ที่มาของ พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ
พ.ศ. ๒๕๕๐

สิ่งที่จะต้องคำนึงถึง

- องคร์กรของตนเองถือว่าเป็น “ผู้ให้บริการ” หรือไม่
- การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ หมายถึงข้อมูลอะไรบ้าง
- รูปแบบการจัดเก็บข้อมูลให้ถูกต้องตามวัตถุประสงค์ของ พรบ.
- ความพร้อมขององค์กรในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์
- ระยะผ่อนผันที่นับจากวันที่กฎหมายประกาศใช้

สิ่งที่จะต้องดำเนินการ

- แนวทาง หรือ Guideline ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ให้ถูกต้องและเหมาะสมกับลักษณะการใช้ระบบสารสนเทศ หรือระบบอินเทอร์เน็ตของแต่ละองค์กร
- การแต่งตั้งพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้งโดยรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ดังนั้น ICT จึงได้ประกาศกระทรวงสำหรับหลักเกณฑ์ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ดังกล่าว เพื่อให้เกิดความเหมาะสมในทางปฏิบัติ และเพื่อให้หลายองค์กรได้มีแนวทางที่ชัดเจนในการปฏิบัติว่าข้อมูลจราจรอะไรบ้างที่ควรจัดเก็บ ตลอดจนวิธีการจัดเก็บอย่างถูกต้องตรงตามลักษณะการใช้ระบบสารสนเทศหรือระบบอินเทอร์เน็ตของแต่ละองค์กร

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
ของผู้ให้บริการ พ.ศ. ๒๕๕๐

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

พ.ศ. ๒๕๕๐

ด้วยในปัจจุบันการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์เริ่มเข้าไปมีบทบาทและทวีความสำคัญเพิ่มขึ้นตามลำดับต่อระบบเศรษฐกิจและคุณภาพชีวิตของประชาชน แต่ในขณะเดียวกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีแนวโน้มขยายวงกว้าง และทวีความรุนแรงเพิ่มมากขึ้น ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว

อาศัยอำนาจตามความในมาตรา ๒๖ วรรค ๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ดังนั้น รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดหลักเกณฑ์ไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามประกาศนี้

ข้อ ๔ ในประกาศนี้

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ข้อ ๕ ภายใต้บังคับของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ง. ผู้ให้บริการร้านอินเทอร์เน็ต ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

(๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (๑) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก. แนบท้ายประกาศนี้

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องเก็บรักษา ปรากฏดังภาคผนวก ข. แนบท้ายประกาศนี้

ข้อ ๗ ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๑

(๒) ผู้ให้บริการตามข้อ ๕ (๑) ข. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามประเภท ชนิดและหน้าที่การให้บริการ

(๓) ผู้ให้บริการตามข้อ ๕ (๑) ค. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามประเภท ชนิดและหน้าที่การให้บริการ

(๔) ผู้ให้บริการตามข้อ ๕ (๑) ง. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๓

(๕) ผู้ให้บริการตามข้อ ๕ (๒) มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๔

ทั้งนี้ ในการเก็บรักษาข้อมูลจราจรตามภาคผนวกต่าง ๆ ที่กล่าวไปข้างต้นนั้น ให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น

ข้อ ๘ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

(๓) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

(๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

(๕) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ ๑ ถึงข้อ ๔ ข้างต้น ได้ให้บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้ผู้ให้บริการในข้อ ๑ ถึงข้อ ๔ ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการ

เช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

ข้อ ๙ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ข้อ ๑๐ ผู้ให้บริการซึ่งมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ ๗ เริ่มเก็บข้อมูลดังกล่าวตามลำดับ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นสามสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

(๒) ให้ผู้ให้บริการตามข้อ ๕ (๑) ข. เฉพาะผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (ISP) เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

ผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ ๑๐ (๑) และข้อ ๑๐ (๒) ข้างต้น ให้เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

ประกาศ ณ. วันที่ ๒๑ สิงหาคม ๒๕๕๐

บทวิเคราะห์ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อ ๑ “หลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐”

วัตถุประสงค์ที่แท้จริงของพรบ.ก็คือเมื่อเกิดอาชญากรรมทางคอมพิวเตอร์ หลักฐานต่างๆทางคอมพิวเตอร์นั้นมีความน่าเชื่อถือค่อนข้างน้อยอยู่แล้วและมีโอกาสที่จะไม่พบร่องรอยของการก่ออาชญากรรม หลายครั้งเมื่อตำรวจหรือพนักงานเจ้าหน้าที่ได้เข้าไปขอข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการยกตัวอย่าง เช่น ISP พบว่า ISP ไม่ได้เก็บข้อมูลจราจรดังกล่าว หรือ เก็บไว้ไม่นานเพียงพอเนื่องจากมีพื้นที่จัดเก็บค่อนข้างจำกัดทำให้การพิสูจน์หลักฐานทางคอมพิวเตอร์ทำได้ยากลำบาก หรือ ไม่สามารถทำได้เนื่องจากข้อมูลไม่เพียงพอ ดังนั้นในพรบ.จึงจำเป็นที่จะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้อย่างชัดเจน โดยให้ถือว่าเป็นความรับผิดชอบต่อสังคมที่องค์กรทุกองค์กรต้องปฏิบัติและให้ความร่วมมือเมื่อมีการขอเรียกดูข้อมูลดังกล่าวโดยพนักงานเจ้าหน้าที่หลังจากมีอาชญากรรมเกิดขึ้น

ข้อ ๒ “ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป”

ข้อ ๓ “ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามประกาศนี้”

รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญในการประกาศใช้กฎกระทรวงที่อาจออกตามมาหลังจากการประกาศใช้พรบ.เป็นระยๆ เพราะฉะนั้นเราจึงควรติดตามข้อมูลข่าวสารจากกระทรวงอย่างต่อเนื่อง

ข้อ ๔ “ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนด คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ข้อ ๕ ภายใต้บังคับของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง ยกตัวอย่าง เช่น บริษัทผู้ให้บริการโทรศัพท์เคลื่อนที่ ได้แก่ AIS, DTAC, True Move, HUTCH เป็นต้น

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ นอกจากจะหมายถึง ISP แล้วยังหมายถึงบริษัท โรงเรียน มหาวิทยาลัย และองค์กรทั้งภาครัฐและเอกชนส่วนใหญ่โดยทั่วไป

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ผู้ให้บริการเช่าระบบคอมพิวเตอร์ ยกตัวอย่าง เช่น ผู้ให้บริการเช่า Web Site หรือ Web Hosting

ง. ผู้ให้บริการร้านอินเทอร์เน็ต ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ผู้ให้บริการร้านอินเทอร์เน็ต ยกตัวอย่าง เช่น Internet Cafe ทั่วไป

(๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (๑)

(Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก. แนบท้ายประกาศนี้

ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider) ยกตัวอย่าง เช่น web sanook ,kapook หรือ pantip เป็นต้น

ภาคผนวก ก

แนบท้ายประกาศรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

พ.ศ. ๒๕๕๐

๑. ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบุคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น ตามข้อ ๕ (๑) สามารถจำแนกได้ ๓ ประเภท ดังนี้

ประเภท	ตัวอย่างของผู้ให้บริการ
ก. ผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)	๑) ผู้ให้บริการโทรศัพท์พื้นฐาน (Fixed line service provider) ๒) ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile service provider) ๓) ผู้ให้บริการวงจรเช่า (Leased circuit service provider) เช่น ผู้ให้บริการ leased line, ผู้ให้บริการสายเช่า fiber optic, ผู้ให้บริการ ADSL, ผู้ให้บริการ frame relay, ผู้ให้บริการ ATM, ผู้ให้บริการ MPLS เป็นต้น เว้นแต่ผู้ให้บริการนั้นให้บริการแต่เพียง physical media หรือสายสัญญาณอย่างเดียว (cabling) เท่านั้น (เช่น ผู้ให้บริการ Dark Fiber , ผู้ให้บริการสายใยแก้วนำแสง ซึ่งอาจไม่มีสัญญาน Internet หรือไม่มี IP traffic) ๔) ผู้ให้บริการดาวเทียม (Satellite service provider)

ประเภท	ตัวอย่างของผู้ให้บริการ
ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	๑) ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย ๒) ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด ๓) ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัท หรือ สถาบันการศึกษา

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)	*๑) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web hosting) (ตัวอย่าง การให้บริการเช่า Web server* *๒) ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File server หรือ File sharing)* *๓) ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider)* *๔) ผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)*
ง. ผู้ให้บริการร้านอินเทอร์เน็ต	*๑.ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Cafe)* *๒.ผู้ให้บริการร้านเกมออนไลน์ (Game Online)*

๒. ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม ข้อ ๕ (๒) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก แนบท้ายประกาศนี้

ประเภท	*ตัวอย่างของผู้ให้บริการ*
ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content and Application Provider)	*๑) ผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (blog)* *๒) ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic payment service provider)* *๓) ผู้ให้บริการเว็บเซอร์วิส (Web services)* *๔) ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)*

ภาคผนวก ข

แนบท้ายประกาศรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

พ.ศ. ๒๕๕๐

๑. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ก. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	*รายการ*
ก.ข้อมูลที่สามารถระบุและติดตามถึงแหล่งกำเนิด ต้นทาง ปลายทาง และทางสายที่ผ่านของการติดต่อสื่อสารของระบบคอมพิวเตอร์	*ข้อมูลระบบชุมสายโทรศัพท์พื้นฐาน โทรศัพท์วิทยุมือถือ และระบบตู้โทรศัพท์สาขา* ***(fixed network telephony and mobile telephony)*** *-หมายเลขโทรศัพท์ หรือ เลขหมายวงจร รวมทั้งบริการเสริมอื่นๆ เช่น บริการโอนสาย และหมายเลขโทรศัพท์ที่ได้โอนสาย รวมทั้งหมายเลขโทรศัพท์ซึ่งถูกเรียกจากโทรศัพท์ที่มีการโอน* *-ชื่อ ที่อยู่ของผู้ใช้บริการหรือผู้ใช้งานที่ลงทะเบียน* ***(name and address of subscriber or registered user)*** *- ข้อมูลเกี่ยวกับวันที่, เวลา และที่ตั้งของ Cell ID ซึ่งมีการใช้บริการ* ***(date and time of the initial activation of the service and the location label (Cell ID))***

ข.ข้อมูลที่สามารถระบุวันที่ เวลา และระยะเวลาของการติดต่อสื่อสารของระบบคอมพิวเตอร์	วันที่ รวมทั้งเวลาเริ่มต้นและสิ้นสุดของการใช้งาน (fixed network telephony and mobile telephony, the date and time of the start and end of the communication)
ค.ข้อมูลซึ่งสามารถระบุที่ตั้งในการใช้โทรศัพท์มือถือ หรืออุปกรณ์ติดต่อสื่อสารแบบไร้สาย (Mobile communication equipment)	๑)ที่ตั้ง label ในการเชื่อมต่อ (Cell ID) ณ สถานที่เริ่มติดต่อสื่อสาร ๒)ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถืออันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร ๓)จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

๒. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ข. ถึง ค. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	*รายการ*
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	*๑) ข้อมูล log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่ายซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access logs specific to authentication and authorization servers, such as TACACS+ or RADIUS or DIAMETER used to control access to IP routers or network access servers)* *๒) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server* *๓) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)* *๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP address)* *๕) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling line Identification)*

ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)	*๑) ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (Simple Mail Transfer Protocol : SMTP Log)ซึ่งได้แก่* *- ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)* *-ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-mail Address)* *- ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-mail Address* *- ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมายอิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น* *๒) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server)*

๓) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of Client Connected to server)

๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)

๕) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)

๖) ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อดึงจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ที่เครื่องให้บริการ (POP3 (Post Office Protocol version 3) Log or IMAP4 (Internet Message Access Protocol Version 4) Log)

ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล

๑) ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล

๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)

๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP source address)

๔) ข้อมูลชื่อผู้ใช้งาน (User ID)

๕) ข้อมูลตำแหน่ง (path) และ ชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป (Path and filename of data object uploaded or downloaded)

๔) ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	*๑) ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ* *๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ* *๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น* *๔) ข้อมูลคำสั่งการใช้งานระบบ* *๕) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI : Uniform Resource Identifier) เช่น ตำแหน่งของเว็บเพจ*

จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)	*๑) ข้อมูล log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP log)* *๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)* *๓) ข้อมูลหมายเลข port ในการใช้งาน (Protocol process ID)* *๔) ข้อมูลชื่อเครื่องให้บริการ (Host name)* *๕) ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted message ID)*
ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น	*ข้อมูล log เช่นข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and time of connection of client to server) และ/หรือข้อมูลชื่อเครื่องบนเครือข่าย และ/หรือหมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Hostname and/or IP address) เป็นต้น*

บทวิเคราะห์ : การเข้าถึงระบบเครือข่าย เช่น การเข้าถึงจากระยะไกลผ่านระบบ Remote access จำเป็นต้องมีการ log on หรือ sign on กับ authentication server เช่น RADIUS server เพื่อระบุตัวตนของผู้ใช้บริการโดยระบบควรมีการจัดเก็บชื่อผู้ใช้บริการ, เวลาที่เข้าใช้บริการและหมายเลข IP address ของผู้ใช้บริการ เป็นต้น สำหรับการ log on ในระบบ LAN ผ่านทางระบบ Microsoft Active Directory จาก PC client หรือ Notebook ที่ใช้ Windows XP ขึ้นไปก็ควรมีการจัดเก็บข้อมูลจราจรในลักษณะเดียวกันกับการใช้งานผ่านทางระบบ Remote access เป็นต้น

๓. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ง. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

ประเภท	*รายการ*
ก. ผู้ให้บริการร้านอินเทอร์เน็ต	*๑)ข้อมูลที่สามารถระบุตัวบุคคล* *๒)เวลาของการเข้าใช้ และเลิกใช้บริการ* *๓)หมายเลขเครื่องที่ใช้ IP Address (Internet Protocol Address)*

บทวิเคราะห์ : ผู้ให้บริการร้านอินเตอร์เน็ตมีหน้าที่เก็บข้อมูล 3 ประเภท ได้แก่ข้อมูลที่สามารถระบุตัวบุคคล เช่น เลขประจำตัวบัตรประชาชนของผู้มาใช้บริการหรือรูปถ่ายของผู้มาใช้บริการจากกล้องดิจิตอล หรือกล้องโทรทัศน์วงจรปิดก็ได้เช่นกัน และต้องเก็บเวลาการเข้าใช้และเวลาการเลิกใช้บริการของผู้ใช้บริการด้วยวิธีใดก็ได้แล้วแต่ความสะดวกของผู้ให้บริการ รวมถึงต้องจัดเก็บหมายเลข รวมถึงต้องจัดเก็บหมายเลข IP address ของคอมพิวเตอร์ที่ให้บริการแต่ละเครื่องให้สอดคล้องกับผู้ใช้บริการและเวลาที่ใช้ เพื่อให้สามารถระบุตัวตนของผู้ใช้บริการในขณะใดขณะหนึ่งได้

๔. ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๒) มีหน้าที่ต้องเก็บรักษามีดังต่อไปนี้

ประเภท	*รายการ*
ก. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	*๑) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ และ/หรือเลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการ และ/หรือเลขประจำตัวผู้ใช้บริการ (User ID) และ/หรือที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ* *๒) บันทึกข้อมูลการเข้าใช้บริการ* *๓) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือ ผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล*

บทวิเคราะห์ : โดยปกติแล้วผู้ที่เข้ามาแสดงความเห็นในเว็บบอร์ดมักจะไม่ลงชื่อและไม่ลงทะเบียน เมื่อมีข้อพิพาทเกิดขึ้น เช่น มีการหมิ่นประมาท ก็มักจะหาตัวของคู่กรณีไม่พบ ดังนั้นกฎหมายจึงระบุให้ผู้ให้บริการเว็บบอร์ด หรือ ผู้ให้บริการที่อนุญาติให้บุคคลทั่วไปเข้ามาแสดงความคิดเห็นได้ ยกตัวอย่าง เช่น เว็บของหนังสือพิมพ์ต่างๆในทุกวันนี้ ควรต้องมีระบบสมาชิกที่สามารถระบุตัวตนของผู้ที่เข้ามาแสดงความคิดเห็นได้ เช่น ชื่อ ที่อยู่ หรือ **Email address** ของผู้ใช้บริการที่พอจะตามตัวได้ ตลอดจนบันทึกข้อมูลการเข้าใช้บริการว่ามาจาก **IP address** ใด ซึ่งส่วนใหญ่จะเก็บไว้ใน **Log File** ของ **Web Server** อยู่แล้ว

ระบบโครงสร้างพื้นฐานที่องค์กรควรจัดทำเพื่อรองรับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ระบบโครงสร้างพื้นฐานสารสนเทศ (IT infrastructure) ที่องค์กรควรจัดทำเพื่อรองรับ พรบ.การกระทำผิดเกี่ยวกับคอมพิวเตอร์นั้นควรมีระบบอย่างน้อย ดังต่อไปนี้

ระบบที่จำเป็นต้องมี (Mandatory)

- ระบบโครงสร้างพื้นฐานสำหรับการพิสูจน์ตัวตน (Identification and Authentication System)
- ระบบโครงสร้างพื้นฐานสำหรับการเก็บปูมระบบที่ส่วนกลาง (Centralized Log Management System) หรือ ระบบ SEM (Security Event Management System)
- ระบบโครงสร้างพื้นฐานสำหรับการกำหนดเวลาให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยใช้ NTP (Network Time Protocol)

ระบบที่ช่วยเพิ่มประสิทธิภาพ (Add-on Option)

- ระบบวิเคราะห์ปูมระบบ (Security Information Management System)
- ระบบบริหารจัดการการใช้งานระบบเครือข่าย (Bandwidth Management System)
- ระบบ Proxy Cache
- ระบบ ANTI-MalWare
- ระบบ ANTI-SPAM
- ระบบ Patch Management

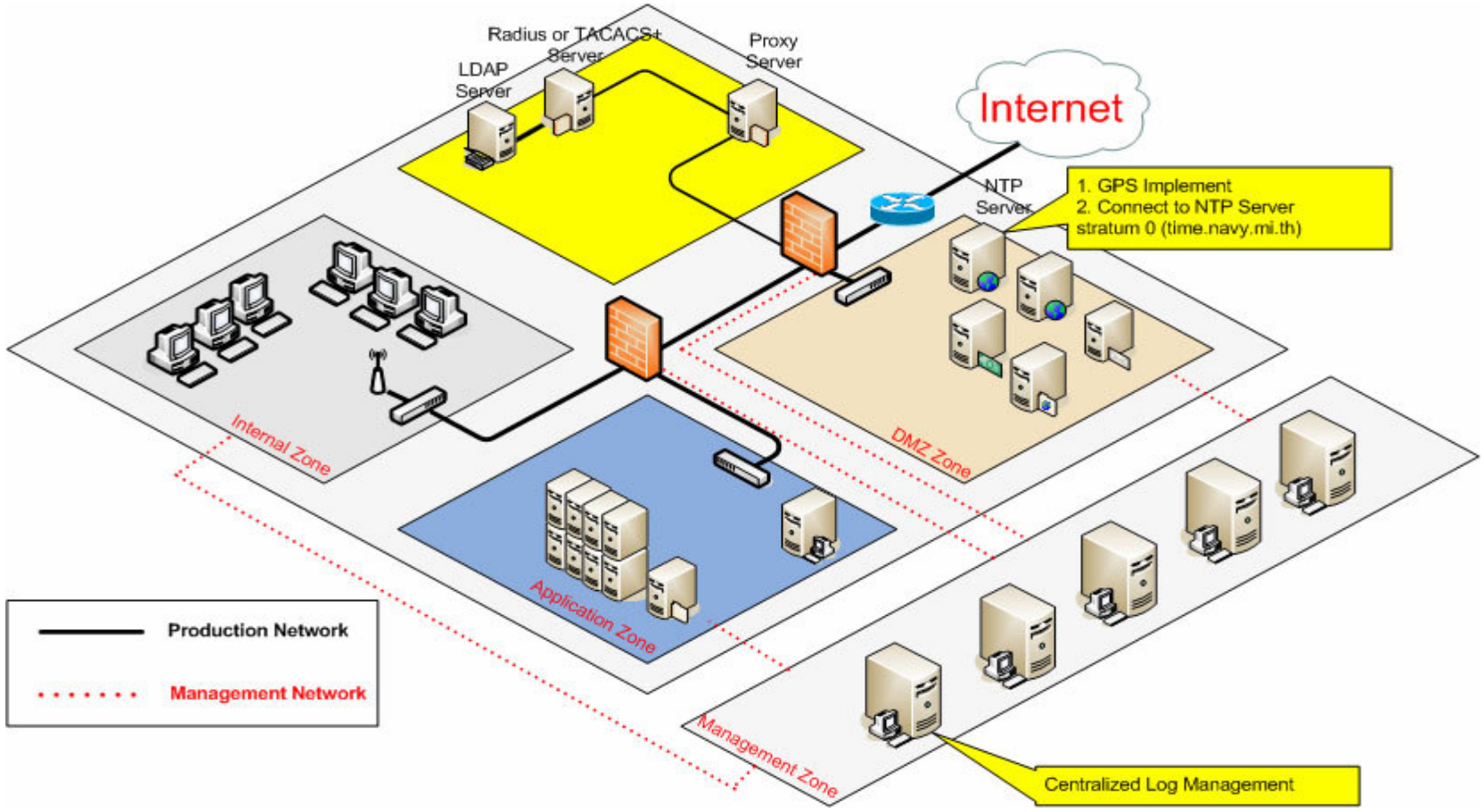
รายละเอียดการจัดเก็บ Log
ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
ของผู้ให้บริการ ตามประกาศข้อ ๕ (๑) ข. ถึง ค.

(1) การเก็บ Log ที่เกิดจากการเข้าถึงระบบเครือข่าย (Authentication Server)

- ระบบ Local Area Network (LAN) ที่เราใช้กันอยู่ในทุกวันนี้ โดยปกติแล้วไม่มีการ Logon เข้าระบบ Domain ที่ส่วนกลาง – หลายองค์กรมีการ Logon แบบ “Local Logon” คือ Logon เข้าที่เครื่องตนเอง
- ควรให้ทุกเครื่องในระบบเครือข่ายขององค์กรทำการ “Join Domain” เชื่อมเข้าสู่ระบบการพิสูจน์ตัวตนจากส่วนกลาง (Microsoft Active Directory) เพราะการ Logon จะเกิดขึ้นที่เครื่อง Domain Controller (DC) – ดังนั้น การจัดเก็บ Log การ Logon เข้า – ออก ก็สามารถทำได้ง่ายจากส่วนกลาง โดยเราสามารถดึง Log จาก Domain Controller มายัง Centralized Log Server

ตัวอย่างโปรดักส์ RADIUS/TACACS+ ที่นิยมในท้องตลาด



(2) การเก็บ Log ที่เครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (eMail Server)

- กรณีการใช้ Free eMail (ที่เป็น Web-based eMail)
  - การเก็บ Log ที่ทางประกาศกระทรวงฯ ให้จัดเก็บนั้นทำได้ยากลำบาก เพราะไม่ได้มีการเก็บ eMail ไว้ที่เครื่องแม่ข่ายในองค์กร
  - ทำได้แค่เพียงจัดเก็บการ Authenticate กับ Proxy Sever หรือ Firewall ก่อนที่จะออกสู่ระบบอินเทอร์เน็ต เท่านั้น
  - การ Authentication ที่ Hotmail หรือ Gmail นั้นก็จัดเก็บได้ยาก เพราะเป็นการ Authentication ด้วย SSL Protocol (https)
    - การ Terminate SSL ต้องใช้ Key ในการถอดรหัส SSL Session เพื่อบันทึก Username ในทางเทคนิคสามารถทำได้ แต่ค่อนข้างยากและอุปกรณ์มีราคาสูงพอสมควร

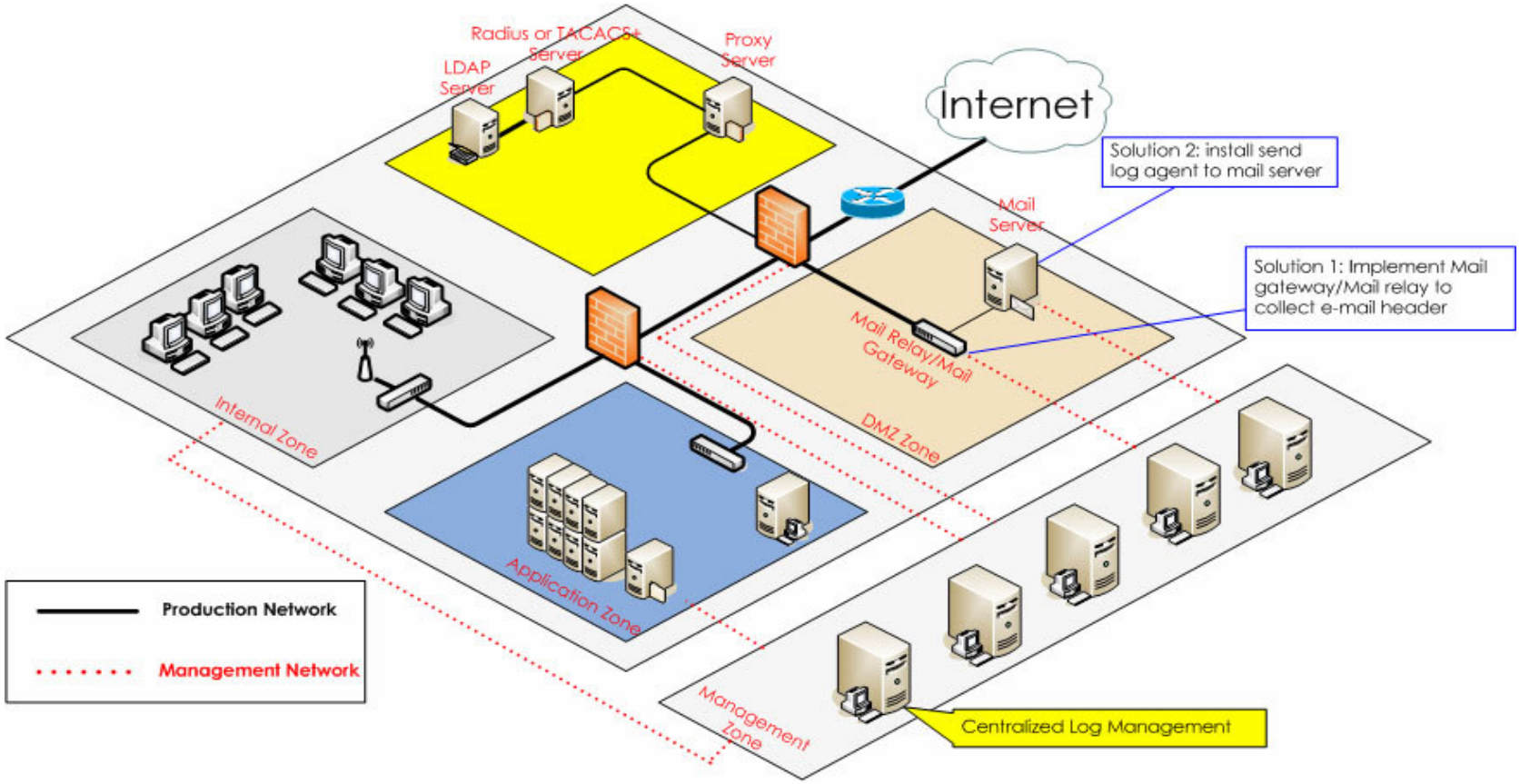
(2) การเก็บ Log ที่เครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (eMail Server)

- สำหรับองค์กรที่มีระบบ eMail เป็นของตัวเอง เช่น Microsoft Exchange หรือ Lotus Notes
- ควรที่จะจัดเก็บข้อมูล eMail Log ตามที่ประกาศกระทรวงฯ ได้กำหนดไว้
  - จัดเก็บ เฉพาะ eMail Header เท่านั้น ไม่ต้องเก็บ Body (เนื้อความ) ของ eMail
  - ไม่ต้องเก็บ attached File (ไฟล์แนบ)
- เพื่อเป็นการป้องกันไม่ให้ผู้ใช้ลบ eMail ในกรณีดังกล่าว ควรมีการ archive eMail หรือ backup eMail เก็บไว้เสียก่อนเป็นระยะๆ

(2) การเก็บ Log ที่เครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (eMail Server)

- การดึง Log ออกจาก eMail Server ต้องการการติดตั้ง และปรับแต่งในระดับลึก จึงควรศึกษา หรือว่าจ้างผู้เชี่ยวชาญมาช่วยในการติดตั้งและปรับแต่ง
- แนวคิดในการเก็บ Log ที่ Mail Relay หรือ Mail Gateway เช่น CISCO IronPort
- การนำข้อมูล Log จาก Router หรือ Switching ในรูปแบบของ Netflow Traffic
  - ต้องเป็นรุ่นที่มี Netflow Feature
  - อุปกรณ์ที่จัดเก็บ Log ใน Format ของ Netflow ต้องมีความจุของฮาร์ดดิสก์มากพอในระดับหนึ่ง
  - ต้องมีซอฟท์แวร์ในการวิเคราะห์ Netflow Traffic ด้วย (อาจใช้ Open source หรือ Freeware ก็ได้)

การเก็บ Log ที่เครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (eMail Server)



(3) การจัดเก็บ Log จากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล (File Sharing Server)

- ระบบที่ใช้การโอนถ่ายไฟล์ข้อมูล ไม่ได้มีเฉพาะโปรโตคอล FTP
  - อาจใช้โปรโตคอลอื่น เช่น HTTP, SSH, https
  - โปรโตคอลที่ใช้ในการ Map Network Drive ในระบบของ Microsoft เช่น โปรโตคอล SMB
  - ในระบบ UNIX / LINUX นิยมใช้โปรโตคอล NFS

(3) การจัดเก็บ Log จากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล (File Sharing Server)

- ประกาศกระทรวง ฯ มีเจตนาให้ครอบคลุมทุกโปรโตคอลดังกล่าว
  - ระยะที่หนึ่ง ควรจัดเก็บข้อมูลการโอนย้ายถ่ายไฟล์ข้อมูลระหว่างระบบภายในกับระบบอินเทอร์เน็ต
  - ระยะที่ 2 ควรทำกับระบบโอนย้ายถ่ายไฟล์ข้อมูลภายในด้วย เผื่ออาจเกิดเหตุการณ์ Security Incident ขึ้นภายในองค์กรเองก็มีโอกาสที่เป็นไปได้เช่นกัน
- การจัดเก็บ Log ของระบบดังกล่าวให้เก็บเฉพาะชื่อไฟล์, วันเวลา, ชื่อผู้ใช้ และเส้นทาง (PATH) ที่เก็บไฟล์ในเครื่องแม่ข่าย
  - ไม่มีความจำเป็นต้องเก็บเนื้อไฟล์ซึ่งมีขนาดใหญ่จนหลายองค์กรไม่สามารถทำได้ในทางปฏิบัติ

(4) การจัดเก็บ log บนเครื่องผู้ให้บริการเว็บ (Web Server)

- หลายคนสับสนกับการจัดเก็บ log ของ Web Server ว่าเป็น “ขาเข้า” หรือ “ขาออก” กันแน่
- การจัดเก็บ log ของ Web Server เป็นการจัดเก็บ Log ใน “ขาเข้า” คือการที่บุคคลภายนอกเข้ามาเยี่ยมชม Web Site ขององค์กรเอง
- สำหรับการจัดเก็บข้อมูล “ขาออก” ให้อ้างไปยังข้อ (1) คือ การจัดเก็บ Log ในการเข้าถึงระบบเครือข่าย เช่น

(4) การจัดเก็บ log บนเครื่องผู้ให้บริการเว็บ (Web Server)

- ก่อนที่พนักงานจะใช้งานระบบอินเตอร์เน็ต ควรมีการ Logon หรือ Authentication ที่ Proxy Server หรือ Firewall เสียก่อน
- การใช้ Proxy Sever ก็สามารถจัดเก็บ URI (Uniform Resource Identifier) ที่ผู้ใช้งานอินเทอร์เน็ตในองค์กรเข้าเรียกชม Web site ต่างๆ ได้ เพื่อที่จะได้สามารถนำมา “MAP” หรือ เชื่อมโยงในการแกะรอยตามสืบสวนว่าใครเป็นคนใช้อินเตอร์เน็ตเข้า Web site ในช่วงเวลาดังกล่าว
- หากขาด Log ในส่วนใดส่วนหนึ่งไปก็จะทำให้หลักฐานไม่สมบูรณ์
- ประเด็นเรื่อง NTP Server ที่ควรติดตั้งในองค์กรโดยนำเวลาที่อ้างอิงมาจาก Stratum 0 มาจ่ายให้กับ Proxy Server และ Web Server ทั้งนี้ก็เพื่อให้ Log ใน Server ทั้งสองไม่ผิดเพี้ยนไปจากที่ควรจะเป็น

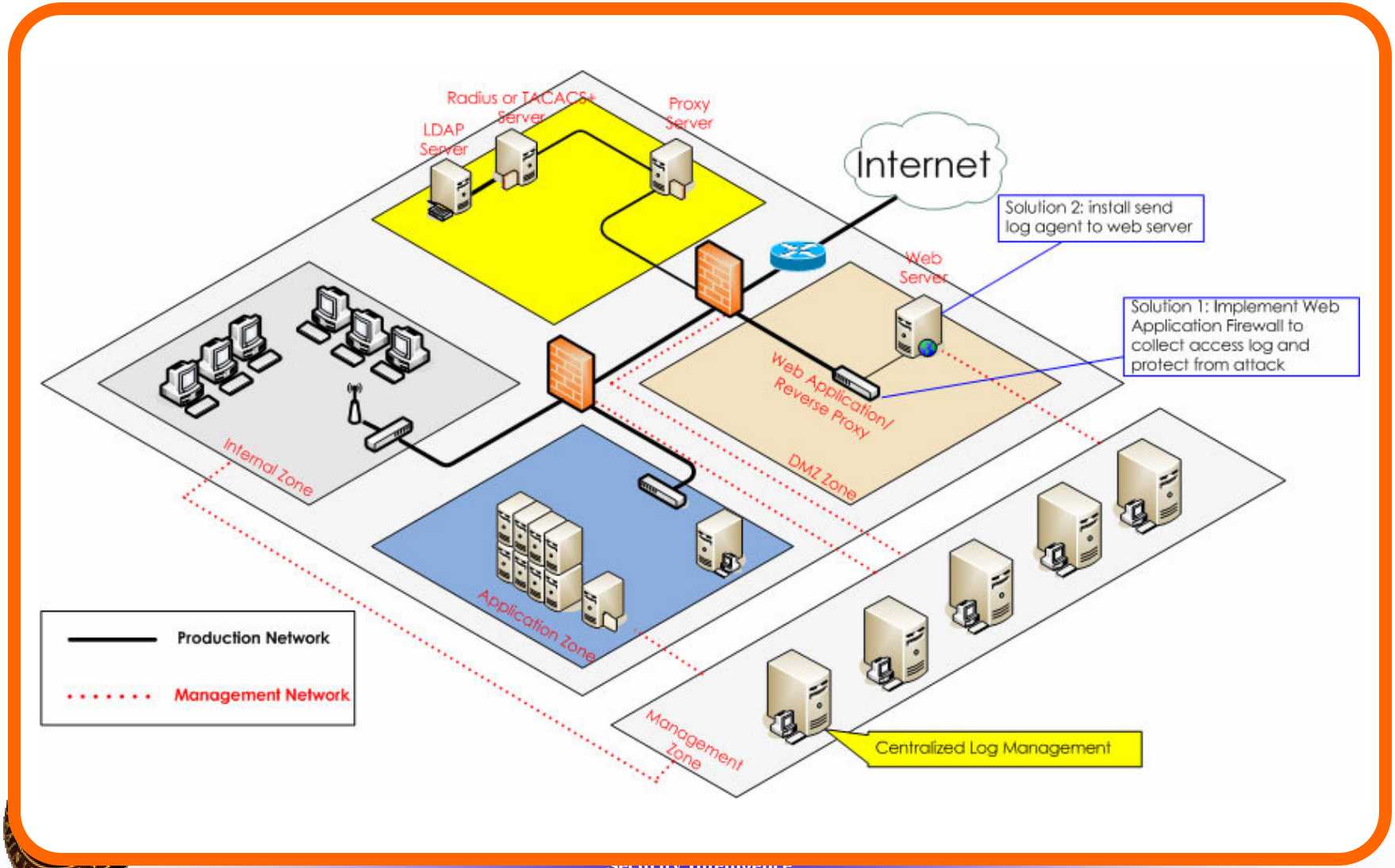
(4) การจัดเก็บ log บนเครื่องผู้ให้บริการเว็บ (Web Server)

- ปัญหาในการจัดเก็บ Log จาก Web Server
  - Web Server ที่เรานิยมใช้ ปกติแล้วจะไม่ส่ง Log มายัง Log Server ที่ส่วนกลาง เพราะเป็นธรรมชาติของ Web Server เอง
  - ต้องใช้วิธีติดตั้ง Agent หรือ การทำ “Batch Job” เพื่อส่งข้อมูล Log มายัง Log Server ที่ส่วนกลาง

(4) การจัดเก็บ log บนเครื่องผู้ให้บริการเว็บ (Web Server)

- อีกปัญหาหนึ่ง คือ Web Browser และ Web Server มักจะติดต่อกันด้วย 2 Method เป็นประจำ คือ Method “GET” และ Method “POST”
  - สำหรับ Method “GET” ทาง Web Server มีการจัดเก็บอยู่แล้วไม่มีปัญหา
  - สำหรับ Method “POST” ซึ่งมักจะมีการคีย์ข้อมูลของผู้เข้าถึง Web Server หรือ มีการคีย์ข้อมูลที่เป็นการโจมตีของแฮกเกอร์นั้น ปกติ Web Server จะไม่เก็บข้อมูล Method “Post” เหล่านี้ ดังนั้นเราต้องมีการจัดวาง “Reverse Proxy” หรือ “Web Application Firewall” มาช่วยในการเก็บข้อมูลดังกล่าว

(4) การจัดเก็บ log บนเครื่องผู้ให้บริการเว็บ (Web Server)



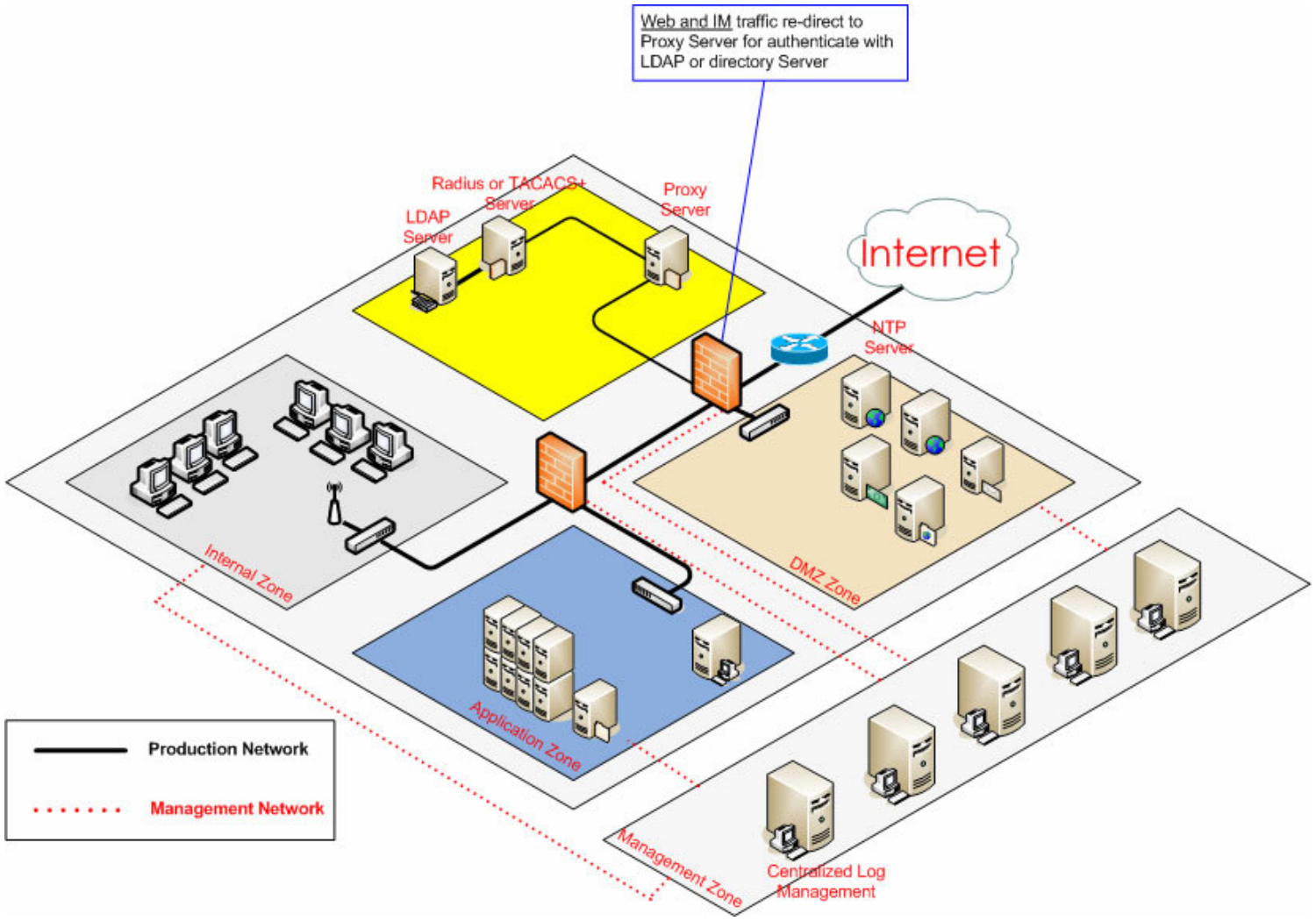
(5) การจัดเก็บ Log ของระบบ USENET

- ระบบ USENET หรือ NEWSGROUP ที่ใช้โปรโตคอล NNTP
- ในปัจจุบัน เราไม่ค่อยได้ใช้กันแล้วจึงไม่มีความจำเป็นต้องจัดเก็บแต่อย่างใด แต่ถ้ามีความจำเป็นต้องใช้ก็ต้องจัดวางโครงสร้างพื้นฐานให้รองรับการเก็บ Log ด้วย

(6) การจัดเก็บ Log ของระบบ IRC และ IM

- ในปัจจุบันการใช้งานโปรโตคอล IRC ไม่เป็นที่นิยมแล้ว เพราะผู้ใช้งานส่วนใหญ่นิยมใช้บริการ Instant Messaging เช่น MSN, Yahoo Messenger เป็นต้น
- ในโลกของแฮกเกอร์ กลับนิยมใช้โปรโตคอล IRC ในการควบคุม BOT ที่แฮกเกอร์ได้ทำการยึดเครื่องคอมพิวเตอร์ของเหยื่อแล้วควบคุมเครื่องเหล่านั้นหลายๆ เครื่อง ซึ่งกลายเป็นปัญหา “BOTNET” หรือ “Robot Network”
- การจัดเก็บ Log ของการใช้งาน IRC คงมีไม่มากนัก ถ้าจะดูการโจมตีด้วย BOTNET ก็สามารถดู Log จากระบบ IPS หรือ IDS ได้
- สำหรับ IM เราควรเก็บ Log เมื่อผู้ใช้ IM ทำการ “Authen” หรือ “Logon” เข้าสู่ระบบ แต่ควรแยกแยะได้ว่า เป็นการ Authen เพื่อออกไปใช้งาน Internet โดยทั่วไป หรือเป็นการ Authen เพื่อออกไปใช้งาน IM เช่น MSN เป็นต้น

(6) การจัดเก็บ Log ของระบบ IRC และ IM



ความเข้าใจผิดเกี่ยวกับ พรบ.ฯ
และประกาศกระทรวงเทคโนโลยีสารสนเทศ และการสื่อสารฯ

(1) เข้าใจว่าไม่ต้องเก็บ Log เป็นรายบุคคล และไม่ต้องมีระบบ Authentication

- การที่กฎหมายกำหนดให้มีการเก็บ Log อย่างน้อย 90 วันนั้น จะไม่มีประโยชน์เลย ถ้า Log ที่เก็บไว้ไม่สามารถระบุตัวบุคคลเป็นรายบุคคลได้
- วัตถุประสงค์ที่แท้จริงของกฎหมาย คือ การสืบสวนสอบสวนหาตัวผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์เป็นรายบุคคล
- ดังนั้น จึงจำเป็นต้องมีระบบ Authentication ที่เก็บข้อมูลผู้ใช้เป็นรายบุคคลแบบ “หนึ่งคน หนึ่งชื่อผู้ใช้ หนึ่งรหัสผ่าน” (Accountability) เพื่อให้สามารถแยกแยะตัวบุคคลได้ในที่สุด

(2) เข้าใจว่าไม่ต้องจัดเก็บ Log แบบ Centralized Log (เก็บลง Log Server ที่ส่วนกลาง)

- การเก็บ Log ของเครื่องแม่ข่ายและอุปกรณ์เครือข่ายต่างๆ นั้น เป็นเรื่องสำคัญที่มีความจำเป็นต้องเก็บ Log ลงบน Log Server ที่ส่วนกลาง
  - เนื่องด้วย Log ที่อยู่ในเครื่องแม่ข่ายสามารถถูกแก้ไขได้โดยผู้ดูแลระบบ (System Administrator) หรือสามารถถูกแก้ไขโดยแฮกเกอร์หรือไวรัสคอมพิวเตอร์ก็เป็นไปได้
  - ทำให้ความน่าเชื่อถือของ Log ที่มาจากเครื่องแม่ข่ายค่อนข้างต่ำ เวลานำขึ้นพิจารณาในชั้นศาล อาจจะไม่สามารถนำมาใช้ได้ เรียกว่า หลักฐานอ่อน ไม่มีน้ำหนักเพียงพอ
- ดังนั้น จึงควรจัดเก็บ Log ลงใน Log Server ที่ส่วนกลาง (Centralized Log Server) หรือใช้ระบบ SEM (Security Event Management) ก็จะสามารถเพิ่มความน่าเชื่อถือให้กับระบบการจัดเก็บ Log โดยรวม

(3) เข้าใจว่าไม่ต้องจัดทำ Security Awareness Training ให้กับผู้บริหารระดับสูง และผู้ใช้งานคอมพิวเตอร์ทั่วไป

- การให้ข้อมูลเรื่องกฎหมายกับผู้บริหารระดับสูงและผู้ใช้งานคอมพิวเตอร์ส่วนใหญ่ที่ไม่ใช่ “คนไอที” ถือเป็นเรื่องที่สำคัญอย่างยิ่งยวด ไม่สามารถจะมองข้ามได้ เ
- หากผู้บริหาร และผู้ใช้งานคอมพิวเตอร์ (โดยเฉพาะพนักงานทั่วไป) ไม่เข้าใจขั้นตอน ตลอดจนไม่ให้ความร่วมมือ โอกาสที่จะประสบความสำเร็จในเรื่องที่เราต้องการให้ทุกคนปฏิบัติตาม พรบ. การกระทำผิดเกี่ยวกับคอมพิวเตอร์ฯ ก็คงเป็นเรื่องที่ยากเต็มที
- ดังนั้น การที่ทุกคนควรจะมีความรู้ความเข้าใจจึงเป็นเรื่องที่องค์กรควรรีบเร่งปฏิบัติก่อนที่จะถึงเส้นตายที่กฎหมายได้กำหนดไว้

(4) เข้าใจว่าจัดซื้อจัดจ้างระบบจัดเก็บ Log ที่ส่วนกลางน่าจะเพียงพอแล้วกับการที่กฎกระทรวงฯ ประกาศบังคับ

- การจัดซื้อระบบเก็บ Log ที่ส่วนกลาง หรือ “SEM” เป็นเรื่องที่ควรทำ
  - ต้องติดตั้ง และปรับแต่งระบบที่จำเป็นต้องทำโดยผู้เชี่ยวชาญในอุปกรณ์แต่ละแบบที่มีความแตกต่างกัน
- การซื้อระบบเก็บ Log เป็นแค่จุดเริ่มต้นเท่านั้น
  - ยังต้องการการปรับแต่ง (Fine tuning) อีกมากพอสมควร
  - ระบบช่วยวิเคราะห์ Log ก็จะทำให้เรารู้ล่วงหน้าว่าระบบเรากำลังถูกโจมตีหรือไม่ เรียกว่า “Proactive Defense”
  - การ “Outsource” ใช้ MSSP (Managed Security Service Provider) น่าจะดีกว่าในมุมของ ROI และ TCO

(5) เข้าใจว่าการติดตั้งระบบ NTP Server นั้นยุ่งยาก และมีค่าใช้จ่ายสูง

- การติดตั้ง NTP Server สามารถทำได้โดยจัดหาเครื่องแม่ข่ายที่ไม่ต้อง Spec สูงมากนัก และติดตั้งโปรแกรม NTP Server ที่มีให้เลือกมากมายในอินเทอร์เน็ต ซึ่งไม่มีค่าใช้จ่ายแต่อย่างใด (เป็น Freeware หรือ Open source)
- รับค่าสัญญานนาฬิกาอ้างอิงจาก Stratum 0 เช่น กรมอุทกศาสตร์กองทัพเรือ หรือสถาบันมาตรวิทยา
  - เปิด Port UDP 123 ที่ไฟล์วอลล์ด้านนอกที่ต่อเชื่อมกับ ISP เพื่อให้สามารถ “SYNC” เวลาได้
- ในองค์กร ควรปรับแต่งค่าให้เครื่องแม่ข่าย และอุปกรณ์เครือข่ายทุกเครื่อง ให้อ้างอิงเวลาจาก NTP Server

10 ข้อควรปฏิบัติเพื่อความปลอดภัยขององค์กร และเป็นไปตามที่กฎหมายกำหนด

10 ข้อควรปฏิบัติเพื่อความปลอดภัยขององค์กร และเป็นไปตามที่กฎหมายกำหนด

- (M) ติดตั้ง Proxy Server, firewall, NAC or … เพื่อทำการ Authentication ระบุตัวตนของผู้ใช้งานระบบเครือข่ายเป็นรายบุคคลกับ RADIUS หรือ LDAP server
- (M) ติดตั้ง Microsoft Active Directory หรือ LDAP Server อื่นๆ เช่น OpenLDAP เพื่อเก็บชื่อผู้ใช้และรหัสผ่าน (directory service)
- (M) ติดตั้งระบบ NTP Server เพื่อตั้งค่านาฬิกาของระบบทั้งองค์กรให้ตรงกัน โดยอ้างอิงจาก Stratum 0 และ ปรับแต่งค่าเครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้อ้างอิงเวลากับ NTP Server ดังกล่าว
- (M) ติดตั้งระบบ SEM (security Event Management) หรือ ระบบ Centralized Log Management ที่สามารถกับ Log ได้ไม่น้อยกว่า 90วัน
- (A) ติดตั้งระบบ SIM (security Information Management) เพื่อวิเคราะห์ Log

10 ข้อควรปฏิบัติเพื่อความปลอดภัยขององค์กร และเป็นไปตามที่กฎหมายกำหนด

- (M) ปรับแต่งระบบต่างๆเพื่อให้ส่ง Log มายัง Log Server ที่ส่วนกลางได้
- (M) พัฒนานโยบายด้านความปลอดภัยระบบสารสนเทศ(Information Security Policy) และจัดทำ Acceptable Use Policy (AUP) ให้พนักงานทุกคนเซ็นต์รับทราบ
- (M) จัดฝึกอบรมหลักสูตรความรู้ด้านปลอดภัยเบื้องต้น “Security Awareness Training” ให้กับพนักงานทุกระดับ
- (M) จัดเตรียมข้อมูลให้ผู้บริหารระดับสูงได้รับทราบในเรื่องของข้อกฎหมายที่ผู้บริหารควรทราบ
- (A) ประเมินความเสี่ยงระบบสารสนเทศด้วยการทำ Gap Analysis , Vulnerability Assessment Penetration Testing

ปัญหาในภาพรวมของการปฏิบัติตาม พรบ.ฯ และประกาศกระทรวงฯ และแนวทางแก้ปัญหาที่ถูกต้อง

(1) ปัญหาคอขวด (Bottleneck)

- ปัญหาคอขวด (Bottleneck) ที่อาจเกิดขึ้นได้ในทุกองค์กร หากออกแบบระบบไม่ดี โดยไม่มีการเผื่อขนาดของอุปกรณ์ (Sizing) ก็อาจก่อให้เกิดปัญหาเวลาที่มีผู้ใช้งานระบบเครือข่ายเป็นจำนวนมาก
- ควรมีการกำหนดค่า EPS หรือ Event Per Second ให้กับอุปกรณ์เวลาจัดซื้อจัดจ้างให้รองรับ Log จากเครื่องแม่ข่าย และอุปกรณ์เครือข่ายทั้งหลายได้อย่างไม่มีปัญหา

(2) ปัญหาผู้ใช้งานระบบไม่ยอมรับ

- ปัญหาผู้ใช้งานระบบไม่ยอมรับ เป็นปัญหาเกี่ยวกับ “คน” ไม่ใช่ “เทคโนโลยี”
  - เนื่องจากในปัจจุบันผู้ใช้งานเครือข่ายและระบบอินเตอร์เน็ตมี “ความเคยชิน” กับการใช้งานอินเตอร์เน็ตที่สะดวกสบาย
  - ภายหลังจากการติดตั้งระบบ Authentication เวลาที่ทุกคนต้องการใช้งานอินเตอร์เน็ตก็ต้องป้อน Username และ Password ในทุกครั้งไป ทำให้ผู้ใช้งานอาจเกิดความไม่สะดวก และไม่เข้าใจถึงเหตุผลที่ต้องทำเช่นนี้
- องค์กรควรมีการจัดทำ “Security Awareness Program” ภายในให้กับผู้ใช้งานเครือข่ายและระบบอินเตอร์เน็ต
  - เพื่อช่วยให้ผู้ใช้งานฯ มีความเข้าใจมากขึ้น อีกทั้งยังพร้อมที่จะปฏิบัติตามนโยบายด้านความปลอดภัยขององค์กรด้วยเต็มใจ ไม่ใช่โดยการบังคับ

(3) ปัญหาผู้ใช้งานระบบไม่ยอมรับ

- ปัญหาเรื่องไม่มีงบประมาณ หรืองบประมาณไม่เพียงพอ ก็เป็นอีกปัญหาหนึ่งที่ต้องรีบแก้ไข
  - โดยเฉพาะหน่วยงานราชการที่ต้องวางแผนในการใช้งบประมาณล่วงหน้าเป็นปี
- เส้นตายของการติดตั้งระบบ Centralized Log ตามกฎหมาย คือ วันที่ 18 สิงหาคม พ.ศ. 2551
- องค์กรไม่ควรเพิกเฉยในขณะที่ยังพอมีเวลาในการดำเนินการของบประมาณที่จะจัดซื้อจัดจ้างให้เรียบร้อยเสียก่อนจะถึงกำหนดเวลาดังกล่าว
- ต้องเร่งสร้างความรู้ความเข้าใจให้กับผู้บริหารระดับสูง และผู้ใช้งานคอมพิวเตอร์ทั่วไป

(4) ปัญหาเรื่องผู้บริหารระดับสูงไม่ใส่ใจเรื่องกฎหมายมากเพียงพอ

- ปัญหาเรื่องผู้บริหารระดับสูงไม่ใส่ใจเรื่องกฎหมายมากเพียงพอ นับว่าเป็นปัญหาใหญ่ที่ต้องรีบแก้ไขอย่างรีบด่วน
  - ผู้บริหารระดับสูงไม่ได้รับทราบข้อมูลเรื่องกฎหมายอย่างเพียงพอ
  - ผู้บริหารไม่ใช่คนไอที ไม่ทราบว่าตน และองค์กรต้องปฏิบัติอย่างไร
  - ความปลอดภัยข้อมูลคอมพิวเตอร์มักจะเป็น “Second Priority” เสมอ
- ควรมีการให้ข้อมูลกับผู้บริหารระดับสูง
  - การจัดทำ“Security Awareness Training” ให้กับผู้บริหารระดับสูงซึ่งควรใช้เวลาประมาณ 1-3 ชั่วโมง เพื่อสร้างความเข้าใจในเรื่องกฎหมาย พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์
- ผู้บริหารจะต้องเป็นผู้รับผิดชอบในข้อกฎหมายซึ่งอาจจะมาถึงตัวเมื่อใดก็ได้หลังจากการเกิดอาชญากรรมทางคอมพิวเตอร์

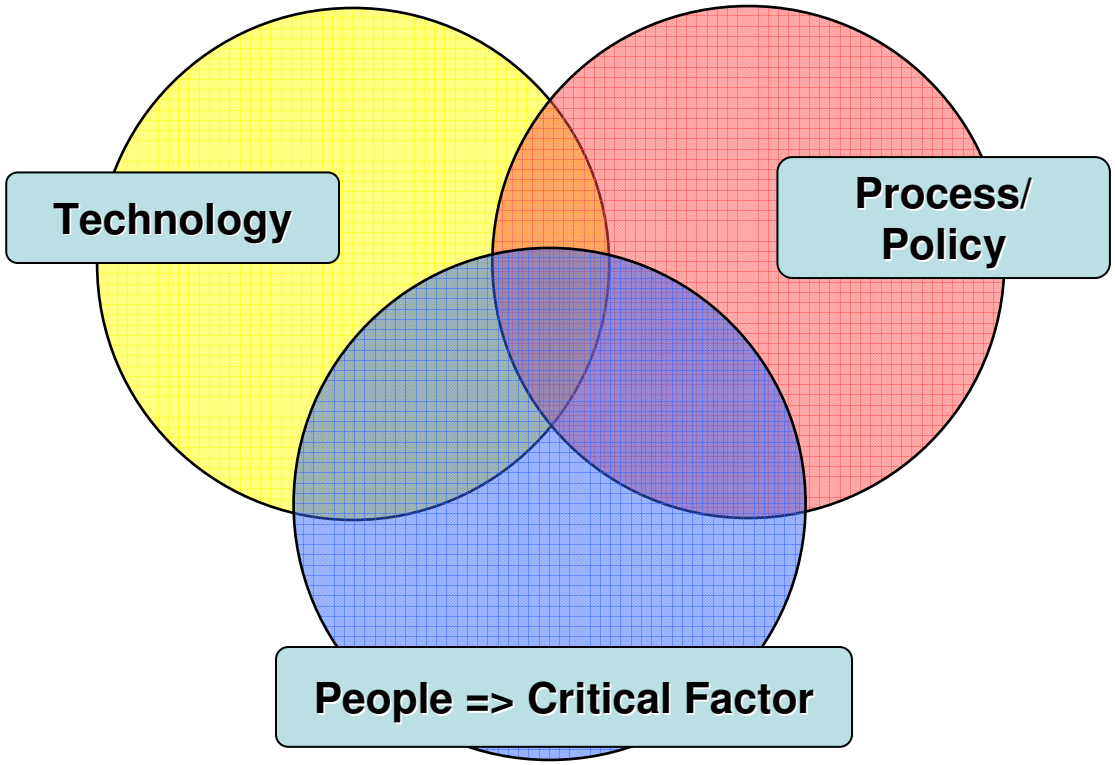
(5) ปัญหาเรื่องการขาดบุคลกรที่มีความเชี่ยวชาญในเรื่องการจัดเก็บ และการวิเคราะห์ Log

- ปัญหาเรื่องการขาดบุคลากรที่มีความเชี่ยวชาญในเรื่องการจัดเก็บ และการวิเคราะห์ Log ปัญหานี้เป็นปัญหาปกติที่สามารถแก้ได้โดยง่าย
  - องค์กรสามารถ Outsource ให้ผู้เชี่ยวชาญจากภายนอกมาช่วยได้
  - ผู้ให้บริการประเภท MSSP หรือ “Managed Security Services Provider” มีบุคลากรผู้เชี่ยวชาญด้านความปลอดภัยข้อมูลสารสนเทศ และมีนักวิเคราะห์ด้านความปลอดภัยฯ หรือ “Security Analyst” เพื่อให้บริการด้านการวิเคราะห์ข้อมูลจาก Log Server อยู่แล้ว
- ดังนั้น องค์กรจึงไม่มีความจำเป็นต้องลงทุนเพิ่มเรื่องบุคลากร ตลอดจนไม่ต้องทำในสิ่งที่องค์กรไม่มีความถนัดและความเชี่ยวชาญ รวมทั้งสามารถประหยัดงบประมาณโดยรวมให้กับองค์กรอีกด้วย

สรุป

- การปฏิบัติตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์นั้นถือเป็นหน้าที่ที่ทุกองค์กรต้องปฏิบัติเพื่อแสดงความรับผิดชอบต่อสังคมโดยรวม
- การเก็บ Log หรือ Traffic Data อย่างน้อย 90 วัน ที่มีกำหนดขีดเส้นตายสำหรับทุกองค์กรในประเทศไทย ในวันที่ 23 สิงหาคม พ.ศ. 2551 จึงมีความสำคัญอย่างยิ่งกับสภาวะการพัฒนาสังคมด้านสารสนเทศในประเทศไทยไปอีกขั้นหนึ่ง

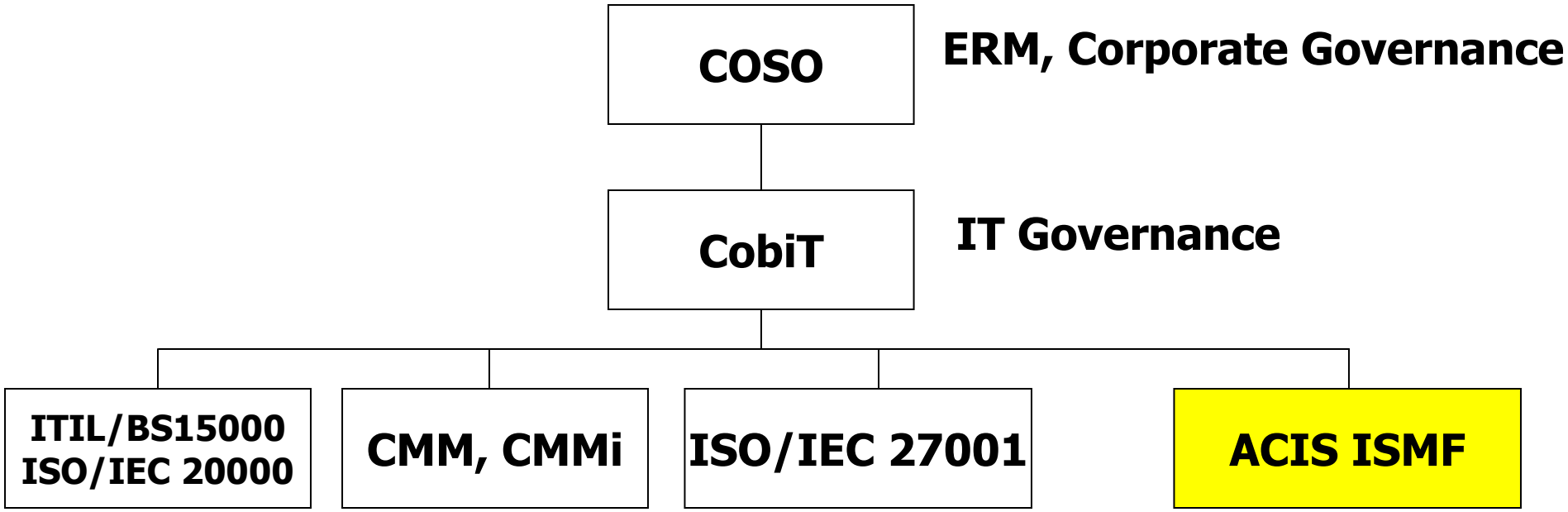
PPT concept
People, Process/Policy and Technology



Year 2008 : “IT Regulatory Compliance Year”

- **Corporate Governance => IT Governance**
  - CobiT 4.1 (Control Objectives for Information and related Technology) from ISACA and ITGI
  - BS7799 part1 => ISO/IEC 17799:2005 Second Edition (June 05 released)
  - BS7799 part 2 => ISO/IEC 27001:2005 (October 05 released)
  - ITIL (IT Infrastructure Library) => BS15000 => ISO/IEC 20000
  - ACIS ISMF (Information Security Management Framework) version I and II

COSO, CobiT, ITIL, CMM, ISO/IEC27001 => ACIS ISMF

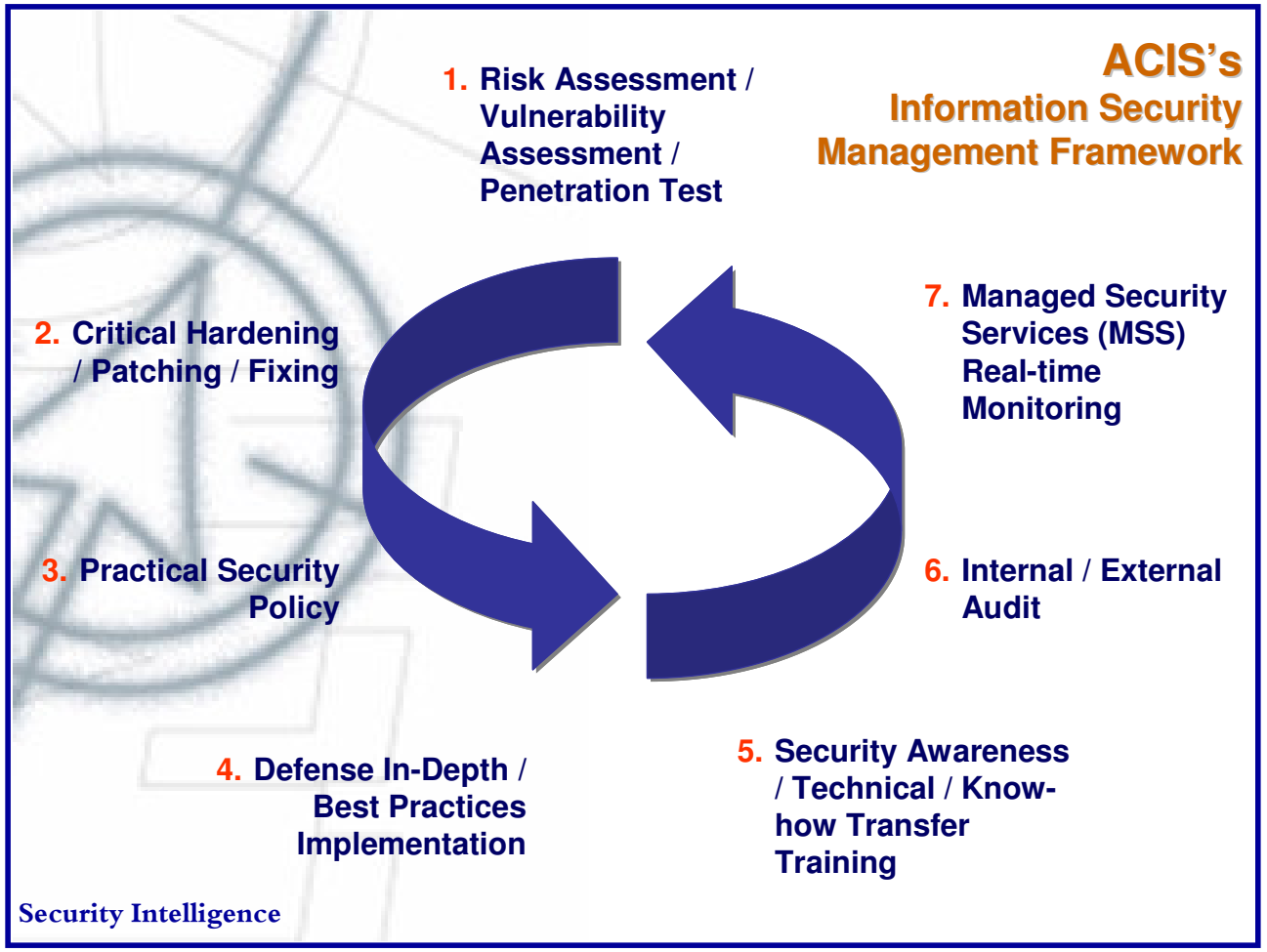


Process Perspective

- Customized Information Security Management framework based on existing industry best practices : ISO/IEC27001, COSO, CobiT, ITIL, CMM, NIST, etc..

- ACIS ISMF version 1 : 2004
- ACIS ISMF version 2 : 2006

ACIS Information Security Management Framework (ISMF version 1) – 7 Steps



Final Recommendation from ACIS

Seven Things to do NOW !

1. IT Risk Assessment : Gap Analysis, Vulnerability Assessment and Penetration Testing
2. Implement Anti-Malware/Anti-SPAM Solution at Gateway
3. Implement Vulnerability Management/Patch Management
4. Harden your networks, systems and applications
5. Develop and Enforce Information Security Policy in your organization
6. Rise up Users and Executives Information Security Awareness Training by iSAT program (harden your people !)
7. Implement Centralized Log Management and Real-time Security Monitoring Solution from MSSP (Regulatory Compliance)

Security isn’t just an IT issue.
It’s everyone’s business.

For more information about Information Security Articles and Solution, please visit

ACIS Professional Center Web : http://www.acisonline.net ,
or FM 100.5 MHz. 21:00-22:00 (1st Saturday Night)

Tel. +662-650-5571, contact K. Siriwan

email : prinya@acisonline.net