คู่มือวิธีปฏิบัติสำหรับองค์กรตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

โดย ปริญญา หอมเอนก, CISSP, SSCP, CISA, CISM, SANS GIAC GCFW, Security+, ITIL และทีมงาน ACIS Professional Center & ACIS i-Secure

ACIS Professional Center
http://www.acisonline.net

1. ที่มาของ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
2. พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
3. ประกาศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
4. บทวิเคราะห์ พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
5. บทวิเคราะห์ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
6. ระบบโครงสร้างพื้นฐานที่องค์กรควรจัดทำเพื่อรองรับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
7. รายละเอียดการจัดเก็บ Log ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ตามประกาศข้อ ๕ (๑) ข. ถึง ค.
8. ความเข้าใจผิดเกี่ยวกับ พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ และประกาศกระทรวงเทคโนโลยีสารสนเทศ และการสื่อสาร
9. 10 ข้อควรปฏิบัติเพื่อความปลอดภัยขององค์กรและเป็นไปตามที่กฎหมายกำหนด (10 Checklist)
10. ปัญหาในภาพรวมของการปฏิบัติตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ประกาศกระทรวงฯ และแนวทางแก้ปัญหาที่ถูกต้อง

1. ที่มาของ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

ในปัจจุบันการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือ ระบบอิเล็กทรอนิกส์ได้เข้ามามีบทบาท และ ทวีความสำคัญเพิ่มขึ้นตามลำดับต่อระบบเศรษฐกิจและคุณภาพชีวิตของประชาชนในประเทศไทย แต่ในขณะเดียวกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็มีแนวโน้มขยายวงกว้างและทวีความรุนแรงเพิ่มมากขึ้นด้วย ดังนั้น ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดี อันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ ใน พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว

จากการประกาศใช้ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีผลบังคับใช้แล้ว ตั้งแต่ วันพุธที่ 18 กรกฎาคม 2550 ทำให้หลายองค์กรทั้งภาครัฐและภาคเอกชนต้องมีการปรับตัวครั้งใหญ่ เนื่องจากมาตรา 26 ใน พรบ. ได้กล่าวไว้ว่า “ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท” ทำให้หลายคนเกิดความสงสัยว่าองค์กรของตนถือเป็น “ผู้ให้บริการ” หรือไม่และการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ดังกล่าวนั้นหมายถึงข้อมูลอะไรบ้าง ควรมีการจัดเก็บแบบใดถึงจะถูกต้องตามวัตถุประสงค์ของ พรบ. โดยที่องค์กรแต่ละองค์กรมีลักษณะการใช้ระบบสารสนเทศที่แตกต่างกัน ดังนั้นจึงควรมีการแนวทาง หรือ ”Guideline” ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ให้ถูกต้องและเหมาะสมกับลักษณะการใช้ระบบสารสนเทศหรือระบบอินเทอร์เน็ตของแต่ละองค์กรที่มีความแตกต่างกันค่อนข้างมาก รวมทั้งร้านอินเทอร์เน็ตคาเฟ่ที่มีอยู่มากมายในประเทศไทย ควรจัดเก็บข้อมูลอย่างไรเป็นต้น ตลอดจน หลายองค์กรยังไม่มีความพร้อมในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ทำให้ผู้บริหารระบบสารสนเทศขององค์กรต้องการทราบระยะเวลาในการผ่อนผันว่าทางการจะผ่อนผันได้นานกี่วันนับจากวันที่กฎหมายประกาศใช้ ก่อนที่จะมีการตรวจสอบหรือการขอข้อมูลโดยพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งโดยรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ดังนั้นทางกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้ออกประกาศกระทรวงฯ สำหรับหลักเกณฑ์ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ดังกล่าว เพื่อให้เกิดความเหมาะสมในทาง

ปฏิบัติและเพื่อให้หลายองค์กรได้มีแนวทางที่ชัดเจนในการปฏิบัติ ว่าข้อมูลจราจรอะไรบ้างที่ควรจัดเก็บ ข้อมูลอะไรที่ไม่ต้องจัดเก็บ ตลอดจนวิธีการจัดเก็บอย่างถูกต้อง ตรงตามลักษณะการใช้ระบบสารสนเทศหรือระบบอินเทอร์เน็ตของแต่ละองค์กร เช่น การจัดเก็บในลักษณะ “Centralized Log” เป็นต้น

2. **พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (ดู พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ที่อยู่ในรูปไฟล์** PDF)
3. **ประกาศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ (ดู ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่อยู่ในรูปไฟล์** PDF)

4. **บทวิเคราะห์ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐**

บทวิเคราห์มาตรา 5 ถึง มาตรา 17

มาตรา 5 ถึง มาตรา 10 เป็นการนำหลักการ CIA (Confidentially, Integrity และ Availability) มาประยุกต์ใช้กับการโจมตีของผู้ไม่หวังดีในแบบต่างๆ เช่น การเจาะระบบเข้าไปแอบขโมยสำเนาข้อมูล, การแอบดูชื่อและรหัสผ่านโดยใช้โปรแกรมประเภท Sniffer หรือการโจมตีเปลี่ยนหน้าเว็บไซต์ (Web Defacement, see www.zone-h.org) ตลอดจนการโจมตีให้เว็บไซต์ล่ม (Denial of Services) ล้วนแต่เข้าข้อกฎหมายในมาตรา 5 ถึง มาตรา 10 ทั้งสิ้น ซึ่งมีโทษทั้งจำทั้งปรับ

มาตรา 11 นั้น เกี่ยวข้องโดยตรงกับผู้ที่ชอบส่ง “SPAM Mail” **โดยไม่ระบุชื่อผู้ส่ง** ซึ่งมีโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา 12 เป็นการกระทำผิดที่มีโทษในกรณีที่มีผลกระทบต่อความมั่นคงทางเศรฐกิจของประเทศหรือบริการสาธารณะ โทษสูงสุดถึงจำคุก 15 ปี และปรับถึง 3 แสนบาท แต่ถ้าหากทำให้ผู้อื่นถึงแก่ความตาย โทษจะสูงสุดถึงจำคุก 20 ปีเลยทีเดียว

มาตรา 14 ถึง 16 นั้น ผู้ใช้คอมพิวเตอร์ ตลอดจนผู้ให้บริการตามข้อกำหนดของกฎหมาย ต้องระมัดระวังไม่ให้ข้อมูลอัน “ไม่เหมาะสม” ปรากฏอยู่บนอินเทอร์เน็ตในลักษณะการปรากฏของตัวข้อมูลเอง เช่น รูปภาพ หรือ ข้อความ ที่ถูก Upload ขึ้นไป รวมถึง Link ที่พาไปยังข้อมูลดังกล่าวด้วย เพราะฉะนั้นท่านที่ชอบ Forward Mail โดยไม่ระวัง อาจเข้าข้อกฎหมายในมาตราที่ 14 ข้อ 5 ซึ่งมีโทษจำคุกไม่เกิน 5 ปี หรือ ปรับไม่เกิน 1 แสนบาท หรือ ทั้งจำทั้งปรับ

เราได้วิเคราะห์ถึงหมวด 1 “ความผิดเกี่ยวกับคอมพิวเตอร์” ตั้งแต่มาตรา 5 ถึง มาตรา 17 โดยที่มาตรา 5, 6, 7, 8, 9, 10 และ มาตรา 12 กล่าวถึง ความผิดที่กระทำต่อคอมพิวเตอร์ และ มาตรา 11 และ มาตรา 13 ถึง

มาตรา 16 กล่าวถึงการใช้คอมพิวเตอร์ในการกระทำความผิด ตลอดจนมาตรา 17 กล่าวถึงการกระทำความผิดนอกราชอาณาจักรต้องรับโทษในราชอาณาจักร สรุปสาระสำคัญของมาตรา 5 ถึงมาตรา 17 ได้ดังนี้

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

ฐานความผิดและบทลงโทษสำหรับการกระทำโดยมิชอบ	
มาตรา ๕	การเข้าถึงระบบคอมพิวเตอร์
มาตรา ๖	การล่วงรู้มาตรการป้องกันการเข้าถึง
มาตรา ๗	การเข้าถึงข้อมูลคอมพิวเตอร์
มาตรา ๘	การดักข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา ๙	การรบกวนข้อมูลคอมพิวเตอร์
มาตรา ๑๐	การรบกวนระบบคอมพิวเตอร์
มาตรา ๑๑	สแปมเมล์ (Spam Mail)
มาตรา ๑๒	การกระทำความผิดต่อความมั่นคง
มาตรา ๑๓	การจำหน่าย/เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด
มาตรา ๑๔	การปลอมแปลงข้อมูลคอมพิวเตอร์/เผยแพร่เนื้อหาอันไม่เหมาะสม
มาตรา ๑๕	ความรับผิดของผู้ให้บริการ
มาตรา ๑๖	การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง
มาตรา ๑๗	การกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักร
รวม ๑๓ มาตรา	

บทกำหนดโทษ

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา ๕ เข้าถึงคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๖ เดือน	ไม่เกิน ๑๐,๐๐๐ บาท
มาตรา ๖ ล่วงรู้มาตรการป้องกัน	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๗ เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๒ ปี	ไม่เกิน ๔๐,๐๐๐ บาท
มาตรา ๘ การดักข้อมูลคอมพิวเตอร์	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท
มาตรา ๙ การรบกวนข้อมูลคอมพิวเตอร์	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๐ การรบกวนระบบคอมพิวเตอร์ มาตรา ๑๑ สแปมเมล์	ไม่เกิน ๕ ปี ไม่มี	ไม่เกิน ๑๐๐,๐๐๐ บาท ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๒ การกระทำต่อความมั่นคง (๑) ก่อความเสียหายแก่ข้อมูลคอมพิวเตอร์ (๒) กระทบต่อความมั่นคงปลอดภัยของประเทศ/เศรษฐกิจ วรรคท้าย เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	ไม่เกิน ๑๐ ปี ๓ ปี ถึง ๑๕ ปี ๑๐ ปี ถึง ๒๐ ปี	+ ไม่เกิน ๒๐๐,๐๐๐ บาท ๖๐,๐๐๐-๓๐๐,๐๐๐ บาท ไม่มี
มาตรา ๑๓ การจำหน่าย/เผยแพร่ชุดคำสั่ง	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๑๔ การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๕ ความรับผิดของ ISP	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๖ การตัดต่อภาพผู้อื่น ถ้าสุจริต ไม่มีความผิด	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท

สำหรับมาตรา 18 ถึง มาตรา 30 อยู่ใน *หมวด 2 "พนักงานเจ้าหน้าที่"* ซึ่งรวมถึง ข้อปฏิบัติของผู้ให้บริการที่ต้องให้ความร่วมมือกับพนักงานเจ้าหน้าที่ด้วย

บทวิเคราห์มาตรา 18 ถึง มาตรา 30

มาตรา 18 ให้อำนาจพนักงานเจ้าหน้าที่ซึ่งผ่านหลักสูตรการฝึกอบรมเรื่อง Computer and Network Forensic และมีคุณสมบัติตามที่กฎกระทรวงกำหนด เช่น ผ่านการสอบ Local Security Certification ที่ทางกระทรวงได้กำหนดขึ้น หรือ ผ่านการสอบ International Security Certification สากลเช่น CompTIA Security+, SSCP หรือ CISSP มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้เพื่อมาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้และสั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่ เพื่อใช้ข้อมูลดังกล่าวเป็นหลักฐานในการสืบสวนสอบสวนและประกอบการพิจารณาคดี โดยมาตราที่ 18 วรรค 4 ถึง 8 นั้น พนักงานเจ้าหน้าที่ ต้องยื่นคำร้องต่อศาลและขอหมายศาลก่อนถึงจะมีอำนาจสำเนาข้อมูล ส่งให้ส่งมอบ, ตรวจสอบเข้าถึง, ถอดรหัส สลักข้อมูล รวมทั้งการยึดและอายัดระบบ ทั้งนี้ในมาตรา 19 บัญญัติไว้ว่าพนักงานเจ้าหน้าที่ต้องส่งสำเนาบันทึกรายละเอียดให้แก่ศาลภายใน 48 ชม. และจะยึด/อายัดห้ามเกิน 30 วันขยายได้เต็มที่อีกไม่เกิน 60 วัน สำหรับมาตรา 20 ได้บัญญัติถึงเรื่องการระงับการทำให้แพร่หล่ายของข้อมูลที่อาจกระทบกระเทือนต่อความมั่นคงแห่ง

ราชอาณาจักรหรือข้อมูลที่มีลักษณะต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ยกตัวอย่าง เช่น พนักงานเจ้าหน้าที่มีอำนาจในการ Block เว็บไซด์ที่ไม่เหมาะสม เป็นต้น และในมาตรา 21 พนักงานเจ้าหน้าที่สามารถร้องขอให้ศาลมีคำสั่งห้ามจำหน่ายหรือเผยแพร่หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้งานและทำลายข้อมูลนั้นได้ โดยที่ชุดคำสั่งไม่พึงประสงค์ หมายถึง มัลแวร์ (MalWare) ต่างๆ เช่น ไวรัส, หนอนคอมพิวเตอร์ (worm), ม้าโทรจัน, สปายแวร์ ตลอดจน โปรแกรม Hacking Tool ต่าง ๆ

พนักงานเจ้าหน้าที่ก็มีความรับผิดชอบในการเก็บรักษาข้อมูลที่ได้มาเช่นกัน ดังที่บัญญัติไว้ในมาตราที่ 22 ถึงมาตรา 24 ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลที่ได้มาตามมาตรา 18 แก่บุคคลใด หากฝ่าฝืน พนักงานเจ้าหน้าที่ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือ ปรับไม่เกิน 6 หมื่นบาท หรือ ทั้งจำทั้งปรับ โดยในมาตรา 23 หากพนักงานเจ้าหน้าที่ประมาทเลินเล่อ ทำให้ผู้ล่วงรู้ข้อมูลดังกล่าวต้องระวางโทษทั้งจำคุกและปรับ และ มาตรา 24 ได้บัญญัติผู้อื่นที่ล่วงรู้ข้อมูลที่ได้ว่าจากพนักงานเจ้าหน้าที่ก็มีโทษจำคุกและปรับ เช่นเดียวกันกับพนักงานเจ้าหน้าที่ ที่ปฏิบัติตนไม่ชอบ

มาตราสำคัญที่เป็น ประเด็นร้อนวันนี้คือ มาตรา 26 และมาตรา 27 ซึ่ง มาตรา 26 บัญญัติให้ผู้ให้บริการต้องเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ไม่ต่ำกว่า 90 วัน แต่ไม่เกิน 1 ปี ซึ่งรายละเอียดข้อมูลจราจรคอมพิวเตอร์ที่ต้องจัดเก็บจะอยู่ในประกาศรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารที่กำลังทยอยออกตามหลังการประกาศใช้งานกฎหมายฉบับนี้ โดยผู้ให้บริการจะมีภาระหน้าที่เก็บข้อมูลจราจรเท่าที่จำเป็น เพื่อให้สามารถรบุตัวผู้ใช้บริการได้ หากผู้ให้บริการผู้ใดไม่ปฏิบัติ ต้องระวางโทษปรับไม่เกิน 5 แสนบาท และในมาตรา 27 บัญญัติไว้ชัดเจนว่าหากผู้ใดไม่ให้ความร่วมมือในการปฏิบัติตาม มาตรา 18 หรือ มาตรา 20 หรือไม่ปฏิบัติตามมาตรา 21 ต้องระวางโทษปรับไม่เกิน 2 แสนบาท และที่สำคัญต้องโทษปรับ รายวันอีก ไม่เกินวันละ 5 พันบาท "จนกว่าจะปฏิบัติให้ถูกต้อง"

จะเห็นได้ว่าผู้ใช้บริการคงจะอยู่เฉยไม่ได้แล้ว ควรจะจัดหาอุปกรณ์ฮาร์ดแวร์และซอฟท์แวร์มาใช้ในการเก็บ Log ตามข้อกฎหมาย โดยอุปกรณ์ที่ใช้ควรมีการจัดเก็บ Log ในลักษณะ "Centralized Log Server" ที่สามารถป้องกันการแก้ไขจากแฮกเกอร์หรือการแก้ไขจากผู้ดูแลระบบเอง ข้อมูลจราจร หรือ Log ที่เกิดขึ้นจากอุปกรณ์ต่างๆ ในระบบควรอยู่ในรูปแบบข้อมูลดิบ (Raw Data) ที่ถูกป้องกันจากการแก้ไขเพราะข้อมูลจราจรดังกล่าวจะถูกนำไปใช้ในการพิจารณาคดีในขั้นศาล ดังนั้น ข้อมูลจราจร (Log) ควรที่จะมีความถูกต้องแน่นอนตามจริงและสามารถระบุตัวตน (Accountability) ของผู้กระทำความผิดได้โดยไม่มีข้อโต้แย้งในชั้นศาล

สำหรับมาตรา 28 ได้บัญญัติถึงการแต่งตั้งพนักงานเจ้าหน้าที่ซึ่งมีความรู้และความสามารถเฉพาะทางในด้าน "Computer Forensic" และมีคุณสมบัติตามที่รัฐมนตรีกำหนด เพื่อให้สามารถแน่ใจได้ว่าพนักงานเจ้าหน้าที่นั้นมีความรู้ความเข้าใจขั้นตอนในการเก็บข้อมูลหลักฐานและการวิเคราะห์สืบสวนหาหลักฐานนี้อยู่ในรูปดิจิทัล (Digital Format) ตลอดจนสามารถปฏิบัติตามวิธีการที่ถูกต้องในการเก็บจัดการข้อมูลจนถึงการพิจารณาคดีในขั้นศาล (Chain of Custody) โดยในมาตรา 29 บัญญัติให้พนักงานเจ้าหน้าที่ต้องเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ซึ่งมีอำนาจรับคำร้องทุกข์หรือคำกล่าวโทษได้ และมีอำนาจในการสืบสวน

สอบสวน แต่อำนาจในการจับกุมให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสวบสวนผู้รับผิดชอบเพื่อดำเนินงานตามหน้าที่

มาตราสุดท้าย (มาตรา 30) บัญญัติว่า พนักงานเจ้าหน้าที่ต้องมี “บัตรประจำตัว” เพื่อแสดงตนโดยรายละเอียดรูปแบบบัตรฯ ให้เป็นไปตามที่รัฐมนตรีประกาศต่อไป

กล่าวโดยสรุป จะเห็นได้ว่ากฎหมายฉบับนี้มีผลกระทบต่อสังคมสารสนเทศของประเทศไทยในระดับหนึ่ง ซึ่งถือเป็นการเปลี่ยนแปลงครั้งสำคัญในแวดวงไอทีที่ผู้ใช้คอมพิวเตอร์ทุกคนควรให้ความสนใจศึกษารายละเอียดของกฎหมายฉบับนี้ ตลอดจนมีการเตรียมตัวและปรับตัวให้องค์กรปฏิบัติตามกฎหมาย เช่น ไม่ส่งต่อจดหมายอิเล็กทรอนิสก์ (Forward Email) ที่มีเนื้อหาใจความที่ไม่เหมาะสม หรือการจัดเก็บ Log ไว้ไม่ต่ำกว่า 90 วัน เป็นต้น การเติบโตของสังคมแหล่งภูมิปัญญาและการเรียนรู้ มีความจำเป็นต้องมีกฎหมายเฉพาะทางดังเช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ใช้เวลาในการพัฒนาร่างกฎหมายถึง 9 ปี เต็ม เพื่อที่จะทำให้การใช้งานระบบสารสนเทศ รวมถึงระบบอินเทอร์เน็ต มีน่าเชื่อถือและความปลอดภัยมากขึ้นอันจะส่งผลถึงการพัฒนาเศษฐกิจและสังคมของประเทศไทยในอนาคต ดังนั้น เราจึงควรร่วมกันปฏิบัติตามข้อกฎหมายอย่างเคร่งครัดด้วยความเข้าใจที่ถูกต้องตามวัตถุประสงค์ของกฎหมายดังที่กล่าวมาแล้วในตอนต้น

อาชญากรรมคอมพิวเตอร์ในปัจจุบันและอนาคตทวีความซับซ้อนและเพิ่มความรุนแรงของผลกระทบมากขึ้น เนื่องจากอาชญากรรมคอมพิวเตอร์ในปัจจุบันมีการทำงานในลักษณะ “Organized Crime” **คือ ทำเป็นกลุ่มเป็นองค์กรและมีการโจมตีเพื่อหวังผลและมีจุดประสงค์ชัดเจน เรียกว่า** “Targeted Attack” **ซึ่งส่วนใหญ่จะมุ่งประโยชน์ทางด้านการเงิน เช่น การโจมตีระบบอินเทอร์เน็ตแบงก์กิ้ง หรือ การโจมตีระบบบัตรเครดิต รวมถึง การเข้า** “Hack” **ระบบเครือข่ายของบริษัทสื่อสารใหญ่ ๆ เพื่อแอบขโมยโทรศัพท์ฟรีโดยการเปลี่ยนแปลงข้อมูลในระบบ** PRE-PAID **ดังที่เป็นข่าวหน้าหนึ่งของหนังสือพิมพ์หลายฉบับมาแล้ว**

ดังนั้น จึงมีความจำเป็นอย่างยิ่งในระดับชาติที่กฎหมายการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ควรถูกบัญญัติ และมีผลบังคับใช้ให้เร็วที่สุดเท่าที่จะทำได้ **เพราะ อาชญากรรมคอมพิวเตอร์นั้นเกิดขึ้นอย่างรวดเร็วและมีการเปลี่ยนแปลงอยู่ตลอดเวลา อีกทั้งยังมีคดีความเก่า ๆ ที่คั่งค้างไม่สามารถเอาผิดกับผู้กระทำผิดได้อย่างชัดเจนอีกหลายคดี จึงสรุปได้ว่า ปี พ.ศ. 2550 นี้เป็นนิมิตรหมายที่ดีสำหรับ ประเทศไทย ที่เราจะได้มีกฎหมายเกี่ยวกับ** “Computer Crime” **เหมือนกับหลาย ๆ ประเทศในแถบเอเชียที่มีกฎหมายในลักษณะนี้มาเป็นระยะเวลานานแล้วและจากนี้ไปหากใครคิดจะเป็นแฮกเกอร์หรือคิดกระทำความผิดก็คงต้องคิดใหม่และตระหนักถึงบทลงโทษในกฎหมายที่มีโทษจำคุกสูงสุดถึง 20 ปี ในภาพรวมจึงถือว่ากฎหมายฉบับนี้สอบผ่านและช่วยทำให้สังคมมีความสงบสุขมากขึ้นได้ในที่สุด**

5. บทวิเคราะห์ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

สำหรับรายละเอียดของประกาศกระทรวงฯ ณ วันที่ ๒๓ สิงหาคม พ.ศ. ๒๕๕๐ โดยรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และ บทวิเคราะห์ มีดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า "หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐"

บทวิเคราะห์ ; วัตถุประสงค์ที่แท้จริงของ พรบ. ก็คือเมื่อเกิดอาชญากรรมทางคอมพิวเตอร์ หลักฐานต่างๆ ทางคอมพิวเตอร์นั้นมีความน่าเชื่อถือค่อนข้างน้อยอยู่แล้วและมีโอกาสที่จะไม่พบร่องรอยของการก่ออาชญากรรม หลายครั้งเมื่อตำรวจหรือพนักงานเจ้าหน้าที่ได้เข้าไปขอข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการยกตัวอย่าง เช่น ISP ก็มักพบว่า ISP ไม่ได้เก็บข้อมูลจราจรดังกล่าวหรือเก็บไว้ไม่นานเพียงพอเนื่องจากมีพื้นที่จัดเก็บค่อนข้างจำกัดทำให้การพิสูจน์หลักฐานทางคอมพิวเตอร์ทำได้ยากลำบาก หรือ ไม่สามารถทำได้เนื่องจากข้อมูลไม่เพียงพอ ดังนั้นใน พรบ. จึงจำเป็นที่จะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้อย่างชัดเจนโดยให้ถือว่าเป็นความรับผิดชอบต่อสังคมที่องค์กรทุกองค์กรต้องปฏิบัติและให้ความร่วมมือเมื่อมีการขอเรียกดูข้อมูลดังกล่าวโดยพนักงานเจ้าหน้าที่หลังจากมีอาชญากรรมเกิดขึ้น

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป
ข้อ ๓ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามประกาศนี้

บทวิเคราห์: หมายถึง รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญในการประกาศใช้กฎกระทรวงที่อาจออกตามมาหลังจากการประกาศใช้ พรบ. เป็นระยๆ เพราะฉะนั้นเราจึงควรติดตามข้อมูลข่าวสารจากกระทรวงอย่างต่อเนื่อง

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

บทวิเคราะห์ ; ข้อมูลจราจร หรือTraffic data ไม่ได้หมายถึงข้อมูลที่ไหลผ่านระบบเครือข่ายหากแต่หมายถึงข้อมูลที่เกิดขึ้นในระบบคอมพิวเตอร์ เช่น ข้อมูลในเครื่อง web server ที่เกิดจากการเข้าถึงข้อมูลโดยผู้เข้าเยี่ยมชมเว็บไซต์ (web site) เป็นต้น โดยปกติแล้วข้อมูลดังกล่าวนิยมเรียกกันโดยทั่วไปว่า log file ซึ่งระบบคอมพิวเตอร์มักจะเก็บ log file ไว้ในเครื่องซึ่ง log file ดังกล่าวอาจถูกเขียนข้อมูลทับในระยะเวลาไม่ถึง 90 วันตามที่กฎหมายกำหนดและ log file อาจถูกแก้ไขโดยผู้ดูแลระบบ (system administrator) หรือถูกลบโดยแฮกเกอร์ก็มีความเป็นไปได้สูง ดังนั้นประกาศกระทรวงฉบับนี้จึงมีข้อกำหนดวิธีการเก็บวิธีการเก็บ log file อย่างถูกต้องซึ่งกำหนดไว้ในข้อ ๘

"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

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

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

บทวิเคราะห์ ; ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ นอกจากจะหมายถึง ISP แล้วยังหมายถึงบริษัท โรงเรียน มหาวิทยาลัย และองค์กรทั้งภาครัฐและเอกชนส่วนใหญ่โดยทั่วไป

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

บทวิเคราะห์: ผู้ให้บริการเช่าระบบคอมพิวเตอร์ ยกตัวอย่าง เช่น ผู้ให้บริการเช่า Web Site หรือ Web Hosting

ง. ผู้ให้บริการร้านอินเทอร์เน็ต ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

บทวิเคราะห์: ผู้ให้บริการร้านอินเทอร์เน็ต ยกตัวอย่าง เช่น Internet Cafe ทั่วไป

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

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

บทวิเคราะห์ในภาพรวม : จะเห็นได้ว่าทุกองค์กรที่มีการใช้งานระบบสารสนเทศต่อเชื่อมกับระบบอินเทอร์เน็ตถือเป็นผู้ให้บริการทั้งหมด

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

บทวิเคราะห์ : จะเห็นได้ว่าผู้ให้บริการตามข้อ ๕(๑) ก มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์แตกต่างจากผู้ให้บริการตามข้อ ๕(๑) ข. และ ค. ซึ่งมีการจัดเก็บข้อมูลเหมือนกัน สำหรับผู้ให้บริการตามข้อ ๕(๑)ง. หรือ Internet cafe และ ผู้ให้บริการตามข้อ ๕ (๒) หรือ Content Provider มีการจัดเก็บข้อมูลเฉพาะในแบบของตนเอง

ทั้งนี้ ในการเก็บรักษาข้อมูลจราจรตามภาคผนวกต่าง ๆ ที่กล่าวไปข้างต้นนั้น ให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น

บทวิเคราะห์ : หมายความว่าข้อมูลจราจรที่ไม่เกี่ยวข้องกับบริการของตนไม่ต้องจัดเก็บ

ข้อ ๘ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

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

บทวิเคราะห์ : สื่อ (Media) ที่จัดเก็บข้อมูลจราจร ควรต้องเป็นสื่อที่สามารถป้องกันความปลอดภัยจากการแก้ไขข้อมูลโดยมิชอบของผู้ที่ไม่มีส่วนเกี่ยวข้องได้เป็นอย่างดี เรียกได้ว่าสามารถรักษาความถูกต้องของข้อมูลจราจรไว้ได้เพื่อให้มีน้ำหนักในชั้นศาลในการสืบสวนสอบสวนต่อไปและควรต้องมีระดับชั้นความปลอดภัยในการเข้าถึงข้อมูลจราจรดังกล่าว (Access Control) โดยระบุเป็นตัวบุคคลได้ ซึ่งควรต้องมีระบบ Authentication หรือ Identity Management เป็นต้น (ระบบ Authentication ยกตัวอย่าง เช่น การใช้ระบบ Microsoft Active Directory)

(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

บทวิเคราะห์ : การเก็บ log file ไว้ในเครื่องนั้นอาจทำให้ความปลอดภัยของ log file ไม่ดีพอและไม่น่าเชื่อถือเนื่องจาก log file อาจถูกแก้ไขโดยผู้ดูแลระบบ (system administrator) ของเครื่องนั้น หรืออาจถูกแก้ไขโดยแฮกเกอร์ ดังนั้นจึงควรจัดเก็บ log file ในแบบรวมศูนย์ (Centralized Log) และมีการตรวจสอบ Integrity โดยการทำ Data hashing เมื่อ log file มีปริมาณมากก็ควรทำ Data Archiving เพื่อทำให้มีพื้นที่ในการจัดเก็บ log file เพิ่มขึ้น รวมทั้งผู้ที่สามารถเข้าถึงข้อมูล log file ควรเป็นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) หรือ ผู้เชี่ยวชาญด้านความปลอดภัยข้อมูล หรือ บุคคลที่องค์กรมอบหมายให้ติดต่อกับพนักงานเจ้าหน้าที่เท่านั้น โดยที่ system admin ไม่ควรมีสิทธิเข้ามาแก้ไข log file ดังกล่าว

(๓) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

บทวิเคราะห์ : ผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ควรถูกแต่งตั้งโดยผู้บริหารระดับสูงขององค์กรไว้ล่วงหน้าเพื่อเวลาพนักงานเจ้าหน้าที่ต้องการข้อมูลจะได้ประสานงานได้อย่างถูกต้องและรวดเร็ว

(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

บทวิเคราะห์ : การที่จะระบุผู้ใช้บริการเป็นรายบุคคลได้นั้นองค์กรจำเป็นที่จะต้องมีระบบ Authentication เพื่อให้ผู้ใช้บริการเข้ามา Log on หรือ Sign On กับระบบ โดยอาจผ่านทางระบบ proxy หรือระบบ cache โดยสามารถตรวจสอบผู้ใช้บริการเป็นรายบุคคลแบบหนึ่งต่อหนึ่ง ซึ่งผู้ใช้บริการควรเก็บรักษารหัสผ่านของตนไว้เป็นความลับและไม่ควรมีการใช้ชื่อร่วมกัน (Shared User ID) ในการเข้าใช้งานระบบทุกระบบโดยเฉพาะระบบอินเทอร์เน็ต

สำหรับบริการของ Service provider เช่นการใช้ Air card หรือ การใช้ SIM card แบบ prepaid ก็ควรต้องระบุตัวตนของผู้ใช้งานหรือผู้ที่จดทะเบียนเป็นเจ้าของ Air card หรือ SIM card ดังกล่าวเพื่อที่จะให้พนักงานเจ้าหน้าที่สามารถติดตามตรวจสอบการใช้งานของผู้ต้องสงสัยได้

(๕) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ ๑ ถึงข้อ ๔ ข้างต้น ได้ให้บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้ผู้ให้บริการในข้อ ๑ ถึงข้อ ๔ ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการเช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

บทวิเคราะห์ : ยกตัวอย่างผู้ให้บริการเช่าเว็บไซต์ (web site) ที่จดทะเบียนทำธุรกิจในประเทศไทยแต่ใช้คอมพิวเตอร์ที่ทำหน้าที่เป็นเว็บไซต์ (web server) อยู่ในประเทศสหรัฐอเมริกา ซึ่งไม่สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ได้ผู้ให้บริการดังกล่าวควรมีระบบสมาชิกที่สามารถติดตามผู้ใช้บริการที่มาเช่าเว็บไซต์ (web site) ได้ เพื่อที่จะให้สามารถระบุตัวบุคคลของผู้ใช้บริการได้อย่างไม่มีปัญหา

ข้อ ๙ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

บทวิเคราะห์ : การอ้างอิงเวลาของระบบที่องค์กรใช้งานอยู่ให้ตรงกับเวลาสากล ได้แก่ การรับสัญญาณนาฬิกาจากดาวเทียม หรือ การใช้ระบบ GPS หลายคนรู้จักกันในนาม atomic clock ซึ่งเทียบได้กับ Stratum 0 สำหรับการรับสัญญาณนาฬิกาโดยการใช้ Network Time Protocol จาก NTP server ก็ถือว่าอนุโลมได้เพราะตัว NTP server มีการอ้างอิงเวลามาจาก Stratum 0 เช่นกัน

ข้อ ๑๐ ผู้ให้บริการซึ่งมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ ๗ เริ่มเก็บข้อมูลดังกล่าวตามลำดับ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นสามสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

(๒) ให้ผู้ให้บริการตามข้อ ๕ (๑) ข. เฉพาะผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (ISP) เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศในราชกิจจานุเบกษาผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ ๑๐ (๑) และข้อ ๑๐ (๒) ข้างต้น ให้เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

บทวิเคราะห์ : จะเห็นว่าองค์กรภาครัฐและเอกชนทั่วไปมีเวลาเตรียมการในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไม่เกินหนึ่งปี ดังนั้นควรจะเตรียมการล่วงหน้าก่อนถึงเวลาสิ้นสุดการผ่อนผัน

ภาคผนวก ก
แนบท้ายประกาศรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ
พ.ศ. ๒๕๕๐
.....

๑. ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้โดยผ่านทางระบุคอมพิวเตอร์ 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 เว้นแต่ผู้ให้บริการนั้น ให้บริการแต่เพียง 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)ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถือ อันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร
	๓)จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

บทวิเคราะห์ : ในปัจจุบันและอนาคตการใช้โทรศัพท์เคลื่อนที่หรือใช้ระบบ Air card ในการทำอาชญากรรมทางคอมพิวเตอร์มีแนวโน้มสูงขึ้นเรื่อยๆ เนื่องจากเป็นบริการแบบไร้สายที่สะดวกสบายสำหรับอาชญากรสมัยใหม่ ดังนั้นการสืบค้นข้อมูลจาก Cell ID จึงมีความสำคัญอย่างมากที่จะสามารถระบุตัวผู้ต้องสงสัยได้ในเวลาไม่นานนัก รวมทั้งตำแหน่งที่อยู่ของโทรศัพท์หรือ Air card ที่ใช้ในการก่ออาชญากรรม ถ้ามีการเก็บข้อมูลไว้ก็จะมีประโยชน์ในการสืบสวนสอบสวนได้ง่ายยิ่งขึ้น

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)

ประเภท	รายการ
	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)
ง) 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 เช่นกัน

สำหรับการเก็บข้อมูลจราจรของระบบอีเมล์ ประกาศกระทรวงฯไม่ได้กำหนดให้ต้องเก็บตัวเนื้อความในจดหมายหรือไฟล์แนบแต่อย่างใด หากต้องการให้เก็บเฉพาะ Email header ที่สามารถติดตามหาข้อมูลผู้รับผู้ส่งได้ก็ถือว่าเพียงพอแล้วซึ่งโดยปกติเรามักเก็บอีเมล์ไว้เกินเก้าสิบวันอยู่แล้วจึงไม่น่าจะมีปัญหาในกรณีนี้ ส่วนการเก็บข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล หมายความ รวมถึง FTP server, SSH server และ HTTP server ที่มีการ Upload และ Download แฟ้มข้อมูล จึงควรมีระบบ Authentication ในการตรวจสอบการเข้าถึงแฟ้มข้อมูลของผู้ใช้บริการเช่นเดียวกัน

สำหรับข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บจากเครื่องให้บริการเว็บ (Web Server) ควรมีการจัดเก็บข้อมูลผู้เข้ามาเยี่ยมชมเว็บโดยมีการเก็บ IP address และตำแหน่งของ web page และข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูลที่ผู้เข้ามาเยี่ยมชมได้เรียกเว็บเพจ (web page) จากเครื่องให้บริการเว็บ (web server) ซึ่งในทางเทคนิคเรียกว่า URI (Universal Resource Identifier)

ในส่วนข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) ยกตัวอย่าง เช่น การ chat ผ่าน MSN หรือ การใช้ program windows messenger ก็ควรมีการจัดเก็บบันทึกการใช้งานของผู้ใช้บริการตามที่ประกาศกระทรวงฯ ได้กำหนดไว้โดยไม่จำเป็นต้องเก็บข้อมูลการสนทนาแต่อย่างใดเพราะถ้ามีการจัดเก็บอาจถือได้ว่าเป็นการละเมิดสิทธิส่วนบุคคลได้ หากไม่ได้แจ้งให้ผู้ใช้บริการทราบล่วงหน้า

๓.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ง. มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

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

บทวิเคราะห์ : ผู้ให้บริการร้านอินเทอร์เน็ตมีหน้าที่เก็บข้อมูล 3 ประเภท ได้แก่ข้อมูลที่สามารถระบุตัวบุคคล เช่น เลขประจำตัวบัตรประชาชนของผู้มาใช้บริการหรือรูปถ่ายของผู้มาใช้บริการจากกล้องดิจิตอล หรือกล้องโทรทัศน์วงจรปิดก็ได้เช่นกันและต้องเก็บเวลาการเข้าใช้และเวลาการเลิกใช้บริการของผู้ใช้บริการด้วยวิธีใดก็ได้แล้วแต่ความสะดวกของผู้ให้บริการรวมถึงต้องจัดเก็บหมายเลข IP address ของคอมพิวเตอร์ที่ให้บริการแต่ละเครื่องให้สอดคล้องกับผู้ใช้บริการและเวลาที่ใช้เพื่อให้สามารถระบุตัวตนของผู้ใช้บริการในขณะใดขณะหนึ่งได้

๔.ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๒) มีหน้าที่ต้องเก็บรักษา มีดังต่อไปนี้

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

บทวิเคราะห์ : โดยปกติแล้วผู้ที่เข้ามาแสดงความเห็นในเว็บบอร์ดมักจะไม่ลงชื่อและไม่ลงทะเบียน เมื่อมีข้อพิพาทเกิดขึ้น เช่น มีการหมิ่นประมาท ก็มักจะหาตัวของคู่กรณีไม่พบ ดังนั้นกฎหมายจึงระบุให้ผู้ให้บริการเว็บบอร์ดหรือผู้ให้บริการที่อนุญาตให้บุคคลทั่วไปเข้ามาแสดงความคิดเห็นได้ ยกตัวอย่าง เช่น เว็บของหนังสือพิมพ์ต่างๆ ในทุกวันนี้ ควรต้องมีระบบสมาชิกที่สามารถระบุตัวตนของผู้ที่เข้ามาแสดงความคิดเห็นได้ เช่น ชื่อ ที่อยู่ หรือ Email address ของผู้ใช้บริการที่พอจะตามตัวได้ ตลอดจนบันทึกข้อมูลการเข้าใช้บริการว่ามาจาก IP address ใด ซึ่งส่วนใหญ่จะเก็บไว้ใน Log File ของ Web Server อยู่แล้ว

สรุปได้ว่าผู้บริหารองค์กรควรตั้งคณะทำงานเพื่อทำการวิเคราะห์ พรบ.การกระทำความผิดฯ และประกาศกระทรวงฯ อย่างละเอียดรอบคอบตลอดจนจัดเตรียมงบประมาณในการจัดซื้ออุปกรณ์ ฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ที่เหมาะสมและสอดคล้องกับวัตถุประสงค์ของกฎหมายหรืออาจมีทางเลือกโดยการ Outsource ให้ผู้เชี่ยวชาญหรือ MSSP เข้ามาบริหารจัดการให้แบบครบวงจรก็จะช่วยแบ่งเบาภาระของผู้บริหารองค์กรเป็นการประหยัดเวลาของผู้บริหารได้เป็นอย่างดีตลอดจนเป็นการ Transfer Risk อย่างชาญฉลาดอีกด้วย การปฏิบัติตาม พรบ.การกระทำความผิดฯ ถือเป็นหน้าที่อันพึงปฏิบัติของคนไทยทุกคนในสังคมยุคสารสนเทศที่คอมพิวเตอร์ได้เข้ามามีบทบาทสำคัญกับการทำงานและการใช้ชีวิตประจำวันของพวกเราทุกคนอย่างหลีกเลี่ยงไม่ได้

6. ระบบโครงสร้างพื้นฐานที่องค์กรควรจัดทำเพื่อรองรับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ระบบโครงสร้างพื้นฐานสารสนเทศ (IT infrastructure) ที่องค์กรควรจัดทำเพื่อรองรับ พรบ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นควรมีระบบอย่างน้อย ดังต่อไปนี้

ระบบที่จำเป็นต้องมี (Mandatory)

- ระบบโครงสร้างพื้นฐานสำหรับการพิสูจน์ตัวตน (Identification and Authentication System)
- ระบบโครงสร้างพื้นฐานสำหรับการเก็บปูมระบบที่ส่วนกลาง (Centralized Log Management System) หรือระบบ 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

7. รายละเอียดการจัดเก็บ Log ตามประกาศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ตามประกาศข้อ ๕ (๑) ข. ถึง ค. ทั้งหมด 6 ประเภท ได้แก่

7.1 การเก็บ Log ที่เกิดจากการเข้าถึงระบบเครือข่าย (Authentication Server)

ระบบ Local Area Network (LAN) ที่เราใช้กันอยู่ในทุกวันนี้ โดยปกติแล้วไม่มีการ Logon เข้าระบบ Domain ที่ส่วนกลาง (นิยมเรียกว่า Logon เข้า Microsoft Active Directory) หลายองค์กรมีการ Logon แบบ "Local Logon" คือ Logon เข้าที่เครื่องตนเอง ซึ่งการปฏิบัติที่ถูกต้อง ควรให้ทุกเครื่องในระบบเครือข่ายขององค์กรทำการ "Join Domain" เชื่อมเข้าสู่ระบบการพิสูจน์ตัวตนจากส่วนกลาง (Microsoft Active Directory) น่าจะเป็นแนวทางที่ดีกว่า เพราะการ Logon จะเกิดขึ้นที่เครื่อง Domain Controller (DC) ไม่ได้เกิดขึ้นที่เครื่อง Workstation ดังนั้น การจัดเก็บ Log การ Logon เข้า – ออก ก็สามารถทำได้ง่ายจากส่วนกลางโดยเราสามารถดึง Log จาก Domain Controller มายัง Centralized Log Server

ตัวอย่าง ผลิตภัณฑ์ที่สามารถเก็บ Log แบบ Centralized Log ได้ ที่นิยมเรียกว่า SEM (Security Event Management) ยกตัวอย่าง เช่น

- Cisco MARS
- ACIS i-Secure Logger

สำหรับการวิเคราะห์ Log หลายองค์กรนิยม Outsource ให้ MSSP (Managed Security Service Provider) จัดการไปเลย จะประหยัดค่าใช้จ่ายให้องค์กรได้มากกว่าการซื้อ "SIM" หรือ "Security Informaion Management" มาใช้เอง ซึ่งมีค่าใช้จ่ายค่อนข้างสูง

ตัวอย่างผลิตภัณฑ์ SIM หรือ SIEM (Security Information and event management) ได้แก่

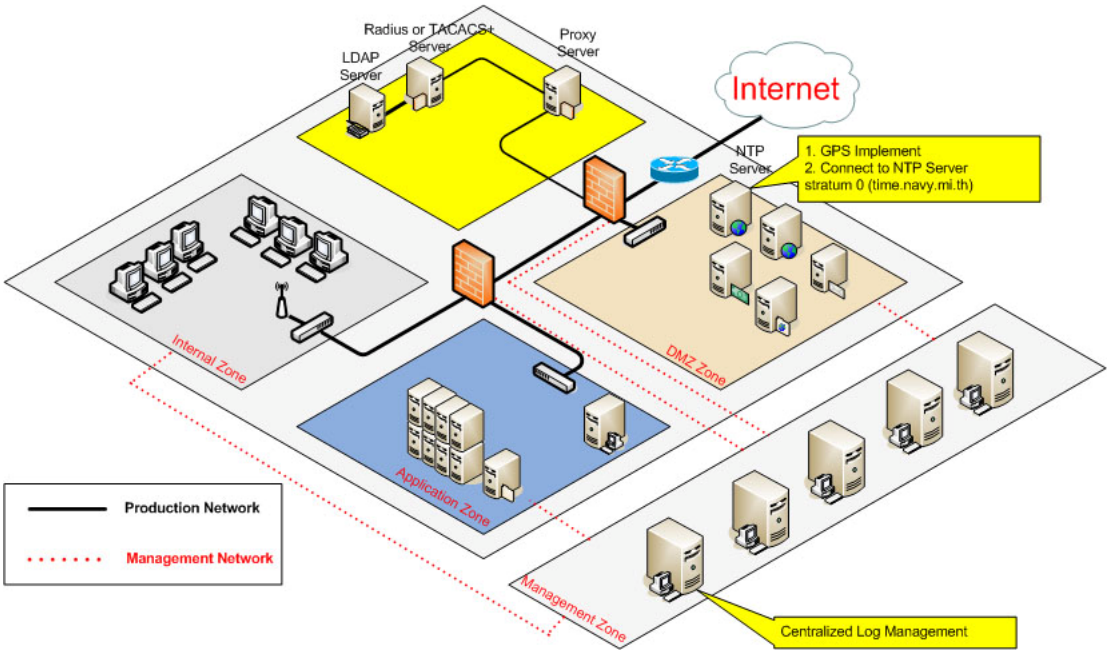
- Cisco MARS (**เป็นทั้ง SIM และ SEM รวมเรียกว่า SIEM**)
- ACIS i-Secure IntelligenceLogic Engine (SIM)

การทำผลิตภัณฑ์ที่มีลักษณะผสมผสานระหว่าง SIM และ SEM ที่เรียกว่า SIEM นั้น ต้องพิจารณาทั้งขนาดของระบบหรือ "SIZING" ด้วย เพราะถ้าเป็นระบบขนาดใหญ่ที่มีปริมาณ Traffic Data หรือ Log จากอุปกรณ์จำนวนมาก ก็อาจจะทำให้เกิดปัญหาคอขวด (Bottleneck) ในการจัดเก็บ Log ที่ส่วนกลางได้ เพราะอุปกรณ์ต้องทำงานทั้งสองอย่างคือ เก็บ Log เพื่อวิเคราะห์ Log ด้วย ถ้าอุปกรณ์เป็นรุ่นใหญ่ที่มีประสิทธิภาพสูงก็ไม่น่าจะมีปัญหา แต่ถ้าเป็นอุปกรณ์รุ่นเล็กก็อาจจะเกิดปัญหาได้ จึงต้องระมัดระวังในประเด็นนี้

สำหรับการ Logon ที่ไม่ได้เชื่อมต่อกับ Microsoft Active Directory (AD) ตรงๆ ก็สามารถเชื่อมกับ RADIUS Server ที่เป็น 3rd Party ได้ จากนั้นค่อยต่อจาก RADIUS มายัง Microsoft AD อีกทีหนึ่ง การเก็บชื่อและรหัสผู้ใช้ควรเก็บไว้ใน LDAP Server หรือ Microsoft AD Server

ตัวอย่างโปรดักส์ RADIUS/TACACS+ ที่นิยมในท้องตลาดวันนี้ ได้แก่ Cisco Secure ACS

การ Logon ภายในระบบ LAN หรือ ระบบอินทราเน็ต (Intranet) ก็ควรจะมีการจัดเก็บ Log เช่นเดียวกัน ถึงแม้ว่าประกาศกระทรวงจะระบุแต่เพียงการเชื่อมต่อกับระบบอินเทอร์เน็ต (Internet) เพื่อยกเป็นตัวอย่าง เราจึงควรที่จะจัดเก็บการใช้งานที่เชื่อมกับระบบ Internet ก่อน จากนั้นค่อยทำให้ครบโดยจัดเก็บการใช้งานที่เชื่อมกับระบบ Intranet ด้วย หรือจะเก็บควบคู่กันไปเลยก็ยิ่งดี



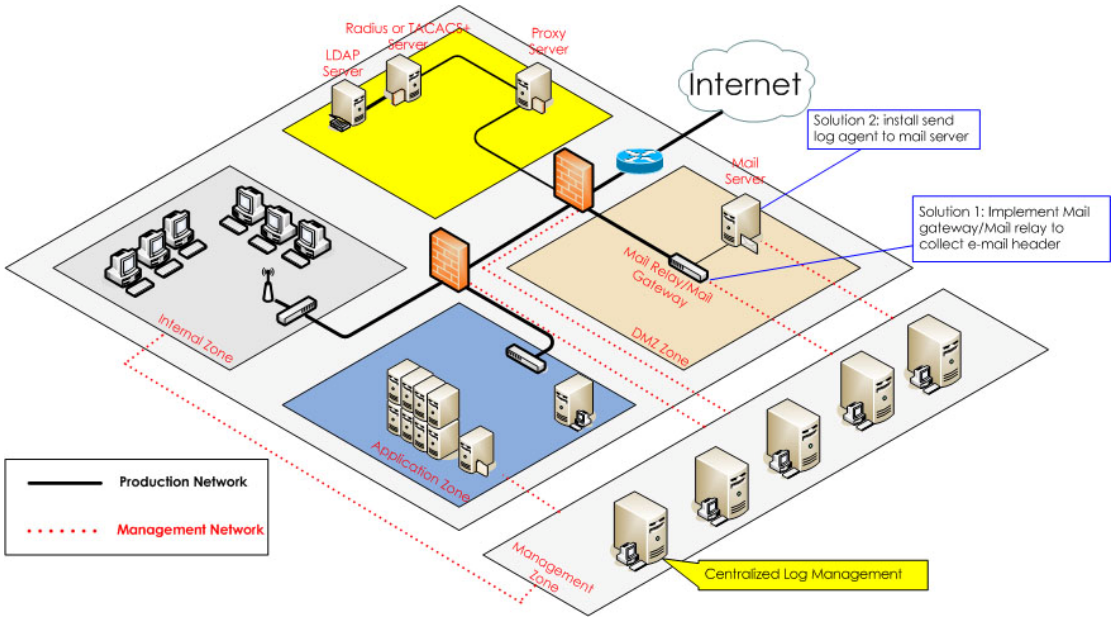
7.2 การเก็บ Log ที่เครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (eMail Server)

หลายองค์กรมีปัญหาในการจัดเก็บ Log ที่ระบบ eMail กันพอสมควร เพราะส่วนใหญ่ในทุกวันนี้พนักงานในองค์กรหันมาใช้ Free eMail ที่เป็น Web-based eMail เช่น Hotmail หรือ Gmail เป็นต้น ทำให้การเก็บ Log ที่ทางประกาศกระทรวงฯ ให้จัดเก็บนั้นทำได้ยากลำบาก เพราะไม่ได้มีการเก็บ eMail ไว้ที่เครื่องแม่ข่ายในองค์กร ในกรณีนี้ก็คงทำได้แค่เพียงจัดเก็บการ Authenticate กับ Proxy Sever หรือ Firewall ก่อนที่จะออกสู่ระบบอินเทอร์เน็ต เท่านั้น ส่วนการ Authentication ที่ Hotmail หรือ Gmail นั้นก็จัดเก็บได้ยากเพราะเป็นการ Authentication ด้วย SSL Protocol (https) การ Terminate SSL ต้องใช้ Key ในการถอดรหัส SSL Session เพื่อบันทึก Username ในทางเทคนิคสามารถทำได้ แต่ค่อนข้างยากและอุปกรณ์มีราคาสูงพอสมควร

สำหรับองค์กรที่มีระบบ eMail เป็นของตัวเอง เช่น Microsoft Exchange หรือ Lotus Notes ควรที่จะจัดเก็บข้อมูล eMail Log ตามที่ประกาศกระทรวงฯ ได้กำหนดไว้โดยประกาศกระทรวงฯ ให้จัดเก็บเฉพาะ eMail Header เท่านั้นไม่ต้องเก็บ Body (เนื้อความ) ของ eMail และไม่ต้องเก็บ attached File (ไฟล์แนบ ซึ่งโดยปกติ

แล้ว หลายองค์กรก็มีการเก็บ eMail ไว้นานกว่า 3 เดือนอยู่แล้ว (eMail Header ก็อยู่ใน Mailbox ด้วย ถ้าผู้ใช้ eMail ยังไม่ลบ eMail เสียก่อน) ดังนั้นเพื่อเป็นการป้องกันไม่ให้ผู้ใช้ลบ eMail ในกรณีดังกล่าว ควรมีการ archive eMail หรือ backup eMail เก็บไว้เสียก่อนเป็นระยะๆ ก็เป็นแนวคิดหนึ่งที่ทำได้

อีกแนวคิดหนึ่งก็คือ การดึง Log ออกจาก eMail Server ซึ่งต้องการการติดตั้งและปรับแต่งในระดับลึกพอสมควร ต้องว่าจ้างผู้เชี่ยวชาญมาช่วยในการติดตั้งและปรับแต่ง บางองค์กรมีแนวคิดในการเก็บ Log ที่ Mail Relay หรือ Mail Gateway เช่น CISCO IronPort ก็สามารถทำได้เช่นกันหรืออาจจะดึงข้อมูลจาก Router หรือ Switching ในรูปแบบของ Netflow Traffic ก็ได้ แต่ต้องเป็นรุ่นที่มี Netflow Feature และอุปกรณ์ที่จัดเก็บ Log ใน Format ของ Netflow ต้องมีความจุของฮาร์ดดิสก์มากพอในระดับหนึ่ง รวมทั้งมีซอฟต์แวร์ในการวิเคราะห์ Netflow Traffic ด้วย ซึ่งอาจจะใช้ซอฟต์แวร์ที่เป็น Open source หรือ Freeware ก็สามารถทำได้เช่นกัน



7.3 การจัดเก็บ Log จากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล (File Sharing Server)

ระบบที่ใช้การโอนถ่ายไฟล์ข้อมูล ไม่ได้มีเฉพาะโปรโตคอล FTP แต่อาจจะใช้โปรโตคอลอื่น เช่น HTTP, SSH, https หรือโปรโตคอลที่ใช้ในการ Map Network Drive ในระบบของ Microsoft เช่น โปรโตคอล SMB ซึ่งในระบบ UNIX / LINUX นิยมใช้โปรโตคอล NFS

ประกาศกระทรวง ฯ มีเจตนาให้ครอบคลุมทุกโปรโตคอลดังกล่าว แต่หากทำทั้งระบบอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) พร้อมกันอาจเป็นงานที่หนักเกินไป ควรทำเป็นระยะๆ เช่น ระยะที่หนึ่ง ควรจัดเก็บข้อมูลการโอนย้ายถ่ายไฟล์ข้อมูลระหว่างระบบภายในกับระบบอินเทอร์เน็ตเสียก่อน จากนั้นในระยะที่ 2 ก็ควรทำกับระบบโอนย้ายถ่ายไฟล์ข้อมูลภายในด้วย เผื่ออาจเกิดเหตุการณ์ Security Incident ขึ้นภายในองค์กรเองก็มีโอกาสที่เป็นไปได้เช่นกัน การจัดเก็บ Log ของระบบดังกล่าวให้เก็บเฉพาะชื่อไฟล์, วันเวลา, ชื่อผู้ใช้ และเส้นทาง (PATH) ที่เก็บไฟล์ในเครื่องแม่ข่าย โดยไม่มีความจำเป็นต้องเก็บเนื้อไฟล์ซึ่งมีขนาดใหญ่จนหลาย

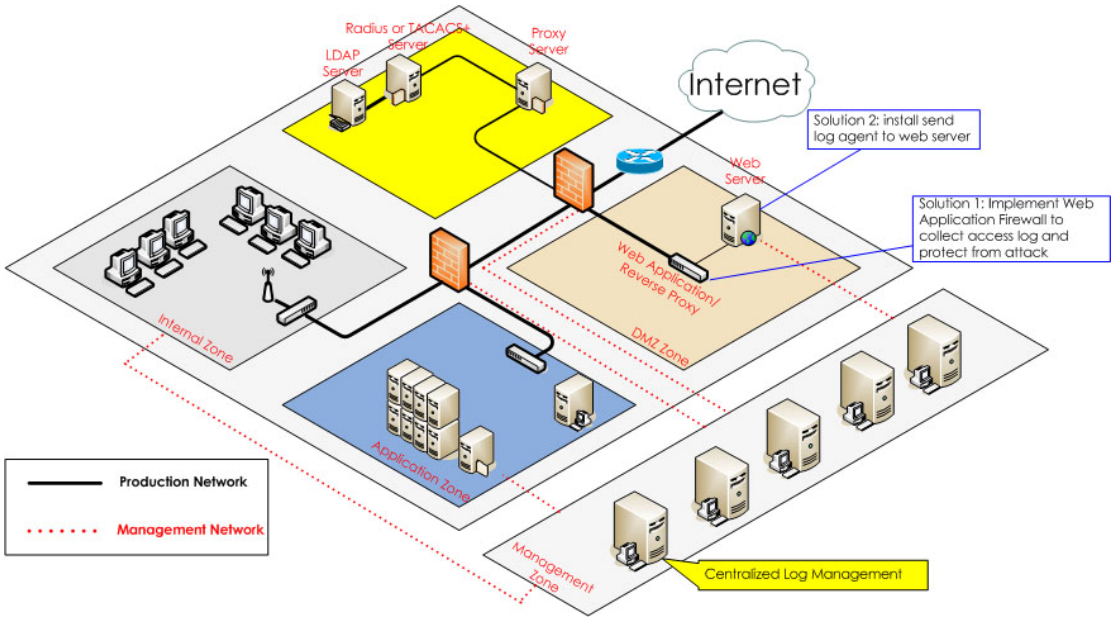
องค์กรไม่สามารถทำได้ในทางปฏิบัติ (แนวทางนี้สามารถนำไปใช้กับการจัดเก็บ Log ของ Web Server ในข้อต่อไปด้วย)

7.4 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 7.1 คือ การจัดเก็บ Log ในการเข้าถึงระบบเครือข่าย เช่น ก่อนที่พนักงานจะใช้งานระบบอินเทอร์เน็ต ควรมีการ Logon หรือ Authentication ที่ Proxy Server หรือ Firewall เสียก่อน ถ้าใช้ Proxy Sever ก็สามารถจัดเก็บ URI (Uniform Resource Identifier) ที่ผู้ใช้งานอินเทอร์เน็ตในองค์กรเข้าเรียกชม Web site ต่างๆ ได้ เพื่อที่จะได้สามารถนำมา "MAP" หรือ เชื่อมโยงในการแกะรอยตามสืบสวนว่าใครเป็นคนใช้อินเทอร์เน็ตเข้า Web site ในช่วงเวลาดังกล่าว เช่น ถ้ามีการแจ้งความว่ามีการนำเข้าข้อมูลอันเป็นเท็จใน Web Board แห่งหนึ่ง ทางพนักงานเจ้าหน้าที่ก็มีความจำเป็นต้องแกะรอยจาก Proxy Server หรือ Authentication Server และ Web Server เพื่อเชื่อมโยงข้อมูลเข้าด้วยกัน ดังนั้นถ้าหากขาด Log ในส่วนใดส่วนหนึ่งไปก็จะทำให้หลักฐานไม่สมบูรณ์ และยังมีประเด็นเรื่อง NTP Server ที่ควรติดตั้งในองค์กรโดยนำเวลาที่อ้างอิงมาจาก Stratum 0 มาจ่ายให้กับ Proxy Server และ Web Server อีกด้วย ทั้งนี้ก็เพื่อให้ Log ใน Server ทั้งสองไม่ผิดเพี้ยนไปจากที่ควรจะเป็น

ปัญหาในการจัดเก็บ Log จาก Web Server ก็คือ 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

อีกปัญหาหนึ่งก็คือ Web Browser และ Web Server มักจะติดต่อกันด้วย 2 Method เป็นประจำ คือ Method "GET" และ Method "POST" สำหรับ Method "GET" ทาง Web Server มีการจัดเก็บอยู่แล้วไม่มีปัญหาแต่สำหรับ Method "POST" ซึ่งมักจะมีการคีย์ข้อมูลของผู้เข้าถึง Web Server หรือ มีการคีย์ข้อมูลที่เป็นการโจมตีของแฮกเกอร์นั้น ปกติ Web Server จะไม่เก็บข้อมูล Method "Post" เหล่านี้ ดังนั้นเราต้องมีการจัดวาง "Reverse Proxy" หรือ "Web Application Firewall" มาช่วยในการเก็บข้อมูลดังกล่าว เพื่อนำไปใช้เป็นหลักฐานในอนาคต หรือ ใช้เพื่อการวิเคราะห์โดยระบบ SIM ว่ามีการโจมตี Web Server ของเราหรือไม่ ดังนั้นเราจึงต้องเพิ่มอุปกรณ์และออกแบบระบบให้รองรับกับการเก็บ Log ของ Web Server ดังที่กล่าวมาแล้ว

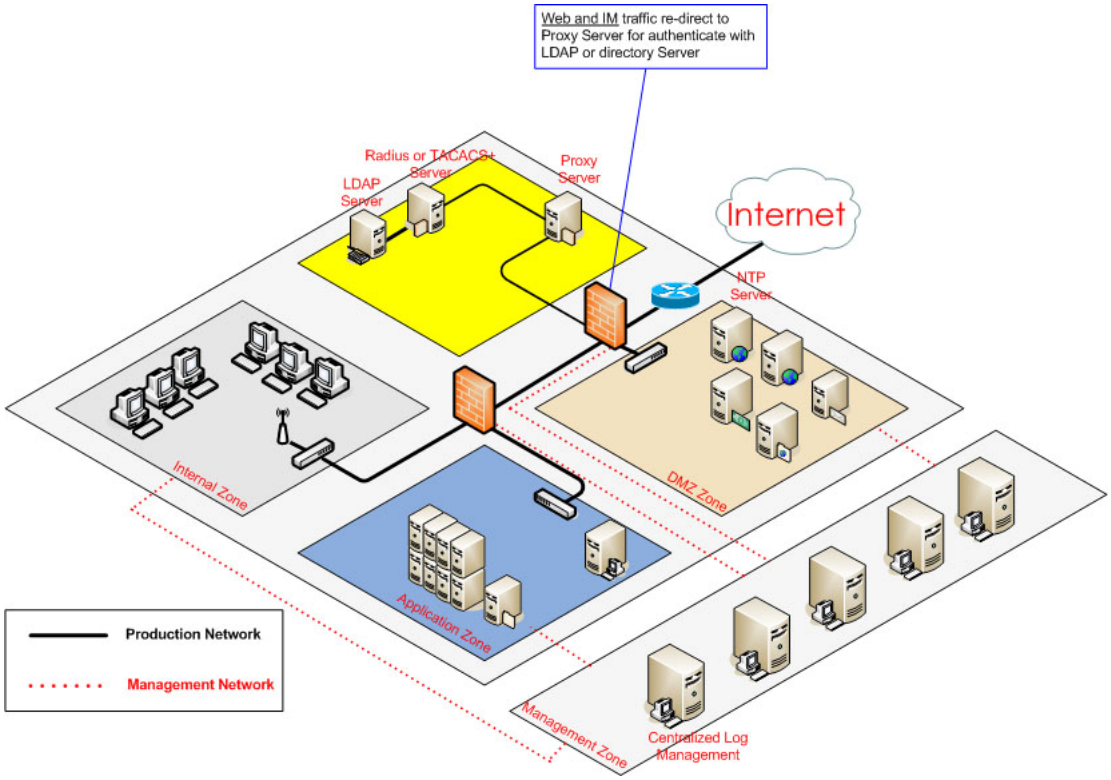


7.5 การจัดเก็บ Log ของระบบ USENET

ระบบ USENET หรือ NEWSGROUP ที่ใช้โปรโตคอล NNTP ในปัจจุบัน เราไม่ค่อยได้ใช้กันแล้วจึงไม่มีความจำเป็นต้องจัดเก็บแต่อย่างใด แต่ถ้ามีความจำเป็นต้องใช้ก็ต้องจัดวางโครงสร้างพื้นฐานให้รองรับการเก็บ Log ด้วย

7.6. การจัดเก็บ Log ของระบบ IRC และ IM

ในปัจจุบันการใช้งานโปรโตคอล IRC ไม่เป็นที่นิยมแล้ว เพราะผู้ใช้งานส่วนใหญ่นิยมใช้บริการ Instant Messaging เช่น MSN, Yahoo Messenger เป็นต้น **แต่ในทางตรงกันข้าม ในโลกของแฮกเกอร์ กลับนิยมใช้โปรโตคอล IRC ในการควบคุม BOT ที่แฮกเกอร์ได้ทำการยึดเครื่องคอมพิวเตอร์ของเหยื่อแล้วควบคุมเครื่องเหล่านั้นหลาย ๆ เครื่องซึ่งกลายเป็นปัญหา "BOTNET" หรือ "Robot Network" ซึ่งกำลังกลายเป็นปัญหาใหญ่ของ ISP ทั่วโลกในเวลานี้** ดังนั้นการจัดเก็บ Log ของการใช้งาน IRC คงมีไม่มากนัก ถ้าจะดูการโจมตีด้วย BOTNET ก็สามารถดู Log จากระบบ IPS หรือ IDS ได้ แต่สำหรับ IM เราควรเก็บ Log เมื่อผู้ใช้ IM ทำการ "Authen" หรือ "Logon" เข้าสู่ระบบ (จะเข้าเงื่อนไขแบบเดียวกับข้อ 7.1) แต่เราควรแยกแยะได้ว่า เป็นการ Authen เพื่อออกไปใช้งาน Internet โดยทั่วไป เช่น ชม Web site, ส่ง Web Mail หรือ เป็นการ Authen เพื่อออกไปใช้งาน IM เช่น MSN เป็นต้น



8. ความเข้าใจผิดเกี่ยวกับ พรบ.ฯ และ ประกาศกระทรวงเทคโนโลยีสารสนเทศ และการสื่อสาร ฯ

8.1 เข้าใจว่าไม่ต้องเก็บ Log เป็นรายบุคคล และ ไม่ต้องมีระบบ Authentication

<u>คำอธิบาย</u> การที่กฎหมายกำหนดให้มีการเก็บ Log อย่างน้อย 90 วันนั้น จะไม่มีประโยชน์เลยถ้า Log ที่เก็บไว้ไม่สามารถระบุตัวบุคคลเป็นรายบุคคลได้ เพราะวัตถุประสงค์ที่แท้จริงของกฎหมายก็คือ การสืบสวนสอบสวนหาตัวผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นรายบุคคล ดังนั้นจึงจำเป็นต้องมีระบบ Authentication ที่เก็บข้อมูลผู้ใช้เป็นรายบุคคลแบบ “หนึ่งคน หนึ่งชื่อผู้ใช้ หนึ่งรหัสผ่าน” (Accountability) เพื่อให้สามารถแยกแยะตัวบุคคลได้ในที่สุด

8.2. เข้าใจว่าไม่ต้องจัดเก็บ Log แบบ Centralized Log (เก็บลง Log Server ที่ส่วนกลาง)

<u>คำอธิบาย</u> การเก็บ Log ของเครื่องแม่ข่ายและอุปกรณ์เครือข่ายต่างๆ นั้น เป็นเรื่องสำคัญที่มีความจำเป็นต้องเก็บ Log ลงบน Log Server ที่ส่วนกลาง ก็เป็นเพราะว่า Log ที่อยู่ในเครื่องแม่ข่ายสามารถถูกแก้ไขได้โดยผู้ดูแลระบบ (System Administrator) หรือ สามารถถูกแก้ไขโดยแฮกเกอร์หรือไวรัสคอมพิวเตอร์ก็เป็นไปได้ ทำให้ความน่าเชื่อถือของ Log ที่มาจากเครื่องแม่ข่ายค่อนข้างต่ำ เวลานำขึ้นพิจารณาในชั้นศาล อาจจะไม่สามารถนำมาใช้ได้ เรียกว่า หลักฐานอ่อน ไม่มีน้ำหนักเพียงพอ ดังนั้นเราจึงควรจัดเก็บ Log ลงใน Log Server

ที่ส่วนกลาง (Centralized Log Server) หรือใช้ระบบ SEM (Security Event Management) ก็จะสามารถเพิ่มความน่าเชื่อถือให้กับระบบการจัดเก็บ Log โดยรวม

8.3 เข้าใจว่าไม่ต้องจัดทำ Security Awareness Training ให้กับผู้บริหารระดับสูงและผู้ใช้งานคอมพิวเตอร์ทั่วไป โดยอบรมเฉพาะเจ้าหน้าที่ฝ่ายสารสนเทศเท่านั้น

<u>คำอธิบาย</u> การให้ข้อมูลเรื่องกฎหมายกับผู้บริหารระดับสูงและผู้ใช้งานคอมพิวเตอร์ส่วนใหญ่ที่ไม่ใช่ "คนไอที" ถือเป็นเรื่องที่สำคัญอย่างยิ่งยวด ไม่สามารถจะมองข้ามได้ เพราะถ้าหากผู้บริหารและผู้ใช้งานคอมพิวเตอร์โดยเฉพาะพนักงานทั่วไปไม่เข้าใจขั้นตอนตลอดจนไม่ให้ความร่วมมือ โอกาสที่จะประสบความสำเร็จในเรื่องที่เราต้องการให้ทุกคนปฏิบัติตามกฎหมาย พรบ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ก็คงเป็นเรื่องที่ยากยิ่ง ดังนั้น การที่ทุกคนควรจะมีความรู้ความเข้าใจจึงเป็นเรื่องที่องค์กรควรรีบเร่งปฏิบัติก่อนที่จะถึงเส้นตายที่กฎหมายได้กำหนดไว้

8.4 เข้าใจว่าจัดซื้อจัดจ้างระบบจัดเก็บ Log ที่ส่วนกลางน่าจะเพียงพอแล้ว กับการที่กฎกระทรวงฯ ประกาศบังคับ

<u>คำอธิบาย</u> การจัดซื้อระบบเก็บ Log ที่ส่วนกลาง หรือ "SEM" เป็นเรื่องที่ควรทำ แต่ปัญหาอยู่ที่การติดตั้งและปรับแต่งระบบที่จำเป็นต้องทำโดยผู้เชี่ยวชาญในอุปกรณ์แต่ละแบบที่มีความแตกต่างกัน เช่น log ของ Web Server Apache ก็มีความแตกต่างกับ log ของ Web Server IIS เป็นต้น **ดังนั้นการซื้อระบบเก็บ Log เป็นแค่จุดเริ่มต้นเท่านั้น เรายังต้องการการปรับแต่ง (Fine tuning) อีกมากพอสมควร** ตลอดจนถ้าได้ระบบช่วยวิเคราะห์ Log ก็จะทำให้เรารู้ล่วงหน้าว่าระบบเรากำลังถูกโจมตีหรือไม่ เรียกว่า "Proactive Defense" ในกรณีนี้การ "Outsource" ใช้ MSSP (Managed Security Service Provider) น่าจะดีกว่าในมุมของ ROI และ TCO

8.5 เข้าใจว่าการติดตั้งระบบ NTP Server นั้นยุ่งยากและมีค่าใช้จ่ายสูง

<u>คำอธิบาย</u> การติดตั้ง NTP Server สามารถทำได้โดยจัดหาเครื่องแม่ข่ายที่ไม่ต้อง Spec สูงมากนักและให้ติดตั้งโปรแกรม NTP Server ที่มีให้เลือกมากมายในอินเทอร์เน็ต ซึ่งไม่มีค่าใช้จ่ายแต่อย่างใด (เป็น Freeware หรือ Open source) โดยสามารถรับค่าสัญญานนาฬิกาอ้างอิงจาก Stratum 0 เช่น กรมอุทกศาสตร์กองทัพเรือ หรือสถาบันมาตรวิทยา โดยให้เปิด Port UDP 123 ที่ไฟล์วอลล์ด้านนอกที่ต่อเชื่อมกับ ISP เพื่อให้สามารถ "SYNC" เวลาได้ จากนั้น ในองค์กร เราก็ควรปรับแต่งค่าให้เครื่องแม่ข่ายและอุปกรณ์เครือข่ายทุกเครื่อง ทำการอ้างอิงเวลาจาก NTP Server ที่เราเริ่มติดตั้งใช้งานในองค์กรก็จะทำให้เวลามีความเที่ยงตรงตามที่กฎหมายกำหนด

9. “10 **ข้อควรปฏิบัติเพื่อความปลอดภัยขององค์กรและเป็นไปตามที่กฎหมายกำหนด**” (10 Checklist)

ลำดับที่	**รายการที่ควรต้องทำ** (Thing to do)	M* or A*	**ทำแล้ว** (Y)	**ยังไม่ทำ** (N)	**หมายเหตุ**
1	ติดตั้ง Proxy Server เพื่อทำการ Authentication ระบุตัวตนของผู้ใช้งานระบบเครือข่ายเป็นรายบุคคลกับ RADIUS หรือ LDAP server	M			
2	ติดตั้ง Microsoft Active Directory หรือ LDAP Server อื่นๆ เช่น OpenLDAP เพื่อเก็บชื่อผู้ใช้และรหัสผ่าน	M			
3	ติดตั้งระบบ NTP Server เพื่อตั้งค่านาฬิกาของระบบทั้งองค์กรให้ตรงกัน โดยอ้างอิงจาก Stratum 0 และ ปรับแต่งค่าเครื่องแม่ข่ายและอุปกรณ์เครือข่ายให้อ้างอิงเวลากับ NTP Server ดังกล่าว	M			
4	ติดตั้งระบบ SEM (security Event Management) หรือ ระบบ Centralized Log Management ที่สามารถกับ Log ได้ไม่น้อยกว่า 90วัน	M			
5	ติดตั้งระบบ SIM (security Information Management) เพื่อวิเคราะห์ Log	A			
6	ปรับแต่งระบบต่างๆ เพื่อให้ส่ง Log มายัง Log Server ที่ส่วนกลางได้	M			
7	พัฒนานโยบายด้านความปลอดภัยระบบสารสนเทศ(Information Security Policy) และจัดทำ Acceptable Use Policy (AUP) ให้พนักงานทุกคนเซ็นต์รับทราบ	M			
8	จัดฝึกอบรมหลักสูตรความรู้ด้านปลอดภัยเบื้องต้น “Security Awareness Training” ให้กับพนักงานทุกระดับ	M			
9	จัดเตรียมข้อมูลให้ผู้บริหารระดับสูงได้รับทราบในเรื่องของข้อกฎหมายที่ผู้บริหารควรทราบ	M			
10	ประเมินความเสี่ยงระบบสารสนเทศด้วยการทำ Gap Analysis , Vulnerability Assessment Penetration Testing	M			

หมายเหตุ *

M = Mandatory

A = Add-on Option

10. ปัญหาในภาพรวมของการปฏิบัติตาม พรบ.ฯ และประกาศกระทรวงฯ และ แนวทางแก้ปัญหาที่ถูกต้อง

1. ปัญหาคอขวด (Bottleneck) ที่อาจเกิดขึ้นได้ในทุกองค์กร ถ้าออกแบบระบบไม่ดี โดยไม่มีการเผื่อขนาดของอุปกรณ์ (Sizing) ก็อาจก่อให้เกิดปัญหาเวลาที่มีผู้ใช้งานระบบเครือข่ายเป็นจำนวนมาก ดังนั้น จึงควรมีการกำหนดค่า EPS หรือ Event per Second ให้กับอุปกรณ์เวลาจัดซื้อจัดจ้างให้รองรับ Log จากเครื่องแม่ข่าย และอุปกรณ์เครือข่ายทั้งหลายได้อย่างไม่มีปัญหา

2. ปัญหาผู้ใช้งานระบบไม่ยอมรับ เป็นปัญหาเกี่ยวกับ “คน” ไม่ใช่ “เทคโนโลยี” เนื่องจากในปัจจุบันผู้ใช้งานเครือข่ายและระบบอินเทอร์เน็ตมี “ความเคยชิน” กับการใช้งานอินเทอร์เน็ตที่สะดวกสบาย ไม่มีหน้าจอ POP-UP ขึ้นมาถาม Username และ Password ให้รำคาญใจ แต่ภายหลังจากการติดตั้งระบบ Authentication เวลาที่ทุกคนต้องการใช้งานอินเทอร์เน็ตก็ต้องป้อน Username และ Password ในทุกครั้งไป ทำให้ผู้ใช้งานอาจเกิดความไม่สะดวก และ ไม่เข้าใจถึงเหตุผลที่ต้องทำเช่นนี้

ดังนั้นแนวทางในการแก้ปัญหาที่ถูกต้องก็คือ องค์กรควรมีการจัดทำ “Security Awareness Program” ภายในให้กับผู้ใช้งานเครือข่ายและระบบอินเทอร์เน็ต โครงการฝึกอบรมความเข้าใจพื้นฐานด้านความปลอดภัยข้อมูลและความเข้าใจในเรื่องของกฎหมาย ICT ต่างๆ ที่ควรทราบ ผ่านทางการจัด “Security Awareness Program” ก็สามารถที่จะช่วยให้ผู้ใช้งานฯ มีความเข้าใจมากขึ้น อีกทั้งยังพร้อมที่จะปฏิบัติตามนโยบายด้านความปลอดภัยขององค์กรด้วยเต็มใจ ไม่ใช่การบังคับโดยไม่มีเหตุผล

3. ปัญหาเรื่องไม่มีงบประมาณ หรือ งบประมาณไม่เพียงพอ ก็เป็นอีกปัญหาหนึ่งที่ต้องรีบแก้ไขตั้งแต่เนิ่นๆ โดยเฉพาะหน่วยงานราชการที่ต้องวางแผนในการใช้งบประมาณล่วงหน้าเป็นปี จะสังเกตุได้ว่าเส้นตายของการติดตั้งระบบ Centralized Log **ตามกฎหมาย คือ วันที่** 24 **สิงหาคม พ.ศ.** 2551 **ดังนั้นองค์กรไม่ควรเพิกเฉยในขณะที่ยังพอมีเวลาในการดำเนินการของบประมาณที่จะจัดซื้อจัดจ้างให้เรียบร้อยเสียก่อนจะถึงกำหนดเวลาดังกล่าว** อีกทั้งยังต้องเร่งสร้างความรู้ความเข้าใจให้กับผู้บริหารระดับสูงและผู้ใช้งานคอมพิวเตอร์ทั่วไปอีกด้วย

4. ปัญหาเรื่องผู้บริหารระดับสูงไม่ใส่ใจเรื่องกฎหมายมากเพียงพอ นับว่าเป็นปัญหาใหญ่ที่ต้องรีบแก้ไขอย่างรีบด่วน ซึ่งอาจเกิดจากการที่ผู้บริหารระดับสูงไม่ได้รับทราบข้อมูลเรื่องกฎหมายอย่างเพียงพอ ทำให้ตัวผู้บริหารเองซึ่งไม่ใช่คนไอที ไม่ทราบว่าตนและองค์กรต้องปฏิบัติอย่างไร อีกทั้งเรื่องความปลอดภัยข้อมูลคอมพิวเตอร์มักจะเป็น “Second Priority” เสมอ ผู้บริหารส่วนใหญ่จึงไม่ค่อยให้ความสำคัญเท่าใดนัก จนกว่าจะเกิดปัญหาขึ้น ซึ่งบางครั้งก็สายเกินไป ดังนั้น จึงควรมีการให้ข้อมูลกับผู้บริหารระดับสูง เช่น การจัดทำ“Security Awareness Training” ให้กับผู้บริหารระดับสูงซึ่งควรใช้เวลาประมาณ 1-3 ชั่วโมง เพื่อสร้างความเข้าใจในเรื่องกฎหมาย พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ เพราะหากผู้บริหารไม่ใส่ใจหรือไม่มีความเข้าใจ ผู้บริหารจะต้องเป็นผู้รับผิดชอบในข้อกฎหมายซึ่งอาจจะมาถึงตัวเมื่อใดก็ได้หลังจากการเกิด

อาชญากรรมทางคอมพิวเตอร์ เมื่อผู้บริหารได้รับทราบข้อมูลแลมีความเข้าใจในเรื่องกฎหมายดังกล่าวแล้ว เชื่อว่าคงไม่มีผู้บริหารคนไหนที่จะนิ่งเฉยไม่ปฏิบัติตามกฎหมายเป็นแน่

5. ปัญหาเรื่องการขาดบุคลกรที่มีความเชี่ยวชาญในเรื่องการจัดเก็บและการวิเคราะห์ Log ปัญหานี้เป็นปัญหาปกติที่สามารถแก้ได้โดยง่าย กล่าวคือหลายองค์กรไม่ได้มีผู้เชี่ยวชาญด้านความปลอดภัย หรือ ผู้เชี่ยวชาญเรื่องการจัดเก็บและวิเคราะห์ Log โดยตรง แต่องค์กรสามารถ Outsource ให้ผู้เชี่ยวชาญจากภายนอกมาช่วยได้ ซึ่งส่วนใหญ่แล้วบริษัทประเภท MSSP หรือ “Managed Security Provider” ควรต้องมีบุคลากรผู้เชี่ยวชาญด้านความปลอดภัยข้อมูลสารสนเทศและมีนักวิเคราะห์ด้านความปลอดภัยฯ หรือ “Security Analyst” เพื่อให้บริการด้านการวิเคราะห์ข้อมูลจาก Log Server อยู่แล้ว ดังนั้นองค์กรจึงไม่มีความจำเป็นต้องลงทุนเพิ่มเรื่องบุคลากรตลอดจนไม่ต้องทำในสิ่งที่องค์กรไม่มีความถนัดและความเชี่ยวชาญ รวมทั้งสามารถประหยัดงบประมาณโดยรวมให้กับองค์กรอีกด้วย

กล่าวโดยสรุป การปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ นั้นถือเป็นหน้าที่ที่ทุกองค์กรต้องปฏิบัติเพื่อแสดงความรับผิดชอบต่อสังคมโดยรวม เพราะเมื่อเกิดเหตุการณ์หรืออาชญากรรมทางคอมพิวเตอร์ การสืบสวนของตำรวจและพนักงานเจ้าหน้าที่จำเป็นที่จะต้องมีหลักฐานทางคอมพิวเตอร์ หรือ Digital Evidence เพื่อใช้ประกอบการพิจารณาคดีในชั้นศาล และระบุหาต้นตอและแหล่งที่มาของผู้กระทำความผิดดังกล่าว

ดังนั้น การเก็บ Log หรือ Traffic Data อย่างน้อย 90 วัน ที่มีกำหนดขีดเส้นตายสำหรับทุกองค์กรในประเทศไทย ในวันที่ 24 สิงหาคม พ.ศ. 2551 จึงมีความสำคัญอย่างยิ่งกับสภาวะการพัฒนาสังคมด้านสารสนเทศในประเทศไทยไปอีกขั้นหนึ่ง ทำให้เกิดความมั่นใจในการใช้งานระบบสารสนเทศมากขึ้นในเรื่องของปัญหาด้านความปลอดภัยข้อมูลระบบสารสนเทศ ส่งผลให้ภาพลักษณ์ของประเทศไทยโดยรวมดีขึ้น มีมาตรฐานมากขึ้นในสายตาประชาคมโลก