PREFACE

องค์กรสมัยใหม่ไม่ว่าจะเป็นภาครัฐหรือเอกชน ล้วนแล้วแต่อาศัยเทคโนโลยีสารสนเทศในการดำเนินธุรกิจ หรือสนับสนุนภารกิจหรือธุรกิจถึงขั้นขาดไม่ได้ การลงทุนด้านไอทีจึงเป็นสิ่งที่สำคัญ เพื่อให้การดำเนินธุรกิจมีประสิทธิภาพและพัฒนาธุรกิจให้ก้าวหน้ายิ่งขึ้น สร้างความได้เปรียบต่อคู่แข่ง แต่ละองค์กรจะมีระบบเทคโนโลยีสารสนเทศที่หลากหลาย ตั้งแต่ ระบบอีเมล เว็บไซต์ ระบบบัญชี ระบบอีคอมเมิร์ซ ไปจนถึงระบบเฉพาะอย่างเช่น ระบบควบคุมกระบวนการอุตสาหกรรม ระบบสื่อสารโทรคมนาคม และระบบควบคุมสภาพแวดล้อม เป็นต้น ปัจจุบันภัยคุกคามทางด้านไซเบอร์ได้ทวีความรุนแรงขึ้นเรื่อยๆ ซึ่งทำให้ระบบต่างๆ เหล่านี้ล้วนแล้วแต่มีความเสี่ยงที่จะถูกโจมตีหรือถูกทำลาย ซึ่งส่งผลกระทบต่อการดำเนินธุรกิจขององค์กร และสร้างความเสียหายต่อทรัพย์สินของทั้งส่วนบุคคลและองค์กร นอกจากนี้ปัจจุบันยังได้เกิดการทำสงครามรูปแบบใหม่ที่เรียกว่า สงครามไซเบอร์ (Cyber Warfare) ซึ่งเป็นการปฏิบัติการสงครามที่เกิดขึ้นในสมรภูมิโลกไซเบอร์ แต่ส่งผลกระทบในโลกจริง

ภัยคุกคาม (Threat) หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่ง หรือมากกว่าหนึ่งด้าน อันได้แก่ ความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ความเสี่ยง (Risk) เกิดจากการที่ภัยคุกคาม (Threat) ใช้ประโยชน์จากช่องโหว่ (Vulnerability) แล้วเกิดผลกระทบ (Impact) ต่อข้อมูลหรือระบบสารสนเทศ ภัยคุกคามอาจรวมถึงการโจมตีทางไซเบอร์ ภัยธรรมชาติ ความผิดพลาดอันเกิดจากคนหรือเครื่องจักร หรือแม้กระทั่งปัญหาจากเรื่องโครงสร้างอาคารสถานที่ ภัยคุกคามนั้นอาจจะไม่เกิดขึ้นเลยก็ได้ถ้ามีการป้องกันที่ดี หรือถ้ามีการเตรียมการที่ดี เมื่อมีเหตุการณ์เกิดขึ้นก็จะช่วยลดความเสียหายหรือผลกระทบได้ การกระทำที่อาจก่อให้เกิดความเสียหายเราจะเรียกว่า การโจมตี (Attack) ส่วนผู้ที่ทำเช่นนั้น หรือผู้ที่เป็นเหตุให้เหตุการณ์ดังกล่าวเกิดขึ้นจะเรียกว่า ผู้โจมตี (Attacker) ภัยคุกคามหลักของระบบคอมพิวเตอร์คือ แฮคเกอร์และมัลแวร์ ที่แตกต่างกันคือ แฮคเกอร์เป็นคน ส่วนมัลแวร์เป็นโปรแกรมที่ทำงานอัตโนมัติ อย่างไรก็ตาม แฮคเกอร์อาจใช้มัลแวร์เป็นเครื่องมือในการโจมตีอีกทีหนึ่งก็ได้ แต่ที่เหมือนกันก็คือ ทั้งแฮคเกอร์และมัลแวร์จะใช้ประโยชน์จากช่องโหว่ของระบบคอมพิวเตอร์ ซึ่งก็คือ จุดอ่อนหรือข้อผิดพลาดของโปรแกรม รวมไปถึงความหละหลวมในการคอนฟิกระบบ และช่องโหว่ทางกายภาพ เช่น การวางอุปกรณ์ทิ้งไว้โดยไม่มีคนดูแล เป็นต้น

การรักษาความปลอดภัย เป็นหลักการที่รวมเอาการบริหารจัดการด้านนโยบายและกระบวนการ บุคลากร และเทคโนโลยี (PPT) มาใช้เพื่อเพิ่มประสิทธิภาพในการรักษาความลับ, การรักษาความถูกต้อง และการทำให้พร้อมใช้งานของข้อมูล หนังสือเล่มนี้จะได้อธิบายในรายละเอียดของกระบวนการในการรักษาความปลอดภัยข้อมูล ซึ่งเนื้อหาส่วนใหญ่ได้จากประสบการณ์การทำงานสิบกว่าปีที่ผ่านมา ผู้เขียนหวังเป็นอย่างยิ่งว่าผู้อ่านจะได้ประโยชน์จากหนังสือเล่มนี้ และผู้เขียนมุ่งมั่นที่จะพัฒนาและปรับปรุงให้เนื้อหาทันสมัยอยู่เรื่อยๆ

ขอขอบคุณ
จตุชัย แพงจันทร์
jatuchai@rtaf.mi.th

CONTENTS

Part 1 Information Security

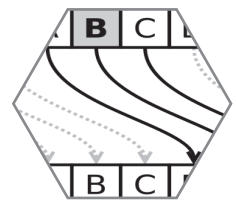
บทที่ 1 Cybersecurity

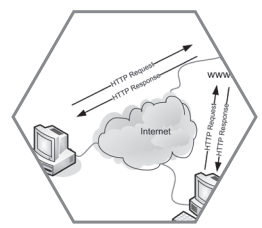
บทที่ 2 IT Security Governance

บทที่ 3 การบริหารความเสี่ยง (Risk Management)

บทที่ 4 Access Control

บทที่ 5 Cryptography

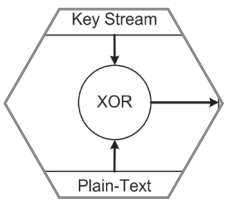




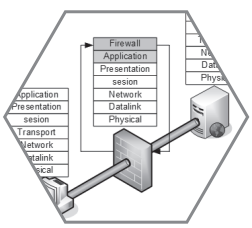
Part 2 Network Security

บทที่ 6 Network Security

บทที่ 7 Wireless LAN Security



บทที่ 8 Firewall

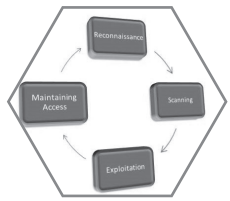


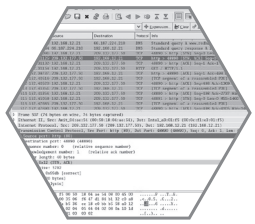
บทที่ 9 Intrusion Detection System

Part 3 Malware and Hacker

บทที่ 10 Malware

บทที่ 11 Hacking

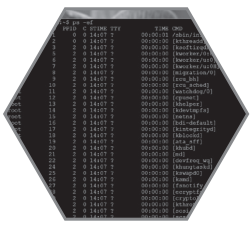




บทที่ 12 การกู้คืนระบบ

Part 4 Endpoint Security

บทที่ 13 Windows Security

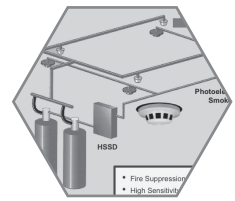


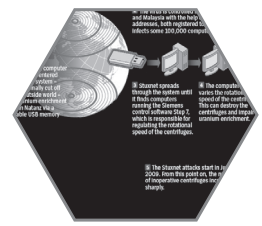
บทที่ 14 Linux Security

Part 5 Physical Security, Cyber Law & Cyber Warfare

บทที่ 15 Physical and Environmental Security

บทที่ 16 กฎหมายอาชญากรรมคอมพิวเตอร์





บทที่ 17 Cyber Warfare

Master in Security 3rd Edition

PART 1

Information Security

หลักการในการรักษาความปลอดภัยนั้นคือ การรักษาไว้ซึ่งคุณสมบัติทั้ง 3 มิติคือ ความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) การบริหารจัดการด้านการรักษาความปลอดภัยข้อมูล เป็นสิ่งที่องค์กรจะต้องทำควบคู่กับการบริหารองค์กรด้านอื่นๆ โดยกระบวนการนั้นจะเริ่มต้นด้วยการวิเคราะห์ความเสี่ยง แล้วกำหนดมาตรการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และควรต้องทำทั้ง 3 ส่วนควบคู่กันไปคือ คน (People), กระบวนการ (Process) และเทคโนโลยี (Technology) โดยกระบวนการที่เป็นมาตรฐานและเป็นที่ยอมรับ ได้แก่ ISO 27001

CHAPTER 1

Cybersecurity

วัตถุประสงค์

- รู้และเข้าใจวิวัฒนาการของการรักษาความปลอดภัยไซเบอร์
- รู้และเข้าใจหลักการของการรักษาความปลอดภัยข้อมูล
- รู้และเข้าใจภัยคุกคามรูปแบบต่างๆ ในปัจจุบันและแนวโน้มในอนาคต

ในยุคข้อมูลข่าวสารในปัจจุบันถือได้ว่า ข้อมูลเป็นทรัพย์สินที่มีค่ายิ่งขององค์กร ไม่ว่าจะเป็นองค์กรภาครัฐหรือธุรกิจเอกชน การประยุกต์ใช้ระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม จะช่วยเพิ่มประสิทธิภาพ ศักยภาพ และส่งเสริมให้พัฒนาไปสู่องค์กรที่มีประสิทธิภาพสูงและองค์กรแห่งการเรียนรู้ ส่งผลให้ได้เปรียบในด้านการแข่งขันทางธุรกิจ ดังนั้นองค์กรต่างๆ จึงมีความตื่นตัวในด้านการพัฒนาองค์กร เพื่อจะก้าวให้ทันกับสภาวการณ์ของโลกที่กำลังเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะอย่างยิ่งความเจริญก้าวหน้าด้านเทคโนโลยีสารสนเทศ ทำให้เกิดการใช้ประโยชน์จากข้อมูลข่าวสารอย่างมีประสิทธิภาพและสร้างโอกาสทางธุรกิจ ซึ่งถือเป็นความท้าทายขององค์กรสมัยใหม่ ที่จะต้องมีการพัฒนาให้เจริญก้าวหน้าและไม่ให้ตนเองตกอยู่ในสภาวะล้าหลัง

ข้อมูลหรือสารสนเทศ (Information) ถือว่าเป็นทรัพย์สินประเภทหนึ่งที่มีค่าสูงและมีความสำคัญต่อองค์กร เนื่องจากองค์กรที่รู้ข้อมูลมากกว่าย่อมได้เปรียบคู่แข่งเสมอ แต่ถ้าข้อมูลที่สำคัญขององค์กรถูกขโมยไป หรือระบบสารสนเทศถูกแฮคจนไม่สามารถใช้งานได้ ก็ย่อมส่งผลกระทบต่อองค์กรอย่างแน่นอน ดังนั้น การปกป้องรักษาข้อมูลและระบบสารสนเทศจึงเป็นสิ่งที่สำคัญไม่แพ้ไปกว่าการปกป้องรักษาทรัพย์สินประเภทอื่นๆ เช่น ผลิตภัณฑ์ วัตถุดิบ อาคารสถานที่ เงิน เป็นต้น ข้อมูลที่ถูกจัดเก็บไว้ในระบบสารสนเทศนั้นมีความเสี่ยงที่จะถูกโจมตีจากหลายแหล่ง เช่น ผู้ใช้งานที่รู้เท่าไม่ถึงการณ์ การโจมตีจากทั้งภายในและภายนอก การแพร่กระจายของไวรัส เวิร์ม โทรจันฮอร์ส หรือมัลแวร์ประเภทอื่นๆ ซึ่งอาจถูกส่งผ่านทางอีเมล เว็บ หรืออาจมีผู้ไม่หวังดีหรือแฮคเกอร์จากอินเทอร์เน็ตพยายามที่จะเจาะเข้าระบบเพื่อทำลายระบบหรือลบทิ้ง เปลี่ยนแปลงแก้ไข ขโมยไปใช้งาน หรือทำให้เข้าถึงข้อมูลไม่ได้ ดังนั้น ระบบสารสนเทศจึงจำเป็นที่ต้องมีระบบรักษาความปลอดภัยที่แข็งแกร่งพอที่จะรับมือกับภัยคุกคามต่างๆ ได้

ปัจจุบันเครือข่ายอินเทอร์เน็ตขยายตัวอย่างรวดเร็ว องค์กรสมัยใหม่จำเป็นต้องเชื่อมต่อเข้ากับอินเทอร์เน็ตเพื่อใช้ประโยชน์จากแหล่งข้อมูลที่ใหญ่ที่สุดในโลกนี้ อินเทอร์เน็ตนั้นเปรียบเสมือนดาบสองคม ประโยชน์ที่ได้รับจากอินเทอร์เน็ตนั้นอาจมากเกินกว่าที่จะจินตนาการ แต่โทษนั้นก็มีมากมายเช่นกัน เหตุผลหนึ่งก็เนื่องจากข้อมูลและเครื่องมือที่ใช้สำหรับการเจาะระบบนั้น สามารถค้นหาและดาวน์โหลดจากอินเทอร์เน็ตได้อย่างง่ายดาย และเครื่องมือหรือโปรแกรมเหล่านี้ยังง่ายต่อการใช้งาน ถึงแม้ว่าคนที่ไม่มีความรู้เกี่ยวกับคอมพิวเตอร์มากนัก ก็สามารถใช้เครื่องมือโจมตีเครือข่ายเหล่านี้ได้ไม่ยากนัก ดังนั้น ฝ่ายไอทีหรือผู้ที่มีหน้าที่ดูแลระบบ จึงจำเป็นที่ต้องวิเคราะห์ความเสี่ยง ออกแบบติดตั้ง ระบบรักษาความปลอดภัย และเฝ้าระวังระบบรักษาความปลอดภัยในเครือข่าย ให้มีใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ ดังนั้น การรักษาความปลอดภัยในเครือข่ายจึงเป็นสิ่งที่สำคัญและจำเป็นสำหรับองค์กร

ไม่มีระบบใดที่ปลอดภัยร้อยเปอร์เซ็นต์ ยังเป็นคำกล่าวที่เป็นจริงเสมอ การรักษาความปลอดภัยนั้นเป็นทั้งศาสตร์และศิลป์ การมีระบบรักษาความปลอดภัยที่ดีที่สุดนั้นไม่ได้หมายความว่า ข้อมูล ระบบคอมพิวเตอร์ และองค์กรจะปลอดภัยจากอันตรายทั้งปวง การรักษาความปลอดภัยของข้อมูลเป็นกระบวนการ ไม่ใช่แค่การติดตั้งเทคโนโลยีด้านการรักษาความปลอดภัยที่ดีที่สุด แต่จะรวมถึงกระบวนการบริหารความเสี่ยง (Risk Management) ซึ่งเริ่มตั้งแต่การระบุภัยคุกคาม (Threat) และช่องโหว่หรือจุดอ่อน (Vulnerability) ขององค์กร แล้วประเมินโอกาสที่จะเกิดขึ้น (Likelihood) และผลกระทบ (Impact) หากเกิดเหตุการณ์ดังกล่าวขึ้น หลังจากนั้นจะเป็นการกำหนดนโยบายการรักษาความปลอดภัย การบังคับใช้นโยบาย การเฝ้าระวังเหตุการณ์อยู่ตลอดเวลา หนังสือเล่มนี้เขียนขึ้นโดยมีจุดมุ่งหมายเพื่อแนะนำแนวทางหรือวิธีปฏิบัติที่เหมาะสมสำหรับการรักษาความปลอดภัยข้อมูลขององค์กร

ก่อนที่จะเรียนรู้เกี่ยวกับกระบวนการรักษาความปลอดภัยข้อมูล มาทำความรู้จักเกี่ยวกับคำว่า การรักษาความปลอดภัยข้อมูล (Information Security) กันก่อน เราสามารถแยกคำนี้ออกเป็นสองคำคือ ข้อมูล (Information) ซึ่งหมายถึง ความรู้ ความคิด ข่าวสาร และข้อเท็จจริง ส่วนการรักษาความปลอดภัย (Security) หมายถึง การทำให้รอดพ้นจากอันตราย หรือการทำให้รอดพ้นจากความกลัว ความทุกข์ใจ หรือความกังวล ดังนั้น เมื่อเรานำคำสองคำนี้มารวมกัน เราก็จะได้ว่า การรักษาความปลอดภัยข้อมูล หมายถึง การทำให้ความรู้ ความคิด ข่าวสาร และข้อเท็จจริง รอดพ้นจากอันตราย และถ้าตีความให้เข้ากับไอทีก็จะได้ว่า การรักษาความปลอดภัยข้อมูล หมายถึง มาตรการที่ใช้สำหรับป้องกันผู้ที่ไม่ได้รับอนุญาตในการเข้าถึง ลบ แก้ไข หรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตใช้งาน ความรู้ แนวคิด และข้อเท็จจริง

ความหมายที่กล่าวถึงข้างต้นนั้นเป็นความหมายที่กว้างมาก ซึ่งจะรวมถึงมาตรการทุกอย่างที่อาจใช้สำหรับป้องกันไม่ให้สิ่งไม่ดีเกิดขึ้นกับความรู้ ความคิด ข่าวสาร และข้อเท็จจริง นอกจากนี้รูปแบบของข้อมูลก็ยังไม่ได้จำกัดเฉพาะรูปแบบใดรูปแบบหนึ่ง มันอาจเป็นความรู้ หรืออาจเป็นความสามารถก็ได้ อย่างไรก็ตามมาตรการในการรักษาความปลอดภัยข้อมูลนั้นไม่สามารถที่จะรับรองได้ว่า ข้อมูลจะปลอดภัยร้อยเปอร์เซ็นต์ ยกตัวอย่างเช่น ถึงแม้ว่าเราจะสามารถสร้างกำแพงเมืองได้ใหญ่และแข็งแรงมากแค่ไหน แต่ศัตรูก็อาจสามารถสร้างปืนใหญ่ที่สามารถทำลายกำแพงลงได้อย่างง่ายดาย หรือถึงแม้ว่าเราจะมีไฟร์วอลล์ที่มีประสิทธิภาพดีมากแค่ไหน แต่ผู้โจมตีนั้นอาจอยู่ภายในเครือข่ายเป็นต้น การรักษาความปลอดภัยนั้นเป็นการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

โดยทั่วไปแล้วคำว่าข้อมูล (Data) จะใช้ในความหมายที่แตกต่างจากสารสนเทศ (Information) โดยข้อมูลนั้นส่วนใหญ่จะหมายถึง ข้อมูลดิบ ส่วนสารสนเทศจะหมายถึง ผลลัพธ์ที่ได้จากการนำข้อมูลมาประมวลผล เพื่อให้ได้สิ่งที่เป็นประโยชน์ในการนำไปใช้งานมากขึ้น และเมื่อนำสารสนเทศผ่านกระบวนการวิเคราะห์ไตร่ตรองอย่างดี ก็จะได้ผลออกมาเป็นความรู้ (Knowledge) ที่สามารถนำไปประยุกต์ใช้ในปัญหานั้นๆ ได้ และหากประมวลความรู้จากหลายๆ ด้านก็จะได้สิ่งที่เรียกว่า ปัญญา (Wisdom) อย่างไรก็ตามในระบบคอมพิวเตอร์นั้นจะมองว่าทุกอย่างเป็นข้อมูลเหมือนกันหมด เพราะฉะนั้นในหนังสือเล่มนี้อาจใช้คำว่า ข้อมูลหรือสารสนเทศในความหมายเดียวกัน

อีกคำหนึ่งที่กำลังได้รับความนิยมคือ การรักษาความปลอดภัยไซเบอร์ (Cybersecurity) ซึ่งหมายถึง กระบวนการที่จะทำให้องค์กรปราศจากความเสี่ยงและอันตรายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมถึงการรักษาความปลอดภัยของระบบสารสนเทศและเครือข่ายที่ใช้ในการเก็บเข้าถึง ประมวลผล และกระจายข้อมูลข่าวสารนั้นด้วย นอกจากนี้ยังรวมถึงการระวังป้องกันต่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่างๆ ต่อข้อมูลข่าวสารขององค์กรอีกด้วย

วิวัฒนาการของการรักษาความปลอดภัย

รูปแบบของการรักษาความปลอดภัยของข้อมูลและทรัพย์สินอื่นๆ นั้นได้มีวิวัฒนาการกับกาลเวลาเหมือนกับสังคมและเทคโนโลยีอื่นๆ การเรียนรู้และเข้าใจวิวัฒนาการนี้จะช่วยให้เข้าใจระบบการรักษาความปลอดภัยที่มีอยู่ในปัจจุบัน และอาจเป็นบทเรียนที่ช่วยให้เราไม่ต้องทำผิดเหมือนกับที่เคยเกิดขึ้นในอดีตได้

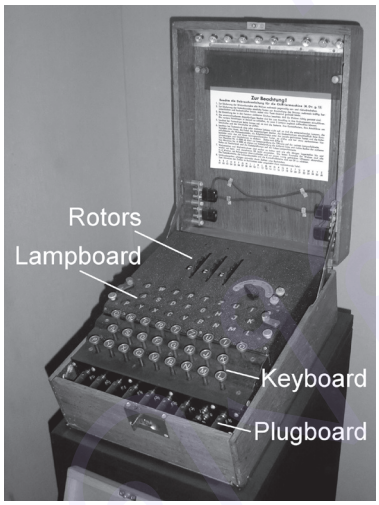
การรักษาความปลอดภัยด้านกายภาพ (Physical Security)

แต่ก่อนนั้นทรัพย์สินส่วนใหญ่จะเป็นวัตถุที่จับต้องได้ ข้อมูลที่สำคัญก็อยู่ในรูปแบบวัตถุเช่นกัน เนื่องจากข้อมูลจะถูกบันทึกไว้บนแผ่นหิน แผ่นหนัง หรือกระดาษ และบุคคลสำคัญในอดีตส่วนใหญ่จะไม่นิยมบันทึกข้อมูลที่สำคัญมากๆ ลงบนสื่อถาวร เช่น แผ่นหนังหรือกระดาษ และจะไม่สนทนาเกี่ยวกับข้อมูลเหล่านี้กับบุคคลอื่นนอกเหนือจากที่บุคคลที่ไว้ใจได้เท่านั้น นี่อาจเป็นที่มาของคำว่า **"ความรู้คืออำนาจ (Knowledge is power)"** ซึ่งหมายความว่า ผู้ที่มีความรู้คือผู้ที่มีอำนาจนั่นเอง และนี่อาจเป็นรูปแบบการรักษาความปลอดภัยที่ดีที่สุดในขณะนั้นก็ได้ ซันซู นักปรัชญาชาวจีน ได้กล่าวไว้ว่า **"ความลับที่รู้โดยคนมากกว่าหนึ่งคน ก็ไม่ถือว่าเป็นความลับอีกต่อไป"** การที่จะปกป้องทรัพย์สินที่เป็นวัตถุนั้นก็ต้องใช้การปกป้องทางด้านกายภาพ เช่น ป้อมปราการ ประตู กำแพง ประสาท ห้อง ตู้ กล่อง กุญแจ ยาม เป็นต้น

ถ้าต้องมีการส่งข้อมูลไปที่อื่นก็จะใช้ผู้ส่งข่าว และส่วนใหญ่ก็จะมีผู้คุ้มกันติดตามไปด้วย ภัยอันตรายนั้นจะอยู่ในรูปแบบทางกายภาพทั้งสิ้น ไม่มีทางที่จะได้ข้อมูลมาโดยที่ไม่ต้องไปคว้ามาด้วยมือ โดยส่วนใหญ่ทรัพย์สิน เช่น เงิน ทอง หรือข้อมูลที่บันทึกลงบนสื่อ จะถูกขโมยหรือถูกแย่งไปจากเจ้าของหรือผู้ดูแลทรัพย์สินนั้น

การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

อย่างไรก็ตามการรักษาความปลอดภัยเฉพาะด้านกายภาพด้านเดียวนั้น ก็มีข้อบกพร่อง จุดอ่อน หรือช่องโหว่หลายอย่าง กล่าวคือ ถ้าเอกสารหรือวัตถุที่ใช้บันทึกข้อมูลถูกขโมยระหว่างการรับส่ง ศัตรูก็สามารถเปิดอ่านและเข้าใจข้อมูลนั้นได้เลยทันที จนกระทั่งเมื่อราวยุคของจูเลียส ซีซาร์ (Julius Caesar) ข้อบกพร่องนี้ได้ถูกค้นพบ โดยในสมัยนั้น (ยุคศตวรรษที่ 2) ได้มีการคิดค้นวิธีการที่ใช้สำหรับการ "ซ่อน" ข้อมูล หรือการเข้ารหัสข้อมูล (Encryption) ซึ่งข้อมูลจะถูกเข้ารหัสก่อนที่จะส่งไปให้อีกฝ่ายหนึ่ง ดังนั้น ถ้ามีการขโมยข้อมูลระหว่างทาง ผู้อ่านก็จะไม่เข้าใจเนื้อหาที่แท้จริงของข้อมูลถ้าไม่รู้วิธีถอดรหัส



รูปที่ 1.1 : Enigma เครื่องมือเข้า/ถอดรหัสที่ใช้ในช่วงสงครามโลกครั้งที่ 2

แนวคิดนี้ได้ถูกพัฒนามาใช้ในช่วงสงครามโลกครั้งที่ 2 โดยเยอรมันใช้เครื่องมือที่เรียกว่า เอ็นนิกมา (Enigma) ดังแสดงในรูปที่ 1.1 : Enigma สำหรับเข้ารหัสข้อมูลที่รับส่งระหว่างหน่วยทหาร ในขณะนั้นเยอรมันเชื่อว่าไม่มีใครสามารถถอดรหัสลับนี้ได้ แต่ในที่สุดฝ่ายพันธมิตรก็สามารถถอดรหัสของเครื่องเอ็นนิกมานี้ได้ ทำให้ฝ่ายพันธมิตรสามารถอ่านข้อมูลที่รับส่งได้ ซึ่งส่งผลให้เยอรมันแพ้สงครามในที่สุด อย่างไรก็ตามช่องโหว่นั้นไม่ใช่เพราะเทคนิคการเข้ารหัสไม่แข็งแกร่งพอ แต่เกิดจากข้อผิดพลาดของผู้ใช้งานเครื่องนี้เอง ที่ไม่ระมัดระวังเกี่ยวกับการเก็บรักษารหัสลับที่ใช้เข้ารหัสข้อมูล ทำให้หลุดรั่วออกไปยังฝ่ายตรงข้ามได้

ในช่วงสงครามโลกครั้งที่ 2 นี้ การสื่อสารทางด้านการทหารนั้น จะใช้รหัสแทนชื่อจริงของหน่วยทหารหรือสถานที่อยู่แล้ว ตัวอย่างเช่น ญี่ปุ่นนั้นก็ใช้รหัสแทนชื่อเรียกทั่วไปในการสื่อสารกัน ถึงแม้ว่าสหรัฐฯ จะสามารถถอดรหัสข้อมูลได้ แต่ก็ยังต้องทำความเข้าใจกับรหัสที่ใช้แทนชื่อทั่วไปนี้อีก ซึ่งเป็นการเพิ่มความยากในการเข้าใจข้อมูลจริงๆ ตัวอย่างเช่น ในช่วงก่อนที่จะเกิดสงครามที่เกาะมิดเวย์ระหว่างญี่ปุ่นและสหรัฐฯ ในตอนนั้นสหรัฐฯ สามารถถอดรหัสลับของญี่ปุ่นได้ แต่ยังไม่เข้าใจรหัสที่ใช้แทนชื่อสถานที่ โดยในข้อความที่ส่งนั้นญี่ปุ่นจะโจมตีเป้าหมายที่มีรหัสว่า "AF" แต่ในที่สุดสหรัฐฯ ก็สามารถถอดรหัสนี้ได้ และรู้ว่า "AF" นั้นหมายถึง มิดเวย์นั่นเอง เทคนิคการถอดรหัสของสหรัฐฯ ทำได้โดยสหรัฐฯ ส่งข้อความหลอกว่า "เกาะมิดเวย์ขาดแคลนน้ำจืด" โดยข้อความนี้ไม่ได้เข้ารหัส เพื่อหลอกให้ญี่ปุ่นอ่านข้อความนี้ ญี่ปุ่นจะเข้ารหัสข้อความนี้ แล้วส่งต่อให้หน่วยอื่นทราบ สหรัฐฯ สามารถดักอ่านข้อความนี้ได้และถอดรหัสออกมาแล้วในข้อความนั้นมีอักษรว่า "AF" ที่ระบุสถานที่ ทำให้สหรัฐฯ รู้ได้ทันทีว่าอักษร "AF" นั้นหมายถึงเกาะมิดเวย์นั่นเอง

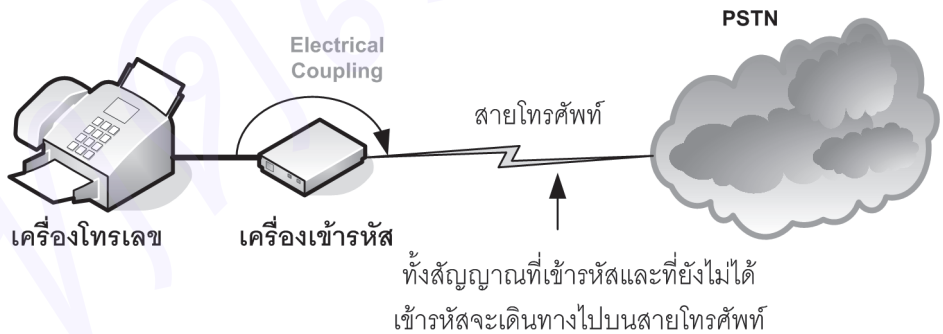
ข้อความไม่ใช่แค่ตัวอักษรที่เข้ารหัสในระหว่างการสื่อสารกัน ข้อความที่สื่อสารด้วยเสียง เช่น วิทยุและโทรศัพท์ ก็เป็นอีกข้อมูลประเภทหนึ่งที่ต้องเข้ารหัสเพื่อปกป้องความลับของข้อมูล หรือเพื่อป้องกันการดักฟังการสื่อสารด้วยเสียง สหรัฐฯ เข้ารหัสเสียงโดยใช้ "นาวาโฮโค้ดทอล์คเกอร์ (Navaho Code Talker)" นาโวโฮเป็นชนเผ่าหนึ่งที่มีภาษาเป็นของตัวเอง ผู้รับส่งข่าวนั้นจะใช้ภาษานี้ในการสื่อสารกัน ซึ่งถ้าฝ่ายศัตรูมีการดักฟังวิทยุที่สื่อสารกันก็อาจจะได้ยินแต่คงไม่เข้าใจภาษาได้

หลังจากสงครามโลกครั้งที่ 2 สหภาพโซเวียตได้ใช้วันไทม์แพ็ด (One time pad) เพื่อเข้ารหัสข้อมูลที่รับส่งโดยสายลับ วันไทม์แพ็ดใช้การเข้ารหัสโดยการส่งข้อความบนปึกกระดาษ โดยแต่ละหน้าจะประกอบด้วยตัวเลขที่เป็นเลขสุ่ม แต่ละหน้านั้นจะใช้แทนหนึ่งข้อความเท่านั้น รูปแบบการเข้ารหัสแบบนี้จะไม่สามารถถอดรหัสได้ถ้ามีการใช้อย่างถูกต้องคือ ใช้หนึ่งคีย์ต่อการเข้ารหัสหนึ่งข้อความ แต่สหภาพโซเวียตได้ใช้คีย์มากกว่าหนึ่งครั้ง ทำให้ข้อความที่ส่งนั้นถูกถอดรหัสได้โดยง่าย

การรักษาความปลอดภัยการแผ่รังสี (Emissions Security)

การถอดรหัส เป็นสิ่งที่ยากมากถ้าใช้เทคนิคการเข้ารหัสข้อมูลที่ดี อย่างไรก็ตามการถอดรหัสโดยใช้เทคนิคทางคณิตศาสตร์นั้นไม่ใช่วิธีการเดียวที่จะถอดรหัสข้อมูลได้ ดังนั้น จึงได้มีความพยายามที่จะคิดค้นเทคนิคใหม่ๆ สำหรับอ่านข้อมูลที่เข้ารหัส ในช่วงทศวรรษ 1950 ได้มีการค้นพบว่าข้อมูลที่รับส่งนั้น สามารถอ่านได้โดยการอ่านสัญญาณไฟฟ้าที่ส่งผ่านสายโทรศัพท์ อุปกรณ์อิเล็กทรอนิกส์ทุกประเภทจะมีการแผ่รังสีออกมา ซึ่งรวมถึงเครื่องพิมพ์โทรสารและเครื่องสำหรับเข้าและถอดรหัสข้อมูลด้วย เครื่องเข้ารหัสจะรับเข้าข้อความแล้วเข้ารหัสและส่งไปบนสายโทรศัพท์ ในช่วงนั้นได้มีการค้นพบว่าสัญญาณไฟฟ้าที่แทนข้อมูลที่ยังไม่ได้เข้ารหัส ก็ถูกส่งไปบนสายโทรศัพท์ด้วยเช่นกัน นั่นหมายความว่าข้อมูลเดิมที่ยังไม่ได้ถูกเข้ารหัสนั้น สามารถกู้คืนได้ถ้าใช้เครื่องมืออ่านสัญญาณไฟฟ้าที่ดี

ปัญหานี้เป็นเหตุให้สหรัฐฯ ต้องกำหนดมาตรฐานที่ชื่อ เทมเปสต์ (TEMPEST) ซึ่งเป็นมาตรฐานที่ควบคุมการแผ่รังสีของอุปกรณ์คอมพิวเตอร์ และใช้กับระบบที่สำคัญๆ จุดมุ่งหมายก็เพื่อลดการแผ่รังสีที่อาจใช้สำหรับการกู้คืนข้อมูลได้



รูปที่ 1.2 : สัญญาณที่ส่งผ่านสายโทรศัพท์

การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

การเข้ารหัสข้อมูลและการควบคุมการแผ่รังสี เป็นมาตรการการรักษาความปลอดภัยของข้อมูลที่เพียงพอ ถ้าระบบสื่อสารข้อมูลนั้นมีเพียงแค่การใช้เครื่องส่งโทรสารเหมือนดังในรูปที่ 1.2 แต่ต่อมาได้มีการนำคอมพิวเตอร์เข้ามาใช้งานแทนเครื่องส่งโทรสาร และข้อมูลส่วนใหญ่ก็อยู่ในรูปแบบดิจิตอล และได้มีการพัฒนาคอมพิวเตอร์เพื่อให้ใช้งานง่ายและสะดวกมากขึ้นเรื่อยๆ ทำให้ผู้ที่มีเครื่องคอมพิวเตอร์สามารถเข้าถึงข้อมูลทั้งหมดที่จัดเก็บในเครื่องนั้นด้วยเช่นกัน จึงเกิดปัญหาความไม่ปลอดภัยในการจัดเก็บข้อมูลในระบบคอมพิวเตอร์

ดังนั้น ในช่วงทศวรรษ 1970 เดวิด เบลล์ (David Elliott Bell) และลีโอนาร์ด ลา พาดูลา (Leonard J. La Padula) ได้พัฒนาแม่แบบสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์ (Bell-La Padula Model) แม่แบบนี้พัฒนาจากแนวคิดในการจัดระดับความปลอดภัยของข้อมูลของรัฐบาลสหรัฐฯ ซึ่งแบ่งออกได้เป็น 4 ชั้นคือ ไม่จัดระดับ, ลับ, ลับมาก และลับที่สุด (Unclassified, Confidential, Secret, Top Secret) และระดับสิทธิ์ของผู้ที่เข้าถึงข้อมูลลับนี้ (Clearance) ซึ่งมี 4 ระดับเหมือนกัน หลักการของระบบนี้คือ ผู้ที่สามารถเข้าถึงข้อมูลในระดับใดระดับหนึ่งได้ จะต้องมีสิทธิ์ (Clearance) เท่ากับหรือสูงกว่าชั้นความลับของข้อมูลนั้น ดังนั้น ผู้ที่มีสิทธิ์น้อยกว่าชั้นความลับของไฟล์ก็จะไม่สามารถเข้าถึงไฟล์นั้นได้

แนวคิดนี้ได้ถูกนำไปใช้ในกระทรวงกลาโหมของสหรัฐฯ โดยได้ชื่อว่า มาตรฐาน 5200.28 หรือ TCSEC (Trusted Computing System Evaluation Criteria) หรือเป็นที่รู้จักทั่วไปว่า ออเรนจ์บุ๊ค (Orange Book) เหตุที่เรียกชื่อนี้เนื่องจากหนังสือมาตรฐานนี้มีปกสีส้มนั่นเอง ในมาตรฐานนี้ได้กำหนดระดับความปลอดภัยของคอมพิวเตอร์ออกเป็นระดับต่างๆ ได้ดังนี้

D – Minimal protection Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division.		
C – Discretionary protection		
	C1 – Discretionary Security Protection	■ Identification and authentication. ■ Separation of users and data. ■ Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis. ■ Required System Documentation and user manuals.
	C2 – Controlled Access Protection	■ More finely grained DAC. ■ Individual accountability through login procedures. ■ Audit trails. ■ Object reuse. ■ Resource isolation.
B – Mandatory protection		

	B1 – Labeled Security Protection	■ Informal statement of the security policy model. ■ Data sensitivity labels. ■ Mandatory Access Control (MAC) over selected subjects and objects. ■ Label exportation capabilities. ■ All discovered flaws must be removed or otherwise mitigated. ■ Design specifications and verification.
	B2 – Structured Protection	■ Security policy model clearly defined and formally documented. ■ DAC and MAC enforcement extended to all subjects and objects. ■ Covert storage channels are analyzed for occurrence and bandwidth. ■ Carefully structured into protection-critical and non-protection-critical elements. ■ Design and implementation enable more comprehensive testing and review. ■ Authentication mechanisms are strengthened. ■ Trusted facility management is provided with administrator and operator segregation. ■ Strict configuration management controls are imposed. ■ Operator and Administrator roles are separated.

	B3 – Security Domains	■ Satisfies reference monitor requirements. ■ Structured to exclude code not essential to security policy enforcement. ■ Significant system engineering directed toward minimizing complexity. ■ Security administrator role defined. ■ Audit security-relevant events. ■ Automated imminent intrusion detection, notification, and response. ■ Trusted system recovery procedures. ■ Covert timing channels are analyzed for occurrence and bandwidth. ■ An example of such a system is the XTS-300, a precursor to the XTS-400.
A – Verified protection		
	A1 – Verified Design	■ Functionally identical to B3. ■ Formal design and verification techniques including a formal top-level specification. ■ Formal management and distribution procedures. ■ Examples of A1-class systems are Honeywell's SCOMP, Aesec's GEMSOS, and Boeing's SNS Server. Two that were unevaluated were the production LOCK platform and the cancelled DEC VAX Security Kernel.

ในแต่ละระดับออเรนจ์บุ๊คได้กำหนดฟังก์ชันต่างๆ ที่ระบบต้องมีและการประกัน ดังนั้น ระบบที่ต้องการใบรับรองว่าจัดอยู่ในระดับใด ระบบนั้นต้องมีทั้งฟังก์ชันต่างๆ ที่กำหนดในระดับนั้น พร้อมทั้งการรับประกันในระดับนั้นได้ด้วย ข้อกำหนดเกี่ยวกับการรับประกันสำหรับระบบเพื่อให้เป็นไปตามมาตรฐานนั้น ต้องใช้เวลาและค่าใช้จ่ายสูงสำหรับบริษัทผู้ผลิต นี่เป็นผลที่ทำให้มีไม่กี่ระบบที่ได้รับการรับรองเหนือกว่าระดับ C2 ที่ผ่านมามีแค่ระบบเดียวเท่านั้นที่ได้รับใบรับรองในระดับ A1 นั่นคือ ระบบ Honeywell SCOMP แต่ระบบนี้ล้าสมัยไปในตอนที่ผ่านกระบวนการตรวจสอบเสร็จ

หลังจากนั้นได้มีการกำหนดมาตรฐานใหม่ขึ้นมาแทนออเรนจ์บุ๊ค เพื่อแก้ข้อบกพร่องในเรื่องของเวลาที่ใช้ในการตรวจทดสอบเพื่อออกใบรับรอง เช่น German Green Book (1989), Canadian Criteria (1990), ITSEC : Information Technology Security Evaluation Criteria (1991) และ Federal Criteria (1992) ซึ่งแต่ละมาตรฐานที่กล่าวมานี้ก็เพื่อกำหนดกระบวนการในการออกใบรับรองว่าระบบคอมพิวเตอร์นั้นมีความปลอดภัยระดับไหน อย่างไรก็ตามคอมพิวเตอร์มีวิวัฒนาการอย่างรวดเร็ว ระบบปฏิบัติการสมัยใหม่และฮาร์ดแวร์ใหม่ๆ ได้ถูกพัฒนาขึ้นมาแทนที่ระบบเก่าเร็วกว่าก่อนที่ระบบเก่าจะได้รับใบรับรอง

แต่สิ่งที่ยังขาดคือ กระบวนการสำหรับการตรวจทดลองเพื่อออกใบรับรองว่าระบบคอมพิวเตอร์นั้นปลอดภัย เทคโนโลยีมีการเปลี่ยนแปลงที่เร็วมากกว่าเวลา ที่ใช้กับกระบวนการตรวจทดลองความปลอดภัยของระบบ เพราะเป็นการยากมาก หรือแทบจะเป็นไปไม่ได้เลยเกี่ยวกับการที่จะพิสูจน์ว่าระบบใดปลอดภัยหรือไม่

การรักษาความปลอดภัยเครือข่าย (Network Security)

ปัญหาหนึ่งที่เกี่ยวกับการตรวจทดลอง เพื่อออกใบรับรองมาตรฐานระดับความปลอดภัยให้แก่ระบบคอมพิวเตอร์ก็คือ การขาดความเข้าใจเกี่ยวกับเรื่องเครือข่าย เมื่อคอมพิวเตอร์ถูกเชื่อมต่อกันเข้าเป็นเครือข่าย ปัญหาใหม่ก็เกิดขึ้น และปัญหาเก่าก็เกิดจากอีกทางหนึ่ง ยกตัวอย่างเช่น การสื่อสารคอมพิวเตอร์นั้นเปลี่ยนจาก WAN มาเป็นแบบ LAN ซึ่งมีแบนด์วิธที่สูงมาก และอาจมีหลายเครื่องที่เชื่อมต่อเข้ากับสื่อเดียวกัน การเข้ารหัสโดยใช้เครื่องเข้ารหัสเดี่ยวๆ อาจไม่ได้ผล การแผ่รังสีจากสายทองแดงที่ใช้สื่อสารนั้นมีสูงมาก เพราะสายทองแดงจะกระจายทั่วทั้งห้องหรือทั่วทั้งอาคารก็ได้ และสุดท้ายก็มีผู้ใช้หลายๆ คนที่สามารถล็อกอินได้จากหลายๆ ที่โดยอาจมีระบบบริหารจัดการที่เป็นศูนย์กลาง

ออเรนจ์บุ๊คไม่ได้มีข้อกำหนดเกี่ยวกับเครือข่ายคอมพิวเตอร์ ดังนั้น การเชื่อมต่อคอมพิวเตอร์เข้ากับเครือข่ายอาจทำให้ใบรับรองเป็นโมฆะหรือไม่มีประโยชน์ ทางออกสำหรับปัญหานี้คือ การใช้มาตรฐาน TNI (Trusted Network Interpretation) ของ TCSEC หรือที่รู้จักในชื่อ เร้ดบุ๊ค (Red Book) ซึ่งออกมาในปี 1987 ข้อกำหนดในเร้ดบุ๊คมาจากออเรนจ์บุ๊คทั้งหมด และได้เพิ่มส่วนที่เกี่ยวข้องกับเครือข่ายเข้าไป อย่างไรก็ตามเนื่องจากมีข้อกำหนดเกี่ยวกับฟังก์ชันและการรับประกันมากทำให้ใช้เวลามาก เกินไปในการตรวจทดลองระบบ โดยจะมีเพียงบางระบบเท่านั้นที่ผ่านการตรวจทดลองของ TNI และในระบบที่ได้รับใบรับรองนั้นไม่มีระบบใดเลยที่ใช้ในเชิงพาณิชย์

การรักษาความปลอดภัยข้อมูล (Information Security)

จากประวัติศาสตร์ที่ได้กล่าวมานั้น เราสามารถสรุปได้ว่าไม่มีวิธีการใดที่สามารถแก้ปัญหาเกี่ยวกับการรักษาความปลอดภัยได้ทั้งหมด แท้ที่จริงแล้วการรักษาความปลอดภัยที่ดีนั้นจะต้องใช้ทุกๆ วิธีการที่กล่าวมาร่วมกัน การรักษาความปลอดภัยทางด้านกายภาพ ก็ยังเป็นวิธีการที่ดีสำหรับการปกป้องทรัพย์สินที่เป็นวัตถุ การรักษาความปลอดภัยด้านการสื่อสาร (COMSEC) เป็นวิธีที่ใช้ปกป้องข้อมูลในระหว่างการสื่อสาร การรักษาความปลอดภัยเกี่ยวกับการแผ่รังสี (EMSEC) เป็นสิ่งที่จำเป็น เมื่อฝ่ายตรงกันข้ามมีเครื่องมือที่สามารถอ่านข้อมูลจากรังสีที่แผ่ออกจากระบบคอมพิวเตอร์ การรักษาความปลอดภัยคอมพิวเตอร์ (COMPSEC) เป็นสิ่งที่จำเป็นสำหรับการควบคุมการเข้าถึงระบบคอมพิวเตอร์ และการรักษาความปลอดภัยเครือข่าย (NETSEC) ก็เป็นสิ่งที่จำเป็นสำหรับการควบคุมการใช้งานเครือข่าย และวิธีการที่กล่าวมาทั้งหมดนี้รวมกัน ก็สามารถให้บริการการรักษาความปลอดภัยข้อมูล (INFOSEC) ได้

การรักษาความปลอดภัยข้อมูลนั้นเป็นการปกป้องคุณสมบัติทั้ง 3 ด้านของข้อมูล ซึ่งได้แก่ ความลับ ความถูกต้อง และความพร้อมใช้งาน การรักษาความลับของข้อมูล หมายถึง การอนุญาตให้เฉพาะผู้มีสิทธิ์เท่านั้นที่จะเข้าถึงข้อมูลได้ ส่วนการรักษาความถูกต้องของข้อมูล หมายถึง การอนุญาตให้เฉพาะผู้ที่มีสิทธิ์เท่านั้นที่สามารถแก้ไขข้อมูลได้ และด้านสุดท้ายคือ ความพร้อมใช้งาน ซึ่งผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้เมื่อต้องการ

เนื่องจากข้อมูลปัจจุบันจะอยู่ในรูปแบบดิจิตอล และอาจถูกจัดเก็บไว้ในมีเดียหรือฮาร์ดดิสก์ในเครื่องคอมพิวเตอร์ หรืออาจอยู่ในระหว่างการประมวลผลในระบบคอมพิวเตอร์ หรืออาจอยู่ระหว่างการส่งผ่านเครือข่าย หรืออาจบันทึกไว้บนกระดาษหรือกระดานประกาศข่าวก็ได้ ไม่ว่าข้อมูลจะอยู่ที่แห่งใด การรักษาความปลอดข้อมูลนั้นจำเป็นต้องมีอยู่เสมอ ดังนั้น มาตรการรักษาความปลอดภัยทั้งหมดที่กล่าวมา จึงมีความจำเป็นสำหรับการปกป้องคุณสมบัติทั้ง 3 ด้านของข้อมูลนั่นเอง

การรักษาความปลอดภัยไซเบอร์ (Cybersecurity)

การรักษาความปลอดภัยไซเบอร์ หมายถึง การใช้เทคโนโลยีและกระบวนการในการป้องกันระบบคอมพิวเตอร์ เครือข่าย และข้อมูล จากการเข้าถึงโดยไม่ได้รับอนุญาต หรืออีกนัยหนึ่งคือ การป้องกันอันตรายในโลกออนไลน์ ที่มีผลกระทบต่อตัวผู้ใช้งานและข้อมูลซึ่งเป็นทรัพย์สินประเภทหนึ่ง ซึ่งในปัจจุบันมีผู้ใช้งานออนไลน์ทั่วโลกเพิ่มมากขึ้น ทั้งนี้เนื่องมาจากปัจจัยหลายๆ ด้าน ไม่ว่าจะเป็นอัตราค่าบริการที่ถูกลง หรือการเพิ่มขึ้นของอุปกรณ์พกพาต่างๆ เช่น สมาร์ทโฟนและแท็บเล็ต เป็นต้น

ไซเบอร์ (Cyber) คือ คำที่กร่อนมาจากคำว่า ไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายหรือสังคมเครือข่าย เช่น ระบบอินเทอร์เน็ต ไซเบอร์เนติกส์ เป็นวิชาการที่ศึกษาเกี่ยวกับระบบควบคุมของสิ่งมีชีวิต เช่น ระบบประสาทของสิ่งมีชีวิต เพื่อนำไปใช้ประยุกต์ใช้กับระบบที่มนุษย์สร้างขึ้นหรือระบบอิเล็กทรอนิกส์ วิชานี้เปรียบเทียบความคล้ายคลึงกันระหว่างสิ่งมีชีวิตกับสิ่งไม่มีชีวิต และยึดหลักการพื้นฐานทางด้านการสื่อสารและการควบคุม ที่สามารถอธิบายการทำงานของทั้งสิ่งมีชีวิตและสิ่งไม่มีชีวิตได้ ชื่อของวิชานี้มาจากคำภาษากรีก หมายความว่า นำหรือปกครอง ทั้งนี้มีคำหรือกลุ่มคำที่มีความหมายใกล้เคียงและมีความสัมพันธ์กัน ได้แก่ Electronic, Cyber และ Virtuality ซึ่งมักใช้นำหน้าผลิตภัณฑ์หรือการบริการ ที่มีระบบอิเล็กทรอนิกส์หรือคอมพิวเตอร์เป็นส่วนประกอบสำคัญ เช่น E- ย่อมาจาก อิเล็กทรอนิกส์ (Electronic) ใช้ในนำหน้าผลิตภัณฑ์หรือบริการที่อยู่ในรูปของอิเล็กทรอนิกส์ เช่น จดหมายอิเล็กทรอนิกส์ (E-mail), การค้าอิเล็กทรอนิกส์ (E-commerce), ธุรกิจอิเล็กทรอนิกส์ (E-business), การธนาคารอิเล็กทรอนิกส์ (E-banking) และหนังสืออิเล็กทรอนิกส์ (E-book) เป็นต้น ปัจจุบันมีความนิยมที่จะใช้คำว่า ไซเบอร์ (Cyber) แทนคำว่าอิเล็กทรอนิกส์นั่นเอง

ไซเบอร์ เป็นคำนำหน้านามที่กร่อนมาจากคำว่า ไซเบอร์เนติกส์ (Cybernetics) เป็นคำมาจากภาษากรีก แปลว่าความสามารถในการนำ (Steering) หรือการปกครอง (Governing) ทั้งนี้ไซเบอร์เนติกส์ยังมีความหมายในการควบคุมการพูดและกระบวนการในการทำงานของสมอง ซึ่งนำไปใช้ในเรื่องเกี่ยวกับคอมพิวเตอร์และอิเล็กทรอนิกส์ ในการทำงานของระบบควบคุมระยะไกล หรือการควบคุมแบบเครือข่ายอิเล็กทรอนิกส์ และเมื่อนำไปใช้ในคำว่า ไซเบอร์สเปซ (Cyberspace) มีความหมายครอบคลุมถึงขอบเขตการทำงานของระบบเครือข่ายคอมพิวเตอร์ หรือระบบอิเล็กทรอนิกส์ระยะไกล ซึ่งมีความหมายเหมือนกับคำว่า เวอร์ชวลสเปซ (Virtual Space) หรือเวอร์ชวลยูนิเวิร์ส (Virtual Universe)

โดยรวมแล้วไซเบอร์จึงเป็นความหมายในเชิงนามธรรม หมายถึง ขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ ซึ่งจะครอบคลุมมากกว่าคอมพิวเตอร์ ซึ่งมีความหมายในเชิงรูปธรรมของอุปกรณ์ระบบคอมพิวเตอร์ทั่วไป แต่หากเปรียบเทียบกับระบบข้อมูลข่าวสาร (Information System) สามารถกำหนดให้ไซเบอร์เป็นส่วนหนึ่ง หรือสับเซตของระบบข้อมูลข่าวสารได้ แต่หากว่าในทางปฏิบัติเพื่อรักษาความปลอดภัยของระบบข้อมูลข่าวสาร ไซเบอร์สเปซและเครือข่ายคอมพิวเตอร์นั้นไม่สามารถแยกแยะออกจากกันได้ ไซเบอร์สเปซเป็นขอบเขตที่กำหนดโดยการใช้อุปกรณ์อิเล็กทรอนิกส์ และแถบคลื่นแม่เหล็กไฟฟ้าในการจัดเก็บ แก้ไขเปลี่ยนแปลง และแลกเปลี่ยนข้อมูล ผ่านทางระบบเครือข่ายและโครงสร้างพื้นฐานทางกายภาพที่เกี่ยวข้อง

การรักษาความปลอดภัยไซเบอร์ (Cyber Security หรือ Cybersecurity) คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยงและความเสียหาย ที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้การรักษาความปลอดภัยไซเบอร์ยังรวมถึงการระวังป้องกันต่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่างๆ

สงครามไซเบอร์ (Cyber Warfare)

การนำเทคโนโลยีสารสนเทศมาใช้ทางด้านการทหารอย่างแพร่หลาย จนทำให้กองทัพต้องปรับเปลี่ยนรูปแบบในการทำสงครามแบบใหม่ หรือที่เรียกว่ายุคการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ซึ่งเป็นยุคที่จำเป็นต้องใช้เทคโนโลยีสารสนเทศและการสื่อสารเข้ามาเป็นองค์ประกอบที่สำคัญในการขับเคลื่อนปฏิบัติการทางทหาร ยกตัวอย่าง เช่น ระบบบัญชาการและควบคุม ระบบเชื่อมโยงข้อมูลทางยุทธวิธี ระบบป้องกันภัยทางอากาศ ระบบอาวุธยุทโธปกรณ์ และระบบส่งกำลังบำรุง เป็นต้น การใช้ประโยชน์จากเทคโนโลยีสารสนเทศจะช่วยเพิ่มประสิทธิภาพในการปฏิบัติการอย่างไรก็ตามระบบต่างๆ เหล่านี้มีความเสี่ยงสูงที่จะเป็นเป้าหมายของการถูกโจมตีผ่านทางไซเบอร์สเปซ จนปัจจุบันได้เกิดการทำสงครามรูปแบบใหม่ ที่เรียกว่า สงครามไซเบอร์ (Cyber Warfare) ซึ่งเป็นการปฏิบัติการสงครามที่เกิดขึ้นในโลกไซเบอร์แต่ส่งผลกระทบในโลกจริง

ตัวอย่างที่เห็นชัดเจนคือ กรณีของสตักซ์เน็ต (Stuxnet) ซึ่งเป็นอาวุธไซเบอร์ชนิดหนึ่ง สามารถทำลายโรงงานผลิตอาวุธนิวเคลียร์ของประเทศอิหร่านได้ จากตัวอย่างกรณีนี้และอีกหลายๆ เหตุการณ์ ทำให้หลายประเทศได้เห็นความสำคัญ และเริ่มกระบวนการพัฒนาอาวุธไซเบอร์เพื่อใช้โจมตีเป้าหมายทางทหารบางประเภท ดังนั้น กองทัพจึงมีความจำเป็นอย่างยิ่งที่ต้องเตรียมการในการป้องกันการโจมตีจากไซเบอร์สเปซ และในขณะเดียวกันจำเป็นที่ต้องพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ ซึ่งจะเป็นการทวีกำลังทางทหารในการต่อสู้ในสงครามรูปแบบใหม่ที่จะเกิดขึ้นอย่างแน่นอนในอนาคตอันใกล้

หลักการพื้นฐานของการรักษาความปลอดภัยข้อมูล

การที่จะบอกได้ว่าข้อมูลนั้นมีความปลอดภัยหรือไม่ ก็โดยการวิเคราะห์คุณสมบัติหลักทั้ง 3 ด้านคือ ความลับ ความถูกต้อง และความพร้อมใช้งานว่ามีอยู่ครบหรือไม่ ถ้าขาดคุณสมบัติด้านใดด้านหนึ่งก็แสดงว่าข้อมูลนั้นไม่มีความปลอดภัย ดังนั้น การรักษาความปลอดภัยข้อมูลจึงเป็นการปกป้องรักษาคุณสมบัติทั้ง 3 ด้านดังต่อไปนี้

- **ความลับ** (Confidentiality) : หมายถึง ข้อมูลสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- **ความถูกต้อง** (Integrity) : หมายถึง ข้อมูลสามารถถูกแก้ไขได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- **ความพร้อมใช้งาน** (Availability) : หมายถึง ข้อมูลสามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเมื่อต้องการ

รูปที่ 1.3 : คุณสมบัติของความปลอดภัยข้อมูล

ความลับ (Confidentiality)

การรักษาความลับของข้อมูล หมายถึง การอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้ หรือถ้ามองอีกมุมหนึ่งก็จะหมายถึง การปกป้องข้อมูลไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้นั่นเอง ข้อมูลบางอย่างมีความสำคัญและจำเป็นต้องเก็บไว้เป็นความลับ เพราะถ้าถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตรายต่อเจ้าของได้

Master in SECURITY 3rd Edition

ปัจจุบันเราได้ดำเนินชีวิตในโลกไซเบอร์ควบคู่กับการดำเนินชีวิตประจำวัน ระบบไอทีช่วยให้ชีวิตง่ายขึ้น แต่ก็เป็นอาวุธที่กำลังทำลายเราด้วยเช่นกัน มาสเตอร์อินซีเคียวริตี้ เป็นหนังสือที่จะแนะนำท่านให้รู้จักภัยคุกคามด้านไซเบอร์และแนวทางการป้องกันที่ได้ผล เริ่มตั้งแต่สิ่งที่คุ้นเคยคือ ไวรัส ไปจนถึงแฮคเกอร์ที่พยายามจะขโมยข้อมูลของเราหรือองค์กร หรือแม้กระทั่งบางประเทศก็พัฒนาอาวุธเพื่อโจมตีในไซเบอร์ได้ ส่วนแนวทางการป้องกันนั้นก็จะใช้หลักการป้องกันเชิงลึก โดยวิเคราะห์สาเหตุแล้วนำเอามาตรการป้องกันหรือเครื่องมือมาใช้ หนังสือเล่มนี้ได้รวบรวมข้อมูลสำคัญไว้ถึง 5 Part หลักๆ ที่จะช่วยพัฒนาทักษะและความรู้ จนคุณกลายเป็นผู้ดูแลระบบเครือข่ายมืออาชีพได้อย่างไม่ยากนัก

I : Information Security

บทที่ 1 Introduction to Cybersecurity หลักการในการรักษาความปลอดภัยคือ การรักษาไว้ซึ่งความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability)

บทที่ 2 Information Security Governance การบริหารจัดการด้านการรักษาความปลอดภัยข้อมูล เป็นสิ่งที่องค์กรจะต้องทำควบคู่กับการบริหารองค์กร โดยกระบวนการที่เป็นมาตรฐานและเป็นที่ยอมรับ ได้แก่ ISO 27001, ISO 17799, COBIT, ITIL

บทที่ 3 Risk Management การบริหารความเสี่ยงเป็นเครื่องมือที่สำคัญสำหรับผู้บริหารองค์กร เนื่องจากภัยคุกคามด้านไซเบอร์ได้มีการพัฒนาและเปลี่ยนแปลงมากขึ้น จนทำให้องค์กรต้องบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

บทที่ 4 Access Control เพื่อความปลอดภัยของระบบ จำเป็นต้องมีการควบคุมการเข้าถึง เช่น การกำหนดให้มีการล็อกอินเข้าใช้งานระบบ แต่ก่อนอื่นจะต้องมีบัญชีผู้ใช้ และสิ่งที่ใช้พิสูจน์ทราบตัวตนนั้นมี 3 แบบคือ สิ่งที่คุณรู้ สิ่งที่คุณมี และสิ่งที่คุณเป็น

บทที่ 5 Cryptography การเข้ารหัสข้อมูล (Encryption) ช่วยปกป้องความลับของข้อมูล ผู้มีคีย์ (Key) เท่านั้นจึงจะเข้าถึงเนื้อหาของข้อมูลได้ มาตรฐานการเข้ารหัสข้อมูลที่ได้รับความนิยม เช่น AES, RSA, DH, DSA, SHA, MD5 เป็นต้น

II : Network Security

บทที่ 6 Network Security การรักษาความปลอดภัยในระดับเน็ตเวิร์คนั้น สามารถทำได้โดยการเข้ารหัสข้อมูลในแพ็กเก็ตที่รับส่งผ่านเครือข่าย ในระดับเน็ตเวิร์คนั้นก็จะใช้โปรโตคอล IPSec ซึ่งเข้ารหัสข้อมูลด้วยอัลกอริทึม AES ระดับแอพพลิเคชันก็ใช้ S/MIME เพื่อเข้ารหัสข้อมูลสำหรับอีเมล ส่วนเว็บนั้นก็จะใช้ HTTPS เพื่อเข้ารหัสข้อมูลผ่านโปรโตคอล SSL

บทที่ 7 Wireless LAN Security ไวร์เลสแลนถูกใช้งานกันอย่างแพร่หลาย เนื่องจากความสะดวกในการใช้งาน แต่การใช้ไวร์เลสแลนที่ปลอดภัยนั้น จะต้องมีการพิสูจน์ทราบตัวตนของผู้ใช้ และมีการเข้ารหัสข้อมูล

บทที่ 8 Firewall ถูกใช้เพื่อปกป้องเครือข่ายภายในจากการโจมตี ไฟร์วอลล์ใช้วิธีการบล็อคพอร์ตที่ไม่มีการใช้งานนั้นล้าสมัยแล้ว ปัจจุบันไฟร์วอลล์ได้ถูกพัฒนาจนให้ทราบรูปแบบการทำงานของโปรโตคอลต่างๆ อย่างละเอียด ช่วยปกป้องการถูกโจมตีได้ดียิ่งขึ้น

บทที่ 9 Intrusion Detection System อุปกรณ์ที่คอยเฝ้าระวังหรือมอนิเตอร์สิ่งที่ผิดปกติที่เกิดขึ้นในเครือข่ายแล้วแจ้งเตือนภัย อุปกรณ์ที่ว่านี้คือ IDS และอุปกรณ์ที่มีความสามารถในการป้องกันภัยได้ก็จะเรียกว่า IPS ทั้งสองช่วยปกป้องเครือข่ายได้ดียิ่งขึ้น

III : Malware and Hacker

บทที่ 10 Malware ภัยคุกคามที่สร้างปัญหาให้กับระบบไอทีมากที่สุดคือ ไวรัสหรือมัลแวร์ ซึ่งจะใช้ประโยชน์จากช่องโหว่ของระบบ ปัจจุบันมีการพัฒนาไปถึงขั้นที่เรียกว่า APT (Advance Persistent Threat) โดยใช้เทคนิคขั้นสูงและหลากหลายยากต่อการป้องกัน

บทที่ 11 Hacking เครื่องมือที่ใช้สำหรับการเจาะระบบนั้น สามารถค้นหาและดาวน์โหลดมาใช้งานได้ง่าย แม้แต่ผู้ที่ไม่มีความชำนาญเกี่ยวกับคอมพิวเตอร์เลยก็สามารถใช้เครื่องมือเหล่านี้ได้ การป้องกันที่ดีที่สุดคือ การติดตั้งแพตช์ เพื่อปิดช่องโหว่ของระบบ หรือแอพพลิเคชันที่ติดตั้งในเครื่องนั้น

บทที่ 12 System Recovery หลังจากเครื่องคอมพิวเตอร์หรือระบบถูกโจมตีจากไวรัสหรือแฮคเกอร์นั้น ก็จะทำให้ระบบไม่สามารถทำงานได้เป็นปกติ การกำจัดมัลแวร์หรือแบ็คดอร์ที่แฮคเกอร์ทิ้งไว้เพื่อไม่ให้เป็นช่องทางเข้ามาใช้งานในภายหลัง การแบ็คอัพข้อมูลจะช่วยให้การกู้คืนระบบสะดวกและรวดเร็วยิ่งขึ้น

IV : Endpoint Security

บทที่ 13 Windows Security ภัยคุกคามหลักของการใช้งานระบบวินโดวส์คือ ไวรัส ซึ่งใช้ประโยชน์จากช่องโหว่ ไมโครซอฟท์พยายามออกแพตช์ให้เร็วที่สุด แต่ผู้ใช้งานต้องดาวน์โหลดแพตช์มาติดตั้ง และควรใช้ซอฟต์แวร์ป้องกันไวรัส และมีการสแกนระบบเป็นประจำ

บทที่ 14 Linux Security ภัยคุกคามหลักของลีนุกซ์นั้นไม่ใช่ไวรัส แต่เป็นแฮคเกอร์หรือบอตเน็ตที่คอยสแกนหาโฮสต์ที่ไม่ได้ติดตั้งแพตช์หรือช่องโหว่ ผู้ดูแลระบบจำจะต้องดาวน์โหลดมาติดตั้งแพตช์ด้วยตนเอง เนื่องจากไม่มีเครื่องมืออัตโนมัตินั่นทำให้ลีนุกซ์มีช่องโหว่มากเช่นกัน

V : Physical Security, Cyber Law & Cyber Warfare

บทที่ 15 Physical Security คือ การปกป้องระบบไอทีจากภัยธรรมชาติและการกระทำของคน ศูนย์กลางของระบบไอทีคือ ดาต้าเซ็นเตอร์ ซึ่งมีเซิร์ฟเวอร์และคอร์สวิตช์ของเน็ตเวิร์ค สิ่งหลักที่ต้องดูแลคือ ระบบไฟฟ้า ระบบปรับอากาศ การป้องกันอัคคีภัย ระบบควบคุมการเข้าออก เป็นต้น

บทที่ 16 Cyber Law การปฏิบัติตามกฎหมายหรือระเบียบต่างๆ นั้นก็เป็นสิ่งที่สำคัญ โดยเฉพาะปัจจุบันประเทศไทยมี พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งรับรองให้สามารถใช้หลักฐานดิจิตอลเพื่อใช้ในคดีความในศาลยุติธรรมได้

บทที่ 17 Cyber Warfare ภัยคุกคามด้านไซเบอร์นั้นได้ทวีความรุนแรงขึ้น ผู้ก่อการร้ายอาจใช้ประโยชน์จากอาวุธไซเบอร์ในการก่ออุตสาหกรรม ที่มุ่งเป้าไปที่การทำลายที่มีผลกระทบในวงกว้าง เช่น ระบบจ่ายไฟฟ้า โครงข่ายสื่อสาร บางประเทศได้พัฒนาศักยภาพในการทำสงครามไซเบอร์ เพื่อให้เป็นการปฏิบัติการที่ควบคู่ไปกับการทำสงครามตามแบบ การปฏิบัติการสงครามไซเบอร์ เป็นการทวีกำลังทางทหารในการต่อสู้แบบเบ็ดเสร็จกับข้าศึก

ประวัติผู้แต่ง น.ท. จตุชัย แพงจันทร์ CISSP, CISM, CISA

- สำเร็จการศึกษาระดับปริญญาตรี สาขาวิศวกรรมไฟฟ้า (B.S. EE) จากโรงเรียนนายเรืออากาศสหรัฐฯ (USAF Academy, USA)
- ปริญญาโท สาขาวิศวกรรมคอมพิวเตอร์ (M.S. Comp Eng) จากมหาวิทยาลัยมินเนโซต้า (U of M, USA) ปัจจุบันรับราชการที่กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ เป็นผู้แต่งหนังสือ เจาะระบบ Network 3rd Edition และมีประสบการณ์ด้าน Network และ Security กว่ายี่สิบปี

info PRESS
MASTER GUIDE

ผู้แต่ง จตุชัย แพงจันทร์
บรรณาธิการ อรรณพ ขันธิกุล

จัดจำหน่ายโดย IDC PREMIER
ISBN 885-916-100-437-0
8 859161 004370
450 บาท