“ภาพรวมกฎหมาย ยุคเศรษฐกิจดิจิทัลและการเตรียมพร้อมรับมือของภาครัฐ”

หลักสูตรนักบริหารรัฐบาลอิเล็กทรอนิกส์ รุ่นที่ ๖

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

SECURITY STANDARD LAW

Soft Infrastructure

to sustain

the Digital Economy

ประเทศไทยกำลังขับเคลื่อนด้วย ระบบ digital และ ข้อมูล

ประชากรไทย

65 ล้านคน

ที่มา ประกาศสำนักทะเบียนกลาง
เรื่อง จำนวนราษฎรทั่วราชอาณาจักร เมื่อวันที่ 11 กุมภาพันธ์ 2558

จำนวนผู้ใช้มือถือ

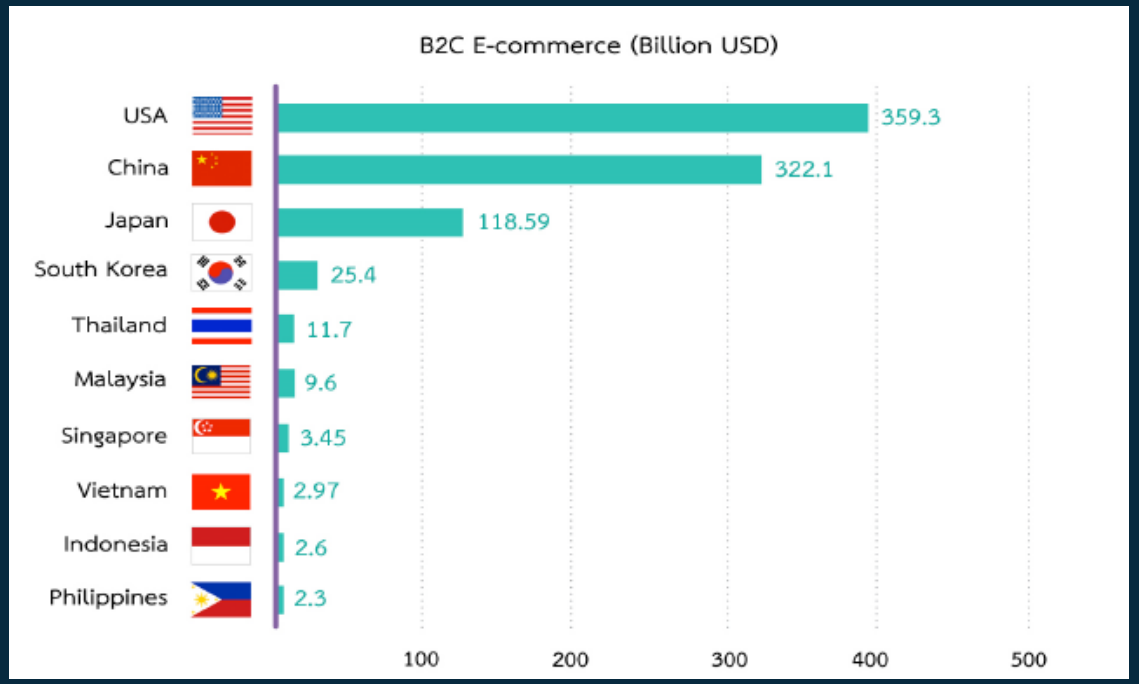
93.05 ล้านเลขหมาย

ที่มา NBTC ไตรมาส 4 ปี 2015

ประเทศไทยกำลังขับเคลื่อนด้วย ระบบ digital และ ข้อมูล

สถิติ E-Commerce ไทย

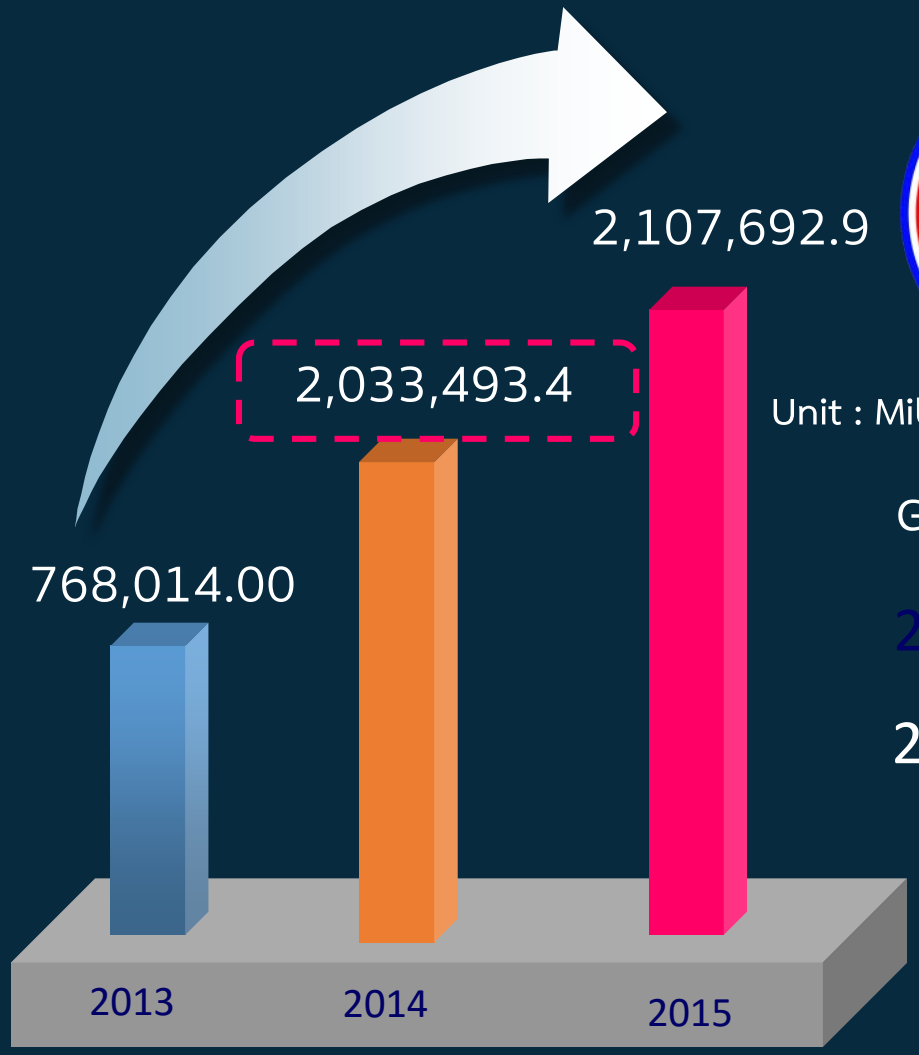
เปรียบเทียบมูลค่า E-Commerce เฉพาะ B2C ในปี 2557



Social Media กิจกรรมยอดฮิต

ที่มา: รายงานผลการสำรวจมูลค่าอิเล็กทรอนิกส์ในประเทศไทย 2558 โดย สพธอ.

Value of e-Commerce in Thailand 2013-2015



Unit : Million Baht

Growth Rate

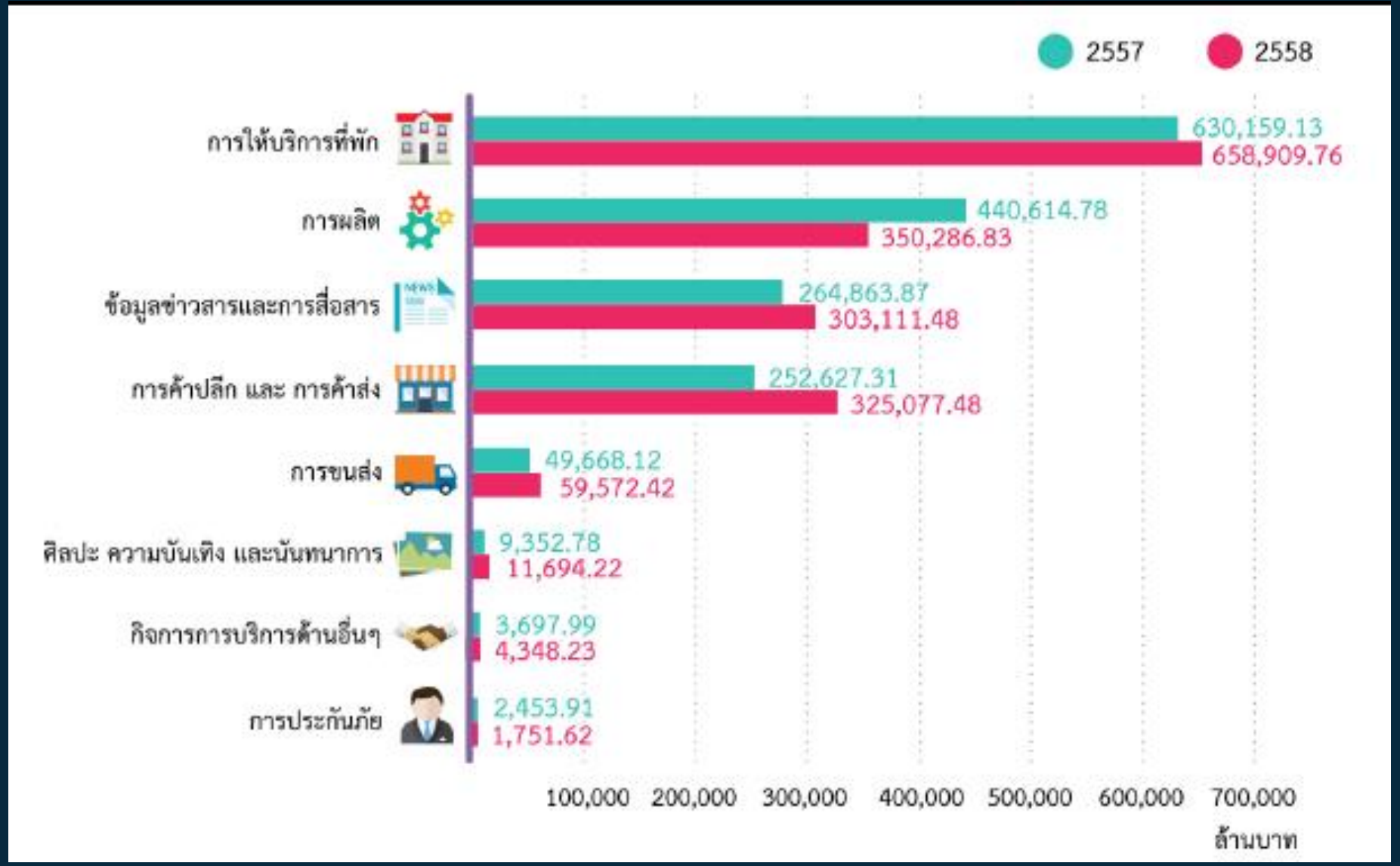
2014	164.77%
2015	3.65%

Remarks :
2013 surveyed by National Statistical Office of Thailand
2014-2015 surveyed by ETDA

Source : ETDA, The Survey of Value of e-Commerce in Thailand, 2015

มูลค่า e-Commerce ปี 2557 และแนวโน้มปี 2558

ที่มา: รายงานผลการสำรวจมูลค่าอิเล็กทรอนิกส์ในประเทศไทย 2558 โดย สพธอ.



สถิติภัยคุกคามไซเบอร์ในปี 2558

ThaiCERT handled 4,371 incidents

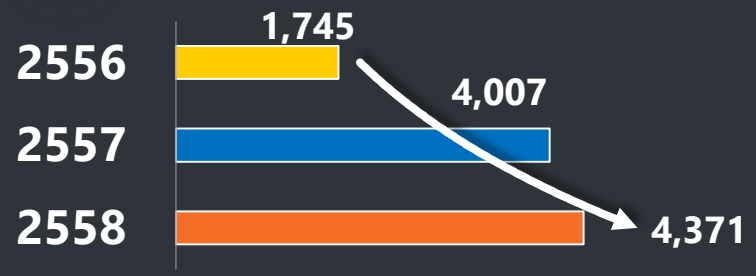
ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

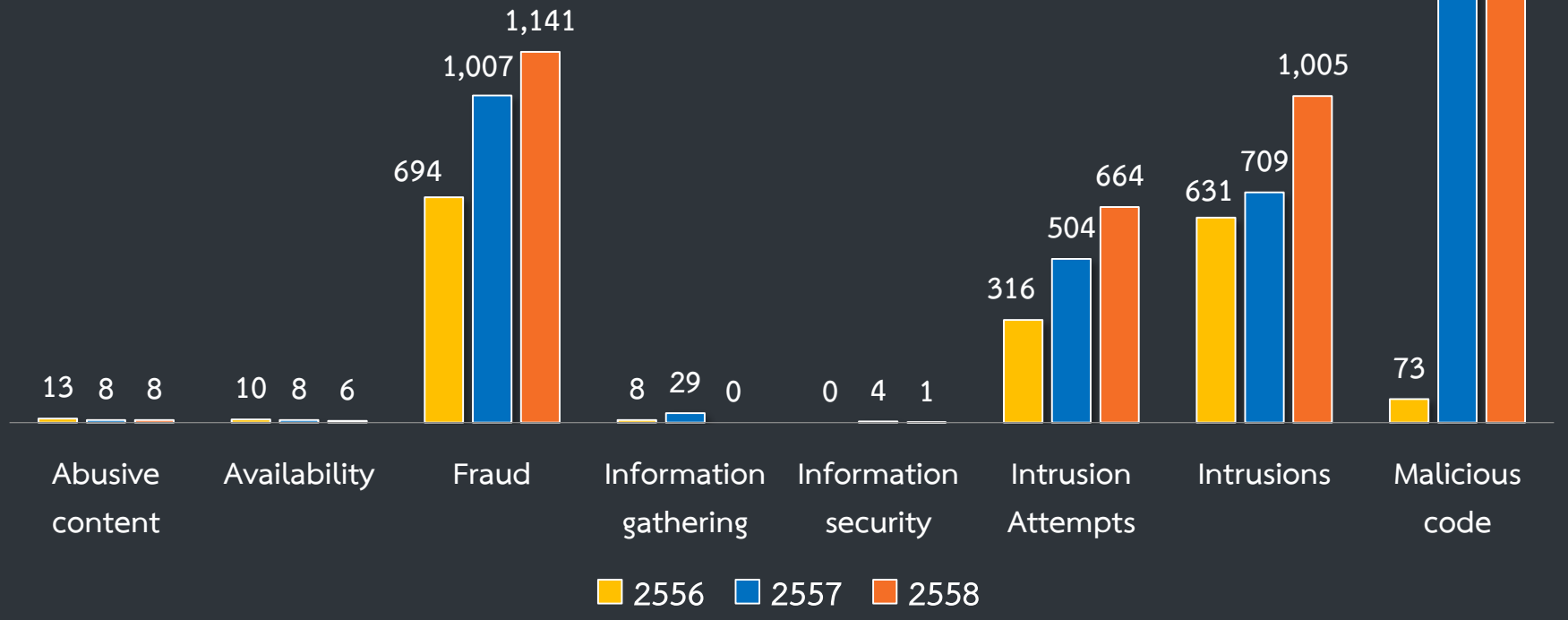
Report by Incident Type

- Malicious code 1,546 (35.3%)
- Fraud (Phishing) 1,141 (26.1%)
- Intrusion 1,005 (22.9%)

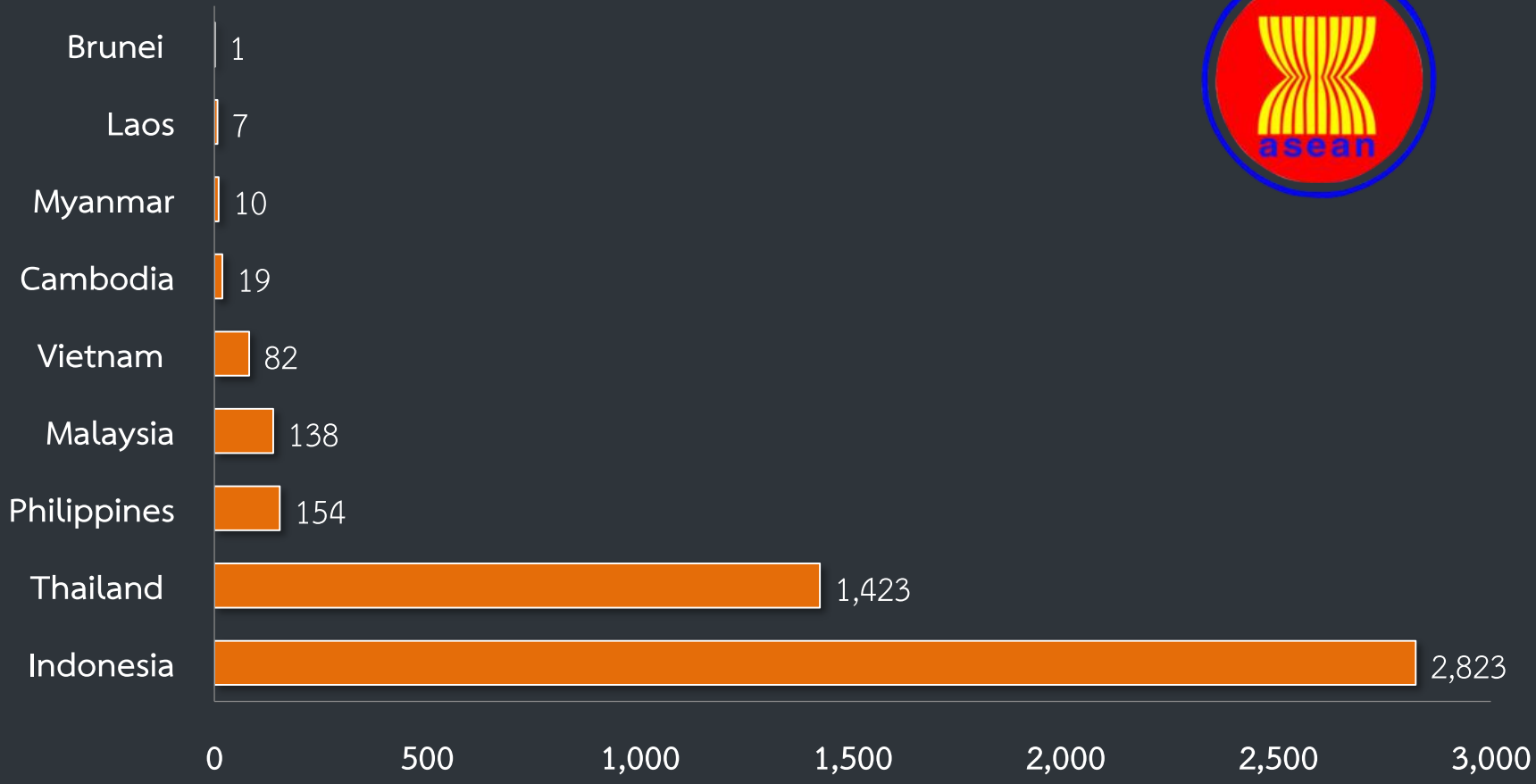
ThaiCERT Statistics

รายงานเปรียบเทียบสถิติภัยคุกคามที่ไทยเซิร์ตได้รับแจ้งในปี 2556 2557 และ 2558



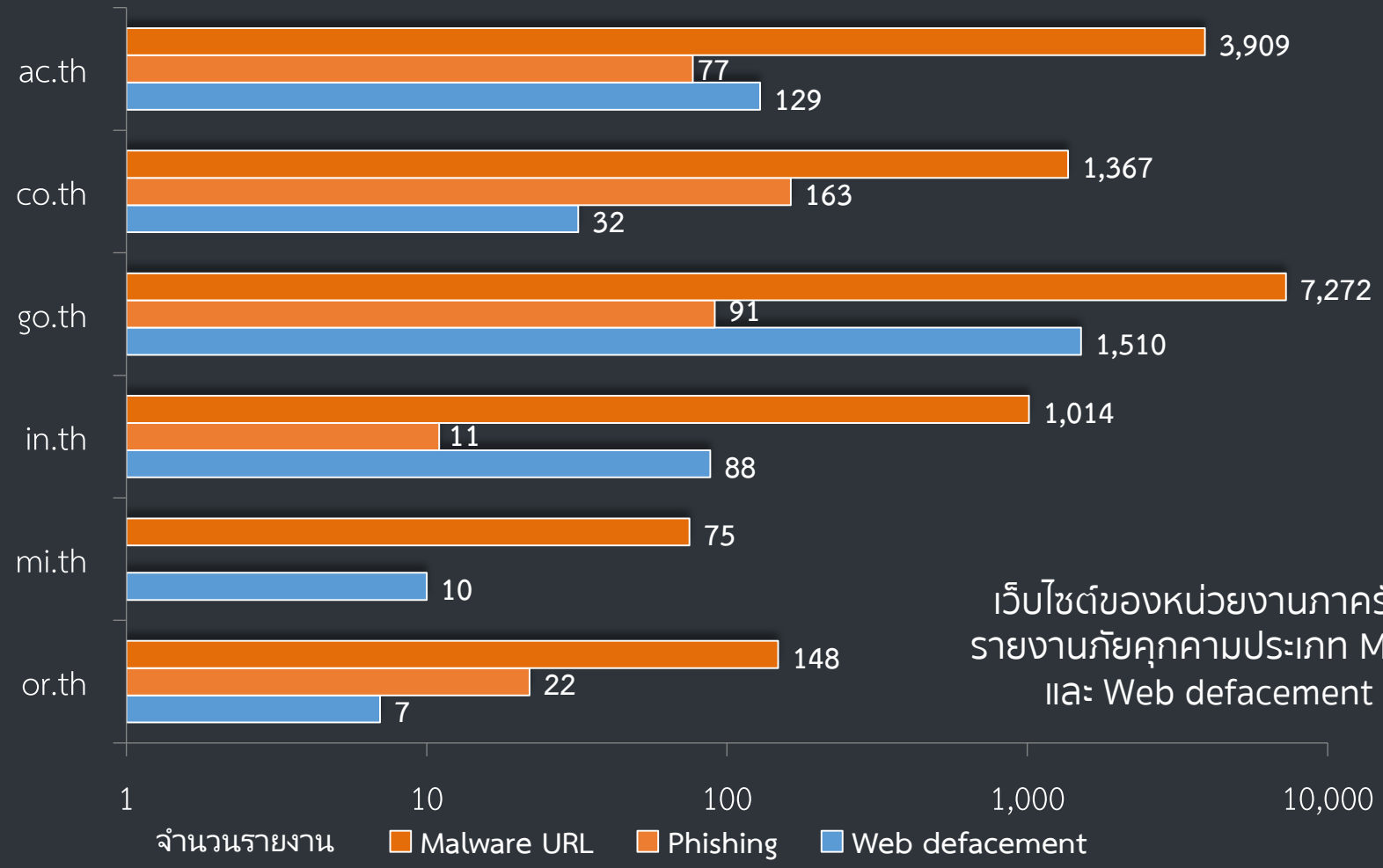


สถิติภัยคุกคาม Web defacement ใน ASEAN ปี 2558



หมายเหตุ: ข้อมูลจากระบบ ThreatWatch ของไทยเซิร์ต

สถิติภัยคุกคามที่เกี่ยวกับเว็บไซต์ .th ในปี 2558



เว็บไซต์ของหน่วยงานภาครัฐ มีจำนวนรายงานภัยคุกคามประเภท Malware URL และ Web defacement สูงที่สุด

ThaiCERT Statistics

รายงานเปรียบเทียบสถิติภัยคุกคามประเภทการโจมตีเว็บไซต์ (Web Attack)
ของหน่วยงานในประเทศไทยที่ ThaiCERT ได้รับรายงาน

*Web Attack = Malware URL, Phishing, and Web Defacement

การรับมือภัยคุกคามไซเบอร์

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

Incident Response

Alerts and Warnings

Artifact Handling

Awareness Building

Education or Training

Cybersecurity Operation Center (CSOC)

Digital Forensics Center (DFC)

Incident Drill

Publication

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

Government

โครงการ ThaiCERT Government Monitoring System (GMS)

- Government Threat Monitoring **(GTM)**
- Government Website Protection **(GWP)**

Critical Infrastructure

โครงการ CERT Readiness

- ประเมิน**ช่องโหว่เว็บไซต์**หน่วยงาน **200 ระบบ**
- สร้าง **Cyber Expert** ประจำหน่วยงาน **30 คน**
- พี่เลี้ยงจัดตั้ง **Sector CERT**

เป้าหมาย

- คาดว่าจะติดตั้งอุปกรณ์ให้ครบ **280 หน่วยงาน** ภายในปี 2560
- ป้องกันการเจาะระบบและโจมตี DDoS ของเว็บไซต์ของหน่วยงานของรัฐ
- **Sector CERT ในกลุ่มโครงสร้างพื้นฐานสำคัญ เช่น สถาบันการเงิน ตลาดทุน ประกันภัย และพลังงาน**

ประโยชน์ที่จะได้รับ

เสริมศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานรัฐ

เพิ่มขีดความสามารถในการ วิเคราะห์ รับมือ และตอบสนองต่อภัยคุกคามไซเบอร์ให้ ThaiCERT

สร้างความเชื่อมั่นกับประชาชนในการทำธุรกรรมออนไลน์

นโยบายด้าน IT ของภาครัฐที่สำคัญ

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

คณะรัฐมนตรีมีมติเห็นชอบเมื่อวันที่ 5 เมษายน 2559

เป้าหมาย	ตัวชี้วัด
1. เพิ่มขีดความสามารถในการแข่งขันก้าวทันเวทีโลก	▪ World Competitiveness ติด 15 อันดับแรก ▪ GDP เพิ่มขึ้นร้อยละ 25
2. สร้างโอกาสและความเท่าเทียมทางสังคม	▪ ประชาชนทุกคนเข้าถึง internet ความเร็วสูง ▪ ICT Development Index ติด 40 อันดับแรก
3. พัฒนาทุนมนุษย์สู่ยุคดิจิทัล	▪ ประชาชนมีความตระหนักรู้และเข้าใจ
4. ปฏิรูปภาครัฐ	▪ UN E-Government Ranking ติด 50 อันดับแรก

ที่มา: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

1. พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง ให้ครอบคลุมทั่วประเทศ
2. ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล
3. สร้างสังคมคุณภาพด้วยเทคโนโลยีดิจิทัล
4. ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล
5. พัฒนากำลังคนให้พร้อมเขาสู่ยุคเศรษฐกิจและสังคมดิจิทัล
6. สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

Digital Economy Law

มาตรการทางกฎหมายที่จำเป็นเพื่อรองรับ Digital Economy

ช่วงที่ 1 (2558)

1. กฎหมายลิขสิทธิ์
   - การปกป้องมาตรการทางเทคโนโลยี (จำเป็นต้องมี Best Practice)
2. กฎหมายอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ

ช่วงที่ 2 (2559)

ร่างกฎหมาย 8 ฉบับ

1. ปรับปรุงกระทรวง ICT
2. พัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (รวมเอา คกก.DE, กองทุน และการส่งเสริม DE ไว้ด้วยกัน)
3. กสทช. : กสช. & กทค.
4. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์
5. ธุรกรรมทางอิเล็กทรอนิกส์
6. คุ้มครองข้อมูลส่วนบุคคล (ตั้งแต่ 2541-2558 = 17 ปีเต็ม)
7. Cybersecurity
8. จัดตั้ง สพธอ.

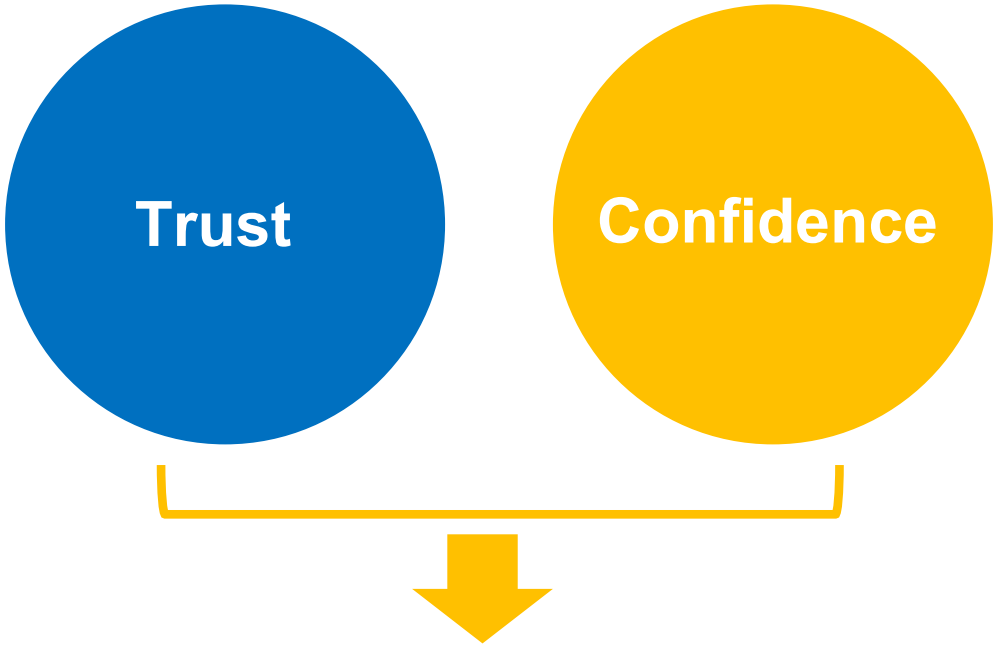
ช่วงที่ 3

1. การจัดซื้อจัดจ้าง
2. ระบบสารบรรณอิเล็กทรอนิกส์
3. การรักษาความลับ
4. การรักษาความปลอดภัย (เมื่อไม่มีมาตรการทำลายเอกสารที่เหมาะสม ก็ยังคงมีภาระในการมีและเก็บทั้งกระดาษและอิเล็กทรอนิกส์ควบคู่กัน ซึ่งเป็นต้นทุนทางเศรษฐกิจมหาศาล)
5. กฎหมายข้อมูลข่าวสารของราชการ
6. กฎหมาย e-Government ?
7. Online Consumer Protection

ช่วงที่ 4

1. การคุ้มครองทรัพย์สินทางปัญญาทั้งระบบ ??
2. มาตรการทางภาษี การเงิน และการคลัง การร่วมลงทุนระหว่างรัฐและเอกชนในโครงสร้างพื้นฐานสำคัญ/ขนาดใหญ่
3. E-transferable Record
4. การระงับข้อพิพาททางออนไลน์ (Online Dispute Resolution)
5. Internet Governance - IGF

กลไกในการสร้าง Trust และ Confidence



- ☑ **Soft Law :** Self-Regulation
- ☑ **Co-Regulation :** Standard
- ☑ **Binding Law :** Legislation

Key Success Factors

Balance	with **Fundamental Rights** Privacy / Freedom of Expression
Transparency	**Open Data & Monitor** by User
Multi-Stakeholders	**Share Experiences**
International Collaboration	**Cooperate & Set Norm**

- **แนวโน้มจัดทำ/ปรับแก้กฎระเบียบให้มีความทันสมัยและสอดคล้องมากขึ้น** (Legal Harmonization & Modernization)
- **แนวโน้มจัดทำ Soft Law เพื่อให้การปรับใช้กฎหมายมีประสิทธิภาพ** (Legal Implementation) เช่น Guideline, Recommendation, Best Practice

บทบาทของ Soft Law เป็นแนวทางที่ช่วยให้ปฏิบัติได้สอดคล้องตามกฎหมาย

- Social Media
- Data Protection
- Information Security
- Critical Infrastructure
- Trust Mark เช่น TRUSTe, Privacy Policy
- ISO 27017 Cloud Security
- ISO 27018 Cloud Privacy
- ISO 27001 Information Security

ICT law Legal Framework 2541

- กฎหมายธุรกรรมทางอิเล็กทรอนิกส์
- กฎหมายลายมือชื่ออิเล็กทรอนิกส์
- กฎหมายการชำระเงินทางอิเล็กทรอนิกส์

→ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

- กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์

→ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

- กฎหมายคุ้มครองข้อมูลส่วนบุคคล

→ ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

Digital Economy Law 2558

วางนโยบาย & ปรับปรุงโครงสร้าง

- ร่าง พ.ร.บ. การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม
- ร่าง พ.ร.บ. ปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ ..)

ปรับบทบาท & เชื่อมโยงนโยบาย

- ร่าง พ.ร.บ. กสทช. (ฉบับที่ ..)

เพิ่มกลไก ความเชื่อมั่น

- ร่าง พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..)
- ร่าง พ.ร.บ. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..)
- ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- ร่าง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์
- ร่าง พ.ร.บ. สพธอ.

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

Why ?

- นโยบายหลากหลาย ไม่สอดคล้องและต่อเนื่อง
- ขาดการนำ ICT ไปเพิ่มมูลค่าทางเศรษฐกิจและสังคม

Policy Maker

นโยบายและแผนชาติ ด้าน **Digital Economy**

คณะกรรมการระดับชาติ จากรัฐและเอกชน

คณะกรรมการเฉพาะเรื่อง **ช่วยติดตาม/กำกับการทำงาน**
โครงสร้างพื้นฐานดิจิทัล / ส่งเสริมและพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

หน่วยงานรัฐ	ส่งเสริม**ภาคเอกชน**	**กองทุน DE**
ต้องทำตามนโยบาย	ให้มีส่วนร่วม (PPP)	สนับสนุนการทำงาน

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

Why ?

- คลื่นความถี่ คือ โครงสร้างพื้นฐานหลัก แต่การจัดสรรยังไม่ตอบโจทย์
- เทคโนโลยีหลอมรวม (โทรคมนาคม / วิทยุโทรทัศน์)
- ประสิทธิภาพและธรรมาภิบาล ในการทำงานยังถูกตั้งคำถาม

นโยบายจัดสรรคลื่น

สอดคล้องนโยบาย DE แต่ไม่กระทบอิสระในการกำกับ

กลไกจัดสรรคลื่น

เกณฑ์การจัดสรรที่ประชาชนได้ประโยชน์ (Spectrum Sharing , Reframing)

หน่วยงานกำกับ

ปรับองค์ประกอบ /ที่มา กสทช. (ยกเลิก กสท. และ กทค.)
เพิ่มมาตรการติดตามประสิทธิภาพ
ปรับปรุงองค์กรกำกับประเมินผล เพื่อติดตามดูแล

เมื่อโลกและประเทศไทยกำลังขับเคลื่อนด้วย ระบบ digital และ ข้อมูล

Security & Privacy **คือประเด็นที่ต้องคำนึงถึง**

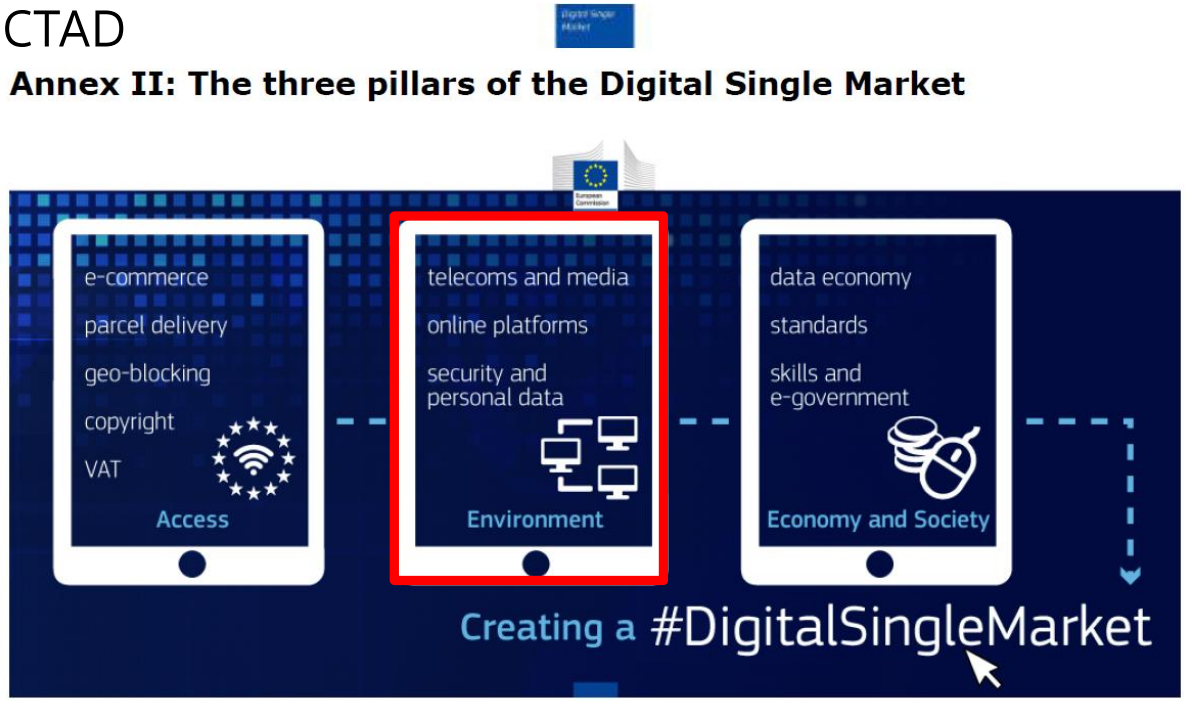
ทำไม 2 เรื่องนี้ จึงสำคัญ

1. เป็นปัจจัยที่ส่งผลต่อความพร้อมด้าน digital ที่องค์กรต่าง ๆ ให้คำแนะนำ

- INFORMATION ECONOMY REPORT 2015 โดย UNCTAD
- Digital Single Market โดย EU
- Information security and privacy โดย OECD

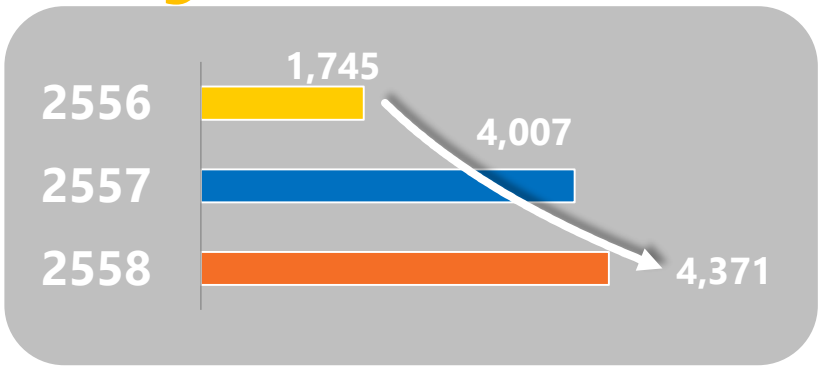
  OECD Recommendation on Digital Security Risk Management

  2013 OECD Privacy Guidelines



ร่าง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

Why ?



ThaiCERT Statistics

- ภัยคุกคามไซเบอร์รุนแรงมากขึ้น
- ระบบ IT อ่อนแอ และหน่วยงานส่วนใหญ่ไม่สนใจ IT Security

Policy &
National Flow

National
CERT

Capacity
Building &
Awareness

National Security **VS** **Fundamental Right**

Privacy / Freedom of Expression

ร่าง พ.ร.บ. การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. ....

Why ?

- เกิดปัญหาในการตีความ / บังคับใช้กฎหมาย
- กระแสสังคมเรียกร้องหลักประกันสิทธิเสรีภาพในการแสดงความคิดเห็น
- ความผิดอื่นทำผ่านออนไลน์มากขึ้น เกิดปัญหาในการจัดการ

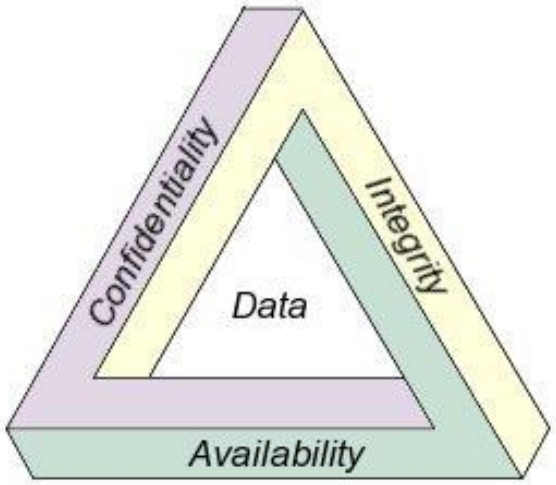
ปรับ **ฐานความผิด** ให้ชัดเจนขึ้น

ช่วยเหลือทางเทคนิค เพิ่มความน่าเชื่อถือให้พยานหลักฐาน

สนับสนุนการทำงานเจ้าหน้าที่ งบประมาณ / เงินเพิ่ม

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

กำหนดมาตรการในการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์



รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (**Authenticity**) ความรับผิด (**Accountability**) การห้ามปฏิเสธความรับผิด (**Non-repudiation**) และความน่าเชื่อถือ (**Reliability**)

ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)
C.I.A. = หลักการพื้นฐานของ Information Security และ Cybersecurity

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

บททั่วไป

- ระบบคอมพิวเตอร์
- ข้อมูลคอมพิวเตอร์
- ข้อมูลจราจรทางคอมพิวเตอร์
- ผู้ให้บริการ
- ผู้ใช้บริการ
- พนักงานเจ้าหน้าที่
- รัฐมนตรี

ม.12 บทหนัก

หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์

กระทำต่อคอมพิวเตอร์

- **ม.**5 การเข้าถึงระบบคอมฯ
- **ม.6** การล่วงรู้มาตรการการป้องกันการเข้าถึง
- **ม.7** การเข้าถึงข้อมูลคอมฯ
- **ม.8** การดักรับข้อมูลคอมฯ
- **ม.9** การรบกวนข้อมูลคอมฯ
- **ม.10** การรบกวนระบบคอมฯ
- **ม.13** การจำหน่าย/ เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด

ใช้คอมพิวเตอร์กระทำความผิด

- **ม.11** Spam mail
- **ม.14** การปลอมแปลงข้อมูลคอมพิวเตอร์/เผยแพร่เนื้อหาอันไม่เหมาะสม
- **ม.15** ความรับผิดของผู้ให้บริการ
- **ม.16** การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง

กระทำความผิดนอกราชอาณาจักร ต้องรับโทษภายในราชอาณาจักร (ม.17)

การรับฟังพยานหลักฐานที่ได้มาตาม พ.ร.บ. ฉบับนี้ (ม.25)

หมวด 2 พนักงานเจ้าหน้าที่

พนักงานเจ้าหน้าที่

อำนาจหน้าที่ (ม.18) : (1) มีหนังสือ/เรียกเพื่อให้ถ้อยคำ/เอกสาร (2) เรียกข้อมูลจราจร (3) สั่งให้ส่งมอบข้อมูลที่อยู่ในครอบครอง (4) ทำสำเนาข้อมูล (5) สั่งให้ส่งมอบข้อมูล/อุปกรณ์

ข้อจำกัด/การตรวจสอบการใช้อำนาจ (ม.19) : ยื่นคำร้องต่อศาลในการใช้อำนาจตาม ม.18 (4)-(8), ส่งสำเนาบันทึกรายละเอียดให้แก่ศาลภายใน 48

การ block เว็บไซต์ พนักงานเจ้าหน้าที่โดยความเห็นชอบของ [illegible] ยื่นคำร้องต่อศาล

ความรับผิดของพนักงานเจ้าหน้าที่: (ม.22 ถึง มาตรา 24)

พยานหลักฐานที่ได้มาโดยมิชอบ อ้างและรับฟังมิได้ (ม.25)

การแต่งตั้ง/กำหนดคุณสมบัติพนักงานเจ้าหน้าที่/การประสานงาน (ม.28-29)

ผู้ให้บริการ

ม.26 เก็บข้อมูลจราจร 90 วัน ไม่เกิน 1 ปี

ม.27: ไม่ปฏิบัติตามคำสั่งพนักงานเจ้าหน้าที่หรือคำสั่งศาล ระวางโทษปรับ

หน้าที่ของผู้ให้บริการ ภายใต้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ม.26 หน้าที่ของผู้ให้บริการในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

<u>หากไม่ปฏิบัติตาม</u> ผู้ให้บริการถูกปรับไม่เกิน 500,000 บาท

ข้อมูลจราจรทางคอมพิวเตอร์ คือ ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรือ อื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

- เก็บรักษา**ข้อมูลจราจรทางคอมพิวเตอร์**เท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้บริการ**ไม่น้อยกว่า 90 วัน** นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ (รัฐมนตรีจะเป็นผู้ประกาศในราชกิจจานุเบกษาว่ากรณีดังกล่าวจะใช้บังคับกับผู้ให้บริการประเภทใด)
- **ในกรณีจำเป็น** พนักงานเจ้าหน้าที่สามารถสั่งผู้ให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์**เกิน 90 วันได้ แต่ต้องไม่เกิน 1 ปี**

ประกาศ ทก. เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

- ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการมีหน้าที่ต้องเก็บรักษา
- การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้มั่นคงปลอดภัย

หลักฐานสำคัญในการหาตัวอาชญากร

- ✓ เวลาต้องเที่ยงตรง เพื่อให้ระบุเส้นทางได้ถูก
- ✓ ข้อมูลจราจรทางคอมพิวเตอร์ที่เก็บต้องสามารถระบุตัวบุคคลได้
- ✓ ข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องไม่ถูกแก้ไข

หากไม่เก็บจะทำให้ยากในการติดตามผู้กระทำความผิดและวิเคราะห์ข้อบกพร่องของระบบ

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

ความเป็นส่วนตัว

ข้อมูลส่วนบุคคล

สิทธิขั้นพื้นฐาน ที่รัฐธรรมนูญคุ้มครอง

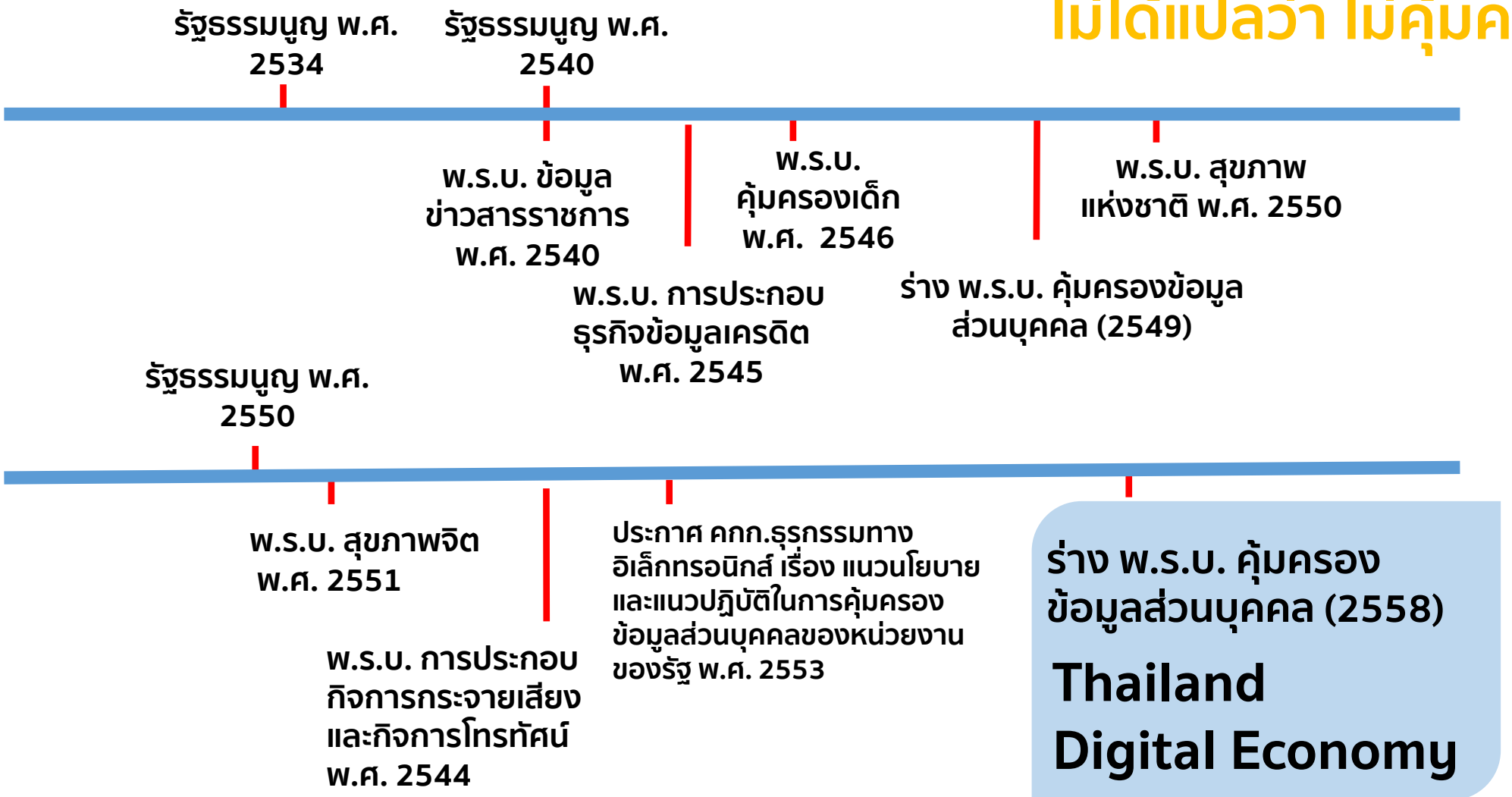
สร้าง **กฎหมายกลาง** เพื่อให้มีมาตรฐานในการดูแล

สอดคล้องหลักการสากล รองรับ Data Flow

ข้อมูลส่วนบุคคล	หน้าที่ผู้ควบคุมข้อมูล	สิทธิเจ้าของข้อมูล
มาตการความปลอดภัย	การละเมิดข้อมูลส่วนบุคคล	Soft Law & Self-Regulation

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

“ไม่มีกฎหมายกลาง
ไม่ได้แปลว่า ไม่คุ้มครอง”



ตัวอย่างการจัดการข้อมูลส่วนบุคคลขององค์กร

Priority
Buy-in from Top

- ✓ระบุและจัดหมวดหมู่ของข้อมูล (Personal Data Inventory)
- ✓กำหนดนโยบายให้สอดคล้องตามหลักเณฑ์สากลและภายในประเทศ (Policy)
- ✓ประเมินความเสี่ยง (Risk Assessment Tools) เพื่อระบุและจัดการความเสี่ยง ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
- ✓อบรมให้ความรู้ ความตระหนัก แก่บุคลากรที่เกี่ยวข้องในองค์กร (Training)
- ✓กำหนดแนวทางการดำเนินงานเมื่อเกิดเหตุการณ์ละเมิดข้อมูล (Breach Handing) เช่น แจ้งเจ้าของข้อมูล หน่วยงานที่เกี่ยวข้อง
- ✓ให้ข้อมูลข่าวสารที่เพียงพอแก่บุคคลภายในและภายนอก เมื่อเกิดเหตุ(Communication)
- ✓ดูแลให้ผู้ประมวลผลข้อมูล (Data Processor Management) ทำหน้าที่ตามข้อตกลง

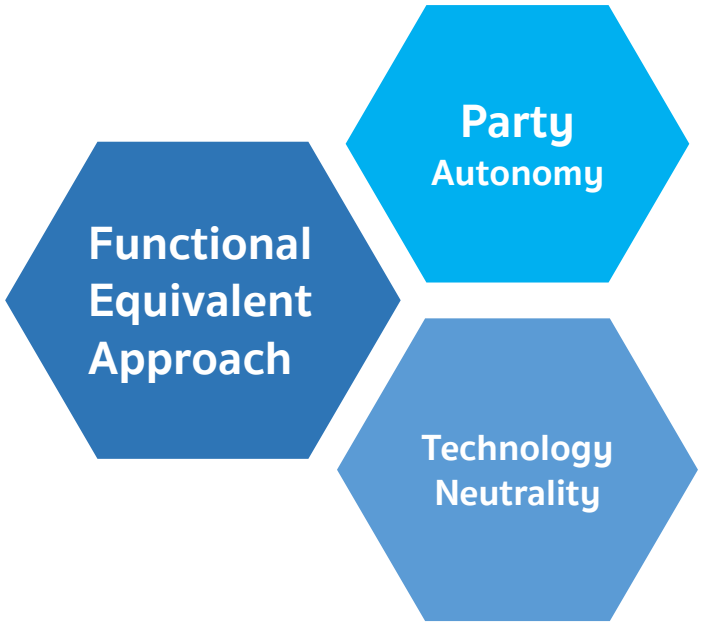
ที่มา: Hong Kong PMP

ร่าง พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. ....

Why ?

- ยังมีข้อจำกัดในการบังคับใช้
- ปรับกลไกการกำกับดูแลให้ Practical
- Harmonize Law รองรับธุรกรรมออนไลน์ระหว่างประเทศ

  Model Law on E-Commerce
  Model Law on E-Signature
  UN Convention on E-Communication



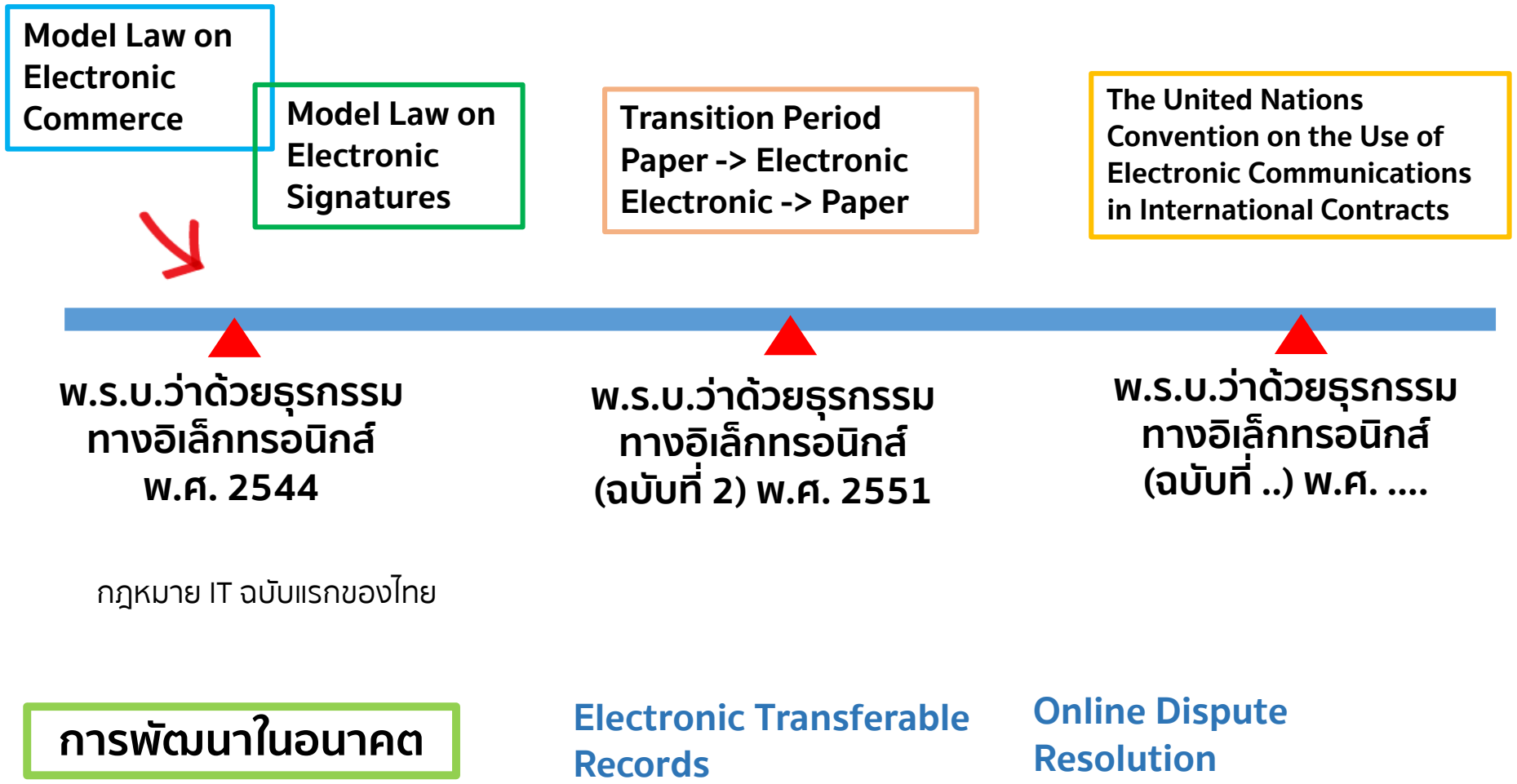
การมีผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์

พัฒนาหลักเกณฑ์ **สอดคล้องสากล**
Input-error, Automated Massage System, Invitation

ปรับ**กลไกการกำกับดูแล** ลดภาระภาคธุรกิจ

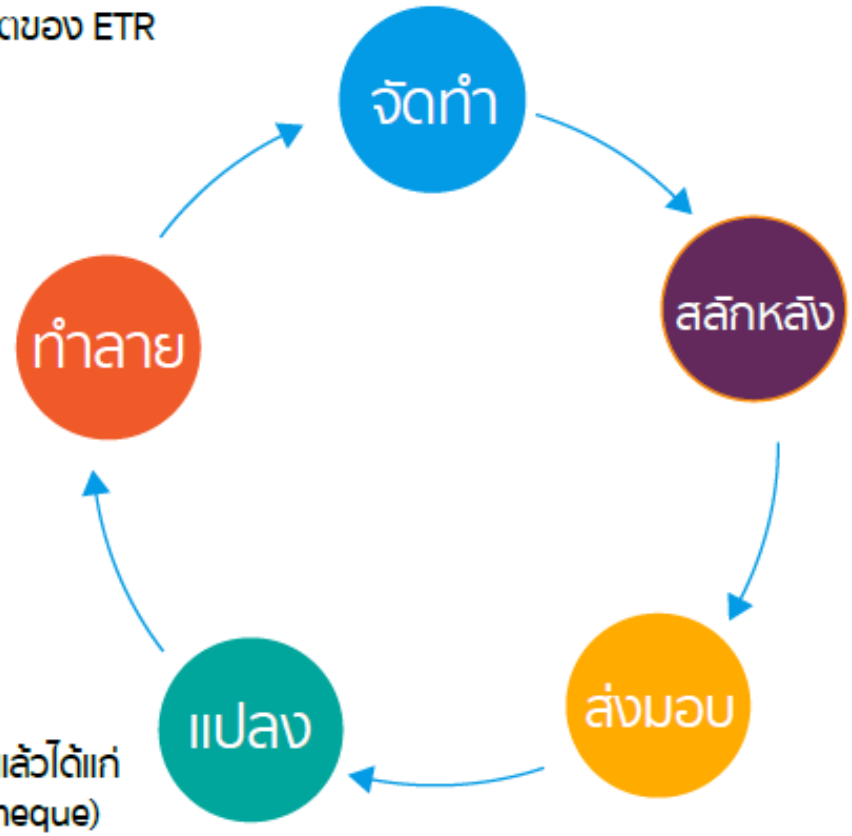
ปรับ**โครงสร้างหน่วยงาน**ร่วมผลักดันธุรกรรมออนไลน์

พัฒนาการกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ของไทย



e-Transferable Record (ETR)
เอกสารที่เปลี่ยนมือได้ทางอิเล็กทรอนิกส์

- UNCITRAL WG 4 กำลัง จัดทำ “ร่างหลักเกณฑ์รองรับ ETR” (เช่น Model Law) กำหนดให้ครบวงจรของชีวิตของ ETR ในระบบอิเล็กทรอนิกส์



- ปัจจุบัน ประเทศที่มีกฎหมายรองรับเรื่อง ETR แล้วได้แก่ เกาหลีใต้ (e-Promissory Note) ฮ่องกง (e-Cheque)

การ Implement ระบบ e-Cheque ในฮ่องกง

ระบบ e-Cheque ในฮ่องกง

ต้นทุนการทำเช็ค กระดาษต่อใบ **17** HKD

วันทำงาน **250** วันต่อปี

มิเช็คในระบบ **500,000** ฉบับต่อวัน

**ลดค่าใช้จ่ายได้กว่า 2 พันล้าน HKD ต่อปี

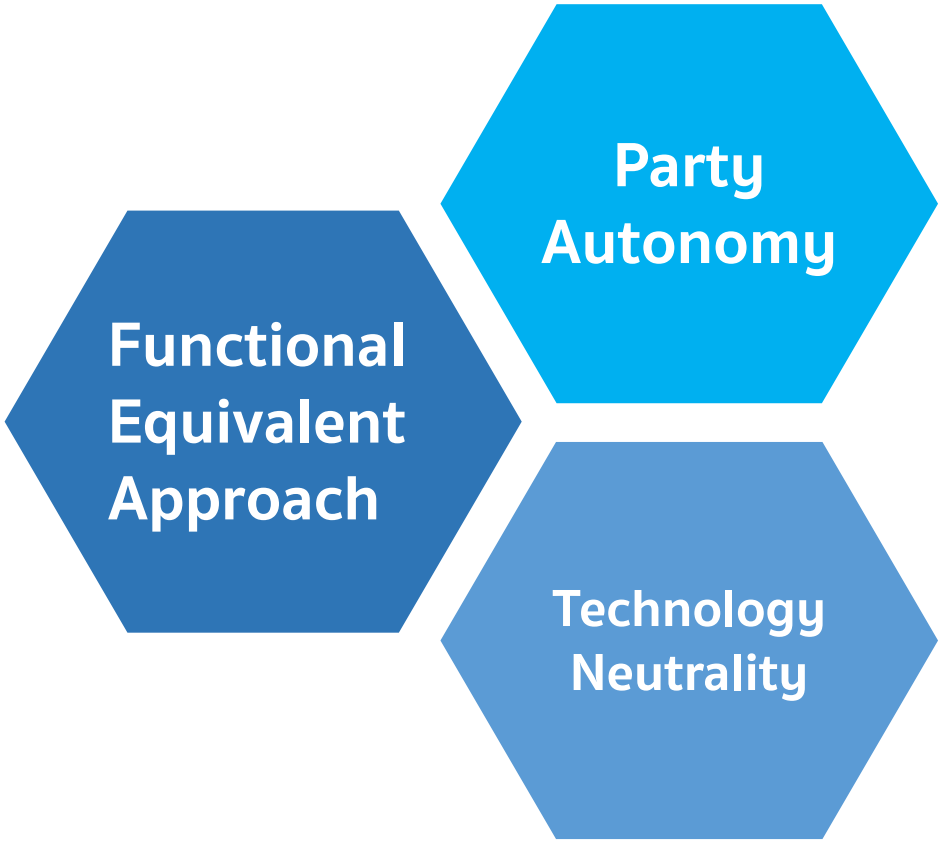
องค์ประกอบของ e - Cheque

ใช้ digital signature เพื่อรับรองตัวตน และตรวจสอบความถูกต้อง

Digital Certificate ของผู้สั่งจ่าย	KYC โดย CA	จัดเก็บใน Smart Card
Digital Certificate ของธนาคารผู้สั่งจ่าย	KYC โดยธนาคาร	จัดเก็บในอุปกรณ์ Hardware Security Module

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

“รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์” (ม.7)



E-Document
(ม.8)

E-Signature
(ม.9 และหมวด 2)

Print out
(ม.10 วรรค 4)

E-Evidence
(ม.11)

E-Payment
(หมวด 3)

E-Government
(หมวด 4)

IT Security, Critical Infrastructure
(ม.25)

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

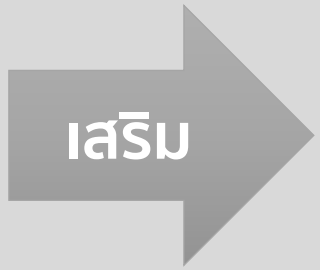
“ใช้บังคับเพื่อเสริมกฎหมายอื่น”

(เสริมให้ทำในรูปแบบอิเล็กทรอนิกส์ได้)

ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

เช่น

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ



พ.ร.บ. การอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ

(ร่าง พ.ร.บ. การจัดซื้อจัดจ้างภาครัฐฯ)

หมายเหตุ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ไม่ใช้กับ (1) ธุรกรรมเกี่ยวกับครอบครัว

(2) ธุรกรรมเกี่ยวกับมรดก

ทำไมต้องรู้ว่าอะไรคือสิ่งที่กฎหมายกำหนด และอะไรเป็นขั้นตอนของเราเอง

Law

ต้องปฏิบัติตาม

กฎหมายกำหนดแบบ ขั้นตอน เงื่อนไข อย่างไรบ้าง

(หากกฎหมายข้อไหนจะเป็นอุปสรรค/ไม่จำเป็นสำหรับระบบอิเล็กทรอนิกส์
ต้องเสนอแก้ไขกฎหมาย)

Business Process

ปรับเปลี่ยนให้เหมาะสมกับระบบอิเล็กทรอนิกส์

ขั้นตอนภายในของเรากำหนด Business Process ไว้อย่างไร

(หากขั้นตอนไหนเป็นอุปสรรค/ไม่จำเป็นสำหรับระบบอิเล็กทรอนิกส์
เสนอผู้บริหารเพื่อปรับเปลี่ยนแก้ไข)

โครงกฎหมาย

- **“ธุรกรรมทางอิเล็กทรอนิกส์”**
  รองรับการทำธุรกรรมในรูปแบบข้อมูลอิเล็กทรอนิกส์ในเรื่องต่างๆ

- **“ลายมือชื่ออิเล็กทรอนิกส์”**
  รองรับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

- **“ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์”**
  รองรับการกำกับดูแลธุรกิจบริการที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ที่สำคัญและมีผลกระทบวงกว้าง

- **“ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ”**
  รองรับการให้บริการภาครัฐด้วยวิธีการทางอิเล็กทรอนิกส์

- **“คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์”**
  รองรับการมีคณะกรรมการเพื่อส่งเสริมและพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ

Mandatory Rules

- ม. 7 ห้ามปฏิเสธเพียงเพราะเป็นธุรกรรมที่ทำในแบบอิเล็กทรอนิกส์
- ม. 8 การทำข้อมูลอิเล็กทรอนิกส์เป็นหนังสือ
- ม. 9 การลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์
- ม. 10 ความเป็นต้นฉบับของข้อมูลอิเล็กทรอนิกส์
- ม. 11 การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานในศาล
- ม. 12 การเก็บรักษาข้อมูลอิเล็กทรอนิกส์
- ม. 12/1 การแปลงเอกสารกระดาษเป็นข้อมูลอิเล็กทรอนิกส์
- ม. 25 วิธีการที่เชื่อถือได้ที่ได้ประโยชน์จากข้อสันนิษฐานทางกฎหมาย

เมื่อตกลงใช้ธุรกรรมทางอิเล็กทรอนิกส์
หลักเกณฑ์เหล่านี้ตกลงเป็นอย่างอื่นไม่ได้

หลักเกณฑ์อื่นนอกจากนี้
ในหมวด 1 และ 2
สามารถตกลงเป็นอย่างอื่นได้

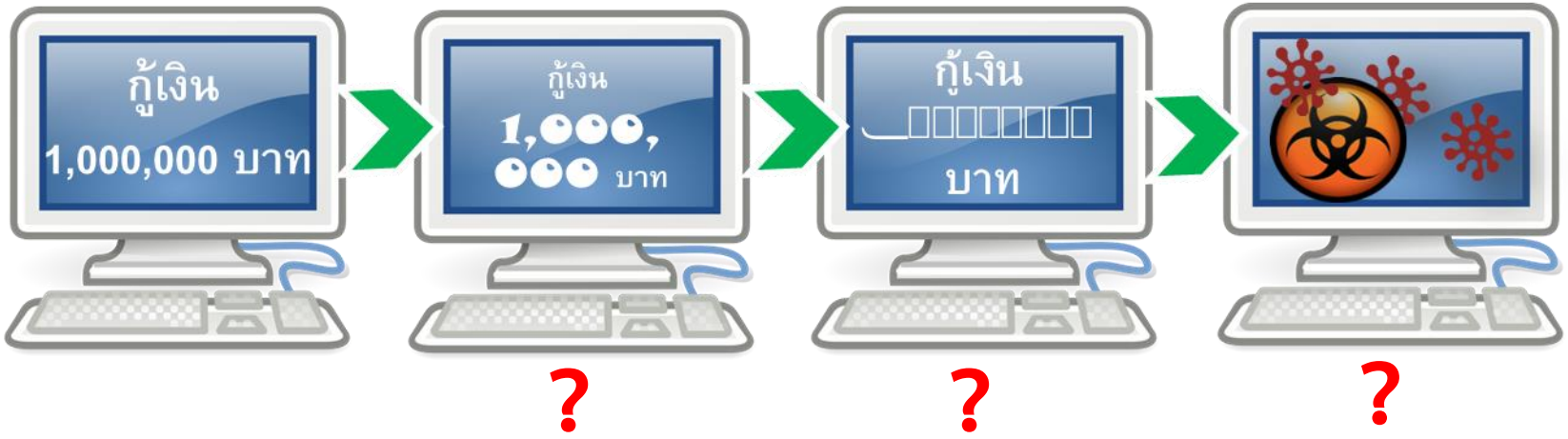
หลักเกณฑ์อื่น ๆ ที่ตกลงเป็นอย่างอื่นได้

- ม. 13 คำเสนอ / คำสนองในรูปแบบอิเล็กทรอนิกส์
- ม. 14 การแสดงเจตนา / บอกกล่าวในรูปแบบอิเล็กทรอนิกส์
- ม. 15 – ม. 21 การส่ง – รับ ข้อมูลอิเล็กทรอนิกส์
- ม. 22 มีการส่งข้อมูลอิเล็กทรอนิกส์เมื่อไหร่
- ม. 23 ได้รับข้อมูลอิเล็กทรอนิกส์เมื่อไหร่
- ม. 24 สถานที่ส่ง – รับ ข้อมูลอิเล็กทรอนิกส์คือที่ใด

สามารถตกลง
ร่วมกันในกลุ่มธุรกิจ
เพื่อให้เป็นมาตรฐาน
เดียวกันได้

E-Document (ม.8)

1. เข้าถึงได้
2. นำกลับมาใช้ได้
3. ความหมาย ไม่เปลี่ยนแปลง

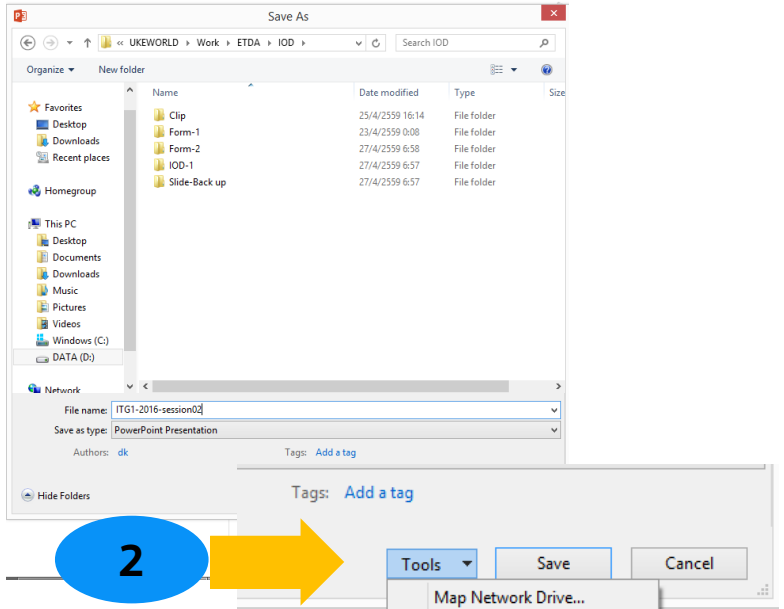


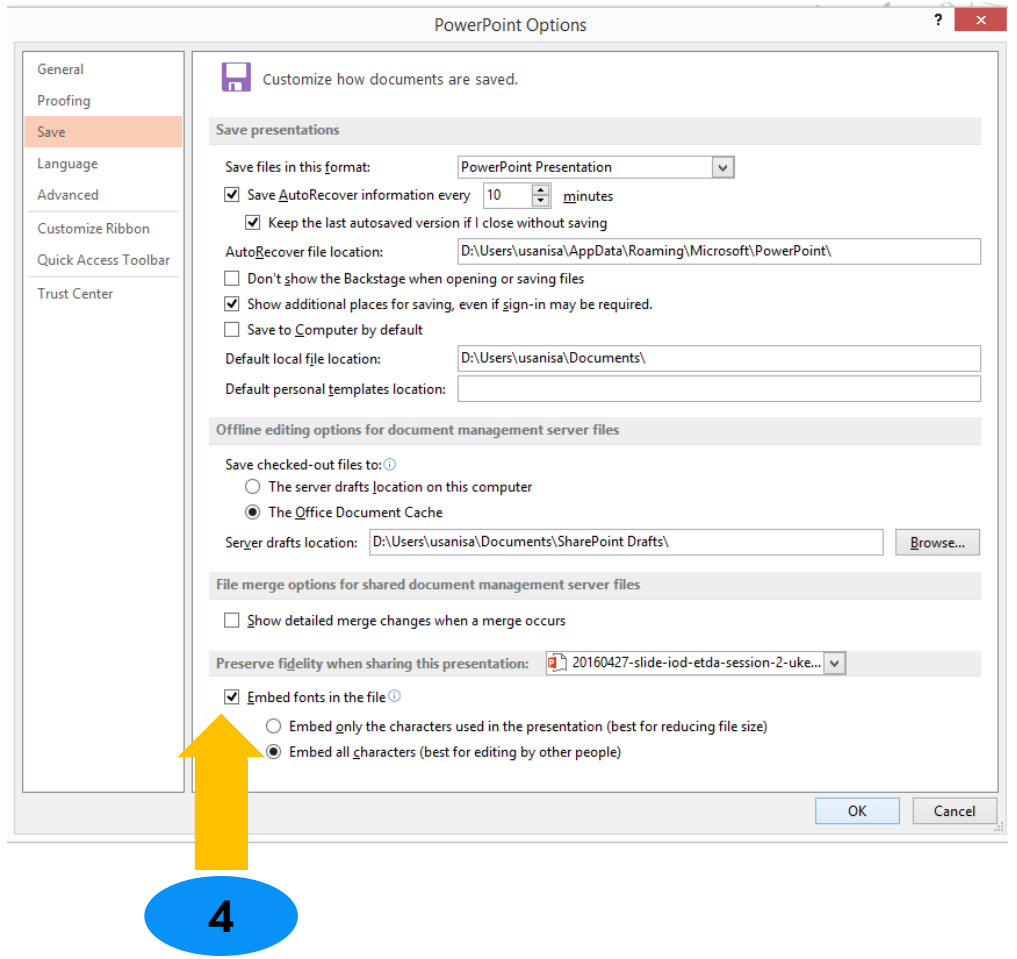
หากไม่ทำตามเงื่อนไขที่กฎหมายกำหนด
ถือว่า ไม่มีหนังสือ หลักฐานเป็นหนังสือ หรือเอกสาร สำหรับฟ้องร้องคดี

E-Document (ม.8)

วิธีการฝัง fonts

Save/ Save as → เลือก Tools → เลือก Save Options → เลือก Embed fonts in the file





E-Signature (ม. 9)

เช่น User Name & Password

1. ระบุตัวผู้เป็นเจ้าของลายมือชื่อได้
2. แสดงได้ว่าเจ้าของลายมือชื่อยอมรับข้อความนั้น
3. ใช้วิธีการที่น่าเชื่อถือ

- ความมั่นคงและรัดกุมของวิธีการที่ใช้
- ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำฯลฯ
- ความรัดกุมของระบบติดต่อสื่อสาร

รหัสผ่านยอดนิยมแห่งปี 2014 ? ? ?

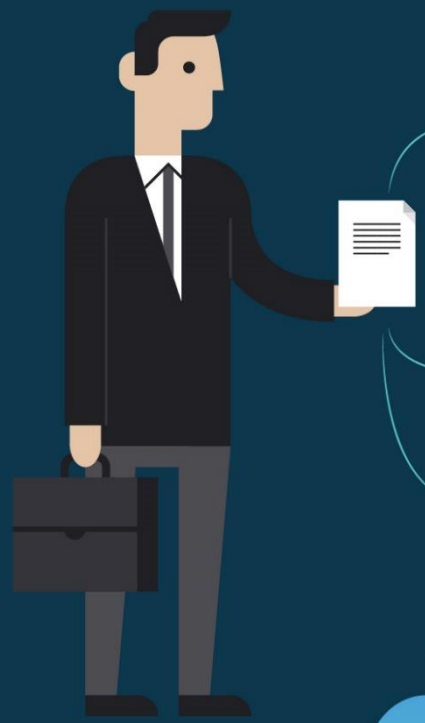
1. 123456
2. password
3. 12345
4. 12345678

ที่มา: SplashData

หากไม่ทำตามเงื่อนไขที่กฎหมายกำหนด ถือว่า ไม่มีการลงลายมือชื่อ

e-AUTHENTICATION

SECURED & FLEXIBLE



LoA 1

LoA 2

LoA 3

LoA 4

Service ภาครัฐ

พิจารณา Level of Assurance
ตามระดับความเสี่ยงของธุรกรรม

*LoA = Level of Assurance

มาตราฐานสากล ISO 29115

ตัวอย่างคำพิพากษาต่างประเทศ

- **Mehta v J Pereira Fernandes**
  หากคู่สัญญาหรือตัวแทนของคู่สัญญาได้พิมพ์ชื่อหลักของตนไว้ท้ายอีเมลถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์

- **Golden Ocean Group Ltd v Salgaocar Mining Industries PVT Ltd [2012] EWCA Civ 265**

  หากคู่สัญญาได้เขียนอีเมลหากันหรือลงลายมือชื่อถือว่าคู่สัญญาได้ผูกพันตามข้อความในอีเมลนั้น อย่างไรก็ตามหากเป็นการพิมพ์ชื่อท้ายอีเมลและพิมพ์คำว่า “ตามสัญญา” (subject to contract) ถือว่า ข้อความหรือสัญญาที่ได้ตกลงในอีเมลไม่เป็นผลถึงแม้จะมีการลงลายมืออิเล็กทรอนิกส์ก็ตาม

- **Sims v. Stapleton Realty, Ltd., 305 Wis.2d 655, 2007 WL 2386494 (Wis.App.)**
  การพิมพ์ชื่อไว้ในเนื้อความของอีเมลที่มีการส่งไปมาหากันถือว่าเป็นการลงลายมือชื่ออิเล็กทรอนิกส์

E-Government (ม.35)

พ.ร.ฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

“หน่วยงานของรัฐ” (มาตรา 4)

- กระทรวง ทบวง กรม ส่วนราชการ ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น
- รัฐวิสาหกิจที่ตั้งขึ้นโดย พ.ร.บ. หรือ พ.ร.ฎ.
- นิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใดๆ

กำหนดหลักเกณฑ์ 3 เรื่อง ได้แก่

การจัดให้มีระบบเอกสารที่ทำในรูปข้อมูลอิเล็กทรอนิกส์ (ม. 3 และ ม. 4)

- รูปแบบที่เหมาะสม & แสดงหรืออ้างอิงได้ในภายหลัง & ข้อความครบถ้วน
- กำหนดระยะเวลาเริ่มต้นหรือสิ้นสุดและอาจกำหนดระยะเวลาดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

จัดให้มีแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Security Policy) (ม. 5)

ประกาศ คธอ. เรื่อง แนวนโยบาย/แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2553

จัดให้มีแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) (ม. 6)

ประกาศ คธอ. เรื่อง แนวนโยบาย/แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

- ต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
- หน่วยงานของรัฐนำไปปฏิบัติ
- ตรวจสอบการนำไปปฏิบัติ

Data Protection

ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

นโยบายและข้อปฏิบัติต้องสอดคล้องกัน และต้องคำนึงถึงหลักเกณฑ์ 8 ประการ ดังนี้

สอดคล้องกับ OECD

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle)
2. คุณภาพของข้อมูลส่วนบุคคล (Data Quality Principle)
3. การระบุวัตถุประสงค์ในการเก็บรวบรวม (Purpose Specification Principle)
4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้ (Use Limitation Principle)
5. การรักษาความมั่นคงปลอดภัย (Security Safeguards Principle)
6. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล (Openness Principle)
7. การมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)
8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล (Accountability Principle)

Security

ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และฉบับที่ 2 พ.ศ. 2556

นโยบาย (Policy)

1. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
2. การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน
3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อปฏิบัติ (Practice)

1. การเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)
2. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control)
3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)
4. หน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)
5. ควบคุมการเข้าถึงเครือข่าย (network access control)
6. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)
7. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)
8. จัดทำระบบสำรอง
9. ให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
10. กำหนดหน้าที่ความรับผิดชอบที่ชัดเจน หากเกิดกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใด

แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับที่ 2)

- หน่วยงานของรัฐ **ต้องกำหนดความรับผิดชอบที่ชัดเจน**

- **ผู้บริหารระดับสูงของหน่วยงาน (CEO)**

  เป็นผู้รับผิดชอบต่อความเสียหายที่เกิดขึ้น แก่ระบบ

  คอมพิวเตอร์ ข้อมูล หรือผู้ใด จากความบกพร่องหรือฝ่าฝืน

ถ้าไม่ดูแลระบบให้ดีจนไปสร้างความเสียหายให้ผู้อื่น
CEO หน่วยงานต้องรับผิดชอบ

ที่มา: ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556

E-Evidence (ม.11)

ห้ามมิให้ปฏิเสธการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ (ม.11)

แต่ศาลจะเชื่อหรือไม่ ขึ้นอยู่กับ
ความน่าเชื่อถือของพยานหลักฐาน
การชั่งน้ำหนักพยานหลักฐาน

มาตรา 25 แห่ง พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ฯ

+

พ.ร.ฎ.ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

เกณฑ์ขั้นต่ำที่กฎหมายกำหนดในแต่ละเรื่อง **มาตรา 8-31**

วิธีการแบบปลอดภัย

ประโยชน์จาก**ข้อสันนิษฐานตามกฎหมาย**
ว่าได้ใช้วิธีการที่น่าเชื่อถือในการทำธุรกรรม

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ดังนี้
- ✓ ความมั่นคงปลอดภัยด้านการบริหารจัดการและระบบสารสนเทศ
- ✓ การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ / ข้อมูลอิเล็กทรอนิกส์
- ✓ การจัดการเหตุการณ์ที่ไม่พึงประสงค์ด้านความมั่นคงปลอดภัย
- ✓ ความต่อเนื่องในการให้บริการ เป็นต้น

หากพยานหลักฐานทางอิเล็กทรอนิกส์ขาดความน่าเชื่อถือ อาจส่งผลต่อรูปคดี

การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบมั่นคงปลอดภัย

(ประกาศ คธอ. เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555)

การประเมินระดับผลกระทบที่เกิดขึ้นใน 1 วัน	Security Basic ผลกระทบระดับต่ำ	Security Medium ผลกระทบระดับกลาง	Security High Level ผลกระทบระดับสูง
(1) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน	≤ 1 ล้านบาท	≧ 1 ล้านบาท ≤ 100 ล้านบาท	≧ 100 ล้านบาท
(2) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิตร่างการหรือนามัย	ไม่มีผู้ใช้บริการได้รับผลกระทบต่อชีวิตร่างกาย หรืออนามัย	ผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัย ≧ 1 คน ≤ 1,000 คน	ผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัย ≧ 1,000 คน หรือต่อชีวิตตั้งแต่ 1 คน
(3) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจาก (2)	ผู้ใช้บริการได้รับผลกระทบ ≤ 10,000 คน	ผู้ใช้บริการได้รับผลกระทบ ≧ 10,000 คน แต่ ≤ 100,000 คน	ผู้ใช้บริการได้รับผลกระทบ ≧ 100,000 คน
(4) ผลกระทบด้านความมั่นคงของรัฐ	**ไม่มี**ผลกระทบต่อความมั่นคงของรัฐ	-	**มี**ผลกระทบต่อความมั่นคงของรัฐ
		หากมีผลกระทบระดับกลางอย่างน้อย 2 ด้านขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับกลางขึ้นไป	หากมีผลกระทบระดับสูงเพียง 1 ด้านต้องใช้วิธีการแบบมั่นคงปลอดภัยในระดับเคร่งครัด

วิธีการที่น่าเชื่อถือ

มาตรา ๙ ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(๒) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

วิธีการที่เชื่อถือได้ตาม (๒) ให้คำนึงถึง

ก. ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคลสภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมายระดับความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

ข. ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ จำนวนครั้งหรือความสม่ำเสมอในการทำธุรกรรม ประเพณีทางการค้าหรือทางปฏิบัติ ความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

ค. ความรัดกุมของระบบการติดต่อสื่อสาร

ให้นำความในวรรคหนึ่งมาใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ ด้วยโดยอนุโลม

วิธีการที่น่าเชื่อถือ

มาตรา ๑๐ ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

(๑) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(๒) สามารถแสดงข้อความนั้นในภายหลังได้

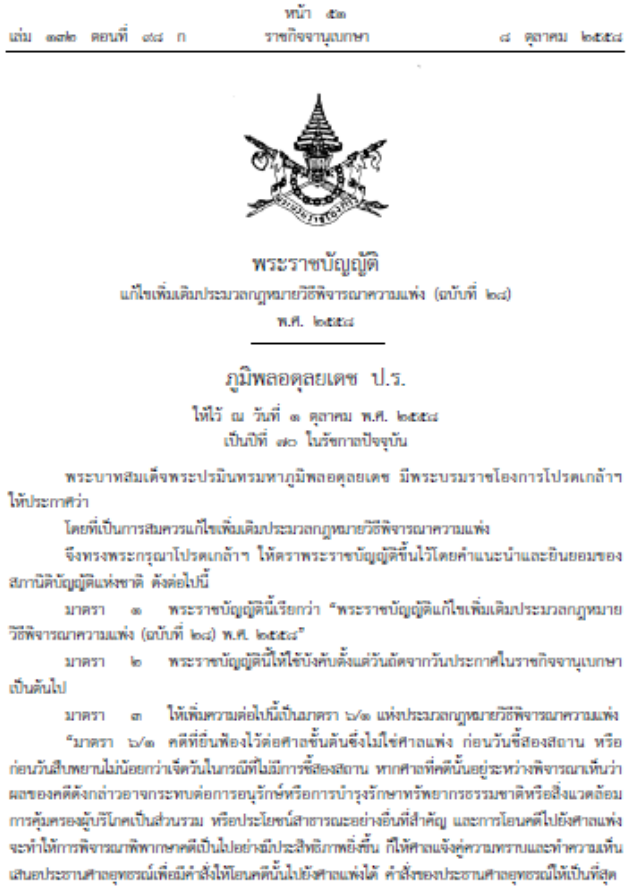
ความถูกต้องของข้อความตาม (๑) ให้พิจารณาถึงความครบถ้วนและไม่มีการในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความตาม (๑) ให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้น

ในกรณีที่มีการทำสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ตามวรรคหนึ่งสำหรับใช้อ้างอิงข้อความของข้อมูลอิเล็กทรอนิกส์ หากสิ่งพิมพ์ออกนั้นมีข้อความถูกต้องครบถ้วนตรงกับข้อมูลอิเล็กทรอนิกส์ และมีการรับรองสิ่งพิมพ์ออกโดยหน่วยงานที่มีอำนาจตามที่คณะกรรมการประกาศกำหนดแล้ว ให้ถือว่าสิ่งพิมพ์ออกดังกล่าวใช้แทนต้นฉบับได้[๕]

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

คำพิพากษาศาลฎีกา 8089/2556

- การเบิกถอนเงินสดจากบัญชีสินเชื่อเงินสด ผ่านตู้ ATM เป็นธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งรับฟังได้ตามมาตรา 7
- การนำบัตรกดเงินสดไปถอนเงินและใส่รหัสส่วนตัว เสมือนการลงลายมือชื่อตนเอง ซึ่งถือเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 9
- เมื่อจำเลยนำบัตรกดเงินสดไปถอนเงิน ใส่รหัสเพื่อทำรายการถอนเงิน และกดยืนยันทำรายการ พร้อมรับเงินสดและสลิป การกระทำดังกล่าวจึงถือเป็นหลักฐานการกู้ยืมเงิน ตามมาตรา 8 วรรคหนึ่ง



หน้า ๕๓
เล่ม ๑๓๒ ตอนที่ ๑๔๔ ก ราชกิจจานุเบกษา ๘ ตุลาคม ๒๕๕๘

พระราชบัญญัติ
แก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ ๒๘)
พ.ศ. ๒๕๕๘

ภูมิพลอดุลยเดช ป.ร.
ให้ไว้ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๕๘
เป็นปีที่ ๗๐ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ ๒๘) พ.ศ. ๒๕๕๘"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๖/๑ แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง

"มาตรา ๖/๑ คดีที่ยื่นฟ้องไว้ต่อศาลชั้นต้นซึ่งไม่ใช่ศาลแพ่ง ก่อนวันชี้สองสถาน หรือก่อนวันสืบพยานไม่น้อยกว่าเจ็ดวันในกรณีที่ไม่มีการชี้สองสถาน หากศาลที่คดีนั้นอยู่ระหว่างพิจารณาเห็นว่าผลของคดีดังกล่าวอาจกระทบต่อการอนุรักษ์หรือการบำรุงรักษาทรัพยากรธรรมชาติหรือสิ่งแวดล้อม การคุ้มครองผู้บริโภคเป็นส่วนรวม หรือประโยชน์สาธารณะอย่างอื่นที่สำคัญ และการโอนคดีไปยังศาลแพ่งจะทำให้การพิจารณาพิพากษาคดีเป็นไปอย่างมีประสิทธิภาพยิ่งขึ้น ก็ให้ศาลแจ้งคู่ความทราบและทำความเห็นเสนอประธานศาลอุทธรณ์เพื่อมีคำสั่งให้โอนคดีนั้นไปยังศาลแพ่งได้ คำสั่งของประธานศาลอุทธรณ์ให้เป็นที่สุด

ทิศทางการพัฒนา e-Court

พ.ร.บ. แก้ไขเพิ่มเติมประมวลวิธีพิจารณาความแพ่ง (ฉบับที่ 28) พ.ศ. 2558

ประกาศราชกิจจานุเบกษาเมื่อ 8 ตุลาคม 2558

- รองรับการจัดทำสารบบความ สำนวนความในรูปแบบข้อมูลอิเล็กทรอนิกส์ รวมถึง Print out ของข้อมูลดังกล่าว
- รองรับการยื่นคำคู่ความและเอกสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ เช่น ผ่านอีเมล

เทคโนโลยีและกฎหมาย ถูกนำมาปรับใช้ร่วมกันมากขึ้น

ธุรกรรม การติดต่อสื่อสารทำผ่านระบบออนไลน์มากขึ้น

สัญญากู้ยืมเงินทางอิเล็กทรอนิกส์
(ฎีกาที่ 8089/2556)

การเบิกถอนเงินสดจากบัญชีสินเชื่อเงินสด ผ่านตู้ ATM เป็นธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งรับฟังได้

การนำบัตรกดเงินสดไปถอนเงินและใส่รหัสส่วนตัว เสมือนการลงลายมือชื่อตนเอง ถือเป็นการลงลายมือชื่ออิเล็กทรอนิกส์

จำเลยนำบัตรกดเงินสดไปถอนเงิน ใส่รหัสเพื่อทำรายการถอนเงินและกดยืนยันทำรายการ พร้อมรับเงินสดและสลิป ถือเป็นหลักฐานการกู้ยืมเงิน

Trend ของอาชญากรรมกำลังเพิ่มขึ้นในโลกอินเทอร์เน็ต

ฎีกายกฟ้อง คดี 112 'เบนโตะ' โพสต์บอร์ดประชาไท ชี้แค่เลข IP address บ่งชี้ไม่ได้ (ฎีกาที่ อ.599/2554)

Tue, 2015-10-20 14:29

หลังจากเมื่อวันที่ 11 ก.ย. ที่ผ่านมา ศาลอาญา รัชดา ได้นัดฟังคำพิพากษาศาลฎีกา คดีนพวรรณ หรือ เบนโตะ ผู้โพสต์ในเว็บบอร์ดประชาไทปี 51 แต่เนื่องจากจำเลยไม่มาศาล โดยนายประกันระบุว่าไม่สามารถติดต่อจำเลยได้ ศาลจึงอนุมัติหมายจับ เพื่อนำตัวมาฟังคำพิพากษา พร้อมเลื่อนฟังคำพิพากษามาวันนี้ (20 ต.ค. 58) ซึ่ง โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) รายงานว่า ศาลอ่านคำพิพากษาฎีกาคดีดังกล่าวสรุปความว่า "ตัวเลข IP address บ่งชี้ไม่ได้ว่าจำเลยมีความเกี่ยวโยงกับข้อความที่โพสต์และพยานโจทก์ก็มีความสงสัยตลอดมา ศาลจึงฎีกาจำเลยกลับ ให้ยกฟ้อง

โดย ประชาชาติธุรกิจ รายงานคำพิพากษาว่า ศาลฎีกาพิเคราะห์จากคำเบิกความของโจทก์ แล้วเห็นว่าไม่สอดคล้องกัน ซึ่งนางสาวนพวรรณ ก็ให้การปฏิเสธ มาโดยตลอด จึงยกประโยชน์แห่งความสงสัยให้จำเลย ศาลฎีกาพิพากษากลับยกฟ้อง

ที่มา www.prachatai.com/

THANK YOU