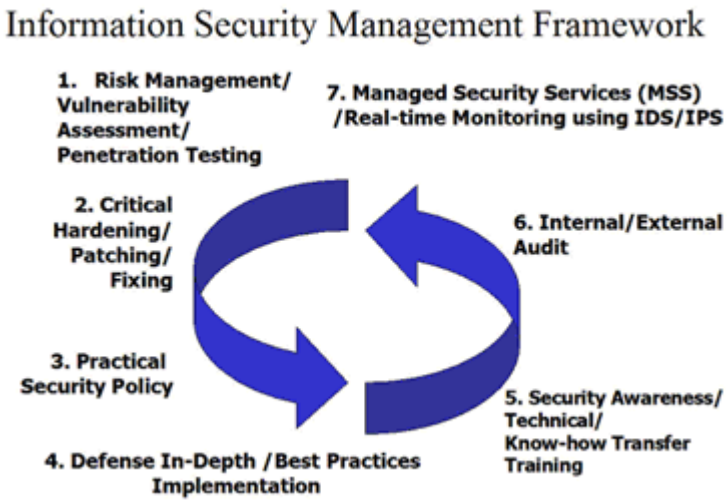
Information Security Management Framework (ISMF) ตอนที่ 1

by A.Pinya Hom-anek, GCFW, CISSP, CISA

ACIS Professional Team

E-mail: prinya@acisonline.net

จากฉบับที่แล้ว ผมได้กล่าวถึง Information Security Management Framework ทั้ง 7 Steps ไปแล้ว



(ดูรูปที่ 1)

การจัดการระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพโดยนำ ISMF มาใช้นั้น เราควรปฏิบัติจาก ขั้นตอนที่ 1 ไปจนถึง ขั้นตอนที่ 7 จากการที่เราได้ปฏิบัติตาม ISMF จนครบทั้ง 7 Steps เพื่อให้ได้ผล เราควรจะทำตาม ISMF ทุกๆ 3 เดือน หรือ ขั้นต่ำ 2 ครั้งต่อปี เพื่อเป็นหลักประกันความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ที่เราใช้งานอยู่ว่ามีความน่าเชื่อถือ และ ความมั่นคง ต่อการจู่โจมของเหล่า Hacker และ Virus Computer ที่มีอยู่มากมายในเวลานี้ และ เพื่อให้สอดคล้องกับหลักการ ICT Governance คือ การนำ ICT มาใช้ในการทำงานขององค์กรอย่างมีประสิทธิภาพและ ประสิทธิผล ทำให้เพิ่มความน่าเชื่อถือ ให้กับองค์กร ในสายของพนักงานในองค์กรเอง และ สายตาของคนภายนอกให้ลูกค้า หรือ คู่ค้า เกิดความมั่นใจในระบบการรักษาความปลอดภัยข้อมูลของเราเพราะเรามีหลักการในการปฏิบัติอย่างจริงจัง และ ถูกต้องตามมาตรฐานสากล

ISMF นั้นได้นำเอาหลักการด้าน Information Security Policy ของมาตรฐานสากล ISO17799 ตลอดจนมาตรฐาน Cobit ของ ISACA (www.isaca.org) และ CBK (Common Body of Knowledge) ของ ISC2 (www.isc2.org) มาประยุกต์ใช้ให้ได้ประโยชน์สูงสุด และสามารถนำมาปฏิบัติได้จริงในสภาวะแวดล้อม ICT

ในปัจจุบัน

เริ่มตั้งแต่ขั้นตอนที่ 1 คือ "Risk Management, Vulnerability Assessment และ Penetration testing"

ขั้นตอนที่ 1 จากทั้งหมด 7 ขั้นตอนนี้เป็นขั้นตอนแรกที่ต้องปฏิบัติและมีความ สำคัญส่งผลกระทบไปยังขั้นตอนต่อ ๆ ไป โดยรวมเราเรียกขั้นตอนนี้ว่า "การวิเคราะห์ และ ประเมินความเสี่ยงของระบบ ICT" ขั้นตอนนี้ จะรวมถึงการ วิเคราะห์ตรวจหาช่องโหว่ในระบบ ที่เรียกว่า "Vulnerability Assessment" และ การทดสอบเจาะระบบเพื่อนำเอาข้อมูลที่สำคัญ เช่น Username และ Password ออกมาจากระบบโดยการทดลอง Hack (Ethical Hacking) เสมือนว่า มี Hacker ข้ามา เจาะระบบโดยเราเรียกขั้นตอนนี้ว่า "Penetration Testing" การทำ Penetration Testing นั้น จะรวมไปถึงการทดสอบความแข็งแกร่งของระบบโดยการจำลอง Attack แบบ "DoS Attack" หรือ Denial Of Services Attack เพื่อให้ระบบใช้งานไม่ได้ (ขั้นตอนนี้ต้องทำด้วยความระมัดระวังและควรแจ้งให้ User ทราบก่อนล่วงหน้าจะได้มีการเตรียมตัวให้พร้อมกับการทดสอบ)

การทำ Penetration Testing นั้น แบ่งออกเป็น 2 ประเภทคือ Black-Box และ White-Box (ดูรูปที่ 2)

การทำ Black-Box Penetration Testing เป็นการเจาะระบบ โดยที่ผู้ที่รับจ้างเจาะระบบจะไม่ได้รับข้อมูลจากผู้ว่าจ้างนอกจากเป้าหมายที่เป็น Web Site หรือเป็น IP Address เท่านั้น ที่เหลือผู้รับจ้างต้องพยายามเจาะเข้ามาจาก Internet โดยใช้ความสามารถของผู้รับจ้างเอง

การทดสอบเจาะระบบแบบ Black-Box Penetration Testing มีข้อดี ก็คือ เราสามารถประเมินความแข็งแกร่งของระบบเราได้ จากภายนอกก็คือจากพวก Hacker ที่เจาะเข้ามาจากทาง Internet โดยตรง แต่ ข้อเสียก็คือผู้รับจ้างอาจจะไม่สามารถเจาะเข้า มาได้เพราะข้อมูลไม่เพียงพอ หรือ ความสามารถของผู้รับจ้างมีไม่มากพอที่จะเจาะเข้าสู่ระบบได้

แต่การเจาะระบบในแบบ White-box Penetration Testing นั้น จะเป็นการเจาะระบบที่ผู้รับจ้างจะต้องเข้ามาที่ Office และ On-line เข้าสู่ระบบ LAN หรือ Intranet ของผู้ว่าจ้าง เรียกว่าเป็นการเจาะจากข้างใน เพื่อเป็นการประเมินความเสี่ยงภายในองค์กร เช่น อาจจะมีผู้ใช้คอมพิวเตอร์บางคนติด Virus และ Virus สามารถแพร่กระจายใน LAN เราก็สามารถประเมินความเสียหายโดยผู้รับจ้างจะลองทดสอบ Penetrate ระบบโดยทำตัวเป็น Virus และพยายามเข้าสู่ระบบจากภายใน

ข้อดีของวิธีเจาะระบบแบบ White-Box Penetration Testing ก็คือ เราสามารถประเมินความเสี่ยงได้ใกล้เคียงกับ

สถานะ การณ์จริงมากกว่าแบบ Black-Box Penetration Testing เพราะ ผู้รับจ้างเจาะระบบ จะมีข้อมูลภายในมากกว่าแบบแรก แต่ข้อเสียก็คือ เราไม่สามารถประเมินจากภายนอกได้เหมือนแบบแรก

กล่าวโดยสรุปก็คือ เราควรทำทั้งสองแบบแล้วนำผล Summary Report จากการทำ Black-box และ White-box box Penetration Testing มาประมวลผลรวมกัน เพื่อหาแนวทางในการแก้ไขในขั้นตอนที่ 2 ของ ISMF ต่อไป ซึ่งขั้นตอนที่ 2 จะเป็นเรื่องของการปิดช่องโหว่ที่มีความสำคัญ เราเรียกว่าเป็นการทำ "Critical Hardening" ซึ่งผมจะขอกล่าวโดยละเอียดในฉบับหน้าครับ

จากฉบับที่แล้ว Information Security Management Framework (ISMF) ประกอบด้วยขั้นตอนทั้งหมด 7 ขั้นตอน โดยที่ขั้นตอนแรกที่เราต้องทำก่อนก็คือ Risk Management/Vulnerability Assessment ซึ่งเป็นการประเมินความเสี่ยงโดยรวมของระบบ รวมถึง Penetration Testing (PEN-Test) ทั้งแบบ Black-Box และ White-Box หลังจากที่เราได้ผ่านขั้นตอนการประเมินความเสี่ยงของระบบ และได้รายงานสรุปว่าระบบของเรามีช่องโหว่ที่ถูกค้นพบ (Found Vulnerabilities) จากการตรวจสอบด้วยวิธีดังกล่าว เราต้องมาประเมินว่าช่องโหว่นั้น สามารถก่อให้เกิดความเสียหายกับระบบมากน้อยเพียงใด ช่องโหว่บางอย่างอาจไม่ใช่ช่องโหว่ที่จำเป็นต้องปิดในทันที และไม่มีผลกระทบรุนแรงกับระบบเท่าใดนักหากยังไม่ได้รับการแก้ไข แต่ช่องโหว่บางอย่างก็เป็นช่องโหว่ที่ค่อนข้างที่จะส่งผลกระทบ รุนแรงกับระบบหากเราไม่รีบแก้ไข

ดังนั้นเราจึงจำเป็นต้องมีหลักเกณฑ์ในการประเมินผลจากรายงานช่องโหว่ที่เราตรวจพบ และทำการ "Prioritize" หรือจัดลำดับความสำคัญของช่องโหว่ที่เราพบว่า ช่องโหว่แบบไหนมีความจำเป็นต้องแก้ไขโดยด่วน ซึ่งปกติเราจะเรียกช่องโหว่ในลักษณะนี้ว่า "High Risk" ซึ่งก็จะต่างกับช่องโหว่แบบ "Medium Risk" หรือ "Low Risk" ที่หมายความว่ายังไม่ก่อผลกระทบรุนแรงให้กับระบบเหมือนแบบ "High Risk"

หลักเกณฑ์ในการประเมินความเสี่ยงที่ว่าช่องโหว่แบบใดที่เป็น "High Risk" ดูได้จากผลจากรายงานของ "Vulnerability Scanner" ในเบื้องต้น ซึ่ง Vulnerability Scanner ที่ใช้ควรจะใช้หลายๆ ตัวประกอบกัน ยกตัวอย่างที่นิยมใช้กันโดยทั่วไปได้แก่ Nessus (Open Source), Retina, Internet Scanner, Shadow Security Scanner เป็นต้น

ผลจากการรายงานของ Vulnerability Scanner นั้นบางทีก็เชื่อถือไม่ได้เสมอไป เราควรที่จะรวบรวมผลจากการ Scan ที่ได้จาก Scanner หลายๆ ตัว มาประมวลผลรวมกัน โดยใช้ประสบการณ์ในการทำงานด้าน Penetration Testing ประกอบกับข้อมูลเทคนิคการ "Hack" ระบบใหม่ๆ ของพวก Hacker มาช่วยประเมินว่าเราต้องจัดการแก้ปัญหากับช่องโหว่ตัวไหนก่อนเพื่อที่จะทำให้ระบบของเรายังคงมีความปลอดภัย และมีเสถียรภาพเพียง

พอที่จะต่อกรกับการโจมตีของ Hacker

วิธีการประเมินความเสี่ยงในส่วนที่เป็น "High Risk" นั้น ให้ยึดหลักของ SANS/FBI Top 20 (http://www.sans.org/top20) เป็นเกณฑ์ในการประเมินเบื้องต้น SANS/FBI Top 20 จะประกอบด้วยช่องโหว่ของ Windows Platform 10 ช่องโหว่และช่องโหว่ของ UNIX/Linux Platform อีก 10 ช่องโหว่ ที่ IT Auditor ตรวจพบอยู่เป็นประจำ ซึ่งช่องโหว่เหล่านี้ล้วนเป็นช่องโหว่ที่เหล่า Hacker ชอบใช้ในการเจาะระบบโดยทั่วไป ซึ่งช่องโหว่บางตัวนั้นก็เป็นช่องโหว่เก่าที่รู้กันมานานหลายปีแล้ว แต่ผู้ดูแลระบบก็ยังไม่ค่อยได้ระมัดระวังเท่าที่ควร

จากประสบการณ์ที่ผมได้ทำงานด้าน Risk Assessment มาพอสมควร พบว่าองค์กรต่างๆ ในประเทศไทยส่วนใหญ่จะตรวจพบช่องโหว่ที่ติดอันดับอยู่ใน SANS/FBI Top 20 ทั้งสิ้น ไม่ว่าจะเป็น Windows Platform หรือ UNIX/Linux Platform ซึ่งแสดงให้เห็นว่าช่องโหว่เหล่านี้ ยังไม่ได้รับการแก้ไขและดูแลอย่างจริงจังจากผู้ดูแลระบบ อาจเกิดจากการที่ไม่เคยประเมินความเสี่ยงของระบบเลยไม่รู้ว่าระบบนั้นมีช่องโหว่ติดอยู่ใน SANS/FBI Top 20 หรือไม่ก็อาจจะทราบว่าระบบมีช่องโหว่ แต่ระบบกำลังใช้งานจริงอยู่จึงเกิดความรู้สึกกลัวว่าเมื่อแก้ไขช่องโหว่ของระบบอาจทำให้ระบบมีปัญหาได้เป็นต้น

Information Security Management Framework (ISMF) ในขั้นตอนที่ 2 จะเน้นไปที่การปิดช่องโหว่หรือการ "Harden" ระบบ ซึ่งเราเน้นไปที่ช่องโหว่ที่เป็นแบบ "High Risk" ก่อน เพราะมีผลกระทบกับระบบมากที่สุด หากเราละเลยไม่ปิดช่องโหว่เหล่านั้น หลักการในการ "Harden" ระบบนั้นหัวใจสำคัญก็คือไม่เปิดใช้บริการที่เราไม่มีความจำเป็นต้องใช้ เช่น ถ้าเราใช้เครื่องทำเป็น Web Server อย่างเดียว เราก็ควรเปิดใช้บริการเฉพาะพอร์ต 80 (http) และพอร์ต 443 (https) เท่านั้น แต่ปัญหาก็คือ เครื่องที่เรานำมาใช้งานเป็น Web Server นั้น ยกตัวอย่างเช่น Windows Platform มีการเปิดใช้งานบริการอื่นๆ โดยเป็นค่า "Default" มาจากการติดตั้งระบบในตอนแรก เช่น จะมีการเปิดพอร์ต TCP 135 ซึ่งเป็น RPC (Remote Procedure Call) Service เป็นผลให้ติด Virus Worm Blaster หรือ Nachi เป็นต้น นอกจากนี้ ยังเปิดพอร์ต TCP139 และ TCP/IP445 เป็นค่าโดยกำหนด ซึ่งเป็นการให้บริการ "File & Print Sharing" เช่นการ Map Network Drive เป็นต้น จะเห็นว่าไม่มีความจำเป็นต้องเปิดพอร์ตดังกล่าว ถ้าเรานำเครื่องมาใช้เป็น Web Server

ดังนั้นการ "Harden" ก็คือการปิดพอร์ตที่ผมได้กล่าวมาแล้วในตอนต้น วิธีการก็มีหลายวิธีเช่น การไป "Stop Service" ที่เราไม่มีความจำเป็นต้องใช้งาน หรือใช้ TCP Filter ซึ่งเป็นความสามารถที่ Windows NT/2000/2003 Server มีมาให้เราใช้งานอยู่แล้ว เรียกได้ว่าเป็น Firewall ให้กับเครื่องแบบไม่ต้องลงทุน บางท่านอาจจะใช้โปรแกรมประเภท Personal Firewall ในการป้องกันและตรวจจับ IP Address ของผู้บุกรุก หรือพวก Virus

Worm ทั้งหลายก็จะช่วยได้อีกระดับหนึ่ง

การ "Harden" ที่ได้กล่าวมาแล้วเป็นการทำที่ตัว Host หรือ Server ที่เราใช้งานอยู่โดยตรง ไม่ได้เป็นการไปปิดพอร์ตหรือบริการต่างๆ ที่ Border Firewall หรือ Border Router ของระบบ ซึ่งการที่เราทำการปิดพอร์ตที่ตัวเครื่องโดยตรงจะทำให้เครื่องมีความปลอดภัยมากกว่าการปิดเฉพาะที่ Firewall หรือ Router ลักษณะการปิดพอร์ตเฉพาะที่ตัว Host หรือ Server เราเรียกว่า การทำเครื่องให้เป็น "Bastion Host" ที่มีความปลอดภัยสูงถึงแม้ Hacker จะเจาะผ่าน Firewall มาได้ก็ยังมาติดที่ตัวเครื่องอยู่ดี การใช้งาน Border Firewall หรือ Border Router ACL (Access Control List) ในการปิดช่องโหว่นั้นก็เป็นสิ่งจำเป็นที่ยังต้องทำอยู่ เพราะจะเป็นการผ่อนหนักให้เป็นเบา โดยการ Harden เสริมที่ตัวเครื่อง จะทำให้เกิดความปลอดภัยมากขึ้น

สำหรับการ "Patch" หรือการลง "Hotfix" ให้กับระบบนั้น ก็เป็นสิ่งจำเป็นที่ต้องทำนอกเหนือจากการปิดบริการหรือพอร์ตที่เราไม่ได้ใช้งานเช่นกัน เพราะบริการที่เราใช้อยู่เช่น พอร์ต 80 ที่เปิดบริการ Web Server นั้นอาจจะมีช่องโหว่ที่ตัว Web Server เอง และเราก็จำเป็นต้องเปิดใช้บริการ ดังนั้น เราจึงต้องมีการติดตามลง "Patch" หรือโปรแกรมแก้ไขช่องโหว่ที่เกิดขึ้นในระบบ ซึ่งช่องโหว่ของระบบโดยทั่วไปจะเกิดขึ้นทุกเดือน (ดูข้อมูลได้ที่ www.cert.org หรือ www.securityfocus.com) เราจึงต้องคอยติดตามข่าวช่องโหว่ใหม่ๆ และเข้าไป Download "Patch", "Service Pack" หรือ "Hotfix" มาลงในเครื่องของเราให้ปลอดจากช่องโหว่ที่มีการค้นพบกันทุกเดือน ยกตัวอย่างถ้าใช้ Windows Platform อยู่ ให้ไปดูที่ www.microsoft.com/security เป็นต้น

จะเห็นได้ว่าการ Harden ระบบนั้น ไม่ใช่ทำเสร็จแล้วจะจบเลย การ Harden ครั้งแรกจนระบบปลอดจากช่องโหว่นั้นเราเรียกว่า "**Get Secure**" แต่ปัญหาก็คือ เราจะทำอย่างไรให้ "**Stay Secure**" นั่นคือ เราต้องคอยติดตามข่าวสารช่องโหว่ใหม่ๆ รายเดือน บางทีอาจเป็นรายสัปดาห์หรือรายวันก็มี และเราต้องคอยลง Patch, Horfix ตลอดจน Service Pack ต่างๆ ที่จะออกมาเป็นระยะๆ เพื่อให้ระบบของเรามีความปลอดภัยอยู่เสมอ

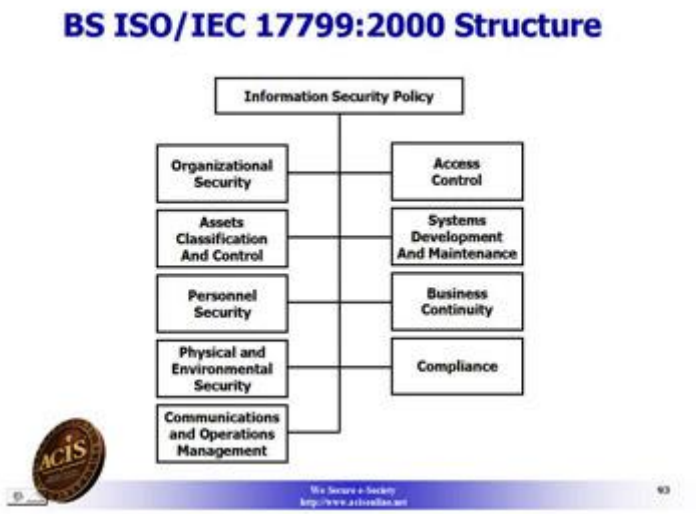
ในฉบับหน้า ผมจะกล่าวถึง Information Security Management Framework (ISMF) ในขั้นตอนที่ 3 ได้แก่ "Practical Information Security Policy" อย่าลืมตืดตามนะครับ

หลังจากที่เราได้ปฏิบัติตาม ISMF (ดูรูปที่ 1) ในขั้นตอนที่ 1 และ 2 คือ Risk Management / Vulnerability Assessment / Penetration Testing และ Critical Hardening/Patching/Fixing แล้ว (อ่านย้อนหลังได้ใน eLeader 2 ฉบับก่อนหน้านี้ หรือใน Web Site: www.acisonline.net) เราจะเข้าสู่ขั้นตอนที่ 3 คือ "**Practical Information Security Policy**" ซึ่งเป็นขั้นตอนที่มีความสำคัญกับองค์กรอย่างมากในการจัดการกับระบบรักษา ความปลอดภัยข้อมูลคอมพิวเตอร์อย่างได้ประสิทธิผลในการปฏิบัติจริง เพราะหากองค์กรไม่มีการกำหนด "**นโยบายการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตอย่างปลอดภัย**" ก็จะทำให้ระบบยังคงมีปัญหาได้

อาทิ ระบบติดไวรัส, แฮกเกอร์ใช้ Trojan Horse เจาะเข้าระบบจากความผิดพลาดของผู้ใช้งาน (User) ที่โดนแฮกเกอร์ใช้เทคนิค "Social Engineering" เจาะเข้ามา เป็นต้น ไม่ว่าเราจะติดตั้ง Firewall, IDS ตลอดจน Anti Virus Software อย่างเต็มระบบแค่ไหน ก็เป็นเพียงการป้องกันในระดับเทคนิค (Technical Level) เท่านั้น (ดูรูปที่ 2) เรายังขาดการป้องกันในระดับบริหารจัดการ (Administrative Level) ซึ่งหมายถึงเรื่อง Policy , Standard, Guideline และ Procedure ที่ต้องถูกนำมาใช้เป็นนโยบายใน การปฏิบัติของผู้ใช้ IT ในองค์กร

(ดูรูปที่ 2)

โดยปกติแล้วองค์กรมักจะนิยมเขียนนโยบายด้านความปลอดภัยข้อมูลคอมพิวเตอร์ โดยอิงจากมาตรฐาน BS ISO/IEC 17799:2000 (ดูรูปที่ 3) ซึ่งประกอบไปด้วยหัวข้อต่างๆ 10 เรื่อง โดยเน้นในรูปของภาพรวมไม่เจาะลึกด้านปฏิบัติ



(ดูรูปที่ 3)

ดังนั้นในบางองค์กรเช่น ธนาคารหรือสถาบันการเงิน อาจนำหลักการด้านนโยบายจากหน่วยงานอื่นที่ไม่ใช่ ISO มาเป็นต้นแบบก็ได้ เช่น มาตรฐาน CobiT (Control Objectives for Information and Related Technology) Framework ของ สถาบัน IT Governance Institute (www.itgi.org) ซึ่งเน้นในการตรวจสอบโดยผู้ตรวจสอบด้าน Information System โดยตรงคือ CISA (Certified Information System Auditor) ที่ได้รับการรับรองจากสถาบัน ISACA (www.isaca.org) ซึ่งเป็นผู้ที่ช่วยกำหนดมาตฐานในการตรวจสอบ (Audit) ระบบ Information System ตามขั้นตอนและอ้างอิงมาตรฐาน CobiT

นอกจาก BS ISO/IEC 17799:2000 และ CobiT แล้วก็ยังมีแนวทางการกำหนดนโยบาย ด้านการรักษาความปลอดภัยระบบ คอมพิวเตอร์อีกจาก 2 หน่วยงานที่มีบทบาทสำคัญ และเน้นการนำไปใช้งานจริง กล่าวคือ เป็น Information Security Policy ที่ได้รับการขัดเกลาและประยุกต์แล้ว ได้แก่ CBK (Common Body of Knowledge) ดูรูปที่ 4 จาก ISC2.org และ SANS/FBI Top 20 ของ SANS Institute ซึ่งร่วมมือกับ FBI (รายละเอียดเพิ่มเติมที่ www.sans.org/top20)

(ดูรูปที่ 4)

CBK นั้น เป็นองค์ความรู้ที่ สำคัญ และ จำเป็น ในการกำหนดนโยบายด้านความปลอดภัยระบบข้อมูลคอมพิวเตอร์ คิดค้นขึ้นโดยสถาบัน (ISC)2 (www.isc2.org) ผู้ที่ต้องการศึกษาอย่างลึกซึ้ง ควรลองเข้าไปสอบ CISSP (Certified Information Systems Security Professional) ซึ่งเป็นใบรับรอง (Certificate) ที่จะทำให้เรามีความเข้าใจลึกซึ้งใน CBK ทั้ง 10 โดเมน มากขึ้นและสามารถนำมาใช้ในภาคปฏิบัติกับองค์กรของเราได้อย่างดี

ส่วน SANS/FBI Top 20 Vulnerabilities นั้นเหมาะสำหรับผู้ดูแลระบบหรือ System Administrator ที่จะนำไปใช้กับ Platform ที่ตนเองดูแลอยู่ ได้แก่ UNIX Platform Top 10 Vulnerabilities และ Windows Platform Top 10 Vulnerabilities

ความหมายของ Policy หมายถึง นโยบายในภาพรวมที่กระชับและได้ใจความ เรียกว่า "Goal" หรือ เป้าหมายที่เราต้องการบรรลุ , Standard หมายถึง มาตรฐานที่ต้องบังคับในการปฏิบัติจริง เช่น รหัสผ่านต้องมีความยาวไม่ต่ำกว่า 8 ตัวอักษร เป็นต้น , Guideline หมายถึง แนวทางในการปฏิบัติที่ไม่ได้บังคับ แต่แนะนำเพื่อให้ผู้ปฏิบัติให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น และ Procedure หมายถึง รายละเอียดปลีกย่อยเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่ง Standard ที่ได้วางไว้ (ดูรูปที่ 5)

(ดูรูปที่ 5)

การกำหนดรายละเอียดของนโยบายด้านการรักษาความปลอดภัยระบบข้อมูลคอมพิวเตอร์ จึงต้องประกอบไปด้วย 4 ส่วนหลักๆ นี้ใน การพัฒนารายละเอียดต่างๆ ในนโยบาย ซึ่งนโยบายของแต่ละองค์กรอาจจะไม่เหมือนกัน ขึ้นกับการทำงานด้าน Information System ขององค์กรนั้นๆ อาทิ พฤติกรรมของผู้ใช้งาน, ทิศทางของผู้บริหารระดับสูงด้าน Information System หรือ Platform ที่เลือกใช้ อาจต้องมีการกำหนด "Best Practices" ให้กับ Platform ที่เราใช้อยู่โยเฉพาะ เช่นเราใช้ "Apache" เป็น Web Server อยู่เราก็ใช้ "Best Practices" สำหรับ Web Server Apache โดยเฉพาะ ซึ่งก็จะมีรายละเอียดและข้อกำหนดต่างๆ ที่เราสามารถนำไปจัดการใช้กับ Web Server ได้ในทางปฏิบัติ

จะเห็นได้ว่า เราไม่สามารถนำ Information Security Policy จากสถาบันต่างๆ ดังได้กล่าวมาแล้วทั้ง 4 สถาบันมาใช้งานได้ทันที เนื่องจาก เราต้องมีการประเมินสถานการณ์ความเสี่ยงขององค์กรเราเสียก่อน ซึ่งก็คือ

ขั้นตอนที่ 1 ของ ISMF (Risk Management / Vulnerability Assessment / Penetration Testing) นั่นเอง **หากปราศจากขั้นตอนนี้ แล้วเรามาทำนโยบายก่อน จะทำให้เราขาดข้อมูลประกอบการตัดสินใจในการกำหนดนโยบายให้ใช้งานได้จริง เพราะฉะนั้น การกำหนดนโยบายต้องทำภายหลังจากการประเมินความเสี่ยงแล้ว**

ปัญหาใหญ่ๆ อีกอย่างหนึ่งสำหรับองค์กรที่มีนโยบายที่ดีและได้ลงทุนลงแรงไปมากกับการพัฒนานโยบายความปลอดภัยข้อมูล คอมพิวเตอร์ หน่วยงานบางแห่งใช้เวลามากกว่า 2 ปีในการทำงานนโยบาย แต่กลับพบว่าเมื่อได้คลอดนโยบายออกมาเป็นรูปธรรม เพื่อให้คน IT ในองค์กรได้ปฏิบัติ แล้ว ผลลัพธ์ออกมาไม่เป็นอย่างที่คาดหวังไว้ เพราะหลายๆ คนไม่ยอมทำตามนโยบาย บางคนอ่านแล้วไม่เข้าใจ บอกว่าศัพท์เทคนิคมากเกินไป บางคนบอกว่าไม่ตรงกับงานที่รับผิดชอบอยู่นำมาใช้งานจริงไม่ได้ เป็นต้น ทางแก้ปัญหาที่ถูกต้องคือ ต้องมีการทำ Security Awareness Training ให้กับผู้ใช้ IT เสียก่อน ตั้งแต่ระดับผู้บริหารกระทั่งถึง ระดับผู้ใช้ทั่วไป เพื่อให้มีความตระหนักถึงภัยจากการใช้งานอินเทอร์เน็ตอย่างไม่ระมัดระวังและไม่ถูกต้อง (ซึ่งผมจะกล่าวถึงใน ISMF ขั้นตอนที่ 5 ต่อไปในรายละเอียด) ในฉบับหน้าเราจะมาดูรายละเอียดของ ISMF ในขั้นตอนที่ 4 คือ "Defense In-Depth / Best Practices Implementation" ว่ามีรายละเอียดอย่างไรบ้าง อย่าลืมติดตามนะครับ สวัสดีครับ

การจัดการกับระบบรักษาความปลอดภัยข้อมูลอย่างเป็นระบบและมีประสิทธิภาพด้วย ISMF นั้น ประกอบไปด้วยขั้นตอนทั้ง 7 ขั้นตอน ซึ่งเราปฏิบัติตามขั้นตอนต่าง ๆ ทีละขั้น เริ่มจาก ขั้นตอนที่ 1 คือการตรวจสอบช่องโหว่และประเมินความเสี่ยงให้กับระบบของเราเอง (Risk Management / Vulnerability Assessment) จากนั้นให้ดำเนินการปิดช่องโหว่ที่มีผลกระทบกับระบบในขั้นตอนที่ 2 (Critical Hardening) และกำหนดนโยบายด้านการรักษาความปลอดภัยข้อมูลในเชิงปฏิบัติเพื่อแก้ไขปัญหาในระยะยาวในขั้นตอนที่3 (Practical Security Policy)

สำหรับขั้นตอนที่ 4 ได้แก่ "Defense-In-Depth" และ "Best Practices Implementation" เป็นขั้นตอนที่ใช้เวลานานและมีผลกับองค์กรในระยะยาว ดังนั้น ขั้นตอนนี้จึงเป็นขั้นตอนที่ค่อนข้างละเอียดและต้องการกำลังคนและเวลาในการปฏิบัติ ตลอดจนความรู้เชิงลึกในด้าน Information Security เพื่อทำให้ระบบขององค์กรมีความปลอดภัยทั้งในปัจจุบันและอนาคต เรียกได้ว่าเป็นการจัดการ Information Security แบบบูรณาการ

คำว่า 'Defense-In-Depth" นั้นเน้นการจัดการแบบ "Layered Security" คือมีการป้องกันระบบเป็นชั้น ๆ เปรียบเสมือนมีประตูหลายชั้นก่อนจะเข้าถึงตัวระบบได้ และมีการแบ่งระบบออกเป็นหลายส่วน ในทางเทคนิคเราเรียกว่า "Compartmentalization" เช่น การทำ VLAN แยกระบบที่สำคัญออกจากกัน หรือการแบ่ง

DMZ (Demilitarized Zone) ออกเป็นหลาย ๆ DMZ เช่น Web Sever ไม่ควรอยู่กับ Mail Server ใน DMZ เดียวกัน หรือ Primary DNS ไม่ควรอยู่กับ Secondary DNS ใน DMZ เดียวกันเป็นต้น เพื่อที่จะป้องกันในกรณีที่ Hacker เจาะ Server หรือ Host ใด Host หนึ่งใน DMZ สำเร็จ Hacker ก็จะเจาะ Host ที่อยู่ในบริเวณ DMZ เดียวกันได้ง่าย แต่ถ้าเราแบ่งระบบออกเป็น "หลายชั้น/หลายส่วน" Hacker ก็ต้องใช้ความพยายามมากขึ้นที่จะ "Compromised" หรือ "Hacked" ระบบของเราทั้งหมด

หัวข้อสำคัญที่เราต้องพิจารณาเวลานำยุทธศาสตร์ Defense-In-Depth" มาใช้ประกอบไปด้วย 5 หัวข้อดังนี้

1. "**Re-Design Network Perimeter Architectures" / "ออกแบบระบบป้องกันอย่างรัดกุมและให้ความปลอดภัยสูงสุด**"

   หมายถึง ในกรณีที่มีการใช้สถาปัตยกรรมป้องกันระบบ (Network Perimeter Architecture) แบบเดิมอยู่แล้วให้พิจารณาอย่างละเอียดว่า มีการออกแบบที่ได้ความปลอดภัยสูงสุดแล้วหรือยัง เช่น ภายใน DMZ เดียวกันมีทั้ง Web Server, Applications Server และ Database Server แม้จะอยู่หลัง Firewall ถ้า Hacker เจาะ Web Server ได้ก็มีโอกาสที่จะเจาะ Applications Server และ Database Server ได้อย่างไม่ยากนัก ดังนั้นเราควรแยกออกเป็น 3 ส่วนคือ แยก Applications Server ออกจาก Zone ของ Web Server และแยก Database Server ไปอยู่ใน Zone เฉพาะของ Database Server เท่านั้น เพราะข้อมูลที่อยู่ใน Database Server นั้น ถือเป็นข้อมูลที่มีผลกระทบกับองค์กรอย่างมาก และมีความสำคัญกว่าข้อมูลที่อยู่ใน Web Server หาก Hacker เจาะ Web Server ได้ ข้อมูลใน Database Server ก็ยังไม่มีผลกระทบในทันที Hacker จะต้องใช้ความพยายามในการเจาะผ่านเข้าสู่ DMZ ของ Database Server อีกทีหนึ่งเป็นต้น

   จะเห็นว่าสถาปัตยกรรมที่ใช้หลักการ "Defense-In-Depth" นั้นจะต้องใช้งบประมาณในการติดตั้งและออกแบบระบบค่อนข้างสูงกว่าสถาปัตยกรรมแบบปกติ แต่ก็ให้ผลลัพธ์ที่น่าพอใจในมุมมองของความปลอดภัยข้อมูล

2. "**In-Depth Host and Network Devices Hardening"/"ปรับแต่ง Host และ Network Devices ให้มีช่องโหว่น้อยที่สุดเท่าที่จะทำได้**"

   หมายถึง การป้องกันที่ Firewall อย่างเดียวคงไม่เพียงพอ การป้องกันที่ดีที่สุดคือทำในระดับ Host หรือ Network Devices โดยตรงเลย การปิดช่องโหว่ตลอดจน การลง Patch/Hot Fix ให้กับ Host หรือ

Network Devices นั้น **เป็นเรื่องจำเป็นที่ต้องทำอย่างต่อเนื่องและทำ อย่างเป็นระบบ** เพราะช่องโหว่ (Vulnerability) ของระบบนั้น มีให้เห็นในอินเทอร์เน็ตเป็นประจำทุกเดือน

3. "**Change Management/Log Monitoring" / "การจัดการกับความเปลี่ยนแปลง**"

"Change Management" นั้นถือเป็นเรื่องสำคัญที่อยู่ใน ISMF ขั้นตอนที่ 4 เพราะถ้ามีการเปลี่ยนแปลงเกิดขึ้นในระบบ เราก็ควรที่จะบันทึก Event ลง Audit Trail (Audit Log) เพื่อสามารถนำมาตรวจสอบหรือ ทำ "Forensics" ในภายหลังได้ ปัญหาที่เราพบเป็นประจำก็คือ เราไม่ค่อยได้บันทึกความเปลี่ยนแปลงที่เกิดขึ้นในระบบทำให้เราไม่สามารถที่จะตรวจสอบหรือ "Audit" ระบบได้อย่างมีประสิทธิภาพ ดังนั้น "Change Management" เป็นเรื่องที่ไม่สามารถที่จะมองข้ามได้เลย

การใช้ Software จัดการกับ "Integrity" ของระบบ เช่น TripWire ว่านับเป็นความคิดที่ดีในการทำ "Change Management" ตลอดจนการใช้ Software ประเภท "Application Firewall" เช่น URLScan/IISLockDown ของ Microsoft หรือ SecureIIS ของ Eeye ก็เป็นวิธีที่สามารถป้องกันระบบในเชิงลึกได้ดีเช่นกัน การติดตั้ง IDS (Intrusion Detection Systems) และ การจัดการกับ Log อย่างเป็นระบบ (Centralized Logging Systems) ก็เป็นสิ่งที่แนะนำให้ทำให้หัวข้อนี้เช่นกัน

4. "**Securing your Database and Web Application"/"จัดการระบบความปลอดภัยใน Web Application และ Database Server ในเชิงลึก**"

หมายถึง หากเราเขียน Source Code เช่น ASP หรือ PHP ของ Web Application โดยไม่ระมัดระวัง เรามีโอกาสที่จะถูก Hacker เจาะระบบผ่านทาง Port 80 หรือ Web Application Security Hacking โดย Firewall และ IDS ไม่สามารถที่จะป้องกันได้เลย

การใช้ SSL กับ Web Server นั้นก็ไม่สามารถที่จะป้องกัน Hacker ได้ 100% Hacker ที่ใช้วิธี Hack แบบ "Man-In-The Middle Attack" สามารถ Hijack SSL Session ของเราได้ ดังนั้นวิธีการป้องกันที่ดีที่สุดก็คือ ต้องให้ Web Programmers มี "Awareness" เรื่องความปลอดภัยของ Web Application เสียก่อน เช่น สอนให้รู้เรื่อง Session ID Hacking, Cookies Hijacking, SSL Hackings SQL injection, Cross-Site Scripting ตลอดจนช่องโหว่ต่าง ๆ ทั้ง 10 ข้อของ Web Application จาก OWASP www.owasp.org (Open Web Application Security Project) สำหรับ Database Server ไม่ว่าเราจะใช้ Oracle, IBM DB2, Microsoft SQL Server หรือ Open Source MySQL เราก็ต้องคำนึงถึงช่องโหว่ (Vulnerability) และค่าโดยกำหนด (Default Parameter) ต่าง ๆ ที่มากับตัว Database ที่ทำให้เกิดช่อง

โหว่ เราควรทำ "Presentation Testing" จาก ISMF ในขั้นตอนที่หนึ่ง และดำเนินการปิดช่องโหว่ในขั้นตอนนี้โดยละเอียด

5. **"Thinking on Business Continuity Planning/Disaster Recovery Planning"/ "แผนกู้ระบบฉุกเฉินและแผนการจัดการกับความเสียหายของระบบสารสนเทศโดยไม่ให้กระทบกับธุรกิจ"**
หมายถึง เราต้องคำนึงในความจริงว่าไม่มีระบบใดที่ปลอดภัย 100% สักวันหนึ่งระบบของเราก็อาจจะถูก Hack และเกิดความเสียหายให้กับธุรกิจ ดังนั้น เราควรเตรียมแผนสำรองฉุกเฉินและดำเนินการกู้ระบบให้เร็วที่สุด (Minimized Downtime) เพื่อให้ผลเสียจากการถูก Hacker มา Compromised (Hacked) ระบบ มีผลกระทบน้อยที่สุดกับธุรกิจ DRP (Disaster Recovery Planning) นั้นเป็นแผนกู้ระบบฉุกเฉินขณะที่ BCP เป็นแผนใหญ่ที่ใช้ในการจัดการกับความปลอดภัยของระบบในระยะยาว เพื่อทำให้ระบบมี Availability ได้ตาม SLA (Services Level Agreement) ที่ฝ่าย IT ต้องทำให้ผู้ใช้คอมพิวเตอร์ตลอดจนผู้บริหารมีความพอใจในระดับหนึ่ง และ ทำให้องค์กรนำ IT มาใช้งานได้อย่างมีประสิทธิภาพ

ส่วนของ "Best Practices" นั้นเป็นส่วนหนึ่งของหลักการ "IT Governance Implementation" กล่าวคือ "Best Practices" นั้น หมายถึง การนำเอาสูตรสำเร็จ หรือ ตัวอย่างการ Implement ที่ดีมาจัดการกับระบบของเรา เช่น ถ้าเราใช้ Microsoft IIS 5.0 เป็น Web Server อยู่ เราก็ควรนำ "IIS 5.0 Best Practices" มาใช้เป็นหลักการในการติดตั้งและตรวจสอบ Web Server ของเรา ซึ่ง "Best Practices" จะประกอบไปด้วยรายละเอียดทางด้านเทคนิคของ Microsoft IIS 5.0 ที่เราควรนำมาปฏิบัติ ตั้งแต่การติดตั้งไปจนถึงการใช้งานรายวันว่าเราควรพิจารณาปิดช่องโหว่ในส่วนใดบ้าง เช่น การจัดการกับค่าโดยกำหนด (Default) ต่างๆ และ การลบไฟล์ตัวอย่าง (Examples Files) ที่ไม่จำเป็นต้องใช้งาน เป็นต้น

จาก ISMP ขั้นตอนที่ 4 "Defense In-Depth/Best Practices Implementation" ในส่วนของ "Best Practices" นั้นเป็นส่วนหนึ่งของหลักการ "IT Governance Implementation" กล่าวคือ "Best Practices" นั้น หมายถึง การนำเอาสูตรสำเร็จ หรือ ตัวอย่างการ Implement ที่ดีมาจัดการกับระบบของเรา เช่น ถ้าเราใช้ Microsoft IIS 5.0 เป็น Web Server อยู่ เราก็ควรนำ "IIS 5.0 Best Practices" มาใช้เป็นหลักการในการติดตั้งและตรวจสอบ Web Server ของเรา ซึ่ง "Best Practices" จะประกอบไปด้วยรายละเอียดทางด้านเทคนิคของ Microsoft IIS 5.0 ที่เราควรนำมาปฏิบัติ ตั้งแต่การติดตั้งไปจนถึงการใช้งานรายวันว่าเราควรพิจารณาปิดช่องโหว่ในส่วนใดบ้าง เช่น การจัดการกับค่าโดยกำหนด (Default) ต่างๆ และ การลบไฟล์ตัวอย่าง (Examples Files) ที่ไม่จำเป็นต้องใช้งาน เป็นต้น

หลังจากที่เราได้ทำตามขั้นตอนที่ 4 แล้ว ในขั้นตอนที่ 5 นั้น กล่าวถึง การฝึกอบรมความรู้ความเข้าใจด้านการ

รักษาความปลอดภัยข้อมูลให้กับ ผู้บริหารตลอดจนพนักงานให้มีความเข้าใจและมีความตระหนักให้ระวังภัยจากการใช้งานคอมพิวเตอร์โดยเฉพาะอินเทอร์เน็ตโดยไม่ระมัดระวังเพียงพอ ซึ่งอาจก่อให้เกิดความเสียหายกับองค์กรได้โดยไม่รู้ตัว

ขั้นตอนนี้เป็นขั้นตอนที่หลายๆคนมองข้าม และมองว่าควรจะมีการฝึกอบรมเฉพาะฝ่าย IT และฝ่าย Security แต่ในความเป็นจริงแล้ว ผู้บริหารระดับสูง และ ระดับกลาง ตลอดจนพนักงานที่ใช้งานคอมพิวเตอร์ในองค์กรก็มีความจำเป็นที่จะต้องถูกฝึกอบรม "Security Awareness Training" ด้วยเช่นกัน เพราะการแก้ปัญหาด้านความปลอดภัยเครือข่าย โดยเฉพาะปัญหา "Virus Computer" ซึ่งนับวันจะทวีความรุนแรงมากขึ้นเรื่อยๆ เช่น อาจมีพนักงานบางคนหมุนโทรศัพท์โดยใช้ Local Modem ที่อยู่ในเครื่อง Notebook ต่อเข้าอินเตอร์เน็ต ขณะที่ตนเองใช้ระบบ LAN ของบริษัทอยู่ ทำให้ Virus สามารถแพร่เข้าสู่ระบบ Internal LAN ของบริษัทได้อย่างง่ายดาย หรือ ผู้บริหารอาจใช้ Notebook ที่บ้านและติด Virus มาจากการเล่นอินเตอร์เน็ต จากนั้นก็นำ Notebook ดังกล่าวมาใช้ในระบบ Internal LAN ขององค์กรก็เท่ากับว่า ผู้บริหารท่านนั้นนำ Virus มาแพร่ภายในองค์กรโดยไม่รู้ตัว เป็นต้น

ดังนั้น วิธีการที่จะทำให้ระบบมีความปลอดภัยจาก Virus ดังกล่าว นอกจากการติดตั้งโปรแกรมประเภท Anti-virus แล้วก็คือ การฝึกอบรมให้ผู้บริหารและพนักงานที่ใช้คอมพิวเตอร์ในการทำงานเป็นประจำทุกวันรู้เท่าทันถึงภัยจากการใช้งานอินเตอร์เน็ตและเครือข่ายโดยไม่ระมัดระวัง วิธีการก็คือ การฝึกอบรมต้องมีการแสดงกรณีตัวอย่าง หรือ Case Study ให้ผู้เข้ารับการอบรมเห็นว่า Hacker และ Virus มีวิธีการในการโจมตีเราได้อย่างไร เมื่อทุกคนได้เห็นตัวอย่างแล้วก็จะเกิดความตระหนักได้ด้วยตนเองว่า จากนี้ต้องใช้งานเครือข่ายและอินเทอร์เน็ตด้วยความระมัดระวังมากขึ้นโดยไม่ต้องมีฝ่าย IT คอยบังคับหรือคอยบอกโดยไม่เข้าใจว่าทำไมต้องทำตามคำแนะนำของฝ่าย IT เช่น เมื่อฝ่าย IT แนะนำให้ใช้ Personal Firewall ส่วนใหญ่แล้วผู้ใช้คอมพิวเตอร์ทั่วไปก็มักจะรำคาญหรือไม่เข้าใจประโยชน์จากการติดตั้ง Personal Firewall ในเครื่องของตนเอง บางคนขอให้ฝ่าย IT ช่วยเอาโปรแกรม Personal Firewall ออกจากเครื่องก็มี

จะเห็นว่า "Security Awareness Training" เป็นเครื่องสำคัญที่ถูกมองข้ามและถูกเข้าใจผิดว่าเป็นเรื่องที่ทำเฉพาะฝ่าย IT เท่านั้น แต่ในความเป็นจริงต้องมีการฝึกอบรมเป็นประจำทุกปี และควรฝึกอบรมให้ครบ 6 กลุ่มดังนี้

<u>กลุ่มที่ 1</u> ผู้บริหารระดับสูง (Top Management)
<u>กลุ่มที่ 2</u> ผู้บริหารระดับกลาง (Middle Management)

การฝึกอบรม "Security Awareness Training" ให้กับผู้บริหารระดับสูงนั้นควรจะเป็นเรื่องความเสี่ยงที่มีอยู่ในอินเทอร์เน็ตทุกวันนี้ (Information Security Risk), โอกาสที่จะเกิดความเสียหายขึ้นจากการจู่โจมของ Hacker หรือ Virus Computer, ความจำเป็นที่ระบบต้องมีการควบคุมด้วย "Control" เช่น การติดตั้ง Enterprise Firewall และ Intrusion Detection System ตลอดจนการติดตั้ง Personal Firewall และ Anti-Virus ในทุก workstation การฝึกอบรมควรใช้ระยะเวลาสั้นๆ ไม่เกิน 3 ชั่วโมงและไม่ควรใช้ศัพท์เทคนิคมากเกินไป

ผลที่ได้จากการฝึกอบรมผู้บริหารจะทำให้ผู้บริหารมีความเข้าใจเรื่อง Information Security มากขึ้น และมีผลอย่างมากกับองค์กร เนื่องจากผู้บริหารจะให้ความสนับสนุนฝ่าย IT มากยิ่งขึ้น หลังจากที่ได้ทำความเข้าใจกับปัญหาทางด้านความปลอดภัยคอมพิวเตอร์หลังจากการฝึกอบรมแล้ว

กลุ่มที่ 3 กลุ่มผู้ดูแลระบบ (System Administrators)
กลุ่มที่ 4 กลุ่มผู้ดูแลความปลอดภัยคอมพิวเตอร์โดยตรง (Security Administrators)
กลุ่มที่ 5 กลุ่มผู้ตรวจสอบระบบสารสนเทศ (IT Auditors)

การฝึกอบรมทั้ง 3 กลุ่มนี้ควรเน้นเนื้อหาทางด้านเทคนิคเพิ่มขึ้นจากการฝึกอบรมผู้บริหาร และควรมีกรณีศึกษา (Security Incident case study) ของระบบต่างๆ และ แสดงให้เห็นถึงวิธีการโจมตีของ Hacker และ Virus ตลอดจน วิธีการป้องกันที่ถูกต้องและมีประสิทธิภาพ โดยอาจมีรายละเอียดและระยะเวลาในแต่ละกลุ่มแตกต่างกัน ตั้งแต่ 6 ชั่วโมง จนถึง 30 ชั่วโมง ในกรณีที่ต้องการให้มีความเข้าใจมากขึ้น ควรมี "Hand-on" ให้ผู้เข้าอบรมได้ใช้คอมพิวเตอร์ฝึกปฏิบัติในห้องเรียนด้วย (ซึ่งการอบรมในกลุ่มที่ 1 และ 2 ไม่จำเป็นต้องให้ผู้เข้าอบรมใช้คอมพิวเตอร์ก็ได้)

กลุ่มที่ 6 กลุ่มผู้ใช้งานคอมพิวเตอร์ทั่วไป (Users)

กลุ่มนี้เป็นกลุ่มที่มีความเสี่ยงสูงที่จะปล่อย Virus เข้าสู่ระบบโดยไม่รู้ตัว พอๆ กับกลุ่มที่ 1 และ 2 เนื่องจากไม่มีความรู้พื้นฐานทางเทคนิคเพียงพอ ดังนั้น การฝึกอบรมต้องแสดงให้เห็นถึงการใช้งานคอมพิวเตอร์รายวันที่ผู้ใช้ต้องใช้คอมพิวเตอร์ในการทำงานของตนเองเป็นประจำอยู่แล้ว เช่น การเข้าไปหาข้อมูลใน Web site และการรับ-ส่ง e-Mail การฝึกอบรมควรจะแสดงให้เห็นถึงภัยต่าง ๆ จากการเข้า Web site ที่ไม่เหมาะสม หรือ การถูกโปรแกรม SpyWare ประเภท Key Logger มาฝังในเครื่องโดยผ่านทาง Attached file ที่มากับ e-Mail การใช้งานอินเทอร์เน็ตโดยไม่มี Personal Firewall ก็เป็นอีกปัญหาหนึ่งของผู้ใช้งานโดยทั่วไปที่ต้องเน้นในการฝึกอบรมเช่นกัน

หลังจากการฝึกอบรม "Security Awareness Training" และการฝึกอบรม "Technical Know-how Transfer Training" ในเชิงลึกด้านเทคนิคแล้ว จะทำให้ทั้ง 6 กลุ่มซึ่งก็คือพนักงานทุกคนในองค์กร มีความเข้าใจเรื่องภัยจากอินเทอร์เน็ตรวมทั้งวิธีการป้องกันตนเองและองค์กรให้พ้นภัยจากเหล่า Hacker และ Virus ได้ดียิ่งขึ้น ส่งผลให้ระบบมีความปลอดภัยและมีเสถียรภาพเพิ่มมากขึ้น ฝ่าย IT ก็ทำงานง่ายขึ้นด้วย เพราะฉะนั้น โปรแกรมนี้ควรถูกบรรจุเข้าไว้ใน IT Master Plan ขององค์กรและควรเตรียมงบประมาณไว้ให้เพียงพอสำหรับค่าใช้จ่ายด้านการฝึกอบรมในแต่ละปีด้วย เพื่อที่องค์กรของเราจะได้ลดปัญหาทางด้านความปลอดภัยคอมพิวเตอร์ลงไม่ให้มีผลกระทบรุนแรงอย่างเช่นในทุกวันนี้

จาก ISMF ขั้นตอนที่ 5 เกี่ยวกับการฝึกอบรมพัมนาบุคลากรให้มีความเกี่ยวกับการรักษาความปลอดภัยระบบเครือข่ายและระบบคอมพิวเตอร์ตามมาตรฐานสากลแล้ว ในขั้นตอนที่ 6 จะเน้นเรื่องการ "ตรวจสอบ" หรือ "IT Auditing" ซึ่งเป็นส่วนหนึ่งของแนวคิด "IT Governance" ที่องค์กรสมัยใหม่นิยมนำมาประยุกต์ใช้ หลังจากที่เราได้ทำการประเมินความเสี่ยงของระบบและปิดช่องโหว่ของระบบแล้ว เราจะทราบได้อย่างไรว่าช่องโหว่ที่มีผลกระทบกับระบบได้ถูกจัดการแก้ไขอย่างถูกต้อง ดังนั้น เราจึงต้องทำการตรวจสอบซ้ำเป็นครั้งที่ 2 การตรวจสอบทำโดยการทำ Re-Assessment รายละเอียดเหมือน ISMF ขั้นตอนที่ 1 แต่จะสรุปผลออกมาในภาพรวมมากขึ้น โดยมีการเปรียบเทียบกับผลจากขั้นตอนที่ 1 ก่อนที่เราจะ "Hardening" หรือ ปิดช่องโหว่ในขั้นตอนที่ 2 เราจะได้ความแตกต่างจาก "GAP Analysis" แสดงให้เห็นถึงผล "ก่อน Hardening" และ "หลัง Hardening" ว่ามีความแตกต่างกันอย่างไร ถ้าการ Hardening ยังไม่สมบูรณ์ก็ต้องมีการ Re-Hardening อีกครั้งเพื่อให้แน่ใจว่าได้ปิดช่องโหว่จนความเสี่ยงอยู่ระดับที่ยอมรับได้ (Risk Acceptance Level) การตรวจสอบระบบนั้นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) ควรมี "Compliance Checklist" เพื่อนำไปตรวจสอบระบบต่างๆ และนำผลลัพธ์มาทำ "GAP Analysis" ว่าระบบที่ใช้อยู่นั้นได้มีการจัดการด้านระบบรักษาความปลอดภัยเป็นไปตาม "IT Security Policy" ขององค์กรหรือไม่และได้ทำตาม "Best Practices" ที่เหมาะสมกับระบบนั้นๆ แล้วหรือยัง

หลักการในการตรวจสอบระบบสารสนเทศที่ถูกต้องก็คือ ต้องมีการประเมินความเสี่ยง (Risk Assessment) ขององค์กรเสียก่อน ซึ่งมีขั้นตอนสำคัญที่ต้องปฏิบัติ เช่น การระบุปัจจัยที่มีผลทำให้เกิดความเสี่ยง และ การระบุความเสี่ยงที่มีโอกาสเกิดขึ้น (Risk Identification), การวิเคราะห์ความเสี่ยง (Risk Analysis) และการบริหารจัดการกับความเสี่ยง (Risk Management)

การตรวจสอบระบบสารสนเทศต้องพิจารณาเรื่องของ Control หรือ การควบคุม ว่าได้มีการจัดการอย่างถูกต้องหรือไม่ การตรวจสอบการควบคุมแบ่งออกเป็น 3 ประเภทใหญ่ๆ คือ

1. การควบคุมแบบป้องกันล่วงหน้า (Preventive Control)

2. การควบคุมแบบค้นหาประวัติเหตุการณ์ที่เกิดขึ้น (Detective Control)
3. การควบคุมแบบแก้ไขปัญหาจากเหตุการณ์ที่เกิดขึ้น (Corrective Control)

IT Auditor ควรจะพิจารณาการควบคุม (Control) ไปพร้อมๆกันทั้ง 3 มุมมอง ได้แก่

1. มุมมองทางด้านการบริหารจัดการ (Administrative Control)
2. มุมมองทางด้านเทคนิค (Technical Control)
3. มุมมองทางด้านกายภาพ (Physical Control)

IT Auditor ต้องมีความรู้ความเข้าใจในขั้นตอนกระบวนการตรวจสอบระบบสารสนเทศ (IT Audit Process) ตลอดจนมีความรู้ด้านเทคนิคเชิงลึก (IT Audit Technical Know-how) ในระบบที่ต้องเข้าไปตรวจสอบ เราสามารถแบ่งประเภทของงานตรวจสอบระบบสารสนเทศออกเป็น 7 ประเภทใหญ่ๆ ดังนี้

1. **การตรวจสอบระบบปฏิบัติการ (NOS Audit)** เช่น การตรวจสอบระบบ Server ที่ใช้ MS Windows เช่น Windows NT, Window 2000 Server ตลอดจน Workstation ที่ใช้ Windows XP เป็นต้น การตรวจสอบควรจะครอบคลุมถึงระบบปฏิบัติการอื่นด้วย เช่น การตรวจสอบระบบปฏิบัติการ Unix เช่น Sun Solaris, HP/UX, IBM AIX และ ระบบปฏิบัติการ Linux ที่ได้รับความนิยมเพิ่มขึ้นเรื่อยๆ
2. **การตรวจสอบอุปกรณ์เครือข่าย (Network Devices Audit)** เช่น การตรวจสอบ Router, การตรวจสอบ Switching และ การตรวจสอบ Remote Access Server ตลอดจน การตรวจสอบโครงสร้างของเครือข่าย (Network Infrastructure Audit) และ ประสิทธิภาพของเครือข่าย (Network Performance Audit) โดยใช้โปรแกรมตรวจสอบประเภท Packet Sniffer หรือ RMON Probe เป็นต้น
3. **การตรวจสอบอุปกรณ์รักษาความปลอดภัย (Security Devices Audit)** เช่น การตรวจสอบ Firewall, การตรวจสอบ Intrusion Detection System (IDS), การตรวจสอบ Intrusion Prevention System (IPS), การตรวจสอบโปรแกรม Enterprise Anti-Virus, การตรวจสอบ VPN Server เป็นต้น การตรวจสอบอุปกรณ์รักษาความปลอดภัยนั้นเป็นสิ่งที่มีความจำเป็นอย่างสูง เพราะถ้าอุปกรณ์รักษาความปลอดภัยมีปัญหาเสียเอง หรือโดน Hacker เจาะเข้ามา compromised ก็จะทำให้เกิดปัญหากับความปลอดภัยของระบบโดยรวม ผู้ตรวจสอบควรเป็นผู้ชำนาญงานด้านการใช้งาน Firewall หรือ IDS/IPS มาก่อนด้วยจะช่วยได้มาก
4. **การตรวจสอบโปรแกรมฐานข้อมูล (RDBMS Audit)** เช่น การตรวจสอบ Oracle, IBM DB2, Microsoft SQL Server, Informix, SYBASE หรือ MySQL RDBMS การตรวจสอบโปรแกรมฐานข้อมูลควรกระทำควบคู่ไปกับการตรวจสอบระบบปฏิบัติการที่โปรแกรมฐานข้อมูลทำงานอยู่ เช่น Oracle ทำงานบน Unix เป็นต้น เพื่อที่จะเจาะลึกลงไปในด้านความปลอดภัยของตัวโปรแกรม

ฐานข้อมูลเองว่ามีช่องโหว่หรือไม่ ผู้ตรวจสอบควรเป็นผู้เชี่ยวชาญการใช้งานโปรแกรมฐานข้อมูลนั้นๆมาก่อน เพราะการตรวจสอบต้องใช้ความรู้เชิงลึกทางด้าน RDBMS ด้วย

5. **การตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการในลักษณะ Server (Application Specific Audit)** เช่น การตรวจสอบ Web Server IIS บน Microsoft Windows Platform และ การตรวจสอบ Web Server Apache บน Unix/Linux Platform ซึ่งทั้ง 2เป็นโปรแกรม Web Server ยอดนิยมอยู่ในขณะนี้ นอกจากการตรวจสอบ Web Server แล้ว IT Auditor ควรตรวจสอบ Mail Server, FTP Server, LDAP Server, RADIUS Server ตลอดจน DNS Server ซึ่งถือเป็นหัวใจหลักของระบบ หาก DNS Server มีปัญหาจะทำให้ระบบไม่สามารถอ้างอิง Hostname ได้ ซึ่งจะก่อให้เกิดปัญหาใหญ่กับระบบโดยรวม
6. **การตรวจสอบกระบวนการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control)** จากข้อ 1 ถึง ข้อ 5 เป็นการตรวจสอบในมุมมองทางด้านเทคนิค (Technical Control) การตรวจสอบในมุมมองการบริหารจัดการนั้น ได้แก่ การตรวจสอบ Policy, Standard, Guideline และ Procedure ที่องค์กรมีอยู่ว่าครอบคลุม และ มีการปฏิบัติตามหรือไม่ ในขั้นตอนนี้รวมถึงการตรวจสอบว่าองค์กรมีการจัดฝึกอบรมด้านการรักษาความปลอดภัย (Security Awareness Training) หรือไม่ ซึ่งตามปกติควรจะ มีเป็นประจำทุกปี การตรวจสอบการบริหารจัดการนั้นต้องพิจารณาจากโครงสร้างหน่วยงาน, การแบ่งแยกหน้าที่ต่างๆในหน่วยงาน, การจัดทำแผนสำรองฉุกเฉิน และแผนรับเหตุการณ์ (Business Continuity Planning, Disaster Recovery Planning and Incident Response Procedure) ตลอดจนการควบคุมการเปลี่ยนแปลงระบบงาน (Change Control Management)
7. **การตรวจสอบด้านกายภาพ (Physical Control)** ได้แก่ การตรวจสอบระบบควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์, การตรวจสอบ Hardware ระบบ Backup/Restore และ ระบบไฟสำรอง เช่น มี UPS เพียงพอหรือไม่ การตรวจสอบอุปกรณ์เฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) เป็นต้น

ISMF ขั้นตอนที่ 6 นั้นเป็นขั้นตอนที่สำคัญและต้องการบุคลากร IT Auditor ที่มีประสบการณ์และมีความรู้จริงในการตรวจสอบระบบ เพื่อให้ผลจากการตรวจสอบเข้าใกล้ความเป็นจริงมากที่สุด เพราะปัญหาส่วนใหญ่ในการตรวจสอบระบบสารสนเทศ ก็คือ IT Auditor ยังขาดประสบการณ์เพราะความรู้ เทคนิคยังไม่ลึกพอที่จะเข้าไปตรวจสอบระบบ เช่น

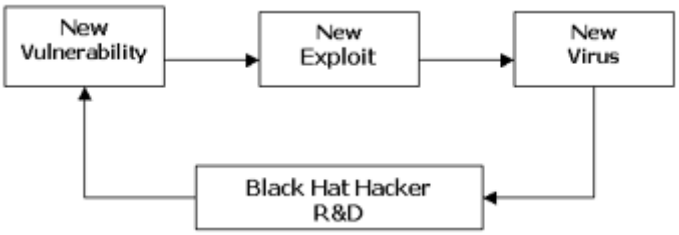
- ความรู้ด้าน Vulnerability Assessment และ Penetration Testing ในลักษณะ Ethical Hacking หรือ White Hat Hacking
- ความรู้พื้นฐานทางด้านเครือข่าย เช่น ISO OSI Layer Model, TCP/IP Protocol Suite
- ความรู้การใช้งานระบบปฏิบัติการพื้นฐาน คือ Microsoft Windows และ Unix/Linux

- ความรู้พื้นฐานในการใช้งานอุปกรณ์เครือข่าย Router หรือ Switching ซึ่ง IT Auditor ควรมีความรู้พื้นฐานในระดับ CCNA (Cisco Certified Network Associate)
- ความรู้ทางด้านความปลอดภัยข้อมูล เช่น Concept ของ CIA TRIAD (Confidentiality, Integrity and Availability), การทำงานของ Firewall และ IDS ในบริเวณ Network Perimeter ขององค์กร ตลอดจนวิธีการบุกรุกของ Hacker และ การทำงานของ Virus

ดังนั้น IT Auditor ควรจะมี CISA Certification เพื่อแสดงถึงความรู้ในด้าน IT Audit Process แล้ว ก็ควรจะมีความรู้พื้นฐานทางด้านเทคนิคด้วย ทั้งด้านระบบเครือข่ายและระบบปฏิบัติการที่ตนเองต้องเข้าไปตรวจสอบ ทางแก้ปัญหาในเชิงบูรณาการก็คือ IT Auditor ต้องเข้ารับการฝึกอบรมทางด้านเทคนิคเพิ่มเติม หรือ หาความรู้เพิ่มด้วยตนเองจากการติดตามข่าวสารเทคโนโลยีด้านความปลอดภัยใหม่ๆอยู่ตลอดเวลา เพื่อให้ทันกับยุคที่การสื่อสารไร้พรมแดน และ ภัยอินเตอร์เน็ต ไม่ว่าจะเป็น Hacker และ Virus ที่นับวันจะทวีความรุนแรงมากขึ้น ในโลกยุค Digital ที่มีความเปลี่ยนแปลงอยู่ตลอดเวลา

หลังจากที่เราได้จัดการกับระบบความปลอดภัยข้อมูลคอมพิวเตอร์อย่างเป็นขั้นตอนด้วย Information Security Management Framework (ISMF) จาก ISMF ขั้นตอนที่ 1 จนถึง ISMF ขั้นตอนที่ 6 แล้วนั้น เราพบว่าช่องโหว่ของระบบที่ถูกค้นพบขึ้นใหม่ (New Vulnerability) เกิดขึ้นอยู่ตลอดเวลา เพราะทางกลุ่ม Black Hat Hacker มีความพยายามในการทำ Research & Development (R&D) เพื่อที่จะค้นพบช่องโหว่ใหม่ๆ ของระบบปฏิบัติการหรือโปรแกรมประยุกต์ที่เรานิยมใช้ เมื่อบรรดา Black Hat Hacker หรือ Hacker ฝ่ายอธรรมได้ค้นพบช่องโหว่ใหม่ๆ ก็จะมีการรายงานผ่านทาง Security Web Site ต่างๆ ที่เกี่ยวข้องกับด้าน Vulnerability Report เช่น www.securityfocus.com จากนั้นก็จะมีการพัฒนาโปรแกรมที่ใช้ในการเจาะช่องโหว่ที่เพิ่งถูกค้นพบ ซึ่งเราเรียกว่า "Exploit"

Exploit ส่วนใหญ่จะเป็น Secure Code โปรแกรมภาษา C ที่สามารถทำงานได้บน Linux Platform และหลังจากที่ Exploit ถูก Upload ให้บรรดา Black Hat Hacker ได้ลองใช้งานกันสักระยะหนึ่งก็จะมีพัฒนาการต่อเป็น Virus ออกมา และ Virus ก็จะพัฒนาเป็น Version ต่างๆ เช่น Bagle.A, Bagle.B, Bagle.H, Bagle.Q ไปเรื่อยๆ จนกว่าบริษัทที่ผลิต Anti-Virus จะตรวจพบ



วงจรการพัฒนา Exploit/Virus ของ Black Hat Hacker ดูได้ดังรูป

ดังนั้นแม้ว่าเราจะจัดการกับระบบความปลอดภัยข้อมูลคอมพิวเตอร์ตามขั้นตอน ISMF จาก 1 ถึง 6 แล้ว เมื่อเวลาผ่านไประบบก็มีโอกาสที่จะเกิด Vulnerability ใหม่ๆ อยู่ตลอดเวลา และ เราก็ต้องคอยตามลง Patch หรือ Hotfix ต่างๆ ให้กับระบบอย่างทันท่วงที เรียกว่า วัดกันที่ความเร็วว่าใครจะรู้ข่าวก่อนกัน ถ้าเรารู้ข่าวช่องโหว่ใหม่ แล้วรีบทำการปิดช่องโหว่เสียก่อนโอกาสที่จะติด Virus หรือโดน Hack ก็จะน้อยลง แต่ถ้าเราละเลยไม่สนใจข่าวสารเรื่องการค้นพบ Vulnerability ใหม่ๆ หรือรู้ข่าวแต่ยังนิ่งนอนใจไม่ลง Patch ให้กับระบบ โอกาสที่จะถูกจู่โจมโดย Hacker หรือ Virus ก็จะมีมากขึ้น

จากปัญหาข้างต้น เราพบว่าเมื่อเวลาผ่านไป เราต้องกลับไปทำ ISMF ในขั้นตอนทั้ง 6 อีกเป็นระยะๆ เรียกว่าเป็น "Continuous Process" ที่หยุดไม่ได้ ดังนั้นเราจึงต้องคอยศึกษาและติดตามข้อมูลข่าวสารด้าน Information Security อยู่ตลอดเวลา ซึ่งต้องเสียทั้งกำลังคนและทรัพยากรต่างๆ ในองค์กรพอสมควร ตลอดจนต้องมีการเฝ้าระวังการจู่โจมจาก Hacker หรือ Virus โดยระบบ IDS/IPS และ ยังต้องมีเจ้าหน้าที่ดูแลวิเคราะห์ Log และสถานการณ์ต่างๆ ที่เกิดขึ้นจากอุปกรณ์ IDS/IPS ตลอดจน Firewall Log, Network Device Log และ Host Log เช่น Windows 2000 Log หรือ Unix/Linux SysLog เป็นต้น

การเฝ้าระวังโดยการวิเคราะห์ Log ด้วยบุคลากรภายในองค์กรของเราเองนั้น นอกจากจะใช้เวลาค่อนข้างมาก แล้วยังต้องการผู้เชี่ยวชาญที่แยกแยะระหว่าง Fault Alarm กับ Real Attack Alarm ซึ่งผู้เชี่ยวชาญต้องมีความชำนาญเป็นพิเศษด้านการวิเคราะห์การบุกรุกระบบ (Intrusion Analyst) ตลอดจนในปัจจุบันค่าตัวของบุคลากรที่มีความเชี่ยวชาญดังกล่าวก็ค่อนข้างสูงอยู่พอสมควร

จากปัญหาดังกล่าวจึงเกิดแนวคิดในการ "Outsource" ด้านการจัดการระบบรักษาความปลอดภัยซึ่งเรียกว่า "Managed Security Services" หรือ "MSS" การจัดจ้าง Outsource ด้าน Security โดยเฉพาะ เป็นแนวคิดที่ต้องการให้ Outsource มาช่วยในการจัดการบริหารความเสี่ยง และ ช่วยลดความเสี่ยงให้กับระบบโดยรวม (Risk Management & Risk Mitigation)

บริษัทที่ให้บริการ Outsource Security เราเรียกว่า MSSP หรือ Managed Security Service Provider ควรมีการให้บริการครอบคลุมในหัวข้อต่างๆ ดังนี้

1. บริหารจัดการ และ เฝ้าระวัง (Managing and Monitoring) Network Perimeter Security ที่ External Firewall, Border Router, IDS/IPS, VPN ตลอดจน Server ในบริเวณ DMZ

2. บริหารจัดการ Vulnerability ให้กับระบบขององค์กรอย่างต่อเนื่อง เช่น การทำ Vulnerability Assessment และ Penetration Testing รายเดือน เป็นต้น
3. เฝ้าระวัง Internal Network จาก Virus และ Hacker ตลอดจน Internal Firewall and Server Farm ภายในระบบ LAN ขององค์กร
4. รับปรึกษาปัญหาเวลาเกิด Security Breach Incident, รับแก้ปัญหาในลักษณะ Incident Response และ Digital Forensic
5. บริหารจัดการ Centralized Log Management และ Centralized Patch Management อย่างเป็นระบบ
6. บริการแจ้งข่าวสารความเคลื่อนไหวด้าน Information Security โดยเฉพาะเรื่อง New Vulnerability/Exploit และ New Virus ให้ทราบในลักษณะวันต่อวัน (Day by Day report)

การเลือก MSSP จึงเป็นหัวใจสำคัญ สำหรับผู้บริหารระบบต้องมีการกำหนด SLA (Services Level Agreement) ให้ชัดเจนใน RFP (Request for Proposal) โดยควรมีรายละเอียดให้มากที่สุดเท่าที่จะทำได้ เช่น ขอบเขตในการให้บริการของ MSSP, ระยะเวลาในการให้บริการ และ การตอบสนองของ MSSP, ค่าใช้จ่ายที่เกิดขึ้นในแต่ละเดือน ตลอดจนความรับผิดชอบของ MSSP ในแง่กฎหมายและบทปรับหาก MSSP ปฏิบัติไม่ได้ตาม SLA ที่ได้ตกลงกันไว้ใน Contact เป็นต้น

การ Outsource Security นั้นจะช่วยลดต้นทุนให้กับองค์กรในด้านของอัตรากำลังของบุคลากรผู้เชี่ยวชาญ ตลอดจน Hardware และ Software ต่างๆ ที่ลงทุนโดย MSSP และ องค์กรยังได้รับข่าวสารใหม่ๆ ด้าน Information Security เช่น การค้นพบ Vulnerability และ Virus ใหม่ๆ เพื่อที่องค์กรจะได้เตรียมตัวรับความเสี่ยงที่อาจเกิดขึ้น นอกจากนี้ MSSP ควรจะมีผู้เชี่ยวชาญ หรือ Security Expert คอยให้คำปรึกษา และ คอยเตือนภัยทางอินเตอร์เน็ตให้องค์กรทราบอยู่ตลอดเวลา

สำหรับปัญหาจากการ Outsource Security ที่เราควรคำนึงถึงก็มีเช่นกัน กล่าวคือ ถ้าสัญญาที่ทำกับ MSSP ไม่รัดกุมพอก็จะทำให้เกิดปัญหาในการปฏิบัติได้ ตลอดจนปัญหาในการเลือก MSSP ที่ไม่มีความเชี่ยวชาญเพียงพอก็อาจทำให้ไม่คุ้มค่าในการลงทุนกับการ Outsource Security ในกรณีที่เกิดปัญหาแล้ว MSSP ไม่สามารถแนะนำหรือให้คำปรึกษาได้ตามที่องค์กรคาดหวังว่าจะได้รับจาก MSSP เป็นต้น

กล่าวสรุปโดยรวม ข้อดีในการจ้าง MSSP ก็ยังมีมากกว่าข้อเสียที่ได้กล่าวมาแล้ว การตกลงทำงานร่วมกันกับ MSSP ในลักษณะที่ช่วยเหลือซึ่งกันและกัน โดยงานที่เป็นลักษณะที่ต้องใช้ความสามารถเฉพาะทางก็มอบให้ MSSP เป็นผู้จัดการให้ ส่วนองค์กรมีหน้าที่ในการ Audit ตรวจสอบ MSSP ว่ามีการปฏิบัติตาม SLA หรือไม่ จะทำให้ไม่เกิดปัญหาในระยะยาวจากการจัดจ้าง MSSP และ เป็นการบริหารความเสี่ยงด้าน IT ที่ถูกหลักการเป็นไปตามยุคสมัยของความนิยมในเรื่อง "IT Outsourcing"

จาก : หนังสือ eLeader Thailand

ประจำเดือน เดือนพฤษภาคม 2547

Update Information : 25 เมษายน 2547