แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ของภาคเอกชนตามยุทธศาสตร์ไซเบอร์แห่งชาติ

โดย

นายณัทฐรัชต์ อัศวปัญญาวงศ์
ประธานกรรมการ
กลุ่มบริษัทไทยมาสเตอร์กรุ๊ป

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๐
ประจำปีการศึกษา พุทธศักราช ๒๕๖๐ - ๒๕๖๑

บทคัดย่อ

เรื่อง แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ของภาคเอกชนตามยุทธศาสตร์ไซเบอร์แห่งชาติ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

ผู้วิจัย นายณัทฐรัชต์ อัศวปัญญาวงศ์ **หลักสูตร วปอ.** **รุ่นที่** ๖๐

เพื่อศึกษาและหาแนวทางในการจัดการอย่างเหมาะสมกับภัยคุกคามทางไซเบอร์ต่อภาคเอกชน และเสนอแนะแนวทางที่ภาคเอกชนสามารถสร้างระบบรักษาความปลอดภัยทางไซเบอร์ได้เหมาะสมกับองค์กร ทั้งด้านขนาดและงบประมาณให้สอดคล้องกับยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยทำการศึกษาเนื้อหาเกี่ยวกับ แนวคิด รูปแบบ ทฤษฎีที่เกี่ยวข้องกับการกำหนดนโยบายความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ของภาคเอกชน ข้อมูลยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติและดำเนินการสัมภาษณ์กลุ่มผู้เชี่ยวชาญที่มีความสามารถทางด้านวิชาการ ด้านการบริหาร และผู้ที่มีประสบการณ์ในการจัดทำระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับภาคเอกชน วิธีดำเนินการวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีการดำเนินการรวบรวมข้อมูลเรื่องแนวคิด ทฤษฎี รวมถึงวรรณกรรมที่เกี่ยวข้องกับแนวทางการป้องกันภัยคุกคามและการสร้างความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิมาจัดระเบียบและวิเคราะห์ข้อมูลทั้งหมดที่ได้มาตามขั้นตอนการวิจัยเชิงคุณภาพ นำข้อมูลมาวิเคราะห์ เพื่อแยกแยะให้เห็นถึงส่วนประกอบและความสัมพันธ์ระหว่างส่วนประกอบต่างๆ เหล่านั้น โดยมุ่งเน้นความชัดเจน ความเฉพาะเจาะจง และความสามารถในการแปลงไปสู่แผนการปฏิบัติตามความเหมาะสมของเนื้อหากับกรอบเวลา จากผลการวิจัยสามารถสรุปแนวปฏิบัติในการจัดการได้ดังนี้ กำหนดมาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ตามมาตรฐานสากล โดยสร้างกรอบและแนวทางการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ สำหรับข้อเสนอแนะของการวิจัยสามารถจำแนกตามประเภท ได้แก่ ข้อเสนอแนะเชิงนโยบายและแผน ข้อเสนอแนะเชิงกฎ ระเบียบ และกฎหมายที่เกี่ยวข้อง ข้อเสนอแนะเชิงปฏิบัติการ

ABSTRACT

Title An approach to creating cyber security measures of the private sector, based on national cyber strategies

Field Science and Technology

Name Mr.Nattharatch Aswapanyawongse **Course** NDC **Class** 60

This research was to study and find appropriate ways to manage cyber threats to the private sector it also offers advice on how the private sector can create cyber security, the size and budget be consistent with the national cyber security strategy. Study the content of theoretical concepts related to policy making, security, and cyber threats of the private sector, national cyber security strategy and conduct interviews with experts who are academically competent, management and professional influencer who have experience in developing cyber security systems for the private sector. This research is a qualitative research that collects information on theories, and literature related to prevent of cyber threats and cyber security. Organize and analyze all the data acquired by the qualitative research process, analyze the data to distinguish the components and relationships between the components. Focus on clarity, specificity, and the ability to transform into a plan of action that is appropriate to the time frame. The results of the research can be summarized as follows: Specify cyber security measures in accordance with international standards, establishing a framework and guidelines for safeguarding cyber security. Research recommendations can be categorized by policy and plan recommendations, regulatory recommendations, and related laws action recommendations.

คำนำ

เทคโนโลยีสารสนเทศและการสื่อสาร ได้พัฒนาขึ้นในช่วงสองทศวรรษที่ผ่านมาอย่างก้าวกระโดดและปัจจุบันได้เข้ากับวิถีชีวิตของมนุษย์ในทุกมิติ ซึ่งประเทศไทยได้ก้าวเข้าสู่ยุคดิจิทัลที่มีเศรษฐกิจสังคมและชีวิตประจำวันของประชาชนที่ขึ้นอยู่กับเทคโนโลยีดิจิทัลอย่างมาก ทำให้ประเทศต้องพึ่งพิงเทคโนโลยีดิจิทัล ทั้งเศรษฐกิจและการบริหารราชการแผ่นดินของรัฐบาล รวมทั้งการให้บริการสาธารณะที่จำเป็น ซึ่งปัจจุบันเทคโนโลยีที่สำคัญกับชีวิตประจำวันของเราต่างมีการเชื่อมต่อกับอินเทอร์เน็ตที่อาจเสี่ยงต่อการถูกแทรกแซงและทำลายได้ ดังนั้นจึงจำเป็นที่จะต้องมีแนวทางในการป้องกันอย่างรอบด้าน เพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ การขยายตัวของการโจมตีทางไซเบอร์ทั่วโลกเกิดขึ้นอย่างรวดเร็ว บ่อยครั้งและรุนแรง ซึ่งจะส่งผลต่อการลุกลามของอาชญกรรมไซเบอร์ และจะมีผลกระทบต่อเศรษฐกิจของประเทศทุกประเทศที่กำลังเข้าสู่ยุคอุตสาหกรรม ๔.๐ ซึ่งมีแนวโน้มที่ชัดเจนว่าอาชญากรรมไซเบอร์กำลังเพิ่มมากขึ้น การสร้างความมั่นคงปลอดภัยไซเบอร์ จึงไม่ใช่เรื่องแค่เป็นวิสัยทัศน์อีกต่อไป เพราะหากไม่ลงมือสร้างขีดความสามารถด้านบุคลากรและเครื่องมือทางเทคโนโลยี ประเทศไทยของเราก็จะประสบกับภัยคุกคามทางไซเบอร์ในอนาคตอย่างแน่นอน

……..…….……

(นายณัทฐรัชต์ อัศวปัญญาวงศ์)

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตร วปอ. รุ่นที่ ๖๐

ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญแผนภาพ

บทที่ ๑

บทนำ

ความเป็นมาและความสำคัญของปัญหา

เทคโนโลยีสารสนเทศและการสื่อสาร ได้พัฒนาขึ้นในช่วงสองทศวรรษที่ผ่านมาอย่างก้าวกระโดดและปัจจุบันได้เข้ากับวิถีชีวิตของมนุษย์ในทุกมิติ ซึ่งประเทศไทยได้ก้าวเข้าสู่ยุคดิจิทัลที่มีเศรษฐกิจสังคมและชีวิตประจำวันของประชาชนที่ขึ้นอยู่กับเทคโนโลยีดิจิทัลอย่างมาก ทำให้ประเทศต้องพึ่งพิงเทคโนโลยีดิจิทัล ทั้งเศรษฐกิจและการบริหารราชการแผ่นดินของรัฐบาล รวมทั้งการให้บริการสาธารณะที่จำเป็น ซึ่งปัจจุบันขึ้นอยู่กับความมั่นคงของโลกไซเบอร์และโครงสร้างพื้นฐานดิจิทัล ภัยคุกคามต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศมาจากฮาร์ดแวร์และซอฟแวร์ส่วนใหญ่ที่พัฒนาขึ้นเพื่ออำนวยความสะดวกไม่ได้มีการออกแบบที่มีความปลอดภัยมาตั้งแต่ต้นอย่างเหมาะสม จึงทำให้ผู้โจมตีไม่ว่าจะเป็นรัฐที่เป็นฝ่ายตรงข้ามองค์กรอาชญากรรมหรือผู้ก่อการร้าย และแม้แต่บุคคลทั่วไปก็สามารถใช้ช่องว่างระหว่างความสะดวกและปลอดภัยในการโจมตีได้ ดังนั้นการลดช่องว่างและความเสี่ยงทางไซเบอร์จึงควรได้รับการให้ความสำคัญเป็นอันดับแรก การขยายตัวของอินเทอร์เน็ตที่เชื่อมโยงกับคอมพิวเตอร์และโทรศัพท์เคลื่อนที่มาสู่การใช้งานในระบบอัจฉริยะนั้นเป็นการขยายขอบเขตของการคุกคามทางไซเบอร์ ซึ่งระบบและเทคโนโลยีที่สำคัญกับชีวิตประจำวันของเรา เช่น ระบบการผลิตไฟฟ้า, ระบบควบคุมการจราจรทางอากาศ, ดาวเทียม, เทคโนโลยีทางการแพทย์, โรงงานอุตสาหกรรม และระบบการขนส่ง ต่างมีการเชื่อมต่อกับอินเทอร์เน็ตที่อาจเสี่ยงต่อการถูกแทรกแซงและทำลายได้ ภัยคุกคามด้านไซเบอร์ที่เกิดจากช่องโหว่ที่มีและช่องว่างในขีดความสามารถและการป้องกันของประเทศ ทำให้รัฐบาลต้องเล็งเห็นถึงความสำคัญ เพื่อให้สามารถตอบโต้ได้อย่างเท่าทันต่อภัยคุกคามทางไซเบอร์ โดยจำเป็นที่จะต้องมีแนวทางในการป้องกันอย่างรอบด้านเพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ ควรมีการแก้ปัญหาในภาคธุรกิจและภาคอุตสาหกรรมของเอกชนควบคู่ไปกับภาครัฐโดยอาศัยการประเมินดังต่อไปนี้

๑. ขนาดและเครือข่ายหรือภัยคุกคามทางไซเบอร์ และช่องโหว่ของประเทศ ซึ่งหมายความว่าการใช้แนวทางในปัจจุบัน อาจจะไม่เพียงพอที่จะทำให้ประเทศปลอดภัย

๒. แนวทางที่ขึ้นกับตลาด (Market Based Approach) ทำให้เกิดการลงทุนในภาคเอกชนเพื่อสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ รัฐบาลต้องเป็นผู้นำและแทรกแซงโดยตรง โดยการสร้างกลไกด้านการลงทุนและการนำทรัพยากรที่มีอยู่ไปใช้เพื่อแก้ปัญหาภัยคุกคามทางไซเบอร์

๓. การที่รัฐบาลดำเนินการเพียงฝ่ายเดียวนั้น ไม่สามารถทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ได้ในทุกด้าน ดังนั้นแนวทางสร้างความร่วมมือกับทุกภาคส่วนจึงเป็นสิ่งจำเป็น

๔. ประเทศไทยจำเป็นต้องมีหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ตื่นตัวและสนับสนุนทักษะและขีดความสามารถต่างๆ ที่สามารถก้าวให้ทันและเผชิญกับภัยคุกคามที่กำลังเปลี่ยนแปลงได้

การขยายตัวของการโจมตีทางไซเบอร์ทั่วโลกเกิดขึ้นอย่างรวดเร็ว, บ่อยครั้ง และรุนแรง ซึ่งจะส่งผลต่อการลุกลามของอาชญากรรมไซเบอร์ และจะมีผลกระทบต่อเศรษฐกิจของประเทศทุกประเทศที่กำลังเข้าสู่ยุคอุตสาหกรรม ๔.๐ ซึ่งมีแนวโน้มที่ชัดเจนว่าอาชญากรรมไซเบอร์กำลังเพิ่มมากขึ้นเป็นจำนวนมาก การสร้างความมั่นคงปลอดภัยไซเบอร์ จึงไม่ใช่เรื่องแค่เป็นวิสัยทัศน์อีกต่อไปเพราะหากไม่ลงมือสร้างขีดความสามารถด้านบุคลากรและเครื่องมือทางเทคโนโลยี ประเทศไทยของเราก็จะประสบกับภัยคุกคามทางไซเบอร์ในอนาคตอย่างแน่นอน เนื่องจากภัยคุกคามทางไซเบอร์เริ่มปรากฏชัดที่กำลังจะมีผลกระทบต่อสถาบันหลักของประเทศไทย ดังนั้นประเทศไทยจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการดำเนินการบัญญัติกฎหมายที่เกี่ยวข้อง ในการเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์ และจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างเร่งด่วนเพื่อให้ทันต่อการเติบโตของภัยคุกคามด้านไซเบอร์ในอนาคต ดังนั้นยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรมีการจัดการแบบองค์รวม และมีความสามารถในการรับมือกับการโจมตีในแง่มุมต่างๆ โดยคำนึงถึงวิธีการทั้งในเรื่องการป้องกัน, การตอบสนอง และลดผลกระทบแผนดำเนินการที่มีประสิทธิผลในการสร้างกลยุทธ์ควรมีขั้นตอนที่จะเพิ่มความตระหนัก และยกระดับของความเข้าใจในหมู่ประชาชนทั่วไปด้วยการให้ความรู้แก่เจ้าของธุรกิจ, นักเรียน และหน่วยงานของรัฐ ในเรื่องภัยคุกคามที่มีอยู่รวมทั้งวิธีปกป้อง

เครือข่ายของตนจากการโจมตี การสร้างความพร้อมด้วยการสร้างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) ที่คอยประสานงานเพื่อจัดการภัยคุกคาม รวมถึงแบ่งปันความรู้และทักษะป้องกันการโจมตี ผ่านการสร้างและการดูแลรักษาเครือข่ายคอมพิวเตอร์ ให้มีความมั่นคงปลอดภัยต่อการโจมตี โดยให้อำนาจแก่ผู้ออกกฎหมาย ผู้มีอำนาจควบคุม ผู้จัดทำนโยบาย โดยมีระเบียบข้อบังคับที่ดี และการใช้เครื่องมือที่สามารถต่อสู้กับการโจมตีทางไซเบอร์บรรเทาความเสียหาย เพื่อเรียกคืนความเชื่อมั่นของประชาชนและผู้มีส่วนเกี่ยวข้อง ผ่านการสื่อสารที่มีประสิทธิภาพ และการสร้างความร่วมมือกับภาคเอกชน เพื่อเป็นแนวร่วมในการป้องกันภัยคุกคามทางไซเบอร์ของรัฐบาล

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาและหาแนวทางในการจัดการอย่างเหมาะสมกับภัยคุกคามทางไซ-เบอร์ต่อภาคเอกชน โดยเริ่มจากการศึกษาระบบรักษาความปลอดภัยทางไซเบอร์ที่เหมาะสมกับภาคเอกชน รวมทั้งค่าใช้จ่ายของภาคเอกชนที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์

๒. เพื่อเสนอแนะแนวทางที่ภาคเอกชนสามารถสร้างระบบรักษาความปลอดภัยทางไซเบอร์ได้เหมาะสมกับองค์กร ทั้งด้านขนาดและงบประมาณ รวมทั้งสอดคล้องกับยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อป้องกันภัยภัยคุกคามที่เกิดขึ้นจากการใช้เครือข่ายอินเทอร์เน็ต รวมทั้งสร้างรายการตรวจสอบ (Checklist) ที่ช่วยให้สามารถประเมินความพร้อมในการรักษาความมั่นคงปลอดภัยจากภัยคุกคามที่เกิดขึ้น

ขอบเขตของการวิจัย

การวิจัยเรื่อง “แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ของภาคเอกชนตามยุทธศาสตร์ไซเบอร์แห่งชาติ” มีขอบเขตของการศึกษา ดังนี้

๑. ศึกษาเนื้อหาเกี่ยวกับ แนวคิด รูปแบบ ทฤษฎีที่เกี่ยวข้องกับการกำหนดนโยบายความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ของภาคเอกชน

๒. ศึกษาข้อมูลยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๓. ศึกษาวิจัยเฉพาะนโยบายที่เปิดเผยได้เท่านั้น

๔. ผู้วิจัยจะดำเนินการสัมภาษณ์กลุ่มผู้เชี่ยวชาญที่มีความสามารถทางด้านวิชาการด้านการบริหาร และผู้ที่มีประสบการณ์ในการจัดทำระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับภาคเอกชน และยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

วิธีดำเนินการวิจัย

เนื่องจากผู้วิจัยเห็นว่าภัยคุกคามทางไซเบอร์ที่มีต่อภาคเอกชนเป็นสิ่งที่ควรศึกษาวิจัยและนำเสนอในโครงการวิจัยเพื่อเป็นประโยชน์ในการป้องกันภัยที่เกิดขึ้น สร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร และเป็นไปตามยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีการดำเนินการดังนี้

๑. รวบรวมข้อมูลเรื่องแนวคิด ทฤษฎี รวมถึงวรรณกรรมที่เกี่ยวข้องกับแนวทางการป้องกันภัยคุกคามและการสร้างความมั่นคงปลอดภัยทางไซเบอร์และเปรียบเทียบกับต่างประเทศบางประเทศ รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิเพื่อให้ได้แนวทางในการกำหนดนโยบายความมั่นคงปลอดภัยทางไซเบอร์ต่อภาคเอกชนที่เหมาะสม ทั้งค่าใช้จ่าย ระยะเวลา ให้มีความชัดเจนแปลงไปสู่แผนการปฏิบัติได้จริง

๒. การจัดระเบียบและวิเคราะห์ข้อมูล รวบรวมข้อมูลทั้งหมดที่ได้มาจัดระเบียบและตรวจสอบตามขั้นตอนการวิจัยเชิงคุณภาพ นำข้อมูลมาวิเคราะห์ เพื่อแยกแยะให้เห็นถึงส่วนประกอบและความสัมพันธ์ระหว่างส่วนประกอบต่างๆ เหล่านั้น โดยมุ่งเน้นการวิเคราะห์ความชัดเจน, ความเฉพาะเจาะจง และความสามารถในการแปลงไปสู่แผนการปฏิบัติตามความเหมาะสมของเนื้อหากับกรอบเวลา

ประโยชน์ที่ได้รับจากการวิจัย

๑. สามารถนำผลงานวิจัยไปสร้างมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของภาคเอกชน

๒. สร้างความร่วมมือในการป้องกันภัยคุกคามทางไซเบอร์ระหว่างภาครัฐและภาคเอกชน

๓. การเตรียมความพร้อมในการจัดการภัยคุกคามทางไซเบอร์ของภาครัฐและภาคเอกชน

๔. การตอบสนองต่อภัยคุกคามและลดผลกระทบอันเกิดจากภัยคุกคามไซเบอร์ที่มีต่อภาคเอกชนและภาครัฐ

๕. สร้างความตระหนักและการให้ความรู้แก่สาธารณะ

คำจำกัดความ

เทคโนโลยีสารสนเทศ	หมายถึง การนำเอาเทคโนโลยีมาใช้สร้างมูลค่าเพิ่มให้กับสารสนเทศ ทำให้สารสนเทศมีประโยชน์และใช้งานได้กว้างขวางมากขึ้น เทคโนโลยีสารสนเทศรวมไปถึงการใช้เทคโนโลยีด้านต่างๆ ที่จะรวบรวม จัดเก็บ ใช้งาน ส่งต่อ หรือสื่อสารระหว่างกัน เทคโนโลยีสารสนเทศเกี่ยวข้องโดยตรงกับเครื่องมือเครื่องใช้ในการจัดการสารสนเทศ ซึ่งได้แก่ เครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง ขั้นตอน วิธีการดำเนินการ ซึ่งเกี่ยวข้องกับซอฟต์แวร์ เกี่ยวข้องกับตัวข้อมูล เกี่ยวข้องกับบุคลากร เกี่ยวข้องกับกรรมวิธีการดำเนินงานเพื่อให้ข้อมูลเกิดประโยชน์สูงสุด องค์ประกอบของระบบสารสนเทศนั้นประกอบด้วย ๕ ส่วนหลักๆ ได้แก่ บุคลากร, ขั้นตอนการทำงานม ซอฟแวร์ม ฮาร์ดแวร์ และข้อมูล
ภัยคุกคาม (Threat)	หมายถึง วัตถุ, สิ่งของม ตัวบุคคล หรือสิ่งอื่นใดที่เป็นตัวแทนของการกระทำอันตรายต่อทรัพย์สินขององค์กร หรือสิ่งที่อาจจะก่อให้เกิดเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ได้แก่ ความลับ (Confidentiality), ความสมบูรณ์ (Integrity), ความพร้อมใช้ (Availability) ประเภทของภัยคุกคาม เช่น ภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยเจตนา, ภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยไม่เจตนา, ภัยคุกคามที่เกิดจากภัยธรรมชาติ, ภัยคุกคามที่เกิดจากผู้ใช้ในองค์กรเอง
ความมั่นคงปลอดภัย	หมายถึง สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

ยุทธศาสตร์ด้านไซเบอร์	หมายถึง แผนกลยุทธ์ นโยบาย เป้าหมายและวัตถุประสงค์ของการดำเนินงานให้เหมาะสมกับสภาวะเศรษฐกิจ สังคม ความก้าวหน้าทางเทคโนโลยีและเครือข่าย
ไวรัสคอมพิวเตอร์	หมายถึง โปรแกรมคอมพิวเตอร์ที่บุกรุกเข้าไปในเครื่องคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้ ส่วนมากมักจะมีประสงค์ร้ายและสร้างความเสียหายให้กับระบบของเครื่องคอมพิวเตอร์นั้นๆ บ่อยครั้งที่ผู้คนจะสับสนระหว่างไวรัสกับเวิร์ม เวิร์มนั้นจะมีลักษณะของการแพร่กระจายโดยไม่ต้องพึ่งพาหะส่วนไวรัสนั้นจะสามารถแพร่กระจายได้ก็ต่อเมื่อมีพาหะมาพาไปเท่านั้น เช่น ทางเครือข่าย หรือทางแผ่นดิสก์ โดยไวรัสนั้นอาจฝังตัวอยู่กับแฟ้มข้อมูลและเครื่องคอมพิวเตอร์จะติดไวรัสเมื่อมีการเรียกใช้แฟ้มข้อมูลนั้น
โจมตีแบบ Denial of Service	หมายถึง การปฏิเสธการให้บริการเป็นการโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้
ไทยเซิร์ต (ThaiCERT)	หมายถึง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) จัดตั้งขึ้นในปี พ.ศ. 2543 (ชื่อเดิม ศูนย์ประสานงานรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย) โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ภายใต้สังกัดของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี มีภาระหน้าที่หลักเพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

บทที่ ๒

การพึ่งพาการใช้เทคโนโลยีสารสนเทศของภาคเอกชน

ทุกวันนี้ธุรกิจภาคเอกชน ทั้งที่มีขนาดใหญ่และขนาดเล็กล้วนต้องการสารสนเทศด้วยเหตุผลต่างๆกัน ในการทำธุรกิจนั้น บริษัทและผู้บริหารต้องการสารสนเทศเพื่อการบริหารจัดการการตัดสินใจ และการแก้ปัญหา หากไม่มีสารสนเทศที่เกี่ยวข้องกับเรื่องที่จะต้องตัดสินใจหรือแก้ปัญหาแล้ว การตัดสินใจก็อาจจะผิดพลาดและก่อให้เกิดความเสียหายได้ ด้วยเหตุนี้เองการจัดเก็บสารสนเทศที่ถูกต้องและเหมาะสมเอาไว้อย่างมีประสิทธิภาพเพื่อให้สามารถค้นคืนมาใช้ได้เมื่อจำเป็นจึงมีความสำคัญอย่างยิ่งต่อการที่จะทำให้บริษัทบรรลุเป้าหมายทางธุรกิจแม้ว่าการพัฒนาระบบสารสนเทศส่วนใหญ่จะมีจุดมุ่งหมายเพื่อช่วยประกอบการทำงาน และช่วยในการตัดสินใจแก้ปัญหา นอกจากนี้ยังมีการสร้างระบบสารสนเทศเพื่อให้บริษัทและหน่วยงานใช้สำหรับการวางแผนพัฒนาบริษัทและหน่วยงานในระยะยาว ระบบสารสนเทศแบบนี้เรียกว่า ระบบสารสนเทศเชิงกลยุทธ์ (Strategic Information System หรือ SIS) บริษัทและหน่วยงานสามารถบรรลุความได้เปรียบเชิงกลยุทธ์ได้โดยการใช้กลยุทธ์ในการเสริมสร้างจุดแข็งให้มากที่สุดเมื่อพูดถึงองค์ประกอบรวมของระบบสารสนเทศก็อาจจะกล่าวได้ว่าเป็นการทำงานที่เกี่ยวกับระบบคอมพิวเตอร์ซึ่งประกอบด้วย

๑. ฮาร์ดแวร์ ซึ่งได้แก่อุปกรณ์คอมพิวเตอร์

๒.ซอฟต์แวร์ ซึ่งได้แก่โปรแกรมต่าง ๆ สำหรับประมวลผลข้อมูล

๓. ระบบสื่อสารโทรคมนาคม สำหรับเชื่อมต่ออุปกรณ์คอมพิวเตอร์ต่างๆ เช่น ระบบ LAN และ Network ต่างๆ ในองค์กร

๔. ข้อมูล ซึ่งเป็นข้อเท็จจริงเกี่ยวกับสิ่งที่เกิดขึ้นกับหน่วยงาน

๕. บุคลากร ซึ่งทำหน้าที่ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ

๖. คู่มือและวิธีการปฏิบัติงาน ซึ่งจำเป็นสำหรับใช้เป็นแนวทางการปฏิบัติงานให้สำเร็จ

การใช้บริการอินเทอร์เน็ตภาคเอกชน

๑. การให้บริการอินเตอร์เน็ตในประเทศไทย

ก่อนหน้าที่จะมีการเปิดบริการอินเตอร์เน็ต ในประเทศไทย ในเชิงธุรกิจดังเช่นทุกวันนี้นั้น ได้มีการเริ่มต้นติดตั้งเครื่องคอมพิวเตอร์ เพื่อเชื่อมต่อรับส่งข้อมูลกับเครือข่ายอินเตอร์เน็ต สำหรับใช้ในการศึกษาของมหาวิทยาลัยและหน่วยงานราชการมาเป็นลำดับ เริ่มตั้งแต่มหาวิทยาลัยสงขลานครินทร์ และ AIT (Asian Institute of technology) เชื่อมต่อเครื่องมินิคอมพิวเตอร์ เข้ารับส่งจดหมายอิเล็กทรอนิกส์กับมหาวิทยาลัยเมลเบิร์น ประเทศออสเตรเลีย ในปี พ.ศ. ๒๕๓๐ โดยใช้สายโทรศัพท์ติดต่อรับส่งข้อมูลกันผ่านทางโมเด็ม ซึ่งทางออสเตรเลียจะเป็นผู้ออกค่าใช้จ่ายในการโทรทางไกลเข้ามารับข้อมูลกับมหาวิทยาลัยสงขลานครินทร์และ AIT วันละ ๔ ครั้ง แบ่งเป็นการติดต่อเข้าที่สงขลา ๒ ครั้ง และ ที่ AIT ๒ ครั้ง ซึ่งในขณะนั้นใช้โมเด็ม ความเร็วเพียง ๒,๔๐๐ บิตต่อวินาทีเท่านั้นผู้ใช้บริการทางจดหมายอิเล็กทอนิกส์ ก็คืออาจารย์ในมหาวิทยาลัยทั้งสองแห่ง รวมถึงมหาวิทยาลัยอื่นๆด้วย แต่ผู้ใช้บริการ AIT จะมีมากกว่า เนื่องจากมีอาจารย์ที่ AIT ใช้งานกันมาก และอาจารย์จากมหาวิทยาลัยต่างๆ ในกรุงเทพมหานคร ก็ใช้งานผ่านทาง AIT ด้วย จะเห็นว่ารุ่นบุกเบิกนี้ การรับส่งข้อมูลยังใช้วงจรโทรศัพท์เรียกติดต่อเป็นครั้งคราว ไม่มีการเชื่อมต่อกันตลอดเวลา ระหว่างคู่สาย หรือวงจรเช่า ในปัจจุบันและความเร็ว ในการรับส่งข้อมูลของโมเด็มในยุคนั้น ก็ไม่รวดเร็วเท่าใดนัก

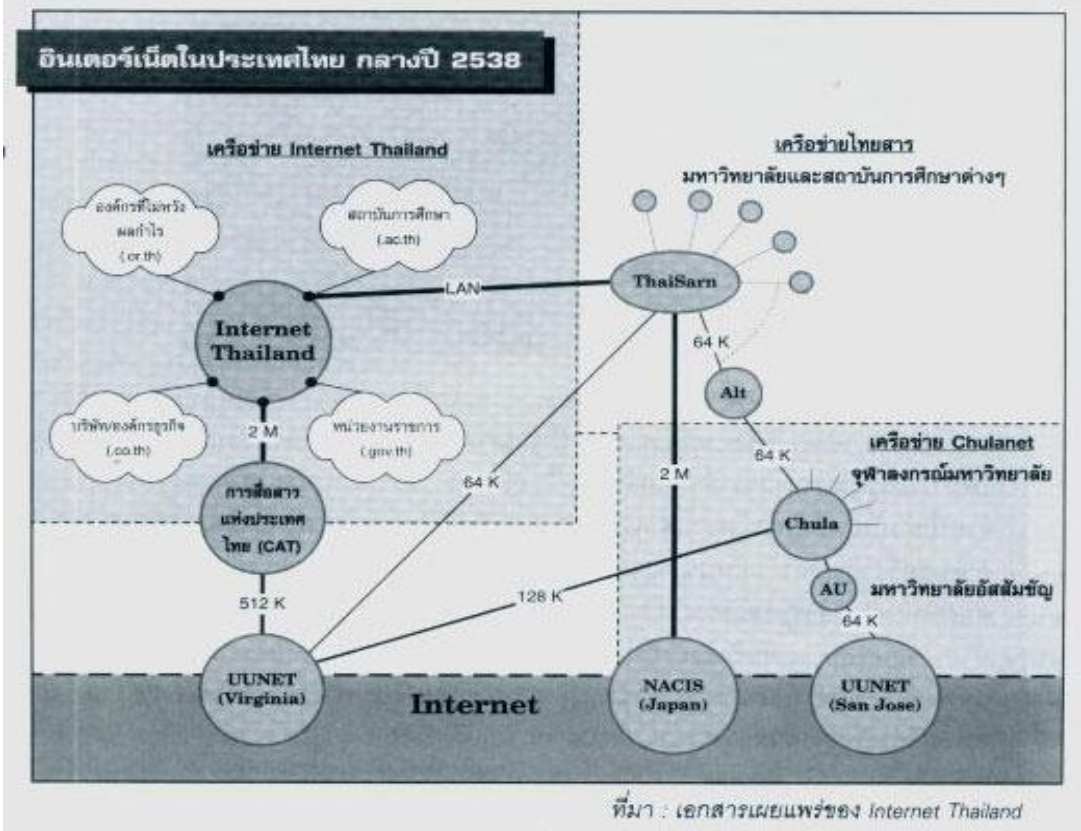
ต่อมาในปี พ.ศ. ๒๕๓๕ จุฬาลงกรณ์มหาวิทยาลัยก็ได้เช่าวงจรถาวรเชื่อมต่อข้อมูลกับอินเตอร์เน็ตแบบออนไลน์ เป็นครั้งแรก ด้วยความเร็ว ๙,๖๐๐ บิตต่อนาที โดยเชื่อมต่อเข้ากับเครือข่ายของอินเตอร์เนตที่ UUNET Technologies ซึ่งทำหน้าที่เป็น ISP ในสหรัฐอเมริกาและศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ หรือ NECTEC (National Electronic and Computer Technology Center) ก็ได้เชื่อมต่อคอมพิวเตอร์ของสถาบันการศึกษาภายในประเทศจำนวน ๖ แห่งเข้าด้วยกัน เพื่อให้บริการอินเตอร์เน็ตภายในประเทศอย่างสมบูรณ์แบบ ประกอบด้วยจุฬาลงกรณ์มหาวิทยาลัย,สถาบันเทคโนโลยีแห่งเอเชีย, มหาวิทยาลัยสงขลานครินทร์, NECTEC, มหาวิทยาลัยธรรมศาสตร์ และมหาวิทยาลัยเกษตรศาสตร์ โดยเรียกเครือข่ายนี้ว่า "ไทยสาร" (Thai Social/Scientific Academic and Research Network, Thai Sarn)

ซึ่งเป็นการใช้งานอินเตอร์เน็ตทางการศึกษาและวิจัยโดยเฉพาะซึ่งนับเป็นจุดเริ่มต้นของบริการอินเตอร์เน็ตในประเทศไทย โดยทั้ง ๖ สถาบันการศึกษาหลังจากนั้นในปี พ.ศ. ๒๕๓๖ เครือข่ายของไทยสารก็ขยายขอบเขตบริการเข้าเชื่อมต่อกับสถาบันการศึกษาและหน่วยงานต่างๆ ของรัฐบาลเพิ่มขึ้นจากเดิม ๖ แห่งหลายเป็น ๑๔ แห่ง ประกอบด้วยสถาบันในระดับอุดมศึกษาจำนวน ๑๕ แห่ง และหน่วยงานรัฐบาลอีก ๔ แห่ง เมื่อมีผู้ใช้บริการมากขึ้นทาง NECTEC จึงได้เพิ่มวงจรระหว่างประเทศความเร็ว ๖๔ กิโลบิตต่อวินาทีขึ้นอีกหนึ่งวงจร ทำให้มีวงจรเชื่อมต่อจากประเทศไทยเข้าสู่เครือข่ายของอินเตอร์เน็ตเพิ่มเป็นสองวงจรเพื่อใช้สำรองซึ่งกันและกันได้ นอกจากนี้ยังทำให้คุณภาพของการใช้งานอินเตอร์เน็ตดีขึ้นมาก ในขณะนั้น NECTEC จึงเป็นจุดเชื่อมต่อเข้ากับอินเตอร์เน็ตจุดหลักแทนที่จุฬาลงกรณ์มหาวิทยาลัย และในปี พ.ศ. ๒๕๓๗ ก็ได้ขยายเครือข่ายออกไปอีก รวมเป็นการเชื่อมต่อหน่วยงานทั้งสิ้น ๒๗ หน่วยงาน แบ่งออกเป็นสถาบันอุดมศึกษา ๒๐ แห่ง และหน่วยงานราชการ ๗ แห่ง ซึ่งได้ให้บริการอินเตอร์เน็ตอย่างสมบูรณ์แบบคือ E-mail, Telnet, ftp, Gopher และ World Wide Web (WWW)

อย่างไรก็ตาม เครือข่ายของไทยสารนี้จัดตั้งขึ้นมาเพื่อใช้ในงานวิจัยและการศึกษาเท่านั้น ไม่ได้จัดตั้งขึ้นมาเปิดบริการในเชิงธุรกิจให้บุคคลทั่วไป เนื่องจากไทยสารเป็นเครือข่ายที่ได้รับเงินสนับสนุนจากรัฐบาลและการเช่าวงจรระหว่างประเทศจากการสื่อสารแห่งประเทศไทยนั้น มีเงื่อนไขว่าจะนำไปให้ผู้อื่นเช่าช่วงหรือเช่าใช้บริการต่อไม่ได้ ดังนั้นบุคคลทั่วไปและบริษัทต่างๆ จึงเชื่อมต่อเข้าใช้บริการอินเตอร์เน็ตจากเครือข่ายของไทยสารไม่ได้ แม้ว่าจะเป็นผู้บุกเบิกการใช้งานอินเตอร์เน็ตในประเทศไทยก็ตาม เมื่อเครือข่ายคอมพิวเตอร์ในประเทศไทยมีการขยายตัวเพิ่มมากขึ้นก็ได้มีการจัดกลุ่มที่ชื่อว่า THAInet (Thailand Access to the Internet) แยกออกจากไทยสาร ซึ่งกลุ่มของ THAInet ประกอบด้วย จุฬาลงกรณ์มหาวิทยาลัย, สำนักวิทยบริการ, วิทยาลัยอัสสัมชัญ เชียงใหม่ และสถาบันเทคโนโลยีแห่งเอเชีย (AIT) ร่วมกันออกค่าใช้จ่ายสำหรับวงจรเช่าระหว่างประเทศจากจุฬาลงกรณ์มหาวิทยาลัยกับ UUNET ความเร็ว ๖๔ กิโลบิตต่อวินาที ส่วนเครือข่ายอื่นๆที่เหลือจะเชื่อมต่อเป็นลูกข่ายของไทยสารตามเดิม โดย NECTEC ยังคงเป็นผู้สนับสนุนค่าใช้จ่ายในการเช่าวงจรต่างประเทศให้ในฐานะที่ NECTEC เป็นหน่วยงานกลางที่ที่รับผิดชอบด้านการวิจัยและพัฒนาของประเทศ ค่าใช้จ่ายส่วนนี้จะเป็นงบประมาณจากรัฐบาลที่ให้การสนับสนุนผ่าน NECTEC อีกทอดหนึ่ง

บริษัทต่างๆ เริ่มมองเห็นประโยชน์ของการใช้งานอินเตอร์เน็ตในประเทศไทย และมีความต้องการใช้งานเพิ่มมากขึ้นเรื่อยๆ การสื่อสารแห่งประเทศไทยและองค์การโทรศัพท์แห่งประเทศไทยจึงได้ร่วมมือกับบริษัทเอกชนที่สนใจเปิดให้บริการอินเตอร์เน็ตโดยแยกเครือข่ายกับไทยสาร เริ่มจากศูนย์บริการอินเตอร์เน็ตประเทศไทย (Internet Thailand Service Center - ITSC หรือเรียกย่อๆว่า Internet Thailand), บริษัท KSC ComNet, บริษัท Loxinfo, บริษัท Infonews และบริษัทอื่นๆอีกหลายบริษัท ให้บริการอินเตอร์เน็ตในประเทศไทยกระจายออกสู่วงกว้าง

แผนภาพที่ ๒-๑อินเตอร์เน็ตในประเทศไทยกลางปี ๒๕๓๘



ที่มา :https://sites.google.com/site/nongleknaka44/prawati-xintexrnet/kar-hi-brikar-xintexrnet-ni-prathesthiy, ๒๕๕๕

๒.บริการต่างๆบนอินเตอร์เน็ต

๒.๑ ไปรษณีย์อิเล็กทรอนิกส์ (Electronic Mail) เรียกกันว่า อีเมล์ (E-mail) ผู้ใช้อินเทอร์เน็ตในการรับส่งจดหมายหรือข้อความ จะต้องมีที่อยู่อีเมล์ (E-mail Address) เพื่อใช้เป็นกล่องจดหมาย ที่อยู่ของอีเมลจะประกอบด้วยส่วนประกอบสำคัญ ๒ ส่วน คือ ผู้ใช้และชื่อโดเมน ซึ่งเป็นชื่อเครื่องคอมพิวเตอร์ ผู้ใช้และชื่อโดเมนจะคั่นด้วยเครื่องหมาย @ (อ่านว่า แอ็ท)

๒.๒ การสนทนาออนไลน์ (Online Chat) เป็นบริการหนึ่งบนอินเทอร์เน็ต ให้ผู้ใช้คุยโต้ตอบกับผู้ใช้คนอื่น ๆ ได้ในเวลาเดียวกัน (Real-Time) การสนทนา Chat (Internet Relay Chat : IRC) การสนทนาใช้ภาพกราฟฟิก ภาพการ์ตูน หรือภาพเคลื่อนไหวต่างๆ แทนตัวผู้สนทนา ตัวอย่างโปรแกรมสนทนาออนไลน์ เช่น ICQ (I Seek You) และ Microsoft MSN Messenger เป็นต้น

๒.๓ เทลเน็ต (Telnet) เป็นบริการที่ให้ผู้ใช้สามารถใช้บริการเครื่องคอมพิวเตอร์ที่ตั้งอยู่ระยะไกล จะใช้การจำลองเครื่องคอมพิวเตอร์ที่กำลังใช้งานอยู่ให้เป็นจอภาพของเครื่องคอมพิวเตอร์ระยะไกลเครื่องนั้น การใช้งานเทลเน็ตจะเป็นการแสดงข้อความตัวอักษร (Text Mode)

๒.๔ การขนถ่ายไฟล์ (File Transfer Protocol) การขนถ่ายไฟล์ เรียกว่า เอฟทีพี (FTP) เป็นบริการที่ใช้สำหรับการแลกเปลี่ยนระหว่างเครื่องคอมพิวเตอร์ทางอินเตอร์เน็ต เครื่องคอมพิวเตอร์ที่ให้บริการไฟล์ เรียกว่า เอฟทีพีเซิร์ฟเวอร์ (FTP Server หรือ FTP Site) ข้อมูลที่ให้บริการมีหลายรูปแบบ ได้แก่ ข้อมูลสถิติ, งานวิจัยม บทความม ข่าวสาร และโปรแกรมฟรีแวร์ ที่สามารถดาวน์โหลดและใช้โปรแกรมได้ฟรี ผู้ใช้บริการจะเรียกว่าดาวน์โหลด การขนถ่ายไฟล์จากเครื่องคอมพิวเตอร์ของผู้ใช้บริการไปยังเครื่องเซิร์ฟเวอร์ เรียกว่าการอัปโหลด

๒.๕ การค้นหาข้อมูลโดยใช้เว็บเบราเซอร์อินเตอร์เน็ต เป็นเครือข่ายใยแมงมุมที่มีการเชื่อมโยงแหล่งข้อมูลที่กระจายอยู่ทั่วโลก การค้นหาข้อมูล สามารถค้นหาแหล่งข้อมูลโดยใช้บริการค้นหาข้อมูลต่างๆ ทำได้สะดวกรวดเร็ว การพัฒนาเว็บไซต์ที่ช่วยสืบค้นหาแหล่งข้อมูลที่เรียกว่า เครื่องมือค้นหา ช่วยให้การค้นหาทั้งในรูปของข้อความและกราฟฟิกกระทำได้โดยง่าย เว็บไซต์ช่วยสืบค้น ได้แก่ google.co.th, yahoo.com, lycos.com และ excite.com เป็นต้น

๒.๖ อินทราเน็ต (Intranets) และเอ็กซ์ทราเน็ต (Extranets) การนำเทคโนโลยีอินเทอร์เน็ตมาประยุกต์ใช้ขององค์การสามารถจำแนกได้เป็น ๒ ประเภท คือ

๒.๖.๑ อินทราเน็ต เป็นระบบเครือข่ายที่ใช้ภายในองค์การคล้ายกับอินเทอร์เน็ต จะใช้เบราเซอร์เว็บไซต์ และเน้นการให้บริการข้อมูลและสารสนเทศแก่พนักงานในองค์การ

๒.๖.๒ เอ็กซ์ทราเน็ต เป็นระบบเครือข่ายที่เชื่อมต่อกับระบบคอมพิวเตอร์ภายนอก เพื่อการติดต่อระหว่างผู้ผลิต และลูกค้าในการธุรกรรม และการดูรายการสินค้าเพื่อช่วยลดค่าใช้จ่ายในการดำเนินการ

๓. พาณิชย์อิเล็กทรอนิกส์ (E-Commerce)

เป็นการซื้อสินค้าและบริการออนไลน์ซึ่งอำนวยความสะดวกให้กับผู้ซื้อที่สามารถซื้อสินค้าได้จากที่บ้านหรือที่ทำงานได้ตลอดเวลา สามารถคัดเลือก เปรียบเทียบราคาสินค้าได้ทุกมุมโลก แค่มีเครือข่ายอินเทอร์เน็ตและ/หรือบัตรเครดิตก็ซื้อสินค้าที่ต้องการได้

๓.๑ ความหมายของพาณิชย์อิเล็กทรอนิกส์ เรียกกันว่าการค้าอิเล็กทรอนิกส์ พาณิชย์อิเล็กทรอนิกส์ คือ การทำธุรกรรมทุกรูปแบบ ได้แก่ การซื้อขายสินค้า, การบริการ, การชำระเงิน, การโฆษณา และการแลกเปลี่ยนสารสนเทศผ่านสื่ออิเล็กทรอนิกส์ เช่น โทรศัพท์, โทรสาร, โทรทัศน์ และเครือข่ายอินเทอร์เน็ต

๓.๒ ความสำคัญของพาณิชย์อิเล็กทรอนิกส์ ธุรกิจบนอินเทอร์เน็ตเป็นช่องทางการตลาดขนาดใหญ่ของโลกสามารถเข้าถึงกลุ่มผู้บริโภคเป้าหมายได้อย่างรวดเร็ว ไร้ขีดจำกัดในเรื่องของเวลาและสถานที่ มีความเร็ว ในการนำเสนอสินค้า การให้บริการ การใช้ต้นทุนต่ำ รวมถึงการสร้างความสัมพันธ์ที่ดีต่อลูกค้าสื่ออิเล็กทรอนิกส์มีความสำคัญอย่างยิ่งในสังคมเศรษฐกิจฐานความรู้ และเป็นทางเลือกหนึ่งของการประกอบธุรกิจในปัจจุบัน

๓.๓ ประเภทของธุรกิจ จำแนกประเภทของธุรกิจได้จากรูปแบบการปฏิสัมพันธ์กับธุรกิจอิเล็กทรอนิกส์ สามารถจำแนกได้ ๓ ประเภท ดังนี้

๓.๓.๑ ธุรกิจแบบบริคและมอร์ต้า เป็นธุรกิจแบบดั้งเดิมมีสถานที่จำหน่าย ไม่มีการทำธุรกิจอิเล็กทรอนิกส์

๓.๓.๒ ธุรกิจแบบคลิกและมอร์ต้า เป็นธุรกิจแบบบริคและมอร์ต้า รวมทั้งร้านค้าออนไลน์ที่ช่วยสนับสนุนการดำเนินธุรกิจปกติ เป็นธุรกิจมีเพียงเว็บไซต์ที่นำเสนอสินค้า และระบุสถานที่จัดจำหน่าย และมีธุรกิจจำนวนมากเพื่อการซื้อขายสินค้าออนไลน์

๓.๓.๓ ธุรกิจแบบคลิกและคลิก เป็นธุรกิจที่ไม่มีสถานที่ร้านค้าเพื่อจำหน่ายสินค้า ผู้ซื้อไม่สามารถที่จะเดินทางไปเลือกซื้อสินค้าได้ มีเฉพาะบนเว็บเท่านั้น เช่น amazon.com หรือ misslily.com เป็นต้น

๓.๔ หมวดหมู่ของสินค้าและการให้บริการ สามารถแบ่งประเภทของธุรกิจได้ดังนี้

๓.๔.๑ ธุรกิจการสื่อสาร เป็นธุรกิจที่มีการประยุกต์ใช้สื่ออิเล็กทรอนิกส์โดยเฉพาะอินเทอร์เน็ต

๓.๔.๒ ธุรกิจการโฆษณา เป็นการใช้เว็บเพจบนอินเทอร์เน็ต สื่อประชาสัมพันธ์สินค้าและบริการ

๓.๔.๓ ธุรกิจการซื้อและการจัดส่งสินค้า เป็นการจำหน่ายสินค้าในลักษณะข้อมูลที่เป็นดิจิทัลและไม่ดิจิทัล สามารถส่งผ่านสื่ออินเทอร์เน็ตโดยให้ผู้ซื้อดาวน์โหลด

๓.๔.๔ ธุรกิจการศึกษาทางไกล ผู้เรียนสามารถศึกษาได้จากทุกที่ทุกเวลาโดยไม่ต้องไปยังสถานศึกษา

๓.๔.๕ ธุรกิจฐานข้อมูลออนไลน์ เป็นการให้บริการด้านข้อมูลและสารสนเทศผ่านสื่ออินเทอร์เน็ต

๓.๔.๖ ธุรกิจการประมูลสินค้า เป็นการเปิดโอกาสให้ผู้ซื้อกำหนดและแข่งขันราคาสินค้าด้วยตนเอง

๓.๔.๗ ธุรกิจศูนย์กลางการค้าอิเล็กทรอนิกส์ การซื้อขายสินค้าให้บริการผ่านเครือข่ายอินเทอร์เน็ต

๓.๔.๘ ธุรกิจด้านการเงิน การให้บริการเกี่ยวกับการติดต่อและทำธุรกรรมเกี่ยวกับการเงิน เช่น บัตรเครดิต

๓.๔.๙ ธุรกิจให้บริการด้านการท่องเที่ยว ให้ข้อมูลและทำธุรกรรมต่างๆ เช่นการจองตั๋วเครื่องบิน

๓.๔.๑๐ ธุรกิจซื้อขายหุ้นผ่านสื่ออิเล็กทรอนิกส์ ให้บริการข้อมูลเกี่ยวกับหลักทรัพย์ ข้อคิดเห็นและคำแนะนำด้านการลงทุน

๓.๕ รูปแบบของพาณิชย์อิเล็กทรอนิกส์

๓.๕.๑ ธุรกิจกับธุรกิจ (Business to Business (B2B)) เป็นการทำธุรกิจด้วยระบบอิเล็กทรอนิกส์ที่มุ่งเน้นการให้บริการกับลูกค้าเป็นองค์การธุรกิจด้วยกัน

๓.๕.๒ ธุรกิจกับลูกค้า (Business to Consumer (B2C)) เป็นการทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์ระหว่างผู้ขายที่เป็นองค์การธุรกิจกับผู้ซื้อหรือลูกค้าแต่ละคน รูปแบบการชำระเงินส่วนใหญ่จะผ่านระบบบัตรเครดิต

๓.๕.๓ ธุรกิจกับภาครัฐ (Business to Government (B2G)) เป็นการทำธุรกรรมทางอิเล็กทรอนิกส์ระหว่างธุรกิจเอกชนกับภาครัฐ

๓.๕.๔ ลูกค้ากับลูกค้า (Consumer to Consumer (C2C)) เป็นการทำธุรกรรมทางอิเล็กทรอนิกส์ระหว่างผู้บริโภคด้วยกัน แลกเปลี่ยน ซื้อ ขายสินค้าผ่านเว็บไซต์

๓.๕.๕ ภาครัฐกับประชาชน (Government to Consumer (G2C)) กิจกรรมที่เกิดขึ้นผ่านสื่ออิเล็กทรอนิกส์ไม่ได้มีวัตถุประสงค์เพื่อการค้า เน้นให้บริการกับประชาชนผ่านสื่อ เป็นนโยบายของรัฐบาล

๓.๖ โครงสร้างของระบบพาณิชย์อิเล็กทรอนิกส์

๓.๖.๑หน้าร้าน (Storefront) เป็นส่วนประกอบที่สำคัญของระบบการค้าแบบพาณิชย์อิเล็กทรอนิกส์สำหรับแสดงข้อมูลสินค้าทั้งหมดของร้านค้า การค้นหาข้อมูลหน้าร้านต้องมีการออกแบบที่ดีเหมาะสมกับกลุ่มเป้าหมาย

๓.๖.๒ ระบบตระกร้ารับคำสั่งซื้อ (Shopping Cart System) เป็นระบบต่อเนื่องจากหน้าร้าน เมื่อลูกค้าต้องการสั่งซื้อสินค้า ให้คลิกที่ สั่งซื้อ หรือสัญลักษณ์รูปตระกร้า จะปรากฏรายการสินค้าที่ลูกค้าต้องการพร้อมคำนวณค่าใช้จ่าย

๓.๖.๓ ระบบการชำระเงิน (Payment System) ผู้ขายต้องมีทางเลือกให้ลูกค้าหลายทางเพื่อความสะดวกของลูกค้า เช่น การโอนเงินเข้าบัญชีธนาคาร การชำระด้วยบัตรเครดิต การส่งผ่านธนาณัติ เป็นต้น

๓.๖.๔ ระบบสมัครสมาชิก (Member System) เป็นการบันทึกข้อมูลที่ต้องการสมัครเป็นสมาชิกเพื่อรับข่าวสาร รวมถึงการสั่งซื้อสินค้า

๓.๖.๕ ระบบขนส่ง (Transportation System) เป็นระบบการจัดส่งสินค้าให้ถึงลูกค้า มีทางเลือกหลายทางให้ลูกค้า ขึ้นอยู่กับความต้องการของลูกค้า ค่าใช้จ่ายแต่ละวิธีจะไม่เท่ากัน เช่น EMS, DHL, FedEx หรือUPS เป็นต้น เพื่อความสะดวกในการคำนวณค่าใช้จ่าย

๓.๖.๖ ระบบติดตามคำสั่งซื้อ (Order Tracking system) ระบบติดตามคำสั่งซื้อเมื่อเสร็จสิ้นการสั่งซื้อแต่ละครั้งลูกค้าจะได้รับหมายเลขคำสั่งซื้อ เพื่อใช้หมายเลขดังกล่าวตรวจสอบสถานะของสินค้าได้ จะทำให้ลูกค้าเกิดความเชื่อถือและมั่นใจว่าได้รับสินค้าแน่นอน

๓.๗ กระบวนการทางพาณิชย์อิเล็กทรอนิกส์

๓.๗.๑ การค้นหาข้อมูล ค้นหาข้อมูลสินค้าที่ต้องการ แล้วนำมาวิเคราะห์เปรียบเทียบการสั่งซื้อ

๓.๗.๒ การสั่งซื้อสินค้า เมื่อเลือกสินค้าที่ต้องการแล้ว นำรายการสินค้าเข้าตระกร้า และมีการคำนวณค่าใช้จ่าย สามารถเลือกรายการสินค้าและปริมาณที่สั่งได้

๓.๗.๓ การชำระเงิน ขึ้นอยู่กับความสะดวกว่าต้องการชำระวิธีไหน

๓.๗.๔ การส่งมอบสินค้า เลือกวิธีการขนส่งสินค้า

๓.๗.๕ การให้บริการหลังการขาย ร้านค้าต้องมีบริการหลังการขายให้กับลูกค้า

๓.๗.๖ บริษัทต่างๆ สามารถใช้งานอินเตอร์เน็ตกับธุรกิจ ในรูปแบบการบริการต่างๆ และพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) ที่มีความต้องการใช้งานเพิ่มมากขึ้นเรื่อยๆในปัจจุบัน

๔. ระบบการป้องกันการโจมตีจากภายนอก

การเข้าถึงข้อมูลในคอมพิวเตอร์ขององค์กรหรืออุปกรณ์เก็บข้อมูลที่พกพาจากระยะไกลได้โดยไม่ได้รับอนุญาตเกิดขึ้นได้ หากว่า “ผู้บุกรุก” อ่านหรือเปลี่ยนแปลงแก้ไขข้อมูลขององค์กรทางอินเทอร์เน็ต หรือในกรณีที่เขาเข้าถึงฮาร์ดแวร์ขององค์กรได้ การปกป้องตัวเองจากภัยคุกคามไม่ประเภทใดก็ประเภทหนึ่งนี้โดยการปรับปรุงความปลอดภัยทางกายภาพและระบบเครือข่ายให้กับข้อมูลขององค์กร ดังนี้

๔.๑ การปกป้องคอมพิวเตอร์องค์กร จากโปรแกรมประสงค์ร้ายและนักเจาะระบบ

การรักษาคอมพิวเตอร์ขององค์กรให้ปลอดภัยเป็นก้าวแรกที่สำคัญอย่างยิ่งบนหนทางสู่ระบบความปลอดภัยที่ดีกว่า ต้องมั่นใจว่าคอมพิวเตอร์ของคุณไม่อ่อนไหวต่อนักเจาะระบบ หรือการระบาดของโปรแกรมประสงค์ร้าย ซึ่งเรียกกันโดยทั่วไปว่ามัลแวร์ เช่น ไวรัส หรือโปรแกรมสปายแวร์ ถ้าไม่เช่นนั้นแล้วก็เป็นไปไม่ได้ที่จะรับประกันความมีประสิทธิภาพของการเตรียมการป้องกันความปลอดภัยอื่นๆ ที่องค์กรอาจจะดำเนินการ ในการเก็บรักษาซอฟต์แวร์ของคุณ และใช้เครื่องมืออย่าง อะแวสท์ (Avast) สปายบอท (Spybot) และ โคโมโด ไฟร์วอลล์ (Comodo Firewall) ในการปกป้องคอมพิวเตอร์ขององค์กรจากอันตรายที่มีอยู่ในปัจจุบันอันเกิดจากการติดมัลแวร์ (malware) และการโจมตีของนักเจาะระบบ ถึงแม้ว่าเครื่องมือที่แนะนำไว้จะสำหรับวินโดวส์ (Windows) ซึ่งเป็นระบบปฏิบัติการที่เปราะบางต่อภัยคุกคามเหล่านี้มากที่สุด อย่างไรก็ตามผู้ใช้ กนู/ลีนุกซ์ (GNU/Linux) และโอเอสเท็น (OS X) ก็ยังมีความเสี่ยงและควรที่จะนำกลยุทธ์ที่จะกล่าวด้านล่างนี้ไปใช้ด้วย

๔.๑.๑ ไวรัสการจัดหมวดหมู่ไวรัสมีหลากหลายวิธี และแต่ละวิธีนั้นก็มาพร้อมกับชื่อเรียกในแต่ละหมวดหมู่อย่างมีสีสันเช่น หนอน (worms) มาโครไวรัส (macroviruses) โทรจัน (trojans) และ ประตูหลัง (backdoors) ซึ่งเป็นตัวอย่างของไวรัสที่รู้จักกันดี ไวรัสหลายๆ ประเภทในจำนวนนี้แพร่กระจายทั่วอินเทอร์เน็ตผ่านอีเมล เว็บเพจประสงค์ร้าย (malicious webpages) หรือวิธีอื่นๆที่บุกรุกเข้าไปยังคอมพิวเตอร์ที่ไม่มีการป้องกัน ไวรัสชนิดอื่นๆ

ยังสามารถแพร่กระจายผ่านสื่อที่เคลื่อนย้ายได้ โดยเฉพาะอย่างยิ่งอุปกรณ์อย่างแฟลชไดรฟ์ และฮาร์ดดิสก์ภายนอก ซึ่งผู้ใช้สามารถที่จะบันทึกและอ่านข้อมูลได้ ไวรัสสามารถทำลาย ก่อความเสียหาย หรือแพร่เชื้อไปยังข้อมูลที่อยู่ในคอมพิวเตอร์ขององค์กรได้ รวมถึงข้อมูลที่เก็บอยู่ในหน่วยความจำภายนอกด้วยเช่นกัน ไวรัสยังสามารถเข้าควบคุมคอมพิวเตอร์ขององค์กรและใช้คอมพิวเตอร์นั้น เพื่อโจมตีคอมพิวเตอร์เครื่องอื่นๆได้ด้วยเช่นกันซอฟต์แวร์ป้องกันไวรัสมีโปรแกรมป้องกันไวรัสที่เป็น ฟรีแวร์ สำหรับวินโดวส์ชื่อว่า อะแวสท์ ซึ่งใช้งานง่าย และอัปเดตเป็นประจำ รวมทั้งได้รับการยอมรับจากผู้เชี่ยวชาญด้านการป้องกันไวรัส โปรแกรมนี้ต้องการเพียงแค่ให้ทำการลงทะเบียนครั้งเดียวทุก 14 เดือน แต่การลงทะเบียน การอัปเดต และตัวโปรแกรมเองไม่มีค่าใช้จ่ายใดๆนอกจากอะแวสท์แล้ว ยังมีโปรแกรมป้องกันไวรัสเชิงพาณิชย์ที่รู้จักกันดีอีกเป็นจำนวนมาก คลามวิน (Clamwin) ก็เป็นซอฟต์แวร์เสรีและโอเพนซอร์ส (Free and Open Source Software-FOSS) ที่เป็นตัวเลือกหนึ่งนอกจากอะแวสท์ ถึงแม้ว่ามันจะขาดคุณลักษณะบางประการที่สำคัญสำหรับการเป็นโปรแกรมป้องกันไวรัสเบื้องต้น แต่คลามวินได้เปรียบตรงที่ว่ามันสามารถทำงานบนแฟลชไดร์ฟได้เพื่อตรวจสอบคอมพิวเตอร์เครื่องที่ไม่ได้รับอนุญาตให้ติดตั้งซอฟต์แวร์ใดๆได้ เคล็ดลับในการใช้ซอฟต์แวร์ป้องกันไวรัสอย่างมีประสิทธิภาพ

๑) อย่าใช้โปรแกรมป้องกันไวรัสสองโปรแกรมทำงานในเวลาเดียวกัน เพราะการทำเช่นนี้อาจทำให้คอมพิวเตอร์ทำงานช้าลงอย่างมาก จนถึงขนาดหยุดการทำงาน

๒) ให้ลบการติดตั้งโปรแกรมหนึ่งออกก่อนที่จะติดตั้งอีกโปรแกรมหนึ่ง

๓) ตรวจดูให้แน่ใจว่าโปรแกรมป้องกันไวรัสอนุญาตให้รับข้อมูลเพื่ออัปเดตโปรแกรมให้ล่าสุดหรือไม่

๔) ควรอัปเดตโปรแกรมเชิงพาณิชย์อย่างสม่ำเสมอ โดยโปรแกรมเชิงพาณิชย์ซึ่งถูกติดตั้งมาในคอมพิวเตอร์เครื่องใหม่ตั้งแต่ต้นหลายโปรแกรมต้องการให้ลงทะเบียน (และต้องเสียค่าใช้จ่าย) เมื่อถึงช่วงเวลาหนึ่ง หรือโปรแกรมเหล่านั้นอาจจะหยุดรับข้อมูลอัปเดตโปรแกรมให้ล่าสุด ซอฟต์แวร์ที่แนะนำในนี้ทั้งหมดสามารถรับข้อมูลเพื่ออัปเดต

๕) ควรสแกนไฟล์ทั้งหมดบนคอมพิวเตอร์เป็นประจำ ไม่จำเป็นต้องทำเช่นนี้ทุกวัน แต่ควรจะสแกนบางครั้งบางคราว จะบ่อยแค่ไหนขึ้นอยู่กับสถานการณ์ว่าได้เชื่อมต่อคอมพิวเตอร์ขององค์กรกับเครือข่ายที่ไม่รู้จักเมื่อไม่นานมานี้หรือไม่ หรือมีการใช้แฟลชไดร์ฟจากภายนอกเข้ามาใช้ในองค์กร

๔.๑.๒ สปายแวร์ (Spyware) หรือ โปรแกรมสอดแนม เป็นโปรแกรมประสงค์ร้ายประเภทหนึ่ง ซึ่งสามารถติดตามงานที่ทำทั้งบนคอมพิวเตอร์และบนอินเทอร์เน็ต และส่งข้อมูลที่ทำไปให้กับใครบางคนที่ไม่ควรได้เข้าถึงข้อมูลนี้ สปายแวร์เหล่านี้สามารถบันทึกคำที่พิมพ์ลงบนคีย์บอร์ด การเคลื่อนไหวของเมาส์ ซึ่งผลก็คือ โปรแกรมเหล่านี้บ่อนทำลายความปลอดภัยบนคอมพิวเตอร์ขององค์กรและเปิดเผยข้อมูลที่เป็นความลับขององค์กร คอมพิวเตอร์สามารถติดสปายแวร์ในลักษณะที่เหมือนกับการติดไวรัส คำแนะนำต่างๆ จากที่ได้กล่าวมาสามารถช่วยที่จะป้องกัน มัลแวร์ได้เพราะเว็บเพจประสงค์ร้ายเป็นแหล่งหลักๆ ที่คอมพิวเตอร์จะติดสปายแวร์ ดังนั้นควรที่จะต้องให้ความใส่ใจเป็นพิเศษในการที่จะเข้าดูเว็บเพจและต้องให้มั่นใจได้ว่ามีการตั้งค่าเบราว์เซอร์ของคอมพิวเตอร์ในองค์กรให้มีความปลอดภัย ซอฟต์แวร์ป้องกันโปรแกรมสอดแนมสามารถใช้เป็นเครื่องมือป้องกันสปายแวร์เพื่อปกป้องคอมพิวเตอร์ขององค์กรจากภัยคุกคามประเภทนี้ได้ สปายบอต (Spybot) เป็นโปรแกรมหนึ่งที่ต่อต้านสปายแวร์ และทำงานได้ดีมากในการระบุและลบมัลแวร์บางชนิดซึ่งโปรแกรมป้องกันไวรัสไม่สนใจออกไป เหมือนกับซอฟต์แวร์ป้องกันไวรัส มันเป็นเรื่องที่สำคัญมากในการที่จะต้องอัปเดตฐานข้อมูลมัลแวร์ของ สปายบอต และสแกนคอมพิวเตอร์เป็นประจำ

๔.๑.๓ ไฟร์วอลล์ (Fire Wall) เป็นโปรแกรมแรกในคอมพิวเตอร์ที่จะมองเห็นข้อมูลขาเข้าจากอินเทอร์เน็ต และเป็นโปรแกรมสุดท้ายที่จะจัดการข้อมูลขาออก มันทำหน้าที่เหมือนพนักงานรักษาความปลอดภัยที่ยืนรักษาความปลอดภัยที่ประตูของตึก และเป็นผู้มีหน้าที่ตัดสินใจว่าใครบ้างที่จะเข้าและออกจากตึกได้ ไฟร์วอลล์เป็นตัวรับ ตรวจสอบ และตัดสินใจเกี่ยวกับข้อมูลขาเข้าและขาออกทั้งหมด โดยปกติแล้ว การปกป้องตัวเองจากการเชื่อมต่อที่ไม่น่าเชื่อถือจากอินเทอร์เน็ตและจากเครือข่ายภายในเป็นสิ่งสำคัญมากสำหรับองค์กร ทั้งสองเครือข่ายนี้เปิดทางโล่งให้กับนักเจาะระบบและไวรัสบุกรุกเข้ามาในคอมพิวเตอร์ขององค์กรได้ กระนั้นก็ตาม ในความเป็นจริงแล้วการเฝ้าตรวจตราการเชื่อมต่อขาออกจากคอมพิวเตอร์ขององค์กรก็มีความสำคัญไม่น้อยไปกว่ากันไฟร์วอลล์ที่ดีจะให้เลือกว่า จะอนุญาตให้มีการเข้าถึงแต่ละโปรแกรมบนคอมพิวเตอร์ขององค์กรหรือไม่ เมื่อหนึ่งในโปรแกรมเหล่านี้พยายามติดต่อโลกภายนอก ไฟร์วอลล์ขององค์กรจะปิดกั้นความพยายามนั้นและเตือน เว้นแต่ว่าไฟร์วอลล์นั้นรู้จักโปรแกรมนั้นและได้มีการตรวจสอบแล้วว่าอนุญาตให้โปรแกรมนั้นเชื่อมต่อกับภายนอกเช่นนั้นได้ การดำเนินการเช่นนี้โดยส่วนใหญ่เป็นการป้องกันไม่ให้มัลแวร์ ที่มีอยู่แพร่กระจายไวรัสหรือเชื้อเชิญให้นักเจาะระบบมาหาคอมพิวเตอร์ขององค์กรในลักษณะเช่นนี้เอง ไฟร์วอลล์ได้ให้แนวป้องกันแนวที่สองและให้ระบบการเตือนแต่เนิ่นๆ ซึ่งอาจช่วยให้รับรู้ได้เมื่อความปลอดภัยคอมพิวเตอร์

ขององค์กรอยู่ภายใต้การคุกคามซอฟต์แวร์ไฟร์วอลล์ไมโครซอฟท์ วินโดวส์ (Microsoft Windows) รุ่นล่าสุดมีไฟร์วอลล์ติดตั้งมาในตัวเองซึ่งอยู่ในสถานะเปิดอยู่โดยอัตโนมัติ แต่เป็นที่น่าเสียดายว่าไฟร์วอลล์ของวินโดวส์มีข้อจำกัดอยู่หลายประการ ตัวอย่างเช่น มันไม่ตรวจสอบการเชื่อมต่อขาออก อย่างไรก็ตาม ฟรีแวร์ ดีๆ ชื่อว่า โคโมโด เพอซัลนัล ไฟร์วอลล์ (Comodo Personal Firewall) ซึ่งทำงานได้ดีกว่าในการรักษาความปลอดภัยให้กับคอมพิวเตอร์ขององค์กร ต้องมั่นใจว่าคอมพิวเตอร์ทั้งหมดที่อยู่ในองค์กรมีการติดตั้งไฟร์วอลล์ถ้ายังไม่มีไฟร์วอลล์ควรพิจารณาติดตั้งไฟร์วอลล์เพิ่มเติมเพื่อที่จะปกป้องเครือข่ายภายใน เราเตอร์ของผู้ให้บริการบรอดแบนด์เชิงพาณิชย์หลายรายได้รวมไฟร์วอลล์แบบง่ายต่อการใช้มาแล้ว และการเปิดใช้งานสามารถช่วยสร้างความปลอดภัยให้กับเครือข่ายขององค์กรได้

๔.๑.๔ ปรับปรุงซอฟต์แวร์ให้ทันสมัยอยู่เสมอโปรแกรมคอมพิวเตอร์มักจะมีขนาดใหญ่และซับซ้อน จึงหลีกเลี่ยงไม่ได้ว่าซอฟต์แวร์บางตัวที่ใช้เป็นประจำอาจมีข้อผิดพลาดที่ยังไม่ถูกค้นพบอยู่ และมีความเป็นไปได้ที่ข้อผิดพลาดเหล่านี้สามารถบ่อนทำลายความปลอดภัยคอมพิวเตอร์ขององค์กรได้ อย่างไรก็ตามผู้พัฒนาซอฟต์แวร์ได้พยายามค้นหาข้อผิดพลาดเหล่านี้ต่อเนื่องกันมาและได้ออกอัพเดทเพื่อที่จะแก้ไขข้อผิดพลาดเหล่านั้น ดังนั้นจึงเป็นเรื่องจำเป็นอย่างยิ่งที่คุณจะต้องอัปเดตซอฟต์แวร์ทั้งหมดในคอมพิวเตอร์ขององค์กร รวมทั้งระบบปฏิบัติการเช่นเดียวกันมันเป็นเรื่องสำคัญมากที่จะต้องแน่ใจว่าซอฟต์แวร์อื่นๆ ที่ติดตั้งอยู่ในคอมพิวเตอร์ขององค์กรนั้นอยู่ในสถานะอัปเดตล่าสุด

๔.๒ การปกป้องข้อมูลขององค์กรให้พ้นจากภัยคุกคามทางกายภาพ

ไม่ว่าจะพยายามมากแค่ไหนในการสร้างแนวป้องกันดิจิทัลรอบๆ คอมพิวเตอร์ขององค์กร เช้าวันหนึ่งอาจพบว่าคอมพิวเตอร์ขององค์กรหรือสำเนาข้อมูลในนั้น หายถูกขโมย หรือเสียหายจากอุบัติเหตุหรือการประสงค์ร้ายต่างๆ เช่น เหตุการณ์อย่างไฟกระชากหน้าต่างที่เปิดทิ้งไว้ จนถึงกาแฟหก อาจนำไปสู่สถานการณ์ที่ข้อมูลทั้งหมดสูญหายและใช้คอมพิวเตอร์ไม่ได้อีกต่อไป การประเมินความเสี่ยงอย่างระมัดระวัง พยายามรักษาสภาพแวดล้อมทางคอมพิวเตอร์ให้ดีอยู่เสมอ และนโยบายความมั่นคง ที่เป็นลายลักษณ์อักษรสามารถช่วยหลีกเลี่ยงหายนะเหล่านี้ได้หลายองค์กรประเมินความสำคัญของการรักษาความปลอดภัยทางกายภาพของอาคารสำนักงานและอุปกรณ์ต่างๆ ต่ำเกินไป ส่งผลให้องค์กรเหล่านั้นมักจะขาดนโยบายที่ชัดเจนในการกำหนดรายละเอียดว่าควรจะใช้มาตรการอะไรบ้างเพื่อปกป้องคอมพิวเตอร์หรืออุปกรณ์เก็บสำรองข้อมูลจากหัวขโมย, สภาพอากาศที่เลวร้าย, อุบัติเหตุ

หรือภัยคุกคามทางกายภาพอื่นๆ ความสำคัญของนโยบายความปลอดภัยนี้อาจจะเห็นค่อนข้างชัดเจนแต่การสร้างนโยบายอย่างเหมาะสมนั้นเป็นเรื่องที่ซับซ้อนกว่านั้นตัวอย่างเช่น หลายองค์กรมีกลอนประตูสำนักงานที่มีคุณภาพดี บ้างก็มีหน้าต่างนิรภัย แต่องค์กรเหล่านั้นไม่ได้ให้ความสนใจเกี่ยวกับประเด็นที่ว่าควรจะทำสำเนากุญแจกี่ดอกและใครเป็นคนเก็บสำเนากุญแจเหล่านั้น ทำให้ข้อมูลอ่อนไหวต่างๆ ยังคงมีความเปราะบางอยู่

๔.๒.๑ พิจารณาวิธีการที่เก็บข้อมูลสำคัญ เช่น ฮาร์ดไดรฟ์ในคอมพิวเตอร์, อีเมล์, เว็ปเซิร์ฟเวอร์, แฟลชไดรฟ์, ฮาร์ดดิสก์ภายนอก, ซีดีหรือดีวีดี, โทรศัพท์มือถือ, กระดาษที่พิมพ์ออกมา หรือจดบันทึกย่อด้วยลายมือ ล้วนแต่เป็นตัวเลือกที่เป็นไปได้พิจารณาว่าอุปกรณ์ต่างๆ เหล่านี้ควรจะเก็บไว้ที่ไหนในทางกายภาพ พวกมันควรอยู่ในสำนักงาน ที่บ้าน ในถังขยะด้านหลัง หรือ ที่มีเพิ่มขึ้นเรื่อยๆ “ที่ไหนสักที่บนอินเทอร์เน็ต” ในกรณีสุดท้ายนั้น จะเป็นเรื่องที่ค่อนข้างท้าทายที่จะตัดสินใจว่าหาสถานที่ทางกายภาพเพื่อเก็บข้อมูลชิ้นใดชิ้นหนึ่งให้พึงระลึกไว้เสมอว่าข้อมูลเดียวกันอาจจะมีความเปราะบางได้ในหลายระดับชั้น เช่นเดียวกับที่อาศัยซอฟต์แวร์ต่อต้านไวรัสเพื่อที่จะป้องกันข้อมูลที่เก็บอยู่ในแฟลชไดร์ฟจากมัลแวร์ จะต้องอาศัยแผนความปลอดภัยทางกายภาพอย่างละเอียดเพื่อปกป้องข้อมูลอันเดียวกันนั้นจากการโจรกรรม การสูญหายหรือการถูกทำลาย ในขณะที่การปฏิบัติเพื่อความปลอดภัยบางอย่าง เช่น การมีนโยบายสำรองข้อมูลต่างสถานที่จากระบบหลัก (off-site backup policy) ที่ดีจะช่วยป้องกันภัยจากการคุกคามดิจิทัลและการคุกคามทางกายภาพ การปฏิบัติรูปแบบอื่นๆ มีความเฉพาะเจาะจงมากกว่า

๔.๒.๒ ปกป้องข้อมูลขององค์กรจากผู้บุกรุก ทางกายภาพผู้ประสงค์ร้ายซึ่งจ้องหาทางที่จะเข้าถึงข้อมูลอ่อนไหวขององค์กรเป็นประเภทหนึ่งของภัยคุกคามทางกายภาพ อาจจะเป็นความคิดที่ผิดในการทึกทักเอาว่ากรณีนี้เป็นเพียงภัยคุกคามชนิดเดียวต่อความปลอดภัยของข้อมูลขององค์กร หากละเลยไม่สนใจต่อภัยคุกคามประเภทนี้ มีหลายขั้นตอนที่ทำได้เพื่อลดความเสี่ยงอันเกิดจากการบุกรุกทางกายภาพ หมวดหมู่และคำแนะนำต่างๆ ด้านล่างนี้สามารถนำไปใช้ได้ทั้งที่บ้านและสำนักงานถือเป็นพื้นฐานที่สามารถนำไปใช้ในเพื่อสร้างมาตรการต่างๆ ให้สอดคล้องกับสถานการณ์ที่มีลักษณะเฉพาะในเรื่องความปลอดภัยทางกายภาพได้ถ้ามีระบบเครือข่ายไร้สาย การรักษาความปลอดภัยให้กับ จุดเข้าถึง (Access Point) เพื่อที่จะกันไม่ให้ผู้บุกรุกสามารถแฝงตัวเข้ามาหรือจับตาการจราจรของข้อมูลในระบบเครือข่ายขององค์กรได้เป็นสิ่งสำคัญอย่างยิ่ง ถ้าใช้เครือข่ายไร้สายที่ไม่มีระบบความปลอดภัย ใครก็ตามที่มีคอมพิวเตอร์พกพาในบริเวณใกล้เรือนเคียงก็อาจจะกลายเป็นผู้บุกรุกได้ กรณีนี้อาจไม่ใช่เป็นคำจำกัดความที่ไม่ปกตินักของคำว่า

“ทางกายภาพ” แต่มันช่วยให้ได้พิจารณาว่า ผู้ประสงค์ร้ายซึ่งสามารถจับตาเครือข่ายไร้สายขององค์กรนั้นสามารถที่จะเข้าถึงข้อมูลได้เท่ากับคนที่แอบเข้ามาในสำนักงาน และเข้าถึงคอมพิวเตอร์ได้ผ่านการเชื่อมต่อสายอีเทอร์เน็ต (Ethernet) สิ่งที่ต้องทำเพื่อรักษาความปลอดภัยให้กับเครือข่ายไร้สายนั้นแตกต่างกันไป มันขึ้นอยู่กับฮาร์ดแวร์และซอฟต์แวร์ของจุดเข้าถึงขององค์กร แต่ขั้นตอนเหล่านั้นก็ไม่ได้ยากอะไรที่จะทำตามซอฟต์แวร์และการตั้งค่าที่เกี่ยวข้องกับความปลอดภัยทางกายภาพต้องแน่ใจว่า เมื่อรีสตาร์ทคอมพิวเตอร์ คอมพิวเตอร์จะถามให้ใส่รหัสผ่านก่อนที่จะยอมให้ใช้งานซอฟต์แวร์และเข้าถึงไฟล์ต่างๆ ทุกครั้ง มีการตั้งค่า 2-3 อย่างที่สามารถทำได้ที่ ไบออส (Bios) คอมพิวเตอร์ซึ่งเกี่ยวข้องกับความปลอดภัยทางกายภาพ ประการแรกควรกำหนดค่าคอมพิวเตอร์เพื่อไม่ให้มัน “บูท” ได้จากอุปกรณ์, USB, ซีดีรอม หรือดีวีดีไดรฟ์ ประการที่สองควรตั้งรหัสผ่านที่ ไบออส เองเพื่อกันไม่ให้ผู้บุกรุกสามารถลบการตั้งค่าที่มีมาก่อนหน้านี้ และย้ำกันอีกครั้งว่าควรเลือกรหัสผ่านที่มีความปลอดภัยรักษาสภาพแวดล้อมสำหรับฮาร์ดแวร์ให้ดีอยู่เสมอ เช่นเดียวกับอุปกรณ์อิเล็กทรอนิกส์อื่นๆ คอมพิวเตอร์นั้นค่อนข้างอ่อนไหว คอมพิวเตอร์ไม่สามารถทำงานได้ดีในสภาวะที่กระแสไฟฟ้าไม่สม่ำเสมอ อุณหภูมิสูงหรือต่ำเกินไป มีฝุ่นมาก ชื้น หรือถูกบีบ มีหลายสิ่งที่ทำเพื่อปกป้องคอมพิวเตอร์และอุปกรณ์เครือข่ายจากภัยคุกคามเหล่านี้ได้ปัญหาเกี่ยวกับกระแสไฟฟ้าเช่น ไฟเกิน, ไฟดับ หรือไฟตก ก็สามารถเป็นสาเหตุของความเสียหายทางกายภาพให้กับคอมพิวเตอร์ได้ สิ่งไม่ปกติเหล่านี้สามารถ “พัง” ฮาร์ดไดรฟ์ได้ ซึ่งสร้างความเสียหายให้กับข้อมูลที่เก็บอยู่ภายใน หรือสร้างความเสียหายทางกายภาพให้กับส่วนประกอบอิเล็กทรอนิกส์ในคอมพิวเตอร์ได้ การติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptible Power Supplies) หรือ UPS ให้กับคอมพิวเตอร์เครื่องที่สำคัญ ในสำนักงาน UPS จะช่วยให้การจ่ายไฟนั้นเป็นไปอย่างสม่ำเสมอและเป็นตัวจ่ายไฟชั่วคราวในกรณีที่เกิดไฟฟ้าดับพยายามใช้เต้าเสียบปลั๊กไฟแบบที่มีสามรู ซึ่งหนึ่งในสามรูนั้นจะทำหน้าที่เป็น “สายดิน” หรือ “สายต่อลงพื้นดิน” การซื้อสายไฟคอมพิวเตอร์, รางปลั๊กไฟ หรือสายพ่วงปลั๊กไฟที่มีคุณภาพสูง ควรหาซื้ออุปกรณ์เหล่านี้ให้เพียงพอที่จะใช้งานทั่วทั้งสำนักงานและสร้างนโยบายความปลอดภัยทางกายภาพเมื่อได้ประเมินภัยคุกคามต่อความเปราะบางขององค์กรจะต้องเผชิญแล้ว จะต้องพิจารณาว่ามีขั้นตอนอะไรที่ทำได้บ้างเพื่อที่จะปรับปรุงความปลอดภัยทางกายภาพ ควรสร้างนโยบายความปลอดภัยที่เป็นรายละเอียดโดยเขียนนโยบายเหล่านี้เป็นขั้นเป็นตอน เอกสารที่ได้เป็นผลลัพธ์นี้จะทำหน้าที่เป็นแนวทางปฏิบัติโดยทั่วไป สำหรับผู้ที่เข้ามาทำงานในองค์กร นโยบายความปลอดภัยนี้ควรจะมีใบรายการตรวจดูว่ามีอะไรที่จะที่ต้องทำบ้างในกรณีที่เกิดเหตุฉุกเฉินด้านความปลอดภัยทางกายภาพรูปแบบต่างๆ ทุกคนที่เกี่ยวข้องควรจะใช้เวลาในการอ่าน ดำเนินการ และรักษาสิ่งต่างๆให้อยู่ภายใต้มาตรฐานที่วางไว้

ควรจะได้รับแรงสนับสนุนให้กล้าที่จะถามคำถามและให้คำแนะนำเพื่อที่จะปรับปรุงเอกสาร เช่น นโยบายความปลอดภัย, นโยบายการเข้าไปในสำนักงาน, นโยบายเกี่ยวกับการจัดพื้นที่ในสำนักงาน , รายการอุปกรณ์สิ่งของ, แผนสำหรับการทิ้งขยะ หรือทำลายที่เป็นกระดาษเอกสารต่างๆ, ขั้นตอนการดำเนินการกรณีฉุกเฉินที่เกี่ยวกับเรื่องต่างๆ และการกู้คืนข้อมูล

๔.๒.๓ จะต้องมีการทบทวนนโยบายความปลอดภัยอยู่เป็นระยะ และปรับปรุงแก้ไขเพื่อที่จะสะท้อนให้รู้ว่ามีนโยบายอะไรได้เปลี่ยนแปลงไปบ้างตั้งแต่มีการทบทวนครั้งที่แล้ว และแน่นอน อย่าลืมที่สำรองเอกสารนโยบายความปลอดภัย ควบคู่ไปกับข้อมูลสำคัญอื่นๆ

๕. ประเภทเอกสารและข้อมูลที่จัดเก็บ

สำนักงานทั้งในภาคเอกชนและรัฐบาลมักจะมีเอกสารเข้า – ออกหลายประเภท เป็นจำนวนมาก ซึ่งมีความสำคัญมากน้อยแตกต่างกัน เอกสารบางชิ้นมีประโยชน์ในการนำข้อมูลไปใช้ในโอกาสต่อไป นอกจากนั้นยังใช้เป็นหลักฐานในการอ้างอิง ฉะนั้นถ้าสำนักงานแห่งใดต้องการดำเนินการด้านเอกสารอย่ามีประสิทธิภาพจำเป็นต้องใช้หลักการบริหาร และการจัดเก็บเอกสารที่ดีมีระบบเพื่อให้นำข้อมูลมาใช้ได้อย่างรวดเร็ว เอกสาร (Records) หมายถึง กระดาษที่ใช้ในธุรกิจ หนังสือ แบบฟอร์ม แผนที่ หรือวัตถุอื่นๆที่บรรจุข้อความทั้งยังอาจรวมถึงสื่อกลางที่ใช้ในการจัดทำข้อมูลต่างๆของธุรกิจด้วย เช่น จดหมายโต้ตอบ, บัตร, เทป หรือไมโครฟิล์ม เป็นต้น การจัดเก็บเอกสาร (Filling) หมายถึง กระบวนการจัดระบบจำแนกและเก็บเอกสารให้เป็นระเบียบสะดวกในการนำมาใช้เมื่อต้องการ ซึ่งถือว่าเป็นเพียงส่วนหนึ่งของการบริหารงานเอกสาร (Records management) เท่านั้น

๕.๑ การวางแผน เป็นการเตรียมงานและเตรียมการปฏิบัติงานเอกสาร เตรียมวัสดุ อุปกรณ์และสถานที่ในการจัดเก็บเอกสาร เตรียมกำลังคนที่มีความรู้ในการจัดเก็บเอกสาร รวมทั้งกำหนดนโยบายปฏิบัติงานต่างๆ ดังนี้

๕.๑.๑ การจัดเก็บเอกสารไว้ทั้งที่ศูนย์และหน่วยงานต่างๆ เป็นการบริหารงานเอกสารโดยให้มีศูนย์กลางของเอกสารหรือจะแยกควบคุมตามหน่วยงานย่อย หรืออาจใช้ทั้ง ๒ ระบบ กำหนดโครงสร้างของงานเอกสารว่าจะให้งานเอกสารเก็บไว้ที่ศูนย์กลางแห่งเดียวกัน (Centralization filing) เก็บไว้ที่หน่วยงานต่างๆ (Decentralization filing) หรือเก็บไว้ทั้งที่ศูนย์กลางและหน่วยงานต่างๆ โดยพิจารณาถึงข้อดีของแต่ละกรณีดังนี้ การเก็บไว้ที่ศูนย์กลาง มีข้อดีคือ ปริมาณงานและอุปกรณ์ในการทำงานน้อย บุคลากรมีความชำนาญเฉพาะด้านและทำงานมีประสิทธิภาพ ประหยัดค่าใช้จ่ายด้านบุคลากรและอุปกรณ์ ส่วนข้อเสียก็คือ หน่วยงานต่างๆ เมื่อต้องการใช้ข้อมูลจะขาดความคล่องตัวในการทำงานการเก็บไว้ที่หน่วยงานต่างๆ มีข้อดีคือ เหมาะกับข้อมูลที่มีลักษณะเป็นความลับ การเก็บและการนำออกมาใช้สะดวกและรวดเร็ว แต่มีข้อเสียก็คือ วัสดุอุปกรณ์และพนักงานต้องกระจายตามหน่วยงานต่างๆทำให้ไม่ประหยัดและวิธีปฏิบัติงานอาจแตกต่างกันการเก็บไว้ทั้งที่ศูนย์และหน่วยงานต่างๆ(Centralization and decentalization filing) การจัดเก็บวิธีนี้มีวัตถุประสงค์จะขจัดข้อเสียของทั้ง ๒ วิธี การจัดแบบนี้อาจทำได้ดังนี้ให้หน่วยงานต่างๆเก็บเอกสารและเพื่อให้เกิดการประสานงานกันและถือปฏิบัติเป็นระบบเดียวกันก็จะจัดให้มีศูนย์กลางการควบคุมทำหน้าที่รับผิดชอบในการบริหารงานเอกสารขององค์การแบ่งเอกสารส่วนหนึ่งเก็บแบบผสม ส่วนหนึ่งเก็บไว้ที่ศูนย์กลางและอีกส่วนหนึ่งเก็บไว้ที่หน่วยงานต่างๆ ทั้งนี้ต้องพิจารณาถึงลักษณะของงานและประเภทของเอกสารที่จัดเก็บ

๕.๑.๒ การเก็บรักษา การเก็บรักษาหนังสือนั้นควรแบ่งออกเป็นการเก็บในระหว่างปฏิบัติ และเก็บเมื่อปฏิบัติเสร็จเรียบร้อยแล้ว วิธีเก็บรักษา เช่น การเก็บในระหว่างปฏิบัติ เป็นการเก็บหนังสือที่ปฏิบัติยังไม่เสร็จก็ถือว่าอยู่ในความรับผิดชอบของผู้ปฏิบัติหรือของผู้ที่รับเรื่องไว้เก็บเมื่อปฏิบัติเสร็จแล้ว ผู้เก็บต้องทำหลักฐานการเก็บหรืออาจโอนเอกสารไปแยกเก็บไว้ต่างหาก เพื่อประหยัดต้นทุนในการเก็บรักษา

การทำลายเอกสารเอกสารที่ไม่มีประโยชน์แล้วอาจทำลายเสียโดยใช้เครื่องมือหรือโดยวิธีอื่นๆ โดยก่อนทำลายนั้นจะต้องเสนอรายการชื่อหนังสือที่สมควรทำลายแก่ผู้บังคับบัญชาพิจารณาให้ทำลาย โดยมีข้อพิจารณาดังนี้เอกสารที่จะต้องเก็บรักษาไว้ มีเอกสารอะไรบ้างที่สำคัญและจะต้องเก็บไว้นานเท่าใด หากไม่มีหลักเกณฑ์ที่รัดกุมแล้ว อาจเป็นเหตุให้สูญเสียเอกสารที่สำคัญไป และอาจก่อให้เกิดความเสียหายตามมา ดังนั้นจึงต้องหาวิธีการจัดการทำลายเอกสารอย่างไร เพื่อไม่ให้ความลับรั่วไหลไปสู่บุคคลภายนอก ปัญหาสำคัญจึงอยู่ที่ว่าจะตัดสินใจอย่างไรว่าเอกสารใดควรเก็บ เอกสารใดควรทำลายทิ้ง สิ่งที่ต้องคำนึงถึงก็คือ ความสำคัญของเอกสารนั้นๆ จึงได้กำหนดคุณค่าของเอกสารลับเป็น ๕ ประการ คือ ๑) คุณค่าทางกฎหมาย ถือว่าเป็นจุดสำคัญที่ต้องมีการเก็บรักษาเอกสาร เพราะเอกสารทุกชิ้นล้วนมีคุณค่าในการใช้เป็นหลักฐานทางกฎหมายทั้งสิ้น ซึ่งจะนำไปแสดงต่อศาลได้เมื่อมีคดีความเกิดขึ้น, ๒) คุณค่าทางด้านการบริหาร เอกสารประเภทนี้มักได้แก่ ระบบคำสั่งคู่มือ การปฏิบัติงานด้านต่างๆ ที่ใช้เป็นบรรทัดฐานในการดำเนินงาน เอกสารเหล่านี้ต้องมีการเก็บรักษาไว้เพื่อใช้เป็นหลักปฏิบัติต่อๆไป ๓) คุณค่าทางวิจัย ได้แก่ ข้อมูลต่างๆ ที่มีการศึกษาค้นคว้าเก็บไว้ ซึ่งสามารถใช้เป็นการประกอบการวางแผนงาน หรือเป็นลู่ทางในการดำเนินการอย่างใดอย่างหนึ่ง ๔) คุณค่าทางประวัติศาสตร์ ได้แก่ เอกสารที่เกี่ยวกับการก่อตั้งบริษัท รายชื่อผู้ถือหุ้น ฯลฯ ซึ่งถูกส่งไปเก็บไว้ที่ศูนย์เอกสารธุรกิจ กรมทะเบียนการค้า กระทรวงพาณิชย์ เพื่อเป็นหลักฐานในการดำเนินงานของบริษัท เอกสารเหล่านี้จะถูกเก็บไว้โดยไม่มีการทำลาย ไม่ว่าบริษัทนั้นๆ จะยังอยู่หรือปิดกิจการไปแล้ว ๕) คุณค่าทางการแจ้งข่าวสาร ได้แก่ เอกสารเกี่ยวกับการประชาสัมพันธ์ข่าวเกตุการณ์ทั่วไป รวมทั้งคำปราศรัย สุนทรพจน์ ฯลฯ ซึ่งเป็นสิ่งที่ก่อให้เกิดความเข้าใจอันดี

อายุการเก็บเอกสารจะพิจารณาว่าเอกสารใดกฎหมายกำหนดให้เก็บไว้นานเท่าใดและไม่สิ้นเปลืองเนื้อที่หรือค่าใช้จ่ายในการจัดเก็บ รวมทั้งความจำเป็นในการใช้เอกสาร และอายุความของการฟ้องร้องทางกฎหมายเกี่ยวข้องกับเอกสารนั้นตามพระราชบัญญัติการบัญชี ให้เก็บรักษาบัญชีและเอกสารประกอบการลงบัญชีไว้ไม่น้อยกว่า ๑๐ ปี นับแต่วันปิดบัญชี ตามประกาศกระทรวงพาณิชย์ ให้เก็บรักษาบัญชีและเอกสารการลงบัญชีสำหรับปีนั้นมาแล้วไม่น้อยกว่า ๕ ปี นับแต่วันปิดบัญชี หรือวันที่ลงรายการครั้งสุดท้ายในบัญชีเงินสด ในกรณีที่ไม่มีการปิดบัญชีต้องมีหนังสือของกรมสรรพากร แสดงว่าได้ชำระภาษีครบถ้วนแล้ว สำหรับปีนั้นๆ และมีการยื่นคำขออนุญาตต่อสำนักงานบัญชีกลางก่อนทำลายตามกฎหมายแรงงาน ให้นายจ้างซึ่งมีลูกจ้างรวมกันตั้งแต่ ๑๐ คนขึ้นไปเป็นประจำ จัดทำทะเบียนลูกจ้างและเอกสารเกี่ยวกับการคำนวณค่าจ้างเป็นภาษาไทยและเก็บไว้ ณ สถานที่ทำงานพร้อมที่จะให้พนักงานตรวจแรงงานตรวจได้ทะเบียนลูกจ้าง

อย่างน้อยต้องมีรายการต่อไปนี้ ชื่อ – สกุล เพศ สัญชาติ วันเดือนปีเกิด อายุ ที่อยู่ปัจจุบัน วันที่เริ่มจ้าง อัตราค่าจ้างและประโยชน์ตอบแทน วันสิ้นสุดของการจ้าง ให้นายจ้างเก็บรักษาทะเบียนลูกจ้างไว้ไม่น้อยกว่า ๒ ปี นับแต่วันสิ้นสุดของการจ้างลูกจ้างแต่ละราย เมื่อมีการเปลี่ยนแปลงรายการในทะเบียนลูกจ้างให้นายจ้างแก้ไขเพิ่มเติมทะเบียนลูกจ้างให้แล้วเสร็จภายใน ๑๔ วัน นับแต่วันที่มีการเปลี่ยนแปลงนั้น สำหรับเอกสารเกี่ยวกับการคำนวณค่าจ้าง ค่าล่วงเวลา และค่าทำงานในวันหยุดนั้นอย่างน้อยต้องมีรายการต่อไปนี้ วันและเวลาทำงาน ผลงานที่ทำได้สำหรับลูกจ้าง ค่าจ้างตามผลงาน (เป็นหน่วย) ค่าล่วงเวลา ค่าทำงานในวันหยุด ลายมือลูกจ้างลงชื่อรับเงินเอกสารที่ต้องเก็บเอาไว้ตลอดไป ได้แก่ เอกสารก่อตั้งบริษัท ทะเบียน หุ้นส่วนทะเบียน และข้อปฏิบัติต่างๆ รวมทั้งรายงานการประชุมเอกสารที่ต้องเก็บไว้ ๑๐ ปี ได้แก่ เอกสารประกอบการลงบัญชี, เอกสารการชำระภาษีอากร และใบเสร็จรับเงิน เอกสารที่ต้องเก็บไว้ ๕ ปี ได้แก่ สัญญาเงินกู้ที่ชำระเสร็จสิ้นแล้ว และหลักฐานการจ่ายค่าจ้างเงินเดือน เอกสารที่ต้องเก็บไว้๒ ปี ได้แก่ หลักฐานการจ่ายค่าแรง บริการ ค่าเช่าต่างๆ และทะเบียนประวัติพนักงานที่ออกแล้ว เอกสารที่ต้องเก็บไว้ ๑ ปี ได้แก่ เอกสารทั่วไปที่ไม่มีความสำคัญ หลักการเก็บที่กล่าวมาข้างต้นเป็นหลักเกณฑ์ทั่วๆไป แต่สำหรับการประกอบธุรกิจในกิจการแต่ละแห่งอาจไม่เหมือนกัน ซึ่งผู้ดูแลรับผิดชอบควรจะได้มีการปรึกษาหารือกับผู้บังคับบัญชา หรือผู้บริหาร เพื่อให้ทราบถึงนโยบายการเก็บรักษาเอกสารจะทำให้สามารถลดความวุ่นวายตามมาในภายหลังได้ มาตรการและขั้นตอนในการทำลายเอกสาร เมื่อหมดความจำเป็นที่จะต้องเก็บรักษาไว้ก็ควรจะทำลายไม่ปล่อยทิ้งไว้ แต่การทำลายต้องมีหลักเกณฑ์ ต้องควบคุมกันอย่างรัดกุม นับตั้งแต่เริ่มขนย้ายไปจนกระทั่งการทำลายเสร็จ มิฉะนั้นอาจเกิดความเสียหายตามมา เช่น ความลับรั่วไหล, เอกสารสำคัญถูกทำลายโดยรู้เท่าไม่ถึงการณ์ และเอกสารอาจถูกทำลายโดยเจตนาการที่ความลับจะรั่วไหลไปได้นั้นอาจมีผู้หยิบเอกสารบางอย่างไปตอนกำลังขนย้ายหรือเอกสารที่หลงเหลือจากการทำลายกลายไปเป็นหลักฐานสำคัญของคู่แข่งขันไป ข้อเสนอแนะในขั้นตอนการทำลายเอกสารมีดังนี้

ขั้นแรก ต้องทำเรื่องของอนุมัติจากผู้บริหารว่าจะทำลายเอกสารนั้นๆแล้ว จะได้ไม่เป็นการทำลายเอกสาร โดยพลการ นอกจากนี้เวลามีคดีอะไรเกิดขึ้นภายหลังก็สามารถอ้างได้ว่ารับคำสั่งมา

ขั้นที่สอง ตั้งคณะกรรมการขึ้นมาพิจารณาเอกสารที่จะทำลายโดยให้ผู้รับผิดชอบและเจ้าของอกสารมาร่วมพิจารณาพร้อมๆกัน ตัวแทนจากส่วนกลางและนักกฎหมายจะช่วยตัดปัญหาการทำลายเอกสาร โดยรู้เท่าไม่ถึงการณ์ได้

ขั้นที่สาม หลังจากที่แน่ใจว่าเอกสารใดทำลายได้ก็จะเป็นขั้นตอนทำลายเอกสาร ซึ่งจะต้องควบคุมการทำลายตั้งต้นจนจบเพื่อไม่ให้เกิดความเสียหายอย่างอื่นตามา เช่น ไม่ปรากฏข้อความใดๆ ลงเหลือให้ใครนำไปใช้ประโยชน์ได้อีก

ขั้นสุดท้าย เมื่อเอกสารถูกทำลายเรียบร้อยแล้วก็ควรทำรายงานเพื่อเสนอต่อผู้บริหารเก็บไว้เป็นหลักฐานต่อไป

ข้อมูลที่ถูกจัดเก็บในภาคเอกชนมีได้หลายรูปแบบ ทั้งในรูปของ ซีดี, แฟลชไดรฟ์, ฮาร์ดดิสก์ วิธีป้องกันภัยคุกคามความปลอดภัยของข้อมูลลักษณะนี้มี ๒ วิธี ๑) การเข้ารหัส (Encrypt) ไฟล์ เพื่อทำให้บุคคลอื่นๆ ไม่สามารถอ่านไฟล์ต่างๆ เหล่านั้นได้ หรือ๒) การซ่อนไฟล์เหล่านั้น โดยหวังว่าผู้บุกรุกจะหาข้อมูลอ่อนไหวไม่เจอ โดยโอเพนซอร์ส (FOSS) นั้นเป็นเครื่องมือที่จะช่วยให้สามารถเข้ารหัสและซ่อนไฟล์ได้ การเข้ารหัสข้อมูลเปรียบได้กับการเก็บข้อมูลไว้ในตู้นิรภัยที่ใส่กุญแจแน่นหนา เฉพาะผู้ที่มีกุญแจหรือรู้วิธีผสมอักษร (Combination) ในกรณีนี้หมายถึงกุญแจถอดรหัส หรือรหัสผ่าน เท่านั้นจึงจะเข้าถึงได้

๖. การจัดการข้อมูลอีเมลที่มีการรับส่ง

ปัญหาเกี่ยวกับเรื่อง Email จำนวนมากจนเต็มที่เก็บข้อมูลเป็นสิ่งที่พบได้ทั่วไปในเกือบทุกองค์กรที่ไม่มีการบริหารจัดการที่ดีพอ จึงต้องเสียเวลากับการจัดการลบหรือตอบจดหมายหลายร้อยฉบับต่อวัน จนไม่มีเวลาไปทำงานสำคัญอย่างอื่น ซึ่งถือเป็นปัญหาสำคัญอย่างมากและหลายบริษัทจึงมีวิธีการที่ค่อนข้างจะรุนแรงเพื่อให้พนักงานของพวกเขารู้จักการจัดการข้อความมหาศาลที่ได้รับอย่างมีประสิทธิภาพมากขึ้น การที่บริษัททั้งหลายเริ่มหาวิธีการจัดการ Email เหล่านี้แสดงให้เห็นว่านี้เป็นปัญหาใหญ่มาก โดยวิธีการจัดการ Email เพื่อช่วยลดปัญหาของจำนวน Email ที่มากเกินนั้นจะอยู่ในส่วนถัดไป ซึ่งปัญหาใหญ่ของการส่ง Email จำนวนมากคือ พนักงานไม่รู้จุดประสงค์ที่ชัดเจนของการทำงานและทำให้การส่ง Email นั้นไม่มีประสิทธิภาพ หากองค์กรมีกระบวนการตัดสินใจที่คลุมเครือและพนักงานก็ไม่เข้าใจว่าต้องการอะไรจากเพื่อนร่วมงาน พวกเขาก็จะส่ง Email จำนวนมากทั้งเรื่องการคุยงานหรือเรื่องการขอนัดประชุมซึ่งทำให้ระบบเกิดสภาวะแน่นขนัด ส่วนคนที่ได้รับ Email เหล่านั้นก็จะเริ่มจมดิ่งไปกับการเปิดดู Email และการขอนัดประชุมอันมากมายที่เหล่าเพื่อนร่วมงานพยายามจะเรียกให้ทุกคนไปประชุมงานกันครั้งแล้วครั้งเล่า

๖.๑ การควบคุมจัดการ Email โดยการปิดทางเข้าเสีย เช่น การยกเลิกการเป็นสมาชิกพวกจดหมายอิเล็กทรอนิกส์ หรือการปิดการแจ้งเตือนจาก Facebook หรือ Twitter หรือบอกเพื่อนร่วมงานไปตรงๆ ว่า “เลิกส่งจดหมายประเภทข้อมูลซ้ำเดิมมาเสียที เวลาที่มีการอัพเดตใหม่หรือต้องการการตัดสินใจขั้นสุดท้ายค่อยส่งมาได้ไหม” ในทางเดียวกันการที่เราส่งน้อยลงและจำกัดการส่งไปยังคนที่เราต้องการจริงๆ ก็สามารถช่วยลดปริมาณ Email ได้เช่นกัน ดังนั้นการส่ง Email ไปด้วยคำสั้นๆ เพียงคำเดียวอย่าง “ขอบคุณ” และอย่าตอบกลับทั้งหมด เพราะมันจะทำให้เป็นภาระในการจัดการ Email ในการทำงานโดยใช่เหตุจัดการ Email ให้กล่องจดหมายขาเข้าสะอาดอยู่เสมอ ขั้นตอนง่ายๆ คือสร้าง Folder ใหม่ขึ้นมาแล้วตั้งชื่อมันว่า “กล่องขาเข้าเก่า” ยัด Email หลายพันฉบับที่ค้างอยู่ในกล่องขาเข้าทั้งหมดลงไป และสามารถเข้าไปค้นหา Email เหล่านั้นได้เมื่อจำเป็นต้องให้ข้อมูลดังกล่าวทำงาน ซึ่งจะทำให้ไม่เกะกะสายตาในกล่องขาเข้าอีกต่อไป พอได้กล่องขาเข้าที่ไม่มี Email หลงเหลืออยู่แล้ว (หรืออาจจะมีเหลืออยู่บ้างเล็กน้อย) ก็จะมีพื้นที่เพียงพอในการรับ Email ใหม่ๆที่สำคัญเพื่อใช้ในการทำงาน

๖.๒ การควบคุมจัดการ Email โดยการแก้ไขหรือลบผู้ติดต่อ ในการเชื่อมต่อบุคคล คลิกผู้ติดต่อ แล้วคลิก แก้ไข หรือ ลบการคืนค่าผู้ติดต่อที่ถูกลบหากคุณลบหรือทำรายชื่อผู้ติดต่อที่สำคัญในการทำงานหายโดยบังเอิญ คุณสามารถคืนค่ารายชื่อเหล่านั้นได้ ให้ดูที่ การคืนค่าผู้ติดต่อที่ถูกลบการลบรายชื่อผู้ติดต่อที่ซ้ำซ้อนกันคุณสามารถรวมรายชื่อผู้ติดต่อที่ซ้ำซ้อนกันให้กลายเป็นรายการเดียว พร้อมข้อมูลติดต่อทั้งหมดใช้ “ล้างรายชื่อผู้ติดต่อ”ในการเชื่อมต่อบุคคล ให้คลิก จัดการ แล้วคลิก ล้างรายชื่อผู้ติดต่อ

๖.๓ การควบคุมจำนวนข้อความอีเมลและแชทที่จัดเก็บไว้ สำหรับผู้ใช้ในองค์กรสามารถระบุจำนวนวันสูงสุดที่ต้องการจัดเก็บข้อความไว้ในกล่องจดหมายของผู้ใช้ได้ การจัดเก็บข้อมูลจะอยู่ภายใต้การควบคุมของการตั้งค่าการลบอีเมลและการแชทอัตโนมัติ การตั้งค่าดังกล่าวจะใช้กับข้อความในกล่องจดหมายของผู้ใช้และข้อความที่เก็บถาวร นอกจากนี้การตั้งค่ายังมีผลกับข้อความที่เพิ่มโดยใช้ Gmail API ด้วย โดยข้อความที่ย้ายข้อมูลมาก่อนระยะเวลาการลบอัตโนมัติที่ระบุไว้จะถูกลบออก ยกเว้นจะมีการติดแท็กด้วยป้ายกำกับเพื่อให้ยกเว้นการลบเพื่อไม่ให้มีข้อมูลล้นฮาร์ดิสที่เป็นที่เก็บข้อมูลขององค์กร นโยบายการจัดเก็บข้อมูลจะนำไปใช้กับข้อความตามเวลาที่กำหนดไว้เป็นช่วง ดังนั้นแม้ว่าจะเกินระยะเวลาจัดเก็บข้อมูลแล้วแต่ข้อความก็อาจจะยังไม่ถูกลบออก

๗. ระบบการสำรองข้อมูล

การสำรองข้อมูลเป็นสิ่งจำเป็นอย่างยิ่ง ต่อการทำงานบนเครื่องคอมพิวเตอร์ ไม่ว่าจะเป็นแบบ Desktop หรือ Server ก็ตาม การทำแบ็คอัพอาจจะช่วยให้องค์กรกู้ข้อมูลสำคัญกลับคืนมา เมื่อระบบเกิดความเสียหาย รวมไปถึงระบบปฏิบัติการล้มเหลวก็สามารถที่จะกู้กลับคืนมาโดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์ที่ติดไวรัส สามารถแก้ปัญหาได้อย่างมีประสิทธิภาพและรวดเร็ว ทำให้บริษัทหรือองค์กร เกิดความเสียหายน้อยที่สุดควรมีมาตรการป้องกันกับปัญหาดังกล่าวที่จะเกิดขึ้นมีดังต่อไปนี้

๗.๑ การสำรองข้อมูลภายในองค์กร (Information backup)

๗.๒ การจัดทำบันทึกการสำรองข้อมูล (Operator logs)

๗.๓ การรายงานข้อผิดพลาด (Fault logging)

๗.๔ การสำรองข้อมูลภายนอกสำนักงาน (Off-site backup)

๗.๕ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ระบบต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญโดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

๗.๖ กำหนดนโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัดและมีนโยบายเกี่ยวกับการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน (Business Continuity Management Policy)

บทที่ ๓

ประเภทการโจมตีและภัยคุกคามด้านไซเบอร์ต่อภาคเอกชน

๓.๑ รูปแบบการโจมตีทางไซเบอร์ในปัจจุบัน

การขยายตัวของการโจมตีทางไซเบอร์ทั่วโลกเกิดขึ้นอย่างรวดเร็ว บ่อยครั้งและรุนแรงซึ่งจะส่งผลต่อการลุกลามของอาชญากรรมไซเบอร์ และจะมีผลกระทบต่อเศรษฐกิจของประเทศทุกประเทศที่กำลังเข้าสู่ยุคอุตสาหกรรม ๔.๐ มีแนวโน้มที่ชัดเจนว่าอาชญากรรมไซเบอร์กำลังเพิ่มมากขึ้นเป็นจำนวนมาก ดังนั้นประเทศไทยจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการดำเนินการบัญญัติกฎหมายที่เกี่ยวข้อง ในการเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์และจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างเร่งด่วนเพื่อให้ทันต่อการเติบโตของภัยคุกคามด้านไซเบอร์ในอนาคต ๗ รูปแบบทั่วไปของการโจมตี Cyber Security เรื่องราวของภัยคุกคามในโลกไซเบอร์จะพบว่า มีการโจมตีมากมายหลายรูปแบบ แต่ไม่มีรูปแบบไหนเลยที่เหมือนกัน แต่ละประเภทของภัยคุกคามจะมีลักษณะการโจมตีเป็นของตัวเองถึงแม้อาจจะมีความคล้ายคลึงกันบ้างก็ตามในทำนองเดียวกันหากผู้ไม่หวังดีที่ต้องการจะคุกคามข้อมูลขององค์กรและสร้างความเสียหายให้กับองค์กร พวกเขาจะเตรียมข้อมูลและพัฒนารูปแบบอาวุธให้มีประสิทธิภาพที่มากพอในการคุกคามซึ่งหากจะทำความเข้าใจเกี่ยวกับ “ภัยคุกคาม” เหล่านี้มากเพียงใด ก็อาจจะไม่มากพอ เพราะสิ่งเหล่านี้จะพยายามหาช่องโหว่ที่จะโจมตีอยู่เสมออย่างไรก็ตามนี่คือ ๗ รูปแบบการโจมตีที่พบมากในปัจจุบัน

๓.๑.๑ Malware เป็นภัยคุกคามรุ่นบุกเบิก หากเคยเห็นการแจ้งเตือนไวรัสที่มักปรากฏขึ้นเป็นหน้าจอคอมพิวเตอร์ หรือในโปรแกรม Anti-Virus ขั้นพื้นฐานเมื่อเกิดความผิดปกติ หรือมีไวรัสปลอมแปลงเข้ามาในคอมพิวเตอร์ ซึ่งมักแฝงตัวมากับไฟล์ที่ดาวน์โหลด อีเมล์ หรือแม้แต่การเชื่อมต่อของอุปกรณ์เสริมต่างๆ

“มัลแวร์” หมายถึงรูปแบบหนึ่งของซอฟต์แวร์ ที่เป็นอันตรายต่อผู้ที่ได้รับ เช่น ไวรัส และ ransomware หากมีมัลแวร์อยู่ในคอมพิวเตอร์แล้วก็จะสามารถสร้างความเสียหายได้อย่างมาก ไม่ว่าจะเป็นการทำลายข้อมูล หรือแม้แต่การเข้าควบคุมระบบ ตัวอย่างที่ระบาดหนักก็คือ WannaCry ที่สร้างความเสียหายให้กับองค์กรทั้งในสหรัฐอเมริกา, สหราชอาณาจักร, จีน, รัสเซีย, สเปน, อิตาลี และไต้หวัน โดยมีการเปิดเผยข้อมูลจากบริษัท AVAST ซึ่งเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์รายงานว่า พบกรณีการโจมตีด้วยมัลแวร์นี้ถึง ๗๕,๐๐๐ ครั้งทั่วโลก โดยวิธีพื้นฐานที่ “มัลแวร์” จะทำงานก็คือการแฝงตัวเข้ามาในรูปแบบต่างๆ เพื่อให้ผู้ใช้ดำเนินการเพื่อติดตั้งมัลแวร์ โดย วิธีที่นิยมมากที่สุดก็คือการแฝงระบบติดตั้งเข้ามาในลิงค์เพื่อดาวน์โหลดไฟล์หรือเปิดไฟล์แนบ (เช่น ไฟล์เอกสาร Word หรือไฟล์ PDF)

๓.๑.๒. การหลอกลวงทางอินเตอร์เน็ต (Phishing) แน่นอนว่า “ภัยคุกคาม” จะไม่มีวันเกิดขึ้นแน่นอนหากไม่เปิดไฟล์หรือข้อมูลที่เป็นความเสี่ยงทั้งหลาย ซึ่งเหล่าอาชญากรไซเบอร์ก็เข้าใจประเด็นนี้เป็นอย่างดี จึงต้องมีระบบการ “Phishing” เพื่อสร้างแรงจูงใจในการเปิดไฟล์ (ที่มีมัลแวร์อันตรายแนบไว้) และเมื่อเหยื่อหลงเชื่อและทำงานเปิดไฟล์เหล่านั้น “มัลแวร์” ก็จะถูกติดตั้งและพร้อมโจมตีคอมพิวเตอร์ได้ทันทีในรูปแบบการโจมตีนี้ ผู้โจมตีอาจจะแสร้งส่งอีเมล์จากบุคคลที่สามารถไว้วางใจและสั่งการได้ เช่น ผู้บริหาร หรือองค์ที่น่าเชื่อถือของภาครัฐพร้อมแนบไฟล์ที่แฝงด้วยมัลแวร์ ตัวอย่างเช่น รายละเอียดในอีเมล์จะทำงานแจ้งว่า “มีการตรวจพบการฉ้อโกงในบัญชี แนะนำให้กรอกข้อมูลหรือเปิดไฟล์นี้เพื่อแสดงความบริสุทธิ์ใจ” ซึ่งแน่นอนว่าสิ่งเหล่านี้ล้วนเป็นกับดัก เพื่อหลอกล่อให้คลิกติดตั้งมัลแวร์นั่นเอง

๓.๑.๓. SQL Injection Attack SQL หมายถึงภาษาที่มีโครงสร้างที่เขียนด้วยภาษาของโปรแกรมที่ใช้สื่อสารกับฐานข้อมูลภายในเซิร์ฟเวอร์ และระบบ SQL นี้ถูกใช้เพื่อจัดการฐานข้อมูลของตนเอง ทำให้เมื่ออาชญาการไซเบอร์เปิดการโจมตีไปที่ SQL ก็จะส่งผลกระทบต่อระบบเซิร์ฟเวอร์โดยตรงและการโจมตีในลักษณะนี้จะเป็นการสร้างปัญหาใหญ่ให้กับองค์กรได้มากมาย เนื่องจากภายในเซิร์ฟเวอร์ของแต่ละองค์กรมักจะรวบรวม ข้อมูลของลูกค้า, ข้อมูลส่วนบุคคล, หมายเลขบัตรเครดิต และระบบการเงิน อีกทั้งการโจมตีในลักษณะนี้จะสามารถเปิดช่องโหว่บนเซิร์ฟเวอร์ SQL ซึ่งสามารถสร้างปัญหาได้ในระยะยาวเลยทีเดียวหากไม่มีการแก้ไขที่ทันท่วงที

๓.๑.๔. Cross-Site Scripting (XSS) การโจมตีในลักษณะ SQL ผู้โจมตีจะทำการโจมตีผ่านเว็บไซต์และเซิร์ฟเวอร์ที่มีช่องโหว่ เพื่อคุกคามฐานข้อมูลสำคัญต่างๆ โดยเฉพาะข้อมูลด้านการเงิน แต่ถ้าผู้โจมตีมีจุดมุ่งหมายใน การโจมตีคนที่เข้ามาใช้บริการเว็บไซต์ พวกเขาจะเลือกใช้การโจมตีแบบ XSS ซึ่งทำงานผ่านการเขียนสคริปต์ข้ามไซต์ โดยจะทำงานคล้ายคลึงกับการโจมตีแบบ SQL แต่จะแตกต่างกันที่ XSS จะไม่สร้างความเสียหายให้กับเว็บไซต์ที่เผยแพร่ข้อมูลวิธีที่เหล่าผู้โจมตีเลือกใช้กันบ่อยที่สุดก็คือ การใส่โค้ดที่เป็นอันตรายลงในช่องที่ผู้ใช้งานเว็บไซต์จะต้องเปิด หรือการฝังลิงค์ไปยัง JavaScript ภายในเว็บไซต์ ถึงแม้ว่าการโจมตีแบบ XSS จะไม่สร้างความเสียหายให้กับเว็บไซต์ แต่อย่างไรก็ตาม XSS จะสร้างความเสียหายให้กับ ชื่อเสียงของเว็บไซต์เป็นอย่างมากเลยทีเดียว สรุปได้ว่า เป้าหมายการโจมตีแบบ XSS จะโจมตีไปที่ผู้ใช้งานเว็บไซต์เท่านั้น ส่วนการโจมตีแบบ SQL จะเป็นการโจมตีที่ตัวเว็บไซต์และเซิร์ฟเวอร์

๓.๑.๕. Denial of Service (DoS) ลองจินตนาการว่า “ถนนหนึ่งเส้นที่ออกแบบขนาดมาให้เพียงพอต่อจำนวนรถที่วิ่งในทุกวัน แต่ถ้าวันหนึ่งจำนวนรถมากขึ้นกะทันหันย่อมสร้างปัญหาจราจรติดขัดให้เกิดขึ้นอย่างแน่นอน” ในทางเดียวกันหากเว็บไซต์ที่เคยรองรับจำนวนผู้ใช้งานได้ในจำนวนปกติ หากมีการเข้าใช้งานเยอะจนเกินไปก็จะทำให้เซิร์ฟเวอร์ของคุณเสียหายได้การโจมตีในลักษณะนี้คือการโจมตีแบบ DoS (Denial of Service) นั่นเอง บ่อยครั้งที่เกิดเหตุการณ์เช่นนี้ขึ้นแต่ก็มักมีเหตุผลที่อ้างกันว่ามีผู้เข้าใช้บริการเว็บจนเยอะเกินไป แต่ในบางครั้งอาจจะเป็นอันตรายจากการคุกคามของ DoS ก็เป็นได้ที่ทำให้เกิดความผิดปกติของเซิร์ฟเวอร์การโจมตีแบบ Dos หากเกิดขึ้นกับระบบคอมพิวเตอร์หลายๆส่วนพร้อมกันจะถูกเรียกว่า DDoSหรือ Distributed Denial of Service Attack ซึ่งการโจมตีในลักษณะอาจจะแก้ปัญหาได้ยากมากเลยทีเดียว เนื่องจากผู้โจมตีมี IP ที่หลากหลายจากทั่วโลกในการเข้ามาสร้างความหนาแน่นของ Traffic บนเซิร์ฟเวอร์

๓.๑.๖. Session Hijacking and Man-in-the-Middle Attacks ทุกครั้งที่ใช้งานอินเตอร์เน็ตระบบคอมพิวเตอร์จะทำการแจ้งไปยังเซิร์ฟเวอร์เพื่อยืนยันว่าเป็นใคร และต้องการขอเข้าเว็บไซต์หรือธุรกรรมใดๆบนอินเตอร์เน็ต ซึ่งในขณะเดียวกัน กระบวนการนี้หรือเซสชันนี้จะทำการเรียกดูข้อความของคอมพิวเตอร์ไม่ว่าจะเป็นเครือข่าย IP และรหัสผ่าน

ซึ่งในกระบวนการนี้เซสชันระหว่างคอมพิวเตอร์กับเว็บเซิร์ฟเวอร์ระยะไกลซึ่งจะได้รับรหัสเซสชันที่ไม่ซ้ำกัน เพื่อการรักษาข้อมูลส่วนตัวเอาไว้ อย่างไรก็ตามในระหว่างกระบวนนี้ผู้บุกรุกจะสามารถโจมตีเซสชันได้ด้วยการจับรหัส และวางตัวเองในคอมพิวเตอร์เครื่องที่ร้องขอการใช้งานเสียเอง ซึ่งแน่นอนว่าการโจมตีในลักษณะนี้จะสามารถดักจับและสกัดข้อมูลได้อย่างทั้งสองทิศทางเลยทีเดียว

๓.๑.๗. Credential Reuse ในทุกวันนี้การเข้าใช้ระบบต่างๆ จะมีการตั้งการเข้าสู่ระบบและรหัสผ่าน ซึ่งจะช่วยสร้างความภัยได้ในระดับหนึ่ง แต่อย่างไรก็ตามการรักษาความปลอดภัยที่ดีที่สุดในระดับสากลก็คือ การมีรหัสผ่านที่ไม่ซ้ำกันสำหรับแอปพลิเคชั่นเว็บไซต์และการเข้าระบบทั้งหมด ซึ่งหากตั้งค่ารหัสผ่านไว้ในแบบเดียวกัน หากโดนขโมยข้อมูลไปเพียงส่วนหนึ่ง ความเสียหายจะครอบคลุมไปได้ในหลายๆส่วนเลยทีเดียว บัญชีหลายๆบัญชีก็จะสามารถถูกแฮ็กเข้าได้อย่างง่ายดาย

๓.๒ การจารกรรมข้อมูลที่เป็นความลับหรือข้อมูลที่สำคัญขององค์กร

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ถือเป็นสิ่งที่ผู้ดูแลระบบ ต้องให้ความสำคัญ ด้วยประโยชน์ที่หลากหลายของการเข้าถึงได้ทุกที่ ทุกเวลา บนเครือข่ายอินเทอร์เน็ต สิ่งที่ต้องพึงระวังคือ ภัยคุกคาม ที่มีผลกระทบต่อความปลอดภัยในชีวิตและทรัพย์สิน ของบุคคลและหน่วยงาน ทั้งในรูปแบบการโจรกรรมข้อมูลส่วนบุคคลอันเป็นความลับ การจารกรรมทางอิเล็กทรอนิกส์ภัยคุกคาม ๓ ลำดับแรก คือ

๑. ความพร้อมใช้งานของระบบ (Availability)

๒. การโจมตีด้วยโปรแกรมไม่พึงประสงค์ (Malicious Code)

๓. การพยายามบุกรุกเข้าไปยังเครื่องคอมพิวเตอร์ของผู้อื่น (Intrusion)

ภัยคุกคาม (Threat) คือ วัตถุ สิ่งของ ตัวบุคคล หรือสิ่งอื่นใดที่เป็นตัวแทนของการกระทำอันตรายต่อทรัพย์สินขององค์กร หรือสิ่งที่อาจจะก่อให้เกิดเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ได้แก่ ความลับ (Confidentiality), ความสมบูรณ์ (Integrity) และความพร้อมใช้ (Availability) ประเภทของภัยคุกคาม เช่น ภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยเจตนา, ภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยไม่เจตนา, ภัยคุกคามที่เกิดจากภัยธรรมชาติ และภัยคุกคามที่เกิดจากผู้ใช้ในองค์กรเอง

ช่องโหว่ (Vulnerabilities) หมายถึง ความอ่อนแอของระบบคอมพิวเตอร์หรือระบบเครือข่ายที่เปิดโอกาสให้สิ่งที่เป็นภัยคุกคามสามารถเข้าถึงสารสนเทศในระบบได้ ซึ่งนำไปสู่ความเสียหายแก่สารสนเทศ เช่น การเข้าใช้งานระบบขาดกลไกการตรวจสอบชื่อผู้ใช้งานและรหัสผ่านที่ดี ทำให้ผู้ไม่ประสงค์ดีสามารถเดารหัสผ่านและลักลอบเข้าสู่ระบบได้โดยไม่ได้รับอนุญาต

ปัจจัยที่ทำให้เกิดช่องโหว่ในระบบ

๑. การจัดการบัญชีรายชื่อผู้ใช้ไม่มีประสิทธิภาพ

๒. Software Bugs

๓. No Patch

๔. ขาดการอัพเดตโปรแกรมป้องกันไวรัส (Antivirus)

๕. การปรับแต่งค่าคุณสมบัติของระบบผิดพลาด

๖. บุคลากรในองค์กร

การโจมตี (Attack) คือการกระทำบางอย่างที่อาศัยความได้เปรียบจากช่องโหว่ของระบบ โดยมีจุดมุ่งหมายเพื่อเข้าควบคุมการทำงานของระบบทำให้ระบบเกิดความเสียหาย โจรกรรมสารสนเทศ เช่น Malicious Code, Malmare, Virus, Worm, Trojan, Spyware, Backdoor, Rootkit, Denial-of-Service (Dos) หรือ Spam

การดักรับข้อมูล เป็นรูปแบบการโจมตีโดยการตั้งชื่อ Wireless Network หรือที่เรียกว่า SSID ให้มีชื่อเหมือนกับ Network เดิมที่มีอยู่ เช่น ICT Free WiFi แล้วแฮ็กเกอร์จะสามารถเห็นข้อมูลที่รับส่งกัน การป้องกันภัยคุกคามนี้มีรายละเอียดดังนี้

๑. หลีกเลี่ยงการใช้งาน Free WiFi ในพื้นที่สาธารณะหากจำเป็นต้องใช้งาน Free WiFiให้ใช้งานเฉพาะจำเป็น ไม่ควรเข้าถึงระบบที่มีความสำคัญ เช่น ระบบ e-Banking และระบบอีเมล์

๒. พิจารณาการใช้งานระบบที่มีความสำคัญที่มีการเข้ารหัสลับ เช่น เว็บไซต์ที่มีการใช้งาน https

๓. ไม่ใช้ Password ที่คาดเดาได้ง่าย เช่น คำที่มีใน Dictionary

๔. การผสมอักขระที่ซับซ้อน

๕. เปลี่ยน Password อย่างสม่ำเสมอ เมื่อถึงเวลาที่เหมาะสม เช่น ทุกๆ ๙๐ วัน

๖. ตั้ง Password ซึ่งผสมอักษรภาษาอังกฤษตัวเล็ก อักษรภาษาอังกฤษตัวใหญ่ ตัวเล็ก และตัวอักขระพิเศษ

วัตถุประสงค์ของการโจมตีทางเทคโนโลยีสารสนเทศส่วนใหญ่ คือ เพื่อล้วงข้อมูลลับ ขโมยความลับทางการค้า หรือหาทางชิงความได้เปรียบเหนือบริษัทคู่แข่ง องค์กร หรือรัฐบาลอื่น หลายปีที่ผ่านมามีเหตุการณ์การจารกรรมข้อมูลเพิ่มขึ้นอย่างมาก องค์กรจำนวนน้อยที่สามารถป้องกันตัวได้แบบครอบคลุม๔๔ ตัวอย่างที่สุ่มมาศึกษา จากคดีดังในช่วงปี ๒๕๕๔-๑๕๕๗ แสดงให้เห็นว่าการถูกเจาะระบบโดยแฮ็กเกอร์ แผ่วงกว้างออกไปเพียงใด เหยื่อมีทั้งร้านค้าปลีก (Zappos ของ Amazon), บริษัทการตลาด (Epsilon), เกมออนไลน์ (Sony), ธนาคาร (Citigroup), หน่วยงานภาครัฐ ต่างๆ (กระทรวงกลาโหมของสหรัฐฯ, รัฐบาลแคนาดา)ม ผู้รับเหมาของกองทัพ (Lockheed Martin), เว็บไซต์เครือข่ายสังคม (RockYou), ผู้ให้บริการ Cloud (Gmail ของ Google) และแม้กระทั่งบริษัทด้านความมั่นคงปลอดภัย (RSA ของ EMC, Stratfor, Symantec) กรณีที่เกิดขึ้นเมื่อเร็วๆนี้อีเมล์ประสงค์รายฉบับหนึ่งถูกส่งไป ถึงเจ้าหน้าที่กรมสรรพากรของเซาท์แคโรไลนา จนนำไปสู่การขโมยหมายเลขประกัน สังคม ๑.๙ ล้านหมายเลข ข้อมูลการคืนภาษี ๓.๘ ล้านรายการ และรายละเอียดบัญชี ธนาคาร ๓.๓ ล้านบัญชีทั่วมลรัฐการโจมตี eBay ซึ่งเป็นบริษัทยักษ์ใหญ่ด้านพาณิชย์อิเล็กทรอนิกส์ในปี๑๕๕๗ ส่งผลให้ข้อมูล เช่น ที่อยู่อีเมล์ รหัสผ่านที่เข้ารหัสไว้ วันเกิด และที่อยู่ทางไปรษณีย์ ถูกขโมย จนทาง eBay ต้องขอให้ผู้ใช้ ๑๔๕ ล้านรายของตนเปลี่ยนรหัสผ่านหลังถูกโจมตี๔๖ เดือนกันยายนปีเดียวกัน ร้านเคหะภัณฑ์ Home Depot รายงานว่าระบบ ชำระเงินของบริษัทถูกโจมตี ทำให้บัตรเครดิตและบัตรเดบิตของลูกค้ากว่า ๕๖ ล้านใบต้องตกอยู่ในความเสี่ยงจำนวนครั้งและชนิดของการบุกรุกระบบรักษาความมั่นคงปลอดภัยส่งผลต่อธุรกิจ ทุกประเภทในปี ๒๕๕๕ บริษัทขนาดกลางและเล็กต่างประสบปัญหาซึ่งเดิมจะพบแต่ ในบริษัทใหญ่ๆ เท่านั้น เช่น ๘๗% ของธุรกิจขนาดเล็กในอังกฤษถูกเจาะระบบในปี ๒๕๕๕

๓.๓ การจารกรรมทางด้านเทคโนโลยีสารสนเทศต่อภาคเอกชน

การจารกรรมทางเทคโนโลยีสารสนเทศ คือ การขโมยความลับที่เก็บในรูปแบบดิจิทัล ซึ่งอาจอยู่บนคอมพิวเตอร์หรือในเครือข่าย การโจมตีเพื่อจารกรรมมีทั้งใช้ วิธีที่อาศัยเทคโนโลยีง่ายๆ และใช้เทคโนโลยีที่ซับซ้อน ตั้งแต่การขโมยข้อมูลส่วน บุคคลไปจนถึงความลับของประเทศ ในปี ๒๕๕๖ บริษัทด้านความมั่นคงปลอดภัยใน แคลิฟอร์เนียให้ข้อมูลที่เปิดเผยได้ว่ามีแฮ็กเกอร์ชาวจีน เริ่มโจมตีองค์กร ๑๔๑ แห่ง ในอุตสาหกรรม ๒๐ ชนิดทางเทคโนโลยีสารสนเทศเป้าหมายมีทั้งหน่วยงานของ รัฐบาลและบริษัทเอกชน ตั้งแต่กระทรวงกลาโหมไปจนถึงสำนักข่าว New York Times เหตุการณ์นี้ทำให้สหรัฐฯ ฟ้องดำเนินคดีแฮ็กเกอร์ชาวจีน ๕ คน ซึ่งเชื่อว่าอยู่เบื้องหลังการขโมยความลับทางการค้าอีกตัวอย่างหนึ่งของการจารกรรมทางเทคโนโลยีสารสนเทศในฟินแลนด์ มีรายงานว่ารัฐบาลตกเป็นเหยื่อของการจารกรรมทางเทคโนโลยีสารสนเทศมานานโดยลักลอบเข้าถึงเอกสารนโยบายต่างประเทศ เอกสารเหล่านี้เชื่อกันว่าทำให้ฟินแลนด์พลาดท่า ในการเจรจาระหว่างประเทศ

๓.๔ ภัยคุกคามที่มุ่งเน้นการโจรกรรมทรัพย์สินทางปัญญา

Advanced Persistent Threats (APT) เป็นภัยคุกคามประเภทใหม่ ที่มักมุ่งเน้นการโจรกรรมทรัพย์สินทางปัญญา ซึ่งมีเป้าหมายแน่ชัด มีความต่อเนื่องรู้จักหลบซ่อนและใช้เทคนิคขั้นสูงจากการสำรวจโดย ISACA ซึ่งเป็นองค์กรเอ็นจีโอด้านการกำกับดูแลไอทีพบว่า ๖๗.๖% ของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยที่ตอบแบบสอบถาม คุ้นเคยว่า APT คืออะไรและมองว่าเป็นภัยคุกคามร้ายแรงต่อความมั่นคงของชาติและเศรษฐกิจ แต่อีก ๕๓.๔% เชื่อว่า APT ไม่ต่างอะไรจากภัยคุกคามเดิมๆ โปรแกรมสอดแนมตระกูล Net Traveler ที่เป็นอันตรายได้เริ่มทำงานตั้งแต่ปี ๒๕๔๗ แต่ไม่ค่อยแสดงพฤติกรรมไม่พึงประสงค์ จนกระทั่งปี ๒๕๕๓-๒๕๕๖ Net Traveler ถูกใช้โดยแฮ็กเกอร์ เพื่อเจาะระบบคอมพิวเตอร์สำคัญกว่า ๓๕๐ เครื่องใน ๔๐ ประเทศ ในปี ๒๕๕๓ Google รายงานว่าทางบริษัทเองรวมทั้งบริษัทอื่นๆ หลายสิบแห่งตกเป็นเหยื่อของการโจมตีแบบ APT ซึ่งมีที่มาจากประเทศจีน และนำไปสู่การจารกรรมทรัพย์สินทางปัญญาจาก Google

การลักขโมย หมายความรวมถึง การลักขโมยสารสนเทศ ซอฟต์แวร์ ฮาร์ดแวร์ และอุปกรณ์ต่างๆขององค์กร ถ้าเป็นการลักขโมยทรัพย์สินที่จับต้องได้ สามารถป้องกันได้โดยติดตั้งสัญญาณเตือนภัยเมื่อมีผู้บุกรุก การล็อกอุปกรณ์ด้วยกุญแจ การล็อกห้องเก็บอุปกรณ์ การออกระเบียบปฏิบัติ การติดตามหาผู้ร้ายทำได้ไม่ยากนักสำหรับทรัพย์สินที่จับต้องไม่ได้ เช่นสารสนเทศ

โค้ดโปรแกรม ต้องอาศัยความร่วมมือและวิธีการป้องกันทางเทคนิควิธีที่ซับซ้อน การติดตามหาผู้ร้ายทำได้ยาก จึงเป็นเหตุผลที่ทำให้เข้าใจถึงความจำเป็นที่องค์กรต้องกำหนดมาตรการ และจัดหาเครื่องมือในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ การลักขโมยเป็นการก่ออาชญากรรมทางคอมพิวเตอร์ที่กระทำเพื่อขโมยโปรแกรมรวมถึงการคัดลอกโปรแกรมโดยผิดกฎหมาย โดยเฉพาะการทำซ้ำหรือการละเมิดลิขสิทธิ์ซึ่งเปรียบได้กับการปล้นทรัพย์สินอันมีค่าของผู้อื่นและยากที่จะจับตัวได้เนื่องจากสามารถทำซ้ำได้ง่ายมาก ส่งผลให้บริษัทผู้ผลิตโปรแกรมได้รับความเสียหาย การใช้งานโปรแกรมที่ผลิตจากบริษัทขนาดใหญ่ได้รับความนิยมจากผู้ใช้มาก มีการผลิตและจำหน่ายออกไปในหลายๆประเทศ สร้างรายได้มหาศาลให้กับบริษัทผู้ผลิต ทำให้การละเมิดลิขสิทธิ์มีมากขึ้นด้วยเช่นกัน ด้วยเหตุนี้บริษัทผู้ผลิตโปรแกรมและบริษัทคอมพิวเตอร์ จึงรวมกันก่อตั้งองค์กรที่เรียกว่า Business Software Alliance (BSA) ขึ้นมาควบคุมและดูแลเรื่องการละเมิดลิขสิทธิ์ รวมถึงทำความเข้าใจกับผู้บริโภคให้ตระหนักถึงการใช้โปรแกรมที่ถูกกฎหมาย (www.bsa.org)องค์กรนี้ประกอบด้วยพันธมิตร ๒๓ ราย เช่น IBM, SyBase, Intel, HP, Cisco Systems, Adobe, RSA security, Bentley, Microsoft เป็นต้น กระจายอยู่ใน ๖๐ ประเทศทั่วโลก ทำให้การละเมิดลิขสิทธิ์ลดลงไปบ้าง

บทที่ ๔

แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ภาคเอกชนตามแนวยุทธศาสตร์ไซเบอร์แห่งชาติ

๔.๑ แนวทางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ตามบันทึกหลักการและเหตุผลประกอบ (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กล่าวว่า จากความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือ การติดต่อสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคลและระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือ ความเสี่ยงบนไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ดังนั้น เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคมหรือการให้บริการโดย ปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่างๆ อันครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม มีการดำเนินการที่รวดเร็ว และมีความเป็นเอกภาพ สมควรกำหนดให้มีคณะกรรมการขึ้นเพื่อกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ให้เป็นไปอย่างมีประสิทธิภาพและเกิดผลสัมฤทธิ์ ทำให้จำเป็นต้องมีการร่างมาตราต่างๆ มาเพื่อให้อำนาจหน้าที่ของคณะกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ โดยกรอบของแนวทางยุทธศาสตร์ไซเบอร์แห่งชาติจะเป็นไปตาม (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ในมาตรา ๔

มาตรา ๔ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องดำเนินการ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจาก ภายในและภายนอกประเทศ ซึ่งครอบคลุมถึง ความมั่นคงทางเศรษฐกิจ ความ

สงบเรียบร้อยภายในประเทศ และอาจส่งผลกระทบต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม ให้มีความเป็นเอกภาพ โดยให้คำนึงถึงความสอดคล้องกับกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ ซึ่งเห็นชอบโดยคณะรัฐมนตรี การดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยจึงต้องครอบคลุมในเรื่องดังต่อไปนี้

(๑) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(๒) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์

(๓) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

(๔) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์

(๔) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์

(๖) การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์

(๗) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

(๘) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์

ดังนั้นจะเห็นว่าจากมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของรัฐ จะมีเรื่องของการประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นเรื่องที่ทางผู้วิจัยกำลังศึกษาแนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ภาคเอกชน เพื่อให้เกิดความร่วมมือระหว่างภาครัฐและเอกชนด้านความมั่นคงปลอดภัยไซเบอร์ ดังจะกล่าวในแนวทางการสร้างระบบมาตรฐานความปลอดภัยไซเบอร์แบบสากลในรูปแบบต่างๆ เพื่อให้ภาคเอกชนนำมาประยุกต์ใช้กับองค์กรของตนเอง รวมทั้งสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยทางไซเบอร์ให้กับองค์กร รวมทั้งเชื่อมโยงแลกเปลี่ยนข้อมูลกับหน่วยงานของรัฐได้อย่างปลอดภัย

๔.๒ ระบบมาตรฐานความปลอดภัยไซเบอร์แบบสากล

มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากลได้แก่ มาตรฐาน U.S. DoD, มาตรฐานISO 27001: 2005, มาตรฐานFIPS PUB200, มาตรฐาน NIST 800 – 14, มาตรฐาน COBIT, และ มาตรฐานIT BPM เป็นต้น ซึ่งมาตรฐานต่างๆ เหล่านี้ทางหน่วยงานของรัฐและภาคเอกชนนำมาใช้กับองค์กรโดยมาตรฐาน ISO 27001 และมาตรฐาน COBIT นิยมนำมาใช้ในภาคเอกชนเพื่อดำเนินงานด้านการรักษาความปลอดภัยทางไซเบอร์ขององค์กร

๔.๒.๑ มาตรฐาน COBIT

กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรด้วยหน่วยงานภาคพื้นกว่า ๙๕,๐๐๐ แห่งใน ๑๖๐ ประเทศ สมาคมไอซาก้า (ISACA) (www.isaca.org) เป็นหนึ่งในผู้นำระดับ สากลในด้านการให้ความรู้ การให้การรับรองด้วยวุฒิบัตร การสร้างชุมชน(ทางวิชาชีพ) การสนับสนุนและให้การศึกษาทางด้านการให้ความเชื่อมั่นและการรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ การกำกับดูแลและการบริหารจัดการ องค์กรในด้านไอที รวมทั้งความเสี่ยงและการปฏิบัติตามกฎระเบียบข้อบังคับที่เกี่ยวข้องกับไอที สมาคมจัดตั้งขึ้นในปีค.ศ.๑๙๖๙ โดยเป็นองค์กรอิสระที่ไม่แสวงหากำไร จัดการประชุมสัมมนา (เชิงวิชาการ) ในระดับสากล ตีพิมพ์วารสาร ISACA® Journal และจัดทำมาตรฐานสากลสำหรับการตรวจสอบและควบคุมระบบสารสนเทศ ซึ่งช่วยให้หน่วยงานภาคพื้นต่างๆ ของ สมาคมมั่นใจได้ถึงความเชื่อมั่นและการสร้างคุณค่าจากระบบสารสนเทศ ทั้งยังช่วยสร้างความก้าวหน้าและให้การรับรองทักษะและความรู้ด้านไอทีผ่านทางการให้วุฒิบัตรที่ได้รับการยอมรับกันทั่วโลกได้แก่Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) และ Certified in Risk and Information Systems ControlTM (CRISCTM) สมาคม ISACAยังคงดำเนินการ ปรับปรุง COBIT® ให้เป็นปัจจุบันอยู่อย่างต่อเนื่อง ซึ่งช่วยให้ผู้ประกอบวิชาชีพทางด้านไอทีและผู้นำในองค์กรสามารถรับผิดชอบการกำกับดูแลและการบริหารจัดการด้านไอที โดยเฉพาะในด้านการให้ความเชื่อมั่น การรักษาความมั่นคงปลอดภัย ความเสี่ยงและการควบคุม ตลอดจนการส่งมอบคุณค่าให้แก่ธุรกิจ

ISACA ได้ออกแบบ COBIT 5 โดยมีวัตถุประสงค์หลักเพื่อเป็นแหล่งความรู้สำหรับผู้ประกอบวิชาชีพทาง ด้านการกำกับดูแลไอทีระดับองค์กร (Governance of Enterprise IT - GEIT)การให้ความเชื่อมั่น ความเสี่ยง และการรักษาความมั่นคงปลอดภัย ISACA ไม่ได้อ้างว่าการใช้ข้อมูลใดๆ ในCOBIT 5 จะสามารถรับรองผลสำเร็จ ไม่ควรถือว่า ข้อมูลขั้นตอนการปฏิบัติงานและการทดสอบที่จำเป็นทั้งหมดเอาไว้ และไม่ควรพิจารณาข้อมูลแยกต่างหากโดยไม่คำนึงถึงข้อมูลขั้นตอนการปฏิบัติงาน และการทดสอบอื่นๆ ที่พอจะสามารถให้ผลลัพธ์ที่เหมือนกันได้ ในการพิจารณาถึงความเหมาะสมของข้อมูล ขั้นตอนการปฏิบัติงาน หรือการทดสอบใดๆ ควรใช้วิจารณญาณ ด้านวิชาชีพของตนเพื่อพิจารณาถึงการกำกับดูแลไอทีในระดับองค์กร การให้ความเชื่อมั่น ความเสี่ยง และการรักษาความมั่นคงปลอดภัย ในสภาพแวดล้อมของระบบหรือเทคโนโลยีสารสนเทศนั้นๆ

COBIT 5 คือ กรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรในปัจจุบันซึ่งบรรจุเนื้อหาที่เป็นกรอบการดำเนินงานที่ใช้สำหรับการกำกับดูแลและการบริหารจัดการไอที ระดับองค์กร เป็นหนึ่งในชุดผลิตภัณฑ์ของ COBIT 5 ดังที่แสดงไว้ในรูปภาพที่๑

แผนภาพที่ ๔ - ๑ชุดผลิตภัณฑ์ของ COBIT 5

ที่มา :http://audit.sat.or.th/v2project/object/Download_File/COBIT-5_res_tha_1213.pdf

กรอบการดำเนินงานของ COBIT 5 จัดทำขึ้นบนหลักการ ๕ ประการซึ่งรายละเอียดจะได้กล่าวถึงในหัวข้อถัดไป และรวมถึงแนวทางที่ครอบคลุมของปัจจัยเอื้อ (Enablers)สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

ชุดผลิตภัณฑ์ COBIT 5 มีผลิตภัณฑ์ต่างๆ ดังต่อไปนี้

๑. กรอบดำเนินงาน (Framework)

๒. แนวทางสำหรับปัจจัยเอื้อ (Enabler guide) ซึ่งอธิบายในรายละเอียดถึงปัจจัยเอื้อด้านการกำกับดูแล และการบริหารจัดการอื่นประกอบด้วย

๒.๑ การสัมฤทธิ์ผลของกระบวนการ (Enabling processes)

๒.๒ การสัมฤทธิ์ผลของสารสนเทศ (Enabling information)

๒.๓ แนวทางของปัจจัยเอื้ออื่นๆ (Enablerguide)

๓. แนวทางด้านวิชาชีพ (Professional guides) ประกอบด้วย

๓.๑ การนำไปใช้งาน (Implementation)

๓.๒ สำหรับความมั่นคงปลอดภัยของสารสนเทศ (For information security)

๓.๓ สำหรับการให้ความเชื่อมั่น (For assurance)

๓.๔ สำหรับความเสี่ยง (For Risk)

๓.๕ แนวทางด้านวิชาชีพอื่นๆ

๔. สภาพแวดล้อมที่เป็นความร่วมมือกันทางออนไลน์ ซึ่งจะจัดให้มีขึ้นในอนาคตเพื่อสนับสนุนการใช้ COBIT 5

สารสนเทศเป็นทรัพยากรหลักสำหรับทุกองค์กรและเทคโนโลยี ซึ่งมีบทบาทตั้งแต่ได้จัดทำขึ้นจนถึงเวลาที่ทำลายทิ้ง เทคโนโลยีสารสนเทศก้าวหน้าขึ้นเรื่อยๆ และใช้กันอย่างแพร่หลายในองค์กร ตลอดจนในสภาพแวดล้อม ทางสังคม สาธารณะและธุรกิจด้วยเหตุนี้ ในปัจจุบันจึงยิ่งทำให้องค์กรและผู้บริหารระดับสูงต่างๆ ต้องเรียกร้องให้มี

๑. การดูแลรักษาสารสนเทศให้ได้คุณภาพสูง เพื่อใช้สนับสนุนการตัดสินใจ

๒. สร้างคุณค่าทางธุรกิจจากการลงทุนโดยมีไอทีเป็นปัจจัยเอื้อ ได้แก่ การใช้งานไอทีอย่างมีประสิทธิผลและสร้างสรรค์เพื่อให้บรรลุเป้าหมายทางกลยุทธ์และก่อให้เกิดประโยชน์ทางธุรกิจ

๓. บรรลุการปฏิบัติงานที่เป็นเลิศผ่านการใช้งานเทคโนโลยีที่เชื่อถือได้และมีประสิทธิผล

๔. ดูแลความเสี่ยงที่เกี่ยวกับไอที ให้อยู่ในระดับที่ยอมรับได้

๕. ดูแลต้นทุนของการให้บริการทางไอทีและต้นทุนทางเทคโนโลยีให้เกิดประโยชน์สูงสุด

๖. ปฏิบัติตามกฎหมาย, กฎระเบียบข้อบังคับ, ข้อตกลงตามสัญญา และนโยบายที่เกี่ยวข้อง

ในทศวรรษที่ผ่านมา คำว่า การกำกับดูแล (Governance) ได้กลายมาเป็นความคิดของธุรกิจในระดับแนวหน้า ที่แสดงให้เห็นถึงความสำคัญของการกำกับดูแลที่ดี และในทางกลับกันก็สะท้อนให้เห็นถึงความล้มเหลวของธุรกิจอันเกิดจากการละเลยการกำกับดูแลองค์กร ซึ่งคณะกรรมการบริหารและผู้บริหารระดับสูงขององค์กรที่ประสบความสำเร็จ ได้ตระหนักดีว่ามีความจำเป็นที่จะต้องนำไอทีมาใช้เสมือนกับส่วนอื่นๆ ที่มีนัยสำคัญในการดำเนินธุรกิจ คณะกรรมการบริหารและผู้บริหารทั้งหน้าที่งานทางด้านธุรกิจและไอทีจึงต้องร่วมมือและทำงานร่วมกันเพื่อให้ไอทีได้รวมอยู่ในวิธีปฏิบัติด้านการกำกับดูแลและการบริหารจัดการ นอกจากนี้ ยังมีการออกกฎหมายใหม่ๆ และกฎข้อบังคับที่นำมาใช้เพิ่มขึ้นอย่างต่อเนื่องเพื่อจัดการกับความจำเป็นดังกล่าว

COBIT 5 นั้นได้ให้กรอบการดำเนินงานที่ครอบคลุม เพื่อช่วยให้องค์กรบรรลุวัตถุประสงค์ในเรื่องการกำกับดูแลและการบริหาร จัดการไอทีระดับองค์กร กล่าวง่ายๆ ก็คือ ช่วยองค์กรสร้างคุณค่าที่เกิดประโยชน์สูงสุดจากไอที โดยการรักษาความสมดุล ระหว่างประโยชน์ที่จะได้รับ กับระดับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุด

COBIT 5 เอื้อให้ไอทีได้รับ การกำกับดูแลและบริหารจัดการในแบบองค์รวมสำหรับทั่วทั้งองค์กร โดยครอบคลุมหน้าที่งานตามความรับผิดชอบทั้งทาง ด้านธุรกิจและไอทีอย่างครบวงจร รวมถึงพิจารณาถึงผลประโยชน์ที่เกี่ยวข้องกับไอทีของผู้มีส่วนได้เสียทั้งภายในและภายนอก

COBIT 5 สามารถใช้ได้ทั่วไปและใช้ประโยชน์ได้สำหรับองค์กรทุกขนาด ไม่ว่าจะเป็นองค์กรการค้า องค์กรที่ไม่แสวงหา กำไร หรือในภาคเอกชน

COBIT 5 ตั้งอยู่บนพื้นฐานของหลักการสำคัญ ๕ ประการในการกำกับดูแลและการบริหารจัดการไอที ระดับองค์กรได้แก่

หลักการที่ ๑ การตอบสนองความต้องการของผู้มีส่วนได้เสีย

องค์กรตั้งอยู่เพื่อที่สร้างคุณค่าสำหรับผู้มีส่วนได้เสีย โดยการรักษาความสมดุลระหว่างผลประโยชน์ที่จะได้รับกับความเสี่ยงและการใช้ทรัพยากรที่ทำให้เกิดประโยชน์สูงสุด โดย COBIT 5 ได้ให้กระบวนการที่จำเป็นทั้งหมดและปัจจัยเอื้ออื่นๆ ที่ใช้สนับสนุนการสร้างคุณค่าแก่ธุรกิจจากการใช้ไอที เพราะว่าทุกองค์กรมีวัตถุประสงค์ที่แตกต่างกัน ซึ่งองค์กรสามารถปรับแต่ง COBIT 5 ให้เหมาะกับบริบทของตนผ่านทางการส่งทอดเป้าหมาย (goal cascade) โดยการแปลงเป้าหมายองค์กรในภาพรวมไปสู่เป้าหมายในระดับที่สามารถบริหารจัดการได้ จะมีความเฉพาะเจาะจง, มีความเกี่ยวข้องกับไอที และการเชื่อมโยงหรือเทียบเป้าหมายนี้กับกระบวนการหรือแนวปฏิบัติหนึ่งๆ

หลักการที่ ๒ การครอบคลุมทั่วทั้งองค์กรอย่างครบวงจร

COBIT 5 บูรณาการการกำกับดูแลไอทีระดับองค์กรเข้าไปในการกำกับดูแลองค์กรและครอบคลุมทุกหน้าที่งานและกระบวนการภายในองค์กร COBIT 5 ไม่เน้นเพียงแค่ ‘หน้าที่งานด้านไอที’ เท่านั้น แต่จะถือว่าสารสนเทศและเทคโนโลยีที่เกี่ยวข้องเป็นสินทรัพย์ที่ทุกคนในองค์กรจำเป็นต้องดูแลเช่นเดียวกับสินทรัพย์อื่นๆ

การพิจารณาการกำกับดูแลและการบริหารจัดการปัจจัยเอื้อที่เกี่ยวข้องกับไอทีทั้งหมด เพื่อให้ครอบคลุมทั่วทั้งองค์กรอย่าง ครบวงจร ได้แก่ การรวมทุกคนและทุกสิ่งทั้งภายในและภายนอกที่เกี่ยวข้องกับการกำกับดูแลและการบริหารจัดการสารสนเทศและไอทีที่เกี่ยวข้อง

หลักการที่ ๓ การประยุกต์ใช้กรอบการดำเนินงานที่บูรณาการเป็นหนึ่งเดียว

มีมาตรฐานและแนวปฏิบัติที่ดีที่เกี่ยวข้องกับไอทีจำนวนมาก ซึ่งแต่ละอย่างก็ให้แนวทางเกี่ยวกับกิจกรรมของไอทีในด้านใดด้านหนึ่ง COBIT 5 นั้นได้นำมาตรฐานและกรอบการดำเนินงานที่เกี่ยวข้องอื่นๆ มาจัดให้สอดคล้องกันในภาพรวม จึงสามารถใช้เป็นกรอบการดำเนินงานที่ครอบอยู่เหนือกรอบการดำเนินงานอื่นๆ สำหรับการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กร

หลักการที่ ๔ การเอื้อให้วิธีปฏิบัติแบบองค์รวมสัมฤทธิ์ผล

การกำกับดูแลและการบริหารจัดการไอทีระดับองคกรที่ มีประสทธิภาพและประสิทธิผลต้องใช้วิธีปฏิบัติแบบองค์รวมที่ได้พิจารณาถึงองค์ประกอบหลายๆ อย่างซึ่งมีปฏิสัมพันธ์ต่อกันโดย COBIT 5 จะระบุถึงกลุ่มของปัจจัยเอื้อทที่ใช้สนับสนุนการนำระบบการกำกับดูแลและการบริหารจัดการไอทีระดับองค์กรไป ใช้งานอย่างครอบคลุม

ปัจจัยเอื้อนั้นนิยามได้อย่างกว้างๆ ว่าเป็นสิ่งที่สามารถช่วยในการบรรลุวัตถุประสงค์ขององค์กร กรอบ การดำเนินงานของ COBIT 5 ระบุถึงปัจจัยเอื้อ ๗ ประเภทดังนี้

๑. หลักการ,นโยบาย และกรอบการดำเนินงาน
๒. กระบวนการ
๓. โครงสร้างการจัดองค์กร
๔. วัฒนธรรม, จริยธรรม และพฤติกรรม
๕. สารสนเทศ
๖. บริการ, โครงสร้างพื้นฐาน และระบบงาน
๗. บุคลากร, ทักษะ และศักยภาพ

หลักการที่ ๕ การแบ่งแยกการกำกับดูแลออกจากการบริหารจัดการ

กรอบการดำเนินงานของ COBIT 5 ระบุความ แตกต่างอย่างชัดเจนระหว่างการกำกับดูแลและการบริหารจัดการ หลักสองประการนี้ครอบคลุมถึงกิจกรรมที่ต่างกัน ต้องการโครงสร้างการจัดองค์กรที่แตกต่างกัน และใช่เพื่อจุดประสงค์ที่แตกต่างกัน ในมุมมองของ COBIT 5 ความแตก ต่างหลักๆ ที่เห็นเด่นชัดระหว่างการกำกับดูแลและการบริหารจัดการคือ **การกำกับดูแล (Governance) การกำกับดูแล ทำให้มั่นใจได้ว่า ความต้องการ เงื่อนไข และทางเลือกของผู้มีส่วนได้เสียได้รับการประเมิน เพื่อกำหนดวัตถุประสงค์ที่องค์กรต้องการให้บรรลุซึ่งมีความสมดุลและเห็นชอบร่วมกันการกำหนด ทิศทางผ่านการจดลำดับความสำคัญและการตัดสินใจและการเฝ้าติดตามผลการดำเนินงานและการ ปฏิบัติตามเทียบกับทิศทางและวัตถุประสงค์ที่ได้ตกลงร่วมกัน**ในองค์กรส่วนใหญ่ คณะกรรมการบริหารเป็นผู้รับผิดชอบการกำกับดูแลโดยรวมภายใต้การชี้นำของประธานกรรมการ ในองค์กรขนาดใหญ่และมีความซับซ้อน หน้าที่บางประการสำหรับการกำกับดูแลอาจมอบหมายให้กับหน่วยงานที่จัดตั้งขึ้น เป็นพิเศษในระดับที่เหมาะสม **การบริหารจัดการ (Management)ผู้บริหารวางแผน สร้าง ดำเนินงาน และเฝ้าติดตามกิจกรรมต่างๆ ให้สอดคล้องกับทิศทางที่กำหนดโดย หน่วยงานกำกับดูแล (Governance body) เพื่อให้บรรลุวัตถุประสงค์ของ**

องค์กรในองค์กรส่วนใหญ่ การบริหารจัดการรับผิดชอบโดยผู้บริหารระดับสูงภายใต้การชี้นำของประธานเจ้าหน้าที่บริหาร (CEO)

เมื่อนำหลักการทั้ง ๕ ประการนี้มารวมกันจะทำให้องค์กรสามารถสร้างกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการที่มีประสิทธิผล ซึ่งส่งผลให้การใช้สารสนเทศและการลงทุนด้านเทคโนโลยีเกิดประโยชน์สูงสุด เพื่อยังประโยชน์ให้กับผู้มีส่วนได้เสีย

แผนภาพที่๔ - ๒ หลักการของ COBIT5

ที่มา :http://audit.sat.or.th/v2project/object/Download_File/COBIT 5_res_tha_1213.pdf

๔.๒.๒ มาตรฐาน ISO / IEC 27001 ระบบมาตรฐานด้านความปลอดภัยของข้อมูล

ISO/IEC 27001:2005 (Information Security Management System: ISMS) เป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง ซึ่งข้อกำหนดต่างๆกำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศคือ ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) การประยุกต์ใช้ ISMS จะช่วยให้กิจกรรมทางธุรกิจต่อเนื่องไม่สะดุด และช่วยป้องกันกระบวนการทางธุรกิจจากภัยร้ายแรงต่างๆเช่น แผ่นดินไหว, วาตภัย, อุทกภัย และฯลฯ รวมถึงความเสียหายของระบบข้อมูล โดยครอบคุม ทุกกลุ่มอุตสาหกรรมและทุกกลุ่มธุรกิจ มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร และใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัย ให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย ก่อนจะมาเป็นมาตรฐานสากลนี้มาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799:2005 ได้รับการแก้ไขปรับปรุงมาจากมาตรฐานเดิมที่ชื่อว่า BS 77991 และ ISO/IEC 17799: 2000 ตามลำดับ เนื้อหาของมาตรฐาน ISO 27001 : 2005 จะเกี่ยวข้องกับการจัดตั้งและปฏิบัติใช้งาน

การระบบบริหารความมั่นคงของข้อมูลขึ้นในองค์กร แนวคิดของมาตรฐานส่วนนี้จะเป็นแนวทางสำคัญเนื้อหาของมาตรฐาน ISO 27001 : 2005 แบ่งออกเป็น ๘ ส่วนดังนี้

๑. ขอบเขต (Scope)

๒. มาตรฐานอ้างอิง (Normative reference)

๓. คำจำกัดความและนิยาม (Term and definitions)

๔. ระบบบริหารความมั่นคงของข้อมูล (Information security management system)

๕. หน้าที่และความรับผิดชอบของฝ่ายบริหาร (Management responsibility)

๖. การตรวจประเมินการบริหารความมั่งคงของข้อมูลภายใน (Internal ISMS audit)

๗. การทบทวนการบริหารความมั่นคงของข้อมูล (Management review of the ISMS)

๘. การปรับปรุงการบริหารความมั่นคงของข้อมูล (ISMS improvement)

เอกสารแสดงมาตรการในมาตรฐาน ISO/IEC 27001 ที่องค์กรได้มีการนำมาใช้งานและเหตุผลของการใช้ รวมทั้งมาตรการที่ไม่ได้นำมาใช้งานและเหตุผลที่ไม่ได้ใช้งาน โดยการดำเนินการดังกล่าวต้องครอบคลุมหัวข้อหลัก (Domain) ที่จำเป็นในการปฏิบัติตามเกณฑ์มาตรฐานระบบคุณภาพ ISO 27001 ซึ่งมีอยู่ทั้งหมด ๑๑ หัวข้อหลัก

หัวข้อหลักที่ ๑ ในมาตรฐานว่าด้วยเรื่อง Security Policy หรือ นโยบายการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

หัวข้อหลักที่ ๒ ในมาตรฐานว่าด้วยเรื่อง Organization of Information Security หรือ โครงสร้างพื้นฐานด้านการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

หัวข้อหลักที่ ๓ ในมาตรฐานว่าด้วยเรื่อง Asset Management หรือ การบริหารจัดการสินทรัพย์ที่เกี่ยวกับสารสนเทศขององค์กร

หัวข้อหลักที่ ๔ ในมาตรฐานว่าด้วยเรื่อง Human Resource Security หรือการรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคลที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

หัวข้อหลักที่ ๕ ในมาตรฐานว่าด้วยเรื่อง Physical & Environmental Security หรือการรักษาความมั่นคงปลอดภัยทางกายภาพที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

หัวข้อหลักที่ ๖ ในมาตรฐานว่าด้วยเรื่อง Communications & Operations Management หรือ การบริหารจัดการเรื่องการสื่อสารและการปฏิบัติงานที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

หัวข้อหลักที่ ๗ ในมาตรฐานว่าด้วยเรื่อง Access Control หรือ การควบคุมการเข้าถึงข้อมูลสารสนเทศ

หัวข้อหลักที่ ๘ ในมาตรฐานว่าด้วยเรื่อง Information Systems Acquisition Development &Maintenance หรือ การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

หัวข้อหลักที่ ๙ ในมาตรฐานว่าด้วยเรื่อง Information Security Incident Management หรือ การบริหารการเตรียมความพร้อมเพื่อรับเหตุการณ์ที่ไม่คาดฝันที่อาจเกิดขึ้นกับระบบสารสนเทศ

หัวข้อหลักที่ ๑๐ ในมาตรฐานว่าด้วยเรื่อง Business Continuity Management หรือการบริหารการดำเนินธุรกิจอย่างต่อเนื่อง

หัวข้อหลักที่ ๑๑ ในมาตรฐานว่าด้วยเรื่อง Compliance หรือ การปฏิบัติตามกฎระเบียบข้อบังคับ

ทั้งนี้ในแต่ละหัวข้อหลัก หรือ Domain จะประกอบไปด้วย วัตถุประสงค์ของการควบคุมตามเกณฑ์มาตรฐาน หรือ Control Objectives และในแต่ละ Control Objectives นั้นจะประกอบไปด้วย ตัวควบคุมตามเกณฑ์มาตรฐาน หรือ Controls ดังนั้นใน เกณฑ์มาตรฐานระบบคุณภาพISO 27001 ซึ่งประกอบด้วย Domain ทั้งหมด ๑๑ หัวข้อ จะมี Control Objectives ทั้งหมด ๓๙ ข้อ และมี Controls ทั้งหมด ๑๓๓ ข้ออย่างไรก็ตามองค์กรไม่จำเป็นต้องมีการดำเนินงานตาม Control Objectives ทั้งหมด ๓๙ ข้อ และไม่จำเป็นต้องมีการดำเนินงานตาม Controls ทั้งหมด ๑๓๓ ข้อ เนื่องจากทั้งนี้ทั้งนั้นขึ้นอยู่กับ ลักษณะภารกิจ และ การวิเคราะห์ผลกระทบทางธุรกิจ หรือ Business ImpactAnalysis : BIA ของแต่ละองค์กรนั่นเอง

๔.๓ แนวทางมาตรการรักษาความปลอดภัยไซเบอร์ตามขนาดของธุรกิจ

กลุ่มธุรกิจที่สามารถนำบริษัทเข้าจดทะเบียนในตลาดหลักทรัพย์ได้จะต้องมีการดำเนินการมาตรการรักษาความปลอดภัยตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ อธ./น. 5/2547 เรื่องแนวทางปฏิบัติในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์เพื่อให้บริษัทหลักทรัพย์สามารถปฏิบัติตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ที่ สธ./น. 34/2547 เรื่องการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ ได้อย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกันสำนักงานจึงได้วางแนวทางให้บริษัทหลักทรัพย์ใช้ในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศโดยแนวทางปฏิบัตินี้ประกอบด้วยแนวทางข้อที่มีนัยสำคัญ (Mandatory [M]) และแนวทางที่เป็นข้อเสนอแนะเพิ่มเติม (Accredit [A]) โดยหากบริษัทหลักทรัพย์ได้ปฏิบัติตามแนวทางข้อที่มีนัยสำคัญ (Mandatory [M]) อย่างครบถ้วน สำนักงานจะถือว่าบริษัทหลักทรัพย์ได้ปฏิบัติเป็นไปตามประกาศข้างต้นแล้ว ทั้งนี้หากบริษัทหลักทรัพย์สามารถปฏิบัติได้ตามแนวทางที่เป็นข้อเสนอแนะเพิ่มเติม (Accredit [A]) จะทำให้บริษัทหลักทรัพย์สามารถควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ซึ่งจะมีผลให้ได้รับการประเมินการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศอยู่ในระดับที่ดียิ่งขึ้น อย่างไรก็ดีบริษัทหลักทรัพย์อาจดำเนินการในแนวทางปฏิบัติอื่นที่แตกต่างจากแนวทางปฏิบัติฉบับนี้ได้หากแสดงต่อสำนักงานได้ว่าแนวทางอื่นนั้นสามารถป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศได้และมีประสิทธิภาพเพียงพอ ตลอดจนอยู่ในมาตรฐานที่ยอมรับได้สำหรับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์

สาระสำคัญของแนวทางปฏิบัติฉบับนี้ประกอบด้วย

๑. นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศเพื่อให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งได้รับทราบเกี่ยวกับหน้าที่และความรับผิดชอบ และแนวทางปฏิบัติในการควบคุมความเสี่ยงด้านต่างๆ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการจัดทำนโยบาย รายละเอียดของนโยบาย และการปฏิบัติตามนโยบาย

๒. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์ ซึ่งเป็นการลดความเสี่ยงด้าน Infrastructure risk

๓. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security) เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึงล่วงรู้ (Access risk), แก้ไขเปลี่ยนแปลง (Integrity risk) หรือการก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ ส่วนการป้องกันความเสียหายมีวัตถุประสงค์เพื่อป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (Availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ และระบบป้องกันความเสียหายต่างๆ ที่บริษัทหลักทรัพย์ควรจัดให้มีภายในศูนย์คอมพิวเตอร์

๔. การรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ และระบบเครือข่าย (Information and Network Security) เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึงล่วงรู้ (Access risk) หรือแก้ไขเปลี่ยนแปลง (Integrity risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง ส่วนการป้องกันการบุกรุกผ่านระบบเครือข่ายมีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส รวมทั้ง Malicious code ต่างๆ มิให้เข้าถึง (Access risk) หรือสร้างความเสียหาย (Availability risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมรายละเอียดเกี่ยวกับแนวทางในการรักษาความปลอดภัยข้อมูลระบบคอมพิวเตอร์ เครื่องแม่ข่าย และระบบเครือข่าย

๕. การควบคุมการพัฒนา หรือแก้ไขเปลี่ยนแปลงของระบบงานคอมพิวเตอร์ (Change Management) เพื่อให้ระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องของผู้ใช้งาน ซึ่งเป็นการลดความเสี่ยงด้าน integrity risk โดยมีเนื้อหาครอบคลุมกระบวนการพัฒนา หรือแก้ไขเปลี่ยนแปลงตั้งแต่เริ่มต้นซึ่งได้แก่การร้องขอไปจนถึงการนำระบบงานที่ได้รับการพัฒนา หรือแก้ไขเปลี่ยนแปลงไปใช้งานจริง

๖. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่องมีประสิทธิภาพ และในเวลาที่ต้องการ (Availability risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบและการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน

๗. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ (Computer Operation) เพื่อให้มีการใช้งานระบบคอมพิวเตอร์ได้อย่างถูกต้อง ต่อเนื่อง และมีประสิทธิภาพ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ต่างๆซึ่งได้แก่ การติดตามการทำงานของระบบคอมพิวเตอร์ การจัดการปัญหา และการควบคุมการจัดทำรายงาน ซึ่งเป็นการลดความเสี่ยงด้าน Integrity risk และ Availability risk

๘. การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) อาจก่อให้เกิดความเสี่ยงต่อบริษัทหลักทรัพย์ในรูปแบบที่แตกต่างไปจากการดำเนินงานปกติโดยบริษัทหลักทรัพย์เอง เช่น ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล (Access risk) ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการประมวลผลของระบบงาน (Integrity risk) ที่อาจเพิ่มขึ้นจากการดำเนินงานของผู้ให้บริการ เป็นต้น ดังนั้น การควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นจึงมีวัตถุประสงค์เพื่อให้บริษัทหลักทรัพย์ใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นได้อย่างมีประสิทธิภาพ เป็นที่น่าเชื่อถือ และสามารถควบคุมความเสี่ยงที่เกี่ยวข้องได้ โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางในการคัดเลือกและควบคุมการปฏิบัติงานของผู้ให้บริการ

ส่วนกลุ่มธุรกิจที่ไม่ได้เป็นบริษัทที่เข้าจดทะเบียนในตลาดหลักทรัพย์ ซึ่งมีเป็นจำนวนมากทั้งขนาดใหญ่ ขนาดกลางและขนาดเล็ก อาจไม่คิดถึงความปลอดภัยทางไซเบอร์เพราะไม่ได้ถูกกำหนดให้ต้องดำเนินการและก็คงไม่คิดว่าจะเกิดความไม่ปลอดภัยทางไซเบอร์ขึ้นกับบริษัทในขณะที่เศรษฐกิจกำลังเติบโต มีบริษัทที่ไม่สามารถปกป้องข้อมูลของตัวเองได้จำนวนที่มากยิ่งขึ้น ในขณะที่มีบริษัทจำนวนมากที่อ้างว่า ไม่จำเป็นต้องปกป้องตัวเองเนื่องจากบริษัทมีขนาดเล็กจนเกินกว่าที่จะถูกโจมตี ดังนั้นจึงไม่ต้องการใช้เวลาหรือเงินไปกับบางสิ่งที่พวกเขาไม่เชื่อว่าจะเกิดขึ้น อย่างไรก็ตาม การป้องกันการโจมตีไม่ให้เกิดขึ้นตั้งแต่แรกมีค่าใช้จ่ายน้อยกว่าการแก้ไข มีวิธีการอย่างไรบ้างที่จะป้องกันการโจมตีทางไซเบอร์นี้ได้คือ การให้ความรู้และอัพเดทข่าวสารกับพนักงานของบริษัทเกี่ยวกับการโจมตีทางไซเบอร์ถือเป็นวิธีที่ดีที่สุดอย่างหนึ่งในการป้องกัน อย่างไรก็ตามควรระมัดระวังให้มากและควรกำหนดมาตรการเบื้องต้นในการควบคุมความปลอดภัยทางไซเบอร์ของกลุ่มธุรกิจเหล่านี้ ดังต่อไปนี้

๑. การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)

๒. การแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) เพื่อให้มีการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในฝ่ายคอมพิวเตอร์ ซึ่งเป็นการลดความเสี่ยงด้าน infrastructure risk

๓. การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)

๔. ติดตั้งซอฟต์แวร์ป้องกันไวรัส หรือใช้ Firewall ปกป้องไวรัสไม่ให้เข้ามายังเครื่องคอมพิวเตอร์

๕. ใช้ VPN หรือ Virtual Private Networks เพื่อให้พนักงานที่ทำงานผ่านทางไกลสามารถทำงานได้อย่างปลอดภัยบนเครือข่ายของบริษัท VPN จะสร้างอุโมงค์ระหว่างอุปกรณ์ของพนักงานกับเซิฟเวอร์ของบริษัท ซึ่งจะช่วยปกป้องมันจากแฮคจากบุคคลภายนอก

๔.๔ กระบวนการจัดทำระบบรักษาความปลอดภัยไซเบอร์ตามมาตรฐานสากล

กระบวนการจัดทำระบบรักษาความปลอดภัยไซเบอร์ตามองค์กรต่างๆ ทั้งภาครัฐและภาคเอกชนต่างก็ให้ความสำคัญอย่างมากต่อการพัฒนาระบบเพื่อการดูแลรักษาความมั่นคงปลอดภัยของสารสนเทศขององค์กร ซึ่งมีการพัฒนามาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัย

สารสนเทศออกมาอย่างต่อเนื่อง เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่างๆ ที่มีต่อระบบสารสนเทศขององค์กร ซึ่งนับวันจะทวีความรุนแรง และท้าทายต่อผู้บริหารองค์กรที่ ๕๐ รับผิดชอบในการดูแลระบบเป็นอย่างมากทำให้เกิดการพัฒนาระบบรักษาความปลอดภัยไซเบอร์ตามมาตรฐานสากลต่างๆ เพิ่มขึ้น เช่น COBIT5, ISO/IEC 27001 เป็นต้น

๔.๕ การกำหนดรายการตรวจสอบแผนความมั่นคงปลอดภัยไซเบอร์

เอกชนควรพิจารณาเรื่องดังต่อไปนี้เพื่อสร้างแผนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๑. การสร้างความตระหนักและการให้ความรู้แก่สาธารณะ

๑.๑ เตรียมโปรแกรมสร้างความตระหนัก สำหรับกลุ่มธุรกิจ ขนาดใหญ่, ขนาดกลาง และขนาดเล็ก

๑.๒ จัดฝึกอบรมอย่างสม่ำเสมอในเรื่องการใช้เทคโนโลยีสารสนเทศแก่เจ้าหน้าที่และการบังคับใช้ซอฟต์แวร์ที่อัปเกรดและมาจากแหล่งที่น่าเชื่อถือ แนวทางการใช้อินเทอร์เน็ตอย่างมั่นคงปลอดภัยและการใช้แอนติไวรัสเพื่อป้องกันมัลแวร์

๑.๓ มีแนวปฏิบัติที่เคร่งครัดในการตรวจสอบผู้จำหน่ายอุปกรณ์และระบบเทคโนโลยีสารสนเทศ เพื่อให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยด้านต่างๆ เช่น ความมั่นคงปลอดภัยของข้อมูลสาธารณะและความมั่นคงของชาติ

๑.๔ ปรับปรุงหลักสูตรการสร้างความตระหนักในเรื่องความมั่นคงปลอดภัย ทางเทคโนโลยีสารสนเทศและจัดฝึกอบรมอย่างสม่ำเสมอ

๒. การเตรียมความพร้อมในการจัดการภัยคุกคามยามวิกฤต

๒.๑ มีแผนเรื่องความมั่นคงปลอดภัยทางทางเทคโนโลยีสารสนเทศ ให้ทุกฝ่ายที่เกี่ยวข้องมีแนวทางที่ตรงกัน

๒.๒ มีหน่วยงานที่รับผิดชอบในการประสานเพื่อเตรียมความพร้อมด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการป้องกัน

๒.๓ ระบุและติดต่อผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญ เพื่อสร้างเครือข่ายประสานงานและตอบสนองที่ฉับไวเมื่อถูกโจมตี

๓. การป้องกันภัยคุกคาม

๓.๑ มีนโยบายด้านความมั่นคงปลอดภัยสำหรับการจัดซื้อ เมื่อจัดซื้อซอฟต์แวร์ของแท้ ได้รับการอัปเดต และจัดซื้อแอนติไวรัสที่น่าเชื่อถือเพื่อป้องกันมัลแวร์

๓.๒ พัฒนาแนวปฏิบัติที่ดีในการจัดซื้อสำหรับภาคเอกชน ผู้ให้บริการอินเทอร์เน็ต กลุ่มธุรกิจขนาดใหญ่, ขนาดกลาง และขนาดเล็ก

๓.๓ พัฒนา จัดทำ และบังคับใช้มาตรฐานความมั่นคงปลอดภัยทางเทคโนโลยี สารสนเทศสำาหรับผู้จัดจำาหน่ายผลิตภัณฑ์ทางเทคโนโลยีสารสนเทศ

๓.๔ พิจารณาการใช้งานบน Cloud เพื่อความมั่นคงปลอดภัย

๔. การตอบสนองต่อภัยคุกคาม

๔.๑ พัฒนาแนวทางปฏิบัติที่ดี มีการกำหนดระยะเวลาและมาตรฐานในการ อัปเกรดและอัปเดตซอฟต์แวร์ที่ใช้ในภาครัฐเป็นประจำ

๕. การลดผลกระทบอันเกิดจากภัยคุกคาม

๕.๑ พัฒนาหรือเข้าร่วมกับเครือข่ายความมั่นคงด้านเทคโนโลยีสารสนเทศ ของรัฐอื่นหรือองค์กรระหว่างประเทศอื่น เพื่อแลกเปลี่ยนข้อมูล ข่าวกรอง และสร้างแนวร่วม

๔.๖ แนวทางการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ตามแนวนโยบายภาครัฐ

ด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้นทำให้ผู้ประกอบการตลอดจนองค์กรภาครัฐและภาคเอกชนที่มีการดำเนินงานใดๆในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร เพื่อให้การดำเนินการใดๆด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมาตรฐานเป็นที่ยอมรับในระดับสากลคณะกรรมการธุรกรรมทางอิเลกทรอนิกส์จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐขึ้นมา ดังนั้นงานวิจัยฉบับนี้จึงนำเสนอแนวการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ตามแนวนโยบายภาครัฐมีแนวปฏิบัติดังต่อไปนี้

๑. กำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๒. จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๔. ต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๕. ต้องประกาศนโยบายและข้อปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าใจปฏิบัติตามนโยบายและข้อปฏิบัติได้

๖. ต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

๗. ต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

๘. มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึง สารสนเทศและการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งาน ตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๙. มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตร การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๑๐. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตการเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๑๑. มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control)เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๑๒. มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๑๓. มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

การปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ตามแนวนโยบายภาครัฐที่นำเสนอนี้เป็นเพียงแนวทางที่กำหนดให้หน่วยงานของรัฐปฏิบัติ ภาคเอกชนที่ไม่ได้มีการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ตามมาตรฐานสากล สามารถนำมาประยุกต์ใช้กับองค์กรของตนเองเพื่อให้มีความปลอดภัย

บทที่ ๕

สรุปและข้อเสนอแนะ

สรุป

ประเภทการโจมตีและภัยคุกคามด้านไซเบอร์ที่มีต่อภาคเอกชนและหน่วยงานของรัฐในปัจจุบันมีด้วยกันหลายรูปแบบ จึงมีความจำเป็นที่ภาครัฐและเอกชนต้องร่วมมือกันในการกำหนดมาตรการรักษาความปลอดภัยทางไซเบอร์ เพื่อเป็นแนวปฏิบัติในการจัดการภัยคุกคามทางไซเบอร์ โดยมีกรอบแนวคิดดังนี้

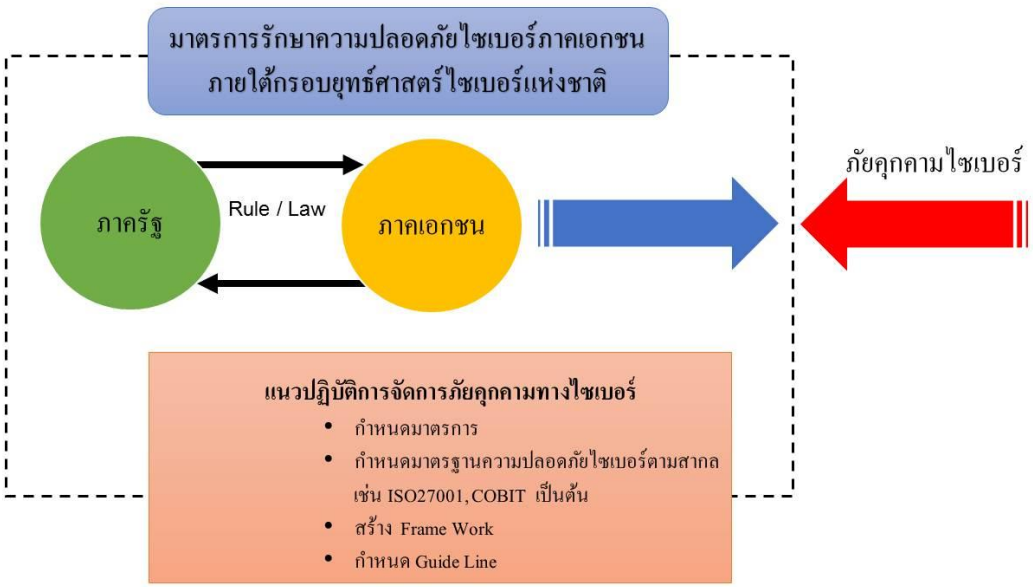
๑. กำหนดมาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์

๒. กำหนดมาตรฐานความปลอดภัยไซเบอร์ตามสากล

๓. สร้างกรอบการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ (Framework)

๔. กำหนดแนวทางการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ (Guideline)

แผนภาพที่ ๕-๑ กรอบความคิดของการวิจัย



รายละเอียดของกรอบแนวคิดที่เกี่ยวข้องกับมาตรการรักษาความปลอดภัยทางไซเบอร์และมาตราฐานความปลอดภัยไซเบอร์ตามมาตรฐานสากล ในส่วนของการสร้างกรอบการปฏิบัติตามมาตรฐานและแนวทางปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ สามารถอธิบายได้ดังนี้

๑. กำหนดมาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์

มาตราการที่เกี่ยวข้องกับการกำกับดูแลและรักษาความปลอดภัยไอทีระดับองค์กร ซึ่งมีเนื้อหาที่เป็นกรอบการดำเนินงานที่ใช้สำหรับการกำกับดูแลและรักษาความปลอดภัยไอทีควรมีรายละเอียดดังนี้

๑.๑. กำหนดนโยบายการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

๑.๒. การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคลที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

๑.๓. การรักษาความมั่นคงปลอดภัยทางกายภาพที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

๑.๔. การบริหารจัดการเรื่องการสื่อสารและการปฏิบัติงานที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

๑.๕. การควบคุมการเข้าถึงข้อมูลสารสนเทศ

๑.๖. การปฏิบัติตามกฎระเบียบข้อบังคับ และนโยบายที่เกี่ยวข้องกับระบบสารสนเทศ

๑.๗. การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

๑.๘. การเตรียมความพร้อมฉุกเฉินเพื่อรับเหตุการณ์ที่ไม่คาดฝัน

๑.๙. การบริหารการดำเนินธุรกิจอย่างต่อเนื่อง

๒. กำหนดมาตรฐานความปลอดภัยไซเบอร์ตามสากล

จากผลการวิจัยนี้ได้ทำการวิจัยเชิงคุณภาพ (Qualitative Research) โดยรวบรวมข้อมูลเรื่องแนวคิด ทฤษฎี รวมถึงวรรณกรรมที่เกี่ยวข้องกับแนวทางการป้องกันภัยคุกคามและการสร้างความมั่นคงปลอดภัยทางไซเบอร์และเปรียบเทียบกับต่างประเทศบางประเทศ รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิทางด้านนี้ เพื่อให้ได้แนวทางการสร้างมาตรฐานความปลอดภัยไซเบอร์ตามสากล งานวิจัยนี้ได้นำเสนอ

ตัวอย่างมาตรฐานสากลที่นิยมใช้กันแพร่หลายในภาคเอกชน คือ มาตรฐาน ISO / IEC 27001 และ COBIT ซึ่งผู้วิจัยได้ทำการสัมภาษณ์ผู้ทรงคุณวุฒิเกี่ยวกับการกำหนดมาตรฐานที่เหมาะสมโดย Compliance ตามมาตรฐานสากล ผู้ทรงคุณวุฒิทั้งหมดให้ความเห็นตรงกันว่าประเทศไทยยังไม่มีผู้เชี่ยวชาญหรือหน่วยงานด้านมาตรฐานเป็นที่ยอมรับในระดับสากล มากำหนดมาตรฐานขึ้นมาเพื่อใช้ในประเทศ ทำให้จำเป็นต้องทำตามมาตรฐานสากลที่มีอยู่และดัดแปลงบางอย่างให้เหมาะสมกับขนาดขององค์กร

๓. สร้างกรอบการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ (Framework)

กรอบการปฏิบัติงตามมาตรฐานความปลอดภัยไซเบอร์มีขั้นตอนการดำเนินการบริหารความมั่นคงปลอดภัยสารสนเทศ จะขับเคลื่อนเป็นวงจร PDCA ดังนี้ การวางแผน (Plan) การลงมือทำ (Do) การตรวจสอบ (Check) และการปรับปรุงแก้ไข (Act)

๓.๑. การวางแผน (Plan) คือ การกำหนดนโยบายความมั่นคงปลอดภัยและระบบบริหารความมั่นคงปลอดภัย

๓.๒. การลงมือทำ (Do) คือ ลงมือดำเนินการตามระบบบริหารความมั่นคงปลอดภัย

๓.๓. การตรวจสอบ (Check) คือ การตรวจสอบและทบทวนผลการดำเนินงาน

๓.๔ การปรับปรุงแก้ไข (Act) คือ ดูแลและรักษาระบบบริหารความมั่นคงปลอดภัย

๔. กำหนดแนวทางการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์(Guideline)

แนวทางการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศมีการดำเนินการตามกรอบที่กำหนดไว้ดังนี้

การวางแผน (Plan) มีขั้นตอนของการวางแผน ดังนี้

๑. การกำหนดขอบเขต (Scope) ของระบบ โดยคำนึงถึงลักษณะทางธุรกิจ องค์กร สถานที่ ทรัพย์สิน และ เทคโนโลยี

๒. การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security management system policy)

๓. การกำหนดแนวทางในการประเมินความเสี่ยง สำหรับองค์กรและความมั่นคงปลอดภัย สารสนเทศทางธุรกิจ รวมถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

๔. การระบุความเสี่ยง

๕. การวิเคราะห์และประเมินความเสี่ยง โดยการประเมินถึงผลกระทบทางธุรกิจซึ่งเกิดจากความล้มเหลวในความมั่นคงปลอดภัย โดยคำนึงถึง ความสูญเสียในการรักษาความลับ ความสมบูรณ์หรือความพร้อมของทรัพย์สิน

๖. การกำหนดและประเมินแนวทางในการจัดการความเสี่ยง โดยแนวทางที่ใช้ในการจัดการความเสี่ยง

๗. การจัดเลือกรายการควบคุมและวัตถุประสงค์การควบคุม สำหรับการจัดการความเสี่ยง โดยในขั้นตอนนี้จะเป็น การจัดเลือกหัวข้อการควบคุม และวัตถุประสงค์การควบคุม รวมถึงการนำไปปฏิบัติเพื่อให้สอดคล้องกับแนวทางที่กำหนดจากการประเมิน และกระบวนการจัดการความเสี่ยง โดยการจัดเลือกจะพิจารณาถึงเกณฑ์ การยอมรับความเสี่ยง รวมถึงข้อกำหนดทางกฎหมาย และข้อสัญญา ต่างๆ

๘. การอนุมัติความเสี่ยงที่เหลืออยู่ โดยผู้บริหารระดับสูงขององค์กร

๙. การจัดเตรียมเอกสารแสดงการประยุกต์ใช้งาน ที่อธิบายถึงรายการของหัวข้อควบคุม (Control) และวัตถุประสงค์การควบคุม (Control objectives) ที่ได้เลือกไว้ และเหตุผลของการเลือก รวมถึงหัวข้อควบคุมและวัตถุประสงค์ควบคุมที่มีการดำเนินการอยู่ใน ปัจจุบัน หรือที่เรียกว่า Base line control ในกรณีที่หัวข้อการควบคุมใดที่ระบุว่าจะไม่มีการดำเนินการ จะต้องมี การระบุถึงเหตุผลของการยกเว้นไว้ด้วย

การลงมือทำ (Do) มีขั้นตอนของการลงมือทำ ดังนี้

๑. การจัดทำแผนการจัดการความเสี่ยง โดยระบุรายละเอียดของการดำเนินงาน ทรัพยากรที่ต้องการ ความรับผิดชอบและลำดับความสำคัญในการดำเนินงานสำหรับ การจัดการกับความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศ

๒. การดำเนินการตามแผนการจัดการความเสี่ยง เพื่อให้บรรลุตามวัตถุประสงค์การควบคุมที่ได้กำหนดไว้ รวมถึงการพิจารณาจัดสรรเงินทุนและกำหนดหน้าที่ความรับผิดชอบในการดำเนินการด้วย

๓. การดำเนินการตามการควบคุมที่ได้กำหนดไว้ เพื่อให้ได้ตามวัตถุประสงค์การควบคุม

๔. การกำหนดแนวทางในการวัดความมีประสิทธิผลของการควบคุม หรือกลุ่มการควบคุมที่ได้กำหนด

๕. การจัดฝึกอบรมและการสร้างการรับรู้ขึ้นภายในองค์กรตามมาตรฐานที่กำหนด

๖. การบริหารงานตามมาตรฐานที่กำหนด

๗. การจัดการทรัพยากรสำหรับตามมาตรฐานที่กำหนด

๘. การดำเนินงานตามวิธีการปฏิบัติงาน และการควบคุมอื่นๆ เพื่อให้สามารถตรวจ สอบเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัย และการตอบสนองต่อเหตุการณ์นั้นๆ

การตรวจสอบ (Check) องค์กรจะต้องมีการดำเนินการต่างๆ ดังนี้

๑. การดำเนินการเฝ้าติดตาม และทบทวนวิธีการปฏิบัติงานและการควบคุมต่างๆ

๒. การดำเนินการทบทวนความมีประสิทธิผลของมาตราฐานอย่างสม่ำเสมอ โดยคำนึงถึงผลของการตรวจประเมิน ความมั่นคงปลอดภัย (Audit) เหตุการณ์ที่เกิดขึ้น ผลของการวัดความมีประสิทธิผล ข้อเสนอแนะ และข้อมูลแจ้งกลับจากหน่วยงานต่างๆ ที่เกี่ยวข้อง

๓. การวัดความมีประสิทธิผลของการควบคุม เพื่อทวนสอบถึงความสอดคล้องตามข้อกำหนดความมั่นคงปลอดภัย

๔. ทบทวนการประเมินความเสี่ยงตามแผนที่ได้กำหนดไว้ รวมถึงทบทวนความเสี่ยงที่เหลืออยู่และระดับของความเสี่ยงที่สามารถยอมรับได้ โดยคำนึงถึงการเปลี่ยนแปลงในองค์กร เทคโนโลยี วัตถุประสงค์และกระบวนการทางธุรกิจ ภัยคุกคามที่ระบุไว้ ความมีประสิทธิผลของการควบคุม และเหตุการณ์ภายนอก เช่น การเปลี่ยนแปลงใน ข้อกฎหมาย ข้อบังคับตามสัญญาที่เปลี่ยนแปลง และการเปลี่ยนแปลงทางสังคม

๕. การดำเนินการตรวจประเมินมาตรฐานภายใน

๖. การดำเนินการทบทวนโดยฝ่ายบริหาร เพื่อดูแลความเพียงพอของขอบเขต และการดำเนินการปรับปรุง กระบวนการมาตรฐานที่ใช้ในองค์กร

๗. การปรับปรุงแผนความมั่นคงปลอดภัย โดยคำนึงถึงสิ่งที่พบจากการเฝ้าติดตามและการทบทวน

๘. การบันทึกผลการดำเนินการ และเหตุการณ์ที่อาจส่งผลต่อความมีประสิทธิผลหรือผลการดำเนินงานของมาตรฐาน

การปรับปรุงแก้ไข (Act) มีขั้นตอนการของการปรับปรุงและแก้ไขระบบ ดังนี้

๑. การดำเนินการปรับปรุงมาตรฐานตามที่ได้กำหนดไว้

๒. การปฏิบัติการแก้ไขและการป้องกันอย่างเหมาะสม รวมถึงการนำบทเรียนจากประสบการณ์ความมั่นคง ปลอดภัยขององค์กรอื่นๆ และขององค์กรเองมาปรับใช้อย่างเหมาะสม

๓. การสื่อสารการดำเนินการ และการปรับปรุงไปยังหน่วยงานต่างๆ ที่เกี่ยวข้องทั้งหมด การดูแลให้มั่นใจว่าการปรับปรุงเป็นไปตามวัตถุประสงค์ที่ได้กำหนดไว้

ข้อเสนอแนะ

สรุปข้อเสนอแนะของการวิจัยจำแนกตามประเภท ได้แก่ ข้อเสนอแนะเชิงนโยบายและแผน ข้อเสนอแนะเชิงกฎ ระเบียบ และกฎหมายที่เกี่ยวข้อง

๑. ข้อเสนอแนะเชิงนโยบายและแผน

๑.๑ กำหนดสิทธิประโยชน์ต่างๆ ให้กับภาคเอกชนที่ดำเนินการตามระบบมาตรฐานรักษาความปลอดภัยไซเบอร์สากลหรือที่หน่วยงานที่กำกับดูแลระบบมาตรฐานได้กำหนดขึ้น เช่น สิทธิประโยชน์ทางภาษี เป็นต้น

๑.๒ กำหนดแผนงานสนับสนุนภาคเอกชน ให้สามารถเข้าอบรมและวางแผนกำลังคนที่จะเข้ามาสู่ระบบมาตรฐานรักษาความปลอดภัยไซเบอร์สากลได้ตามแผนนโยบายยุทธศาสตร์ไซเบอร์แห่งชาติ เช่น สนับสนุนหลักสูตรการอบรมระบบมาตรฐานต่างๆ

๒. ข้อเสนอแนะเชิงกฎ ระเบียบ และกฎหมาย

๒.๑ พิจารณากฎ ระเบียบ ภาครัฐในการเชื่อมต่อข้อมูล หรือส่งข้อมูลระหว่างภาครัฐและภาคเอกชน โดยบังคับให้ภาคเอกชนที่ต้องการส่งข้อมูลหรือเชื่อมต่อข้อมูลกับภาครัฐต้องได้รับมาตรฐานรักษาความปลอดภัยไซเบอร์สากลหรือจากหน่วยงานกำกับดูแลระบบมาตรฐาน

๒.๒ พิจารณากฎหมาย “การรักษาความมั่งคงปลอดภัยทางไซเบอร์แห่งชาติ” ให้ภาคเอกชนมีหน้าที่รายงานข้อมูลเกี่ยวกับภัยคุกคาม ที่อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ เสนอต่อ กปช. ทันทีและ กปช. มีอำนาจสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง ที่มีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

๓. ข้อเสนอแนะเชิงปฏิบัติการ

๓.๑ ร่วมจัดทำโครงการความร่วมมือระหว่างภาครัฐและเอกชนในด้านการรักษาความมั่งคงปลอดภัยทางไซเบอร์แห่งชาติ ซึ่งจะทำให้เกิดการขับเคลื่อนที่สำคัญ เช่น การระดมสมอง ทรัพยากร และสรรพกำลังจากทุกภาคส่วนมาช่วยกันพัฒนา มาตรการการรักษาความปลอดภัยทางไซเบอร์

๓.๒ เชิญชวนหน่วยงานต่างๆ เข้าร่วมสนับสนุนโครงการ ความร่วมมือระหว่างภาครัฐและเอกชนด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

บรรณานุกรม

ภาษาไทย

หนังสือ

คณะจัดทำกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม. กรุงเทพฯ : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ๒๕๕๙.

วารสารและหนังสือพิมพ์

“ระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ”, ราชกิจจานุเบกษา. เล่มที่ ๑๓๔ (ตอนพิเศษ ๒๕๙ ง), ๒๐ ตุลาคม ๒๕๖๐.

สัมภาษณ์

ปรัชญา เฉลิมวัฒน์,พล.ต. ผู้ชำนาญการสำนักงานปลัดกระทรวงกลาโหม. แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ของภาคเอกชนตามยุทธศาสตร์ไซเบอร์แห่งชาติ. ๒๓ พฤษภาคม ๒๕๖๑.

พีรสัณห์ บุณยคุปต์, อดีตนายกสมาคมส่งออกอุตสาหกรรมซอฟต์แวร์ไทย. แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ของภาคเอกชนตามยุทธศาสตร์ไซเบอร์แห่งชาติ. ๓๐ พฤษภาคม ๒๕๖๑.

หงษ์ลัดดา พงศ์สุวรรณ, ผู้เชี่ยวชาญด้านมาตรฐาน ISO29110 และ ISO27001. แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ของภาคเอกชนตามยุทธศาสตร์ไซเบอร์แห่งชาติ. ๘ มิถุนายน ๒๕๖๑.

ฐานข้อมูลอิเล็กทรอนิกส์

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. “มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์”. (ออนไลน์). เข้าถึงได้จาก : www.cpe.ku.ac.th/~srp/603352/Chapter2_ISO27001.docx, ๒๕๕๐.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์(องค์การมหาชน),สำนักงาน. “cybersecurity_survey_2016”. (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/downloads /files/Cyber security_Survey_2016.pdf, ๒๕๕๙.

เศรษฐพงค์ มะลิสุวรรณ,พ.อ. “แนวทางการพัฒนายุทธศาสตร์ ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Strategy)”. (ออนไลน์). เข้าถึงได้จาก : www.rtna.ac.th/download/cyber/nationalcybersecurity.pdf, ๒๕๕๘.

ไอซาก้าสมาคม (ISACA). “กรอบการดำเนินงานทางธุรกิจสำหรับการกำกับดูแลการบริหารจัดการไอทีระดับองค์กร (COBIT5)”. (ออนไลน์). เข้าถึงได้จาก : https://www.isaca.org /COBIT/Pages/COBIT-5-Thai.aspx, ๒๕๕๖.

ภาคผนวก

ผนวก ก
ร่างพ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

บันทึกหลักการและเหตุผลประกอบ
(ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ .....

หลักการ

ให้มีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เหตุผล

จากความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือ การติดต่อสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งใน ระดับบุคคลและระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงบนไซเบอร์จึงต้องอาศัย ความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ดังนั้น เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดย ปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่างๆ อันครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม มีการดำเนินการที่รวดเร็ว และมีความเป็นเอกภาพ สมควรกำหนดให้มีคณะกรรมการขึ้นเพื่อกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ให้เป็นไปอย่างมีประสิทธิภาพและเกิดผลสัมฤทธิ์

(ร่าง)

พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พ.ศ .....

โดยที่เป็นการสมควร .....

อาศัยอำนาจตามความใน

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติ พ.ศ ”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศ ในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“ความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

“หน่วยงานของรัฐ” หมายความว่า กระทรวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรมราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น องค์การมหาชน รัฐวิสาหกิจ และหน่วยงานที่ตั้งขึ้น โดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่ากรณีใด ๆ

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“เลขาธิการ” หมายความว่า เลขาธิการสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๔ ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้

หมวด ๑

การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๔ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องดำเนินการ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจาก ภายในและภายนอกประเทศ ซึ่งครอบคลุมถึง ความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ และอาจส่งผลกระทบต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม ให้มีความเป็นเอกภาพ โดยให้คำนึงถึงความสอดคล้องกับกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ ซึ่งเห็นชอบโดยคณะรัฐมนตรี

การดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยจึงต้องครอบคลุมในเรื่องดังต่อไปนี้

(๑) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(๒) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์

(๓) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

(๔) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์

(๔) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์

(๖) การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์

(๗) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

(๘) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์

หมวด ๒

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๖ ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กปช.” และให้ใช้ชื่อภาษาอังกฤษว่า “National Cybersecurity Committee” เรียกโดยย่อว่า “NCSC” ประกอบด้วย

(๑) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ

(๒) กรรมการโดยตำแหน่งจำนวนสี่คน ได้แก่ เลขาธิการสภาความมั่นคงแห่งชาติ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงกลาโหม ผู้บังคับการกองบังคับการปราบปรามการ กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ

(๓) กรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านนิติศาสตร์ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการ รักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการ เป็นกรรมการและเลขานุการโดยตำแหน่ง และให้แต่งตั้งเจ้าหน้าที่เป็น ผู้ช่วยเลขานุการได้ตามความจำเป็น

การคัดเลือกผู้ทรงคุณวุฒิเพื่อแต่งตั้งเป็นกรรมการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ และวิธีการที่คณะรัฐมนตรีกำหนดโดยประกาศในราชกิจจานุเบกษา

มาตรา ๗ ให้ กปช. มีอำนาจหน้าที่ ดังต่อไปนี้

(๑) กำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่ส่งผลกระทบ หรืออาจก่อให้เกิดผลกระทบ ความสูญเสีย หรือความเสียหายอย่างมีนัยสำคัญหรือ อย่างร้ายแรง เพื่อให้เป็นศูนย์กลางการดำเนินการเมื่อมีเหตุการณ์หรือสถานการณ์ความมั่นคงปลอดภัยได้ อย่างทันท่วงที มีความเป็นเอกภาพ เว้นแต่ภัยคุกคามทางไซเบอร์นั้นเป็นภัยที่กระทบต่อความมั่นคงทางทหาร ซึ่งเป็นอำนาจของสภากลาโหมหรือสภาความมั่นคงแห่งชาติ

(๒) กำหนดขั้นตอนการดำเนินการเพื่อให้มีการประสานความร่วมมือและอำนวยความ สะดวกในการดำเนินการกับคณะกรรมการที่ตั้งขั้นตามกฎหมายฉบับอื่น หน่วยงานของรัฐหรือหน่วยงาน ภาคเอกชน เพื่อให้การยับยั้งปัญหา ภัยคุกคามไซเบอร์ ได้รับการแก่ไขอย่างมีประสิทธิภาพและรวดเร็ว

(๓) กำหนดมาตรการและแนวทางในการยกระดับทักษะความเชี่ยวชาญระดับสูงของ เจ้าพนักงานผู้ปฏิบัติหน้าที่ซึ่งได้รับการแต่งตั้งตามกฎหมายฉบับนี้

(๔) จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่สอดคล้องกับ นโยบาย ยุทธศาสตร์ และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบาย และแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

(๔) จัดทำรายงานสรุปผลการดำเนินงานที่มีผลกระทบอย่างมีนัยสำคัญ รายงานให้สภาความมั่นคงแห่งชาติ และคณะรัฐมนตรีทราบตามสำคัญ

(๖) เสนอแนะและให้ความเห็นต่อคณะกรรมการติจิทัลเพื่อเศรษฐกิจและสังคม หรือ คณะรัฐมนตรีในการพิจารณาอนุมัติแผนงาน โครงการ หรือการปฏิบัติงานของหน่วยงานของรัฐ และการ พิจารณาแนวทางการแก้ไขปัญหาหรือข้อขัดข้องต่างๆ รวมถึงการจัดให้มีหรือปรับปรุงกฎหมายที่มีความเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ให้การดำเนินการปกป้อง รับมือ ป้องกันและลด ความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอก ประเทศมีความมั่นคงและยั่งยืน

(๗) แต่งตั้งคณะอนุกรรมการ หรือคณะทำงาน เพื่อพิจารณาหรือทำการใด ๆ ตามที่ คณะกรรมการมอบหมาย

(๘) สั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใด ที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ

(๙) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้

(๑๐) ดำเนินการอื่นใดในเรื่องที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมหรือคณะรัฐมนตรีมอบหมาย

มาตรา ๘ กรรมการผู้ทรงคุณวุฒิต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามดังต่อไปนี้

(๑) มีสัญชาติไทย

(๒) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๓) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๔) ไม่เคยต้องคำพิพากษาถึงที่สุดให้จำคุก ไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) ไม่เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐ หรือรัฐวิสาหกิจ หรือจากหน่วยงานของเอกชน เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

มาตรา ๙ กรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งคราวละสามปี ในกรณีที่กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระ คณะรัฐมนตรีอาจแต่งตั้งผู้อื่นเป็น กรรมการแทนได้ และให้ผู้ที่ได้รับแต่งตั้งให้ดำรงตำแหน่งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน เว้นแต่วาระการดำแหน่งของกรรมการผู้ทรงคุณวุฒิเหลือไม่ถึงเก้าสิบวันจะไม่แต่งตั้งก็ได้

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง หากยังมิได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่ากรรมการ ผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระ อาจได้รับการแต่งตั้งอีกได้แต่จะดำรง ตำแหน่งติดต่อกันเกินสองวาระไม่ได้

มาตรา ๑๐ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๘ กรรมการผู้ทรงคุณวุฒิซึ่ง คณะรัฐมนตรีแต่งตั้งพ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออกเพราะมีความประพฤติเสื่อมเสีย บกพร่อง หรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา ๗

มาตรา ๑๑ การประชุม การลงมติ และการปฏิบัติงานของกปช. คณะอนุกรรมการ และ คณะทำงานให้เป็นไปตามระเบียบที่คณะกรรมการกำหนด

ในการปฏิบัติหน้าที่ กปช. อาจมอบหมายให้กรรมการคนหนึ่งหรือหลายคนปฏิบัติงานแทน กปช. ได้ แต่ กปช. จะปฏิเสธความรับผิดเพราะเหตุที่ได้มอบหมายให้กรรมการไปทำแทนแล้วไม่ได้

มาตรา ๑๒ กปช. มีอำนาจแต่งตั้งที่ปรึกษา เพื่อพิจารณาศึกษา เสนอแนะ หรือดำเนินการ อย่างหนึ่งอย่างใดตามที่ กปช. มอบหมายได้

การแต่งตั้งที่ปรึกษาตามวรรคหนึ่ง ให้แต่งตั้งได้ไม่เกินห้าคน

มาตรา ๑๓ให้กปช.ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

คณะอนุกรรมการ คณะทำงาน และที่ปรึกษาที่ กปช. แต่งตั้งให้ได้รับเบี้ยประชุม และ ประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่ กปช. กำหนด

หมวด ๓
สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๑๔ ให้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขึ้นเป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคล ไม่เป็นส่วนราชการและรัฐวิสาหกิจ

มาตรา ๑๕ ให้สำนักงานมีสำนักงานใหญ่ในกรุงเทพมหานครหรือจังหวัดใกล้เคียง

มาตรา ๑๖ กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครอง แรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการ คุ้มครองแรงงาน กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

มาตรา ๑๗ ให้สำนักงานมีอำนาจและหน้าที่ ดังต่อไปนี้

(๑) ตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่ส่งผลกระทบ หรืออาจ ก่อให้เกิดผลกระทบ ความสูญเสีย หรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรง โดยวางมาตรการ เกี่ยวกับการดำเนินการที่คำนึงถึงชั้นความลับและการเข้าถึงข้อมูลที่มีชั้นความลับ

(๒) ประสานความร่วมมือทางปฏิบัติในการดำเนินการกับหน่วยงานของรัฐ หรือหน่วยงานภาคเอกชน เพื่อให้การยับยั้งปัญหาภัยคุกคามไซเบอร์ ได้รับการแก้ไขอย่างมีประสิทธิภาพและรวดเร็ว

(๓) ประสานงานกับหน่วยงานของรัฐและเอกชน เพื่อรวบรวมข้อมูลเกี่ยวกับภัยคุกคาม การป้องกัน การรับมือ ความเสี่ยงจากสถานการณ์ด้านภัยคุกคามทางไซเบอร์ และข้อมูลอื่นใดอันเกี่ยวกับ การรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อวิเคราะห์เสนอต่อ กปช.

(๔) บริหารแผนงานรวม ประสานการบริหารและการปฏิบัติการตามแผนปฏิบัติการหรือตาม คำสั่งการของ กปช.

(๕) ติดตามและเร่งรัดการปฏิบัติงานของหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความ มั่นคงปลอดภัยไซเบอร์ และรายงานต่อ กปช.

(๖) เป็นศูนย์กลางเครือข่ายข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศทั้งภายใน และภายนอกประเทศ

(๗) ติดตาม เฝ้าระวัง รวมทั้งสร้างความตระหนักเกี่ยวกับภัยคุกคามทางระบบสารสนเทศ รวมทั้งจัดตั้งและบริหารจัดการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT)

(๘) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำ ข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๙) ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับการรักษา ความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะเกี่ยวกับมาตรฐานความมั่นคง ปลอดภัย หรือกรณีอื่นใดเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๐) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามระเบียบนี้ รวมทั้งปัญหา และอุปสรรคต่อ กปช.

(๑๑) รับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของ กปช.

(๑๒) จัดทำรายงานสรุปผลการดำเนินงานรายงานประจำปีให้กปช.ทราบ เว้นแต่เป็นกรณี ฉุกเฉินให้รายงานให้กปช.ทราบโดยเร็ว

(๑๓) ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่ กปช. หรือคณะรัฐมนตรีมอบหมาย

เมื่อคณะรัฐมนตรีอนุมัติแผนปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติตาม (๑) ให้สำนักงานร่วมกับหน่วยงานของรัฐที่เกี่ยวข้องปฏิบัติการให้เป็นไปตามแผนดังกล่าว

มาตรา ๑๘ เพื่อให้บรรลุวัตถุประสงค์ตามมาตรา ๑๗ให้สำนักงานมีอำนาจหน้าที่ดังต่อไปนี้

(๑) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพย์สิทธิต่าง ๆ

(๒) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อ ประโยชน์ในการดำเนินกิจการของสำนักงาน

(๓) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานอื่นทั้งภาครัฐและภาคเอกชนทั้งใน ประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามวัตถุประสงค์ของสำนักงาน

(๔) ดำเนินการอื่นใดที่จำเป็นหรือต่อเนื่องเพื่อให้บรรลุวัตถุประสงค์ของสำนักงาน

มาตรา ๑๙ ทุนและทรัพย์สินในการดำเนินงานของสำนักงาน ประกอบด้วย

(๑) เงินและทรัพย์สินที่ได้รับโอนตามมาตรา ๓๔

(๒) เงินอุดหนุนทั่วไปที่รัฐบาลจัดสรรให้ตามความเหมาะสม

(๓) เงินอุดหนุนจากภาคเอกชน องค์กรปกครองส่วนท้องถิ่น หรือองค์กรอื่น รวมทั้งจาก ต่างประเทศหรือองค์การระหว่างประเทศ และเงินหรือทรัพย์สินที่มีผู้อุทิศให้

(๔) ดอกผลของเงินหรือรายได้จากทรัพย์สินของสำนักงานการรับเงินหรือทรัพย์สินตาม (๓) จะต้องไม่กระทำในลักษณะที่ทำให้สำนักงานชาดความเป็น อิสระหรือความเป็นกลาง

มาตรา ๒๐ บรรดารายได้ที่สำนักงานได้รับให้ตกเป็นของสำนักงานเพื่อเป็นค่าใช้จ่ายสำหรับ การดำเนินงานของสำนักงาน และไม่ต้องนำส่งคลังเป็นรายได้แผ่นดิน

มาตรา ๒๑ ให้สำนักงานมีเลขาธิการคนหนึ่ง รับผิดชอบการปฏิบัติงานของสำนักงาน ขึ้นตรงต่อประธานกรรมการ และเป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน

ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการเป็นผู้แทนของสำนักงาน เพื่อการนี้ เลขาธิการอาจมอบอำนาจให้บุคคลใดปฏิบัติงานเฉพาะอย่างแทนก็ได้ ทั้งนี้ตามระเบียบที่ คณะกรรมการกำหนดโดยประกาศในราชกิจจานุเบกษา

คณะกรรมการเป็นผู้มีอำนาจสรรหา แต่งตั้ง และถอดถอนเลขาธิการ

มาตรา ๒๒ ผู้ที่จะได้รับการแต่งตั้งเป็นเลขาธิการต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีสัญชาติไทย

(๒) มีอายุไม่เกินหกสิบห้าปีบริบูรณ์

(๓) สามารถทำงานให้แก่สำนักงานได้เต็มเวลา

มาตรา ๒๓ ผู้มีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้ ต้องห้ามมิให้เป็นเลขาธิการ

(๑) เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษ สำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เป็นข้าราชการ พนักงานหรือลูกจ้างของส่วนราชการหรือรัฐวิสาหกิจหรือหน่วยงานอื่น ของรัฐหรือของราชการส่วนท้องถิ่น

(๕) เป็นหรือเคยเป็นข้าราชการการเมือง ผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่น หรือผู้บริหารท้องถิ่น เว้นแต่จะได้พ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี

(๖) เป็นหรือเคยเป็นกรรมการหรือผู้ดำรงตำแหน่งอื่นในพรรคการเมืองหรือเจ้าหน้าที่ของ พรรคการเมือง เว้นแต่จะได้พ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี

(๗) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐหรือรัฐวิสาหกิจหรือ จากหน่วยงานของเอกชน เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

มาตรา ๒๔ ให้คณะกรรมการเป็นผู้กำหนดอัตราเงินเดือนและประโยชน์ตอบแทนอื่นของเลขาธิการ

มาตรา ๒๕ เลขาธิการอยู่ในตำแหน่งคราวละสี่ปี

เลขาธิการซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้ แต่ต้องไม่เกินสองวาระติดต่อกัน

มาตรา ๒๖ นอกจากการพ้นจากตำแหน่งตามวาระ เลขาธิการพ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) ขาดคุณสมบัติตามมาตรา ๒๒ หรือมีลักษณะต้องห้ามตามมาตรา ๒๓

(๔) คณะกรรมการมีมติให้ออกเพราะบกพร่องต่อหน้าที่หรือทุจริตต่อหน้าที่ มีความประพฤติ เสื่อมเสีย หรือหย่อนความสามารถ

หมวด ๔

การปฏิบัติการและการรับมือภัยคุกคามทางไซเบอร์

มาตรา ๒๗ เมื่อ กปช. จัดทำแผนแม่บทความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้สำนักงาน จัดทำแนวทาง มาตรการ แผนปฏิบัติการ หรือโครงการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ สอดคล้องและเป็นไปตามนโยบายและแผนดังกล่าว

เมื่อคณะกรรมการให้ความเห็นชอบแนวทาง มาตรการ แผนปฏิบัติการ หรือโครงการ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และมีผลใช้บังคับแล้ว หากมีกรณีจำเป็นให้ กปช. มีอำนาจ แก้ไขเปลี่ยนแปลงหรือเพิ่มเติมให้เหมาะสมแก่สถานการณ์ได้

มาตรา ๒๘ ให้หน่วยงานของรัฐดำเนินการภายใต้กฎหมายที่กำหนดอำนาจหน้าที่ของ หน่วยงานของรัฐนั้นให้สอดคล้องกับแนวทาง มาตรการ แผนปฏิบัติการ หรือโครงการตามมาตรา ๒๗ โดยถือ เป็นการปฏิบัติตามที่คณะรัฐมนตรีกำหนด

ให้หัวหน้าหน่วยงานของรัฐมีหน้าที่รับผิดชอบอำนวยการให้การปฏิบัติตามวรรคหนึ่งให้ เป็นไปด้วยความเรียบร้อยและสำเร็จตามเป้าหมายและระยะเวลาที่กำหนด

ในกรณีที่กปช.ติดตามความก้าวหน้าและประเมินผลการดำเนินการตลอดจนการปฏิบัติการใด ๆ ให้หน่วยงานของรัฐมีหน้าที่ช่วยเหลือและอำนวยความสะดวกในการปฏิบัติหน้าที่

มาตรา๒๙ ในกรณีที่เห็นสมควรกปช.อาจกำหนดให้หน่วยงานของรัฐแจ้งรายชื่อผู้รับผิดชอบตามแนวทาง มาตรการ แผนปฏิบัติการ หรือโครงการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ไซเบอร์ หรือผู้รับผิดชอบในพื้นที่ต่อ กปช. เพื่อพิจารณาแต่งตั้งเป็นผู้รับผิดชอบการปฏิบัติงานในการ ดำเนินการป้องกันและแก้ไขปัญหาภัยคุกคามทางไซเบอร์

ผู้ซึ่งได้รับแต่งตั้งตามวรรคหนึ่งต้องปฏิบัติงานโดยยึดถือแผนปฏิบัติการ มติ หรือการสั่งการ ของ กปช. หรือคำสั่งของประธานกรรมการ กปช. หรือผู้ซึ่งประธานกรรมการโดยความเห็นชอบ ของ กปช. มอบหมายเป็นสำคัญ

การไม่ปฏิบัติตามวรรคสองถือเป็นการชัดคำสั่งผู้บังคับบัญชา

มาตรา ๓๐ ให้รัฐมนตรีเป็นผู้บัญชาการมีอำนาจควบคุมและกำกับการรักษาความมั่นคง ปลอดภัยไซเบอร์ทั่วราชอาณาจักรให้เป็นไปตามแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และพระราชบัญญัตินี้ในการนี้ให้มีอำนาจบังคับบัญชาและสั่งการผู้รับผิดชอบการปฏิบัติงานตามมาตรา ๒๘ ได้ทั่วราชอาณาจักร

มาตรา ๓๑ ในกรณีที่ กปช. มีมติว่ากระทรวง หน่วยงานของรัฐ หรือผู้มีหน้าที่ปฏิบัติตาม พระราชบัญญัตินี้ไม่ปฏิบัติตามพระราชบัญญัตินี้หรือปฏิบัติการโดยขัดหรือแย้งกับแนวทางตามที่กำหนดใน พระราชบัญญัตินี้ให้ กปช. แจ้งให้กระทรวง หน่วยงานของรัฐ หรือผู้มีหน้าที่ปฏิบัติดังกล่าวดำเนินการแก้ไข ยกเลิก หรือยุติการดำเนินการดังกล่าวภายในเวลาที่กำหนด ในกรณีที่กระทรวง หน่วยงานของรัฐ หรือผู้มี หน้าที่ปฏิบัติดังกล่าวไม่ดำเนินการตามมติ กปช. ภายในเวลาที่กำหนดโดยไม่มีเหตุอันสมควร ให้ถือว่า ปลัดกระทรวง หัวหน้าหน่วยงานของรัฐหรือผู้มีหน้าที่ปฏิบัติดังกล่าว แล้วแต่กรณี กระทำผิดวินัย และให้ กปช.ส่งเรื่องให้ผู้มีอำนาจดำเนินการทางวินัยของผู้นั้นดำเนินการตามอำนาจหน้าที่ต่อไป

ในกรณีที่ผลของการไม่ดำเนินการตามมติ กปช. ตามวรรคหนึ่งก่อให้เกิดความเสียหายแก่ทางราชการอย่างร้ายแรง ให้ถือว่าเป็นการปฏิบัติหน้าที่โดยไม่ขอบหรือเป็นความผิดวินัยอย่างร้ายแรง แล้วแต่กรณี ในกรณีที่ผู้ไม่ปฏิบัติการตามมติ กปช. ตามวรรคหนึ่งเป็นรัฐมนตรีเจ้าสังกัด ให้ กปช. รายงาน นายกรัฐมนตรีเพื่อพิจารณาสั่งการตามที่เห็นสมควรต่อไป

มาตรา ๓๒ ในกรณีเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้นในระบบสารสนเทศ ซึ่งอยู่ในความดูแลของหน่วยงานของรัฐหน่วยงานใด ให้หน่วยงานของรัฐหรือผู้รับผิดชอบการปฏิบัติงานตาม มาตรา ๒๘ รายงานเหตุดังกล่าวไปยังเลขาธิการโดยเร็ว

เมื่อเลขาธิการได้รับทราบเหตุตามวรรคหนึ่ง ให้รีบดำเนินการป้องกันหรือแก้ไขเหตุภัยคุกคาม นั้นตามความเหมาะสมทันที และรายงานให้ กปช. ทราบเพื่อพิจารณาสั่งการตามที่เห็นสมควรต่อไป

มาตรา ๓๓ เมื่อมีเหตุฉุกเฉินหรือภยันตรายอันเนื่องมาจากภัยคุกคามทางไซเบอร์ที่อาจ ก่อให้เกิดผลกระทบต่อความมั่นคงของประเทศ ให้ กปช. มีอำนาจสั่งการให้หน่วยงานของรัฐทุกแห่งดำเนินการอย่างหนึ่งอย่างใดเพื่อป้องกัน แก้ไขปัญหา หรือบรรเทาความเสียหายที่เกิดหรืออาจจะเกิดขึ้นได้ ตามที่เห็นสมควร และอาจให้หน่วยงานของรัฐ หรือบุคคลใด รวมทั้งบุคคลซึ่งได้รับอันตรายหรืออาจได้รับ อันตรายหรือความเสียหายดังกล่าว กระทำหรือร่วมกันกระทำการใด ๆ อันจะมีผลเป็นการควบคุม ระงับ หรือ บรรเทาผลร้ายจากอันตรายและความเสียหายที่เกิดขึ้นนั้นได้อย่างทันท่วงที

ในกรณีที่ทราบว่าบุคคลใดเกี่ยวข้องกับการก่อให้เกิดภัยคุกคามทางไซเบอร์ ให้ กปช. มี อำนาจสั่งบุคคลนั้นไม่ให้กระทำการใดอันจะมีผลเป็นการเพิ่มความรุนแรงอันเกิดจากภัยคุกคามทางไซเบอร์นั้นได้

มาตรา ๓๔ ในกรณีที่มีความจำเป็นเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยทาง ไซเบอร์ที่อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ กปช. อาจสั่ง การให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง และให้รายงานผลการ ปฏิบัติการต่อ กปช. ตามที่ กปช. ประกาศกำหนด

หมวด ๕
พนักงานเจ้าหน้าที่

มาตรา ๓๔ เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ให้พนักงานเจ้าหน้าที่ที่ ได้รับมอบหมายเป็นหนังสือจากเลขาธิการ มีอำนาจดังต่อไปนี้(๑) มีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำ ชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการ ปฏิบัติการตามพระราชบัญญัตินี้

(๒) มีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่ง การปฏิบัติหน้าที่ของ กปช.

(๓) เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ใน การปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

การดำเนินการตาม (๓) ให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่คณะรัฐมนตรีกำหนด

มาตรา ๓๖ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลที่ได้มาตามมาตรา ๓๕ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำ ความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจ หน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหก หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๓๗ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มี ความรู้ความเชี่ยวชาญเกี่ยวกับระบบคอมพิวเตอร์หรือการรักษาความมั่นคงปลอดภัยสารสนเทศและมี คุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๓๘ เพื่อประโยชน์ในการประสานงานหรือการปฏิบัติการ ให้เจ้าหน้าที่ของ กระทรวงกลาโหมที่ได้รับมอบหมายในการปฏิบัติภารกิจเพื่อตอบสนองและรับมือกับภัยคุกคามไซเบอร์ที่ กระทบต่อความมั่นคงทางทหาร เป็นพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

มาตรา ๓๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ให้พนักงานเจ้าหน้าที่เป็นเจ้าพนักงาน ตามประมวลกฎหมายอาญา

ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อ บุคคลซึ่งเกี่ยวข้อง และบัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจา บุเบกษา

หมวด ๖

บทเฉพาะกาล

มาตรา ๔๐ ให้โอนบรรดากิจการ อำนาจหน้าที่ ทุนและทรัพย์สิน ของสำนักความมั่นคง ปลอดภัย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ที่มีอยู่ในวันที่พระราชบัญญัตินี้ใช้ บังคับไปเป็นของสำนักงาน ตามพระราชบัญญัตินี้

มาตรา ๔๑ ให้เจ้าหน้าที่ และลูกจ้าง ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์แห่งชาติ ตามมาตรา ๔๒ ซึ่งปฏิบัติหน้าที่อยู่ในวันที่พระราชบัญญัตินี้ใช้บังคับถ้าสมัครใจจะโอนไปเป็น พนักงานหรือลูกจ้างของสำนักงาน ให้แสดงเจตนาเป็นหนังสือต่อผู้บังคับบัญชาภายในสามสิบวันนับแต่วันที่ พระราชบัญญัตินี้ใช้บังคับ สำหรับผู้ที่ไม่ได้แจ้งความจำนงภายในระยะเวลาดังกล่าว ให้กลับไปปฏิบัติหน้าที่ใน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์แห่งชาติ

การบรรจุและแต่งตั้งเจ้าหน้าที่ และลูกจ้างตามวรรคหนึ่งให้ดำรงตำแหน่งใดในสำนักงานให้ เป็นไปตามอัตรากำลัง คุณสมบัติและอัตราเงินเดือนหรือค่าจ้างที่คณะกรรมการกำหนด แต่จะกำหนดให้ได้รับ เงินเดือนหรือค่าจ้างต่ำกว่าเงินเดือนหรือค่าจ้างที่ได้รับอยู่เดิมไม่ได้

มาตรา ๔๒ ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์แห่งชาติ ทำหน้าที่เป็นสำนักงาน คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติไปพลางก่อนจนกว่าจะมีการจัดตั้งสำนักงานตาม พระราชบัญญัตินี้

มาตรา ๔๓ เมื่อพระราชบัญญัตินี้ใช้บังคับ ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ ปลัดกระทรวงดิจิทัลเพื่อ เศรษฐกิจและลังคม เป็นรองประธานกรรมการ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้บังคับการกองบังคับการ ปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ เป็นกรรมการ และให้ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์แห่งชาติ เป็นกรรมการและเลขานุการ

ให้คณะกรรมการตามวรรคหนึ่งปฏิบัติหน้าที่คณะกรรมการตามพระราชบัญญัตินี้เป็นการ ชั่วคราวจนกว่าจะมีคณะกรรมการตามพระราชบัญญัตินี้ ซึ่งต้องไม่เกินเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

ผู้รับสนองพระบรมราชโองการ นายกรัฐมนตรี

ผนวก ข

โครงร่างคำถามในการสัมภาษณ์

คำถามเกี่ยวกับแนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ภาคเอกชนตามแนวยุทธศาสตร์ไซเบอร์แห่งชาติ

1. ท่านคิดว่าระบบมาตรฐานความปลอดภัยไซเบอร์ตามรูปแบบสากล มาตรฐานไหนที่เหมาะสมกับภาคเอกชนที่สุด เพราะเหตุใด

ตอบ……
……
……
……

2. ท่านคิดว่าควรมีการกำหนดมาตรการรักษาความปลอดภัยไซเบอร์ตามขนาดของธุรกิจหรือไม่ ถ้าควรจะมีวิธีการอย่างไร

ตอบ……
……
……
……

3. ท่านคิดว่ากระบวนการจัดทำระบบรักษาความปลอดภัยไซเบอร์ตามมาตรฐานสากล ควรจะทำตามมาตรฐานไหนที่เหมาะสมกับภาคเอกชนในประเทศไทย

ตอบ……
……
……
……

4. ท่านคิดว่าภาครัฐควรตั้งหน่วยงานที่กำหนดมาตรฐานความปลอดภัยไซเบอร์เพื่อให้ภาคเอกชนปฏิบัติตามหรือไม่ ถ้าควรจะมีวิธีการกำหนดอย่างไร

ตอบ……
……
……
……

5. ท่านคิดว่าควรมีกฎหมายหรือข้อบังคับที่จะให้ภาคเอกชนที่จะติดต่อส่งข้อมูลให้กับภาครัฐต้องปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ตามแนวนโยบายภาครัฐหรือไม่ และต้องปฏิบัติอย่างไร

ตอบ……
……
……
……

ประวัติย่อผู้วิจัย

ชื่อ นายณัทฐรัชต์ อัศวปัญญาวงศ์

วัน เดือน ปีเกิด ๑๒ กันยายน พ.ศ. ๒๕๐๘

การศึกษา ระดับปริญญาตรี คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์
ปีพ.ศ. ๒๕๓๑

ประวัติการทำงานโดยย่อ

ผู้จัดการโรงงาน บริษัท ไทยยูรีเทรนพลาสติก จำกัด พ.ศ. ๒๕๓๑
ผู้จัดการทั่วไป บริษัท ต้ากงเคมีคอลอินดัสเทรียล (ไทยแลนด์)
พ.ศ. ๒๕๓๖
กรรมการผู้จัดการ บริษัท ไทยมาสเตอร์คัลเลอร์ จำกัด ตั้งแต่ พ.ศ.๒๕๔๔

ตำแหน่งปัจจุบัน

ประธานกรรมการ กลุ่มบริษัทไทยมาสเตอร์กรุ๊ป
กรรมการผู้จัดการ
บริษัท ไทยมาสเตอร์คัลเลอร์ จำกัด
บริษัท ต้ากงเคมีคอลอินดัสเทรียล (ไทยแลนด์) จำกัด
บริษัท ทีเอ็มจี อินเตอร์เคม จำกัด
บริษัท วินสตาร์เทค จำกัด
ผู้เชี่ยวชาญประจำสมาชิกสภาปฏิรูปแห่งชาติ (สปช.)

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ของภาคเอกชนตามยุทธศาสตร์ไซเบอร์แห่งชาติ

ผู้วิจัย นายณัทฐรัชต์ อัศวปัญญาวงศ์ **หลักสูตร วปอ. รุ่นที่** ๖๐

ตำแหน่ง ประธานกรรมการ กลุ่มบริษัทไทยมาสเตอร์

ความเป็นมาและความสำคัญของปัญหา

เทคโนโลยีสารสนเทศและการสื่อสาร ได้พัฒนาขึ้นในช่วงสองทศวรรษที่ผ่านมาอย่างก้าวกระโดดและปัจจุบันได้เข้ากับวิถีชีวิตของมนุษย์ในทุกมิติ ซึ่งประเทศไทยได้ก้าวเข้าสู่ยุคดิจิทัลที่มีเศรษฐกิจสังคมและชีวิตประจำวันของประชาชนที่ขึ้นอยู่กับเทคโนโลยีดิจิทัลอย่างมาก ทำให้ประเทศต้องพึ่งพิงเทคโนโลยีดิจิทัล ทั้งเศรษฐกิจและการบริหารราชการแผ่นดินของรัฐบาล รวมทั้งการให้บริการสาธารณะที่จำเป็น ซึ่งปัจจุบันขึ้นอยู่กับความมั่นคงของโลกไซเบอร์และโครงสร้างพื้นฐานดิจิทัล ภัยคุกคามต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศมาจากฮาร์ดแวร์และซอฟแวร์ส่วนใหญ่ที่พัฒนาขึ้นเพื่ออำนวยความสะดวกไม่ได้มีการออกแบบที่มีความปลอดภัยมาตั้งแต่ต้นอย่างเหมาะสม จึงทำให้ผู้โจมตีไม่ว่าจะเป็นรัฐที่เป็นฝ่ายตรงข้ามองค์กรอาชญากรรมหรือผู้ก่อการร้าย และแม้แต่บุคคลทั่วไปก็สามารถใช้ช่องว่างระหว่างความสะดวกและปลอดภัยในการโจมตีได้ ดังนั้นการลดช่องว่างและความเสี่ยงทางไซเบอร์จึงควรได้รับการให้ความสำคัญเป็นอันดับแรก การขยายตัวของอินเทอร์เน็ตที่เชื่อมโยงกับคอมพิวเตอร์และโทรศัพท์เคลื่อนที่มาสู่การใช้งานในระบบอัจฉริยะนั้นเป็นการขยายขอบเขตของการคุกคามทางไซเบอร์ ซึ่งระบบและเทคโนโลยีที่สำคัญกับชีวิตประจำวันของเรา เช่น ระบบการผลิตไฟฟ้า, ระบบควบคุมการจราจรทางอากาศ, ดาวเทียม, เทคโนโลยีทางการแพทย์, โรงงานอุตสาหกรรม และระบบการขนส่ง ต่างมีการเชื่อมต่อกับอินเทอร์เน็ตที่อาจเสี่ยงต่อการถูกแทรกแซงและทำลายได้ ภัยคุกคามด้านไซเบอร์ที่เกิดจากช่องโหว่ที่มีและช่องว่างในขีดความสามารถและการป้องกันของประเทศ ทำให้รัฐบาลต้องเล็งเห็นถึงความสำคัญ เพื่อให้สามารถตอบโต้ได้อย่างเท่าทันต่อภัยคุกคามทางไซเบอร์ โดยจำเป็นที่จะต้องมีแนวทางในการป้องกันอย่างรอบด้านเพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ ควรมีการแก้ปัญหาในภาคธุรกิจและภาคอุตสาหกรรมของเอกชนควบคู่ไปกับภาครัฐโดยอาศัยการประเมินดังต่อไปนี้

๑. ขนาดและเครือข่ายหรือภัยคุกคามทางไซเบอร์ และช่องโหว่ของประเทศ ซึ่งหมายความว่าการใช้แนวทางในปัจจุบัน อาจจะไม่เพียงพอที่จะทำให้ประเทศปลอดภัย

๒. แนวทางที่ขึ้นกับตลาด (Market Based Approach) ทำให้เกิดการลงทุนในภาคเอกชนเพื่อสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ รัฐบาลต้องเป็นผู้นำและแทรกแซงโดยตรง โดยการสร้างกลไกด้านการลงทุนและการนำทรัพยากรที่มีอยู่ไปใช้เพื่อแก้ปัญหาภัยคุกคามทางไซเบอร์

๓. การที่รัฐบาลดำเนินการเพียงฝ่ายเดียวนั้น ไม่สามารถทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ได้ในทุกด้าน ดังนั้นแนวทางสร้างความร่วมมือกับทุกภาคส่วนจึงเป็นสิ่งจำเป็น

๔. ประเทศไทยจำเป็นต้องมีหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ตื่นตัวและสนับสนุนทักษะและขีดความสามารถต่างๆ ที่สามารถก้าวให้ทันและเผชิญกับภัยคุกคามที่กำลังเปลี่ยนแปลงได้

การขยายตัวของการโจมตีทางไซเบอร์ทั่วโลกเกิดขึ้นอย่างรวดเร็ว, บ่อยครั้ง และรุนแรง ซึ่งจะส่งผลต่อการลุกลามของอาชญากรรมไซเบอร์ และจะมีผลกระทบต่อเศรษฐกิจของประเทศทุกประเทศที่กำลังเข้าสู่ยุคอุตสาหกรรม ๔.๐ ซึ่งมีแนวโน้มที่ชัดเจนว่าอาชญากรรมไซเบอร์กำลังเพิ่มมากขึ้นเป็นจำนวนมาก การสร้างความมั่นคงปลอดภัยไซเบอร์ จึงไม่ใช่เรื่องแค่เป็นวิสัยทัศน์อีกต่อไปเพราะหากไม่ลงมือสร้างขีดความสามารถด้านบุคลากรและเครื่องมือทางเทคโนโลยี ประเทศไทยของเราก็จะประสบกับภัยคุกคามทางไซเบอร์ในอนาคตอย่างแน่นอน เนื่องจากภัยคุกคามทางไซเบอร์เริ่มปรากฏชัดที่กำลังจะมีผลกระทบต่อสถาบันหลักของประเทศไทย ดังนั้นประเทศไทยจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการดำเนินการบัญญัติกฎหมายที่เกี่ยวข้อง ในการเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์ และจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างเร่งด่วนเพื่อให้ทันต่อการเติบโตของภัยคุกคามด้านไซเบอร์ในอนาคต ดังนั้นยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรมีการจัดการแบบองค์รวม และมีความสามารถในการรับมือกับการโจมตีในแง่มุมต่างๆ โดยคำนึงถึงวิธีการทั้งในเรื่องการป้องกัน, การตอบสนอง และลดผลกระทบแผนดำเนินการที่มีประสิทธิผลในการสร้างกลยุทธ์ควรมีขั้นตอนที่จะเพิ่มความตระหนัก และยกระดับของความเข้าใจในหมู่ประชาชนทั่วไปด้วยการให้ความรู้แก่เจ้าของธุรกิจ, นักเรียน และหน่วยงานของรัฐ ในเรื่องภัยคุกคามที่มีอยู่รวมทั้งวิธีปกป้องเครือข่ายของตนจากการโจมตี การสร้างความพร้อมด้วยการสร้างศูนย์ประสานการรักษาความมั่นคง

ระบบคอมพิวเตอร์(CERT) ที่คอยประสานงานเพื่อจัดการภัยคุกคาม รวมถึงแบ่งปันความรู้และทักษะป้องกันการโจมตี ผ่านการสร้างและการดูแลรักษาเครือข่ายคอมพิวเตอร์ ให้มีความมั่นคงปลอดภัยต่อการโจมตี โดยให้อำนาจแก่ผู้ออกกฎหมาย ผู้มีอำนาจควบคุม ผู้จัดทำนโยบาย โดยมีระเบียบข้อบังคับที่ดี และการใช้เครื่องมือที่สามารถต่อสู้กับการโจมตีทางไซเบอร์ บรรเทาความเสียหาย เพื่อเรียกคืนความเชื่อมั่นของประชาชนและผู้มีส่วนเกี่ยวข้อง ผ่านการสื่อสารที่มีประสิทธิภาพ และการสร้างความร่วมมือกับภาคเอกชน เพื่อเป็นแนวร่วมในการป้องกันภัยคุกคามทางไซเบอร์ของรัฐบาล

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาและหาแนวทางในการจัดการอย่างเหมาะสมกับภัยคุกคามทางไซ-เบอร์ต่อภาคเอกชน โดยเริ่มจากการศึกษาระบบรักษาความปลอดภัยทางไซเบอร์ที่เหมาะสมกับภาคเอกชน รวมทั้งค่าใช้จ่ายของภาคเอกชนที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์

๒. เพื่อเสนอแนะแนวทางที่ภาคเอกชนสามารถสร้างระบบรักษาความปลอดภัยทางไซเบอร์ได้เหมาะสมกับองค์กร ทั้งด้านขนาดและงบประมาณ รวมทั้งสอดคล้องกับยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อป้องกันภัยภัยคุกคามที่เกิดขึ้นจากการใช้เครือข่ายอินเทอร์เน็ต รวมทั้งสร้างรายการตรวจสอบ (Checklist) ที่ช่วยให้สามารถประเมินความพร้อมในการรักษาความมั่นคงปลอดภัยจากภัยคุกคามที่เกิดขึ้น

ขอบเขตของการวิจัย

การวิจัยเรื่อง “แนวทางการสร้างมาตรการรักษาความปลอดภัยไซเบอร์ของภาคเอกชนตามยุทธศาสตร์ไซเบอร์แห่งชาติ” มีขอบเขตของการศึกษา ดังนี้

๑. ศึกษาเนื้อหาเกี่ยวกับ แนวคิด รูปแบบ ทฤษฎีที่เกี่ยวข้องกับการกำหนดนโยบายความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ของภาคเอกชน

๒. ศึกษาข้อมูลยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๓. ผู้วิจัยจะดำเนินการสัมภาษณ์กลุ่มผู้เชี่ยวชาญที่มีความสามารถทางด้านวิชาการด้านการบริหาร และผู้ที่มีประสบการณ์ในการจัดทำระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับภาคเอกชน และยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีการดำเนินการดังนี้

๑. รวบรวมข้อมูลเรื่องแนวคิด ทฤษฎี รวมถึงวรรณกรรมที่เกี่ยวข้องกับแนวทางการป้องกันภัยคุกคามและการสร้างความมั่นคงปลอดภัยทางไซเบอร์และเปรียบเทียบกับต่างประเทศบางประเทศ รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิเพื่อให้ได้แนวทางในการกำหนดนโยบายความมั่นคงปลอดภัยทางไซเบอร์ต่อภาคเอกชนที่เหมาะสม ทั้งค่าใช้จ่าย ระยะเวลา ให้มีความชัดเจนแปลงไปสู่แผนการปฏิบัติได้จริง

๒. การจัดระเบียบและวิเคราะห์ข้อมูล รวบรวมข้อมูลทั้งหมดที่ได้มาจัดระเบียบและตรวจสอบตามขั้นตอนการวิจัยเชิงคุณภาพ นำข้อมูลมาวิเคราะห์ เพื่อแยกแยะให้เห็นถึงส่วนประกอบและความสัมพันธ์ระหว่างส่วนประกอบต่างๆ เหล่านั้น โดยมุ่งเน้นการวิเคราะห์ความชัดเจน, ความเฉพาะเจาะจง และความสามารถในการแปลงไปสู่แผนการปฏิบัติตามความเหมาะสมของเนื้อหากับกรอบเวลา

ผลการวิจัย

ประเภทการโจมตีและภัยคุกคามด้านไซเบอร์ที่มีต่อภาคเอกชนและหน่วยงานของรัฐในปัจจุบันมีด้วยกันหลายรูปแบบ จึงมีความจำเป็นที่ภาครัฐและเอกชนต้องร่วมมือกันในการกำหนดมาตรการรักษาความปลอดภัยทางไซเบอร์ เพื่อเป็นแนวปฏิบัติในการจัดการภัยคุกคามทางไซเบอร์ โดยมีกรอบแนวคิดดังนี้

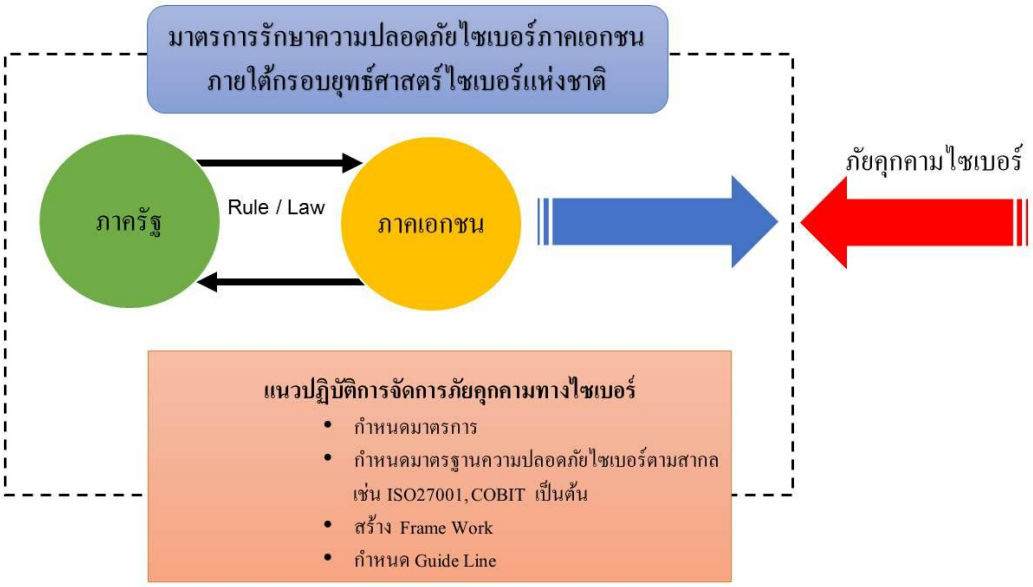
๑. กำหนดมาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์

๒. กำหนดมาตรฐานความปลอดภัยไซเบอร์ตามสากล

๓. สร้างกรอบการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ (Framework)

๔. กำหนดแนวทางการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ (Guideline)

แผนภาพ กรอบความคิดของการวิจัย



รายละเอียดของกรอบแนวคิดที่เกี่ยวข้องกับมาตรการรักษาความปลอดภัยทางไซเบอร์และมาตราฐานความปลอดภัยไซเบอร์ตามมาตรฐานสากล ในส่วนของการสร้างกรอบการปฏิบัติตามมาตรฐานและแนวทางปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ สามารถอธิบายได้ดังนี้

๑. กำหนดมาตรการที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์

มาตราการที่เกี่ยวข้องกับการกำกับดูแลและรักษาความปลอดภัยไอทีระดับองค์กร ซึ่งมีเนื้อหาที่เป็นกรอบการดำเนินงานที่ใช้สำหรับการกำกับดูแลและรักษาความปลอดภัยไอทีควรมีรายละเอียดดังนี้

๑.๑ กำหนดนโยบายการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

๑.๒ การรักษาความมั่นคงปลอดภัยด้านทรัพยากรบุคคลที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

๑.๓ การรักษาความมั่นคงปลอดภัยทางกายภาพที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

๑.๔ การบริหารจัดการเรื่องการสื่อสารและการปฏิบัติงานที่มีผลกระทบต่อความมั่นคงปลอดภัยสำหรับสารสนเทศ

๑.๕ การควบคุมการเข้าถึงข้อมูลสารสนเทศ

๑.๖ การปฏิบัติตามกฎระเบียบข้อบังคับ และนโยบายที่เกี่ยวข้องกับระบบสารสนเทศ

๑.๗ การพัฒนาและการบำรุงรักษาระบบสารสนเทศ

๑.๘ การเตรียมความพร้อมฉุกเฉินเพื่อรับเหตุการณ์ที่ไม่คาดฝัน

๑.๙ การบริหารการดำเนินธุรกิจอย่างต่อเนื่อง

๒. กำหนดมาตรฐานความปลอดภัยไซเบอร์ตามสากล

จากผลการวิจัยนี้ได้ทำการวิจัยเชิงคุณภาพ (Qualitative Research) โดยรวบรวมข้อมูลเรื่องแนวคิด ทฤษฎี รวมถึงวรรณกรรมที่เกี่ยวข้องกับแนวทางการป้องกันภัยคุกคามและการสร้างความมั่นคงปลอดภัยทางไซเบอร์และเปรียบเทียบกับต่างประเทศบางประเทศ รวมทั้งการสัมภาษณ์ผู้ทรงคุณวุฒิทางด้านนี้ เพื่อให้ได้แนวทางการสร้างมาตรฐานความปลอดภัยไซเบอร์ตามสากล งานวิจัยนี้ได้นำเสนอตัวอย่างมาตรฐานสากลที่นิยมใช้กันแพร่หลายในภาคเอกชน คือ มาตรฐาน ISO / IEC 27001 และ COBIT ซึ่งผู้วิจัยได้ทำการสัมภาษณ์ผู้ทรงคุณวุฒิเกี่ยวกับการกำหนดมาตรฐานที่เหมาะสมโดยสอดคล้องกับมาตรฐานสากล ผู้ทรงคุณวุฒิทั้งหมดให้ความเห็นตรงกันว่าประเทศไทยยังไม่มีผู้เชี่ยวชาญหรือหน่วยงานด้านมาตรฐานเป็นที่ยอมรับในระดับสากลมากำหนดมาตรฐานขึ้นมาเพื่อใช้ในประเทศ ทำให้จำเป็นต้องทำตามมาตรฐานสากลที่มีอยู่และดัดแปลงบางอย่างให้เหมาะสมกับขนาดขององค์กร

๓. สร้างกรอบการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ (Framework)

กรอบการปฏิบัติงตามมาตรฐานความปลอดภัยไซเบอร์มีขั้นตอนการดำเนินการบริหารความมั่นคงปลอดภัยสารสนเทศ จะขับเคลื่อนเป็นวงจร PDCA ดังนี้ **การวางแผน (Plan) การลงมือทำ (Do) การตรวจสอบ (Check) และการปรับปรุงแก้ไข (Act)**

๓.๑ การวางแผน (Plan) คือ การกำหนดนโยบายความมั่นคงปลอดภัยและระบบบริหารความมั่นคงปลอดภัย

๓.๒ การลงมือทำ (Do) คือ ลงมือดำเนินการตามระบบบริหารความมั่นคงปลอดภัย

๓.๓ การตรวจสอบ (Check) คือ การตรวจสอบและทบทวนผลการดำเนินงาน

๓.๔ การปรับปรุงแก้ไข (Act) คือ ดูแลและรักษาระบบบริหารความมั่นคงปลอดภัย

๔. กำหนดแนวทางการปฏิบัติตามมาตรฐานความปลอดภัยไซเบอร์ (Guideline)

แนวทางการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยสารสนเทศมีการดำเนินการตามกรอบที่กำหนดไว้ดังนี้

๔.๑ **การวางแผน (Plan)** มีขั้นตอนของการวางแผน ดังนี้

๔.๑.๑ การกำหนดขอบเขต (Scope) ของระบบ โดยคำนึงถึงลักษณะทางธุรกิจ องค์กร สถานที่ ทรัพย์สิน และ เทคโนโลยี

๔.๑.๒ การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security management system policy)

๔.๑.๓ การกำหนดแนวทางในการประเมินความเสี่ยงสำหรับองค์กรและความมั่นคงปลอดภัย สารสนเทศทางธุรกิจ รวมถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

๔.๑.๔ การระบุความเสี่ยง

๔.๑.๕ การวิเคราะห์และประเมินความเสี่ยง โดยการประเมินถึงผลกระทบทางธุรกิจ ซึ่งเกิดจากความล้มเหลวในความมั่นคงปลอดภัย โดยคำนึงถึง ความสูญเสียในการรักษาความลับความสมบูรณ์หรือความพร้อมของทรัพย์สิน

๔.๑.๖ การกำหนดและประเมินแนวทางในการจัดการความเสี่ยงโดยแนวทางที่ใช้ในการจัดการความเสี่ยง

๔.๑.๗. การจัดเลือกรายการควบคุม และวัตถุประสงค์การควบคุมสำหรับการจัดการความเสี่ยง โดยในขั้นตอนนี้จะเป็น การจัดเลือกหัวข้อการควบคุม และวัตถุประสงค์การควบคุม รวมถึงการนำไปปฏิบัติเพื่อให้สอดคล้องกับแนวทางที่กำหนดจากการประเมินและกระบวนการจัดการความเสี่ยงโดยการจัดเลือกจะพิจารณาถึงเกณฑ์ การยอมรับความเสี่ยง รวมถึงข้อกำหนดทางกฎหมายและข้อสัญญาต่างๆ

๔.๑.๘ การอนุมัติความเสี่ยงที่เหลืออยู่โดยผู้บริหารระดับสูงขององค์กร

๔.๑.๙ การจัดเตรียมเอกสารแสดงการประยุกต์ใช้งานที่อธิบายถึงรายการของหัวข้อควบคุม (Control) และวัตถุประสงค์การควบคุม (Control objectives) ที่ได้เลือกไว้ และเหตุผลของการควบคุม (Control objectives) ที่ได้เลือกไว้ และเหตุผลของการเลือก รวมถึงหัวข้อควบคุมและวัตถุประสงค์ควบคุมที่มีการดำเนินการอยู่ใน ปัจจุบัน หรือที่เรียกว่า Base line control ในกรณีที่หัวข้อการควบคุมใดที่ระบุว่าจะไม่มีการดำเนินการจะต้องมี การระบุถึงเหตุผลของการยกเว้นไว้ด้วย

๔.๒ **การลงมือทำ (Do)** มีขั้นตอนของการลงมือทำ ดังนี้

๔.๒.๑ การจัดทำแผนการจัดการความเสี่ยง โดยระบุรายละเอียดของการดำเนินงาน ทรัพยากรที่ต้องการ ความรับผิดชอบและลำดับความสำคัญในการดำเนินงานสำหรับ การจัดการกับความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศ

๔.๒.๒. การดำเนินการตามแผนการจัดการความเสี่ยง เพื่อให้บรรลุตามวัตถุประสงค์การควบคุมที่ได้กำหนดไว้ รวมถึงการพิจารณาจัดสรรเงินทุนและกำหนดหน้าที่ความรับผิดชอบในการดำเนินการด้วย

๔.๒.๓ การดำเนินการตามการควบคุมที่ได้กำหนดไว้ เพื่อให้ได้ตามวัตถุประสงค์การควบคุม

๔.๒.๔ การกำหนดแนวทางในการวัดความมีประสิทธิผลของการควบคุม หรือกลุ่มการควบคุมที่ได้กำหนด

๔.๒.๕ การจัดฝึกอบรมและการสร้างการรับรู้ขึ้นภายในองค์กรตามมาตรฐานที่กำหนด

๔.๒.๖ การบริหารงานตามมาตรฐานที่กำหนด

๔.๒.๗. การจัดการทรัพยากรสำหรับตามมาตรฐานที่กำหนด

๔.๒.๘ การดำเนินงานตามวิธีการปฏิบัติงาน และการควบคุมอื่นๆ เพื่อให้สามารถตรวจ สอบเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัย และการตอบสนองต่อเหตุการณ์นั้นๆ

๔.๓ **การตรวจสอบ (Check)** องค์กรจะต้องมีการดำเนินการต่างๆ ดังนี้

๔.๓.๑ การดำเนินการเฝ้าติดตาม และทบทวนวิธีการปฏิบัติงานและการควบคุมต่างๆ

๔.๓.๒ การดำเนินการทบทวนความมีประสิทธิผลของมาตราฐานอย่างสม่ำเสมอ โดยคำนึงถึงผลของการตรวจประเมินความมั่นคงปลอดภัย (Audit) เหตุการณ์ที่เกิดขึ้น ผลของการวัดความมีประสิทธิผล ข้อเสนอแนะ และข้อมูลแจ้งกลับจากหน่วยงานต่างๆ ที่เกี่ยวข้อง

๔.๓.๓ การวัดความมีประสิทธิผลของการควบคุม เพื่อทวนสอบถึงความสอดคล้องตามข้อกำหนดความมั่นคงปลอดภัย

๔.๓.๔ ทบทวนการประเมินความเสี่ยงตามแผนที่ได้กำหนดไว้ รวมถึงทบทวนความเสี่ยงที่เหลืออยู่และระดับของความเสี่ยงที่สามารถยอมรับได้ โดยคำนึงถึงการเปลี่ยนแปลงในองค์กร เทคโนโลยี วัตถุประสงค์และกระบวนการทางธุรกิจ ภัยคุกคามที่ระบุไว้ ความมีประสิทธิผลของการควบคุม และเหตุการณ์ภายนอก เช่น การเปลี่ยนแปลงใน ข้อกฎหมาย ข้อบังคับตามสัญญาที่เปลี่ยนแปลง และการเปลี่ยนแปลงทางสังคม

๔.๓.๕. การดำเนินการตรวจประเมินมาตรฐานภายใน

๔.๓.๖ การดำเนินการทบทวนโดยฝ่ายบริหาร เพื่อดูแลความเพียงพอของขอบเขต และการดำเนินการปรับปรุง กระบวนการมาตรฐานที่ใช้ในองค์กร

๔.๓.๗ การปรับปรุงแผนความมั่นคงปลอดภัย โดยคำนึงถึงสิ่งที่พบจากการเฝ้าติดตาม และการทบทวน

๔.๓.๘ การบันทึกผลการดำเนินการ และเหตุการณ์ที่อาจส่งผลต่อความมีประสิทธิผล หรือผลการดำเนินงานของมาตรฐาน

๔.๔ **การปรับปรุงแก้ไข (Act)** มีขั้นตอนการของการปรับปรุงและแก้ไขระบบดังนี้

๔.๔.๑ การดำเนินการปรับปรุงมาตรฐานตามที่ได้กำหนดไว้

๔.๔.๒ การปฏิบัติการแก้ไขและการป้องกันอย่างเหมาะสม รวมถึงการนำบทเรียนจากประสบการณ์ความมั่นคง ปลอดภัยขององค์กรอื่นๆ และขององค์กรเองมาปรับใช้อย่างเหมาะสม

๔.๔.๓ การสื่อสารการดำเนินการ และการปรับปรุงไปยังหน่วยงานต่างๆ ที่เกี่ยวข้องทั้งหมด การดูแลให้มั่นใจว่าการปรับปรุงเป็นไปตามวัตถุประสงค์ที่ได้กำหนดไว้

ข้อเสนอแนะ

สรุปข้อเสนอแนะของการวิจัยจำแนกตามประเภท ได้แก่ ข้อเสนอแนะเชิงนโยบายและแผน ข้อเสนอแนะเชิงกฎ ระเบียบ และกฎหมายที่เกี่ยวข้อง

๑. ข้อเสนอแนะเชิงนโยบายและแผน

๑.๑ กำหนดสิทธิประโยชน์ต่างๆ ให้กับภาคเอกชนที่ดำเนินการตามระบบมาตรฐานรักษาความปลอดภัยไซเบอร์สากลหรือที่หน่วยงานที่กำกับดูแลระบบมาตรฐานได้กำหนดขึ้น เช่น สิทธิประโยชน์ทางภาษี เป็นต้น

๑.๒ กำหนดแผนงานสนับสนุนภาคเอกชน ให้สามารถเข้าอบรมและวางแผนกำลังคนที่จะเข้ามาสู่ระบบมาตรฐานรักษาความปลอดภัยไซเบอร์สากลได้ตามแผนนโยบายยุทธศาสตร์ไซเบอร์แห่งชาติ เช่น สนับสนุนหลักสูตรการอบรมระบบมาตรฐานต่างๆ

๒. ข้อเสนอแนะเชิงกฎ ระเบียบ และกฎหมาย

๒.๑ พิจารณากฎระเบียบภาครัฐในการเชื่อมต่อข้อมูล หรือส่งข้อมูลระหว่างภาครัฐและภาคเอกชน โดยบังคับให้ภาคเอกชนที่ต้องการส่งข้อมูลหรือเชื่อมต่อข้อมูลกับภาครัฐต้องได้รับมาตรฐานรักษาความปลอดภัยไซเบอร์สากลหรือจากหน่วยงานกำกับดูแลระบบมาตรฐาน

๒.๒ พิจารณากฎหมาย “การรักษาความมั่งคงปลอดภัยทางไซเบอร์แห่งชาติ” ให้ภาคเอกชนมีหน้าที่รายงานข้อมูลเกี่ยวกับภัยคุกคาม ที่อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ เสนอต่อคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ (กปช) ทันทีและ กปช. มีอำนาจสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง ที่มีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

๓. ข้อเสนอแนะเชิงปฏิบัติการ

๓.๑ ร่วมจัดทำโครงการความร่วมมือระหว่างภาครัฐและเอกชนในด้านการรักษาความมั่งคงปลอดภัยทางไซเบอร์แห่งชาติ ซึ่งจะทำให้เกิดการขับเคลื่อนที่สำคัญ เช่น การระดมสมอง ทรัพยากร และสรรพกำลังจากทุกภาคส่วนมาช่วยกันพัฒนา มาตรการการรักษาความปลอดภัยทางไซเบอร์

๓.๒ เชิญชวนหน่วยงานต่างๆ เข้าร่วมสนับสนุนโครงการ ความร่วมมือระหว่างภาครัฐและเอกชนด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ