Type of Data

1. Banking Database
2. Other Database
3. Search Engine
4. People Search Websites
5. Social Media

พยานหลักฐานในคดีการเงินธนาคาร

1. การเก็บพยานหลักฐานในฐานะผู้ให้บริการ

2. การรวบรวมพยานหลักฐานในฐานะผู้สืบสวนค้นหาความจริง

ขั้นตอนการรวบรวมหลักฐานเพื่อแจ้งความดำเนินคดี

1. ซักถามปากคำลูกค้า ผู้เสียหาย ผู้เกี่ยวข้อง
2. ดูว่าประเด็นพิพาทอยู่ตรงจุดใด ลูกค้ายอมรับจุดใด ไม่ยอมรับจุดใด
3. พิจารณาเบื้องต้น ว่าเข้าข่ายผิดกฎหมายใด
4. เชื่อมโยงพยานหลักฐาน เช่น **CCTV ,** หมายเลขโทรศัพท์ **, IP Address , Statement ,** พยานบุคคล ฯลฯ จากนั้น เขียนแผนผังลำดับเวลาเหตุการณ์
5. มอบอำนาจให้ตัวแทนที่ทราบเหตุการณ์ มาแจ้งความ พร้อมนำ **Log** พยานหลักฐานที่มีมาประกอบ

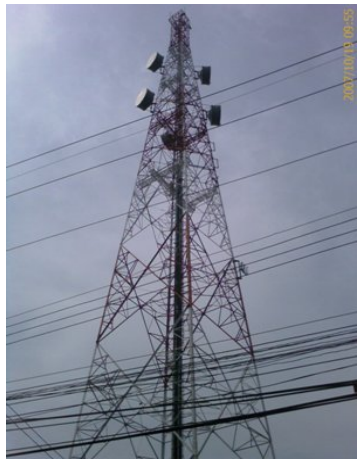
Fraud Investigation

1. Investigation by evidence
2. Open source intelligence (OSINT)
3. Technique investigation

5.1 Investigation by evidence

What is my ip address

223.24.56.253



Whois Domaintool

Pantip.com

203.151.13.166

223.24.56.253

5.2 Open source intelligence (OSINT)

5.3 Technique investigation

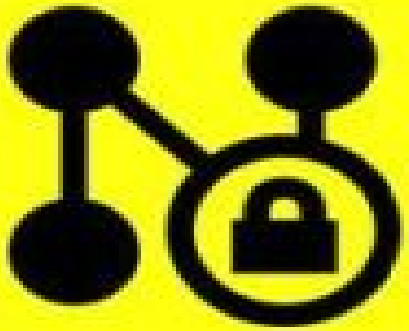
6.Fraud Law and Regulation

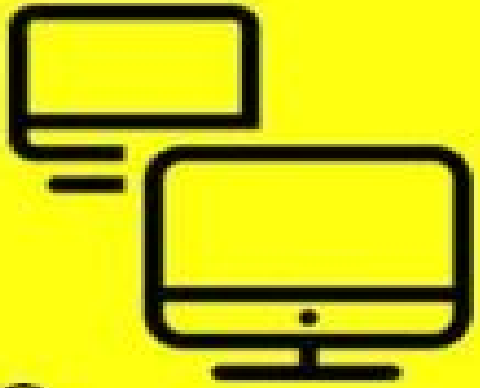
Privacy & Security

- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์
- พ.ร.บ.คอมพิวเตอร์

กฎหมายอื่นที่เกี่ยวข้อง

ร่าง พ.ร.บ.
มั่นคงปลอดภัยไซเบอร์
ไทย





กฎการรักษา
ความมั่นคงไซเบอร์
สหภาพยุโรป

EU Cybersecurity Directive : 2557

พ.ร.บ.ไซเบอร์ฯ ที่มา

- **Infrastructure** ถูกคนร้ายพยายามโจมตี ตลอดเวลา
- หากคนร้ายโจมตีสำเร็จ แม้เพียงครั้งเดียว จะเกิดความเสียหายวงกว้าง (กรณีธนาคารข้อมูลลูกค้ารั่วไหล)
- ทำให้เกิดความเชื่อมั่นจาก ตปท. เมื่อมาลงทุนในไทย
- เป็นที่มา พ.ร.บ.ไซเบอร์ ที่มุ่งป้องกันก่อนเกิดเหตุ **(Active)** ต่างจาก พ.ร.บ.คอมพิวเตอร์ ที่เป็นหลังเกิดเหตุค่อยหาตัว **(Passive)**

หน่วยงานหลัก ๆ

หน่วยงานควบคุมหรือกำกับดูแล

ดูแลการดำเนินงานของหน่วยงานรัฐหรือโครงสร้างพื้นฐานสำคัญให้มีมาตรฐาน เช่น ธนาคารแห่งประเทศไทย กำกับดูแลสถาบันการเงิน กสทช.กำกับดูแลผู้ให้บริการโทรคมนาคม

สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เป็นศูนย์กลางเฝ้าระวังความปลอดภัยไซเบอร์ของประเทศ และให้การช่วยเหลือในการป้องกันและรับมือเมื่อเกิดภัยคุกคามในระดับร้ายแรง

ภัยคุกคามทางไซเบอร์ระดับร้ายแรง

ระบบในการให้บริการที่สำคัญของหน่วยงานโครงสร้างพื้นฐานถูกโจมตี จนไม่สามารถให้บริการได้

ภัยคุกคามทางไซเบอร์ระดับวิกฤติ

ระบบบริการพื้นฐานที่สำคัญถูกโจมตี ไม่สามารถให้บริการได้เป็นวงกว้าง กระทบกับชีวิตและความปลอดภัยของประชาชนจำนวนมาก และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”
Critical Information Infrastructure (CII)

(1) ด้านความมั่นคงของรัฐ
(2) ด้านบริการภาครัฐที่สำคัญ
(3) ด้านการเงินการธนาคาร
(4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
(5) ด้านการขนส่งและโลจิสติกส์
(6) ด้านพลังงานและสาธารณูปโภค
(7) ด้านสาธารณสุข
(8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

* คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ส่วนที่ ๓

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๘ โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ และเป็นหน้าที่ของสำนักงานในการสนับสนุนและให้ความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑) ด้านความมั่นคงของรัฐ

(๒) ด้านบริการภาครัฐที่สำคัญ

(๓) ด้านการเงินการธนาคาร

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

(๕) ด้านการขนส่งและโลจิสติกส์

(๖) ด้านพลังงานและสาธารณูปโภค

(๗) ด้านสาธารณสุข

(๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

ส่วนที่ ๔
การรับมือกับภัยคุกคามทางไซเบอร์

มาตรา ๕๘ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

มาตรา ๗๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา ๕๗ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท

มาตรา ๖๐ การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรง

ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ทั้งนี้ รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้คณะกรรมการเป็นผู้ประกาศกำหนด

แนวทางดำเนินการความมั่นคงปลอดภัยไซเบอร์ระดับชาติ

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ในการกำหนดกรอบมาตรฐานตามวรรคหนึ่ง (๔) ให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

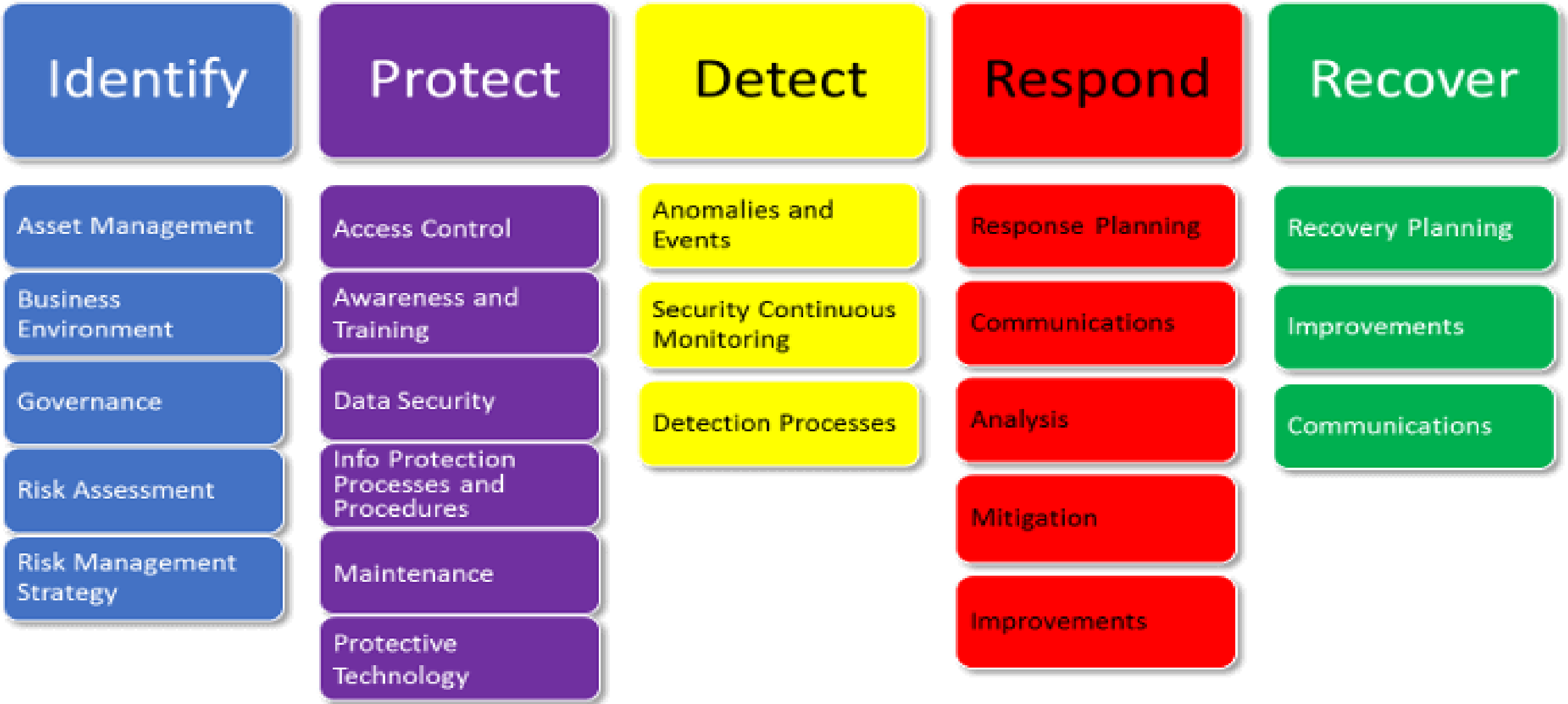
(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

NIST Cybersecurity Framework

Functions	Cybersecurity Framework (CSF) Core Functions:
IDENTIFY	**Identify**—Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
PROTECT	**Protect**—Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
DETECT	**Detect**—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
RESPOND	**Respond**—Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
RECOVER	**Recover**—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

NIST Cyber Security Framework



นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

กลุ่มเอไอเอส

1. บทนำ

1.1 วัตถุประสงค์

1) เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์
2) เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ รวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม
3) เพื่อให้พนักงานและผู้ที่ต้องใช้หรือเชื่อมต่อระบบคอมพิวเตอร์ของบริษัท ให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม
4) เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท โดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่างๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจของบริษัท

1.2 ขอบเขต

นโยบายฉบับนี้ครอบคลุมการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัท ทั้งที่อยู่ภายในหรือภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งคลาวด์ที่บริษัทจัดหา ซึ่งครอบคลุมถึง

1) พนักงานและหน่วยงานทั้งหมดของบริษัท
2) บุคคลภายนอกบริษัทที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์และข้อมูลสารสนเทศของบริษัท

1.3 หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยนี้ มีหลักการเพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- **ความลับ (Confidentiality)** – การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นกรรมสิทธิ์ของบริษัท
- **ความสมบูรณ์ (Integrity)** – การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- **ความพร้อมใช้งาน (Availability)** – การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้

วิธีการปฏิบัติงาน แผนฉุกเฉินกรณีการโจมตีระบบเทคโนโลยีสารสนเทศทางไซเบอร์

Cyber-attack on Information Technology System

Contingency Plan

SECTION : DOCUMENT CONTROL

DEPARTMENT :

หมายเลขเอกสาร DOCUMENT NO.:	แก้ไข REV.	วันที่มีผลบังคับใช้ EFFECTIVE DATE	จำนวนหน้า Q'TY PAGE
	0		12

TB-CERT

Manupat | Home | Create

TB-CERT

Home

Reviews

Photos

Posts

About

Community

Create a Page

Liked | Following | Share | ...

Send Message

Write a post...

Photo/Video | Tag Friends | Check in | ...

Search for posts on this Page

Visitor Posts

Chat

gambling-web-62/?fbclid=IwAR1moJR03fYmI0XP5gKBEiWHPuSxEwiS_tKK1zpYJEU5mXveUTm1jRCBUIs

สรุปสาระ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์

- การทำธุรกรรมกับ ตปท. จะดูว่าเรามี **Cyber Security** และ **PDPA** ไหม
- กฎหมาย **Cyber Security** ไทย อ้างอิงสิงคโปร์เยอะสุด
- **ETDA** เป็นต้นเรื่องร่างกฎหมายนี้

- มีการตั้งสำนักงานและคณะกรรมการความมั่นคงปลอดภัยไซเบอร์เพื่อกำกับดูแล

- การป้องกัน รับมือ ลดความเสี่ยง เป็นจุดประสงค์ของ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ เพราะแต่ละหน่วยงาน ยังไม่ความพร้อม ไม่เท่ากัน

- **Critical Information Infrastructure (CII)**

- **PDPA** บังคับใช้กับทุกคน **CII** บังคับใช้เฉพาะกลุ่ม

- ตีความภัยคุกคามไซเบอร์ว่าครอบคลุมเพียงใด

- พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ ประเมินผลกระทบขณะเกิดเหตุยาก เพราะไม่มีเฉพาะเรื่องความมั่นคงปลอดภัยอย่างเดียว แต่มีผลกระทบเชิงธุรกิจด้วย
- พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ **Focus** ในระดับภัยร้ายแรงและระดับวิกฤติเท่านั้น
- ส่วนภัยไม่ร้ายแรง จะเป็น พ.ร.บ.คอมพิวเตอร์

- CII ต้องทำมาตรฐานขั้นต่ำหลายอย่าง ส่งผลให้เกิด Cost ทางธุรกิจ ดังนั้น การทำมาตรฐานกลางแบบ One Size Fit All (มาตรฐานเดียวใช้กับทุก Business Unit) จะไม่เหมาะ

- ดังนั้น ธนาคาร จะกำหนด Critical Service ของตนเอง ว่ามีอะไรบ้าง (ไม่อยู่ใน พ.ร.บ.ฯ แต่จะอยู่ในประกาศของกฎหมายลูก)

- เช่น Payment จำนวนตั้งแต่เท่าใด ถือเป็น Critical Service เป็นต้น

หลักคิดเปลี่ยนจาก หากถูกโจมตีจะป้องกันอย่างไร มาเป็น เมื่อถูกโจมตี จะตอบสนองอย่างไร

ปรับกลยุทธ์สู่ Cyber Resillience ต่อให้ถูกโจมตี ระบบ IT ยังคงต้องดำเนินต่อได้ ไม่เกิดเป็นอุปสรรคขัดขวางธุรกิจ

หลัก พ.ร.บ.ไซเบอร์ที่เกี่ยวกับธุรกิจการเงิน

<u>มาตรา 42</u> นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมาย และแนวทางอย่างน้อยดังต่อไปนี้ (1-8)

(7) สร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ม.46 แจ้งรายชื่อ จนท.บริหารและปฏิบัติการ ไปยัง สนง. คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ม.52 แจ้งรายชื่อและข้อมูลติดต่อเจ้าของ ผู้ครอบครอง ผู้ดูแลระบบคอมพิวเตอร์ ไปยังสำนักงานฯ

ม.53 ควบคุม กำกับดูแล ตรวจสอบ มาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์

ม.54 Audit IT Security อย่างน้อยปีละ 1 ครั้ง

ม.56 กำหนดให้มีกลไกหรือขั้นตอนการเฝ้าระวังภัย คุกคามทางไซเบอร์

ม.57 มีเหตุภัยคุกคามทางไซเบอร์อย่างมีนัยสำคัญต่อระบบของหน่วยงาน ให้รายงานสำนักงานฯ

ม.58 เกิดหรือคาดว่าจะเกิดการโจมตีทางไซเบอร์ ให้ **Digital Forensic** เพื่อหาสาเหตุและวิธีป้องกัน

ม.60 แบ่งระดับภัยคุกคามไซเบอร์ **3** ระดับ คือ ไม่ร้ายแรง ร้ายแรง และวิกฤติ (เพื่อกำหนดมาตรการรับมือที่ต่างกัน)

ม.73 ไม่รายงานเหตุภัยคุกคามไซเบอร์ โดยไม่มีเหตุอันควร ปรับไม่เกินสองแสนบาท

ม.77 ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้น เกิดจากการสั่งการหรือการกระทำ ของกรรมการหรือผู้จัดการหรือบุคคลใด ซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการ และละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ

พ.ร.บ.คอมพิวเตอร์ มาตรา 14

- โดยทุจริต หลอกลวง นำเข้าข้อมูลคอมฯที่บิดเบือน ปลอม เท็จ น่าจะเกิดความเสียหายแก่ประชาชน และไม่ใช่ความผิดฐานหมิ่นประมาท ทำต่อบุคคลหนึ่งบุคคลใด คุก 3 ปี ปรับไม่เกิน 60,000 บาท ยอมความได้
- นำเข้าข้อมูลเท็จ น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ โครงสร้างพื้นฐาน หรือเกิดความตื่นตระหนกแก่ประชาชน
- นำเข้าข้อมูลคอมพิวเตอร์ เป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ก่อการร้าย
- นำเข้าข้อมูลคอมพิวเตอร์ลามก และประชาชนทั่วไปอาจเข้าถึงได้
- เผยแพร่ ส่งต่อข้อมูลข้างต้น

คุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท

พ.ร.บ.คอมฯ ม.16

- นำเข้าข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น
- เป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลง
- น่าจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง

คุกไม่เกิน 3 ปี ปรับไม่เกิน 6 หมื่นบาท

- รูปคนตายก็เช่นกัน

ยอมความได้

พ.ร.บ.คอมฯ ม.5

- เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์
- ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ
- และมาตรการนั้นมิได้มีไว้สำหรับตน

คุกไม่เกิน 6 เดือน ปรับไม่เกินหนึ่งหมื่นบาท

พ.ร.บ.คอมฯ ม.7

- เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์
- ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ
- และมาตรการนั้นมิได้มีไว้สำหรับตน

คุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท

พ.ร.บ.คอมฯ ม.9

- ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง
- ข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

คุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท

พ.ร.บ.คอมฯ ม.10

- กระทำโดยมิชอบ เพื่อให้การทำงานของระบบคอมฯ ผู้อื่น
- ถูกระงับ ขัดขวาง รบกวนจนไม่สามารถทำงานได้ปกติ

คุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท

พ.ร.บ.คอมฯ ม.11

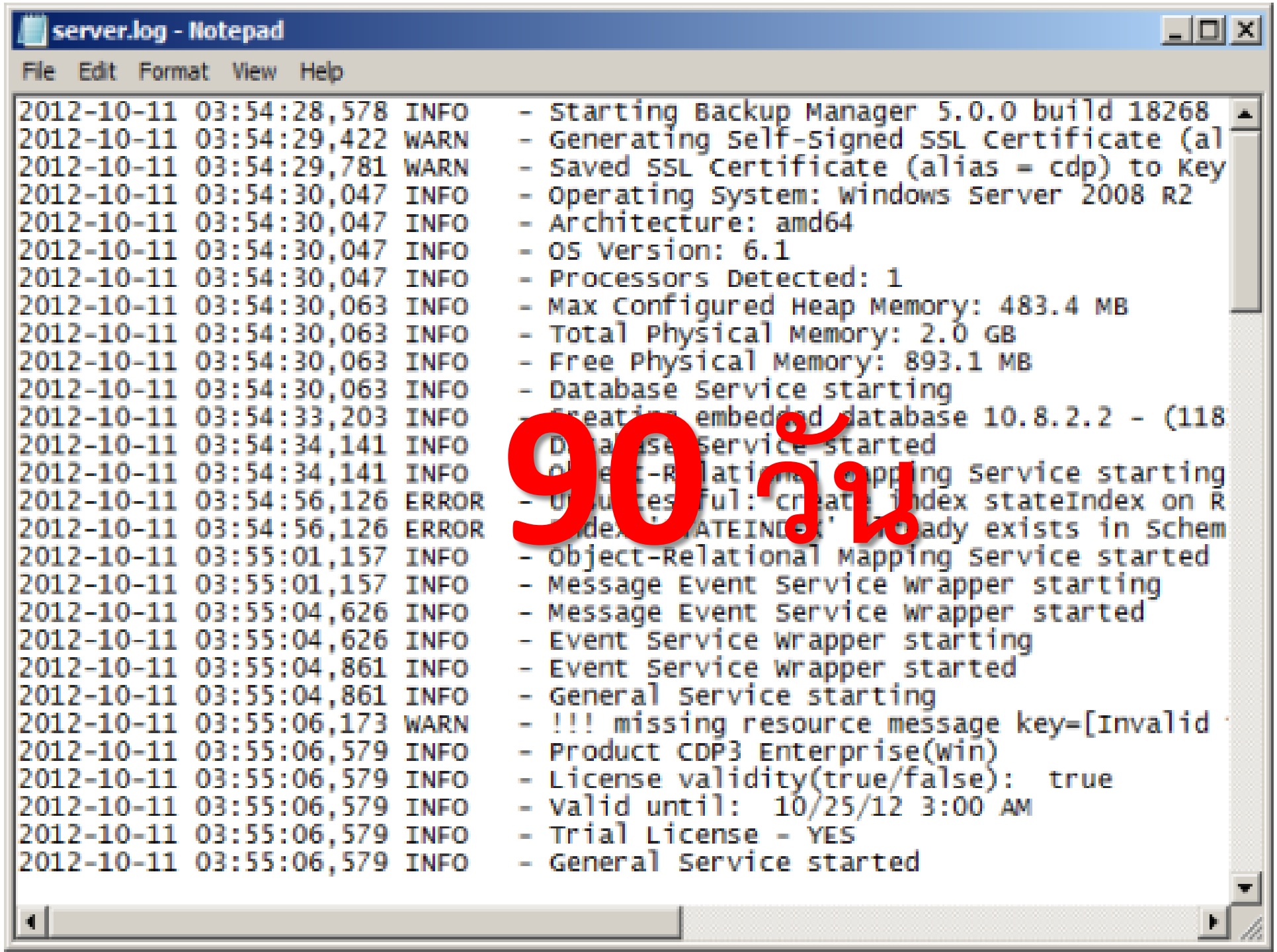
- ส่งข้อมูลคอมฯหรือจดหมายอิเล็กทรอนิกส์แก่ผู้อื่น
- ก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ
- ไม่เปิดโอกาสให้ผู้รับบอกเลิกการรับโดยง่าย

ปรับไม่เกิน 2 แสนบาท

พ.ร.บ.คอม

การเก็บ log

(ข้อมูลจราจรคอมพิวเตอร์)


server.log - Notepad
File Edit Format View Help
2012-10-11 03:54:28,578 INFO - Starting Backup Manager 5.0.0 build 18268
2012-10-11 03:54:29,422 WARN - Generating Self-Signed SSL Certificate (al
2012-10-11 03:54:29,781 WARN - Saved SSL Certificate (alias = cdp) to Key
2012-10-11 03:54:30,047 INFO - Operating System: Windows Server 2008 R2
2012-10-11 03:54:30,047 INFO - Architecture: amd64
2012-10-11 03:54:30,047 INFO - OS Version: 6.1
2012-10-11 03:54:30,047 INFO - Processors Detected: 1
2012-10-11 03:54:30,063 INFO - Max Configured Heap Memory: 483.4 MB
2012-10-11 03:54:30,063 INFO - Total Physical Memory: 2.0 GB
2012-10-11 03:54:30,063 INFO - Free Physical Memory: 893.1 MB
2012-10-11 03:54:30,063 INFO - Database Service starting
2012-10-11 03:54:33,203 INFO
2012-10-11 03:54:34,141 INFO
2012-10-11 03:54:34,141 INFO
2012-10-11 03:54:56,126 ERROR
2012-10-11 03:54:56,126 ERROR
2012-10-11 03:55:01,157 INFO - Object-Relational Mapping Service started
2012-10-11 03:55:01,157 INFO - Message Event Service Wrapper starting
2012-10-11 03:55:04,626 INFO - Message Event Service Wrapper started
2012-10-11 03:55:04,626 INFO - Event Service Wrapper starting
2012-10-11 03:55:04,861 INFO - Event Service Wrapper started
2012-10-11 03:55:04,861 INFO - General Service starting
2012-10-11 03:55:06,173 WARN - !!! missing resource message key=[Invalid
2012-10-11 03:55:06,579 INFO - Product CDP3 Enterprise(Win)
2012-10-11 03:55:06,579 INFO - License validity(true/false): true
2012-10-11 03:55:06,579 INFO - Valid until: 10/25/12 3:00 AM
2012-10-11 03:55:06,579 INFO - Trial License - YES
2012-10-11 03:55:06,579 INFO - General Service started
90%

กฎหมายอื่น ที่เกี่ยวข้อง

1. วิธีพิจารณาความแพ่งและพาณิชย์
2. หลักความยินยอม
3. วิธีพิจารณาความอาญา
4. ประกาศธนาคารแห่งประเทศไทย
5. ข้อเสนอแนะสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)
6. พรบ.ธุรกรรมทางอิเล็กทรอนิกส์

ป.วิ.แพ่ง ม.94

เมื่อกฎหมายบังคับให้ต้องมีหลักฐานเป็นเอกสารมาแสดง ห้ามไม่ให้ศาลรับฟังพยานบุคคล แม้คู่ความจะยินยอม ดังนี้

1 สืบพยานบุคคลแทนเอกสาร เมื่อไม่สามารถนำเอกสารมาแสดง

2 สืบพยานบุคคลประกอบข้ออ้าง เมื่อนำเอกสารมาแสดงแล้ว ว่ายังมีข้อความเพิ่มเติม ตัดทอน เปลี่ยนแปลงแก้ไข ข้อความในเอกสาร

เว้นแต่นำพยานบุคคล มาสืบประกอบ ข้ออ้างว่า <u>เอกสารนั้นเป็นเอกสารปลอมหรือไม่ถูกต้องทั้งหมด หรือแต่บางส่วน</u>

ป.อาญา ม.264

ทำเอกสารปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด
เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในเอกสารที่แท้จริง
หรือประทับตราปลอม หรือลงลายมือชื่อปลอมในเอกสาร
โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน
ถ้าได้กระทำเพื่อให้ ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นเอกสารที่แท้จริง
ผู้นั้นกระทำความผิดฐานปลอมเอกสาร

ป.อาญา ม.1 (14)

“บัตรอิเล็กทรอนิกส์” หมายความว่า

(ก) เอกสารหรือวัตถุอื่นใด ไม่ว่าจะมีรูปลักษณะใด ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้

(ข) ข้อมูล รหัส หมายเลขบัญชีหมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใด ๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในทำนองเดียวกับ (ก)

ป.อาญา ม.269 (5)

<u>ใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ</u> ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ

พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์

“ลายมือชื่ออิเล็กทรอนิกส์” หมายความว่า อักษร อักขระ ตัวเลข เสียง สัญลักษณ์อื่นใด ที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์

โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคล ผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 9 ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อ รับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(2) วิธีการดังกล่าว เป็นวิธีการที่เชื่อถือได้ โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 8 ภายใต้บังคับบทบัญญัติแห่งมาตรา 9
ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ
มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง
ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ ที่สามารถเข้าถึง
และนำกลับมาใช้ได้ โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความ
นั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานใน กระบวนการพิจารณาตามกฎหมาย ทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็น ข้อมูลอิเล็กทรอนิกส์

มาตรา 11 วรรค 2 ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

แต่ไม่ได้หมายความว่า ธนาคาร จะให้พนักงานติดต่อ ทำสัญญากับลูกค้า ผ่านทางไลน์ได้

พยานหลักฐานที่ได้จากเฟซบุ๊ก : คำพิพากษาฎีกาที่ 15386/2558

บันทึกรับสารภาพด้วยลายมือ ของ อ. ที่ว่า อ. ซื้อเมทแอมเฟตามีนจากจำเลย
โดยติดต่อทางโทรศัพท์เคลื่อนที่ และทางอินเทอร์เน็ตผ่านเว็บไซต์เฟซบุ๊กของจำเลย
และโอนเงินเข้าบัญชีธนาคารของจำเลย
เป็นคำซัดทอดผู้ที่กระทำความผิดด้วยกัน
แต่ก็มิได้กระทำเพื่อให้ตนเองพ้นผิดจากความผิด
และมีข้อเท็จจริง ทั้งเฟซบุ๊กของจำเลยและรายละเอียดบัญชีธนาคารของจำเลยที่
อ. โอนเงินเข้าบัญชีเพื่อชำระค่าเมทแอมเฟตามีน
เป็นข้อเท็จจริงแวดล้อมประกอบ ทำให้น่าเชื่อว่าจะพิสูจน์ความจริงได้
คำให้การของ อ. ดังกล่าว จึงรับฟังได้ยิ่งกว่าคำเบิกความเป็นพยานโจทก์ต่อศาล

ความสัมพันธ์ระหว่างข้อความในเฟซบุ๊คกับพยานหลักฐานทางกายภาพและพยานบุคคล หากมีความสัมพันธ์เชื่อมโยงกันมากขึ้นเท่าใด ก็ยิ่งทำให้พยานหลักฐานที่ได้มาทางอิเล็กทรอนิกส์มีความน่าเชื่อถือมากขึ้นเท่านั้น