. การจัดตั้ง CERT เพื่อเป็นหน่วยงานหลักในทางปฏิบัติของแต่ละประเทศ

๓. การดำเนินงานจะครอบคลุมทั้งภาคเอกชน ภาครัฐ และประชาชน (บางประเทศเพิ่มกลุ่ม Military)

๔. การกำหนดนโยบายที่ส่งเสริมการแบ่งปันข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องเพื่อช่วยในการวางแผนรับมือกับภัยได้ทันท่วงที

๕. การกำหนดกลุ่มธุรกิจ Critical Infrastructure ที่ชัดเจน และมีนโยบายเฉพาะเพื่อรองรับ

๖. แผนการพัฒนาบุคลากรจะควบคู่ไปกับการสร้าง Awareness

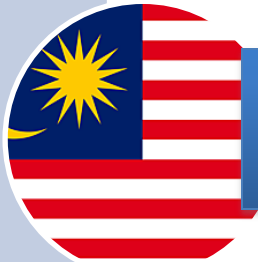
๗. การสนับสนุน R&D ด้าน Security

ออสเตรเลีย

2009 Cyber Security Strategy โดย Australian Government ร่วมกับ CSOC (CERT Australia and the Cyber Security Operations Center)

เกาหลีใต้

Korean Cybersecurity Framework โดยรัฐบาล (National Cybersecurity Strategy Council) ร่วมกับ Ministry of National Defense/KrCERT



มาเลเซีย

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

สิงคโปร์

Infocomm Security Masterplan 2 (MP2) ภายใต้แผน iN2015 โดย Info-communications Development Authority of Singapore (IDA) ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

นโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๕ – ๒๕๕๙ (สมช.)

ส่วนที่ (๑) นโยบายที่มีความสำคัญเพื่อเสริมสร้างความมั่นคงที่เป็นแก่นหลักของชาติ

ประเด็นนโยบายที่ ๑ การเสริมสร้างความมั่นคงของสถาบันหลัก
ประเด็นนโยบายที่ ๒ สร้างความเป็นธรรมและความสมานฉันท์
ประเด็นนโยบายที่ ๓ แก้ไขและป้องกันปัญหาการก่อความไม่สงบและการใช้ความรุนแรงในจังหวัดชายแดนภาคใต้

ส่วนที่ (๒) นโยบายความมั่นคงแห่งชาติทั่วไป

ประเด็นนโยบายที่ ๑ เสริมสร้างเสถียรภาพและภูมิคุ้มกันความมั่นคงและการจัดการภัยคุกคาม
- แนวนโยบาย ๑.๑ พัฒนาระบบ กลไก และมาตรการเพื่อสร้างความเข้มแข็งในการป้องกันและแก้ไขปัญหาการก่อการร้ายและอาชญากรรมข้ามชาติ
- แนวนโยบาย ๑.๒ แก้ไขปัญหาผู้หลบหนีเข้าเมืองทั้งระบบ
- แนวนโยบาย ๑.๓ เสริมสร้างความมั่นคงบริเวณชายแดน
- แนวนโยบาย ๑.๔ ดำเนินการป้องกันและรักษาผลประโยชน์ของชาติทางทะเล
- แนวนโยบาย ๑.๕ เสริมสร้างความมั่นคงของชาติจากภัยยาเสพติด
- แนวนโยบาย ๑.๖ เสริมสร้างความมั่นคงของชาติจากภัยทุจริตคอร์รัปชั่น
- แนวนโยบาย ๑.๗ รักษาความมั่นคงทางเทคโนโลยีสารสนเทศ
  - ๑.๗.๑ เสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ (สพธอ./ก.ไอซีที*)
  - ๑.๗.๒ ปรับปรุงกลไกการบังคับใช้กฎหมาย (สำนักงานตำรวจแห่งชาติ*)
  - ๑.๗.๓ พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ (ก.ไอซีที*)

ประเด็นนโยบายที่ ๒ เสริมสร้างและพัฒนาศักยภาพการป้องกันประเทศ
ประเด็นนโยบายที่ ๓ พัฒนาความพร้อมเพื่อเสริมสร้างความมั่นคง
ประเด็นนโยบายที่ ๔ เสริมสร้างเกียรติภูมิและรักษาผลประโยชน์ของชาติในระบบความสัมพันธ์ระหว่างประเทศ

หมายเหตุ *(๑) * หน่วยงานรับผิดชอบหลัก*
(๒) ได้มีการนำหลักการจากนโยบายความมั่นคงแห่งชาติมาเป็นแนวทางหนึ่งที่สำคัญของ (ร่าง) กรอบนโยบายฯ

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

ETDA สพธอ
www.etda.or.th

(ร่าง) กรอบนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

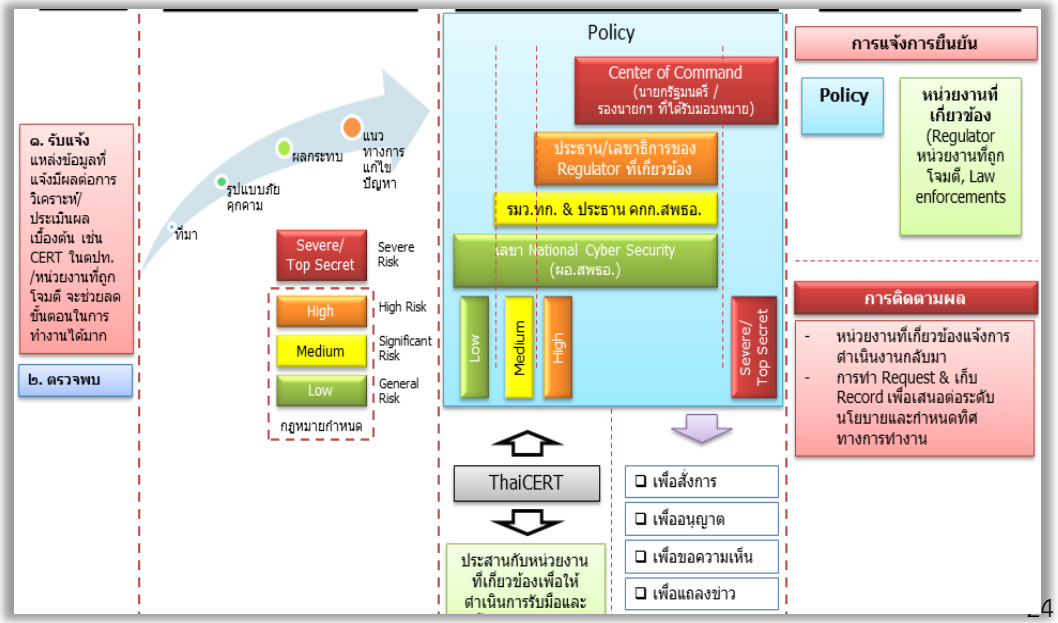
3 Main Strategies

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

(ร่าง) ขั้นตอนการแจ้ง/รับมือเหตุภัยคุกคามที่กระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศ



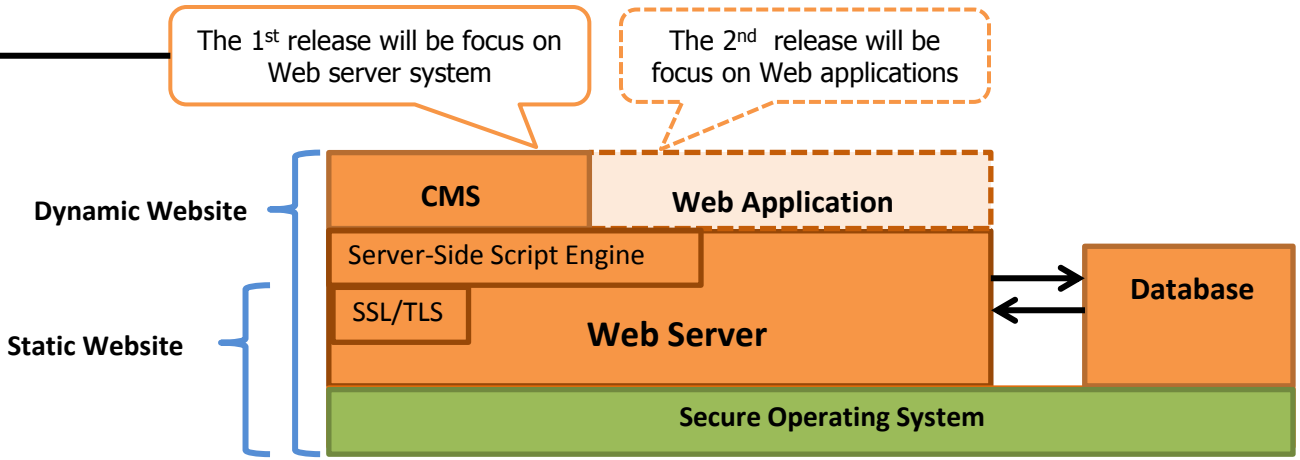
(ร่าง) มาตรฐานความมั่นคงปลอดภัยเว็บไซต์

ETDA สพธอ www.etda.or.th

Content

- Website planning
- Web server installation and configuration
- Data Backup
- Security incident handling
- Assessment form

Scope



Audit types

- Self assessment
- Certified by external party

References

- "Guidelines on Securing Public Web Server," National Institute of Standards and Technology, 2007.
- "SAC 40 Measure to Protect Domain Registration Services Against Exploitation or Misuse," ICANN Security and Stability Advisor Committee (SSAC), 2009
- National Vulnerability Database, "National Vulnerability Database-CVE Static"
- OWASP, "OWASP Top10 2013"

การสร้างความแข็งแกร่งด้าน Cybersecurity

Direction

- National Policy & Plan เพื่อกำนด Direction ที่ชัดเจนระดับนโยบายของประเทศ
- Rule & Regulation Development

Sector - based CERT

- ธนาคาร สถาบันการเงิน และตลาดทุน
- โครงสร้างพื้นฐานสำคัญอื่นๆ
- กำลังพล

Strengthening Collaboration

- การบูรณาการการทำงานร่วมกัน โดยลดข้อจำกัดเรื่อง Jurisdiction & Authority
- National Incident Handling Flow
- National Business Continuity Plan (BCP)

ก้าวต่อไปของ ThaiCERTs ของ ETDA

1. การ Survey วิเคราะห์ และจัดทำ **Statistics & Indicator** เพื่อจัดทำ **Annual Cybersecurity** ของประเทศ
2. การทำ **Incidents Drill**
3. การจัดทำ **e-Authentication Framework** ของ ASEAN
4. การสร้าง **Capacity Building** – Inter.Cert., Malware Analysis, Mobile Forensic
5. การผลักดันมาตรฐาน & **Accreditation Body**
6. การผลักดัน **Sector-based CERTs**
7. การจัดทำ National BCP (อยู่ระหว่างจัดทำ Focus Group) & National Plan
8. ยกระดับ **Collaboration** ภายในประเทศ และระดับ Global
9. National **Cybersecurity Agency** กับความจำเป็นในการจัดตั้ง
10. การส่งเสริมและสนับสนุนให้เกิด **Self Regulation ของ MoB : Making online Better**

ETDA
สพธอ
www.etda.or.th

surangkana@etda.or.th