บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่อง “การพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม” มีวัตถุประสงค์ (1) เพื่อศึกษาถึงอิทธิพลของปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และอิทธิพลของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (2) เพื่อพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (3) เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (4) เพื่อทำการประเมินตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล และ (5) เพื่อทำการพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยผู้วิจัยได้ทำการตรวจสอบแนวคิด ทฤษฎี และงานวิจัยที่ได้ศึกษามาก่อนหน้านี้ ซึ่งเกี่ยวข้องกับประเด็นปัญหาที่ทำให้ต้องมีการศึกษาวิจัย และเป็นพื้นฐานสำคัญที่ใช้ในการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ซึ่งผู้วิจัยได้กำหนดกรอบในการทบทวนวรรณกรรมโดยได้แบ่งเป็นหัวข้อต่าง ๆ ได้ดังต่อไปนี้

2.1 โซ่อุปทานดิจิทัล
- 2.1.1 ความหมายของโซ่อุปทานดิจิทัล
- 2.1.2 คุณลักษณะของโซ่อุปทานดิจิทัล
- 2.1.3 เทคโนโลยีที่เกี่ยวข้องกับโซ่อุปทานดิจิทัล

2.2 การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล
- 2.2.1 ภัยคุกคามทางไซเบอร์
- 2.2.2 ความมั่นคงปลอดภัยไซเบอร์
- 2.2.3 การจัดการภัยคุกคามทางไซเบอร์
- 2.2.4 แนวโน้มภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อโซ่อุปทานดิจิทัล
- 2.2.5 องค์ประกอบของการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล

2.3 ความร่วมมือกันของโซ่อุปทานดิจิทัล

2.3.1 ความหมายของความร่วมมือกันของโซ่อุปทานดิจิทัล

2.3.2 องค์ประกอบของความร่วมมือกันของโซ่อุปทานดิจิทัล

2.4 การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

2.4.1 ความเสี่ยงของโซ่อุปทาน

2.4.2 การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

2.4.3 องค์ประกอบของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

2.5 การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

2.5.1 ความเป็นมาและความหมายของการคืนสภาพได้

2.5.2 แนวคิดการคืนสภาพได้ที่มีต่อระบบโซ่อุปทาน

2.5.3 การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

2.6 การจัดการความต่อเนื่องของธุรกิจดิจิทัล

2.6.1 แนวคิดของการจัดการความต่อเนื่องทางธุรกิจ

2.6.2 มาตรฐานด้านการจัดการความต่อเนื่องทางธุรกิจ

2.7 ตัวแบบวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล

2.7.1 ตัวแบบวุฒิภาวะความสามารถ

2.7.2 ตัวแบบวุฒิภาวะความสามารถในการจัดการโซ่อุปทาน

2.7.3 ตัวแบบวุฒิภาวะความสามารถความมั่นคงปลอดภัยทางไซเบอร์

2.7.4 องค์ประกอบในการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม

2.8 วิสาหกิจขนาดกลางและขนาดย่อม

2.8.1 จำนวนวิสาหกิจขนาดกลางและขนาดย่อม

2.8.2 ความสำคัญวิสาหกิจขนาดกลางและขนาดย่อม ต่อระบบเศรษฐกิจไทย

2.8.3 แนวทางการสนับสนุนวิสาหกิจขนาดกลางและขนาดย่อมภายในประเทศ

2.8.4 ความมั่นคงปลอดภัยทางไซเบอร์กับวิสาหกิจขนาดและขนาดย่อม

2.8.5 การศึกษาที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ของวิสาหกิจขนาดกลางและขนาดย่อม

2.1 โซ่อุปทานดิจิทัล (Digital Supply Chain)

เทคโนโลยีดิจิทัลได้เข้ามาเปลี่ยนแปลงวิธีการในการติดต่อสื่อสาร แนวทางในดำเนินชีวิตของผู้คนไปอย่างมาก ความแปลกใหม่ทางด้านเทคโนโลยีรวมไปถึงอุปกรณ์ส่วนบุคคล เช่น อุปกรณ์มือถือ คอมพิวเตอร์ส่วนบุคคล รถยนต์ที่ขับด้วยตนเอง โดรน เทคโนโลยีขั้นสูงที่เชื่อมต่อกับโทรทัศน์ สมาร์ตโฟน และ สมาร์ตวอช ได้เข้ามาเปลี่ยนวิธีการในการเข้าถึงและแลกเปลี่ยนข้อมูลระหว่างกัน การเกิดขึ้นในเทคโนโลยีใหม่ ๆ เหล่านี้ ได้เข้ามาส่งผลกระทบต่อทุก ๆ อุตสาหกรรม การบริการด้านโลจิสติกส์และโซ่อุทานก็ไม่มีข้อยกเว้นเช่นกัน อย่างไรก็ตาม การดำเนินการหลายอย่างที่เกิดขึ้น สำหรับการผลิตและการส่งมอบสินค้าหรือบริการไปยังลูกค้าได้ดำเนินการอย่างเป็นอิสระในโครงสร้างองค์กรปัจจุบัน

โซ่อุทานสามารถนิยามได้ว่าเป็น กิจกรรมต่าง ๆ ที่มีความเชื่อมโยงถึงกัน ซึ่งเกี่ยวข้องกับการประสานงาน การวางแผนและการควบคุมสินค้าและบริการ ระหว่างซัพพลายเออร์และลูกค้า โครงสร้างองค์กรจำนวนมากเหล่านี้ไม่สามารถที่จะพึ่งพาตนเองได้อีกต่อไป อันเป็นผลเนื่องมาจากการพัฒนาทางด้านเทคโนโลยีดิจิทัลที่ได้เข้ามามีบทบาทต่อชีวิตมนุษย์เกือบทุกด้านทั่วโลก และแน่นอนว่าได้ส่งผลกระทบต่อกระบวนการโซ่อุปทานอย่างมาก ตามที่การคาดการณ์ของตลาด (Penthin S. et al., 2015) ที่ระบุไว้ว่า 76% ของประชากรโลกสามารถเข้าถึงอินเทอร์เน็ต โดยครึ่งหนึ่งของจำนวนประชาการที่เข้าถึงอินเทอร์เน็ตจะมีการใช้โซเชียลมีเดีย ยิ่งไปกว่านั้นผู้ใช้อินเทอร์เน็ต 9 ใน 10 รายทำการสั่งซื้อสินค้าออนไลน์ 43% ของ บริษัทต่าง ๆ ใช้ประโยชน์จากการวิเคราะห์ข้อมูลขนาดใหญ่ที่มีความซับซ้อน รวมไปถึงการจัดเก็บข้อมูลบนคลาวด์ก็ได้ถูกคาดการณ์ไว้ว่าข้อมูลจะถูกเก็บประมาณ 37% ของข้อมูลที่สร้างขึ้นทั้งหมดในปี 2020

ในเวลาเดียวกัน ก็มีการคาดการณ์ว่าจะมีจำนวนผู้ใช้งานกว่า 26 พันล้านผู้ใช้ ที่จะสามารถเชื่อมต่อกับ “สรรพสิ่ง (things)” บนอินเทอร์เน็ตได้ การเปลี่ยนผ่านทางดิจิทัลแบบฉับพลันนี้จะมีผลต่ออุตสาหกรรมต่าง ๆ ก่อให้เกิดผลกระทบทางด้านมูลค่าและเครือข่ายแทบทั้งสิ้น ในอนาคตผู้คนอาจจะสามารถขับขี่ยานพาหนะด้วยอุปกรณ์มือถือง่าย ๆ หรืออาจเป็นไปได้ที่จะคำนวณหาพื้นที่ของตู้สินค้าด้วยการเพียงแค่มองผ่านระบบอิเล็กทรอนิกส์ อีกไม่นานอาจจะมีคอมพิวเตอร์ที่สวมใส่ได้จะมีวางจำหน่าย ด้วยความเป็นไปได้ที่มีอยู่มากมายนี้เอง จึงเป็นผลทำให้องค์กรต่าง ๆ ได้ตระหนักถึงการพัฒนาที่มีศักยภาพเหล่านี้มากขึ้น และทำให้เห็นว่าโซ่อุปทานดิจิทัลจะสามารถเพิ่มมูลค่าให้กับบริษัทได้อย่างไร ยิ่งเมื่อได้ทำการพิจารณาถึงเป้าหมายหลักขององค์กรที่ต้องการรักษาและเสริมสร้างความสามารถหลัก เพื่อการเข้าสู่ตลาดที่มีการแข่งขัน ยิ่งต้องพัฒนาให้องค์กรมีความทันสมัย และมีปฏิสัมพันธ์กับตัวแทนจำหน่ายผ่านกระบวนการโซ่อุปทานดิจิทัล เพื่อให้เกิดประโยชน์ต่อการผลิตและการส่งมอบสินค้าและบริการของบริษัทต่อไป

แม้ว่าโซ่อุปทานดิจิทัลยังอยู่ในขั้นเริ่มต้น และจะยังไม่สามารถที่จะสร้างมูลค่าให้ได้อย่างเต็มศักยภาพเท่าไหร่นัก แต่ก็ได้ทำให้อุตสาหกรรมทางด้านโลจิสติกส์และซัพพลายเชนมีการเปลี่ยนแปลงไปอย่างรวดเร็วด้วยนวัตกรรมความก้าวหน้าทางเทคโนโลยีที่ได้ถูกพัฒนาด้วยรูปแบบของข้อมูลทางดิจิทัลที่ได้ถูกพัฒนาขึ้น ศูนย์ข้อมูล (Data Center) ข้อมูลที่มีลักษณะเป็นบิต (Bits) รวมไปถึงแบนด์วิดธ์ (Bandwidth) ได้ถูกนำเข้ามาแทนที่ข้อมูลทางกายภาพ (Physical) มีการเปลี่ยนแปลงในช่องทางการจัดการจากศูนย์กระจายสินค้าทั่วไปไปยังผู้ค้าปลีก ผู้ให้บริการบรอดแบนด์เพื่อการดำเนินการทางออนไลน์ และโดยตรงไปยังลูกค้า สำหรับนวัตกรรมที่เกี่ยวกับโซ่อุปทานดิจิทัลมีมากมายหลาย อาทิเช่น เทคโนโลยีโลกเสมือนผสานโลกแห่งความจริง (Augmented Reality: AR) ข้อมูลขนาดใหญ่ (Big Data: BD) การประมวลผลแบบคลาวด์(Cloud Computing: CC) หุ่นยนต์ (Robotics: R) เทคโนโลยีเซ็นเซอร์ (Sensor Technology: ST) เทคโนโลยีการติดต่อสื่อสารหลากหลายช่องทาง (Omni Channel: OC) อินเทอร์เน็ตประสานสรรพสิ่ง(Internet of Thingss: IoT) ยานพาหนะที่ขับเคลื่อนด้วยตนเอง (Self-Driving Vehicles: SDV) อากาศยานไร้คนขับ (Unmanned Aerial Vehicle: UAV) นาโนเทคโนโลยี (Nanotechnology: N) และ การพิมพ์ 3 มิติ (3D Printing: 3DP)

2.1.1 ความหมายของโซ่อุปทานดิจิทัล

จากการทบทวนวรรณกรรม ทำให้ได้ความหมายและคำจำกัดความของโซ่อุปทานดิจิทัลที่มีนักวิจัยหรือนักวิชาการได้ให้ความหมายไว้อย่างมากมาย โดยมีรายละอียดดังต่อไปนี้

Capgemini Consulting (Raab, M. and Griffin-Cryan, B., 2011) อธิบายว่าโซ่อุปทานแบบดั้งเดิมอาศัยส่วนผสมของกระบวนการทางอิเล็กทรอนิกส์และกระดาษเป็นหลักในการจัดทำเอกสาร โครงสร้างองค์กรมักแสดงให้เห็นโดยจัดทำเพื่อให้เห็นเพียงแค่ลักษณะทางภูมิศาสตร์ โดยไม่เต็มใจที่จะแบ่งปันข้อมูลอย่างเปิดเผยซึ่งนำไปสู่ประสิทธิภาพที่ดีที่สุด ในทางกลับกันโซ่อุปทานดิจิทัลมีความสามารถในการทำอย่างกว้างขวางมีข้อมูลการทำงานร่วมกันที่เหนือกว่าและการสื่อสารข้ามแพลตฟอร์มดิจิทัล ที่จะส่งผลให้เพิ่มความน่าเชื่อถือความคล่องตัวและประสิทธิผล

Bhargava et al. [42] อธิบายว่าโซ่อุปทานดิจิทัลประกอบด้วยระบบต่าง ๆ เช่น ซอฟต์แวร์ ฮาร์ดแวร์ เครือข่ายการสื่อสาร เป็นต้น ที่รองรับปฏิสัมพันธ์ระหว่างองค์กรที่กระจายอยู่ทั่วโลกและประสานกิจกรรมของคู่ค้าในซ่อุปทาน กิจกรรมเหล่านี้รวมถึงการซื้อ การสร้าง การจัดเก็บ การย้าย และการขายผลิตภัณฑ์

Accenture Consulting (Raj, S. and Sharma, A., 2014) เสนอว่าระบบดิจิทัลมีศักยภาพในการเปลี่ยนโซ่อุปทานโดยให้บริการที่มีคุณค่ามากขึ้น สามารถเข้าถึงได้และราคาไม่แพง ดังนั้นด้วยมุมมองที่แตกต่างกัน เทคโนโลยีดิจิทัลจึงเป็นสิ่งจำเป็นสำหรับการสร้างโอกาสใหม่ในโซ่อุปทาน องค์กรควรทบทวนโซ่อุปทานของตนใหม่ในฐานะเครือข่ายอุปทานดิจิทัลที่ไม่เพียง แต่รวมการไหลของสินค้าและบริการเข้าด้วยกัน แต่ยังรวมถึงความสามารถข้อมูลและการเงินในแง่นามธรรม ผู้คนและข้อมูล รวมถึงวัสดุผลิตภัณฑ์และวัสดุสิ้นเปลืองจะต้องทำงานร่วมกันทั่วทั้งองค์กรขนาดใหญ่

การวิเคราะห์รายงานที่จัดทำโดย A.T. Kearney และ WHUOtto Beisheim School of Management (Schmidt, B. et al., 2015) ได้กำหนดว่าโซ่อุปทานดิจิทัลว่าเป็นเทคโนโลยีที่เหมาะสมที่สุดที่ใช้ในการสนับสนุนและประสานกระบวนการของโซ่อุปทาน – รวมถึงระบบคลังสินค้าและการขนส่ง การระบุความถี่วิทยุ (RFID) เทคนิคการจัดเก็บขั้นสูง และนวัตกรรมการวางแผนและระบบการตั้งเวลาได้อย่างรวดเร็ว การแก้ไขปัญหาที่เกิดขึ้นต่อโซ่อุปทาน เช่นของเสียในโซ่อุปทานในโลกที่ความต้องการมีความผันผวนและมีความเสี่ยงสูง

The Digital Supply Chain Initiative (2015) อธิบายถึงโซ่อุปทานดิจิทัลว่าเป็นแพลตฟอร์มที่มีลูกค้าเป็นศูนย์กลาง และการใช้ข้อมูลตามเวลาจริงที่เกิดขึ้นเพื่อเพิ่มประสิทธิภาพสูงสุดจากความหลากหลายของแหล่งที่มา พวกเขาแนะนำว่าโซ่อุปทานดิจิทัลช่วยกระตุ้นอุปสงค์ได้ การจับคู่และการจัดการเพื่อให้ได้ประสิทธิภาพสูงสุดและลดความเสี่ยง

Rouse (2016) โซ่อุปทานดิจิทัลถูกสร้างขึ้นจากความสามารถในการใช้งานเว็ปเบส (Web-based) ระบบโซ่อุปทานเป็นจำนวนมากจะใช้กระบวนการผสมผสานกันระหว่างกระบวนการที่ทำงานบนด้วยกระดาษกับความสามารถทางด้านไอที โซ่อุปทานดิจิทัลมีความชาญฉลาดในการเชื่อมต่อข้อมูลและสามารถรวบรวมและจัดเก็บข้อมูล ได้อย่างมีประสิทธิภาพ

Cecere L. (2016) นิยามว่าโซ่อุปทานดิจิทัลเป็นกระบวนการที่ใช้เทคโนโลยีใหม่เพื่อกำหนดกระบวนการรับรู้และตอบสนอง และเพื่อเตรียมการแบบสองทิศทางจากตลาดไปสู่ตลาด (จากช่องทางการจัดจำหน่ายไปยังเครือข่ายของซัพพลายเออร์) กระบวนการต่าง ๆ เคลื่อนไปตามจังหวะของตลาด

จากคำนิยามที่ได้กล่าวมาทั้งหมดนี้นั้น แสดงให้เห็นว่าโซ่อุปทานดิจิทัลมีคำจำกัดความที่แตกต่างกันอยู่หลายประการ อย่างไรก็ตามสิ่งที่เหมือนกันจากคำนิยามที่ได้มานั้น สามารถสรุปได้ว่า โซ่อุปทานดิจิทัลเป็นเทคโนโลยีที่ชาญฉลาดและมีความเหมาะสมที่สุด เป็นระบบที่มีความสามารถในการจัดการกับข้อมูลขนาดใหญ่ เป็นระบบที่ต้องอาศัยความร่วมมือและการสื่อสารที่ยอดเยี่ยม เพื่อรองรับและประสานการทำงานร่วมกันระหว่างองค์กรกับข้อมูลที่เป็นดิจิทัลมากขึ้น

2.1.2 คุณลักษณะของโซ่อุปทานดิจิทัล

องค์กรที่ประสบความสำเร็จส่วนใหญ่ของโลกจะมีความสามารถในการจัดการเกี่ยวกับโซ่อุปทานอยู่แล้ว แต่ก็ยังมีผู้ออกมาโต้แย้งว่าการแข่งขันระหว่างองค์กรนั้นเป็นการแข่งขันกันในโซ่อุปทานขององค์กรเหล่านั้นเอง ตัวอย่างเช่นเครือข่ายซูเปอร์มาร์เก็ตที่ใหญ่ที่สุด 2 แห่งในออสเตรเลีย คือ Woolworths และ Coles ที่มีการแข่งขันกันแบบเผชิญหน้ากับเครือข่ายระดับโลกในด้านความคล่องตัวสูงด้วยความพร้อมทางด้านการบริการและต้นทุน อีกตัวอย่างหนึ่งคือโซ่อุปทานของ iPad ที่มีการผลิตเซมิคอนดักเตอร์ใน 3 ประเทศ และการประกอบจะทำในประเทศที่แตกต่างกัน จอภาพจะถูกนำเข้ามาจากประเทศอื่น ๆ ในขณะที่การออกแบบและการสร้างแบรนด์จะทำในสหรัฐอเมริกาที่สำนักงานใหญ่ของบริษัท Apple Inc. (Xu, J.,2014). โซ่อุปทานกำลังพัฒนาและกำลังจะกลายเป็นสิ่งใหม่ วันที่โซ่อุปทานแบบดั้งเดิมที่มีการย้ายสินค้าจากที่หนึ่งไปอีกที่หนึ่งได้สิ้นสุดลงแล้ว ทุกวันนี้โซ่อุปทานต้องการกิจกรรมที่ซับซ้อนขนาดใหญ่ซึ่งทั้งหมดต้องมีการประสานงานและการติดตาม ดังนั้นภายใต้ระบบดิจิทัลจะทำให้วิวัฒนาการของโซ่อุปทานในยุคต่อไปนำเสนอทั้งความยืดหยุ่นและประสิทธิภาพ เนื่องจากโซลูชันทางดิจิทัลกำลังรบกวนโซ่อุปทานแบบดั้งเดิมจึงมีคุณสมบัติบางอย่างที่แตกต่างกันที่เกี่ยวข้องกับโซ่อุปทานดิจิทัล คุณสมบัติหลัก ๆ 11 ข้อที่สามารถสรุปได้เกี่ยวกับโซ่อุปทานดิจิทัลประกอบด้วย

1. ความเร็ว (Speed) : ความเร็วในการจัดส่งสินค้าถือเป็นหัวใจสำคัญสำหรับซัพพลายเออร์และผู้ที่เกี่ยวข้องใน โซ่อุปทานดิจิทัล บริษัทต่าง ๆ ไม่เพียงต้องการที่จะได้รับสินค้าทันทีที่ต้องการ แต่ผู้ที่ทำงานใน โซ่อุปทานดิจิทัลต้องการที่จะสามารถเคลื่อนไหวได้มากขึ้นในระยะเวลาอันสั้น ความสามารถในการตอบสนองต่อความต้องการอย่างรวดเร็วนี้จะเป็นหนึ่งในเสาหลักที่สำคัญที่สุดของโซ่อุปทานดิจิทัลเนื่องจากองค์กรต่าง ๆ จะมองหาวิธีใหม่ ๆ ในการรับและการจัดส่งผลิตภัณฑ์อย่างรวดเร็ว ตัวอย่างเช่น Amazon (Prime Air) และ Google (Project Wing) ทั้ง 2 บริษัทได้ทดสอบโดรนสำหรับระบบการจัดส่งเพื่อรับพัสดุให้กับลูกค้าภายใน 30 นาที หรือน้อยกว่าเพื่อหลีกเลี่ยงการส่งมอบที่อาจทำให้เกิดความเสียหายแก่ผลิตภัณฑ์ได้ มันอาจถูกมองว่าเป็นนิยายวิทยาศาสตร์ แต่ในปัจจุบันนี้โซ่อุปทานดิจิทัล จะทำความจริงให้เห็นว่าความเร็วในแบบที่ต้องการนี้จะสามารถสำเร็จได้ (Hanifan, G. et al., 2014; Cecere, L. 2016; Penthin, S. et al., 2015)

2. ความยืดหยุ่น (Flexibility) : การทำให้เป็นดิจิทัลในโซ่อุปทาน หมายถึงความต้องการความคล่องตัวในการปฏิบัติงานโดยง่ายในการปรับให้เข้ากับสถานการณ์ที่เปลี่ยนแปลง สิ่งนี้ไม่ได้อธิบายถึงวิธีการจัดส่งสินค้า แต่เป็นการกำหนดถึงวิธีการในการตอบสนองต่อปัญหาภายในโซ่อุปทาน ตัวอย่างเช่น ความไม่มั่นคงทางการเมืองในซีเรีย โรคต่าง ๆ

เช่นโรคระบาดอีโบล่าในแอฟริกาตะวันตก หรือภัยธรรมชาติเช่นแผ่นดินไหวอาจทำลายล้างได้ อย่างไรก็ตามการทำนายเหตุการณ์ดังกล่าวหรือใช้มาตรการที่เหมาะสมและตอบสนองอย่างมีประสิทธิภาพและมีประสิทธิภาพสามารถลดการหยุดชะงักในห่วงโซ่อุปทานได้ ที่กล่าวมานี้เป็นกรณีของโซ่อุปทานแบบดั้งเดิม แต่สำหรับโซ่อุปทานดิจิทัล จะมีความสามารถในการทำให้สิ่งนี้เกือบจะในทันทีโดยการใช้ข้อมูลที่รวบรวมและทำแบบจำลองได้อย่างมีประสิทธิภาพ (Schrauf, S. et al., 2016; Hanifan, G. (2014)

3. ความเชื่อมโยงระดับโลก (Global connectivity): อินเทอร์เน็ตทำให้โลกเล็กลง องค์กรต่าง ๆ ต้องการที่จะส่งมอบสินค้าและบริการทั่วโลกอย่างรวดเร็ว สิ่งนี้จำเป็นต้องมีโซ่อุปทานระดับโลกอย่างแท้จริงเพื่อให้องค์กรไม่เพียงแต่จะส่งมอบสินค้าและบริการได้เท่านั้น แต่ยังเพื่อให้แน่ใจว่าปฏิกิริยาที่อาจเกิดขึ้นได้ในระดับท้องถิ่น หากผลิตภัณฑ์บางอย่างที่ผลิตในยุโรปเป็นที่ต้องการในสหรัฐอเมริกา แล้วไม่สามารถที่จะส่งสินค้านั้น ๆ จาก ยุโรปไปยังสหรัฐอเมริกาในทันทีที่ต้องการ หรือการดำเนินการที่ทำไม่มีประสิทธิภาพก็อาจจะจะใช้เวลาที่ยาวนานและสูญเสียรายได้ที่อาจเกิดขึ้นได้ ดังนั้นโซ่อุปทานดิจิทัล จึงกำหนดวิธีในการสร้างฮับระดับโลกที่มีประสิทธิภาพเพื่อจัดหาสินค้าและบริการในประเทศแทนการพกพาไปทั่วโลกเพื่อการสั่งซื้อเพียงอย่างเดียว (Schrauf, S. et al., 2016; Hanifan, G., 2014)

4. สินค้าคงคลังแบบทันเวลา (Real-time inventory): โซ่อุปทานดิจิทัลเป็นวิธีการที่ทำให้แน่ใจว่าสต็อกสินค้าในมือเพียงพอ แต่ไม่มากเกินไปและตอบสนองความต้องการได้ โซ่อุปทานดิจิทัลทำให้การจัดการคลังสินค้ามีประสิทธิภาพมากขึ้นและตรวจสอบระดับสต็อกอย่างต่อเนื่องด้วยเทคโนโลยีของเซ็นเซอร์หรือผ่านเทคโนโลยีขั้นสูงอื่น ๆ ในขณะที่พฤติกรรมของลูกค้ามีการเปลี่ยนแปลงอย่างรวดเร็ว อุปทานจะต้องตอบสนองความต้องการเสมอ ผู้บริโภคสามารถสั่งซื้อได้ทุกที่ทุกเวลา ดังนั้นควรตรวจสอบสต็อกสินค้าเพื่อให้สามารถส่งมอบได้ในทันที สิ่งที่กระทำอยู่นี้ไม่ได้หมายความว่าควรเก็บปริมาณสินค้าคงคลังเท่ากันทุกศูนย์กระจายสินค้า ในความเป็นจริงควรจะต้องมีการวิเคราะห์ถึงแนวโน้มการซื้อและความต้องการสินค้าและบริการในอนาคตเพื่อจะได้รับการยอมรับล่วงหน้าเพื่อการตัดสินใจอย่างชาญฉลาด โซ่อุปทานดิจิทัลจะมีวิธีการเหล่านี้ที่จำเป็นสำหรับการวิเคราะห์ขั้นสูง (Schrauf, S. et al., 2016; Hanifan, G., 2014)

5. ความฉลาด (Intelligent): เทคโนโลยีรุ่นใหม่จะมีความสามารถที่ชาญฉลาดโดยจะมีความสามารถในการประมวลผลเพียงพอเพื่อให้สามารถเรียนรู้ด้วยตนเองและตัดสินใจได้ด้วยตนเองตามขั้นตอนวิธีที่กำหนดไว้ โซ่อุปทานดิจิทัลจะมีคุณลักษณะที่ครอบคลุมคุณถึงความสามารถเหล่านี้ ซึ่งจะช่วยให้การตัดสินใจที่ดีขึ้นการดำเนินการอัตโนมัติ และสร้างนวัตกรรมใหม่ ๆ ในการดำเนินงาน (Hanifan, G., 2014; Bechtold, J. et al., 2014)

6. ความโปร่งใส (Transparency): ในโซ่อุปทานที่โปร่งใส การเชื่อมโยงในโซ่จะทำความเข้าใจและดำเนินการตามพฤติกรรมและความต้องการของลิงก์อื่น ๆ ในกรณีที่ไม่มีความโปร่งใสกระแสการไหลเวียนภายในโซ่อุปทานจะถูกรบกวนอย่างหลีกเลี่ยงไม่ได้ โซ่อุปทานดิจิทัลสามารถทำให้ บริษัท ต่าง ๆดำเนินการอย่างโปร่งใสและมีความพร้อมเมื่อเกิดเหตุการณ์ที่จะหยุดชะงักได้ดีขึ้นโดยการคาดการณ์สร้างแบบจำลองเครือข่ายสร้างสถานการณ์แบบ What-if และปรับโซ่ให้ทันกับสภาพที่เปลี่ยนแปลง (Schrauf, S. et al., 2016)

7. การลดต้นทุน (Cost-effective): การนำเอาเทคโนโลยีดิจิทัลมาใช้งานจะมีจุดมุ่งหมายหลักคือ การลดค่าใช้จ่ายในทุกพื้นที่ ต้นทุนจากการลงทุนเริ่มแรกอาจสูงสำหรับเทคโนโลยีใหม่ ๆ แต่ก็จะลดลงตามเวลา โซ่อุปทานดิจิทัลนั้นเป็นวิธีที่ประหยัดค่าใช้จ่ายสำหรับองค์กรไม่ใช่เพียงเพราะการใช้ประโยชน์จากเทคโนโลยี แต่ยังเป็นเพราะกระบวนการจัดการโซ่อุปทานด้วย โซ่อุปทาดิจิทัลนั้นสร้างประสิทธิภาพค่าใช้จ่ายสำหรับองค์กร

8. การปรับขนาดได้ (Scalability): การปรับโซ่อุปทานให้มากขึ้นหรือลงตามสถานการณ์ที่จำเป็นมักจะเป็นการสร้างความพยายามครั้งยิ่งใหญ่สำหรับองค์กร เมื่อโซ่อุปทานแบบดั้งเดิมถูกรวมเข้ากับระบบดิจิทัล อย่างไรก็ตามความสามารถในการปรับขยายได้กลายเป็นปัญหาน้อยลง สิ่งนี้ทำให้การเพิ่มประสิทธิภาพและการทำซ้ำของกระบวนการง่ายขึ้นและการตรวจพบความผิดปกติและข้อผิดพลาดที่ง่ายขึ้น (Hanifan, G., 2014; Bechtold, J. et al., 2014)

9. การมีนวัตกรรม (Innovative): ความเป็นเลิศในโซ่อุปทานดิจิทัลถือได้ว่าเป็นคุณลักษณะสำคัญคือ การที่โซ่อุปทานดิจิทัลจะเปิดรับต่อการเปลี่ยนแปลงอยู่เสมอ โลกกำลังถูกครอบงำด้วยเทคโนโลยีใหม่ ๆ ในอัตราที่เร็วกว่าที่เคยเป็นมา โซ่อุปทานดิจิทัลควรมองหาวิธีใหม่ ๆ ในการรวมนวัตกรรมเหล่านี้เข้ากับกระบวนการเพื่อให้สามารถแข่งขันได้และสร้างความมั่นใจในความเป็นเลิศในโซ่อุปทาน นวัตกรรมที่เกิดขึ้นของวันนี้จะกลายเป็นเทคโนโลยีที่หยุดการทำงาน และไม่สามารถทำงานต่อไปได้ของวันพรุ่งนี้ ตัวอย่างได้แก่ วิวัฒนาการของทีวีจากขาวดำไปเป็นสมาร์ตทีวี หรือการเปลี่ยนแปลงจากกระดาษและปากกาไปจนถึงแว่นตาอัจฉริยะในการจัดการคลังสินค้าด้วยการเลือกแนวทางในการจัดเก็บสินคาที่ดีที่สุด เทคโนโลยีเปลี่ยนแปลงอย่างหลีกเลี่ยงไม่ได้ ซึ่งมันกลายเป็นส่วนหนึ่งของนวัตกรรม ข้อมูลกลายเป็นพื้นฐานสำหรับองค์กรการค้าที่ไม่มีการเปลี่ยนแปลงในพัน ๆ ปี ข้อมูลขนาดใหญ่ที่องค์กรต้องจัดเก็บเพื่อนำมาใช้งานก็ถูกเปลี่ยนจากเดิมให้มาเก็บในคอมพิวเตอร์หรือแท็บเล็ต หรือการคิดคำนวณที่พัฒนาขึ้นมาจากลูกคิดให้กลายมาเป็นซูเปอร์คอมพิวเตอร์อย่างในปัจจุบัน (Cukier, K., 2018) นี่เป็นเพียงตัวอย่างเล็ก ๆ น้อย ๆ ของวิธีการที่เป็นนวัตกรรมใหม่ของโซ่อุปทานดิจิทัลในฟังก์ชั่นต่างๆ

10. การแข่งขันเชิงรุก (Proactive): โซ่อุปทานดิจิทัลมีการดำเนินการเชิงรุกเพื่อป้องกันการหยุดชะงักที่อาจเกิดขึ้น สิ่งนี้สามารถทำได้ไม่เพียง แต่ผ่านการแก้ไขปัญหาเท่านั้น แต่ยังสามารถระบุปัญหาที่แฝงไว้ล่วงหน้าผ่านการวิจัย มันต้องการความรู้และการวางแผนจำนวนมากเพื่อประสานงานปัญหาเหล่านี้ นอกจากนั้นโซ่อุปทานดิจิทัลยังได้นำเสนอโซลูชั่นเชิงรุกเพื่อคาดการณ์ปัญหาก่อนเกิดขึ้นกรอบการวิเคราะห์ที่มีประสิทธิภาพและความชาญฉลาดในการดำเนินงานเพื่อตอบสนองผู้บริโภคที่ใช้ระบบดิจิทัล

11. ความเป็นมิตรกับสิ่งแวดล้อม (Eco-friendly): โซ่อุปทานมีผลกระทบต่อสิ่งแวดล้อมในระดับหนึ่ง หากโซ่อุปทานดิจิทัลไม่ให้ความสำคัญกับสภาพแวดล้อมมากพอ มันอาจนำไปสู่การหยุดชะงักทางธุรกิจเนื่องจากการปฏิบัติที่ขัดแย้งกฎหมายสิ่งแวดล้อมหรือการรับรู้ของสาธารณชน การค้นหาโซ่อุปทานแบบดั้งเดิมที่มีแนวปฏิบัติที่เป็นมิตรกับสิ่งแวดล้อมในทุก ๆ ขั้นตอนเป็นภารกิจที่น่ากังวลสำหรับโซ่อุปทานดิจิทัลในยุคใหม่สามารถเพิ่มขีดความสามารถของกระบวนการที่เป็นมิตรกับสิ่งแวดล้อม

2.1.3 เทคโนโลยีที่เกี่ยวข้องกับโซ่อุปทานดิจิทัล

ผู้บริหารหลายคนพยายามอย่างหนักเพื่อขัดขวางกระแสโดยไม่ทำให้เกิดการเปลี่ยนแปลงอย่างใด ๆ กับองค์กรเมื่อต้องเผชิญกับการเปลี่ยนแปลงพื้นฐาน การที่พยายามมองหาวิธีการใหม่ ๆ เพื่อการก้าวไปข้างหน้า เป็นที่สังเกตได้ว่า บริษัท ที่มีชื่อเสียงกำลังพยายามทำให้การดำเนินงานโซ่อุปทานเป็นดิจิทัลมากขึ้น จากเซ็นเซอร์และบริการคลาวด์ไปจนถึงนาโนเทคโนโลยีและข้อมูลขนาดใหญ่ (Big data) เทคโนโลยีหลายอย่างได้เข้ามาช่วยผลักดันให้เกิดเป็นโซ่อุปทานดิจิทัลมากขึ้น ดังนั้นแล้วโซ่อุปทานดิจิทัลจึงมีแนวโน้มทางดิจิทัลที่สำคัญมากมายที่สามารถนำไปใช้ในโซ่อุปทานเพื่อปรับปรุงอนาคตต่อการดำเนินงานเป็นอย่างมาก ดังนั้นแล้วจากรายงานการวิจัยที่ได้มีการตีพิมพ์อย่างมากมายในปัจจุบัน รวมไปถึง บริษัทต่าง ที่ปรึกษาและนักวิจัยต่าง ๆ ทำให้ผู้วิจัยสามารถที่จะสรุปถึงแนวโน้มทางด้านเทคโนโลยีที่จะมาใช้ในงานด้านโซ่อุปทานเพื่อการนำไปสู่การเป็นโซ่อุปทานดิจิทัลต่อไป โดยรายละเอียดของเทคโนโลยีต่าง ๆ ผู้วิจัยได้ทำการสรุปไว้ดังรายละเอียดดังต่ไปนี้

1. เทคโนโลยีโลกเสมือนผสานโลกแห่งความจริง (Augmented Reality: AR) (Cirulis, A. et al., 2013; Glockner, H. et al., 2014) AR ถูกอธิบายว่าเป็นส่วนขยายของความเป็นจริงทางกายภาพโดยการเพิ่มเลเยอร์ของคอมพิวเตอร์ที่สร้างข้อมูลให้กับสภาพแวดล้อมจริง ข้อมูลในบริบทนี้อาจเป็นวัตถุหรือเนื้อหาเสมือนใด ๆ รวมถึงข้อความกราฟิก วิดีโอ เสียงการตอบรับแบบสัมผัสข้อมูล Global Positioning Systems (GPS) และแม้แต่กลิ่น ความท้าทายของ AR ในโซ่อุปทานดิจิทัลนั้นคือ การยอมรับทางสังคม การระบุความเป็นส่วนตัว และผลกำไรสำหรับธุรกิจ

ความท้าทายอื่น ๆ รวมถึงการดำเนินการหยิบสินค้าที่ดีที่สุดและการทดสอบเสมือนจริงของชิ้นส่วนและซัพพลายเออร์ชุดใหม่เพื่อลดการกระจายสินค้าตัวอย่างทางกายภาพ

2. ข้อมูลขนาดใหญ่ (Big data: BD) (Wang, G. et al., 2016; Jeske, M. et al., 2013) BD เป็นคำที่มีการพัฒนาซึ่งใช้เพื่ออธิบายข้อมูลที่มีโครงสร้างกึ่งโครงสร้างหรือไม่มีโครงสร้างจำนวนมากที่มีศักยภาพที่จะทำการหาข้อมูล สำหรับการขนส่งสินค้าหลายล้านรายการที่ทำทุกวัน ต้นกำเนิดและปลายทาง ขนาดน้ำหนัก เนื้อหาและสถานที่ ฯลฯ ล้วนมีการติดตามในเครือข่ายการจัดส่งทั่วโลก แต่การติดตามข้อมูลนี้ใช้ประโยชน์อย่างคุ้มค่าหรือไม่

3. การประมวลผลแบบคลาวด์(Cloud Computing: CC) (Raj, S. et al., 2014; Schmidt, B. et al., 2015) CC มอบเครือข่ายบริการเสมือนจริงเพื่อให้ผู้ใช้สามารถเข้าถึงได้จากทุกที่ในโลกด้วยการสมัครสมาชิกในราคาที่แข่งขันได้ โซ่อุปทานดิจิทัลที่ได้มีการเปิดใช้งานโดย CC มีความท้าทายที่ชัดเจนซึ่งช่วยให้มองเห็นข้อมูลเชิงลึกและยืดหยุ่นอย่างที่ไม่เคยมีมาก่อน ในขณะที่ทำงานอย่างรวดเร็วและเป็นระดับมากขึ้น การสูญเสียการควบคุมข้อมูลที่เคยตั้งอยู่บนเซิร์ฟเวอร์ภายในและ/ หรือฮาร์ดไดรฟ์คอมพิวเตอร์ความปลอดภัยของข้อมูลบนเว็บและสถานการณ์การขัดข้องของบริการก็เป็นความท้าทายเช่นกัน

4. หุ่นยนต์ (Robotics: R) [Schmidt, B. et al., 2015; Bonkenburg, T., 2016) เทคโนโลยีหุ่นยนต์ใน โลจิสติกส์เป็นสาขาวิศวกรรมที่เกี่ยวข้องกับความคิดการออกแบบการผลิตและการดำเนินงานของ หุ่นยนต์ ความท้าทายในหุ่นยนต์มันไม่ได้เป็นความเร็วของการพัฒนา แต่กลับเป็นความกลัวที่อาจเกิดขึ้นจากมนุษย์ รัฐบาลและหน่วยงานกำกับดูแลที่มีต่อเทคโนโลยีความยืดหยุ่นระบบอัตโนมัติที่มีความสามารถในการติดตามความต้องการที่เปลี่ยนแปลงไปหรือความกังวลเกี่ยวกับหุ่นยนต์ที่เข้ามาควบคุมงานทั้งหมดและความปลอดภัย

5. เทคโนโลยีเซ็นเซอร์ (Sensor Technology: ST) (Richter, K. et al., 2013) ST เป็นสิ่งจำเป็นสำหรับการตรวจจับและสถานะการบรรจุคุณภาพผลิตภัณฑ์ คุณภาพบรรจุภัณฑ์ สถานะอุปกรณ์ ในสภาพสนามที่หลากหลาย การวิเคราะห์ข้อมูลแบบเรียลไทม์จากเซ็นเซอร์ปรับปรุงประสิทธิภาพการทำธุรกรรมเนื่องจากการควบคุมกระบวนการที่แพร่หลายและการเพิ่มประสิทธิภาพของโรงงานความจำเป็นในการปรับใช้โครงสร้างพื้นฐานที่กว้างขวางและมีราคาแพงในตำแหน่งทางภูมิศาสตร์

6. เทคโนโลยีการติดต่อสื่อสารหลากหลายช่องทาง (Omni Channel: OC) (Kraemer, D., 2015) OC เป็นวิธีการหลายช่องทางในการขายที่พยายามมอบประสบการณ์การช็อปปิ้งที่ไร้รอยต่อให้กับผู้บริโภคไม่ว่าผู้บริโภคจะช็อปปิ้งออนไลน์จากเดสก์ท็อปหรืออุปกรณ์มือถือ

ทางโทรศัพท์หรือในร้านขายอิฐ ขายตรงให้กับผู้ใช้และผู้บริโภคที่มีขนาดล็อตเล็กและความต้องการคลังสินค้าส่วนกลางและภูมิภาคที่แตกต่างกัน

7. อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of things: IoT) (Macaulay, J. et al., 2015) IoT อ้างถึงวัตถุในชีวิตประจำวันที่มี ไอพีแอดเดรส (IP address) สำหรับการเชื่อมต่ออินเทอร์เน็ตที่อนุญาตให้ส่งและรับข้อมูลดังนั้นการสื่อสารจึงเกิดขึ้นระหว่างวัตถุเหล่านี้กับอุปกรณ์และระบบเครือข่ายอื่น ๆ การใช้ตัวระบุเฉพาะสำหรับสินทรัพย์ประเภทต่าง ๆ ในอุตสาหกรรมต่าง ๆ ในระดับโลกการทำงานร่วมกันอย่างราบรื่นสำหรับการแลกเปลี่ยนข้อมูลเซ็นเซอร์ในสภาพแวดล้อมที่ต่างกันการสร้างความน่าเชื่อถือและความเป็นเจ้าของข้อมูลและการเอาชนะปัญหาความเป็นส่วนตัว

8. ยานพาหนะที่ขับเคลื่อนด้วยตนเอง (Self-Driving Vehicles: SDV) (DHL Trend Research., 2014) SDV เป็นยานพาหนะที่มีความสามารถในการตรวจจับสภาพแวดล้อมและการนำทางโดยไม่มีการป้อนข้อมูลของมนุษย์ เพื่อให้ยานพาหนะสามารถขับขี่ได้จำเป็นต้องมีฟังก์ชั่นการพึ่งพาซึ่งกันและกันพื้นฐานสี่ประการ การวิเคราะห์สถานการณ์ การวางแผน การเคลื่อนที่และการควบคุมวิถี นอกเหนือจากความสามารถทางเทคโนโลยีแล้วความท้าทายที่สำคัญบางประการยังรวมถึงแรงกดดันด้านกฎระเบียบการยอมรับจากสาธารณะและความรับผิด

9. อากาศยานไร้คนขับ (Unmanned Aerial Vehicle: UAV) (Heutger, M. and Kuckelhaus, M., 2014) UAV เป็นเครื่องบินที่ไม่มีนักบินบนเครื่องบิน รู้จักกันในชื่อโดรน UAV สามารถเป็นเครื่องบินควบคุมระยะไกลหรือสามารถบินได้ด้วยตนเองตามแผนการบินที่ตั้งโปรแกรมไว้ล่วงหน้าหรือระบบอัตโนมัติแบบไดนามิกที่ซับซ้อนยิ่งขึ้น สภาพแวดล้อมด้านกฎระเบียบความกังวลด้านความเป็นส่วนตัวและการรวมเข้ากับเครือข่ายที่มีอยู่เป็นความท้าทายที่สำคัญสำหรับ UAV นอกเหนือจากความท้าทายที่จับต้องได้ (และสามารถควบคุมทางเทคนิค) ของน่านฟ้าที่แออัดและความเสี่ยงโดยธรรมชาติแล้วยังมีพื้นที่อื่น ๆ ที่เกี่ยวข้องน้อยกว่าที่กำหนดไว้ในโดเมนสาธารณะ

10. นาโนเทคโนโลยี (Nanotechnology: N) และ การพิมพ์ 3 มิติ (3D Printing: 3DP) (Schmidt, B. et al., 2015) N เป็นวิศวกรรมของระบบการทำงานในระดับโมเลกุล และ 3DP หรือที่รู้จักกันว่าการผลิตแบบเติมแต่ง หมายถึงกระบวนการต่าง ๆ ที่ใช้ในการสังเคราะห์วัตถุ 3 มิติ การประสบความสำเร็จในการนำ N และ 3DP ไปใช้ในด้านโลจิสติกส์และโซ่อุปทานนั้นต้องการความร่วมมือที่แข็งแกร่งพร้อมกับการมีส่วนร่วมระดับสูงระหว่างผู้เล่นและคู่แข่งที่แตกต่างกันภายในห่วงโซ่อุปทานและความเต็มใจทั่วไปในการลงทุน

2.2 การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล

ในปัจจุบันนี้ระบบเทคโนโลยีสารสนเทศที่นำมาใช้สำหรับกิจกรรมในโซ่อุปทานได้ถูกพัฒนาขึ้นให้มีความสามารถในการที่จะช่วยสนับสนุนการทำงานที่จะเชื่อมต่อข้อมูลระหว่างองค์กรต่าง ๆ ภายในโซ่อุปทานหรือระหว่างโซ่อุปทานได้มากยิ่งขึ้น และเนื่องด้วยความก้าวหน้าในด้านเทคโนโลยีได้เปลี่ยนแปลงไปอย่างรวดเร็ว อันจะมีผลกระทบต่อการดำเนินกิจกรรมในโซ่อุปทาน จึงเป็นสิ่งจำเป็นอย่างยิ่งที่แต่ละบริษัทในโซ่อุปทานจะต้องมีการปรับตัวไปตามเทคโนโลยีเหล่านั้น ดั้งนั้นเพื่อให้ธุรกิจสามารถที่แข่งขันได้ในระดับโลก (Global Competition) การบริหารจัดการในโซ่อุปทานจึงต้องมีลักษณะที่มีความยืดหยุ่น (Flexible), มีความคล่องตัว (Agility) มากขึ้นตามไปด้วย

ตัวอย่างเทคโนโลยีสารสนเทศที่ได้รับการสนับสนุนจากทางภาครัฐในปัจจุบันนี้ ได้แก่ เทคโนโลยีระบบการประมวลผลแบบคลาวด์ (Cloud Computing) ซึ่งเป็นเทคโนโลยีที่สามารถสร้างความได้เปรียบทางแข่งการแข่งขัน โดยการประมวลผลแบบคลาวด์นี้จะเข้ามาช่วยแก้ปัญหาเรื่องข้อมูลที่ใช้ในการสื่อสารกันทางธุรกิจระหว่างลูกค้า (Customers) และผู้จำหน่าย (Suppliers) ได้ โดยที่ลักษณะของการทำงานแบบการประมวลผลแบบคลาวด์ จะมีการใช้ข้อมูลร่วมกัน (Information Sharing) ซึ่งก็จะเป็นการแก้ปัญหาในเรื่องของการต้องการรับรู้ข้อมูลแบบทันที (Real-time) ตัวอย่างเช่น ข้อมูลความต้องการสินค้า (Demand Information) จากลูกค้าที่ผู้จำหน่ายจะรู้ได้ทันที ประกอบกับข้อมูลสินค้าคงเหลือ (Stock Balance) ที่ลูกค้าก็สามารถทราบได้ทันทีว่าผู้จำหน่ายมีสินค้าเหลืออยู่หรือไม่ (Grubisic, 2014; Dhar, 2012; Obeidat et al., 2013) สิ่งที่สำคัญประการหนึ่งในการนำใช้เทคโนโลยีการประมวลผลแบบคลาวด์ก็คือ สินค้าและบริการจะถูกจัดส่งด้วยความรวมเร็วและเชื่อถือได้ ในทุก ๆ ที่และทุก ๆ เวลาเมื่อไหร่ก็ได้ที่มีความต้องการ ดังนั้นเมื่อมีการใช้ข้อมูลร่วมกัน ดังที่ได้กล่าวมาแล้วระหว่างลูกค้าและผู้จำหน่ายนั้น สิ่งที่ตามมาก็คือ การที่จะต้องทำให้เกิดความสมดุลขึ้นระหว่างความต้องการซื้อ (Demand) กับ ความต้องการขาย (Supply) ในโซ่อุปทานทั้งหมด

แต่การทำงานด้วยระบบการประมวลผลแบบคลาวด์นี้จะเป็นระบบที่ทำงานผ่านระบบเครือข่ายอินเทอร์เน็ตหรือแม้แต่การทำงานใด ๆ ในปัจจุบันที่ระบบโซ่อุปทานต้องมีการดำเนินงานก็จะผ่านระบบเครือข่ายอินเทอร์เน็ตทั้งสิ้น ไม่ว่าจะเป็นผ่านเว็บเบราเซอร์ (Web-Browser) มือถือ แท็บเล็ต (Toka Agorasti et al., 2013; Durowoju et al., 2011) และเนื่องด้วยในปัจจุบันการทำงานผ่านระบบเครือข่ายอินเทอร์เน็ตมีจำเป็นอย่างยิ่ง หรือกล่าวได้ว่าธุรกิจในทุกประเภทจำเป็นต้องทำงานผ่านระบบเครือข่ายอินเทอร์เน็ตทั้งสิ้น เนื่องจากอินเทอร์เน็ตเป็นเทคโนโลยีที่มีประโยชน์อย่างมหาศาล แต่ในขณะเดียวกันอินเทอร์เน็ตก็แฝงไปด้วยภัยที่อันตรายที่ก่อให้เกิดความเสียหาย

ได้ทั้งในส่วนบุคคลและองค์กรธุรกิจ โดยที่ภัยดังกล่าวนี้ได้เกิดจากมนุษย์ซึ่งเป็นผู้ที่รู้จักกับอินเทอร์เน็ตเป็นอย่างดีที่ได้เป็นผู้สร้างมันขึ้นมา

อินเทอร์เน็ตถือว่าเป็นสังคม ๆ หนึ่ง ที่มีผู้ใช้งานรวมอยู่ด้วยกันเป็นจำนวนมาก ถือได้ว่าเป็นมิติที่มีความซ้อนกันหลายรูปแบบ ตามความชอบบ้าง ตามอาชีพบ้าง ตามภูมิศาสตร์บ้าง ซึ่งย่อมมีทั้งคนดีและคนไม่ดีปะปนกันไป อินเทอร์เน็ตเป็นสังคมที่มีการเชื่อมโยงกันผ่านไอพี ไม่มีเขตแดน ไม่แบ่งชั้นวรรณะย่อมเป็นเรื่องธรรมดาที่จะต้องมีสิ่งดีและสิ่งไม่ดี และเป็นสิ่งที่มีภัยที่เป็นอันตรายแอบแฝงอยู่มาก ดังนั้นอาชญากรรมที่ผ่านมาทางอินเทอร์เน็ตจึงได้เกิดขึ้น โดยการแฝงตัวซึ่งอาจจะเข้ามาทำลายระบบหรือเข้ามาล้วงข้อมูล เพื่อหาผลประโยชน์จากการแฝงตัวเข้ามาดังกล่าวนั้น ด้วยเหตุนี้จึงเป็นจุดอ่อนหรือช่องโหว่ (Vulnerable) ให้กับผู้ที่ไม่ประสงค์ดีในการที่เข้ามาโจมตีและทำลายข้อมูลที่สำคัญต่อการดำเนินงานได้ โดยที่ภัยที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ตเป็นเรื่องที่สามารถเกิดขึ้นได้กับทุกคนหรือทุกองค์กร ผู้วิจัยจึงได้ทำการรวบรวมประเภทของภัยบนอินเทอร์เน็ต จากการเผยแพร่ของนักวิชาการต่าง ๆ เพื่อให้เข้าใจถึงภัยบนอินเทอร์เน็ตดังต่อไปนี้ (http://www.wuttichai.net/forums/archive/index.php?t-94.html)

1. ภัยที่มาจาก สแปมอีเมล์ (Spam Email) และ อีเมล์มุ่งทำร้าย (Malicious Email) โดยที่อีเมล์ทั้งสองนี้ จะมาจากกลุ่มผู้ที่ไม่หวังดีได้ใช้ ในปัจจุบันนี้ได้มีการใช้อีเมล์เป็นเครื่องมือในการส่งข้อมูลที่มีอันตรายให้กับผู้ใช้และองค์กรในรูปแบบต่าง ๆ ทั้งได้มีการแนบไฟล์ (Attached File) หรือในรูปแบบของเนื้อหาล่อลวงในอีเมล์ จากปี ค.ศ.1997 ปริมาณสแปมเมล์เพิ่มขึ้นถึง 10 เท่า และจะเพิ่มขึ้นเป็นทวีคูณในปีต่อ ๆ ไป เหตุผลประการหนึ่งที่ได้เกิดการกระทำในลักษณะเช่นนี้เนื่องจากว่า สแปมอีเมล์ นี้สามารถเป็นอาชีพในด้านมืดที่ทำรายได้อย่างดีให้กับเหล่ามิจฉาชีพทางอินเทอร์เน็ตได้ ในความพยายามที่จะแก้ปัญหาเล่านี้ ตัวอย่างเช่น ประเทศสหรัฐอเมริกาได้ออกกฎหมาย “Anti-Spam Act” ขึ้นมา เพื่อต่อต้านเหล่าบรรดาสแปมเมอร์ แต่ก็ยังไม่สามารถกำจัด สแปมอีเมล์ให้หมดไปจากโลกอินเทอร์เน็ตได้ วิธีการแก้ปัญหาที่ถูกทางคือการใช้ระบบ Anti-Spam/Anti-Virus ที่บริเวณ Internet Gateway หรือ DMZ กรองสแปมอีเมล์ในจุดที่ระบบของผู้ใช้รับ-ส่ง อีเมล์จากอินเทอร์เน็ต และการใช้ Anti-Spam Software ช่วยที่เครื่องพีซีเพื่อกรองแบบละเอียดอีกชั้นหนึ่ง ตลอดจนพยายามไม่ประกาศอีเมล์ในเว็บบอร์ด หรือ ในเว็บไซต์ของเราเอง ถ้าต้องการให้อีเมล์แอดเดรสเพื่อให้ผู้อื่นรับทราบ ควรใช้ทำเป็นรูปภาพ หรือใช้ HTML Character จะปลอดภัยกว่าการประกาศแสดงเป็น Plain Text ธรรมดา

2. ภัยที่มาจากสปายแวร์ (Spyware) ในปัจจุบันปัญหาของผู้ใช้งานที่จะพบคือ เครื่องพีซีที่เราใช้งานอยู่นั้นติดสปายแวร์ ทั้งที่เครื่องพีซีที่ใช้งานอยู่ก็มีโปรแกรมแอนตี้ไวรัส แต่ปัญหาก็คือโปรแกรมสปายแวร์ ไม่ใช่โปรแกรมไวรัส เช่น โปรแกรมดักคีย์บอร์ด และเก็บหน้าจอการใช้งาน

คอมพิวเตอร์ของผู้ใช้ ที่ในวงการเรียกว่าโปรแกรม “Key Logger” เป็นโปรแกรมที่ระบบแอนตี้ไวรัสส่วนมากมองไม่เห็น และไม่สามารถกำจัดออกจากเครื่องคอมพิวเตอร์ได้ สาเหตุที่พีซีติดสปายแวร์ จะมาจากการเข้าชมเว็บไซต์ต่าง ๆ โดยไม่ระมัดระวังให้ดีพอ รวมทั้งการดาวน์โหลด (Download) ไฟล์ที่มีสปายแวร์ติดมาด้วย ตลอดจนการเปิดไฟล์แนบที่มาจากอีเมล์ที่มีโปรแกรมร้ายนี้แนบมาด้วย ขณะที่โปรแกรมดังกล่าวยังมาในรูปของคุกกี้ (Cookies) เวลาเราเข้าเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บภาพลามก หรือ เว็บไซต์ที่ใช้ในการหา Serial number ของซอฟต์แวร์ผิดกฎหมายเป็นต้น ในบางครั้งสปายแวร์ก็ติดมากับโปรแกรมประเภท Peer-to-Peer (P2P) ที่กำลังได้รับความนิยมอยู่ในขณะนี้ แนวทางในการแก้ปัญหาก็คือ ต้องระมัดระวังในการใช้งานอินเทอร์เน็ตให้มากขึ้น ตลอดจนหมั่นใช้โปรแกรมประเภทฟรีแวร์ (Freeware) หรือ แชร์แวร์ (Shareware) เช่น Ad-Aware หรือ Spybot Search & Destroy ในการช่วยตรวจสอบระบบพีซีว่าติดสปายแวร์อยู่หรือไม่ ถ้าตรวจพบก็ควรกำจัดออกโดยเร็วจะทำให้ไม่เสียความเป็นส่วนตัว และทำให้พีซีเร็วขึ้น ตลอดจนประหยัดแบนด์วิธในการใช้งานเครือข่ายโดยรวม

3. ภัยที่มาจากมัลแวร์ (Malware - Malicious Software) มัลแวร์ (Malware) คือ Malicious Software หรือ โปรแกรมมุ่งร้ายที่มาในรูปแบบต่าง ๆ ไม่ว่าจะเป็น ActiveX หรือ Java Applet ที่มากับการใช้งานโปรแกรมบราวเซอร์ โดยไม่ได้รับการติดตั้งแพทช์ (Patch) หรืออาจมาในรูปของไฟล์แนบที่อยู่ในอีเมล์ตลอดจนแฝงมากับแชร์แวร์ หรือโปรแกรมอรรถประโยชน์ (Utility) หรือโปรแกรม P2P ที่เรานิยมใช้ในการดาวน์โหลดเพลง หรือภาพยนตร์ผ่านทางอินเทอร์เน็ต ในช่วงหลัง ๆ มักจะมาในรูปของไฟล์ที่มีการบีบอัด (Zip File) และมีการปลอมแปลงชื่อผู้ส่ง ปลอมแปลงอีเมล์ เทคนิคการหลอกผู้ใช้อีเมล์ให้หลงเชื่อ หรือที่เรียกว่า “Social Engineering” เป็นวิธีการเก่าแก่ที่ผู้ไม่หวังดีนิยมใช้เป็นประจำ ทางแก้ปัญหานอกจากจะใช้โปรแกรมแอนตี้ไวรัส และแอนตี้มัลแวร์ แล้วยังควรจะต้องฝึกอบรม “Information Security Awareness Training” ให้กับผู้ใช้งานคอมพิวเตอร์อีกด้วย โดยเฉพาะกลุ่มผู้ใช้คอมพิวเตอร์ที่ไม่ใช่คนไอที (Non-IT people) เพื่อให้ผู้บริหารหรือผู้ใช้งานคอมพิวเตอร์ทั่วไป มีความเข้าใจถึงวิธีการหลอกลวงของผู้ไม่หวังดี และรู้เท่าทันไม่ตกเป็นเหยื่อของผู้ไม่หวังดี นอกจากนี้ยังมีไวรัสตัวใหม่ ๆ สามารถสั่งปิดการทำงานของโปรแกรมแอนตี้ไวรัสได้ และยังมีไวรัสใหม่ ๆ ที่ออกมาโดยที่โปรแกรมแอนตี้ไวรัสยังไม่มี Signature หรือ Pattern ที่เราเรียกว่า Zero-DayAttack หรือ Virus Outbreak ดังนั้นการฝึกอบรมให้ผู้ใช้คอมพิวเตอร์มีความตระหนักและความเข้าใจ จึงเป็นหนทางที่ไม่อาจถูกมองข้ามได้ในสถานการณ์การแพร่ระบาดไวรัสในขณะนี้และในอนาคต

4. ภัยจากการล่อลวงโดยวิธี Phishing และ Pharming โดย “Phishing” หมายถึง การตกปลา เราอาจตกเป็นเหยื่อของการตกปลา ถ้าเผลอไปติดกับเหยื่อที่เหล่า “Phisher” หรือผู้ไม่หวังดีล่อไว้ วิธีการพวกนี้ คือ การส่งอีเมล์ปลอมแปลง ชื่อคนส่งและชื่อเรื่อง (Email address & Email subject) ตลอดจนปลอมแปลงเนื้อหาในอีเมล์ให้ดูเหมือนจริง เช่น ธนาคารที่ติดต่ออยู่เป็นประจำอีเมล์บอกให้เราลงชื่อเข้าใช้งาน (Login) เข้าใช้งานอินเทอร์เน็ตแบงค์กิ้ง (Internet Banking) โดยจะทำลิ้งค์(Link) มาให้เราคลิก (Click) หากเผลอคลิกโดยไม่ระมัดระวัง เราก็จะเข้าไปติดกับดักที่ Phisher วางไว้ การทำงานของผู้ไม่หวังดีจะกระทำโดยจำลองเว็บไซต์ของธนาคารให้ดูเหมือนจริง แต่จริง ๆ แล้วเป็นเว็บของผู้ไม่หวังดีที่ได้สร้างเอาไว้สำหรับดักจับชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของเรา จากนั้น Phisher จะนำชื่อผู้ใช้งานและรหัสผ่านของเราเข้าไปลงชื่อเข้าใช้งานในเว็บไซต์จริงของธนาคาร และจะโอนเงิน หรือ ชำระเงินค่าสาธารณูปโภค เช่น ค่าน้ำ ค่าไฟ ค่าโทรศัพท์ หรือค่าใช้จ่ายใด ๆ โดยที่เราต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด ธนาคารคงไม่สามารถรับใช้แทนเราได้เพราะเราเป็นคนบอกชื่อผู้ใช้งานและรหัสผ่าน ให้กับผู้ไม่หวังดีเสียเอง เป็นต้น ทางแก้ปัญหาคือเราต้องมีสติ และคอยระมัดระวังอีเมล์ประเภทนี้ บางครั้งอีเมล์อาจมาในรูปของโทรจัน (Trojan) ที่จะเข้ามาแก้ไขไฟล์ Host ในเครื่องให้ Redirect ไปยังเว็บของผู้ไม่หวังดีโดยตรงเลยก็มี วิธีการเช่นนี้ และการ Hijack DNS Server เรียกว่า วิธีฟาร์มมิ่ง "Pharming" ที่กำลังได้รับความนิยมเพิ่มขึ้น

5. ภัยที่มาจากแฮ็กเกอร์ (Hacker) และ Google Hacking Method โดยในปัจจุบันนี้ การแฮกก์ข้อมูลไปยังเว็บแอพลิเคชันที่มีชื่อเสียง จากข้อมูลสถิติจากเว็ปไซต์ http://www.zoneh.org นั้นแสดงให้เห็นว่า มีการเปลี่ยนแปลงรูปแบบไปแล้ว โดยในปัจจุบันแฮ็กเกอร์ได้อาศัยเว็บไซต์ http://www.google.com เป็นช่องทางค้นหา Web ที่มีช่องโหว่ จากนั้นจึงแฮ็กตามวิธีการปกติ และเนื่องจาก Google Hacking นั้น เป็นการแฮกก์แบบไม่เลือกเหยื่อ ดังนั้น ทุกเวปที่มีช่องโหว่ที่ Google เห็น จึงล้วนแล้วแต่มีโอกาสถูกแฮกก์เท่า ๆ กัน ทั้งสิ้น

6. ภัยที่มาจากโปรแกรม “Peer-to-Peer” (P2P) เป็นภัยที่เกิดจากตัวผู้ใช้เป็นหลัก เนื่องจากโปรแกรมประเภทนี้ จะให้ประโยชน์กับเรื่องส่วนตัวของผู้ใช้ เช่น การใช้โปรแกรม Kazaa เพื่อดาวน์โหลดและเล่นภาพยนตร์แบบผิดกฎหมาย หรือใช้โปรแกรม Skype ในการพูดคุยสื่อสารแทนการใช้โทรศัพท์ โดยการใช้โปรแกรมดังกล่าวจะนำภัยมาสู่องค์กร ได้แก่ การสิ้นเปลืองแบนด์วิธในเครือข่ายขององค์กร เนื่องจากการใช้แบนด์วิธจำนวนมาก เช่น การดาวน์โหลดซอฟต์แวร์เถื่อนจากเครื่องพีซีอื่น ๆ ทั่วโลก ส่วนโปรแกรม Skype ที่ใช้เป็นโทรศัพท์ผ่านอินเทอร์เน็ต สร้างปัญหาด้านความเชื่อมั่น (Confidentiality) นอกจากนี้ยังเคยพบว่า มีช่องโหว่บน Kazaa ที่ส่งผลทำให้แฮ็กเกอร์สามารถที่จะเจาะฮาร์ดดิสก์ของคนทั้งโลก ที่ติดตั้งโปรแกรม Kazaa ทำให้ข้อมูลสำคัญ

ขององค์กรหลุดรั่วไปยังมือของผู้ไม่หวังดีได้ สำหรับการแก้ปัญหาทำได้โดยองค์กรควรจะดำเนินการเพื่อการใช้การควบคุมป้องกัน (Implement Preventive Control) โดยใช้โปรแกรมประเภทการจัดการเครื่องคอมพิวเตอร์ (Desktop Management) หรือแอนตี้มัลแวร์ (Anti-Malware) หรือโปรแกรมในการตรวจสอบเครือข่าย (Network Monitoring) ในการเฝ้าระวังเครือข่าย เพื่อเป็นการควบคุมและป้องกันให้กับองค์กรด้วย

7. ภัยที่มาจากการคุกคามบนเครือข่ายไร้สาย (Wireless Network Threat) สำหรับการติดตั้งเครือข่ายไร้สาย (Wireless Network) นั้นเป็นเรื่องที่ค่อนข้างอันตราย เนื่องมาจากโครงสร้างของเครือข่ายไร้สายนั้นออกแบบมาอย่างไม่ปลอดภัย อีกทั้งเทคโนโลยีด้านนี้นั้นยังไร้ขอบเขตสามารถขยายไปยังภายนอกองค์กรได้ด้วย ในขณะที่ผู้ที่ได้นำเทคโนโลยีดังกล่าวนี้มาใช้ ยังมีความรู้ในการใช้งานอย่างปลอดภัยน้อยมาก โดยจากการสำรวจการใช้งานเครือข่ายไร้สายในกรุงเทพมหานคร พบว่าองค์กรที่มีการป้องกันเครือข่ายไร้สาย โดยใช้เทคโนโลยีแบบ Wired Equivalent Provacy (WEP) มีจำนวนไม่มากนัก

8. ภัยที่มาจาก SPIM (SPAM Instant Messaging) SPIM คือ SPAM ที่ใช้ช่องทางจากระบบการส่งข้อมูลทันที หรือ IM (Instant Messaging) ในการกระจายโค้ดร้าย โดยผู้ที่เป็น SPIMMER นั้นจะใช้ บ็อท (BOT) ซึ่งเป็นโปรแกรมอัตโนมัติ สำหรับทำหน้าที่อย่างใดอย่างหนึ่งบนอินเทอร์เน็ต ซึ่งย่อมาจากคำว่า ROBOT เพื่อค้นหาชื่อของคนที่ใช้โปรแกรม IM อยู่ จากนั้น จึงใช้บ็อทแสดงคำพูดให้เหยื่อเข้าใจว่าเป็นมนุษย์ แล้วจึงส่งโฆษณา ข้อมูลหลอกลวง ลิงค์เว็บไซต์ หรือแม้แต่สปายแวร์ และมัลแวร์ต่าง ๆ ให้กับเหยื่อ

9. ภัยที่มาจากหนอนอินเทอร์เน็ตและไวรัสคอมพิวเตอร์ ถือเป็นปัญหาที่เกิดขึ้นพร้อมกับอินเทอร์เน็ตมาตลอด เป็นการเจาะระบบโดยอาศัยช่องโหว่ของระบบปฏิบัติการ เครือข่าย และแอปพลิเคชัน โดยแนวโน้มของการเกิดช่องโหว่ (Vulnerability) นั้น ก็มีเพิ่มขึ้นเรื่อย ๆ อย่างต่อเนื่อง ในปัจจุบันจะพบว่าการกระจายของหนอนอินเทอร์เน็ตจะใช้เวลาในระดับนาที แต่มีการคาดการณ์ว่าในอนาคตจะมีระดับเป็นหน่วยวินาที

10. ภัยที่มาจาก PDA Malware ข้อมูลใน พีดีเอก็มีโอกาสจะเป็นพาหะของหนอนไวรัสโทรจัน และโค้ดร้ายต่าง ๆ ได้เหมือนกับข้อมูลที่อยู่ในพีซี ผลสำรวจการใช้งานพีดีเอของนักธุรกิจในสหรัฐฯ โดยมหาวิทยาลัย Pepperdine University เมื่อปี 2547 พบว่า ครึ่งหนึ่งของจำนวนผู้ที่ถูกสำรวจ ไม่มีการใช้โปรแกรม หรือลงโปรแกรมใด ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลบนพีดีเอ ร้อยละ 81 ของผู้ที่ถูกสำรวจยังบอกด้วยว่า พวกเขาบันทึกข้อมูลที่มีคุณค่าหรือความสำคัญมากในพีดีเอ

จะเห็นได้ว่า ภัยจากอินเทอร์เน็ตนั้นมีอยู่เป็นจำนวนมากทั้งเก่าและใหม่ที่เกิดขึ้นอยู่ทุกวัน ปัญหาเก่าก็ยังไม่สามารถที่จะแก้ปัญหาได้ ปัญหาใหม่ก็เกิดขึ้นอยู่ตลอดเวลา ภัยจากอินเทอร์เน็ตเหล่านี้สามารถที่เป็นอันตรายต่อข้อมูลของผู้ใช้งาน ตั้งแต่การใช้งานในส่วนบุคคลจนไปถึงในระดับขององค์กรหรือบริษัทได้ ซึ่งจะก่อให้เกิดความเสียหายต่อการดำเนินกิจกรรมทั้งหมด ไม่ว่าจะเป็นข้อมูลที่เป็นความลับส่วนบุคคล หรือแม้แต่ข้อมูลที่สำคัญที่เป็นขององค์กร โดยเฉพาะอย่างยิ่ง ถ้าเกิดขึ้นกับองค์กรหรือบริษัทแล้ว ความเสียหายอาจจะไม่สามารถประเมินค่าได้ โดยจะสามารถส่งผลต่อการดำเนินงานของโซ่อุปทานต่อไปได้ เทคโนโลยีที่เปลี่ยนแปลงย่อมส่งผลดีต่อการดำเนินงานให้มีความสะดวกสบายและง่ายต่อการปฏิบัติการ แต่ก็อาจจะส่งผลเสียได้หากใช้อย่างไม่ระมัดระวัง ดังที่ได้กล่าวไว้ในเบื้องต้นถึงภัยอันตรายที่เกิดขึ้นจากการใช้อินเทอร์เน็ตที่สามารถที่จะส่งผลต่อการปฏิบัติงานในโซ่อุปทาน ประกอบกับเทคโนโลยีที่ก้าวหน้าไปอยู่ตลอดเวลา สังคมโลกกำลังก้าวสู่สังคมของอินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Thing : IoT) ดังนั้น ในการเดินไปพร้อมกับเทคโนโลยีที่พัฒนาไปอย่างต่อเนื่องนั้น ประเด็นของภัยคุกคามอันจะเกิดขึ้นกับสิ่งเหล่านี้จึงต้องได้พิจารณาไปพร้อมๆ กันเพื่อเตรียมรับมือกับสิ่งที่จะเกิดขึ้นต่อไป

2.2.1 ภัยคุกคามทางไซเบอร์

แนวโน้มการใช้งานอินเทอร์เน็ตนับวันยิ่งเพิ่มมากขึ้น เราจะปฏิเสธไม่ได้ว่าเครือข่ายอินเทอร์เน็ตในปัจจุบัน มีผลต่อการใช้ชีวิตของคนไทยและทั่วโลก ไม่ว่าจะใช้เพื่อความบันเทิงหรือความสะดวกสบายส่วนตัว หรือแม้แต่กระทั่งใช้ในการดำเนินธุรกิจ ยิ่งในภาคธุรกิจนั้นอินเทอร์เน็ตนับวันยิ่งมีความจำเป็นต่อการดำเนินกิจกรรมต่าง ๆ เป็นอย่างมาก จากเดิมที่เป็นเพียงแค่การทำงานผ่านเครื่องคอมพิวเตอร์ แต่ปัจจุบันก็มีอุปกรณ์ต่าง ๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้เพิ่มขึ้นมามากอย่างมากมายทั้ง โน้ตบุ๊ค มือถือ อุปกรณ์พกพาต่าง ๆ ดังนั้นแล้วผลลัพธ์ที่ตามมาสำหรับการใช้เทคโนโลยีการสื่อสารที่ทันสมัยเหล่านี้ สิ่งที่หลีกหนีไม่ได้ก็คือเรื่องของภัยคุกคามทางไซเบอร์ (Cyber Threats) (Borrett Martin et al., 2013; Galligan Mary E., 2014)

ภัยคุกคาม (Threats) หมายถึงสิ่งต่าง ๆ ที่เมื่อเกิดขึ้นแล้ว จะส่งผลให้เกิดต่อความเสียหายต่อธุรกิจ ที่ซึ่งสามารถแบ่งออกไปได้เป็นภัยคุกคามจากภายนอก (External Threats) กับภัยคุกคามภายใน (Internal Threats) โดยที่ภัยคุกคามที่เกิดขึ้นภายในองค์กร ตัวอย่างเช่น ความไม่พอใจที่เกิดขึ้นจริงหรือที่รู้สึกได้ที่เกิดมาจากพนักงาน ผู้รับจ้างเหมา หรือแม้แต่จากหุ้นส่วนทั้งหมดของธุรกิจ หรือจากการรักษาความปลอดภัยที่บกพร่องของพนักงาน ส่วนภัยคุกคามจากภายนอกนั้น ก็อาจจะมาจากการโจรกรรม การลักลอบขนสินค้า การก่อการร้าย ภัยจากคู่แข่ง ผู้ที่ไม่หวังดีหรือผู้ที่ชอบก่อนความเดือดร้อนให้ผู้อื่น ส่วนจุดอ่อน (Vulnerability) หมายถึงช่องว่างหรือจุดบกพร่องในกลไกที่มีอยู่ในปัจจุบัน ซึ่งเมื่อเจอภัยคุกคามก็จะทำให้เกิดความเสี่ยงขึ้นในองค์กร

และเมื่อความเสี่ยงนั้นเกิดขึ้นก็จะส่งผลให้เกิดความเสียหรือผลกระทบกับการดำเนินงานขององค์กรได้ ซึ่งความเสียหายสามารถแบ่งออกได้เป็น 2 ลักษณะ ได้แก่ ความเสียหายที่จับต้องได้ (Tangible) เช่น ทรัพย์สิน ผลิตภัณฑ์ โครงสร้างพื้นฐาน หรือบุคลากร และความเสียหายที่จับต้องไม่ได้ (Intangible) เช่น ชื่อเสียง ความนิยม ตำแหน่งทางการตลาด

ด้วยเหตุนี้แนวโน้มของภัยคุกคามด้านความมั่นคงได้มีการเปลี่ยนแปลงอย่างชัดเจนมากขึ้น โดยฝ่ายตรงข้ามหรือผู้ก่อการร้ายจะทำการโจมตีจุดสำคัญที่เป็นหัวใจของธุรกิจได้ด้วยการผ่านระบบเครือข่ายโทรคมนาคมและคอมพิวเตอร์ หรือที่เรียกว่า การโจมตีทางไซเบอร์ (Cyber Attack) (Warren Matthew et al., 2000; Zobel Christopher, 2013) แน่นอนว่าภัยคุกคามดังที่ได้กล่าวนี้จะเป็นภัยคุกคามที่มีผลกระทบต่อธุรกิจ รวมไปถึงเศรษฐกิจในระดับนานาชาติ โดยที่ภัยคุกคามดังกล่าวจะแฝงตัวมากับการเติบโตขึ้นทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร จากการที่ในปัจจุบันนี้ได้มีการพัฒนาเครือข่ายอินเทอร์เน็ตไปอย่างมาก สามารถที่จะเชื่อมต่อกันด้วยระบบเครือข่ายใยแก้วนำแสง การเชื่อมต่อแบบไร้สาย หรือแม้แต่ระบบสื่อสารดาวเทียม จนทำให้โลกถูกเชื่อมต่อกันโดยสมบูรณ์และสามารถส่งข้อมูลด้วยความเร็วเท่าแสง และยังมีแนวโน้มที่จะเพิ่มการเชื่อมโยงให้มากขึ้น และสิ่งที่เป็นปัญหาที่สามารถทำให้อาชญากรทางไซเบอร์สามารถที่จะเข้ามาทำการโจรกรรมข้อมูลภายในบริษัทซึ่งเป็นข้อมูลที่เป็นความลับได้นั้น ส่วนหนึ่งก็จะมาจากเทคโนโลยีที่มีใช้อยู่ในท้องตลาดทั่วไปเริ่มมีขีดความสามารถเท่าเทียมกับเทคโนโลยีของหน่วยงานความมั่นคงของประเทศ จึงเป็นเหตุให้อาชญากรทางไซเบอร์มีทางเลือกในการปฏิบัติมากขึ้นและซับซ้อนขึ้น ซึ่งเป็นการยากที่จะตรวจจับได้ และเป็นที่น่าตกใจอย่างยิ่งที่เครื่องมือและคู่มือในการเจาะระบบสารสนเทศสามารถพบเห็นได้ทั่วไปในอินเทอร์เน็ต โดยการสืบค้นจาก Google จนทำให้ทุกวันนี้เด็กอายุเพียง 10 ขวบ สามารถเจาะระบบของธนาคารทั่วโลกได้ เพื่อขโมยหรือลบข้อมูลสำคัญของธนาคาร (เศรษฐพงค์ มะลิสุวรรณ, 2010)

ภัยคุกคามทางไซเบอร์ (Cyber Threats) เป็นเรื่องที่บริษัทหรือหน่วยงานต่าง ๆ ทั้งที่เป็นของรัฐและเอกชนกำลังเผชิญอยู่ ภัยคุกคามทางไซเบอร์เป็นสิ่งที่เกิดขึ้นเพื่อสร้างความเสียหายให้กับระบบคอมพิวเตอร์ที่เกิดขึ้นในปัจจุบัน ระบบคอมพิวเตอร์ดังกล่าวก็คือเครื่องมือที่ใช้ในการทำงานที่ได้กลายเป็นสิ่งจำเป็นสำหรับบริษัทต่าง ๆ ในปัจจุบันนี้ เครื่องมือที่นำมาใช้ในการทำงานก็ได้แก่ เครื่องคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา มือถือ สมาร์ตโฟนต่าง ๆ รวมไปถึงอุปกรณ์แทบเล็ต ซึ่งเป็นสิ่งที่นำมาใช้งานเพื่อทำให้เกิดธุรกรรมต่าง ๆ ในโซ่อุปทาน เพื่อการแข่งขันแทบทั้งสิ้น ดังนั้นจากการที่บริษัทต่าง ๆ ได้นำเอามีอุปกรณ์มากมาย มาใช้เพื่อการทำงานย่อมเท่ากับว่าเป็นการเพิ่มช่องทางให้กับผู้ที่ไม่หวังดีต่อบริษัท อันจะทำให้เป็นเป้าหมายในการสร้างความเสียหายให้เกิดขึ้นกับบริษัท รวมไปถึงเครือข่ายของโซ่อุปทานในที่สุด จุดมุ่งหมายของ

อาชญากรทางไซเบอร์ส่วนใหญ่มุ่งไปใน 3 ลักษณะคือ 1) การนำความลับไปเปิดเผย (Data Confidentiality) 2) การเปลี่ยนแปลงข้อมูล (Data Integrity) และ 3) การทำให้ระบบหยุดบริการหรือไม่สามารถใช้งานได้ (System Availability) (เศรษฐพงค์ มะลิสุวรรณ, 2010) ซึ่งปัจจุบันจะเห็นได้ว่า ปัญหาจากภัยคุกคามด้านความปลอดภัยข้อมูลคอมพิวเตอร์ โดยเฉพาะภัยที่มาจากการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตนับวันจะทวีความรุนแรงและพัฒนารูปแบบของภัยคุกคามที่หลากหลายมากขึ้น และด้วยเหตุนี้เองจึงเป็นผลให้ภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรง และมีความซับซ้อนในการโจมตีมากขึ้นตามไปด้วย ความเสียหายที่เกิดจากการอาชญากรรมทางไซเบอร์ (Cyber Crime) และการโจมตีทางไซเบอร์ (Cyber Attack) จะมีผลต่อธุรกิจอย่างร้ายแรง ซึ่งในทุกองค์กรทั้งภาครัฐและภาคเอกชนจะต้องตระหนักและต้องมีการกำหนดมาตรการในการป้องกันต่อภัยคุกคามทางไซเบอร์ดังกล่าว แม้ว่าในบางองค์กรนั้นอาจจะยังไม่เคยถูกโจมตีทางไซเบอร์มาก่อนก็ตาม แต่ในองค์กรส่วนใหญ่ล้วนให้ความสำคัญกับการป้องกันภัยคุกคามทางไซเบอร์ โดยมีการวางแนวทางป้องกันภัยคุกคามทางไซเบอร์ มีการปรับเปลี่ยนมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ ให้สอดรับกับการเปลี่ยนแปลงยุทธศาสตร์และการดำเนินการทางธุรกิจ และเพื่อให้สอดคล้องกับการเปลี่ยนแปลงทางสภาพแวดล้อมภายนอกของธุรกิจซึ่งผู้บริหารต้องมองลักษณะของภัยคุกคามทางไซเบอร์ให้รอบด้าน

ภัยคุกคามทางไซเบอร์รวมไปถึงอาชญากรรมไซเบอร์เริ่มเห็นชัดขึ้นในทุก ๆ วินาที ด้วยเหตุผลนี้เทคโนโลยีสารสนเทศและการสื่อสาร (ICT) จึงได้ถูกพัฒนาขึ้นเพื่อช่วยเหลือผู้จัดการในโซ่อุปทานอันประกอบไปด้วยเครื่องมือและบริการต่าง ๆ เพื่อที่จะได้นำมาใช้สำหรับการตรวจสอบการหยุดชะงัก ในอันที่จะทำการสนับสนุนการสื่อสารในทันที นอกจากนั้นเทคโนโลยีสารสนเทศและการสื่อสารยังจะมีเพื่อใช้สำหรับการอำนวยความสะดวกในการฟื้นตัวอย่างรวดเร็วของโซ่อุปทาน ดังนั้นแล้วผลจากการเพิ่มขึ้นของการนำเอาระบบเทคโนโลยีสารสนเทศมาใช้นี้ จึงเป็นผลให้นำมาสู่ความเสี่ยงทางที่เพิ่มมากขึ้นต่อองค์กรหรือบริษัท อันเป็นผลที่ทำให้เกิดความอ่อนแอในโซ่อุปทานขึ้นมากได้ ความเสี่ยงดังกล่าวนั้นก็คือความเสี่ยงทางไซเบอร์ (Cyber Risks) และจากรายงานการโจมตีทางไซเบอร์ที่เพิ่มมากขึ้นอันเป็นผลทำให้การดำเนินงานของบริษัทต่าง ๆ ในโซ่อุปทานต้องเกิดความเสียหายนั้น โดยในรายงานได้ เผยให้เห็นถึงจุดอ่อนของโซ่อุปทานอันจะทำให้แฮ็กเกอร์ (Hackers) สามารถที่เข้ามาโจมตีได้ ซึ่งจุดอ่อนในโซ่อุปทานที่ว่านั้นก็เป็นจุดอ่อนที่อาจจะเกิดมาจากความซับซ้อนในห่วงโซ่ที่มีมากขึ้น และจะต้องเป็นส่วนของข้อมูลที่สามารถมองเห็นได้ โดยจุดที่ง่ายสำหรับแฮ็กเกอร์ที่จะเข้ามาโจมตีได้นั้นก็จะเกิดจากการดำเนินงานภายในโซ่อุปทานที่จะต้องมีการใช้ข้อมูลร่วมกัน (Information Sharing) โดยแทบจะเรียกได้ว่า จะมีการแบ่งปันหรือแชร์ (Share) ข้อมูลระหว่างกันในทุก ๆ นาทีเลยทีเดียว

ด้วยเหตุนี้จึงได้กลายมาเป็นเป้าหมายที่ง่ายต่อการโจมตีและมีค่าจากการโจมตีสำหรับอาชญากรทางไซเบอร์ (Cyber Crime) ที่ต้องการความท้าทาย ซึ่งความเสียหายที่เกิดขึ้นก็จะเกิดขึ้นอย่างมากมาย เช่น เกิดความสูญเสียทางการเงิน ความเสียหายที่จะเกิดขึ้นกับชื่อเสียงของแบรนด์และความคุ้มค่าของบริษัท

ผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยและนักวิเคราะห์ต่างเห็นตรงกันว่าปัญหาดังกล่าวที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ที่เกิดขึ้นกับองค์กร เพิ่งจะเป็นเพียงการเริ่มต้นเท่านั้น การจู่โจมที่เกิดขึ้นจะมีทั้งจำนวนและความซับซ้อนที่เพิ่มขึ้นตามเทคโนโลยีที่เปลี่ยนแปลงไป ซึ่งก็ผลทำให้ระบบโซ่อุปทานตกอยู่ในสถานะที่สามารถจะถูกโจมตีได้ตลอดเวลา จากข้อมูลของ Gartner Group ในบทความเรื่อง Hype Cycle for Information Security (2004) แสดงให้เห็นว่าปัญหาด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ยังเป็นประเด็นสำคัญที่องค์กรต่าง ๆ ยังคงต้องให้ความสนใจและจัดการอย่างเป็นระบบ ในขณะที่เทคโนโลยีและบริการที่องค์กรใช้ในการแก้ปัญหาเรื่องดังกล่าวบางเทคโนโลยีล้าสมัยไปแล้ว โดยในปัจจุบันนี้ก็ได้มีเทคโนโลยีใหม่ ๆ เข้ามาแทนที่ ดังนั้นผู้บริหารองค์กรควรมีกลยุทธ์ในการบริหารจัดการเทคโนโลยีสารสนเทศที่ดีและเตรียมพร้อมกับสถานการณ์ปัจจุบัน และอนาคต นอกจากนี้ จากผลการวิจัยของกลุ่ม Gartner Group ในปี 2005 (http://www.gartner.com/DisplayDocument?doc_cd=128160) พบว่าบริษัทระดับสากลทั่วโลกมากกว่า 20% ประสบกับปัญหาเกี่ยวกับภัยคุกคามทางอินเทอร์เน็ตและสร้างความเสียหายให้เกิดกับระบบมาแล้วทั้งนั้น และแน่นอนค่าความสูญเสียที่สามารถนำมาประเมินเป็นตัวเลขได้นั้นมีมูลค่าสูงกว่าครึ่งหนึ่งของค่าใช้จ่ายทั้งหมดที่ใช้ในการป้องกันภัยคุกคาม

2.2.2 ความมั่นคงปลอดภัยไซเบอร์

ในยุคที่ประเทศไทยกำลังขับเคลื่อนธุรกิจของประเทศภายใต้นโยบายเศรษฐกิจดิจิทัล (Digital Economy) ซึ่งเป็นเรื่องที่เต็มไปด้วยการสื่อสารของข้อมูล มีการเชื่อมต่อโดยใช้อินเทอร์เน็ตเป็นสื่อกลางโดยอาศัยเทคโนโลยีที่มีความเจริญก้าวหน้าไปในทุกวินาที เมื่อได้มีการนำเอาเทคโนโลยีมาใช้ ทุกอย่างดูเหมือนว่าจะสะดวกสบายทั้งในเรื่องส่วนตัวและเรื่องของการดำเนินกิจกรรมทางธุรกิจ แต่ในความสะดวกสบายนั้นต้องยอมรับว่าประเด็นของภัยคุกคามต่าง ๆ บนอินเทอร์เน็ตดังที่ได้กล่าวไว้แล้วข้างต้นคือเรื่องที่มิอาจมองข้ามไปได้ โดยเฉพาะอย่างยิ่งเมื่อเทคโนโลยีก้าวหน้าไปเท่าใด ภัยคุกคามเหล่านี้ก็พัฒนาตัวเองให้ก้าวตามไปเช่นเดียวกัน ทำให้มีภัยคุกคามใหม่ ๆ เกิดขึ้นอยู่ตลอดเวลา และผู้บริโภคที่ใช้งานเทคโนโลยีก็มีอยู่ไม่น้อยที่ตกเป็นเหยื่อภัยคุกคามเหล่านี้ ทั้งที่ขาดความรู้ความเข้าใจและบางรายก็เกิดจากความประมาท ดังนั้นหนทางที่ดีที่สุดในการป้องกันภัยคุกคามเหล่านี้ คือการสร้างหาวิธีการในการป้องกันให้กับผู้บริโภคในเรื่องของภัยคุกคาม นั่นคือเรื่องของความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

ความมั่นคงปลอดภัยไซเบอร์ คือ การป้องกันอันตรายทางไซเบอร์ที่มีอยู่ในโลกออนไลน์ ที่มีผลกระทบต่อตัวผู้ใช้งานและทรัพย์สิน (ข้อมูล) ซึ่งในปัจจุบันมีผู้ใช้งานออนไลน์ทั่วโลกเพิ่มมากขึ้น ทั้งนี้เนื่องมาจากปัจจัยหลายๆ ด้าน ไม่ว่าเป็นอัตราค่าบริการที่ถูกลง หรือการเพิ่มขึ้นของอุปกรณ์พกพาต่างๆ เช่น สมาร์ตโฟน และเครื่องคอมพิวเตอร์แบบพกพา ความจำเป็นในเรื่องของความมั่นคงปลอดภัยไซเบอร์นั้นได้เกิดมาจากการพัฒนาระบบเทคโนโลยีการสื่อสารโทรคมนาคม ไม่ว่าจะเป็นการเชื่อมต่อด้วยสายไฟเบอร์ออพติก (Fibre Optics) ระบบเครือข่ายใยแก้วนำแสง หรือระบบสื่อสารดาวเทียม (Collier, Z. A. et al., 2014; Nagurney A. et al., 2015; Atoum, I. et al., 2014) โดยเฉพาะอย่างยิ่งเทคโนโลยีสื่อสารไร้สาย ที่ไม่มีใครปฏิเสธได้ว่าเทคโนโลยีที่เกี่ยวข้องกับโทรศัพท์เคลื่อนที่นั้นกำลังเข้ามามีส่วนในการเปลี่ยนแปลงวิถีชีวิตของคนทั้งโลก ซึ่งสามารถที่จะก่อให้เกิดพลังอำนาจด้านข้อมูลข่าวสารให้แก่ผู้บริโภคในทุกด้าน ก่อให้เกิดการเปลี่ยนแปลงทางด้านสังคมและวัฒนธรรม อีกทั้งยังเป็นตัวผลักดันทำให้เกิดนวัตกรรมทางเทคโนโลยีและธุรกิจตามมาอย่างมากมาย เช่นเทคโนโลยีซอฟต์แวร์ สำหรับอุปกรณ์สื่อสารเคลื่อนที่ (Embedded Software for Mobile Wireless Devices) เทคโนโลยีเชิงพาณิชย์อีเล็กทรอนิกส์เคลื่อนที่ (Mobile Commerce หรือ M-Commerce) เทคโนโลยีสารสนเทศเคลื่อนที่ (Mobile ICT) และอื่น ๆ จนเกิดผลกระทบอย่างมากในยุคเศรษฐกิจดิจิทัล สิ่งนี้เองทำให้เกิดการเปลี่ยนแปลงไปในสภาวะเศรษฐกิจของประเทศและของโลกอย่างก้าวกระโดด ซึ่งจากเดิมที่โลกของเราเคยแยกกันอยู่มาก่อน กลับถูกทำให้เชื่อมต่อกันได้ด้วยความก้าวหน้าทางเทคโนโลยี

ในมิติความมั่นคงของชาติก็เกิดผลกระทบอย่างรุนแรงทั่วโลก เนื่องจากเทคโนโลยีสื่อสารโทรคมนาคม ได้เพิ่มพลังอำนาจให้แก่ผู้ไม่หวังดีต่อ ทั้งประเทศชาติและต่อโลกได้เช่นเดียวกัน และยิ่งแอปพลิเคชันและซอฟต์แวร์ต่าง ๆ ได้ถูกพัฒนาจนมีความชาญฉลาดและมีประสิทธิภาพสูงมากขึ้นเท่าใด เทคโนโลยีสารสนเทศที่มีใช้อยู่ในท้องตลาดโดยทั่ว ๆ ไปก็ยิ่งมีขีดความสามารถเท่าเทียมกับเทคโนโลยีของหน่วยงานความมั่นคงของรัฐมากขึ้นเท่านั้น เนื่องจากผู้ใช้สามารถการเข้าถึงข้อมูลได้สะดวกและง่ายยิ่งขึ้น จนทำให้ผู้ที่คิดจะทำการก่อการร้ายมีทางเลือกในการปฏิบัติมากขึ้นและซับซ้อนขึ้นยากแก่การตรวจจับ ประกอบกับการโจมตีที่สามารถทำได้จากที่ใดก็ได้ในโลกโดยผ่านระบบไซเบอร์สเปซ (Cyberspace) ดังนั้นการโจมตีทางไซเบอร์นี้จึงเป็นภัยคุกคามในทุกระดับ ตั้งแต่ระดับบุคคล กลุ่มบุคคล องค์กรภาคเอกชน องค์กรภาครัฐ และระดับประเทศ ในปัจจุบันคำว่า “ความมั่นคงปลอดภัยไซเบอร์” ได้ถูกกล่าวอย่างกว้างขวางจนถึงระดับนานาชาติ ที่หลาย ๆ ประเทศให้ความสำคัญมากขึ้น โดยในหลายประเทศได้มีการเสนอให้เป็นนโยบายระดับชาติ เนื่องจากได้มีอาชญากรรมทางไซเบอร์เกิดขึ้นซึ่งได้สร้างความเสียหายให้แก่ตัวบุคคล องค์กร บริษัท รวมทั้งประเทศชาติเป็นอย่างมาก

ในอดีตเมื่อยี่สิบกว่าปีก่อน การให้บริการสื่อสารโทรคมนาคมนั้นยังอยู่ในวงแคบ เนื่องจากมีค่าบริการที่สูง อีกทั้งการให้บริการก็มีเพียงสื่อสารด้วยเสียงเท่านั้น ต่อมาการวิจัยและพัฒนาทางด้านเทคโนโลยีโทรศัพท์และคอมพิวเตอร์ได้มีการพัฒนาควบคู่กันไปอย่างรวดเร็ว โดยโทรศัพท์ได้พัฒนาสู่การเคลื่อนที่และมีขนาดเล็กสามารถพกพาได้ ส่วนคอมพิวเตอร์ก็มีการพัฒนาจนสามารถเชื่อมโยงเป็นเครือข่ายได้ อีกทั้งซอฟต์แวร์คอมพิวเตอร์ก็ได้ถูกพัฒนาให้มีความชาญฉลาดและใช้งานง่าย การพัฒนาเครือข่ายคอมพิวเตอร์ที่เรียกว่า “อินเทอร์เน็ต (Internet)” ได้เป็นไปอย่างรวดเร็ว ในเวลาต่อมาหลังจากเทคโนโลยี 2G บนมาตรฐาน GSM ได้พัฒนาและได้รับการยอมรับจนถึงขีดสุด เทคโนโลยี 3G ก็ได้ถูกพัฒนาอย่างต่อเนื่อง จนเปิดให้บริการและได้รับความนิยมแพร่หลายทั่วโลก ซึ่งถือเป็นจุดเปลี่ยนที่สำคัญของโทรศัพท์เคลื่อนที่ที่ใช้เทคโนโลยี 3G เป็นเทคโนโลยีหลักที่ทำให้เกิดการหลอมรวมทางวัฒนธรรมและเทคโนโลยี (Technology Convergence) อย่างรวดเร็วในขณะที่เทคโนโลยีสารสนเทศและการสื่อสารโดยเฉพาะอย่างยิ่งการสื่อสารข้อมูลผ่านอินเทอร์เน็ตที่เป็นเครื่องมือสำคัญในการขับเคลื่อนเศรษฐกิจทุกประเทศทั่วโลก จนได้พัฒนาต่อเนื่องมาจนในปัจจุบันที่เป็นเทคโนโลยี 4G เป็นยุคของเครือข่ายความเร็วสูงสุดชนิดพิเศษ สามารถใช้งานได้แบบไร้สาย รวมถึงคุณสมบัติการเชื่อมต่อเสมือนจริงในรูปแบบสามมิติ (Three-dimensional) ระหว่างผู้โทรออกและผู้รับสาย ความโดดเด่นของ 4G คือถูกออกแบบมาเพื่อการใช้งานบนเครือข่ายที่กินพื้นที่กว้างก็ได้หรือจะทาเป็นเครือข่ายขนาดย่อม ๆ แบบ WLAN ได้อีกด้วย นั่นจึงทาให้หลายคนมองว่า 4G จะมาเบียดเทคโนโลยีของ Wi-Fi หรือไม่ เพราะสามารถใช้งานได้ทั้งสองแบบ แต่มีต้นทุนการผลิตที่สูงมาก ประเทศไทยจึงยังไม่มีให้เห็น (ศุภศิลป์ กุลจิตต์เจือวงศ์, 2012) และจากความก้าวหน้าทางเทคโนโลยีด้านการสื่อสารนี้เอง โดยรายงานของ World Economic Forum (2014) พบว่าทุกประเทศทั่วโลกกำลังประสบปัญหากับอาชญากรรมและภัยคุกคามทางไซเบอร์เป็นอย่างมาก โดยภัยคุกคามทางไซเบอร์ถูกจัดให้อยู่ในอันดับที่ 4 ใน 10 ของโลกที่ทุกประเทศจะต้องพบเจอ

หลายคนมองว่าเรื่องการคุกคามทางโลกไซเบอร์เป็นเรื่องไกลตัว แต่จากสถิติพบว่าในปี 2013 มีเหยื่ออาชญากรรมไซเบอร์เกิดขึ้นจำนวน 378 ล้านรายทั่วโลก ซึ่งมากกว่า 1 ล้านรายต่อวัน หรือหากเทียบเป็นวินาทีมีเหยื่อเกิดขึ้น 12 รายต่อวินาที และก่อความเสียหายคิดเป็นมูลค่ากว่า 113 พันล้านเหรียญสหรัฐ ไม่เว้นแม้แต่ประเทศไทย ผู้ใช้บริการอินเทอร์เน็ตในประเทศไทย เพิ่มจำนวนขึ้นอย่างรวดเร็ว ในช่วง 10 ปีที่ผ่านมา จากจำนวนผู้ใช้บริการเพียง 6 ล้านรายในปี 2003 เพิ่มเป็น 26 ล้านรายในปี 2013 หรือเพิ่มขึ้นร้อยละ 16 ต่อปีและมีแนวโน้มเพิ่มมากขึ้น และจากผลสำรวจพฤติกรรมการใช้งานอินเทอร์เน็ตของคนไทยพบว่าร้อยละ 39 มีการใช้งานอินเทอร์เน็ตมากกว่า 20 ชั่วโมงต่อสัปดาห์ อย่างไรก็ตามในปัจจุบันอุปกรณ์อิเล็กทรอนิกส์ประเภท

สมาร์ตโฟนและแท็บเล็ต กลายเป็นอุปกรณ์ที่ได้รับความนิยมกันอย่างแพร่หลายเนื่องจากราคาเครื่องลดลงจนคนส่วนมากเข้าถึงได้ และกลายเป็นช่องทางในการเชื่อมต่อในโลกอินเทอร์เน็ต ประกอบกับการเข้าถึงข้อมูลที่เชื่อมต่อบนโลกอินเทอร์เน็ตสามารถทำได้ทุกที่ ทุกเวลา เมื่ออินเทอร์เน็ตมีอิทธิพลต่อชีวิตประจำวันมากขึ้น ก็พบว่ามีเหยื่อจากการใช้อินเทอร์เน็ตมากขึ้นทุกวัน ๆ เช่นเดียวกัน เพราะอาชญากรทางไซเบอร์มักอาศัยความง่ายในการเข้าถึงอินเทอร์เน็ตนี้เข้ามาหาผลประโยชน์จากผู้ใช้งานที่ไม่มีความระมัดระวัง และไม่ตระหนักรู้ถึงความสำคัญในเรื่องความปลอดภัยบนโลกไซเบอร์ ดังนั้นความมั่นคงปลอดภัยไซเบอร์จึงเป็นประเด็นที่สำคัญ ซึ่งทุกภาคส่วนไม่ควรเพิกเฉย

ในปัจจุบันกระแสความนิยมการใช้สังคมออนไลน์ (Social Network) อย่างเช่น Facebook, Instagram, Line, WhatsApp และ Twitter บนสมาร์ตโฟนมีมากขึ้น มีการแชร์ภาพและข้อมูลผ่านสังคมออนไลน์ การดาวน์โหลดและติดตั้งแอปพลิเคชันบนโทรศัพท์เคลื่อนที่ การใช้ Cloud และ Dropbox ในการจัดเก็บข้อมูล หรือการรับส่งอีเมล์ ซึ่งการใช้งานดังกล่าวแม้ว่าจะมีการเข้ารหัสผ่านเพื่อความปลอดภัยในการใช้งาน แน่นอนว่าภายใต้การรักษาความปลอดภัยดังกล่าวนั้นอาจมีช่องโหว่ด้านความปลอดภัยที่อาจถูกอาชญากรทางไซเบอร์ใช้เป็นช่องทางเพื่อเข้ามาโจมตี ได้เช่นกัน ซึ่งอาจมาในรูปแบบของ Phishing Malware Identity Theft ตามที่ได้อธิบายไปแล้วนั้น ผลที่ได้รับนั่นคือผู้ใช้อาจโดนขโมยข้อมูลส่วนตัวไปอย่างไม่ทันรู้ตัวและยากที่จะทำการตรวจสอบ เพราะยิ่งเทคโนโลยีมีความก้าวหน้าอย่างรวดเร็วก็ยิ่งมีนักพัฒนาซอฟต์แวร์ให้มีความชาญฉลาดจนสามารถนำมาเป็นเครื่องมือโจมตีในโลกไซเบอร์ได้เช่นกัน

นอกจากนโยบายการป้องกันการโจมตีทางไซเบอร์ของภาครัฐแล้ว ในองค์กรธุรกิจต่าง ๆ ก็ควรจะต้องมีการตระหนักถึงภัยคุกคามด้านนี้ โดยมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทั้งทางด้านแอปพลิเคชั่นที่ใช้ในองค์กร ความปลอดภัยของเครือข่ายและความปลอดภัยของข้อมูล อีกทั้งควรมีการจัดการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ที่สามารถเกิดขึ้นได้ทุกขณะและมีรูปแบบที่แปรเปลี่ยนไปอยู่ตลอดเวลา และที่สำคัญผู้ใช้งานแต่ละบุคคลควรจะต้องมีความตระหนักรู้และคำนึงถึงภัยคุกคามทางไซเบอร์นี้ว่าไม่ใช่เรื่องไกลตัวอีกต่อไป อย่างไรก็ตาม ในยุคที่มีการหลอมรวมทางเทคโนโลยี ก่อให้เกิดการสื่อสารแบบไร้ขีดจำกัด รวมทั้งเครือข่ายอินเทอร์เน็ตที่สามารถเชื่อมโยงกันได้ทั่วโลกด้วยอุปกรณ์สื่อสารไร้สายขนาดเล็ก ทำให้เกิดความร่วมมือกันระหว่างประเทศในการสร้างคุณค่าทางเศรษฐกิจ และต้องเผชิญกับภัยในโลกไซเบอร์ที่คุกคามความมั่นคงของชาติรูปแบบใหม่ที่เหนือความคาดหมายร่วมกันอย่างหลีกเลี่ยงไม่ได้ “ภัยคุกคามที่เกิดจากโลกไซเบอร์” ใกล้ตัวเรามากกว่าที่คิด ดังนั้นจึงควรมีการป้องกันโดยเริ่มจากในระดับบุคคล ระดับองค์กร และในระดับประเทศชาติต่อไป

แนวทางการกำกับดูแลอุตสาหกรรมโทรคมนาคม ที่คณะกรรมการกิจกรรมโทรคมนาคมแห่งชาติ ได้เผยแผนการดำเนินงาน (Roadmap) ออกมานั้น จากปี 2558 ที่ผ่านมามีการยกระดับความเข้มข้นเรื่องการคุ้มครองผู้บริโภคในบริการโทรคมนาคมขึ้น ทั้งนี้การให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ก็จัดเป็นการคุ้มครองผู้บริโภคในเชิงรุก โดยอาศัยการให้ข้อมูลแก่ผู้บริโภค หากผู้บริโภคมีความรู้ความเข้าใจในความมั่นคงปลอดภัยไซเบอร์มากขึ้น ก็จะทำให้สามารถใช้บริการโทรคมนาคมผ่านเทคโนโลยีต่าง ๆ บนอินเทอร์เน็ตได้อย่างสะดวกและปลอดภัยมากขึ้น ตรงตามเจตนารมณ์ของคณะกรรมการกิจการโทรคมนาคมแห่งชาติ ที่ต้องการจะยกระดับความเข้มข้นเรื่องการคุ้มครองผู้บริโภคในบริการโทคมนาคมทั้งด้านคุณภาพและราคา

2.2.3 การจัดการภัยคุกคามทางไซเบอร์

รายงานแนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ สำหรับปี 2016 (Threat Horizon 2016 – On The Edge of Trust, 2016) โดยสถาบัน Information Security Forum (ISF) โดยในรายงานได้แสดงถึงทิศทางเชิงลบทางด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ยังคงมีอยู่อย่างต่อเนื่อง ซึ่งเป็นสิ่งที่กระทบต่อความน่าเชื่อถือที่องค์กรต่างๆ จะต้องรักษาไว้ให้ได้ ในรายงานได้ข้อสรุปหลักๆทั้งหมด 3 ประเด็น และ 10 องค์ประกอบ ดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 รายงานแนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ สำหรับปี 2016

ประเด็น	**องค์ประกอบ**	
ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป	1	การจารกรรมทางไซเบอร์โดยภาครัฐ จะกลายเป็นกระแสหลัก
	2	การควบคุมอินเทอร์เน็ตภายในประเทศหรือภูมิภาคจะสร้างความยุ่งยากต่อธุรกิจ
	3	ผลสืบเนื่องที่ไม่พึงประสงค์จากการแทรกแซงของภาครัฐ
ความเชื่อมั่นในระบบหรือโซลูชันการรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่	4	ผู้ให้บริการ จะกลายเป็นช่องโหว่สำคัญ
	5	ข้อมูลขนาดใหญ่จะกลายเป็นปัญหาใหญ่
	6	แอพพลิเคชั่นมือถือ จะกลายเป็นช่องทางหลักที่ถูกเจาะข้อมูล
	7	การเข้ารหัสข้อมูลไม่เกิดผล

ตารางที่ 2.1 (ต่อ)

ประเด็น	องค์ประกอบ	
ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยไซเบอร์	8	CEO รับรู้ถึงปัญหาเรื่องความมั่นคงปลอดภัยทางไซเบอร์ถึงเวลาที่ต้องลงมือปฏิบัติให้เกิดผลงานส่งมอบที่ได้ผลจริง
	9	ความแตกต่างด้านทักษะ จะมีช่องว่างห่างมากขึ้น
	10	ความมั่นคงปลอดภัยสารสนเทศ จะไม่สามารถใช้ได้กับคนรุ่นใหม่

ที่มา : The Information Security Forum, ISF Threat Horizon 2016 Executive Summary

รายละเอียดในประเด็นทั้ง 3 จะประกอบไปด้วย

1. ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป หมายถึง การจารกรรมทางไซเบอร์ที่สนับสนุนโดยหน่วยงานภาครัฐจะกลายเป็นกระแสหลัก การควบคุมอินเทอร์เน็ตภายในประเทศหรือภูมิภาคจะสร้างความยุ่งยากต่อธุรกิจ โดยจะส่งผลสืบเนื่องที่ไม่พึงประสงค์จากการแทรกแซงของภาครัฐ โดยองค์กรต่าง ๆ จะต้องให้ความสำคัญในประเด็นต่าง ๆ ดังต่อไปนี้

1.1 การจารกรรมทางไซเบอร์โดยภาครัฐ จะกลายเป็นกระแสหลักการจารกรรมทางไซเบอร์โดยภาครัฐที่แต่เดิมส่วนใหญ่จะกระทำแบบปกปิดหรือซ่อนเร้น จะมีการเปิดเผยหรือเปิดโปงมากขึ้น ซึ่งจะทำให้ประเทศต่าง ๆ เข้ามาร่วมวงกันมากขึ้น ผลก็คือ ทำให้เกิดสภาพแวดล้อมในโลกไซเบอร์ที่จะปกครองได้ยากขึ้น

1.2 การควบคุมอินเทอร์เน็ตภายในประเทศหรือภูมิภาคจะสร้างความยุ่งยากต่อธุรกิจ รัฐบาลในหลายประเทศจะมีแนวคิดในการพยายามควบคุม ภูมิรัฐศาสตร์ทางอินเทอร์เน็ตโดยมีการควบคุมหรือกำกับดูแลการใช้งานอินเทอร์เน็ตภายในประเทศ หรืออาจจะเป็นการร่วมมือเฉพาะภายในกลุ่มประเทศหรือภูมิภาค ทั้งเป็นการปกป้องภายในจากภายนอก และการป้องกันภายนอกที่จะรุกล้ำโจมตีจากภายใน

1.3 ผลสืบเนื่องที่ไม่พึงประสงค์จากการแทรกแซงของภาครัฐ องค์กรที่ไม่สามารถปฏิบัติตามกฎระเบียบของภาครัฐ อาจจะถูกแทรกแซงโดยหน่วยงานกำกับดูแลของภาครัฐซึ่งจะทำหน้าที่ตำรวจไซเบอร์ ผู้ตรวจการณ์หรือผู้รักษากฎระเบียบทางอินเทอร์เน็ต เหล่านี้จะก่อให้เกิดผลสืบเนื่องที่ไม่พึงประสงค์ที่มีผลกระทบต่อองค์กร เช่น การสั่งปิดเว็บไซต์ การห้ามใช้

งานสื่อข้อมูลออนไลน์ การห้ามเผยแพร่ข้อมูลบางประเภท เป็นต้น องค์กรจะต้องเตรียมมาตรการรับมือให้เหมาะสำหรับแต่ละอุบัติการณ์ที่อาจเกิดขึ้น

2. ความเชื่อมั่นในระบบหรือโซลูชั่นการรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลายต้องคิดหาแนวทางใหม่ หมายถึง โซลูชั่น ระบบ แนวทาง วิธีการที่ยอมรับกันโดยทั่วไปและดำเนินการสืบเนื่องมา จะกลายเป็นช่องทางของภัยคุกคามทางไซเบอร์ที่จะส่งผลคุกคามและสร้างผลเสียหายต่อองค์กร รวมถึงภัยจากการจ้างงานผู้ให้บริการภายนอก การใช้งานโมบาย สมาร์ตโฟน แอปพลิเคชัน การเข้ารหัสข้อมูล และการจัดการข้อมูลขนาดใหญ่ (Big Data) โดยในประเด็นของความเชื่อมั่นในระบบหรือโซลูชั่นการรักษาความมั่นคงปลอดภัยมีองค์ประกอบดังต่อไปนี้

2.1 ผู้ให้บริการ จะกลายเป็นช่องโหว่สำคัญ จากปัจจุบันที่องค์กรส่วนใหญ่มีการใช้บริการจากผู้ให้บริการภายนอกในประเภทงานต่างๆ เป็นจำนวนมาก ทั้งการจ้างพัฒนาระบบการ วางระบบโครงข่ายสื่อสาร การให้บริการจัดการข้อมูล ฯลฯ ดังนั้นผู้ให้บริการเหล่านี้มีโอกาสจะกลายเป็นช่องโหว่ หรือจุดอ่อนสำคัญตามวงจรของโซ่อุปทานเพราะผู้ให้บริการบางรายสามารถเข้าถึงระบบสารสนเทศที่สำคัญหรือข้อมูลสำคัญขององค์กรได้ แม้ว่าองค์กรจะมีมาตรการความมั่นคงปลอดภัยอย่างดีแล้วก็ตามในขณะเดียวกัน หากผู้ให้บริการมีความหละหลวมหรือไมมีความมั่นคงปลอดภัยที่เพียงพอ เหล่าอาชญากรไซเบอร์ก็อาจจะมุ่งเป้าไปที่ผู้ให้บริการเหล่านี้แทนที่จะโจมตีองค์กรโดยตรง จึงจะเห็นได้ว่าประเทศที่พัฒนาแล้วมักจะบังคับผู้ให้บริการภายนอกของตนเอง หรือบริษัทที่เป็นคู่ค้าด้วยจะต้องมีมาตรการความมั่นคงปลอดภัย หรือดำเนินการจัดทำมาตรฐานความมั่นคงปลอดภัยในมาตรฐานระดับเดียวกัน ซึ่งมาตรฐานด้านความมั่นคงปลอดภัยยอดนิยมในปัจจุบันก็คือ มาตรฐาน ISO/IEC 27001:2013

2.2 ข้อมูลขนาดใหญ่จะกลายเป็นปัญหาใหญ่ องค์กรต่าง ๆ จะมีข้อมูลในองค์กรที่มีขนาดใหญ่ขึ้นและมีจำนวนมากขึ้นเรื่อย ๆ อาทิ การจัดทำ Data Warehouse/Data Mining/ Business Intelligence/Big Data Analytics หรือแนวทางอื่น ๆ ในการจัดการข้อมูลขนาดใหญ่ จะต้องมีการพิจารณาดำเนินการตามโครงสร้างและความพร้อมภายใน และรวมทั้งเทคโนโลยีและปัจจัยสนับสนุนจากภายนอก ซึ่งก็อาจทำให้มีการตัดสินใจเชิงกลยุทธ์ที่ผิดพลาดได้จากการจัดทำชุดข้อมูลที่ผิดพลาดหรือไม่ สมบูรณ์ หากองค์กรไม่สามารถดำเนินการอย่างถูกต้องเหมาะสม ปัญหาการจัดการข้อมูลขนาดใหญ่นี้ก็อาจส่งผลกระทบต่อการดำเนินธุรกิจขององค์กรในที่สุด

2.3 แอปพลิเคชันบนสมาร์ตโฟนจะกลายเป็นช่องทางหลักที่จะถูกโจมตีทางไซเบอร์ ด้วยวัฒนาการด้านความสามารถของคอมพิวเตอร์ที่ไปอยู่ในรูปแบบอุปกรณ์มือถือและสมาร์ตโฟน มีการเปลี่ยนแปลงตลอดเวลาและรวดเร็ว ทำให้วงจรการพัฒนาระบบหรือ

แอพพลิเคชั่นเพื่อการใช้งานในอุปกรณ์มือถือจะต้องรวดเร็วให้สามารถใช้งานได้ทันกับการเปลี่ยนแปลงดังกล่าว ซึ่งอาจทำให้ขาดการพิจารณาประเด็นด้านความมั่นคงปลอดภัย และทำให้โมบายแอพพลิเคชั่นกลายเป็นช่องทางหลักสำหรับอาชญากรไซเบอร์และเหล่าแฮ็กเกอร์ ที่จะเจาะระบบหรือแอบแฝงอยู่ในอุปกรณ์มือถือตามจุดมุ่งหมายและเป้าหมายที่ต้องการ

2.4 การเข้ารหัสข้อมูลไม่เกิดผล การเข้ารหัสข้อมูล (Encryption) ซึ่งเป็นวิธีการพื้นฐานที่นำมาใช้ในการรับส่งข้อมูลผ่านระบบอินเทอร์เน็ตตามที่ใช้กันอยู่นั้นจะเกิดความล้มเหลวหรือไม่เกิดผล ไม่ว่าจะมีการใช้วิธีการและอัลกอริธึมที่พัฒนาให้ปลอดภัยมากเพียงใด เพราะความก้าวหน้าทางเทคโนโลยีในปัจจุบันและอนาคตจะทำให้ความสามารถของระบบประมวลผลคอมพิวเตอร์ มีการปรับปรุงขีดความสามารถเพิ่มขึ้นอีกหลายเท่า ซึ่งรวมกับวิธีการ back-door กับซอฟท์แวร์ที่ใช้อยู่ ทีในอดีตอาจต้องใช้เวลาหลาย ๆ ปีในการถอดรหัส แต่ปัจจุบันสามารถทำได้ภายในไม่กี่ชั่วโมงหรือนาที หรือในระดับวินาที

3. ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นประเด็นที่เกี่ยวกับปัญหาด้านการบริหารจัดการภายในองค์กร ที่แต่เดิมผู้บริหารระดับสูงไม่ได้ให้ความสนใจเรื่องความมั่นคง ปลอดภัยทางไซเบอร์เท่าที่ควร โดยที่ CEO ไม่ตระหนักหรือไม่รับรู้ ปล่อยให้เป็นหน้าที่ของผู้บริหารระดับสูงที่รับผิดชอบ เช่น ผู้บริหารระดับสูงด้านสารสนเทศ (CIO) หรือ ผู้บริหารระดับสูงด้านความมั่นคงปลอดภัยสารสนเทศ (CISO) แต่ในปัจจุบัน CEO เริ่มมีความตระหนักรับรู้เรื่องความมั่นคงปลอดภัยไซเบอร์ในระดับหนึ่ง แต่ปรากฏว่าผู้บริหารระดับสูงที่รับผิดชอบกลับไม่สามารถที่จะดำเนินการหรือหาแนวทางในการจัดการได้ โดยรายละเอียดขององค์ประกอบที่เกี่ยวข้องในประเด็นความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยไซเบอร์ จะเป็นดังนี้

3.1 CEO รับรู้ถึงปัญหาเรื่องความมั่นคงปลอดภัยไซเบอร์ถึงเวลาที่ต้องลงมือปฏิบัติให้เกิดผลงานส่งมอบที่ได้ผลจริง ผู้บริหารระดับสูงสุดขององค์กรได้เริ่มตระหนักถึงภัยคุกคามทางไซเบอร์ และได้มอบหมายให้ CISO หรือผู้บริหารที่รับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ ให้นำเสนอแนวทางและคุณประโยชน์ที่องค์กรจะได้รับ เมื่อเทียบกับงบประมาณค่าใช้จ่ายหรืออาจจะขอให้ดำเนินการในมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ ในขณะที่โครงสร้างขององค์กรไม่พร้อมหรือไม่สามารถดำเนินการได้ ผู้บริหารที่รับผิดชอบนั้นอาจไม่สามารถให้ข้อมูลหรือดำเนินการในมาตรการตามที่ CEO ร้องขอได้ อันเนื่องมาจากข้อจำกัดต่าง ๆ ด้านการบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร

3.2 ความแตกต่างด้านทักษะ จะมีช่องว่างห่างมากขึ้น ความแตกต่างในทักษะด้านการจัดการความมั่นคงปลอดภัยสารสนเทศและด้านที่เกี่ยวข้องกับความปลอดภัยของระบบ

จะมีช่องว่าง (Gap) ห่างมากขึ้น เมื่อเทคโนโลยีก้าวหน้า ภัยคุกคามก้าวล้ำ แต่ทักษะของบุคลากรมีพัฒนาการในสัดส่วนที่ช้ากว่าองค์กรหลายแห่งพยายามส่งเสริมและพัฒนาทักษะความ สามารถให้กับบุคลากรภายใน โดยไม่มีการพิจารณาสรรหาโดย การเฟ้นหาตัวบุคลากรที่มีทักษะความสามารถที่เหมาะสมมาปฏิบัติงาน เนื่องจากไม่มีข้อบังคับหรือบทบัญญัติทางกฎหมายมากดดันในเรื่องดังกล่าว

3.3 ความมั่นคงปลอดภัยสารสนเทศ จะไม่สามารถใช้ได้กับคนรุ่นใหม่ในแต่ละองค์กรจะมีบุคลากรในระดับที่อายุที่แตกต่างกัน ทั้งคนรุ่นเก่าและคนรุ่นใหม่ โดยเฉพาะกลุ่มรุ่นใหม่ Gen-Y และ Gen-Z ที่เติบโตมาพร้อมกับความทันสมัยทางเทคโนโลยีและอุปกรณ์ที่มีการใช้งานหลากชนิด ทั้งแพลตฟอร์ม อุปกรณ์ และช่องทางการใช้งาน ทำให้แนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศที่มีแต่เดิมอาจจะไม่เหมาะสมกับแนวทางในปัจจุบันสำหรับคนรุ่นใหม่เหล่านี้ จึงเป็นสิ่งท้าทายสำหรับ CISO และผู้บริหารระดับสูงที่ต้องรับผิดชอบ

รายงานล่าสุดของ ISF ในปี 2019 จากรายงาน Threat Horizon 2019 ได้รายงานถึงผลกระทบของภัยคุกคามทางไซเบอร์โดยในรายงานได้มีการอธิบายถึงผลต่อเนื่องจากภัยคุกคามทางไซเบอร์นับจากปี 2017 จนถึงปี 2019 โดยประเด็นการโจมตีแสดงได้ดังภาพประกอบที่ 2.1 โดยในรายงานได้ทำการรวบรวมเรื่องราวของบริษัทชั้นนำ 9 แห่งที่ได้รับผลกระทบจากการใช้งานเทคโนโลยี จากการดำเนินงาน และสามารถสรุปถึงผลของทั้งผู้ใช้งานและผู้โจมตี ต่อความผิดพลาดจากการใช้งาน โดยผู้ใช้งานอาจจะมีความผิดพลาดเกิดขึ้นจทำให้ข้อมูลขององค์กรเกิดการรั่วไหลอันเป็นผลมาจากการโจมตีทางไซเบอร์ที่อาจจะไม่รู้ตัวมาก่อน ในขณะที่ผู้โจมตีเองก็ได้เพิ่มพูนความสามารถและไร้กระทำการโจมตีต่อองค์กรเหล่านั้นโดยไร้ซึ่งความปราณี จากผลการรายงานของ Threat Horizon 2019 ทำให้เห็นว่าองค์กรต่าง ๆ จะต้องเผชิญกับภัยคุกคามอย่างหลีกเลี่ยงไม่ได้ในอีกสองถึงสามปีข้างหน้าอันเป็นผลมาจากการของการเปลี่ยนแปลงเทคโนโลยี โดยในรายงานได้สรุปถึงประเด็นหลักของภัยคุกคามนั้นไว้ 3 ประเด็นหลัก ที่สะท้อนถึงผลกระทบที่สำคัญที่ควรเกิดขึ้น ซึ่งได้แก่

ประเด็นที่ 1 – การหยุดชะงัก (Disruption) จากการพึ่งพาการเชื่อมต่อที่บอบบาง

ประเด็นที่ 2 – การบิดเบือน (Distortion) ความน่าเชื่อถือในความสมบูรณ์ของข้อมูลจะสูญหายไป

ประเด็นที่ 3 – การเสื่อมสภาพ (Deterioration) เมื่อตัวควบคุมถูกกัดเซาะโดยข้อบังคับและเทคโนโลยี

โลกในปี 2019 จะขึ้นอยู่กับเทคโนโลยีและการเชื่อมต่อทั้งหมดและองค์กรจะต้องใช้เครื่องมือทุกอย่างเพื่อการดำเนินการให้สามารถก้าวข้ามต่อภัยคุกคามที่จะเข้ามาเพื่อการดำเนิน

ไปข้างหน้า โลกในอนาคตจึงจำเป็นต้องที่จะสร้างวัฒนธรรมในการให้ความร่วมมือที่เข้มแข็งกับคนและเวลาที่เหมาะสมเพื่อที่จะทำให้เกิดการมีความส่วนร่วมระหว่างกันในอันที่จะทำให้เกิดความสำเร็จที่จะรับมือต่อภัยคุกคามได้

ภาพประกอบที่ 2.1 ประเด็นภัยคุกคามทางไซเบอร์ตั้งแต่ปี คศ. 2017 – 2019

ที่มา : Information Security Forum (ISF, 2019)

โดยที่ประเด็นของภัยคุกคามที่เกิดขึ้นดังในรายงานที่อยู่ใน Threat Horizon 2019 ผู้วิจัยสามารถสรุปถึงประเด็นต่าง ๆ พร้อมกับคำแนะนำดังต่อไปนี้

ประเด็นที่ 1 – การหยุดชะงัก (Disruption) จากการพึ่งพาการเชื่อมต่อที่บอบบาง

1.1 การหยุดชะงักของอินเทอร์เน็ตอาจส่งผลต่อภาคธุรกิจ ในสภาพแวดล้อมของความสัมพันธ์ระหว่างประเทศที่ที่มีการค้าขายระหว่างกัน ถ้าเกิดปัญหาทางด้านโครงสร้างพื้นฐานทางอินเทอร์เน็ตขึ้น สิ่งนี้ก็จะกลายเป็นเป้าหมายในของกลุ่มก่อการร้ายมุ่งสร้างความเสียหายทางเศรษฐกิจอย่างกว้างขวางต่อฝ่ายตรงข้าม และย่อมส่งผลต่อประเทศชาติในที่สุด

คำแนะนำ : แผนความต่อเนื่องทางธุรกิจที่มีอยู่อาจไม่สามารถนำมาดำเนินการในการแก้ปัญหาได้อีกต่อไป อาจจะต้องมีการต้องพึ่งพากันระหว่างผู้ที่มีส่วนเกี่ยวข้องทั้งภายในและภายนอก รวมไปถึงผู้มีส่วนได้ส่วนเสียที่จะต้องมองหาแนวทางใหม่ ๆ ในการติดต่อสื่อสาร ซึ่งอาจจะเป็นทางเลือกใหม่ของการสื่อสาร (เช่นเทเล็กซ์, ดาวเทียม, ไมโครเวฟ)

1.2 จะมีแรนซัมแวร์ (Ransomware) ที่คอยเรียกค่าไถ่เกิดขึ้นบนเทคโนโลยีประสานสรรพสิ่ง ซึ่งจะเป็นหนึ่งในวิธีที่แพร่หลายที่สุดในการใช้ประโยชน์จากค่าที่องค์กรต่าง ๆ ใช้ข้อมูลดิจิทัลร่วมกัน แรนซัมแวร์จะถูกพัฒนาให้มีความอัจฉริยะมากขึ้น โดยกำหนดเป้าหมายเชื่อมต่ออุปกรณ์ทางกายภาพซึ่งอาจทำให้ชีวิตที่เป็นอยู่ในปัจจุบันตกอยู่ในอันตราย

คำแนะนำ : ต้องดำเนินการให้เกิดมีความส่วนร่วมกับองค์กรในภาคอุตสาหกรรมเพื่อที่จะดำเนินการในการออกกฎระเบียบเพื่อกำหนดถึงความปลอดภัย อย่างน้อยก็ขั้นต่ำที่สุด เพื่อนำมาใช้ในการควบคุมต่อการใช้งานเกี่ยวกับการใช้งาน รวมถึงมาตรฐานสำหรับอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things: (IoT))

1.3 มาตรการในการลดอภิสิทธิ์สำหรับบุคคลบางกลุ่มที่ได้รับสิทธิ์ในการเข้าถึงการใช้งานจะต้องถูกดำเนินการให้เกิดขึ้น โดยต้องดำเนินการอย่างละมุนละม่อมที่สุด ซึ่งถือได้ว่าเป็นภารกิจสำคัญ เนื่องด้วยการเข้าถึงข้อมูลที่สำคัญจะมีความจำเป็นสำหรับคนบางกลุ่ม โดยการที่จะต้องดำเนินการให้เกิดการสูญเสียให้น้อยที่สุด

คำแนะนำ : ระบุภารกิจสำคัญขององค์กรทางด้าการเข้าถึงสินทรัพย์ ข้อมูลของแต่ละบุคคลเพื่อไม่ให้เกิดความเสียหายต่อข้อมูลอันสำคัญขององค์ได้

ประเด็นที่ 2 – การบิดเบือน (Distortion) ความน่าเชื่อถือในความสมบูรณ์ของข้อมูลจะสูญหายไป

2.1 ข้อมูลที่มีข้อผิดพลาดจะได้รับความน่าเชื่อถือโดยอัตโนมัติ การฝึกฝนในเรื่องการแพร่กระจายข้อมูลที่ผิดโดยเจตนาจะต้องได้รับการพัฒนาไปเป็นเป้าหมายสำคัญขององค์กรโดยเฉพาะข้อมูลทางด้านการค้า ที่มีอัตราความก้าวหน้าอย่างมาก

คำแนะนำ : สร้างสถานการณ์จำลองที่เกี่ยวข้องกับกระบวนการจัดการเหตุการณ์ที่ครอบคลุมการแพร่กระจายของข้อมูลที่ผิดในภาพรวมขององค์กร

2.2 ข้อมูลเท็จทำให้ประสิทธิภาพในการดำเนินการลดลง การโจมตีที่อาจจะลดทอนความสมบูรณ์ขององค์กรภายใน ด้วยการโจมตีข้อมูลจะเพิ่มจำนวนขนาดและความซับซ้อน

คำแนะนำ : ตรวจสอบการเข้าถึงและการเปลี่ยนแปลงที่เกิดขึ้นของข้อมูล โดยใช้gครื่องมือเช่น การระบุอัตลักษณ์และการจัดการการเข้าถึง (Federated Identity and Access Management: FIAM) และระบบการจัดการเนื้อหา (Content Management System: CMS)

2.3 บล็อกเชนจะถูกทำลายความไว้วางใจ ความปลอดภัยของบล็อกเชนโดยเฉพาะในเรื่องของความน่าเชื่อถือจะถูกทำลายลง ซึ่งอาจจะส่งผลให้เกิดการละทิ้งบล็อกเชน ที่ได้รับผลกระทบไปพร้อม ๆ กับการสูญเสียประสิทธิภาพของกระบวนการ

คำแนะนำ : แต่งตั้งผู้สนับสนุนหรือคณะกรรมการกำกับดูแลอย่างกว้างขวางและตัดสินใจเกี่ยวกับการยอมรับและการใช้บล็อกเชนที่มีต่อองค์กร

ประเด็นที่ 3 – การเสื่อมสภาพ (Deterioration) เมื่อตัวควบคุมถูกกัดเซาะโดยข้อบังคับและเทคโนโลยี

3.1 กฎหมายการเฝ้าระวังจะเป็นตัวที่เปิดเผยความลับขององค์กร องค์กรจะไม่สามารถกำหนดการจัดการด้านความปลอดภัยได้ ผู้โจมตีจะใช้ประโยชน์จากสิ่งนี้ในการเข้าถึงแหล่งข้อมูลที่เก็บรวบรวมเป็นจำนวนมากโดยผู้ให้บริการการสื่อสาร เพื่อทำลายข้อมูลอันเป็นความลับขององค์กร

คำแนะนำ : ดำเนินการให้เกิดการทำงานร่วมกันของคนทั้งองค์การ ต้องมีการประเมินความเสี่ยงเพื่อความเข้าใจถึงผลกระทบของข้อมูล ที่อาจเกิดขึ้น

3.2 ข้อกำหนดความเป็นส่วนตัวจะเป็นอุปสรรคต่อการตรวจสอบของภัยคุกคามที่เกิดขึ้น ภายใต้ข้อจำกัด ในการทำโปรไฟล์แต่ละรายการที่อาจจะส่งผลให้เกิดปัญหาสำหรับองค์กร ซึ่งได้แก่ การสูญเสียความสามารถในการตรวจสอบภัยคุกคามภายใน หรือมีการท้าทายต่อกฎระเบียบเกิดขึ้น โดยทั้งสองประเด็นนี้จะมีผลกระทบเชิงลบต่อองค์กรทั้งสิ้น

คำแนะนำ : รับคำแนะนำทางกฎหมายเกี่ยวกับข้อ จำกัด ที่เกี่ยวข้อง การทำโปรไฟล์ผู้ใช้ในทุกเขตอำนาจที่องค์กรดำเนินการ

3.3 ความเร่งรีบในการปรับใช้ปัญญาประดิษฐ์ (AI) นำไปสู่ผลที่คาดไม่ถึง การใช้ปัญญาประดิษฐ์ จะสร้างผลลัพธ์ที่เหนือกว่าความเข้าใจของผู้นำธุรกิจ นักพัฒนา และผู้จัดการ อันจะนำไปสู่ช่องโหว่ใหม่ของระบบที่เกิดขึ้น

คำแนะนำ : พัฒนาผู้จัดการระบบปัญญาประดิษฐ์ ที่มีความรู้ ความเข้าใจ และการรักษาความสามารถด้วยทักษะที่จะเข้าใจและจัดการระบบปัญญาประดิษฐ์อย่างแท้จริง

องค์กรจะต้องเตรียมพร้อมสำหรับการทำงานร่วมกันในระดับที่ไม่เคยมีมาก่อน เพื่อให้ได้ผลลัพธ์ที่ดีที่สุดจากวัฒนธรรมการทำงานร่วมกันที่มากขึ้น ผู้นำทางธุรกิจจะต้องมั่นใจว่าความร่วมมือกันนั้นจะต้องได้รับการสนับสนุนในด้านความชำนาญ ความสามารถและรักษาความรู้เพื่อเตรียมความพร้อมต่อภัยคุกคามที่อาจจะเกิดขึ้นต่อไปได้

2.2.4 แนวโน้มภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อโซ่อุปทานดิจิทัล

ในแง่ของการจัดการทางด้านความเสี่ยงของโซ่อุปทาน (Supply Chain Risk Management) เป็นที่ทราบกันดีอยู่แล้วว่าในทุก ๆ กิจกรรมที่มีการดำเนินไปในโซ่อุปทานนั้น ในทุกขั้นตอนของการดำเนินกิจกรรมจะมีความเสี่ยง (Risk) ที่อาจทำให้เกิดการหยุดชะงัก (Disruption) ในโซ่อุปทานได้ทั้งสิ้น ความเสี่ยงดังกล่าวนี้ผู้จัดการโซ่อุปทานหรือผู้ที่มีส่วนเกี่ยวข้องในโซ่อุปทานทั้งหมด สามารถที่จะทราบได้ว่า ความเสี่ยงเหล่านั้นเป็นความเสี่ยงที่เกิดมาจากสาเหตุอะไร หรืออาจจะไม่สามารถที่จะคาดเดาถึงการเกิดขึ้นของความเสี่ยงเหล่านั้นได้เลย ในกรณีที่ไม่ทราบถึงสาเหตุของความเสี่ยงที่เกิดขึ้นนี้สำหรับโซ่อุปทานที่มีอยู่ทั่วโลกในปัจจุบันนี้ ผู้จัดการโซ่อุปทานต้องพบเรื่องที่ท้าทาย ด้วยสาเหตุที่มาจากการที่วงจรชีวิตของผลิตภัณฑ์สั้นลง และความต้องการของลูกค้าที่เพิ่มขึ้น (Carvalho et al., 2011) ดังนั้นแล้วการเกิดขึ้นของการหยุดชะงักใด ๆ ในโซ่อุปทานย่อมจะส่งผลต่อการดำเนินธุรกิจ โดยที่ผลลัพธ์ที่เกิดขึ้นก็จะทำให้เกิดการดำเนินงานที่ไม่พึงประสงค์ต่อกระบวนการในการจัดการโซ่อุปทาน ซึ่งก็จะมีผลกระทบต่อเสถียรภาพทางด้านการเงินของบริษัท และในท้ายที่สุดก็จะผลต่อผลการดำเนินงานของบริษัท (Shi Min et al., 2013; Jüttner and Maklan, 2011) การหยุดชะงักที่เกิดขึ้น เช่นการสูญเสียของผู้จัดจำหน่ายที่สำคัญ การเกิดเพลิงไหม้ครั้งใหญ่ที่โรงงานการผลิต เกิดการก่อการร้ายที่ร้ายแรง หรือ การเกิดโรคระบาดหรือโรคติดต่อ เหล่านี้จะเป็นสิ่งที่จะส่งผลกระทบต่อรายได้และค่าใช้จ่ายธุรกิจทั้งสิ้น จึงสามารถที่จะบอกได้ว่าการเกิดหยุดชะงักต่อบริษัทนั้น ย่อมจะนำไปสู่ยอดขายของบริษัทที่หายไป รวมทั้งส่วนแบ่งการตลาดที่จะต้องหายไปด้วย ตลอดจนถึงค่าใช้จ่ายที่เพิ่มขึ้น (T. Wakolbinger et al., 2011; Wildgoose Nick et al., 2012; Qiang et al.,, 2009) อันเนื่องมาจากการที่จะต้องเข้ากระตุ้นหรือเร่งบริการในกิจกรรมต่าง ๆ ที่เกิดขึ้นภายในระบบโซ่อุปทาน การหยุดชะงักของโซ่อุปทานสามารถเกิดขึ้นได้จากปัจจัยภายนอกและภายใน โดยปัจจัยที่มาจากแหล่งภายนอก ตัวอย่างเช่น ภัยพิบัติทางธรรมชาติ และ ปัจจัยที่มาจากแหล่งภายใน ตัวอย่างเช่น ความล้มเหลวในการที่จะบูรณาการทำงานทั้งหมดในโซ่อุปทาน บ่อยครั้งที่เหตุการณ์ของการเกิดการหยุดชะงักดังกล่าวเกิดขึ้นอย่างรวดเร็วและโดยไม่มีการแจ้งเตือนให้รับทราบล่วงหน้า

นอกจากนี้การหยุดชะงักยังเป็นผลที่จะเกิดมาจากความพยายามที่จะสร้างประสิทธิภาพที่มากขึ้น ตัวอย่างเช่นในเรื่องของต้นทุนที่เกี่ยวกับสภาวะแวดล้อมของโซ่อุปทาน

กิจกรรมที่เกี่ยวกับโซ่อุปทานที่ได้มีการดำเนินไปในหลาย ๆ บริษัทไม่ว่าจะเป็นการจัดหาวัตถุดิบ การประกอบ การผลิต การกระจายสินค้า ตลอดจนรวมไปถึงการส่งมอบสินค้า ปัจจุบันได้มีการว่าจ้างไปยังผู้จำหน่าย (Supplier) หรือไม่ทำการจ้างเอาท์ซอส (Outsource) อันเป็นผลเนื่องมาจากนโยบายการแข่งขันในระดับโลก ที่ซึ่งลูกค้าที่แต่ละบริษัทจะต้องจัดหาสินค้าหรือบริการนั้นได้มีอยู่ทั่วโลก ดังนั้นสิ่งนี้จึงทำให้บริษัทต่างๆ ต้องดำเนินกิจกรรมเพื่อให้สามารถแข่งขันกับบริษัทอื่น ๆ ได้ ดังนั้นแล้วด้วยโครงสร้างของการดำเนินงานในลักษณะเช่นนี้ ที่ได้ถูกสร้างขึ้นมาจากเงื่อนไขของสภาพแวดล้อมที่ขึ้นอยู่กับโซ่อุปทานนั้น ๆ ดั้งนั้นไม่ว่าเมื่อใดก็ตาม ถ้าหากมีการหยุดชะงัก (Disruption) เกิดขึ้นย่อมจะส่งผลต่อการดำเนินงานของบริษัทซึ่งก็จะมีผลต่อโซ่อุปทานทั้งหมด การหยุดชะงักดังกล่าวนี้จะมีผลมากน้อยเพียงใดนั้นก็จะขึ้นกับโซ่อุปทานที่เกี่ยวข้อง ซึ่งสามารถเกิดขึ้นได้ตั้งแต่ต้นน้ำจนถึงปลายน้ำของโซ่อุปทาน ลักษณะดังกล่าวนี้ก็คือความเสี่ยงที่เกิดขึ้นในโซ่อุปทานและในขณะที่ความเสี่ยงของโซ่อุปทานเพิ่มขึ้นนั้น บริษัททั้งหลายก็จะมีความจำเป็นในการพัฒนากระบวนการสำหรับการจัดการความเสี่ยงของโซ่อุปทาน (Supply Chain Risk Management) (Ismail Golgeci et al., 2013; Cienfuegos et al., 2013; Karen Hardy 2015) และความสมรรถนะทางด้านโซ่อุปทาน (Supply Chain Competency) (Krishnapriya et al.,2014; Ellinger Alexander E. et al., 2011; Wieland Andreas et al., 2013) ที่สามารถช่วยให้พวกบริษัทเหล่านั้นมีความพร้อม (หรือความสามารถ) ในการตอบสนองที่มีประสิทธิภาพและประสิทธิผล และทำให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่องตามที่วางแผนไว้ และเพื่อที่จะลดความเสี่ยงเหล่านี้ โซ่อุปทานจะต้องถูกออกแบบมาเพื่อให้มีความพร้อม (Readiness) กับเหตุการณ์การหยุดชะงักที่จะเกิดขึ้น โดยจะต้องทำให้มีการตอบสนอง (Response) ที่มีประสิทธิผลและมีประสิทธิภาพ และยังจะต้องสามารถกลับคืนสภาพ (Recovery) เข้าสู่สภาพเดิมหรือที่ดีกว่าก่อนที่จะมีการหยุดชะงัก ซึ่งเหล่านี้เองคือ ส่วนประกอบที่สำคัญในการศึกษาในเรื่องของ การคืนสภาพได้ของโซ่อุปทาน (Supply Chain Resilience) (Ponomarov et al., 2009)

รายงานสถานการณ์ภัยคุกคามของ Trend Micro ในปี 2015 ที่ผ่านมา (TrendMicro, 2015) ได้รายงานว่า ในช่วงปี 2015 ที่ผ่านมาภัยคุกคามทางไซเบอร์จะประกอบด้วยภัยคุกคามทั้งแบบเก่าและแบบใหม่ ไม่ว่าจะเป็น มัลแวร์ที่แฝงตัวในโฆษณา (Malvertising) และช่องโหว่ที่เพิ่งค้นพบซึ่งได้แก่ ภัยคุกคามที่ท้าทายความน่าเชื่อถือในระบบโซ่อุปทานและแนวทางปฏิบัติที่เหมาะสม” (Bad Ads and Zero-Days: Reemerging Threats Challenge Trust in Supply Chains and Best Practices), ระบบชำระเงินในธุรกิจค้าปลีกและธุรกิจความงามและสุขภาพ ยังพบ

เจอกับปัญหาภัยคุกคามทางไซเบอร์ที่เพิ่มสูงขึ้น รายงานดังกล่าวเน้นย้ำว่าความไว้วางใจของผู้ใช้อาจก่อให้เกิดความเสี่ยงทางด้านความมั่นคงปลอดภัยไซเบอร์อย่างมากในยุคที่ความผิดพลาดแม้เพียงเล็กน้อยก็อาจก่อให้เกิดปัญหาร้ายแรงได้ แน่นอนว่าองค์กรธุรกิจและผู้ใช้ทั่วไปจะต้องดำเนินการเชิงรุกมากขึ้นเพื่อป้องกันภัยคุกคาม องค์กรธุรกิจต่างๆ จะต้องมีนโยบายความปลอดภัยด้านไอทีเพื่อให้สามารถดำเนินการต่อไปได้ในสภาพแวดล้อมที่ปราศจากความน่าเชื่อถือ (Zero Trust Environment) แนวทางการรักษาความปลอดภัยที่แตกต่างและจริงจังจึงมีความสำคัญอย่างยิ่งต่อการปกป้องทรัพย์สินด้านการเงิน ทรัพย์สินส่วนตัว และทรัพย์สินทางปัญญาให้ปลอดภัย

นอกจากนี้ แอดแวร์ (Adware) ยังครองอันดับสูงสุดในบรรดาภัยคุกคามบนระบบโมบาย (Mobile) โดย TrendMicor ตรวจพบภัยคุกคามบน Android มากกว่า 5 ล้านชนิดจนถึงปัจจุบัน หรือเท่ากับเกือบครึ่งหนึ่งของยอดรวม 8 ล้านที่คาดการณ์ไว้ภายในสิ้นปี 2558 ที่จริงแล้ว Application ที่เป็นอันตรายและ Application ที่มีความเสี่ยงสูงที่ถูก TrendMicro บล็อกไว้โดยมากมีสาเหตุเกี่ยวข้องกับแอดแวร์ทั้งสิ้น นักวิจัยของ TrendMicro ยังตรวจพบการใช้ช่องโหว่ใหม่ ๆ เพื่อโจมตีซอฟต์แวร์ของ Adobe โดยใช้มัลแวร์แฝงตัวมาอยู่ในโฆษณา ซึ่งสามารถทำงานได้ถึงแม้เหยื่อไม่ได้เยี่ยมชมหรือโต้ตอบกับเว็บไซต์อันตรายก็ตาม นอกเหนือจาก iOS™ และระบบชำระเงิน (Point-of-Sale: POS) ที่ตกเป็นเป้าหมายการโจมตีอย่างต่อเนื่องแล้ว ธุรกิจความงามและสุขภาพก็ได้ตกเป็นเป้าหมายใหม่ที่ต้องเผชิญกับการโจมตีทางไซเบอร์ที่เพิ่มขึ้นอย่างมาก เนื่องจากการโจมตีในธุรกิจนี้อยู่ในช่วงเริ่มแรกมานานหลายปี ดังนั้นนักวิจัยจึงเชื่อว่าการเพิ่มขึ้นนี้เป็นผลมาจากการขาดความพร้อม ซึ่งนับเป็นปัญหาสำคัญที่จำเป็นต้องได้รับการจัดการดูแลอย่างจริงจัง ประเด็นที่เราต้องตั้งคำถามก็คือว่า เราดำเนินการอย่างเพียงพอแล้วหรือยังเพื่อที่จะปกป้องตัวเราเองจากภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ เราจำเป็นที่จะต้องอัพเดตระบบเพื่อป้องกันภัยคุกคามใหม่ ๆ อย่างไรก็ตามจากรายงานของ TrendMicro ก็แสดงให้เห็นอย่างชัดเจนว่าเราจะต้องระวังภัยคุกคามเดิม ๆ ด้วยเช่นกัน ซึ่งจะต้องทำโดยให้ครอบคลุมทุกระบบและทุกกลุ่มอุตสาหกรรมอย่างไม่มีข้อยกเว้น

ภัยคุกคามที่เกิดขึ้นมีรูปแบบที่เปลี่ยนไปโดยถูกส่งมาในรูปของข้อมูลข่าวสาร ความรู้ และวิทยาการที่ทันสมัยต่าง ๆ ซึ่งได้ถูกนำเข้ามาสู่ประเทศไทยอย่างต่อเนื่องและไม่สามารถต้านทานได้อีกต่อไป องค์กรจึงไม่สามารถแก้ปัญหาด้านความมั่นคงปลอดภัยรูปแบบใหม่ได้โดยวิธีเดิม ๆ และตามลำพังได้อีกต่อไป การเผชิญภัยคุกคามรูปแบบใหม่ในยุคปัจจุบันที่ได้รับการสนับสนุนจากทางภาครัฐที่ต้องการจะขับเคลื่อนเศรษฐกิจภายในประเทศให้เป็นไปตามนโยบายการขับเคลื่อนเศรษฐกิจภายใต้แนวคิดเศรษฐกิจดิจิทัล (Digital Economy) องค์กรจำเป็นที่จะต้องปรับบทบาทให้มีขีดความสามารถหลากหลายมากขึ้น เพื่อการขับเคลื่อนเศรษฐกิจที่จะเกิดขึ้นต่อไป

ในอนาคตแน่นอนว่าต้องอาศัยเทคโนโลยีสารสนเทศและการสื่อสารซึ่งก็คือผ่านเครือข่ายอินเทอร์เน็ตทั้งสิ้น ดังนั้นการเตรียมความพร้อมสำหรับองค์กรหรือบริษัทต่างๆ ต่อการโจมตีทางด้านไซเบอร์อันเป็นผลมาจากปฏิบัติงานผ่านระบบเครือข่ายอินเทอร์เน็ตจึงเป็นสิ่งจำเป็นอย่างยิ่งสำหรับการดำเนินการในปัจจุบัน

2.2.5 องค์ประกอบของการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล

จุดมุ่งหมายของอาชญากรทางไซเบอร์จะมุ่งไปใน 3 ลักษณะคือ การนำความลับไปเปิดเผย (Data Confidentiality) การเปลี่ยนแปลงข้อมูล (Data Integrity) และการทำให้ระบบหยุดบริการหรือไม่สามารถใช้งานได้ (System Availability) (Settapong Malisuwan, 2010)

จากการศึกษาจากเอกสารงานวิจัย เพื่อทำการศึกษาถึงองค์ประกอบของการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยได้ทำการทบทวนวรรณกรรม และทำการสังเคราะห์วรรณกรรมที่เกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยตารางที่ 2.2 ได้แสดงองค์ประกอบของการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลและแหล่งอ้างอิง

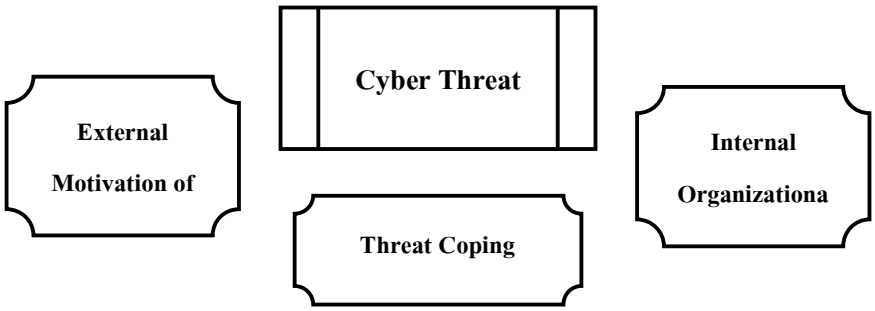
ตารางที่ 2.2 องค์ประกอบของการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลและแหล่งอ้างอิง

แหล่งอ้างอิง	แรงจูงใจจากภายนอก	จุดอ่อนของระบบภายใน	การรับมือต่อภัยคุกคาม
Samuel Waithaka (2016)	✓	✓	
Srisawang, Sirirat (2015)			✓
Rid, T. et al., (2014)	✓	✓	
Ng et. al., (2009)			✓
Choo, K. K. R. (2014)	✓		
Dhillon & Backhouse (2006)		✓	
Roumani, M. A. et al. (2015)	✓	✓	
Anderson & Agarwal (2010)			✓
Rahim, N. et al. (2015)			✓

ตารางที่ 2.2 (ต่อ)

แหล่งอ้างอิง	แรงจูงใจจากภายนอก	จุดอ่อนของระบบภายใน	การรับมือต่อภัยคุกคาม
Yadav, S. A. et al. (2016)	✓	✓	✓
Milan Podhorec (2012).			✓
Chou, T. S. (2013).		✓	
Shakarian et. al., 2013	✓		
Andreasson (2011)	✓		
Gandhi et. al. (2011)	✓		
Kankanhalli et al., (2003)		✓	
Pahnilaa et. al., (2007)			✓
Bulgurcu et al., (2010)		✓	
Pelgrin, (2014)		✓	
Lee & Larsen, (2009)			✓
Liang & Xue (2009)			✓
Crossler, R. E. et al. (2013)	✓	✓	
Woon et. al., (2005)			✓
Workman et. al., (2008)			✓
Herath, T. et al (2012)		✓	✓
Zhang et. al., (2009)			✓
Bulgurcu et. al., (2010)			✓

จากทบทวนวรรณกรรมปัญหาภัยคุกคามทางไซเบอร์ พบว่า การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทาน ประกอบด้วย 3 ประเด็นได้แก่ 1) แรงจูงใจหรือเหตุผลสำหรับผู้โจมตีระบบจากภายนอก (External Motivation of Cyber Attack) 2) ความอ่อนแอหรือจุดอ่อนของระบบภายในที่สามารถเป็นเป้าในการโจมตีจากผู้โจมตี (Internal Organizational Vulnerabilities) และ 3) การรับมือต่อภัยคุกคาม (Threat Coping) ดังภาพประกอบที่ 2.2



ภาพประกอบที่ 2.2 ปัจจัยที่ส่งผลต่อปัญหาภัยคุกคามทางไซเบอร์

2.2.5.1 แรงจูงใจหรือเหตุผลสำหรับผู้โจมตีระบบจากภายนอก (External Motivation of Cyber Attack)

แรงจูงใจเหล่านั้นสามารถเกิดขึ้นมาจากปัญหาทางเศรษฐกิจ การเมือง รวมไปถึงความมั่นคงของชาติวัตถุประสงค์หลักของผู้โจมตีนั้นไม่ชัดเจนหรืออาจมีประเด็นแอบแฝงซ่อนอยู่ การโจมตีทางเว็บไซต์และการโฆษณาชวนเชื่อ รวมไปถึงผลประโยชน์ทางการเงินที่เป็นแรงจูงใจที่สำคัญสำหรับการโจมตีระบบ นอกเหนือไปจากเหตุผลทางการเมือง (Shakarian et. al., 2013; Andreasson, 2011; Gandhi et. al., 2011; Samuel Waithaka, 2016; Rid T. et al., 2014; Roumani, M. A. et al., 2015; Yadav, S. A. et al., 2016; Crossler, R. E. et al., 2013)

2.2.5.2 จุดอ่อนของระบบภายต่อการเป็นเป้าในการโจมตี (Internal Organizational Vulnerabilities)

ในปัจจุบันการรักษาความปลอดภัยระบบสารสนเทศ จะมุ่งเน้นไปที่การใช้เทคโนโลยีในการแก้ไขปัญหาช่องโหว่ของระบบและการโจมตีทางไซเบอร์ที่เกี่ยวข้อง การปกป้องระบบที่สำคัญต้องมาจากองค์กรและบุคลากรภายใน การมีส่วนร่วมของฝ่ายบริหาร การมีนโยบายความปลอดภัย และการฝึกอบรมพนักงานและการรับรู้ ปัจจัยด้านมนุษย์และความเป็นผู้นำ ถือได้ว่าเป็นปัจจัยสำคัญในการรักษาความปลอดภัยในโลกไซเบอร์ที่ประสบความสำเร็จ การเปลี่ยนแปลงและการคุกคามทางเทคโนโลยีที่เกิดขึ้นบ่อยครั้งจะเกิดจากปัจจัยทางด้านมนุษย์ในการจัดการกับการรับรู้และช่องโหว่ที่เกิดขึ้นและสิ่งที่สำคัญคือความเป็นผู้นำ ก็ถือได้ว่าสิ่งสำคัญในการรักษาความปลอดภัยไซเบอร์ที่ยั่งยืน (Dhillon & Backhouse, 2006; Kankanhalli et al, 2003; Bulgurcu et al., 2010; Pelgrin, 2014; Samuel Waithaka, 2016; Rid, T. et al., 2014; Herath, T. et al., 2012; Roumani, M. A. et al., 2015; Yadav, S. A. et al., 2016; Crossler, R. E. et al., 2013; Chou, T. S., 2013)

2.2.5.3 การรับมือต่อภัยคุกคาม (Threat Coping)

การประเมินระดับภัยคุกคามของบุคคล การรับรู้ถึงภัยคุกคามที่เกี่ยวข้องกับแรงจูงใจในการปฏิบัติตามนโยบายความปลอดภัย และเพื่อการดำเนินพฤติกรรมการป้องกันความปลอดภัย บุคคลต่าง ๆ สามารถรับรู้ถึงการคุกคามในระดับต่าง ๆ ได้ เมื่อระดับของภัยคุกคามนั้นสูงขึ้น ผู้ใช้งานมักจะประสบปัญหาเกี่ยวกับความไม่สบายใจ อันเกิดจากผลของภัยคุกคาม ยิ่งผู้ใช้งานรับรู้ถึงผลกระทบในด้านลบเป็นผลมาจากเหตุการณ์ภัยคุกคาม ผู้ใช้งานเหล่านั้นก็จะยิ่งใช้มาตรการป้องกันมากขึ้น นอกจากนี้การประเมินถึงผลของภัยคุกคามยังส่งผลโดยตรงต่อพฤติกรรมความปลอดภัย (Anderson & Agarwal, 2010; Lee & Larsen, 2009; Liang & Xue 2009; Pahnilaa et. al., 2007; Woon et. al., 2005; Workman et. al., 2008; Zhang et. al., 2009; Ng et. al., 2009; Bulgurcu et. al., 2010)

การประเมินความสามารถของบุคคลในการจัดการและป้องกันการสูญเสียหรือความเสียหายที่อาจเกิดขึ้นจากอันตราย การประเมินการเผชิญปัญหา เป็นปัจจัยสำคัญที่ขับเคลื่อนแรงจูงใจและความเต็มใจที่จะปฏิบัติตามนโยบายความปลอดภัยและการนำเทคโนโลยีและแนวทางปฏิบัติด้านความปลอดภัยมาใช้ในองค์กร และตามบ้านที่อยู่อาศัยของประชาชนโดยทั่วไป นอกจากนี้การประเมินการเผชิญปัญหายังส่งผลโดยตรงต่อพฤติกรรมความปลอดภัย (Srisawang, 2015; Herath, T. et al., 2012; Rahim, N. et al., 2015; Yadav, S. A. et al., 2016; Milan Podhorec, 2012))

2.3 ความร่วมมือกันของโซ่อุปทานดิจิทัล

การที่ธุรกิจนำระบบการจัดการโซ่อุปทานมาเป็นยุทธศาสตร์ในการเพิ่มขีดความสามารถในการแข่งขัน จะต้องเข้าใจเกี่ยวกับการจัดการความร่วมมือกัน (Collaboration Management) ถึงแม้ว่าองค์กรขนาดใหญ่ที่ได้รับกล่าวขานว่า มีการจัดการโซ่อุปทานเป็นต้นแบบแล้ว แต่ในทางปฏิบัติพนักงานระดับล่างก็ยังมีความไม่เข้าใจเกี่ยวกับการจัดการคู่ค้าอยู่อย่างมาก Kalwani and Narayandas (1995) ได้ทำการศึกษาแบบแจ้งประจักษ์ถึงผลกระทบของความสัมพันธ์ในระยะยาวกับลูกค้าที่มีการเจาะจงลงไปกับประสิทธิภาพในการดำเนินงานของบริษัทผู้จำหน่ายโดยใช้ข้อมูลแบบ ณ จุดเวลาใดเวลาหนึ่งแบบตัดขวาง (Cross-Sectional Information) และข้อมูลที่มีการเก็บแบบระยะยาว (Longitudinal Information) โดยใช้ข้อมูลจากฐานข้อมูล compustat ที่ได้มีการเก็บรวบรวมไว้ และจากฐานข้อมูลที่ได้มีการเปิดเผยข้อมูลเหล่านี้ไว้ในขณะที่ Kumar et al. (1996) ได้ทำการแบ่งประเภทของระบบระหว่างองค์กร (Interorganizational System, ISO) ที่ประกอบไปด้วย 3 โครงสร้างคือ การนำเอาทรัพยากรสารสนเทศมาใช้ร่วมกัน (Pooled Information Resource)

โซ่คุณค่า/โซ่อุปทาน (Value/Supply Chain) และ ความเป็นเครือข่าย (Networked) เพื่อจะได้การกำหนดถึงความเสี่ยงจากความขัดแย้งที่เกิดขึ้นในเวทีของระบบระหว่างองค์กรและได้แนะนำถึงกลยุทธ์เพื่อที่จะลดถึงความน่าจะเป็นสำหรับการเกิดข้อขัดแย้งดังกล่าว จากการศึกษาของ Barry Shore (2001) ได้มีการชี้ให้เห็นถึงตัวแปรที่มีผลกระทบต่อการไหลของข้อมูลระหว่างลูกค้าและผู้จำหน่าย ตัวแปรเหล่านั้นประกอบไปด้วย อุตสาหกรรม สภาวะแวดล้อมทางการตลาดและการแข่งขัน วัฒนธรรมของชาติ วัฒนธรรมขององค์กร ขนาด และการสนับสนุนทางด้านไอทีของประเทศ โดยงานวิจัยของ Shore ได้นำเสนอและวิเคราะห์ถึงความถูกต้องของตัวแปรเหล่านี้ต่อกลยุทธ์ในการแบ่งปันข้อมูล

บริษัทที่ต้องการจะนำระบบโซ่อุปทานมาใช้เป็นยุทธศาสตร์ในการสร้างความได้เปรียบด้านการแข่งขัน จะต้องดำเนินการในการจัดวางระบบ และพัฒนาการจัดการความสัมพันธ์ของคู่ค้าให้เป็นรูปธรรมเสียก่อน โดยต้องเริ่มต้นที่องค์กรของตนเองก่อนตั้งแต่พนักงานระดับล่าง จนถึงระดับนโยบาย แล้วจึงขยายไปสู่หน่วยธุรกิจ ซึ่งเป็นคู่ค้าตลอดทั้งโซ่อุปทานให้เข้าใจถึงความสำคัญและบทบาทของการจัดการความร่วมมือกัน โดยในปัจจุบันนี้ บริษัทเหล่านั้นต่างก็กำลังมองหาวิธีที่จะสร้างความได้เปรียบในการแข่งขัน วิธีที่สามารถทำได้วิธีหนึ่งที่สมาชิกทั้งหมดในโซ่อุปทานต้องดำเนินการให้สอดคล้องกันคือ การร่วมมือกันของโซ่อุปทาน (Supply Chain Collaboration: SCC) ซึ่งเป็นแนวคิดที่จะใช้ประโยชน์จากทั้งทรัพยากร (Resource) และความรู้ (Knowledge) ของทั้งผู้จำหน่ายและลูกค้า ด้วยการร่วมมือกันและทำการบูรณาการวิธีการทั้งหมดเพื่อให้เกิดการไหลของผลิตภัณฑ์และข้อมูลในโซ่อุปทาน Simatupang and Sridharan (2002) ได้ทำการศึกษาถึงความขัดแย้งที่เกิดขึ้นในความร่วมมือของโซ่อุปทาน โดยในการศึกษาเป็นการเน้นถึงการประสานงานเพื่อทำการสร้างอนุกรมวิธานที่ครอบคลุมวิธีในการประสานงานในโซ่อุปทาน Walter (2003) ได้เสนอและทดสอบรูปแบบของความสัมพันธ์ ที่ได้ตรวจสอบถึงปัจจัยเหตุและคุณลักษณะที่อยู่ตรงกลางของความสัมพันธ์ที่มีความใกล้ชิดกันและผลกระทบต่อการมีส่วนร่วมของผู้จัดจำหน่ายในการพัฒนาผลิตภัณฑ์ใหม่

2.3.1 ความหมายของความร่วมมือกันของโซ่อุปทานดิจิทัล

การร่วมมือกันในโซ่อุปทาน (SCC) เป็นเรื่องที่บริษัทเพียงแค่สองบริษัทหรือมากกว่าได้ดำเนินการสร้างความสัมพันธ์กันในระยะยาวและการมีการทำงานกันอย่างใกล้ชิดในการวางแผนและดำเนินการปฏิบัติการในโซ่อุปทานเพื่อนำไปสู่เป้าหมายที่ร่วมกัน เพื่อที่จำให้บรรลุถึงผลประโยชน์ที่มากขึ้นกว่าที่จะดำเนินการเพียงลำพังแค่บริษัทเดียว ดังนั้นจึงเป็นการแสดงให้เห็นถึงความร่วมมือที่เกิดขึ้นจากการที่ทั้งสองฝ่ายได้ดำเนินการในทำงานร่วมกัน, มีการ

แบ่งปันข้อมูล, ทรัพยากรและความเสี่ยง และได้ทำการตัดสินใจร่วมกันเพื่อให้บรรลุผลประโยชน์ร่วมกันในท้ายที่สุด ในความพยายามที่จะทำงานร่วมกันนี้ จะรวมไปถึงการประสานงานเพื่อการพัฒนาผลิตภัณฑ์และดำเนินการปฏิบัติการเพื่อให้บรรลุตามแนวคิดทันเวลาพอดี, ได้มีการแลกเปลี่ยนข้อมูลเกี่ยวกับการพยากรณ์ความต้องการสินค้าและตารางเวลาการส่งมอบ, มีการแบ่งส่วนของค่าใช้จ่ายบ่างอย่างร่วมกันและข้อมูลเชิงกลยุทธ์อื่น ๆ ที่สามารถจะใช้ร่วมกันได้

ในสภาพแวดล้อมทางธุรกิจในปัจจุบันที่ซับซ้อน ประกอบกับความต้องการที่จะให้มีการผลดำเนินงานที่ต้องการสร้างผลกำไรและลดต้นทุน และการดำเนินงานที่มีความยืดหยุ่นนั้น ด้วยเหตุนี้จึงเป็นเหตุที่ทำให้บริษัทเกิดมีจุดอ่อนที่มากกว่าเดิมที่เคยเป็น ซึ่งทำให้บริษัทต้องพบกับความเสี่ยงอันเนื่องมาจากการเกิดการหยุดชะงักของโซ่อุปทาน จากสถิติในปี 2013 ร้อยละ 75 ของบริษัททั้งหลายต้องประสบกับการหยุดชะงักอย่างน้อยหนึ่งครั้ง อันเนื่องมาจากความผิดปกติของอุปกรณ์ต่อเนื่อง การขาดความต่อเนื่องที่ไม่คาดคิดในการจัดหา ระบบเทคโนโลยีสารสนเทศล่มลงเนื่องมาจากภัยธรรมชาติและภัยพิบัติ ดังนั้นการคืนสภาพได้ของโซ่อุปทาน ซึ่งเป็นแนวคิดที่ช่วยลดผลกระทบจากการหยุดชะงัก ที่เป็นกลยุทธ์ในเชิงรุกที่จะช่วยให้โซ่อุปทานสามารถที่จะดำเนินต่อไปได้ในขณะที่มีกระบวนการที่ทำให้เกิดการกลับไปสู่สภาพเดิมหรือปรับไปสู่การทำงานที่ดีขึ้น (Jüttner and Maklan 2011) ซึ่งเป็นเรื่องที่บริษัทต่าง ๆ ได้ให้ความสนใจที่เพิ่มขึ้น เรื่องนี้เป็นเรื่องที่บริษัทจะต้องพยายามที่จะมองหาวิธีการเพื่อที่จะทำให้เกิดความสามารถของเครือข่ายทั้งหมดภายในห่วงโซ่เพื่อความอยู่รอด เพื่อการปรับตัวและการเติบโตเมื่อต้องเผชิญกับการเปลี่ยนแปลงและความไม่แน่นอน ดังนั้นการให้ความสำคัญต่อความร่วมมือกันในการสร้างการคืนสภาพได้ให้เกิดขึ้นในโซ่อุปทานจึงเป็นสิ่งสำคัญยิ่งเพื่อที่ว่า ความร่วมมือกันในโซ่อุปทานนี้จะทำให้เกิดการยึดเหนี่ยวบริษัทต่าง ๆ ในโซ่อุปทานให้สามารถดำเนินธุรกิจร่วมกันต่อไปได้เมื่อเกิดสภาวะที่วิกฤตขึ้น

ความร่วมมือกันในโซ่อุปทานเป็นเรื่องที่เกี่ยวข้องกับความสามารถของบริษัท 2 บริษัทหรือมากกว่า ที่ทำงานร่วมกันได้อย่างมีประสิทธิภาพ มีการวางแผนและการดำเนินงานในโซ่อุปทานเพื่อการไปสู่เป้าหมายร่วมกัน (Cao et al., 2010) ถึงแม้ว่าความร่วมมือกันระหว่างองค์กรจะเป็นความคิดหลักของการบริหารจัดการความเสี่ยงในโซ่อุปทาน ความร่วมมือกันในโซ่อุปทานช่วยทำให้เกิดการพัฒนาการทำงานร่วมกันระหว่างคู่ค้า, อำนวยความสะดวกในการวางแผนร่วมกัน และกระตุ้นให้เกิดการแลกเปลี่ยนข้อมูลแบบทันที (Real-time) ที่จำเป็นเพื่อการเตรียมความพร้อมสำหรับการตอบสนอง (response) และการกู้คืน (recover) จากการหยุดชะงักของโซ่อุปทาน ในขณะที่กำลังดำเนินการเพื่อที่จะลดผลกระทบที่เกิดขึ้น ถึงแม้ว่าความร่วมมือกันในโซ่อุปทานจะนำมาซึ่งผลประโยชน์ที่เกิดขึ้นหลายอย่างเช่นการแสดงผลที่สูงขึ้นและความยืดหยุ่นและ

ลดเวลานำ แต่ก็ไม่อาจเป็นไปได้อย่างเสมอไป หรือไม่เป็นไปตามที่ต้องการ เพื่อที่จะสร้างความสัมพันธ์ของความร่วมมือกันในระยะยาว เพื่อให้การทำงานร่วมกันระหว่างคู่ค้าในโซ่อุปทานเป็นไปด้วยความสอดคล้องกัน การดำเนินกิจกรรมที่เกี่ยวกับความร่วมมือกันกับผู้จำหน่ายจะถูกผลักดันด้วยความชัดเจนจากความต้องการทางธุรกิจและความสนใจที่มีร่วมกัน การลดผลกระทบของการหยุดชะงักใด ๆ ในโซ่อุปทานเป็นการแสดงให้เห็นถึงความชัดเจนจากความต้องการทางธุรกิจและความสนใจที่มีร่วมกัน (เป้าหมายที่สอดคล้องกัน) ยิ่งไปกว่านั้น ความร่วมมือกันจะต้องเป็นอย่างไรและอะไรที่เป็นกิจกรรมของการร่วมมือกันที่มีความสำคัญที่ยังคงมีความไม่ชัดเจนอยู่

จากการทบทวนวรรณกรรม พบว่า นักวิจัยและนักวิชาการได้ให้ความหมายหรือคำจำกัดความของคำว่า ความร่วมมือกันของโซ่อุปทาน ดังตารางที่ 2.3

ตารางที่ 2.3 ความหมายของความร่วมมือกันของโซ่อุปทานดิจิทัล

แหล่งที่มา	**ความหมายของความร่วมมือกันของโซ่อุปทานดิจิทัล**
Mark Barrett (2004)	วัฒนธรรมของการทำงานร่วมกันประกอบไปด้วย (1) ความไว้ใจ (2) ความร่วมมือ (3) การแลกเปลี่ยนข้อมูล (4) การสื่อสารและความเข้าใจ (5) การเปิดใจและความซื่อสัตย์ แต่จากการขาดความเข้าใจในความหมายขององค์ประกอบเหล่านี้ทำให้การทำงานร่วมกันภายใต้สภาวะของธุรกิจที่มีลักษณะเป็น e-business ที่เป็นโซลูชันสำหรับการทำงานระหว่างองค์กรในปัจจุบัน
Simatupang et al. (2004)	ความร่วมมือกันเป็นกลยุทธ์ของความร่วมมือกันของคู่ค้าในโซ่อุปทานที่มีเป้าหมายร่วมกันในการให้บริการแก่ลูกค้าด้วยวิธีการที่ร่วมกันอันจะก่อให้เกิดต้นทุนที่ต่ำลงและรายได้ที่เพิ่มขึ้น
Samaddar and Kadiyala, 2006	ความสัมพันธ์ในการร่วมมือกันเป็นปัจจัยหนึ่งขององค์กรที่ริเริ่มและนำไปสู่ความพยายามในการสร้างความรู้ร่วมกัน และองค์กรที่มีความร่วมมือกันจะมีการแบ่งปันค่าใช้จ่ายและผลประโยชน์จากการที่ได้สร้างความรู้ร่วมกันซึ่งอาจจะรวมไปถึงการร่วมกันในการจดสิทธิบัตรและลิขสิทธิ์ต่างได้
Fawcett *et al.* 2008	ความสามารถที่จะทำงานตามขอบเขตขององค์กรในการสร้างและจัดการกระบวนการในการสร้างมูลค่าที่เป็นหนึ่งเดียวเพื่อที่จะได้นำไปสู่ความต้องการของลูกค้าที่ดีกว่า

ตารางที่ 2.3 (ต่อ)

แหล่งที่มา	ความหมายของความร่วมมือกันของโซ่อุปทานดิจิทัล
Simatupang and Sridharan (2008)	ความร่วมมือกันเป็นการอธิบายถึงความร่วมมือกันระหว่างบริษัทต่างๆ ที่เป็นอิสระต่อกัน แต่ได้เข้ามาร่วมมือกันในการที่แบ่งปันทรัพยากร และความสามารถในการที่จะตอบสนองต่อลูกค้าที่พิเศษที่สุดหรือไม่ก็มีความต้องการที่เปลี่ยนแปลงไปอยู่ตลอดเวลา
Cao et al.(2010)	ประกอบด้วยองค์ประกอบ 7 ประการที่เชื่อมต่อถึงกัน ได้แก่ (1) การแบ่งปันข้อมูลร่วมกัน (2) การมีเป้าหมายที่สอดคล้องกัน (3) การประสานกันในการตัดสินใจ (4) การมีแรงจูงใจร่วมกัน (5) การแบ่งปันทรัพยากรร่วมกัน (6) ความร่วมมือกันในการสื่อสาร และ (7) การสร้างความรู้ร่วมกัน โดยที่การสื่อสารใดๆ ระหว่างคู่ค้าในโซ่อุปทานที่ผิดพลาดย่อมทำให้เกิดความเข้าใจที่ขัดแย้งกันภายในโซ่อุปทาน ซึ่งจะเป็นผลทำให้เกิดความล้มเหลวในการร่วมมือกันในการดำเนินงาน ความร่วมมือกันในโซ่อุปทานไม่ได้เป็นเพียงแค่การทำธุรกรรมร่วมกัน แต่จะต้องเพิ่มเติมในเรื่องของการแบ่งปันข้อมูลร่วมกันและสร้างความรู้ร่วมกันด้วย
Cao and Zhang, 2011	กระบวนการความร่วมมือของบริษัท 2 บริษัทหรือมากกว่าที่จะทำงานร่วมกันอย่างใกล้ชิดในการวางแผนและดำเนินการกิจกรรมทางด้านโซ่อุปทานด้วยเป้าหมายและผลประโยชน์ร่วมกัน
Maria E. Aviles (2015)	ความสัมพันธ์ร่วมกัน จะเป็นการให้ความสัมพันธ์ที่เกิดขึ้นจากความร่วมกันระหว่างองค์กร ซึ่งจะประกอบไปด้วย (1) กิจกรรมของความสัมพันธ์ ประกอบไปด้วย การประสานงาน การร่วมมือ และกิจกรรมร่วมกันระหว่างคู่ค้า (2) ข้อผูกมัด (3) ความไว้ใจ (4) การให้รางวัล/การแบ่งปันต้นทุน (5) การสื่อสาร และ (6) การแบ่งปันข้อมูลร่วมกัน
Scholten et al. (2015)	กิจกรรมของความร่วมมือกัน ประกอบด้วย (1) การแบ่งปันข้อมูลร่วมกัน (2) ความร่วมมือกันในการสื่อสาร (3) การสร้างความรู้ร่วมกัน และ (4) ความพยายามในการสร้างความสัมพันธ์ร่วมกัน โดยทั้งหมดนี้เป็นกิจกรรมของความร่วมมือกันในโซ่อุปทานที่ได้เพิ่มการคืนสภาพได้ของโซ่อุปทานด้วย

จากการศึกษาของ Kwon and Suh (2004) ได้พยายามที่จะทำการสังเกตถึงความถูกต้องของความสัมพันธ์ระหว่างความไว้ใจและความมุ่งมั่นในบริบทของโซ่อุปทาน ผลลัพธ์ที่ได้แสดงให้เห็นว่า ความไว้ใจมีความสัมพันธ์เชิงบวกต่อสินทรัพย์โดยเฉพาะในเรื่องของการลงทุน และมีความสัมพันธ์เชิงลบต่อลักษณะพฤติกรรมที่ไม่แน่นอน โดยมี Simatupang et al. (2004) ได้ทำการตรวจสอบข้อจำกัดในความร่วมมือกันในโซ่อุปทานและได้มีการนำเอาทฤษฎีแห่งข้อจำกัด (Theory of Constraints – TOC) มาใช้เพื่อดูผลจากความยุ่งยากจากการปล่อยให้เกิดมีผลประโยชน์ร่วมกันจากความร่วมมือกันในโซ่อุปทาน ทั้งนี้ Crook et al. (2008) ได้เสนอไว้ว่า เมื่อบริษัทต่างๆ ได้ร่วมมือกันและแบ่งปันความรู้ระหว่างกันแล้วนั้น บริษัทเหล่านั้นจะสามารถสร้างความได้เปรียบจากการแข่งขันนอกเหนือไปจากการแลกเปลี่ยนที่จะเกิดขึ้นระหว่างคู่ค้าด้วยกันเอง Fawcett et al. (2008) ได้นำเอาปัญหาจากทฤษฎีเชิงสถานการณ์ (Contingency Theory) และ ทฤษฎีแรงเสริม แรงต้าน (Force Field Theory) มาประยุกต์ใช้ในการศึกษาถึงการเอาชนะต่อุปสรรคทางวัฒนธรรมและโครงสร้างที่มีผลต่อความร่วมมือกันในโซ่อุปทานได้อย่างมีประสิทธิภาพ จากการศึกษาของ Forslund and Jonsson (2009) ได้มีการอธิบายถึงระดับของอุปสรรคที่จะมีผลต่อความสัมพันธ์ในโซ่อุปทานและเครื่องมือสำหรับการปฏิบัติการที่จะขัดขวางต่อการบูรณาการร่วมกันของโซ่อุปทานสำหรับการจัดการทางด้านประสิทธิภาพ โดยที่ การศึกษาของ Nyaga et al. (2010) ได้ทำการศึกษาเพื่อหาปัจจัยที่จะทำให้เกิดความความสำเร็จ ในการร่วมมือกันในโซ่อุปทาน ซึ่ง Chen et al (2011) ได้ตรวจสอบถึง ปัจจัยทางด้านการแบ่งปันข้อมูล คุณภาพของข้อมูล และความพร้อมสำหรับการนำไปใช้งานของข้อมูลในการพัฒนาถึงความไว้ใจและความมุ่งมั่นในความสัมพันธ์ของโซ่อุปทาน และ Fawcett *et al.* (2011) ได้พบว่าผู้จัดการจะมีความเข้าใจในธรรมชาติของความไว้ใจหรือการเปลี่ยนแปลงของการสร้างความไว้วางใจ รวมไปถึง Liu and Wang (2011) ที่ได้ทำการวิเคราะห์ถึงวิกฤตการณ์ที่จะเกิดขึ้นในโซ่อุปทานได้รวมไปถึงสาเหตุของการเกิดขึ้นจากความร่วมมกันในโซ่อุปทาน แล Lee et al. (2011) ได้ตรวจสอบถึงปัญหาจากการประสานงาน การร่วมมือกันและกลไกของแรงจูงใจที่สอดคล้องกันระหว่างผู้ผลิตและผู้ค้าปลีกสำหรับการร่วมลงทุนในเทคโนโลยีใหม่ ที่มีประสิทธิภาพในการพัฒนาถึงประสิทธิภาพและความปลอดภัยในโซ่อุปทาน

2.3.2 องค์ประกอบของความร่วมมือของโซ่อุปทานดิจิทัล

ผู้วิจัยได้ทำการทบทวนวรรณกรรม และทำการสังเคราะห์วรรณกรรมที่เกี่ยวกับความร่วมมือกันของโซ่อุปทานดิจิทัล โดยตารางที่ 2.4 ได้แสดงตัวแปรความร่วมมือกันของโซ่อุปทานกับการคืนสภาพได้ของโซ่อุปทานและแหล่งอ้างอิง

ตารางที่ 2.4 ตัวแปรความร่วมมือกันของโซ่อุปทานกับการคืนสภาพได้ของโซ่อุปทานและแหล่งอ้างอิง

แหล่งอ้างอิง	การแบ่งปันข้อมูล	ความไว้ใจ	ความร่วมมือกันในการสื่อสาร	การสร้างความรู้ร่วมกัน
Cai *et al.* (2010)	✓	✓		
Cao and Zhang, (2011)	✓		✓	✓
Chen *et al.* (2011)	✓	✓		
Kwon and Suh, (2004)	✓	✓		
Nyaga *et al.* (2010)	✓	✓		
Simatupang and Sridharan, (2005)	✓			
Simatupang and Sridharan, (2002)	✓			
Simatupang and Sridharan, (2008)	✓			
Fynes *et al.* (2005)		✓	✓	
Fawcett *et al.* (2008)		✓		✓
Forslund and Jonsson, (2009)		✓	✓	
Zacharia et al. (2009)		✓		✓

สำหรับการวิจัยครั้งนี้ ผู้วิจัยจึงได้สรุปความหมายของคำว่า ความร่วมมือกันของโซ่อุปทาน หมายถึง กิจกรรมของความร่วมมือกันระหว่างองค์กรด้วยกัน โดยจะประกอบไปด้วย การแบ่งปันข้อมูลร่วมกัน (Information Sharing) การไว้ใจ (Trust) ความร่วมมือกันในการสื่อสาร (Collaborative Communication) และการสร้างความรู้ร่วมกัน (Knowledge Sharing) ซึ่งผู้วิจัยสามารถอธิบายได้ดังต่อไปนี้

1. การแบ่งปันข้อมูลร่วมกัน (Information Sharing)

การแบ่งปันข้อมูลร่วมกัน หมายถึง การแลกเปลี่ยนข้อมูลที่สำคัญที่เป็นกรรมสิทธิ์ของอีกฝ่ายหนึ่งระหว่างสมาชิกของโซ่อุปทานด้วยกันเองผ่านทางสื่อต่างๆ ไม่ว่าจะเป็นทางการประชุม ทางโทรศัพท์ โทรสาร ไปรษณีย์ รวมไปถึงทางอินเทอร์เน็ต ซึ่งบริษัทต่างๆ จะมีการแบ่งปันข้อมูลที่หลากหลาย ทั้งที่เป็นเรื่องที่มีความเกี่ยวข้องกัน ข้อมูลที่มีความถูกต้อง ความ

สมบูรณ์ของข้อมูล รวมไปถึงข้อมูลที่เป็นความลับ ในช่วงเวลาต่างๆ ที่เหมาะสมระหว่างคู่ค้าทางโซ่อุปทานด้วยกัน (Cai *et al.* (2010); Cao and Zhang, (2011); Chen *et al.* (2011); Kwon and Suh, (2004); Nyaga *et al.* (2010); Simatupang and Sridharan, (2005); Simatupang and Sridharan, (2002); Simatupang and Sridharan, (2008))

2. ความไว้ใจ (Trust)

ความไว้ใจ หมายถึง ความเชื่อในเชิงบวก ทัศนคติ หรือความคาดหวังของอีกฝ่ายหนึ่งที่เกี่ยวกับความเป็นไปได้ว่า การกระทำหรือผลลัพธ์ที่เกิดจากอีกฝ่ายหนึ่งจะเป็นที่น่าพอใจ (Cai *et al.* (2010); Chen *et al.* (2011); Kwon and Suh, (2004); Nyaga *et al.* (2010); Fynes *et al.* (2005); Fawcett *et al.* (2008); Forslund and Jonsson, (2009); Zacharia et al. (2009))

3. ความร่วมมือกันในการสื่อสาร (Collaborative Communication)

ความร่วมมือกันในการสื่อสาร หมายถึง กระบวนการในการติดต่อหรือรับส่งข้อความระหว่างคู่ค้าในโซ่อุปทานซึ่งจะมีกลยุทธ์ต่างๆ กันไป ที่นำมาใช้สำหรับการสื่อสารระหว่างกันได้แก่ ความถี่ ทิศทาง รูปแบบ และ อิทธิพล (Cao and Zhang, (2011); Fynes *et al.* (2005); Forslund and Jonsson, (2009))

4. การสร้างความรู้ร่วมกัน (Knowledge Sharing)

การสร้างรู้ร่วมกัน หมายถึง ขอบเขตที่คู่ค้าของโซ่อุปทานพัฒนาความเข้าใจที่ดีขึ้นและมีการตอบสนองต่อตลาดและสภาพแวดล้อมทางการแข่งขันด้วยการทำงานร่วมกัน (Cao and Zhang, (2011); Fawcett *et al.* (2008); Zacharia et al. (2009))

2.4 การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

2.4.1 ความเสี่ยงของโซ่อุปทาน

ความเสี่ยง (Risk) คือ การวัดความสามารถ ที่จะดำเนินการให้วัตถุประสงค์ของงานประสบความสำเร็จ ภายใต้การตัดสินใจ งบประมาณ กำหนดเวลา และข้อจำกัดด้านเทคนิคที่เผชิญอยู่ อย่างเช่น การจัดทำโครงการเป็นชุดของกิจกรรม ที่จะดำเนินการเรื่องใดเรื่องหนึ่งในอนาคต โดยใช้ทรัพยากรที่มีอยู่อย่างจำกัด มาดำเนินการให้ประสบความสำเร็จ ภายใต้กรอบเวลาอันจำกัด ซึ่งเป็นกำหนดการปฏิบัติการในอนาคต ความเสี่ยงจึงอาจเกิดขึ้นได้ตลอดเวลา อันเนื่องมาจากความไม่แน่นอน และความจำกัดของทรัพยากรโครงการ ผู้บริหารโครงการจึงต้องจัดการความเสี่ยงของโครงการ เพื่อให้ปัญหาของโครงการลดน้อยลง และสามารถดำเนินการให้ประสบความสำเร็จ ตามเป้าหมายที่ตั้งไว้อย่างมีประสิทธิผลและประสิทธิภาพ การจัดการความเสี่ยงหรือ การบริหารความเสี่ยง (Risk Management) คือ การจัดการความเสี่ยง ทั้งในกระบวนการ

ในการระบุ วิเคราะห์ (Risk Analysis) ประเมิน (Risk Assessment) ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับ กิจกรรม หน้าที่และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง หรือเรียกว่าอุบัติภัย (Accident)

ถ้าหากว่าการจัดการเหตุฉุกเฉินจะเกี่ยวข้องกับประเด็นทางด้านความเสี่ยง การหยุดชะงัก และการกู้คืนที่ระดับมหภาคของชุมชน สังคม และ มนุษยชาติโดยทั่วไป การบริหารความเสี่ยงก็จะมีลักษณะที่ปัญหาเดียวกันจากมุมมองธุรกิจ งานวิจัยที่เกี่ยวกับการจัดการโซ่อุปทานได้เกิดขึ้นมามากกว่าสิบปีแล้ว แต่งานวิจัยทางด้านการจัดการความเสี่ยงก็ได้เกิดขึ้นมาก่อนหน้านั้น แต่เกิดขึ้นในมุมมองอื่น ที่ผ่านมานั้นได้มีงานวิจัยที่ชี้ให้เห็นถึงความสำคัญที่เพิ่มขึ้นของการวิจัยทางด้านการจัดการความเสี่ยง และเป็นสิ่งที่แสดงให้เห็นว่าการจัดการความเสี่ยงของโซ่อุปทานก็อยู่ในความสนใจในระดับต้น ๆ เช่นเดียวกัน โดยงานวิจัยใหม่นี้ได้มีการพัฒนาที่จุดที่เชื่อมกันระหว่างการจัดการโซ่อุปทานและการจัดการทางด้านความเสี่ยง (Paulsson, 2004) การคืนสภาพได้ของโซ่อุปทานจะเกี่ยวข้องกับความเสี่ยงในหลาย ๆ ประเภท และหลาย ๆ ขั้นตอนของกระบวนการการจัดการความเสี่ยง โดยสามารถเกิดขึ้นได้ในทุกๆ หน่วยของการวิเคราะห์ที่เกิดขึ้นในโซ่อุปทาน เพราะการคืนสภาพได้เป็นหนึ่งในองค์ประกอบหลักของการจัดการความเสี่ยงในโซ่อุปทาน ดังนั้นจึงเป็นประเด็นหนึ่งที่จะต้องทำการตรวจสอบถึงการจัดการความเสี่ยง เพื่อตรวจสอบดูว่าควรจะรวมอยู่ในกรอบแนวคิดของการคืนสภาพได้ได้อย่างไร

ในปัจจุบันนี้การให้คำนิยามของการจัดการความเสี่ยงในโซ่อุปทานยังไม่เป็นที่ยอมรับ (Christopher et al., 2003) ได้ให้นิยามของความเสี่ยงของโซ่อุปทานความหมายว่าเป็นความเสี่ยงใด ๆ ที่มีผลต่อข้อมูล วัตถุดิบ และ การไหลของสินค้าจากผู้จำหน่ายเริ่มต้นและจัดส่งไปเป็นสินค้าในหน่วยสุดท้าย ในขณะที่ Norrman and Lindroth (2004) ชี้ให้เห็นว่าการจัดการความเสี่ยงในโซ่อุปทาน จะเป็นเรื่องที่เกี่ยวข้องกับการใช้งานร่วมกันต่อเครื่องมือที่ใช้ในกระบวนการการจัดการความเสี่ยง เพื่อวัตถุประสงค์ในการจัดการกับความไม่แน่นอนที่เกี่ยวข้องกับกิจกรรมโลจิสติกส์ โดยที่คำนิยามนี้ได้มีการแนะนำบางประการที่สำคัญ เช่นการทำงานร่วมกัน มุมมองตามกระบวนการ และ ความสำคัญขององค์ประกอบโลจิสติกส์เป็นประเด็นหลักของการบริหารความเสี่ยงในโซ่อุปทาน Juttner et al. (2003) and Juttner (2005) ได้นิยามความหมายของการจัดการความเสี่ยงในโซ่อุปทาน ซึ่งได้ถูก (Manuj and Mentzer 2008) นำมาใช้และขยายความในคำนิยามของการจัดการความเสี่ยงในโซ่อุปทานมากยิ่งขึ้น จากคำนิยามของผู้วิจัยที่ได้ทำการศึกษามาก่อนหน้านั้น ผู้วิจัยจึงได้สรุปนิยามความหมายของการจัดการความเสี่ยงของโซ่อุปทาน โดยการจัดการความเสี่ยงของโซ่อุปทาน หมายถึง การสามารถที่จะจำแนกได้ถึงแหล่งของความเสี่ยงที่มีศักยภาพ

และการนำไปใช้ในกลยุทธ์ที่เหมาะสมผ่านวิธีการประสานงานระหว่างสมาชิกในโซ่อุปทาน เพื่อลดภัยคุกคามและช่องโหว่ในโซ่อุปทาน

จำนวนของแนวโน้มที่สำคัญ ซึ่งเป็นส่วนสำคัญที่เพิ่มขึ้นของการจัดการความเสี่ยงในโซ่อุปทานในช่วงทศวรรษที่ผ่านมา แนวโน้มดังกล่าวที่ว่านั้นได้แก่ โลกที่อยู่ภายใต้ความเป็นโลกาภิวัตน์ (Globalization) การจ้างงานภายนอก (Outsourcing) การเปลี่ยนให้ไปสู่ความเรียบง่ายและการดำเนินงานคล่องตัว และเพิ่มการก่อการร้ายและภัยคุกคามอื่น ๆ งานวิจัยที่ผ่านมาที่ได้มีการศึกษาไว้ก่อนหน้านั้น ที่ได้ถูกตีพิมพ์มีหลาย ๆ งานวิจัย ได้มีการจำแนกถึง ความเสี่ยง ภัยคุกคามและการหยุดชะงัก ไว้ทั้งหมด ตัวอย่างเช่น Manuj and Mentzer (2008) ได้ทำการศึกษางานวิจัยที่มีอยู่ทั้งหมดของโซ่อุปทาน และสาขาอื่น ๆ ที่มีความเกี่ยวข้อง และนำมาเสนอเป็นตัวแบบสำหรับการจัดการความเสี่ยงโดยทั่ว ๆ ไป ซึ่งจะมีด้วยกันทั้งหมด 5 ขั้นตอนได้แก่ การจำแนกของความเสี่ยง (Risk Identification) การประเมินความเสี่ยงและการประเมินผล (Risk Assessment and Evaluation) การเลือกกลยุทธ์ในการจัดการความเสี่ยงที่เหมาะสม (Selection of Appropriate Risk Management Strategies) การดำเนินการนำเอากลยุทธ์ไปปฏิบัติ (Strategy Implementation) และการบรรเทาผลกระทบของความเสี่ยงในโซ่อุปทาน (Mitigation of Supply Chain Risks)

นอกจากนี้ Manuj and Mentzer (2008) ยังได้มีการนำเสนอถึงการจำแนกความเสี่ยงที่มีอยู่ด้วยกันทั้ง 4 ประเภท คือ การจัดหา (Supply) การปฏิบัติการ (Operation) ความต้องการ (Demand) และ ความปลอดภัย (Security) ในขณะที่การศึกษาถึงความเสี่ยงในหลาย ๆ โซ่อุปทานอยู่นอกเหนือขอบเขตของการตรวจสอบนี้ กรอบที่เสนอโดย Norrman and Lindroth (2004) แสดงให้เห็นถึงความซับซ้อนของปัญหา และมีศักยภาพที่โตขึ้นของงานวิจัยทางด้านการจัดการความเสี่ยงในโซ่อุปทาน มิติหลัก ๆ จะมีอยู่ด้วยกัน 3 มิติคือ หน่วยของการวิเคราะห์ (Unit of Analysis), ประเภทของความเสี่ยง/ความไม่แน่นอน, และขั้นตอนของกระบวนการการบริหารความเสี่ยง ซึ่ง Norrman and Lindroth ได้นำมาใช้เพื่อศึกษา โดยได้แสดงให้เห็นถึงลักษณะหลายมิติของงานวิจัยความเสี่ยงการจัดการโซ่อุปทาน

จากการศึกษาของ Paulsson (2004) ที่ได้ทำการทบทวนวรรณกรรมจากบทความกว่า 400 บทความที่ไม่ซ้ำกันที่เกี่ยวข้องกับโซ่อุปทานและการบริหารความเสี่ยงที่ตีพิมพ์ในวารสารทางวิทยาศาสตร์ สรุปได้ว่าขอบเขตของการจัดการความเสี่ยงของโซ่อุปทานมีหลายขอบเขตย่อย แต่สิ่งที่มีเหมือนกันได้แก่ การจัดการ การไหลของความเสี่ยงที่เกี่ยวข้องกันในโซ่อุปทาน Richie and Brindley (2004) ได้สรุปว่าในขณะที่มีคำนิยามที่แตกต่างกันจำนวนมากมายที่เกี่ยวกับความเสี่ยงของโซ่อุปทานและการจัดการความเสี่ยง และความแตกต่างเหล่านี้จะเป็นดูเหมือนว่าไม่ใช่นิยามที่แท้จริงของทั้งความเสี่ยงและการจัดการความเสี่ยงของโซ่อุปทานก็ตาม แต่ความจริงแล้ว

ความแตกต่างกันเหล่านี้ จะเป็นข้อมูลที่นำไปสู่ประเด็นและความลึกของการวิจัยเพื่อนำไปต่อยอดงานวิจัย ซึ่งจะช่วยให้การจัดการความเสี่ยงในโซ่อุปทานเป็นสาขาวิชาความรู้ใหม่ที่ถูกต้องและมีคุณค่าสำหรับการศึกษาต่อไป นอกจากนี้ยังบ่งบอกถึงการศึกษาในสาขาวิชาที่เกิดขึ้นใหม่ซึ่งจำเป็นต้องมีการนิยามที่รวมกัน สาขาวิชาที่เกิดขึ้นใหม่เติบโตโดยการวิจัยโครงสร้างใหม่และการสร้างทฤษฎีใหม่ ความยืดหยุ่นโซ่อุปทานเป็นหนึ่งในโครงสร้างเช่นเดียวกันกับการบริหารความเสี่ยงในโซ่อุปทาน

จากการศึกษาของ Christopher and Lee (2004) ได้ให้ข้อเสนอแนะว่า วิธีที่ดีที่สุดในการจัดการกับความเสี่ยงในโซ่อุปทาน คือการเพิ่มความเชื่อมั่นในโซ่อุปทาน ความเชื่อมั่นในโซ่อุปทานจะเกิดขึ้นได้ก็ต่อเมื่อ โซ่อุปทานจะมีความสามารถในการเปลี่ยนสภาพคืนกลับสู่สภาวะปกติจากการที่ต้องเผชิญกับการเปลี่ยนแปลงที่ส่งผลกระทบต่อการดำเนินงาน จะเห็นได้ว่าประเด็นดังกล่าวนี้ ได้สะท้อนให้เห็นถึงองค์ประกอบของการคืนสภาพได้ ที่สามารถตั้งข้อสังเกตได้ว่าการจัดการความเสี่ยงก็ได้ถูกพิจารณาอยู่ในมุมมองของระบบนิเวศเช่นเดียวกัน นอกจากนี้ Christopher and Lee ยังได้เสนออีกว่าความเชื่อมั่นในโซ่อุปทาน จะได้รับความเชื่อมั่นเพิ่มขึ้นถ้าความเชื่อมั่นดังกล่าวนั้นได้มีการปฏิบัติการโดยผ่านการมองเห็น (Visibility) และการควบคุม กลไกหนึ่งในการควบคุมที่เพิ่มขึ้นคือการจัดการเหตุการณ์ที่เป็นการจัดการต่อเหตุการณ์ที่มีมาก่อนหน้านั้นโดยจำกัดให้อยู่ ณ จุดหรือรอยต่อของความเชื่อมโยงที่สำคัญ ที่ถูกใช้ในการจัดการต่อการไหลของวัตถุดิบที่มีต่อเครือข่ายนั้น ๆ ในกรณีที่กิจกรรมเกินขีดจำกัด การควบคุมการแจ้งเตือนจะถูกส่งไปที่สมาชิกของโซ่อุปทานที่เฉพาะเจาะจงเพื่อให้สามารถการดำเนินการแก้ไขกับกรณีดังกล่าว ดังนั้นการจัดการเหตุการณ์ จึงหมายถึงการตรวจสอบ การรายงาน และการตอบสนองต่อปัญหาที่เกิดขึ้นในโซ่อุปทานอย่างเหมาะสม โซ่อุปทานที่มีระบบการจัดการเหตุการณ์ที่มีประสิทธิภาพนั้น จะทำให้สามารถที่จะลดความเสี่ยงและปรับปรุงการดำเนินงานอย่างมีนัยสำคัญโดยการให้ข้อมูลเกี่ยวกับการเปลี่ยนแปลงสภาพที่อาจจะใช้เวลานานกว่าที่จะรับรู้และตอบสนอง (Stiles, 2002)

2.4.2 การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน (Cyber Supply Chian Risk Management: CSCRM) เป็นสิ่งที่เกิดขึ้นใหม่ โครงสร้างการจัดการเป็นผลมาจากการผสมผสานของแนวคิด วิธีการ และการปฏิบัติ จากแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ที่องค์กรได้นำมาใช้เพื่อการจัดการความเสี่ยงและการจัดการโซ่อุปทาน (Boyson S, 2014) จากในอดีตที่ผ่านการจัดการความเสี่ยงของโซ่อุปทานมีวิวัฒนาการขึ้นมาเป็นลำดับ โดยผู้วิจัยสามารถสรุปถึงแนวทางในการจัดการความเสี่ยงของโซ่อุปทานได้ดังตารางที่ 2.5

ตารางที่ 2.5 วิวัฒนาการของการจัดการความเสี่ยงของโซ่อุปทานดิจิทัล

แนวทางการจัดการความเสี่ยง	ลำดับเหตุการณ์
1. การบริหารความเสี่ยงในองค์กร (Enterprise Risk Management: ERM) "กระบวนการที่ได้รับผลกระทบจากคณะกรรมการ ผู้บริหาร และบุคลากรอื่นๆ ขององค์กร ที่ใช้ในการกำหนดกลยุทธ์และทั่วทั้งองค์กรออกแบบมาเพื่อระบุเหตุการณ์ที่อาจเกิดขึ้นซึ่งอาจส่งผลกระทบต่อกิจการและจัดการความเสี่ยงให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ การประกันที่สมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร"	1995 – การพัฒนามาตรฐานการจัดการความเสี่ยงของสถาบันการเงินในออสเตรเลียซึ่งได้ถูกนำมาใช้ในแคนาดา (1997) และในสหราชอาณาจักร (2000) 1996 – สมาคมนายทะเบียนประกันภัย (National Association of Insurance Commissioners: NAIC) ในสหรัฐอเมริกา แนะนำความต้องการด้านการลงทุนตามความเสี่ยงสำหรับบริษัทประกันภัย 2002 – มีการผ่านพระราชบัญญัติ Sarbanes - Oxley Act ในสหรัฐอเมริกา ให้กำกับดูแลความเสี่ยงขององค์กรที่มีการปฏิบัติด้านการบัญชีขององค์กร 2004 – COSO ERM กรอบการบริหารความเสี่ยงในองค์กรได้ถูกนำไปใช้เป็นมาตรฐานในการจัดการความเสี่ยงในระดับโลก
2. การจัดการโซ่อุปทาน (Supply Chain Management) "การจัดการโซ่อุปทานเป็นฟังก์ชันการบูรณาการที่มีความรับผิดชอบหลักสำหรับการเชื่อมโยงฟังก์ชันทางธุรกิจที่สำคัญและกระบวนการทางธุรกิจภายในและระหว่างบริษัท ในรูปแบบธุรกิจที่มีความสัมพันธ์กันอย่างเหนียวแน่นและมีประสิทธิภาพสูง รวมถึงกิจกรรมการจัดการโลจิสติกทั้งหมด เช่นเดียวกับการดำเนินการผลิตและขับเคลื่อนให้เกิดการประสานกันระหว่างกระบวนการและกิจกรรมภายใน ทั้งงานด้านการตลาด การขาย การออกแบบผลิตภัณฑ์ การเงิน และเทคโนโลยีสารสนเทศ"	1982 – Booz Allen Hamilton ที่ปรึกษาแห่ง Keith Oliver ได้ให้กำเนิดคำว่า "การจัดการโซ่อุปทาน" 1995 – มหาวิทยาลัยแห่งรัฐแมรีแลนด์ทำการศึกษาวิจัยโครงการเพิ่มเติมเกี่ยวกับเอกสารของงานด้านการจัดการโซ่อุปทาน ซึ่งไม่ได้เป็นเพียงแค่การศึกษาความสัมพันธ์ที่เกิดขึ้นภายในองค์กรเท่านั้น แต่ยังได้ศึกษาเพิ่มเติมไปยังภายนอกในส่วนลูกค้าและผู้จำหน่าย งานวิจัยได้ทำการสำรวจจากบริษัท 1300 บริษัท ที่เป็นงานในส่วนของโลจิสติกส์และธุรกรรมที่มีการต่อยอด (Boysonetal., 1999) โดยผลงานวิจัยได้ถูกเผยแพร่ปี 1999 1996 – สภาซัพพลายเชน (Supply Chain Council: SCC) ได้ถูกจัดตั้งขึ้นจากบริษัทที่ร่วมก่อตั้ง 69 บริษัท และได้พัฒนาแบบจำลองอ้างอิงการดำเนินงานในโซ่อุปทาน (SCOR Model) โดยใช้เป็นกรอบและมาตรฐานสำหรับ

ตารางที่ 2.5 (ต่อ)

แนวทางการจัดการความเสี่ยง	ลำดับเหตุการณ์
	เพื่อใช้สำหรับการจัดการโซ่อุปทาน 2002 – สภาการจัดการโลจิสติกส์ (Council of Logistics Management) ได้เปลี่ยนชื่อเป็น สภาผู้เชี่ยวชาญด้านการจัดการโซ่อุปทาน (Council of Supply Chain Management Professionals) ในการตระหนักถึงบทบาทสำคัญที่เกิดขึ้นใหม่ของโซ่อุปทาน
3. ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) “ความมั่นคงปลอดภัยไซเบอร์ คือ ส่วนหนึ่งของเทคโนโลยี กระบวนการ และวิธีการปฏิบัติ ที่ถูกออกแบบมาเพื่อปกป้องเครือข่ายคอมพิวเตอร์ โปรแกรม และข้อมูลจากการโจมตีความเสียหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต”	1969 – สมาชิก 3 รายของthe British Communications Headquarters ได้คิดค้นอัลกอริธึมคีย์อสมาตร (asymmetric key algorithms) ขึ้นเป็นชุดแรก ซึ่งต่อมาได้ถูกพัฒนารวมเข้ากับเทคนิคที่เรียกว่า “non-secret encryption” หรือ “public-key cryptography” 1970 – RAND Report R-609, “Security Controls for Computer Systems” (หรือที่รู้จักในนาม “The Ware Report”) ถูกเผยแพร่ เพื่อที่จะกำหนดและแนะนำแนวทางการรักษาความมั่นคงปลอดภัยที่ – กลไกการป้องกันที่จำเป็นที่ใช้ในการป้องกันข้อมูลที่เป็นความลับที่ต้องถูกเก็บไว้ในระบบที่มีการแบ่งปันการใช้ทรัพยากรร่วมกัน ซึ่งยังได้รวมถึงมาตรฐานความมั่นคงปลอดภัยและการควบคุมที่สำคัญที่มีต่อระบบด้วย 1983 – ได้มีการเผยแพร่เวอร์ชันแรกของ the Trusted Computer Security Evaluation Criteria

ตารางที่ 2.5 (ต่อ)

แนวทางการจัดการความเสี่ยง	ลำดับเหตุการณ์
	(TCSEC) ที่รู้จักกันในนาม “Orange Book” โดยที่ Orange Book ได้กลายมาเป็นมาตรฐานการสำคัญในการป้องกันความมั่นคงปลอดภัยของสหรัฐอเมริกาในปี 1985 อีกทั้งยังได้จัดทำถึงคำแนะนำด้านเทคนิคเกี่ยวกับความมั่นคงปลอดภัยและระเบียบวิธีที่ใช้ในระบบการประเมินความมั่นคงปลอดภัย 1987 – รัฐสภาคองเกรสแห่งสหรัฐอเมริการได้ผ่านพระราชบัญญัติความมั่นคงปลอดภัยทางคอมพิวเตอร์ ปี 1987 เพื่อส่งเสริมการจัดตั้งวิธีปฏิบัติด้านความมั่นคงปลอดภัยขั้นต่ำสำหรับระบบคอมพิวเตอร์ของรัฐบาลกลาง รวมถึงการพัฒนาถึงแผนการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ที่ปรับปรุงแล้ว เพื่อใช้สำหรับข้อมูลที่มีความอ่อนไหวง่าย 2013 – ประธานาธิบดี บารัค โอบาม่า ได้ลงนามในคำสั่งผู้บริหารเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และได้ให้สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) พัฒนากรอบความมั่นคงปลอดภัยไซเบอร์สำหรับรัฐบาลกลางของสหรัฐอเมริการ และได้มีการเผยแพร่ครั้งแรกเมื่อ สิงหาคม 2013

จากตารางที่ 2.5 จะเห็นว่าในแต่ละแนวทางของการจัดการความเสี่ยงได้มีการพัฒนาโดยแยกเป็นอิสระออกจากกัน สำหรับการบริหารความเสี่ยงในองค์กร (ERM) จะเน้นในอุตสาหกรรมบริการทางการเงินเป็นส่วนใหญ่และได้พยายามที่จะคาดการณ์ถึงผลกระทบใด ๆ ที่สามารถส่งผลกระทบต่อรายได้และผลประโยชน์ที่เกิดขึ้นของบริษัท ในช่วงระหว่างที่เกิด

เหตุการณ์ 9/11 ภาคธุรกิจอื่น ๆ เช่นภาคการผลิตทั่วโลกและการผลิตพลังงาน ได้นำเอาแนวทางการบริหารความเสี่ยงขององค์กรมาใช้ เพื่อตรวจสอบและลดความเสี่ยงด้านกลยุทธ์และการดำเนินงาน สำหรับแนวทางด้านการจัดการโซ่อุปทานได้มีการเริ่มต้นและพัฒนาแนวทางการจัดการความเสี่ยงในภาคการผลิต จากนั้นจึงได้มีการปรับปรุงพัฒนาและพัฒนาเพื่อนำมาใช้สำหรับการจัดการในองค์กรบริการทุกประเภท สำหรับแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ได้มีการพัฒนาออกมาจากต้นกำเนิดของธุรกิจ การรวมระบบไอทีและชุดเครื่องมือ ซึ่งได้รับการใช้ประโยชน์จากบริษัทและรัฐบาลต่าง ๆ รอบโลก จะเห็นได้ว่าในแต่ละแนวทางที่กล่าวมานั้นได้สร้างขึ้นจากรากฐานทางทฤษฎีของตัวเอง จากชุมชนที่แตกต่างของตัวเองผู้ปฏิบัติงาน ผู้เชี่ยวชาญ ลำดับชั้นของมาตรฐาน และแนวทางการปฏิบัติที่ดีที่สุด

โครงสร้างของการจัดการความเสี่ยงทางไซเบอร์ ได้เกิดขึ้นมาเพื่อตอบสนองต่อความต้องการเร่งด่วนของสถาปัตยกรรมทางด้านเทคโนโลยี ในการกำหนดกลยุทธ์และชุดเครื่องมือเพื่อควบคุม ออกแบบ การสร้าง และการปรับใช้งานอย่างมีประสิทธิภาพ รวมไปถึงระบบฮาร์ดแวร์และซอฟต์แวร์ และส่วนประกอบต่าง ๆ ที่ไม่รู้ระบบการทำงาน รวมไปถึงข้อมูล และสภาพแวดล้อมเครือข่ายที่มีความไม่แน่นอน

เช่นเดียวกับโซ่อุปทานของผลิตภัณฑ์ทั่ว ๆ ไป โซ่อุปทานไซเบอร์ (Cyber Supply Chain) เป็นกระบวนการแบบ end-to-end Boyson et al. (2009) ได้นิยามถึง โซ่อุปทานไซเบอร์ไว้คือ กิจกรรมการดำเนินการ โครงสร้างขององค์กร และ ระดับของกระบวนหลัก ๆ ที่ร่วมมือกันในการวางแผน สร้าง จัดการ บำรุงรักษา และป้องกันโครงสร้างพื้นฐานของระบบไอที อีกทั้ง Simpson (2010) ได้กล่าวถึง ระบบเทคโนโลยีของโซ่อุปทาน ว่าเป็นการพลวัตที่มีกระจายอยู่ทั่วโลก ซึ่งได้รวบรวมถึงบุคลากร กระบวน และเทคโนโลยีเอาไว้ด้วยกัน Goertzel (2010) ระบุว่าเทคโนโลยีของโซ่อุปทาน ประกอบด้วย กระบวนการ ผลิตภัณฑ์ (รวมไปถึงทรัพย์สินทางปัญญา) การไหลของผลิตภัณฑ์ ข้อมูล (เช่น ข้อมูลด้านผลิตภัณฑ์) การไหลของข้อมูล รวมไปถึงผู้ที่เกี่ยวข้อง (บุคลากร)

ประเด็นที่สำคัญประการหนึ่ เกี่ยวกับความเสี่ยงทางไซเบอร์ของโซ่อุปทาน จากทั้งหน่วยงานภาครัฐ นักวิชาการ รวมไปถึงผู้ปฏิบัติงานคือ ความกังวลใจในเรื่องการประเมินและลดความเสี่ยงที่ฝังอยู่ในโซ่อุปทานไซเบอร์ ด้วยเหตุนี้จึงได้มีการพัฒนากรอบความเสี่ยงที่หลากหลายและรูปแบบในการจัดการความเสี่ยงในเชิงรุก ตัวอย่างเช่น ตัวแบบการอ้างอิงการประกันโซ่อุปทานไซเบอร์ (Cyber Supply Chain Assurance Reference Model) (Boyson et al., 2009), แนวคิดการรับการประกัน (Assurance-based Approach) (Storch, 2011), และแนวคิดการจัดการความเสี่ยง (Risk-based Approach) ในการจัดการความถูกต้องของซอฟต์แวร์ (Storch, 2011).

Borg (2010) อธิบายถึงผลกระทบที่เป็นไปได้ของการโจมตีทางไซเบอร์ ที่มีต่อการทำงานของทางไซเบอร์ของโซ่อุปทาน : การหยุดชะงักของการดำเนินการ การเสียหายจากการดำเนินงาน (โดนโจมตีด้วยมัลแวร์) การทำให้เสื่อมเสียชื่อเสียงของการดำเนินการ (ทำลายความเชื่อมั่นการทำลายคุณค่าของแบรนด์) และการทำลายพื้นฐานของข้อมูล (การสูญเสียการควบคุมการสูญเสียข้อมูลสำคัญ) นอกจากนั้นยังได้มีนำเสนอการแก้ไขที่ควรนำไปใช้ใน 5 ขั้นตอนของโซ่อุปทานได้แก่ ขั้นตอนการออกแบบ ขั้นตอนการประดิษฐ์ ขั้นตอนการประกอบ ขั้นตอนการกระจายและขั้นตอนการบำรุงรักษา The Open Group (2011) พบว่าความน่าเชื่อถือด้านเทคโนโลยีสารสนเทศของโซ่อุปทานทั่วโลกนั้นถูกขัดขวาง เนื่องจากการขาดข้อกำหนดดังต่อไปนี้ มาตรฐานโซ่อุปทาน การปฏิบัติ และแนวทาง ที่สม่ำเสมอ และวิธีการทั่วไปที่ครอบคลุมในการแสดงหลักฐานความน่าเชื่อถือของผลิตภัณฑ์ การปฏิบัติที่ดีที่สุดที่มีประสิทธิภาพในสี่หมวดหมู่ การพัฒนาผลิตภัณฑ์/วิศวกรรม วิศวกรรมความปลอดภัย ความถูกต้องสมบูรณ์ของโซ่อุปทานและวิธีการประเมินผลิตภัณฑ์

Simpson (2010) พัฒนาวิธีการเพื่อลดความเสี่ยงในอุปทาน ด้วยวิธีการ assurance-based การรับประกันซอฟต์แวร์จะยึดตามเสาหลักสามประการต่อไปนี้:

- ความมั่นคงปลอดภัย (Security) ภัยคุกคามนั้นคาดว่าจะได้รับและแก้ไขในระหว่างการออกแบบพัฒนาและทดสอบซอฟต์แวร์
- ความถูกต้องสมบูรณ์ (Integrity) ภัยคุกคามได้รับการแก้ไขในกระบวนการที่ใช้ในการจัดหาส่วนประกอบซอฟต์แวร์สร้างส่วนประกอบซอฟต์แวร์และส่งมอบซอฟต์แวร์ให้กับลูกค้า
- ความเป็นจริง (Authenticity) ซอฟต์แวร์ไม่ใช่ของปลอมและผู้จำหน่ายซอฟต์แวร์มอบให้กับลูกค้า

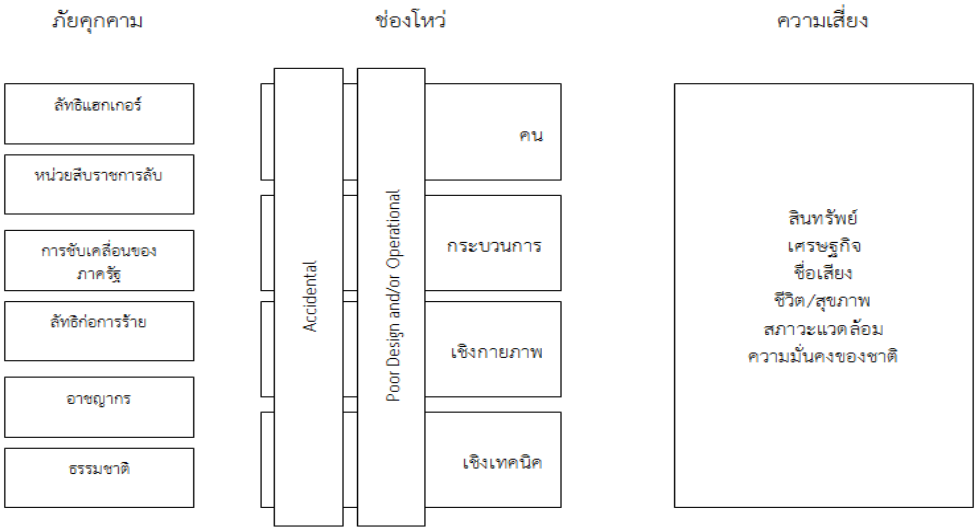
โซ่อุปทานแบบดั้งเดิมหรือทางกายภาพ (SC) มีการดำเนินการโดยการเคลื่อนไหวของผลิตภัณฑ์การเงินและข้อมูล (Peck, 2006) ในขณะที่โซ่อุปทานไซเบอร์เป็นเครือข่ายที่มีโครงสร้างพื้นฐานด้านไอทีและเทคโนโลยีที่ใช้ในการเชื่อมต่อ สร้างและแบ่งปันข้อมูลในแบบเสมือนเครือข่าย (Smith et al., 2007) และสามารถที่จะเปิดรับต่อความเสี่ยงในรูปแบบใหม่ ๆ ที่ไม่ได้เชื่อมต่อกับผลิตภัณฑ์ทางกายภาพ หรือแม้แต่สถานที่ตั้งทางกายภาพที่แตกต่างกัน (เช่น WannaCry ransomware) โซ่อุปทาน เป็นส่วนสำคัญของการพัฒนาที่มีต่อระบบนิเวศเชิงเทคโนโลยี แนวคิดอุตสาหกรรม 4.0 เช่น อินเทอร์เน็ตประสานสรรพสิ่ง (IoT) การผลิตแบบเติม (Additive Manufacturing) ความเป็นจริงเสมือน(Virtual Reality) ปัญญาประดิษฐ์(Artificial Intelligence) และบล็อกเชน (Blockchain) ทั้งหมดได้สะท้อนให้เห็นถึงการเปลี่ยนแปลงและสร้าง

ความสัมพันธ์ระหว่างคู่ค้าในโซ่อุปทาน อย่างไรก็ตามการพัฒนาเพื่อการตอบสนองความปลอดภัยในโลกไซเบอร์จะช้ากว่าความก้าวหน้าในระบบดิจิทัลของโซ่อุปทาน ซึ่งทำให้เป็นที่ถกเถียงกันอยู่ว่า การขยายตัวของโซ่อุปทาน การร่วมมือกับพันธมิตรที่มีความหลากหลายจำนวนมาก อาจทำให้เกิดช่องโหว่โดยไม่ได้ตั้งใจ (Boone, 2017)

2.4.3 องค์ประกอบของการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล

การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Supply Chain Risk Management) เป็นแนวคิดใหม่ที่ได้ถูกออกแบบมาเพื่อช่วยให้องค์กรที่อยู่ภายใต้ความท้าทายของโลกาภิวัตน์ที่เติบโตอย่างรวดเร็วภายใต้ความก้าวหน้าทางเทคโนโลยี ทั้งในส่วนของระบบฮาร์ดแวร์และซอฟต์แวร์ การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัลนี้เป็นแนวคิดการศึกษาโดยรวมเอาองค์ความรู้ต่าง ๆ เหล่านี้มาพิจารณาแบบบูรณาการ ซึ่งได้แก่ ความมั่นคงปลอดภัยไซเบอร์ การจัดการโซ่อุปทาน และการจัดการความเสี่ยงขององค์กร และนำเสอนเป็นแนวคิดใหม่และมีประสิทธิภาพในการควบคุมกระบวนการทั้งหมดขององค์กรรวมไปถึงคู่ค้าทั้งหมดขององค์กร (Sandor Boyson, 2014)

จากการเพิ่มขึ้นของการนำเอาระบบเทคโนโลยีสารสนเทศมาใช้นี้ อันเป็นผลให้นำมาสู่ความเสี่ยงทางด้านไซเบอร์ (Cyber-Risk) ที่เพิ่มขึ้น ซึ่งมีผลกระทบต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน (Hugh Boyes,2015) นอกจากนี้ Boyes (2015) ยังได้เสนอว่า ในการที่จะประเมินการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานนั้น จะต้องพิจารณาถึงความเสี่ยงที่อาจเกิดขึ้นได้ดังแสดงไว้ในภาพประกอบที่ 2.3



ภาพประกอบที่ 2.3 ภัยคุกคามและช่องโหว่ที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์

จากภาพประกอบที่ 2.2 แสดงให้เห็นถึงประเภทของความเสี่ยงที่จำเป็นต้องพิจารณาเมื่อมีการประเมินการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน การปรากฏตัวของธรรมชาติที่อาจจะดูเหมือนมีความได้เปรียบต่อการอภิปรายในประเด็นของการคืนสภาพได้ทางไซเบอร์ แต่มันเป็นสิ่งสำคัญที่จะยอมรับว่าเหตุการณ์ที่เกิดขึ้นตามธรรมชาติสามารถมีผลกระทบอย่างมีนัยสำคัญในการสื่อสารและโครงสร้างพื้นฐานด้านไอที ยกตัวอย่างเช่นพายุสุริยะสามารถรบกวนการสื่อสารไร้สายทั้งในระดับโลกสำหรับการสื่อสารผ่านดาวเทียมและในระดับท้องถิ่นสำหรับการสื่อสารเคลื่อนที่ (3G และ 4G) สาเหตุตามธรรมชาติเช่นแผ่นดินไหว น้ำท่วมและความเสียหายจากสัตว์นอกจากนี้ยังอาจเกิดความเสียหายหรือส่งผลกระทบต่อการดำเนินการเชื่อมต่อสายเคเบิลโทรศัพท์และการจราจรทางอินเทอร์เน็ต ที่ส่งผลต่อโซ่อุปทาน

จากการศึกษาของ Dave Shackleford (2015) แห่งสถาบัน SAAN (SANS™ Institute) ที่ได้ทำการศึกษาในเรื่อง Combatting Cyber Risks in the Supply Chain โดยได้นำเสนอแนวทางการปฏิบัติที่ดีที่สุด (Best Practices) ที่ใช้ในการจัดการด้านความเสี่ยงในโซ่อุปทานดิจิทัลที่ประกอบไปด้วย 3 แนวทาง ซึ่งแก่ได้แก่ คน (People) กระบวนการ (Process) และ เทคโนโลยี (Technology) ดังภาพประกอบที่ 2.4

ภาพประกอบที่ 2.4 Best Practices in Cyber Supply Chain Risk Management

1. บุคลากร (People)

สิ่งที่ควรคำนึงถึงเป็นอันดับแรกสำหรับองค์กรที่ต้องการจะดำเนินการใด ๆ ที่เกี่ยวข้องกับการประเมินความปลอดภัยภายในคือ บุคลากร (People) โดยทั่วไปแล้วองค์กรส่วนใหญ่จะมีงานทางด้านทรัพยากรมนุษย์ที่จะทำหน้าที่ในการตรวจสอบภูมิหลังของคนเมื่อจะรับเข้ามาเป็นพนักงานที่จะเข้ามาร่วมงานภายในองค์กร ซึ่งก็จะสามารถช่วยให้มั่นใจได้ว่าพนักงานคน ๆ นั้นเป็นพลเมืองที่ถูกต้องตามกฎหมายและไม่มีประวัติอาชญากรรมมาก่อน โดยที่คนที่จะ

รับเข้ามาเป็นพนักงานจะต้องไม่มีกิจกรรมหรือการกระทำที่อาจบ่งบอกถึงความเสี่ยงที่อาจเกิดขึ้นกับองค์กร

บุคลากร เรียกได้ว่าเป็นจุดอ่อนใหญ่ของการรักษาความมั่นคงปลอดภัย เมื่อใดก็ตามที่องค์กรใช้เทคโนโลยีที่ยอดเยี่ยม หรือมีกระบวนการที่รัดกุมมากเพียงใด แต่ถ้าพนักงานในองค์กรขาดความรู้และทักษะในการรับมือกับภัยคุกคาม ระบบขององค์กรก็ยังคงตกเป็นเหยื่อของแฮ็คเกอร์ได้ ดังนั้น สิ่งสำคัญที่สุดคือการอบรมให้พนักงานภายในองค์กรทราบถึงรูปแบบของภัยคุกคาม ไซเบอร์ที่พบบ่อยในปัจจุบัน และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย นอกจากนี้ ควรฝึกฝนพนักงานผ่านทางการจำลองสถานการณ์จริง เพื่อให้พนักงานมีประสบการณ์ และสามารถตอบสนองต่อการโจมตีได้อย่างรวดเร็วและถูกต้อง

2. กระบวนการ (Process)

เมื่อมีเทคโนโลยีที่พร้อมรับมือกับภัยคุกคามแล้ว สิ่งสำคัญที่ตามมาคือการมีกระบวนการเพื่อรองรับการใช้งานเทคโนโลยีเหล่านั้น เช่น มีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เพื่อให้ระบบขององค์กรยังคงให้บริการต่อไปได้แม้เกิดภัยพิบัติ หรือ มีการจัดทำ Use Case ของภัยคุกคามและเหตุผิดปกติรูปแบบต่าง ๆ เพื่อให้ผู้ที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและเป็นระบบ นอกจากนี้ องค์กรยังสามารถนำกระบวนการที่เป็นมาตรฐานหรือกรอบการทำงานเข้ามาใช้เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรได้ เช่น มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS หรือ ISO/IEC 27001:2013) หรือ NIST Cybersecurity Framework เป็นต้น

3. เทคโนโลยี (Technology)

เทคโนโลยีด้านความมั่นคงปลอดภัยเปรียบเสมือนเป็นมาตรการควบคุมสำหรับปกป้องค์กรจากภัยคุกคาม ปัจจัยหลักที่ช่วยให้สามารถเลือกใช้เทคโนโลยีได้อย่างถูกต้องและเหมาะสมกับสภาวะแวดล้อมขององค์กร ไม่ได้มาจากความทันสมัยหรือจำนวนฟีเจอร์ของเทคโนโลยี แต่มาจากการประเมินความเสี่ยง เทคโนโลยีที่เลือกมาเป็นมาตรการควบคุมจะต้องลดระดับความเสี่ยงด้านความมั่นคงปลอดภัยขององค์กรลงให้อยู่ในขอบเขตที่ยอมรับได้หรือลดระดับความเสียหายลงได้มากที่สุด มิเช่นนั้นแล้ว เทคโนโลยีอาจแก้ปัญหาไม่ถูกจุด ทำให้ลงทุนไปอย่างไม่คุ้มค่า

จะเห็นได้ว่าในการจัดการความทางไซเบอร์ของโซ่อุปทานดิจิทัล องค์ประกอบหลักทั้ง 3 องค์ประกอบที่กล่าวมาข้างต้นนั้นมีความสำคัญเป็นอย่างมาก ในการเพิ่มความปลอดภัยให้กับระบบขององค์กร ไม่ให้ตกเป็นเหยื่อของแฮ็คเกอร์จากการโจมตีระบบ และจากภัยคุกคามทางไซเบอร์ต่าง ๆ เพราะสิ่งสำคัญเพื่อให้การป้องกัน ตรวจจับ และตอบสนองสัมฤทธิ์ผลไม่ได้ขึ้นอยู่

กับ “เทคโนโลยี” ที่ใช้เพียงอย่างเดียว แต่ยังขึ้นกับ “กระบวนการ” และ “คน” อีกด้วย ยิ่งองค์กรให้ความสำคัญของทั้ง 3 องค์ประกอบที่กล่าวมานี้มากเท่าไหร่ ก็ยิ่งช่วยลดความเสี่ยงที่ระบบจะถูกโจมตีได้มากเท่านั้น

2.5 การคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล

2.5.1 ความเป็นมาและความหมายของการคืนสภาพได้

สำหรับการศึกษาในเรื่องของ การคืนสภาพได้ (Resilience) นี้ ได้มีต้นกำเนิดมาจากการศึกษาในทางทฤษฎีที่เกี่ยวกับการพัฒนาทางด้านจิตวิทยาสังคม แนวความคิดของการคืนสภาพได้ที่ได้เคยมีการศึกษามานั้น จะเป็นเรื่องที่เกี่ยวข้องโดยตรงกับประเด็นที่สำคัญ ๆ ที่ต้องการจะทำการศึกษา ตัวอย่างเช่น ความยืดหยุ่นทางด้านนิเวศวิทยา ความเปราะบางทางด้านสังคมและการเมือง การกู้คืนจากผลของการเกิดภัยพิบัติ การบริหารความเสี่ยงภายใต้ภัยคุกคามต่าง ๆ ที่เพิ่มขึ้น โดยการศึกษาที่ผ่านมา การสร้างขอบเขตของเนื้อหาและองค์ความรู้เพื่อให้ครอบคลุมในเรื่องของการคืนสภาพได้นี้ยังขาดความชัดเจน ดังนั้นเพื่อที่จะเข้าใจปรากฏการณ์ของการคืนสภาพได้ ในเบื้องต้นผู้วิจัยได้ทำการศึกษาถึงวรรณกรรม ในเรื่องของการคืนสภาพได้จากวรรณกรรมที่หลากหลายซึ่งทำให้ถึงมุมมองที่แตกต่างกัน ผลที่ได้หลังจากที่ได้ทำการทบทวนวรรณกรรม ผู้วิจัยจะได้ทำการวิเคราะห์เพื่อหาถึงประเด็นที่มีความเกี่ยวข้องกันมากที่สุดและมีความเหมาะสมสำหรับการทำความเข้าใจในเรื่องของปรากฏการณ์ของการคืนสภาพได้ต่อไป

2.5.1.1 การคืนสภาพได้จากมุมมองทางด้านนิเวศวิทยา

นักนิเวศวิทยาชาวแคนาดา Holling (1973) เป็นนักวิจัยคนแรก ๆ ที่ได้ชี้ให้เห็นว่า ระบบจะมีคุณสมบัติอยู่ 2 ลักษณะที่แตกต่างกัน : การคืนสภาพได้ (Resilience) และความมั่นคง (Stability) การคืนสภาพได้ คือ ความสามารถของระบบในการดูดซับการเปลี่ยนแปลงในขณะที่ ความมั่นคง คือ ความสามารถของระบบที่จะกลับไปสู่สภาพสมดุลหลังจากที่ได้ถูกรบกวนในชั่วขณะหนึ่ง ระบบที่มีความยืดหยุ่นที่ดีกว่าจะคืนสู่สภาวะที่สมดุลได้เร็วกว่า ซึ่งก็จะหมายถึงการที่มีความมั่นคงที่มากกว่า ซึ่งแน่นอนว่าสิ่งนี้ได้เป็นสมมติฐานที่ชัดเจนเกี่ยวกับความมั่นคงในระบบ โดยถ้าปราศจากความมั่นคงที่เคยเกิดขึ้นในระบบ การสันนิษฐานที่เกี่ยวกับเรื่องของการกลับไปสู่ถานะก่อนที่จะมีการรบกวนเกิดขึ้นก็จะไม่เกิดขึ้น แต่การปรับเปลี่ยนกระบวนการหรือวิธีการอย่างใดอย่างเพื่อกลับไปสู่สภาวะความสมดุลย์ใหม่นั้น ผลลัพธ์ที่เกิดก็อาจจะดีกว่าหรือแย่กว่าสถานะก่อนหน้านั้นก็เป็นได้

แนวคิดของการคืนสภาพได้ ได้ถูกทำให้เกิดการเปลี่ยนแปลงไป ตั้งแต่มีบทความสัมมนาของ Holling โดยที่มิติที่สำคัญ ๆ ที่หลากหลายของการคืนสภาพได้ของระบบ

นิเวศได้มีการศึกษาและสรุปโดย Westman (1978) ซึ่งทำให้มีคำนิยามของการคืนสภาพได้และองค์ประกอบต่างๆ ที่เกี่ยว ซึ่งได้รับการยอมรับกันอย่างกว้างขวาง จากนักวิชาการทางด้านระบบนิเวศ ซึ่งได้แสดงไว้ในตารางที่ 2.6

ตารางที่ 2.6 องค์ประกอบของการคืนสภาพได้ : มุมมองทางด้านระบบนิเวศ

	คำนิยาม
การคืนสภาพได้ (Resilience)	ระดับ, ลักษณะ, และระยะของการฟื้นฟูกลับไปยังโครงสร้างและฟังก์ชั่นในจุดเริ่มต้นของระบบนิเวศหลังจากที่ได้ถูกรบกวน
องค์ประกอบของการคืนสภาพได้	
ความยืดหยุ่น (Elasticity)	ความรวดเร็วของการฟื้นฟูกลับไปสู่สถานะที่เหมือนเดิมจากการถูกรบกวน
ความสมบูรณ์ (Amplitude)	ส่วนของความเสียหายที่ระบบจะกลับคืนเข้ามาสู่สถานะเริ่มต้น
ฮีสเทอรีซีส (Hysteresis)	ขอบเขตที่เส้นทางของการย่อยสลายภายใต้การรบกวนเรื้อรัง, และการกู้คืนเมื่อเกิดการรบกวน ซึ่งจะไม่ได้สะท้อนภาพซึ่งกันและกัน
การเปลี่ยนแปลง (Malleability)	ระดับในการกลับไปสู่สถานะที่มั่นคงหลังจากที่ถูกรบกวน ซึ่งต่างจากสถานะที่มั่นคงอยู่เดิม
การหน่วง (Damping)	ระดับและลักษณะของแนวทางของการฟื้นฟูได้ถูกเปลี่ยนแปลงโดยแรงผลักใด ที่ได้เข้ามาเปลี่ยนแรงผลักที่เป็นอยู่เดิม

ที่มา : Ponomarov et al. (2009)

Gunderson and Holling (2001) ได้นิยามความหมายของ การคืนสภาพได้ว่าเป็นความสามารถของระบบในการที่จะต้องเผชิญกับสิ่งรบกวนและต้องดูแลรักษาและควบคุมมัน Carpenter et al. (2001) ได้ทำการศึกษาเพิ่มเติมถึงขนาดของการรบกวน โดยทำการตรวจสอบดูว่าระบบจะทนได้อย่างก่อนหน้าที่จะมีการเปลี่ยนแปลงหรือไม่ ได้ทำการกำหนดปัจจัยพื้นฐานให้อยู่ในขอบเขตที่ต่างกันด้วยการควบคุมที่ต่างกัน นอกจากนี้แล้ว นักวิจัยได้ขยายแนวความคิดของการคืนสภาพได้ โดยการใช้แนวความคิดของวงจรการปรับตัว (Adaptive Cycle) ตามหลักของทฤษฎีของวงจรการปรับตัวนี้ ระบบที่มีพลวัตร (Dynamic Systems) ไม่ได้ส่งผลต่อสถานะที่คงที่หรือสถานะที่มีความสมดุลย์ แต่จะส่งผลต่อสถานะทั้ง 4 สถานะดังนี้ การเติบโตอย่างรวดเร็วและการแสวงหาประโยชน์ การอนุรักษ์ การทำลายความคิดสร้างสรรค์ และการต่ออายุหรือการปรับ

โครงสร้างขององค์กร ในการที่จะปรับตัวเข้าการการรบกวนที่เกิดขึ้น Carpenter et al. (2001) ได้สรุปว่าการคืนสภาพได้ มีคุณสมบัติหลัก ๆ อยู่ 3 ประการดังนี้

(1) ปริมาณของการเปลี่ยนแปลง ที่ระบบสามารถรับได้ ในขณะที่ยังมีการรักษาการควบคุม โครงสร้างและการทำงานให้อยู่เหมือนเดิม

(2) เป็นระดับที่ตัวระบบเองจะมีความสามารถในการจัดการกับตัวเองโดยปราศจากแรงกดดันใด ๆ จากปัจจัยภายนอก

(3) เป็นระดับที่ระบบได้ทำการพัฒนาความสามารถในการเรียนรู้และปรับตัวในการตอบสนองต่อการรบกวน

นอกจากนี้ Dovers and Handmer (1992) ยังได้เน้นให้เห็นถึงความสำคัญของความสามารถในการปรับตัวนี้ ในขณะที่การอธิบายการคืนสภาพได้ในเชิงรุกนั้น การคืนสภาพได้จะต้องเป็นเรื่องที่ต้องยอมรับถึงความจำเป็นของการเปลี่ยนแปลง และความพยายามที่จะสร้างระบบที่มีความสามารถในการปรับตัวให้เข้ากับเงื่อนไขใหม่ ๆ และหลีกเลี่ยงไม่ได้

ดังนั้นแล้ว การคืนสภาพได้ในมุมมองของระบบนิเวศ เป็นการนำเสนอมุมมองที่ยังไม่ได้มีกำหนดถึงพฤติกรรมมนุษย์ พฤติกรรมที่ว่านี้จะเกิดขึ้นมาจากหลาย ๆ สาเหตุเนื่องด้วย สภาพแวดล้อมของมนุษย์นั้นมีความซับซ้อน โดยจะมีการแลกเปลี่ยนเกิดขึ้นในช่วงเวลาที่ผ่านมา (Gunderson, 2000) ด้วยเหตุนี้เอง มุมมองทางด้านระบบนิเวศวิทยานี้ได้ทำให้เกิดองค์รวมของกระบวนการชีวิต ดังนั้นแล้ว แนวคิดของระบบนิเวศมักจะใช้ร่วมกับวิธีการคืนสภาพได้ในทางสังคมศาสตร์

2.5.1.2 มุมมองทางด้านสังคม จิตวิทยา และเศรษฐศาสตร์ของการคืนสภาพได้

แนวคิดของการคืนสภาพได้ได้มีการศึกษาวิจัยเป็นอย่างมาก โดยเฉพาะในสาขาวิชาทางด้านสังคมศาสตร์ โดยสาขาที่มีการศึกษาอยู่จะมีอยู่ใน 3 สาขาหลัก ๆ ได้แก่ สาขาทางด้านสังคม จิตวิทยา และ เศรษฐศาสตร์

2.5.1.2.1 มุมมองทางด้านสังคมศาสตร์

การศึกษาทางด้านสังคมศาสตร์นี้ โดยทั่ว ๆ ไปแล้วการศึกษาถึงการคืนสภาพได้จะเป็นการศึกษาในประเด็นของการที่ได้นำมาใช้เพื่ออธิบายการตอบสนองพฤติกรรมของชุมชนหรือสังคม สถาบันการศึกษารวมไปถึงสภาพเศรษฐกิจ Timmerman (1981) เป็นผู้วิจัยในกลุ่มผู้วิจัยแรก ๆ ที่ได้อธิบายถึงการคืนสภาพได้ทางด้านสังคมว่า เป็นตัววัดความสามารถของระบบในการการดูดซับ (Absorb) และการกู้คืน (Recover) ของเหตุการณ์ที่เป็นอันตรายที่ได้เกิดขึ้นต่อระบบ

สำนักงานว่าด้วยกลยุทธ์ระหว่างประเทศเพื่อการลดภัยพิบัติแห่งสหประชาชาติ (The United Nations International Strategy for Disaster Reduction: UNISDR) (United Nations, 2005) ได้เสนอคำนิยามของการคืนสภาพได้ที่ครอบคลุมความหมายของการคืนสภาพได้ให้มากยิ่งขึ้น โดยคำนิยามของการคืนสภาพได้ หมายถึง ความสามารถของระบบ ชุมชน หรือ สังคมที่อยู่ภาวะที่อันตราย โดยระบบจะต้องสามารถปรับตัวขึ้นมาได้อย่างมีศักยภาพ โดยการต่อต้าน และการเปลี่ยนแปลง เพื่อที่จะไปให้ถึงและรักษาระดับที่สามารถยอมรับได้ ทั้งในส่วนของระดับของการปฏิบัติงานและระดับโครงสร้าง ซึ่งการคืนสภาพได้ดังกล่าวนี้ จะถูกกำหนดโดยระบบของสังคมที่มีระดับความสามารถในการจัดการตัวเอง ทั้งนี้ก็เพื่อเพิ่มขีดความสามารถในการเรียนรู้จากภัยพิบัติที่ผ่านมา สำหรับการป้องกันในอนาคตที่ดียิ่งขึ้น และเพื่อเป็นการพัฒนาประสิทธิภาพสำหรับมาตรการในการลดความเสี่ยง

ความสามารถของระบบในมุมมองทางด้านสังคมศาสตร์นี้ ได้ถูกนิยามไว้ว่าเป็น การรวมกันของ ความแข็งแรง (Strength) ทรัพยากร (Resources) และความสามารถที่มีอยู่ภายในชุมชน (Community) สังคม (Society) หรือองค์กร (Organization) ที่ซึ่งจะนำไปสู่การลดระดับของความเสี่ยงที่เกิดขึ้น หรือ ผลกระทบจากภัยพิบัติ โดยที่ความสามารถดังกล่าวคือ สมรรถนะ (Capacity) ของชุมชน สังคมหรือองค์กร ซึ่งก็อาจจะอธิบายได้ว่าเป็นความสามารถที่ประกอบไปด้วยทรัพยากร (Resource) และ วิธีการ (Means) ทางด้าน กายภาพ (Physical) สถาบัน (Institutional) สังคม (Social) หรือ เศรษฐศาสตร์ (Economic) รวมไปถึงสมรรถนะของบุคคลที่มีความเชี่ยวชาญ ซึ่งก็จะสามารถอธิบายได้ในคุณลักษณะที่มีร่วมกัน ได้แก่ ภาวะผู้นำ (Leadership) และ การจัดการ (Management) โดยทั้งหมดนี้เป็นสิ่งที่ชุมชน สังคมหรือองค์กร ต้องสามารถนำมาใช้เพื่อให้ทนอยู่กับการจัดการอันตรายที่เกิดขึ้น นอกจากนี้ในการเชื่อมโยงสมรรถนะของระบบให้กับการคืนสภาพได้นั้น จากงานวิจัยที่ผ่านมานั้นได้มีการชี้ให้เห็นการคืนสภาพได้ทางสังคมจะมีอยู่ในทุกๆ ระดับทางด้านสังคม ระดับเหล่านี้ประกอบไปด้วย : ความเป็นตัวบุคคล (Individual) ครอบครัว (Family) ชนเผ่าหรือชาติตระกูล (Tribe or clan) ถิ่นที่อยู่อาศัย (Locality) หรือกลุ่มเพื่อนบ้าน (Neighborhood) ชุมชน (Community) สมาคมสังคม (Social Associations) (ตัวอย่างเช่น สโมสร และ กลุ่มนิยมความเชื่อต่าง ๆ) องค์กร (Organization) (ตัวอย่างเช่น หน่วยงานราชการหรือบริษัทเอกชน) และระบบ (Systems) (ตัวอย่างเช่น สภาวะแวดล้อม และ ระบบเศรษฐกิจ) (Ponomarov et al., 2009) ด้วยลักษณะของโครงสร้างของระดับทางสังคมที่ซับซ้อนลักษณะเดียวกันนี้สามารถนำไปปรับใช้ เพื่อการศึกษาในเรื่องของการคืนสภาพได้ของโซ่อุปทาน เพื่อที่จะสะท้อนถึงระดับต่าง ๆ ที่พบในบริษัททั้งหลายที่มีอยู่โซ่อุปทานได้

2.5.1.2.2 มุมมองทางด้านจิตวิทยา

สำหรับมุมมองทางด้านจิตวิทยาของการคืนสภาพได้ ได้มีการทำการวิจัยและเผยแพร่ผลงานอย่างมากมาย ในแง่ของการศึกษาการคืนสภาพได้ในมุมมองทางด้านจิตวิทยานี้ จะรากฐานขององค์ความรู้ที่อยู่ในศาสตร์ด้านนี้อยู่แล้วในการที่จะนำไปพัฒนาทฤษฎีที่เกี่ยวข้องตลอดจนทำการตรวจสอบพฤติกรรมของผู้คนได้ตลอดช่วงชีวิต และยังสามรรถที่จะครอบคลุมไปถึงความเข้าใจในปัจจัยทางจิตวิทยาชีวภาพ อย่างเช่นในเรื่องของจิตวิญญาณ (Conrad, 1999) จากงานวิจัยของ Reich (2006) ได้ทำการตรวจสอบองค์ประกอบทางจิตวิทยาของการคืนสภาพได้ โดยผลของการวิจัยได้สรุปว่า องค์ประกอบทางด้านจิตวิทยาของการคืนสภาพได้จะมีอยู่ 3 ประการ ที่เกิดขึ้นอันเป็นผลมาจากภัยพิบัติทางธรรมชาติหรือที่มนุษย์สร้างขึ้น ซึ่งได้แก่

(1) การควบคุม (Control) ได้แก่ ทิศทาง กฎระเบียบ และการประสานงานของกิจกรรม

(2) การเชื่อมโยง (Coherence) การเสริมสร้างความหมาย ทิศทางและความเข้าใจในช่วงเวลาที่เลวร้ายที่สุด กระบวนการและขั้นตอนที่จำเป็นในการลดความไม่แน่นอน

(3) การเชื่อมต่อ (Connectedness) พฤติกรรมการโน้มเข้ามาหากัน การประสานงานที่เป็นระบบของความพยายามที่จะหลีกเลี่ยงความซ้ำซ้อนและสิ้นเปลืองของการให้บริการ

จากการศึกษาของ Reich ทำให้ได้ข้อสรุปว่า การดำเนินการโดยการผสมผสานกันขององค์ประกอบหลัก ทางด้านจิตวิทยาของการคืนสภาพได้เหล่านี้เข้าไปในแผนการรับภัยพิบัตินั้น จะนำไปสู่การตอบสนองที่ครอบคลุมมากยิ่งขึ้น ซึ่งจะส่งผลให้มีประสิทธิภาพที่ดีมากยิ่งขึ้น ดังนั้น การควบคุม (Control) การเชื่อมโยงกัน (Coherence) และการเชื่อมต่อ (Connectedness) จะเป็นส่วนประกอบหลักของการตอบสนองที่เพียงพอแล้วสำหรับการคืนสภาพได้

นอกจากการที่ได้ค้นพบถึงองค์ประกอบหลักที่สำคัญของการคืนสภาพได้แล้ว ยังมีงานวิจัยที่ได้ทำการศึกษาถึงการคืนสภาพได้ภายใต้มุมมองทางด้านจิตวิทยาอื่น ๆ อีก เช่น Stewart et al. (1997) ได้ทำการวิจัยจากงานวิจัยที่มีอยู่อย่างมากมายที่เกี่ยวข้องกับจิตวิทยา และได้พบถึงงานวิจัยที่เกี่ยวข้องกับการคืนสภาพได้ ดังต่อไปนี้

(1) การคืนสภาพได้ เป็นกระบวนการแบบพลวัตรที่ขึ้นอยู่กับบริบทชีวิต

(2) การคืนสภาพได้ เป็นปฏิสัมพันธ์ที่ซับซ้อนระหว่างลักษณะบางอย่างของบุคคลและสภาพแวดล้อมที่กว้างขึ้น

(3) การลดปัจจัยเสี่ยงเชิงลบเพิ่มการคืนสภาพได้

(4) การคืนสภาพได้ คือการพัฒนาและมีความสำคัญมากที่สุดในช่วงการเปลี่ยนชีวิต

นอกจากนี้ Grotberg (1995) ยังได้เสริมแนวความคิดที่ว่า สมรรถนะ ที่จะนำไปสู่ความการคืนสภาพได้นั้น ไม่ได้ถูกจำกัดอยู่ที่บุคคลใดบุคคลหนึ่ง แต่สมรรถนะของการคืนสภาพได้ จะมีความเป็น “สากล” ที่ครอบคลุมในหลาย ๆ ระดับ จากบุคคลไปยังชุมชน ในการที่จะทำการวางแผน เพื่อการตอบสนองและการกู้คืนจากความทุกข์ยาก

2.5.1.2.3 มุมมองทางด้านเศรษฐศาสตร์

โดยทั่วไปแล้ว การคืนสภาพได้คงที่ทางด้านเศรษฐกิจจะหมายถึง ความสามารถหรือสมรรถนะของระบบในการที่จะดึงดูดหรือบรรเทาความเสียหายหรือความสูญเสีย (Holling, 1973; Perrings, 1994) นอกจากนี้ยังมีคำนิยามที่มากกว่านั้น ซึ่งเป็นความหมายทางด้านพลวัตร โดยจะหมายถึง ความสามารถของระบบในการกู้คืนจากการกระแทกหรือความเครียดอย่างรุนแรง สมมติฐานทฤษฎีระบบคือ ระบบพยายามที่จะรักษาเสถียรภาพของพวกตัวเอง แม้แต่ในขณะที่มันกำลังเปลี่ยนไปก็ตาม Rose (2004) ได้แบ่งการคืนสภาพได้ไว้เป็นสองประเภทที่แตกต่าง

(1) คืนสภาพได้โดยธรรมชาติ (Inherent) คือ ความสามารถภายใต้สถานการณ์ปกติ (ตัวอย่างเช่น ความสามารถในการทดแทนปัจจัยการผลิตอื่น ๆ สำหรับผู้ที่รับความเสียหายจากแรงกระแทกจากภายนอก หรือความสามารถของตลาดที่จะจัดสรรทรัพยากรในการตอบสนองต่อสัญญาณราคา)

(2) คืนสภาพได้เมื่อมีการปรับตัว (Adaptive) คือ ความสามารถในสถานการณ์วิกฤตเนื่องจากความฉลาดหรือความพยายามเป็นพิเศษ (ตัวอย่างเช่น การเพิ่มความเป็นไปได้ทดแทนการป้อนปัจจัยการผลิตในการดำเนินธุรกิจของแต่ละบุคคล หรือการเสริมสร้างการตลาดโดยการให้ข้อมูลเพื่อให้ตรงกับซัพพลายเออร์กับลูกค้า

นอกจากนี้ Rose ยังได้อธิบายต่อไปอีกว่าการคืนสภาพได้นั้นสามารถนำมาใช้งานร่วมกันเศรษฐศาสตร์ใน 3 ระดับ ได้แก่ เศรษฐศาสตร์จุลภาค (Microeconomic) จะอยู่ในระดับส่วนบุคคล (individual) เศรษฐศาสตร์ขั้นกลาง (Mesoeconomic)

จะอยู่ในระดับภาคการตลาดหรือกลุ่มสหกรณ์ และเศรษฐศาสตร์มหภาค (Macroeconomic) จะอยู่ในระดับที่เป็นกลุ่มในแต่ละหน่วยและตลาดรวม โดยที่ระดับเหล่านี้สามารถที่จะสะท้อนมุมมองของระบบสังคมและสามารถนำมาประยุกต์ใช้ได้ในระดับบริษัทและโซ่อุปทานต่อไป

เป้าหมายสูงสุดของการคืนสภาพได้ตามแนวคิดของ Hamel and Valikangas (2003) คือการที่พัฒนาให้บริษัทมีความสามารถในการแข่งขันได้ได้อย่างรวดเร็ว โดยจะต้องไม่เกิดผลร้ายใด ๆ ที่มีผลกระทบต่อองค์กร จากการศึกษาของ Hamel and Valikangas ยังได้ยืนยันว่าการคืนสภาพได้ไม่ได้เป็นเพียงแต่เรื่องที่เกี่ยวข้องกับการกู้คืน (Recovery) เท่านั้น การคืนสภาพได้จะต้องเป็นเรื่องที่สามารถที่จะทำให้เกิดความยืดหยุ่น (Flexibility) ได้ หรือการเตรียมความพร้อมสำหรับสถานการณ์วิกฤต (Crisis Preparedness) ที่อาจจะเกิดขึ้นได้ สิ่งเหล่านี้ได้แสดงให้เห็นว่า องค์กรหรือบริษัทต่าง ๆ จะต้องมีความสามารถในการสร้างสรรค์นวัตกรรมอย่างต่อเนื่อง ด้วยการวิเคราะห์ของ จุดแข็ง (Strength) จุดอ่อน (Weakness) โอกาส (Opportunities) และ อุปสรรค (Threats) ขององค์กรของตน เพื่อที่จะสร้างความได้เปรียบในการตัดสินใจ และบริษัทจะต้องสร้างตัวเลือกเพื่อนำมาสู่การดำเนินธุรกิจได้อย่างรวดเร็วและจะต้องมีการจัดสรรทรัพยากรให้สามารถทำงานได้มีประสิทธิภาพที่มากกว่าคู่แข่งขัน

2.5.1.3 การคืนสภาพได้จากมุมมองทางด้านองค์กร

จากมุมมองขององค์กร การคืนสภาพได้ได้ถูกทำการศึกษาเพิ่มขึ้น โดยได้รับการนิยามขึ้นมาในแง่ของการปรับขีดความสามารถ (Capabilities) หรือความสามารถ (Abilities) โดยคำนิยามได้ทำมาจากงานวิจัยต่าง ๆ ที่ได้เคยมีผู้ที่ได้ทำการวิจัย ได้สรุปไว้ในตารางที่ 2.7 ดังต่อไปนี้

ตารางที่ 2.7 คำนิยามของการคืนสภาพได้ในมุมมองทางด้านองค์กร

แหล่งที่มา	**คำนิยามของการคืนสภาพได้**
Weick et al, 1999;. Bunderson and Sutcliffe 2002; Edmondson, 1999	ความสามารถในการปรับตัวและรักษาหน้าที่ที่พึงประสงค์ภายใต้เงื่อนไขที่ท้าทายหรือเงื่อนไขที่ตรึงเครียดอยู่
Wildavsky, 1988	ความสามารถในการปรับตัวแบบพลวัตรขององค์กรที่เติบโตและพัฒนาอยู่ตลอดเวลา
Sutcliffe and Vogus, 2003	ความสามารถในการกลับมาจากเหตุการณ์ที่เข้ามาก่อกวนหรือสร้างความยากลำบาก
Mitroff and Alpasan (2003)	ความสามารถในการกู้คืนจากเหตุการณ์ที่หยุดชะงัก

โดยเฉพาะการศึกษาของ Mitroff and Alpasan (2003) ที่ได้ให้คำนิยามของการคืนสภาพได้ที่กล่าวไว้ว่าคือ ความสามารถในการกู้คืนจากเหตุการณ์ที่หยุดชะงักนั้น พวกเขากล่าวว่า องค์กรต่าง ๆ ล้วนแต่มีการคืนสภาพได้เป็นกลยุทธ์ในเชิงรุกซึ่งจะทำให้เกิดการกู้คืนที่ดีขึ้นจากความยากลำบากหรือเหตุการณ์ที่ทำให้ต้องหยุดชะงัก แต่อย่างไรก็ตามความสามารถของการคืนสภาพได้ดังกล่าวนี้ไม่ได้เป็นเพียงแค่การกู้คืนเท่านั้น ซึ่งจะต้องมีความสามารถที่มากกว่า อันได้แก่ ระดับของการคืนสภาพได้และความสามารถในการปรับตัวให้เข้าได้กับอิทธิพลที่เป็นทั้งด้านบวกและด้านลบของสภาพแวดล้อม โดยสรุปจากคำนิยามของการคืนสภาพได้จากมุมมองทางด้านองค์กรจะเป็นเรื่องที่เน้นให้ความสำคัญของความสามารถของการคืนสภาพได้ ซึ่งได้แก่ การปรับตัว ความยืดหยุ่น การบำรุงรักษา และการกู้คืน

อีกด้านหนึ่งที่สำคัญที่ได้มีการกล่าวถึงในบริบททางด้านองค์กรคือการจัดการกับผลของการคืนสภาพได้ Hamel และ Valikangas (2003) ได้แสดงให้เห็นว่าการคืนสภาพได้ ไม่ได้เกี่ยวข้องเพียงแค่กับการกู้คืนเท่านั้น แต่การคืนสภาพได้จะยังเกี่ยวข้องกับการเตรียมความพร้อมต่อเหตุการณ์วิกฤตที่จะเกิดขึ้นด้วย นอกจากนี้การคืนสภาพได้ ยังเป็นแหล่งที่มาที่แตกต่างของความได้เปรียบในการแข่งขันที่ยั่งยืนอีกด้วย Coutu (2002) แสดงให้เห็นว่าการคืนสภาพได้เป็นความสามารถที่สำคัญสำหรับความสำเร็จ โดยการศึกษาได้ทำการมุ่งเน้นไปที่การคืนสภาพได้ที่ให้เป็นความสามารถขององค์กรที่โดดเด่น Stoltz (2004) ระบุว่าการคืนสภาพได้เป็นกุญแจสำคัญในการพัฒนาแผนกลยุทธ์ ที่มีความยั่งยืนและความสามารถในการแสดงผลของการปฏิบัติการที่ดีกว่าคู่แข่งมีการคืนสภาพได้น้อย การค้นพบที่ได้กล่าวมาแล้วทั้งหมดข้างต้นเป็นสิ่งสำคัญอย่างยิ่งสำหรับการทำความเข้าใจปรากฏการณ์ของการคืนสภาพได้ที่มีอยู่ทั่วๆ ไป ซึ่งจะเป็นนำไปสู่การเข้าถึงและเข้าใจความหมายของการคืนสภาพได้ในโซ่อุปทานต่อไป

2.5.1.4 ความยืดหยุ่นในมุมมองการจัดการเหตุฉุกเฉินและมุมมองการพัฒนาที่ยั่งยืน

การจัดการเหตุฉุกเฉิน (Emergency Management) เป็นองค์ความรู้ที่เรียกได้ว่าเป็นสหวิทยาการ ที่มีอยู่กับองค์ความรู้ทั้งในด้านวิทยาศาสตร์กายภาพและสังคมศาสตร์ การกู้คืนความเสียหายที่เกิดจากภัยพิบัติที่ผ่านมา จากการศึกษางานวิจัยทางด้านการจัดการเหตุฉุกเฉินที่ผ่านมา ได้มีการนำเสนอการเรียนรู้มุมมองของการคืนสภาพได้เอาไว้ด้วย เช่น Lindell et al. (2007) ได้แสดงให้เห็นว่าการคืนสภาพได้ของชุมชนที่ได้รับผลกระทบจากภัยพิบัตินั้น ชุมชนได้มีการเรียนรู้จากประสบการณ์ของที่ชุมชนที่ได้ประสบกับเหตุการณ์เหล่านั้น ซึ่งจากการศึกษาของ Lindell et al. นี้ได้มีการกำหนดขั้นตอน 4 ขั้นตอน สำหรับจัดการต่อเหตุฉุกเฉิน ประกอบไปด้วย

การลดอันตรายที่จะเกิดขึ้นจากภัยพิบัติ (Reduce) การเตรียมพร้อมต่อภัยพิบัติ (Readiness) การตอบสนองต่อเหตุฉุกเฉินอันเนื่องมาจากภัยพิบัต (Response) และการกู้คืนจากภัยพิบัติ (Recovery)

โดยขั้นตอนต่าง ๆ เหล่านี้ เราอาจจะกล่าวได้ว่า มีความเกี่ยวข้องโดยตรงกับขั้นตอนของการคืนสภาพได้โซ่อุปทาน นอกจากนี้การศึกษาของพวกเขายังได้เน้นถึงมุมมองทางด้านการเรียนรู้ ตัวอย่างเช่น ความเปราะบางของโครงสร้างพื้นฐานที่สามารถทำให้ลดลงได้ในระหว่างขั้นตอนการกู้คืน เช่น สะพานที่ถูกทำลายจากแผ่นดินไหวจะถูกแทนที่ด้วยสะพานใหม่ที่มีการออกแบบที่ดีกว่าและแข็งแกร่งมากขึ้น นอกจากนี้สิ่งที่ยากที่สุดของการกู้คืน คือการปฏิบัติทางสังคมและกิจกรรมทางเศรษฐกิจ กระบวนการของการกู้คืนที่เกี่ยวข้องกับการฟื้นฟูความมั่นคงทางด้านจิตใจของผู้คน นอกจากนี้ยังเกี่ยวข้องกับบทเรียนของการเรียนรู้ที่เกิดขึ้นจากประสบการณ์ในเชิงบวกได้อีกด้วย ในแง่ของโลจิสติกส์จากการศึกษาของ Esper et al. (2007) ทำให้ทราบว่าความสามารถในการเรียนรู้จะเป็นตัวสนับสนุนหลักในการสร้างกลยุทธ์ทางด้านโลจิสติกส์ ในการสร้างความได้เปรียบทางการแข่งขันได้อย่างยั่งยืน

จากมุมมองของการจัดการเหตุการณ์ฉุกเฉินนี้ การคืนสภาพได้อาจกล่าวได้ว่าเป็นหนึ่งในสิ่งที่จำเป็นสำหรับการพัฒนาทางเศรษฐกิจที่ยั่งยืน ซึ่งมีความสอดคล้องกับมุมมองทางด้านองค์กรได้กล่าวไว้ก่อนหน้านี้ การคืนสภาพได้เป็นแหล่งที่มาของความได้เปรียบในการแข่งขัน ตัวอย่างเช่น Folke et al. (2003) กล่าวถึงกลุ่มผลประโยชน์พิเศษในแกรนแคนยอนที่ได้มีการพัฒนาถึงกระบวนการ “การปรับเปลี่ยนการบริหารจัดการกลุ่มงาน” เพื่อเรียนรู้เพิ่มเติมเกี่ยวกับการเสริมสร้างการคืนสภาพได้ของระบบนิเวศ ซึ่งก็จะมีความคิดเห็นที่แตกต่างจากกลุ่ม Florida Everglades ที่ไม่ได้ดูเหมือนว่าจะมีความเข้าใจในวิธีการสร้างการคืนสภาพได้สำหรับการปรับตัวต่อการเปลี่ยนแปลงใด ๆ ที่จะนำไปสู่การคืนสภาพได้ กลุ่มคนเหล่านี้ยังไม่ได้รับการพัฒนาในเรื่องของวัฒนธรรมการเรียนรู้ที่เป็นสิ่งที่จำเป็นสำหรับการพัฒนาเศรษฐกิจอย่างยั่งยืน

2.5.2 แนวคิดการคืนสภาพได้ที่มีต่อระบบโซ่อุปทาน

การศึกษาในประเด็นของการคืนสภาพได้ของโซ่อุปทานได้มีเกิดขึ้นครั้งแรกในสหราชอาณาจักร (Pettit et al., 2010) จากการเกิดขึ้นของการหยุดชะงักเนื่องจากการประท้วงในเรื่องของพลังงานเชื้อเพลิงโดยเฉพาะน้ำมัน ในปี คศ.2000 และเกิดจากการระบาดของโรคปากเท้าเปื่อยในช่วงต้นปี คศ.2001 การศึกษาในช่วงเวลานั้นเป็นการศึกษาจากฐานความรู้ที่มีอยู่ในอุตสาหกรรมของประเทศสหราชอาณาจักร ที่เกี่ยวข้องกับความเปราะบาง (Vulnerability) ของโซ่อุปทานและพบว่า (1) ความเปราะบางของโซ่อุปทานคือประเด็นหลักที่สำคัญทางด้านธุรกิจ (2) งานวิจัยทางด้านความเปราะบางของโซ่อุปทานยังมีอยู่น้อย (3) ความตระหนักถึงปัญหาที่จะเกิดขึ้นตามมายังไม่ได้รับการเอาใจใส่อย่างจริงจัง และ (4) ในเรื่องของระเบียบวิธีที่จะนำมาใช้ใน

การจัดการเกี่ยวกับความเปราะบางของโซ่อุปทานมีความจำเป็นอย่างยิ่ง (Cranfield University, 2003)

ผู้วิจัยได้ทำการศึกษาเพื่อหาคำนิยามของการคืนสภาพได้ของโซ่อุปทานโดยที่สามารถสรุปความหมายของการคืนสภาพได้ของโซ่อุปทานจากการศึกษาที่ผ่านมาดังตารางที่ 2.8

ตารางที่ 2.8 นิยามของการคืนสภาพได้ของโซ่อุปทาน

แหล่งที่มา	**นิยามของการคืนสภาพได้ของโซ่อุปทาน**
Rice and Caniato (2003, p. 25)	สภาวะแวดล้อมทางธุรกิจในปัจจุบันนี้ การคืนสภาพได้จะเป็นคุณสมบัติหนึ่งขององค์กรในการที่แสดงถึงความสามารถ (Capacity) ในการตอบโต้ (React) ถึงการหยุดชะงักใดๆ ที่ไม่คาดคิดได้ ตัวอย่างเช่น การเกิดการโจมตีจากผู้ก่อการร้าย หรือ ภัยพิบัติจากธรรมชาติ โดยสามารถที่จะกลับคืน (Restore) สู่สภาวะปกติได้
Christopher and Peck (2004, p. 2)	ความสามารถ (Ability) ของระบบที่จะกลับคืนสู่สถานะเดิม หรือสถานะใหม่ หรือมากกว่าเดิมที่เป็นอยู่ก่อนที่จะมีการรบกวน
Peck (2005, p. 211)	ความสามารถ (Ability) ของระบบในการกลับคืนสู่สถานะเดิม (หรือมากกว่า) หลังจากที่ถูกรบกวน คำนิยามดั้งเดิมมีรากฐานมาจากความรู้ทางด้านระบบนิเวศ (เป็นการศึกษาในเรื่องของความสัมพันธ์ระหว่างสิ่งมีชีวิตกับสภาวะแวดล้อม) และได้ถูกนำมาใช้เพราะว่ามีความใกล้เคียงกันกับมุมมองทางด้านโซ่อุปทานที่มีเครือข่ายของการปฏิสัมพันธ์
Sheffi (2005, p. 13)	การคืนสภาพได้ เป็นแนวคิดที่ได้ถูกยืมมาจากศาสตร์ทางด้านวัสดุศาสตร์ ที่แสดงให้เห็นถึงความสามารถของวัสดุในการที่จะกลับคืนสู่รูปเดิมได้หลังจากการที่มันถูกทำให้เปลี่ยนสภาพ สำหรับบริษัทแล้ว จะเป็นการวัดถึงความสามารถ (Ability) และความรวดเร็ว (Speed) ในการกลับคืนสู่การดำเนินงานในระดับปกติได้ ทั้งการผลิต การบริการและอัตราการเติมเต็ม หลังจากที่เกิดการรบกวนต่อ HILP (High Impact Low Probability)

ตารางที่ 2.8 (ต่อ)

แหล่งที่มา	นิยามของการคืนสภาพได้ของโซ่อุปทาน
Sheffi and Rice (2005, p. 41)	ความสามารถ (Ability) ของการย้อนกลับ (Bounce Back) จากการรบกวน
Fiksel (2006, p. 16)	ความสามารถ (Capacity) ของบริษัทที่จะทำให้สามารถอยู่รอด (Survive) , ปรับตัว (Adapt), และเติบโต (Grow) ได้ ต่อการเปลี่ยนแปลงที่วุ่นวาย (Turbulent Change)
Peck (2006, p. 132)	ความสามารถ (Ability) ของระบบในการกลับคืนสู่สถานะปกติหรือมากกว่า หลังจากที่ได้ถูกรบกวน ตัวอย่างเช่น ความสามารถในการดูดซับหรือบรรเทาผลกระทบจากการรบกวน
Sarathy (2006, p. 40)	การคืนสภาพได้ของโซ่อุปทาน คือ เรื่องที่ต้องสามารถย้อนกลับ (Bounce Back) อย่างรวดเร็วจากการรบกวน
Datta et al. (2007, p. 189)	การคืนสภาพได้ของโซ่อุปทาน ไม่ได้ถูกนิยามไว้แค่เป็นในเรื่องของความสามารถ (Ability) ในการรักษาการควบคุมผลการดำเนินงานที่จะต้องเปลี่ยนแปลงไปตลอดเวลาที่ต้องเผชิญอยู่กับสิ่งรบกวน แต่จะยังต้องมีคุณสมบัติในเรื่องการปรับตัว (Adaptive) และมีความสามารถ (Capable) ที่จะตอบสนองอย่างยั่งยืนต่อเหตุการณ์ที่เกิดขึ้นอย่างฉับพลัน และการเปลี่ยนแปลงอย่างมีนัยสำคัญของสภาวะแวดล้อมในรูปแบบของความต้องการที่ไม่แน่นอน
Pereira (2009, p. 374)	การสร้างการคืนสภาพได้ของโซ่อุปทานเป็นความสามารถ (Ability) ในการรักษา, การกลับคืน, การกู้คืน สถานะเดิม(หรือสถานะที่ต้องการ) หลังจากที่ได้ถูกรบกวน อีกทั้งมันยังควรจะถูกพิจารณา (และ) เน้นย้ำ จากธรรมชาติที่ควรจะเป็น การคืนสภาพได้จึงควรจะมีความหมายถึงความสามารถ (Ability) ที่จะเปลี่ยนแปลงอย่างราบรื่นและรวดเร็ว โดยอาจจะทำให้เกิดความซ้ำซากหรือความยืดหยุ่นที่เพิ่มขึ้น

ตารางที่ 2.8 (ต่อ)

แหล่งที่มา	นิยามของการคืนสภาพได้ของโซ่อุปทาน
Ponomarov and Holcomb (2009, p. 131)	การปรับเปลี่ยนความสามารถ (Capability) ของโซ่อุปทานในการเตรียมตัวต่อเหตุการณ์ที่ไม่คาดหวัง ตอบสนองต่อการถูกรบกวนและกู้กลับคืนจากเหตุการณ์เหล่านั้น โดยรักษาให้การปฏิบัติงานสามารถที่ดำเนินไปได้อย่างต่อเนื่อง ณ ระดับของการเชื่อมต่อและการควบคุมต่อโครงสร้างและหน้าที่ให้อยู่ในระดับที่สามารถดำเนินการต่อไปได้
Stewart et al. (2009, p. 349)	กระบวนการในการเชื่อมโยงความสามารถในการปรับตัวต่างๆ ให้เป็นไปในแนวทางที่ดีขึ้นหลังจากที่ถูกรบกวน
Voss et al. (2009, p. 6)	ความสามารถ (Ability) ที่ถูกเพิ่มขึ้นในการกู้คืนจากเหตุการณ์ที่อาจเกิดขึ้นได้
Williams et al. (2009, p. 253)	ความสามารถ (Ability) ที่จะตอบสนองต่อสิ่งรบกวนที่ไม่คาดหวังและกู้คืนกลับสู่การทำงานแบบปกติได้
Colicchia et al. (2010, p. 681)	ความสามารถ (Ability) ของระบบในการกลับคืนสู่ระบบเดิม(หรือมากกว่า) หรือเปลี่ยนไปเป็นสถานะใหม่หรือมากกว่า จากการที่ถูกรบกวน
Higgins et al. (2010, p. 964)	การคืนสภาพได้ คือ ความสามารถ (Capacity) ของระบบในการกู้คืนกลับจากการรบกวนและรักษาถึงโครงสร้าง หน้าที่ และการควบคุมให้ดำเนินต่อไปได้
Iakovou et al. (2010, p. 316)	การคืนกู้คืนกลับได้อย่างรวดเร็วจากการรบกวน
Klibi et al. (2010, p. 287 and p. 291)	การคืนสภาพได้คือ ความสามารถ (Capability) ของเครือข่ายของโซ่อุปทานเพื่อที่จะหลีกเลี่ยงต่อการรบกวนหรือการกู้คืนกลับอย่างรวดเร็วจากความล้มเหลว เป็นความสามารถ (Capacity) ของระบบที่จะอยู่รอด ปรับตัว และเติบโตเพื่อต้องเผชิญต่อการเปลี่ยนแปลงที่ไม่คาดคิด รวมไปถึงเหตุการณ์ภัยพิบัติที่เกิดขึ้นด้วย

ตารางที่ 2.8 (ต่อ)

แหล่งที่มา	นิยามของการคืนสภาพได้ของโซ่อุปทาน
Kumar et al. (2010, p. 3721)	การคืนสภาพได้ของเครือข่ายของโซ่อุปทานเป็นความต้องการที่จะสร้างความสามารถ (Ability) ในการรักษา การกลับคืน และการกู้คืนการดำเนินงานให้กลับมาหลังจากที่พบกับการรบกวนใดๆ
Melnyk et al. (2010, p. 34)	การคืนสภาพได้ทำให้มั่นใจได้ว่า โซ่อุปทานจะสามารถถูกกู้กลับคืนสู่สภาพเดิมได้อย่างรวดเร็วและมีประสิทธิภาพทางด้านต้นทุนจากการถูกรบกวน อันเนื่องมาจากเหตุการณ์ภัยพิบัติทางธรรมชาติ (เช่น แผ่นดินไหว) ปัจจัยทางสังคม (เช่นการประท้วงของพนักงาน) เหตุการณ์ฉุกเฉินทางการแพทย์ (เช่นการระบาดของไวรัส H1N1) ความล้มเหลวทางเศรษฐกิจ (เช่นการล้มละลายต่อความเชื่อมต่อที่สำคัญในห่วงโซ่) หรือแม้แต่ความล้มเหลวทางด้านเทคโนโลยี (เช่นวิกฤตการณ์ทางด้านซอฟท์แวร์)
Pettit et al. (2010, p. 1)	ความสามารถ (Capacity) ขององค์กรในการอยู่รอด ปรับตัว และเติบโต เมื่อเผชิญต่อสภาวะการเปลี่ยนแปลงที่วุ่นวาย
Yang and Yang (2010, p. 1903)	ในวรรณกรรม คำว่า "การคืนสภาพได้" ได้มีการนำเอาแนวคิดนี้มาจากความรู้ในสาขาวิชาอื่นๆ เพื่อที่จะนำมาแสดงถึงความสามารถขององค์กร (Organization's Capability) ในการที่กู้คืนกลับสู่การดำเนินงานในสภาวะเริ่มต้นก่อนที่จะมีการรบกวน
Zsidisin and Wagner (2010, p. 3)	การคืนสภาพได้ของโซ่อุปทานประกอบไปด้วย ความสามารถ (Ability) ที่จะกลับคืนสู่ระดับของการดำเนินงานในระดับปกติจากการที่มีการรบกวนเกิดขึ้นในโซ่อุปทาน
Blackhurst et al. (2011, p. 374)	บริษัทต่างๆ สามารถที่จะสร้างการคืนสภาพได้ในเครือข่ายของโซ่อุปทานได้ ที่จะสามารถเพิ่มความสามารถ (Ability) ของบริษัทด้วยการดูดซับการรบกวนหรือทำให้เครือข่ายของอุปทานที่จะกลับคืนสู่เงื่อนไขที่ปกติได้อย่างรวดเร็วอันจะส่งผลกระทบในด้านบวกต่อผลการดำเนินงานของบริษัท ดังนั้นแล้ว ความหมายของ การคืนสภาพได้ของซุ่ปทานคือความสามารถของบริษัทในการที่จะกู้คืนจากเหตุการณ์ที่ถูกรบกวน

ตารางที่ 2.8 (ต่อ)

แหล่งที่มา	นิยามของการคืนสภาพได้ของโซ่อุปทาน
Jüttner and Maklan (2011, p. 247)	การคืนสภาพได้ของโซ่อุปทาน เป็นเรื่องที่เน้นย้ำไปที่ความสามารถ (Ability) ของโซ่อุปทานในการรับมือต่อเหตุการณ์ของความเสี่ยงที่หลีกเลี่ยงไม่ได้เพื่อที่จะกลับคืนไปสู่การดำเนินงานในสภาวะเดิมหรือสภาวะใหม่ หรือสถานะที่ต้องการหลังจากที่ถูกรบกวน
Kumar and Sosnoski (2011, p. 5432)	บริษัทที่มีการคืนสภาพได้จะต้องมีความสามารถ (Ability) ที่จะต้านทานต่อเหตุการณ์ที่ไม่คาดหวังได้
Thomsett (2011, p. 49)	การคืนสภาพได้นี้ คือ กลยุทธ์ทางธุรกิจที่เหมาะสมที่จะหลีกเลี่ยงจุดของความล้มเหลวอันเนื่องมาจากความเสี่ยงที่ไม่คาดคิด (โอกาสที่ต่ำ , ความเสี่ยงที่สูง)
Verbano and Venturini (2011, p. 533)	ความสามารถ (Ability) ที่จะกู้คืนจากความสูญเสีย โดยให้เกิดผลกระทบจากสถานการณ์ของความเสี่ยงที่น้อยที่สุด
Cabral et al. (2012, p. 4831)	การคืนสภาพได้คือ ความสามารถ (Ability) ของโซ่อุปทานต่อเหตุการณ์ที่ถูกรบกวนที่ไม่คาดคิด การคืนสภาพได้ของโซ่อุปทาน จะเกี่ยวข้องกับความสามารถของระบบที่จะกลับคืนสู่สถานะเริ่มต้นหรือสถานะใหม่ที่มีความต้องการที่มากขึ้นหลังจากที่ต้องพบกับความสิ่งที่รบกวน และเพื่อหลีกเลี่ยงต่อเหตุการณ์ความล้มเหลวที่เกิดขึ้น
Carvalho et al. (2012, p. 331)	การคืนสภาพได้ของโซ่อุปทานจะเกี่ยวข้องกับ ความสามารถ (Ability) ของระบบในการกลับคืนสู่สถานะเริ่มต้นหรือมากกว่าหรือที่ต้องการหลังจากที่ได้ถูกรบกวนและหลีกเลี่ยงต่อการดำเนินงานที่ล้มเหลว
Ishfaq (2012, p. 216)	การคืนสภาพได้ของโซ่อุปทาน คือความสามารถ (Ability) ในการที่จะรักษาความต่อเนื่องของการดำเนินงานให้สามารถดำเนินต่อไปได้ภายใต้สภาวะของการถูกการรบกวน

ตารางที่ 2.8 (ต่อ)

แหล่งที่มา	นิยามของการคืนสภาพได้ของโซ่อุปทาน
Levesque (2012, p. 69)	ความสามารถ (Ability) ที่จะกู้คืนกลับจากการเจ็บป่วย การเปลี่ยนแปลง หรือความโชคร้าย
Machowiak (2012, p. 280f.)	การคืนสภาพได้ของโซ่อุปทานคือความสามารถในการต้านทานต่อผลกระทบที่เกิดจากการรบกวนและภัยพิบัติต่อโซ่อุปทาน โดยไม่มีผลกระทบต่อทั้งลูกค้าในขั้นสุดท้ายและต้นทุนในการกู้คืน
Mandal (2012, p. 46)	ความสามารถ (Ability) ในการกลับคืนสู่สถานะของการดำเนินงานแบบเดิมหลังจากที่ได้ถูกรบกวน
Ponis and Koronis (2012, p. 925f.)	ความสามารถ (Ability) ในการวางแผนเชิงรุกและการออกแบบเครือข่ายโซ่อุปทานสำหรับการรับมือต่อเหตุการณ์ที่ไม่คาดคิด (เชิงลบ) และการตอบสนองต่อเหตุการณ์ที่ถูกรบกวนในขณะที่มีการรักษาและควบคุมถึงโครงสร้างและหน้าที่ให้สามารถดำเนินงานกลับไปยังสถานะเดิม
Schmitt and Singh (2012, p. 23)	การคืนสภาพได้ เป็นเรื่องให้เน้นถึงความสามารถของบริษัทในการดำเนินงานที่ยั่งยืนและสามารถกู้คืนได้อย่างรวดเร็วเมื่อเผชิญกับสิ่งรบกวน
Spiegler et al. (2012, p. 6163)	ความสามารถของระบบในการกลับสู่สถานะเดิมหรือใหม่กว่าหรือมากกว่าหลังจากที่ถูกรบกวน
Xiao et al. (2012, p. 2)	การคืนสภาพได้ของโซ่อุปทานสามารถนิยามได้เป็นความสามารถ (Ability) ของโซ่อุปทานในการกลับคืนไปสู่สถานะเดิมหรือสถานะในอุดมคติเมื่อระบบโซ่อุปทานได้ถูกรบกวนโดยการกระทำจากภายนอก และการคืนสภาพได้ของโซ่อุปทานจะแสดงให้เห็นความสามารถ 2 อย่างในการปรับตัวเข้ากับสภาวะแวดล้อมและความสามารถที่กู้คืนของระบบ
Golgeci and Ponomarov (2013, p. 604)	โซ่อุปทานที่มีความสามารถ (Capability) ในการปรับตัวเพื่อเตรียมพร้อมสำหรับเหตุการณ์ที่ไม่คาดหวัง ตอบสนองต่อการรบกวน และกู้คืนได้โดยมีการดำเนินงานที่ต่อเนื่อง

ตารางที่ 2.8 (ต่อ)

แหล่งที่มา	นิยามของการคืนสภาพได้ของโซ่อุปทาน
Hearnshaw and Wilson (2013, p. 458)	สำหรับระบบโซ่อุปทานนั้น การคืนสภาพได้ถือเป็นเรื่องที่สำคัญของบริษัทที่จะทำให้สำเร็จได้ด้วยการพิจารณาถึงความสามารถ (Ability) ของระบบทั้งหมดในการดำเนินงานให้เกิดความต่อเนื่องถึงแม้จะมีการรบกวนก็ตาม
Johnson et al. (2013, p. 325)	การคืนสภาพได้ถูกพิจารณาว่าจะต้องมีการพัฒนาตลอดเวลา ซึ่งจะเป็นเรื่องที่ทำให้องค์กรหรือเครือข่ายอยู่รอดและเติบโตได้ดีเมื่ออยู่ในสถานการณ์ที่ไม่ดี เพื่อวัตถุประสงค์ที่จะสร้างความแข็งแกร่งสำหรับที่จะสร้างการปรับตัวในอนาคต
Pettit et al. (2013, p. 46)	การคืนสภาพได้ - ความสามารถที่จะอยู่รอด ปรับตัว และเติบโตเมื่อเผชิญหน้าต่อการเปลี่ยนที่เกิดขึ้น
Sawik (2013, p. 260)	การคืนสภาพได้แสดงให้เห็นถึงความสามารถ (Capacity) ของบริษัทที่จะอยู่รอด ปรับตัว และ เติบโตได้เมื่อเผชิญหน้าต่อการเปลี่ยนแปลงและความไม่แน่นอน
Wieland (2013, p. 655)	โซ่อุปทานสามารถที่จะมีการคืนสภาพได้ได้ ถ้าสถานะของการดำเนินงานในสถานะเริ่มต้นมีความมั่นคงหรือถ้าการดำเนินการในสถานะใหม่ถูกทำให้สำเร็จ โดยที่สามารถกลับคืนสู่สถานะเดิมได้จากการถูกรบกวน โซ่อุปทานจะมีการคืนสภาพได้ได้ถ้ามีการใช้ทรัพยากรที่สามารถรับมือกับการเปลี่ยนแปลงได้
Wieland and Wallenburg (2013, p. 301)	โซ่อุปทานสามารถที่เกิดมีการคืนสภาพได้ได้ ถ้าสถานะเริ่มต้นมีความมั่นคงหรือสถานะใหม่ถูกทำให้สำเร็จ ในงานวิจัยนี้ การคืนสภาพได้ถูกทำให้เข้าใจได้ว่าเป็นความสามารถของโซ่อุปทานที่จะรับมือต่อการเปลี่ยนแปลงได้
Wu et al. (2013, p. 676)	การคืนสภาพได้ คือ ความสามารถที่จะตอบสนองและกู้คืนจากการหยุดชะงัก

จากนั้นมา ได้มีผู้วิจัยหลายท่าน ได้ทำดำเนินการวิจัยในประเด็นของการคืนสภาพได้ของโซ่อุปทานเพิ่มมากขึ้น ดังที่ได้กล่าวไว้ข้างต้นแนวความคิดการคืนสภาพได้ของโซ่อุปทานที่ได้ถูกนำเสนอในงานวิจัยที่หลากหลาย โดยจะเห็นได้ว่าได้มีการนำเสนอถึงมิติต่าง ๆ ภายใต้ปรากฏการณ์ที่แตกต่างกัน นอกจากนี้การคืนสภาพได้ของโซ่อุปทานนี้ยังได้เป็นแนวคิดที่ค่อนข้างใหม่ ที่ได้มีการทำการวิจัยอยู่ภายใต้แนวคิดของการจัดการความเสี่ยงซึ่งมีอยู่อย่างมากมาย ดังนั้นผู้วิจัยจึงได้ทำการทบทวนวรรณกรรม เพื่อทำศึกษาให้ทราบถึงคำนิยามของการคืนสภาพได้ของโซ่อุปทาน (Supply Chain Resilience) ให้มีความชัดเจนมายิ่งขึ้น จากการศึกษาของ Ponomarov (2009) ได้ให้ความหมายของ การคืนสภาพได้ของโซ่อุปทาน โดยได้พัฒนามาจากมุมมองในหลาย ๆ สาขาวิชา จากการศึกษา Ponomarov ได้นิยามความหมายของการคืนสภาพได้ของโซ่อุปทาน ไว้ดังนี้ “การคืนสภาพได้ของโซ่อุปทาน คือ ความสามารถในการปรับตัวของโซ่อุปทาน เพื่อเตรียมความพร้อม (Readiness) สำหรับเหตุการณ์ที่ไม่คาดคิด และต้องสามารถที่จะตอบสนอง (Response) ต่อการหยุดชะงัก และต้องสามารถที่จะทำการกู้คืน (Recovery) ได้จากเหตุการณ์ต่าง ๆ เหล่านั้น โดยจะต้องทำการรักษาความต่อเนื่องของการดำเนินงานให้อยู่ในระดับที่ต้องการ และจะต้องมีการรักษาและควบคุมต่อโครงสร้างและหน้าที่ต่างๆ ที่มีอยู่ในโซ่อุปทาน”

การศึกษาถึงคำนิยามของการคืนสภาพได้ ทำให้ทราบได้ว่าการคืนสภาพได้นั้นได้มีการศึกษาไว้จากนักวิจัย นักวิชาการ ต่าง ๆ ที่ทำให้สามารถระบุได้ว่า การคืนสภาพได้นั้นเป็นองค์ความรู้ที่มาจากองค์ประกอบสำคัญ ๆ ที่ได้มาจากในหลายสาขาวิชา โดยเฉพาะคำว่า “ความสามารถในการปรับตัว” ซึ่งเป็นคุณลักษณะของการคืนสภาพได้นั้น จะได้มาจากความหมายของการคืนสภาพได้ที่ได้กล่าวไว้ก่อนหน้านี้ ดังนั้นความหมายของความสามารถในการปรับตัว คือ องค์ประกอบที่สำคัญของระบบนิเวศที่มีความยืดหยุ่น ต้องสามารถที่จะทำการตอบสนองและการกู้คืนกลับไปที่สถานะเดิมหรือสถานะที่ดีกว่า โดยจากความหมายที่ได้มานี้เป็นความหมายที่ได้อธิบายถึงลักษณะทั่ว ๆ ไปของการคืนสภาพได้ ที่เกิดมาจากมุมมองในทุก ๆ มุมมอง ที่ได้ทำการศึกษา อันประกอบไปด้วย มุมมองทางด้านนิเวศวิทยา สังคม จิตวิทยา เศรษฐศาสตร์ องค์กรและการจัดการเหตุฉุกเฉิน ดังที่ได้กล่าวไว้แล้วในตอนต้น

เมื่อเกิดเหตุการณ์ที่ทำให้มีการหยุดชะงักเกิดขึ้น การรักษาและการควบคุมต่อโครงสร้างและหน้าที่ต่าง ๆ ถือว่าเป็นคุณสมบัติหลักของการคืนสภาพได้ของระบบนิเวศ โดยที่ลักษณะดังกล่าวนี้จะพบได้จากมุมมองทางด้านองค์กร ที่สถานะของการคืนสภาพได้เป็นสถานะที่มีความสามารถที่จะรักษาไว้ซึ่งหน้าที่ที่ต้องรับผิดชอบ รวมไปถึงผลลัพธ์ที่ต้องการได้ภายใต้ช่วงเวลาที่มีความตึงเครียด ในขณะที่มุมมองทางด้านจิตวิทยา แสดงให้เห็นว่า คุณลักษณะของการคืนสภาพได้ที่สามารถนำมาใช้เสริมเพื่อการกำหนดทิศทางในการดำเนินงาน และเพื่อสร้าง

ความเข้าใจในการดำเนินงานได้นั้นจะต้องประกอบไปด้วยหลัก 3C อันได้แก่ การควบคุม (Control) การเชื่อมโยง (Coherence) และการเชื่อมต่อ (Connectedness) โดยหลักการทั้ง 3 นี้ จะสามารถนำมาเพื่อใช้ในการปรับปรุงในเรื่องของการตอบสนองได้เมื่อเกิดภัยพิบัติทางธรรมชาติหรือที่มนุษย์ทำขึ้น

จากงานวิจัยที่ผู้วิจัยได้ทำการศึกษา ทบทวนวรรณกรรม ทำให้ได้พบว่า การคืนสภาพได้ของโซ่อุปทาน คือ ความสามารถของโซ่อุปทานที่จะต้องทำการปรับตัวภายใต้สภาวการณ์ที่มีการเปลี่ยนแปลง Christopher (2005) แสดงให้เห็นว่า กระบวนการของการคืนสภาพได้ (Resilience Process) เป็นกระบวนการที่ประกอบไปด้วยความยืดหยุ่น (Flexibility) และคล่องตัว (Agility) และต้องสามารถที่จะเปลี่ยนแปลงอย่างรวดเร็ว ลักษณะของความสามารถในการปรับตัวนี้ จะช่วยให้โซ่อุปทานสามารถถูกกู้คืนกลับคืนมาได้หลังจากที่ถูกทำให้หยุดชะงักลง โดยการกลับคืนมานั้นสามารถที่จะให้กลับคืนมาสู่สถานะเดิม หรือในสถานะที่มากกว่าเดิมขึ้นอยู่กับความต้องการจากการดำเนินการในโซ่อุปทาน แนวความคิดของ Christopher ได้กล่าวถึงปัจจัยที่มีต่อการคืนสภาพได้ของโซ่อุปทาน จะประกอบไปด้วยองค์ประกอบ ดังนี้ กลยุทธ์พื้นฐานในด้านการจัดหา (Supply Base Strategy) การวางแผนการทำงานร่วมกัน (Collaborative Planning) ความชัดเจน (Visibility) และปัจจัยความเสี่ยง (Factoring Risk) ที่ได้นำมาพิจารณาเพื่อการตัดสินใจ ในขณะที่ Wieland et al. (2012) ได้ทำการศึกษาเพื่อแสดงให้เห็นถึงความแตกต่างระหว่างองค์ประกอบของการคืนสภาพได้ซึ่งได้แก่ ความคล่องตัว (Agility) และความทนทาน (Robustness) โดยการศึกษาของ Wieland ได้พบว่า ความสามารถเชิงสัมพันธ์ (Relational Competency) ซึ่งได้แก่ การสื่อสาร (Communication) ความร่วมมือกัน (Cooperation) และการบูรณาการ (Integration) เป็นปัจจัยที่ส่งผลกระทบต่อการคืนสภาพได้ของโซ่อุปทาน

ในส่วนขององค์ประกอบของการคืนสภาพได้ (Resilience) ของโซ่อุปทานดิจิทัล ทางผู้วิจัยได้ทำการทบทวนวรรณกรรมและได้ทำการสรุปถึง องค์ประกอบของการคืนสภาพได้ของโซ่อุปทานดิจิทัล ไว้ดังตารางที่ 2.9 ดังนี้

ตารางที่ 2.9 องค์ประกอบของการคืนสภาพได้ของโซ่อุปทานดิจิทัล

แหล่งที่มา	**องค์ประกอบ**	**คำอธิบาย**
Hong and Choi (2002)	1. โครงสร้าง (Structure) 2. ความรู้ (Knowledge)	ความรู้และความเข้าใจต่อโครงสร้างของโซ่อุปทานทั้งภายภาพและสารสเทศเป็นองค์ประกอบที่สำคัญของการคืนสภาพได้ของโซ่อุปทาน

ตารางที่ 2.9 (ต่อ)

แหล่งที่มา	องค์ประกอบ	คำอธิบาย
Chopra and Sodhi (2004)	1. ความชัดเจน (Visibility)	การเพิ่มขึ้นถึงความชัดเจนของข้อมูลความต้องการสินค้าที่มีต่อโซ่อุปทานจะเป็นการลดความเสี่ยงได้
(Sinha et al., 2004; Lee, 2004)	1. ความร่วมมือกัน (Collaboration)	การร่วมมือกันของคู่ค้าจะเป็นตัวช่วยจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ
Smith (2004)	1. การบูรณาการ (Integration) 2. ความสามารถในการปฏิบัติการ (Operational Capabilities) 3. ความโปร่งใส (Transparency)	ในการอธิบายถึง ความสามารถในการปฏิบัติการของการคืนสภาพได้ของโซ่อุปทาน Smith ได้ทำให้เห็นถึงความ สำคัญ ของสภาพแวดล้อมรวมที่ให้การทำงานร่วมกันแบบ end-to-end ของการสั่งซื้อ , สินค้าคงคลัง, การขนส่งและการกระจายเพื่ออำนวยความสะดวกให้กับโซ่อุปทาน
Christopher (2004)	1. ความคล่องตัว (Agility) 2. การตอบสนอง (Responsiveness)	ความคล่องตัวจะเป็นวิธีการที่ดีที่สุดวิธีการหนึ่งในการที่จะบรรลุถึงการคืนสภาพได้ในโซ่อุปทาน โดยที่เครือข่ายในโซ่อุปทานที่มีความคล่องตัวจะสามารถตอบสนองได้อย่างรวดเร็วต่อสภาวะที่มีการเปลี่ยนแปลง
Christopher (2005)	1. ความยืดหยุ่น (Flexibility) 2. ความฟุ่มเฟือย (Redundancy)	ได้กล่าวไว้ว่ากระบวนการทางด้านการคืนสภาพได้จะเป็นกระบวนการที่มีความยืดหยุ่นและคล่องตัวและต้องสามารถเปลี่ยนแปลงได้อย่างรวดเร็วความยืดหยุ่นจะช่วยให้ผู้ผลิตสามารถที่ตอบสนองได้อย่างรวดเร็วและมีประสิทธิภาพต่อการเปลี่ยนแปลงของตลาด (Swamidass and Newell, 1987). Rice and Caniato (2003) ได้เสนอไว้ว่าวิธีการของความยืดหยุ่นและความฟุ่มเฟือยที่มีลักษณะเป็นแบบ Hybrid Flexibility/Redundancy จะช่วยเพิ่มการคืนสภาพได้ให้กับโซ่อุปทาน

ตารางที่ 2.9 (ต่อ)

แหล่งที่มา	องค์ประกอบ	คำอธิบาย
Sheffi and Rice (2005)	1. ความยืดหยุ่น (Flexibility) 2. ความฟุ่มเฟือย (Redundancy)	ความสามารถขององค์กรในการที่จะฟื้นตัวมาจากการหยุดชะงักได้อย่างรวดเร็วนั้นจะมาจากการพัฒนาถึง Redundancy กับ ความยืดหยุ่นเข้าไปในโซ่อุปทาน ซึ่งการลงทุนใน Redundancy เห็นได้ชัดว่าจะเป็นการเพิ่มต้นทุนแต่การลงทุนในเรื่องของความยืดหยุ่นจะเป็นการเพิ่มประสิทธิภาพในการทำงานในแต่ละวันได้
Ponomarov (2009)	1. ความคล่องตัว (Agility) 2. ความชัดเจน (Visibility) 3. ความยืดหยุ่น (Flexibility) 4. ความร่วมมือกัน (Collaboration)	การศึกษาในเรื่องขององค์ประกอบหลักๆ ของการคืนสภาพได้ของโซ่อุปทานได้มีการแยกการทำการศึกษา จากนักวิจัยที่ผ่านๆ มาโดย Panomarov ได้รวบรวมถึงองค์ประกอบหลักเหล่านั้นไว้เพื่อการศึกษาต่อในอนาคตได้
Wieland et al. (2012)	1. ความคล่องตัว (Agility) 1.1 ความเร็ว (Speed) 1.2ความชัดเจน (Visibility) 2. ความทนทาน (Robustness) 2.1ความคาดหวัง (Anticipation) 2.2การเตรียมความพร้อม (Preparedness)	ในการพัฒนาการคืนสภาพได้ให้เกิดมีขึ้นในโซ่อุปทานนั้น ความคล่องตัวและความทนทานเป็นสิ่งที่ต้องถูกพัฒนาตามไปด้วย
Scholten et al. (2015)	1. ความชัดเจน (Visibility) 2. ความเร็ว (Velocity) 3. ความยืดหยุ่น (Flexibility)	การเพิ่มขึ้นของการคืนสภาพได้ของโซ่อุปทานจะเป็นผลทำให้เกิดความชัดเจน ความเร็ว และความยืดหยุ่นเกิดขึ้นในโซ่อุปทาน

จากการศึกษาผู้วิจัยพบว่าการวิจัยที่เกี่ยวกับการคืนสภาพได้ของโซ่อุปทานดิจิทัลยังเป็นภาพของแนวความคิดแบบองค์รวม โดยการศึกษาเป็นเพียงศึกษาในประเด็นขององค์ประกอบที่สำคัญหลาย ๆ องค์ประกอบที่เกี่ยวข้องกับการคืนสภาพได้กับโซ่อุปทาน แต่ในเชิงของการอธิบายถึงความสัมพันธ์ระหว่างองค์ประกอบเหล่านั้น ความเชื่อมเชื่อมโยงกันระหว่างองค์ประกอบเหล่านั้น รวมถึงผลกระทบที่มีต่อการจัดการโซ่อุปทาน และ ระเบียบวิธีในการจัดการกับองค์ประกอบเหล่านั้นยังมีความเข้าใจที่น้อยอยู่ ซึ่งสอดคล้องกับงานวิจัยของ Blackhurst et al. (2005) นอกจากนี้ผู้วิจัยพบว่าบทความที่เกี่ยวข้องกับการคืนสภาพได้ของโซ่อุปทานจะยังมีกล่าวถึงไว้อยู่น้อยมาก ที่ผ่านมาการศึกษาในเรื่องของการคืนสภาพได้ของโซ่อุปทานที่มีอยู่เป็นเพียงแค่การให้ความรู้เท่านั้น สิ่งที่ปรากฏอยู่ในงานวิจัยที่มีอยู่นั้นส่วนมากจะเน้นไปที่การนำเสนอมุมมองในหลาย ๆ แง่มุม ของปรากฏการณ์ที่เกิดขึ้น (Shefi, 2001; Christopher and Lee, 2004; Christopher et al., 2002; Shefi et al., 2003)

โดยจากงานวิจัยที่ผ่าน ๆ มานั้น ผู้วิจัยที่ทำการวิจัยในเรื่องของการคืนสภาพได้ของโซ่อุปทานนี้ ต่างก็มุ่งเน้นไปที่การทำความเข้าใจต่อความสำคัญของการคืนสภาพได้ที่จะมีผลต่อโซ่อุปทานเท่านั้น โดยผู้วิจัยได้ทำการศึกษาถึงผลกระทบต่อการคืนสภาพได้ของโซ่อุปทาน โดยสามารถสรุปปัจจัยต่างๆ ที่มีผลต่อการคืนสภาพได้ของโซ่อุปทานได้ดังตารางที่ 2.10 จะเห็นได้ว่าปัจจัยที่ปัจจัยที่มีผลต่อการคืนสภาพได้ของโซ่อุปทานนั้นจะประกอบได้ด้วย การจัดการความเสี่ยงของโซ่อุปทาน (Supply Chain Risk Management) ความสามารถของโซ่อุปทาน (Supply Chain Competency) ความร่วมมือกันของโซ่อุปทาน (Supply Chain Collaboration) การรีเอ็นจิเนียริ่งของโซ่อุปทาน (Supply Chain Reengineering) ความคล่องตัวของโซ่อุปทาน (Supply Chain Agility) และ การบูรณาการของโซ่อุปทาน (Supply Chain Integration)

ตารางที่ 2.10 ปัจจัยที่มีผลต่อการคืนสภาพได้ของโซ่อุปทานดิจิทัล

	แหล่งที่มา	**ความสามารถของโซ่อุปทาน**	**การรีเอ็นจิเนียริ่งของโซ่อุปทาน**	**ความร่วมมือกันของโซ่อุปทาน**	**ความคล่องตัวของโซ่อุปทาน**	**ความเสี่ยงของโซ่อุปทาน**	**การบูรณาการของโซ่อุปทาน**
1	Rice and Caniato (2003)	✓					

ตารางที่ 2.10 (ต่อ)

	แหล่งที่มา	ความสามารถของโซ่อุปทาน	การรีเอ็นจิเนียริ่งของโซ่อุปทาน	ความร่วมมือกันของโซ่อุปทาน	ความคล่องตัวของโซ่อุปทาน	ความเสี่ยงของโซ่อุปทาน	การบูรณาการของโซ่อุปทาน
2	Christopher and Peck (2004)		✓	✓	✓	✓	
3	Peck (2005)					✓	
4	Fiksel (2006)					✓	
5	Peck (2006)					✓	
6	Sarathy (2006)			✓			
7	Datta et al. (2007)					✓	
8	Pereira (2009)			✓		✓	✓
9	Ponomarov and Holcomb (2009)	✓				✓	
10	Voss et al. (2009)					✓	
11	Williams et al. (2009)					✓	
12	Colicchia et al. (2010)					✓	
13	Iakovou et al. (2010)					✓	
14	Klibi et al. (2010)					✓	
15	Kumar et al. (2010)					✓	
16	Pettit et al. (2010)	✓				✓	

ตารางที่ 2.10 (ต่อ)

	แหล่งที่มา	ความสามารถของโซ่อุปทาน	การรีเอ็นจิเนียริ่งของโซ่อุปทาน	ความร่วมมือกันของโซ่อุปทาน	ความคล่องตัวของโซ่อุปทาน	ความเสี่ยงของโซ่อุปทาน	การบูรณาการของโซ่อุปทาน
17	Yang and Yang (2010)					✓	
18	Zsidisin and Wagner (2010)					✓	
19	Jüttner and Maklan (2011)	✓				✓	
20	Verbano and Venturini (2011)					✓	
21	Levesque (2012)					✓	
22	Machowiak (2012)					✓	
23	Mandal (2012)		✓	✓	✓	✓	
24	Ponis and Koronis (2012)	✓					
25	Schmitt and Singh (2012)					✓	
26	Xiao et al. (2012)					✓	
27	Golgeci and Ponomarov (2013)					✓	
28	Hearnshaw and Wilson (2013)					✓	
29	Pettit et al. (2013)					✓	
30	Sawik (2013)					✓	
31	Wieland and Wallenburg (2013)	✓					

ตารางที่ 2.10 (ต่อ)

	แหล่งที่มา	ความสามารถของโซ่อุปทาน	การรีเอ็นจิเนียริ่งของโซ่อุปทาน	ความร่วมมือกันของโซ่อุปทาน	ความคล่องตัวของโซ่อุปทาน	ความเสี่ยงของโซ่อุปทาน	การบูรณาการของโซ่อุปทาน
32	Richard Wilding (2013)		✓	✓	✓	✓	
33	Aigbogun1 et al.(2014)	✓				✓	
34	Kirstin Scholten Sanne Schilder , (2015)			✓			

จากการทบทวนวรรณกรรมในประเด็นของปัจจัยที่ส่งผลต่อการคืนสภาพได้ของโซ่อุปทานดิจิทัลนี้ ผู้วิจัยสรุปได้ว่า ปัจจัยที่จะส่งผลต่อความหยุ่นของโซ่อุปทานที่จะได้นำมาศึกษาในงานวิจัยฉบับนี้ จะประกอบไปด้วย การจัดการความเสี่ยงของโซ่อุปทาน ความสามารถของโซ่อุปทาน ความร่วมมือกันของโซ่อุปทาน โดยที่ปัจจัยดังกล่าวในงานวิจัยที่ผ่านนั้น แสดงถึงปัจจัยที่ส่งผลการคืนสภาพได้ของโซ่อุปทานที่มีการกล่าวถึงเฉพาะปัจจัยเดียว (Rice and Caniato (2003); Peck (2005); Fiksel (2006); Peck (2006); Sarathy (2006); Datta et al. (2007); Voss et al. (2009); Williams et al. (2009); Colicchia et al. (2010); Iakovou et al. (2010); Klibi et al. (2010); Kumar et al. (2010); Yang and Yang (2010); Zsidisin and Wagner (2010); Verbano and Venturini (2011); Levesque (2012); Machowiak (2012); Ponis and Koronis (2012); Schmitt and Singh (2012); Xiao et al. (2012); Golgeci and Ponomarov (2013); Hearnshaw and Wilson (2013); Pettit et al. (2013); Sawik (2013); Wieland and Wallenburg (2013); Kirstin Scholten Sanne Schilder (2015)) หรืออาจจะมีการกล่าวไว้เพียงแค่ 2 ปัจจัย (Christopher and Peck (2004); Pereira (2009); Ponomarov and Holcomb (2009); Pettit et al. (2010); Jüttner and Maklan (2011); Mandal (2012); Richard Wilding (2013); Aigbogun1 et al.(2014)) แต่การพิจารณาถึงปัจจัยทั้ง 3 ที่ล้วนแต่มีความสำคัญต่อการคืนสภาพได้ของโซ่อุปทานจะยังไม่มีการกล่าวถึง ในขณะที่ก็ยังไม่มีทฤษฎีใดๆ ที่แสดงให้เห็นถึงตัวแบบทางด้านการคืนสภาพได้ จากการศึกษาในเรื่องของการคืนสภาพได้ที่เกิดขึ้นในสาขาวิชาอื่นๆ ดังที่ได้กล่าวมา ประกอบกับจากงานวิจัยที่ได้ทำการทบทวนมาก็เป็นสิ่ง

ยืนยันให้เห็นว่า การคืนสภาพได้นี้ยังอยู่ในขั้นของการพัฒนาในสาขาวิชาต่างๆ ดังนั้นเหล่านี้จึงเป็นโอกาสที่ดีที่จะได้นำมาใช้เพื่อนำไปวิจัยเชิงวิชาการต่อไปได้ ดังนั้นแล้ว งานวิจัยนี้จะได้ทำการศึกษาจากปัจจัยทั้ง 3 ที่จะส่งผลต่อการคืนสภาพได้ของโซ่อุปทานต่อไป

2.5.3 การคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล

การคืนสภาพได้ของโซ่อุปทานดิจิทัล เป็นกลยุทธ์ที่มีบทบาทสำคัญในการสร้างความมั่นใจในการสร้างต่อเนื่องทางด้านธุรกิจและความน่าเชื่อถือในการบริหารต้นทุนที่มีประสิทธิภาพ การป้องกันหรือการกู้คืนจากสถานการณ์ใด ๆ อันทำให้เกิดการหยุดชะงักนั้นจำเป็นต้องมีการเข้าถึงและการวิเคราะห์ข้อมูลจำนวนมาก ยิ่งไปกว่านั้นถ้าการคืนสภาพได้ของโซ่อุปทานดิจิทัล จะต้องนำมาพิจารณาในบริบทที่มีผู้ที่มีส่วนได้ส่วนเสีย การปฏิบัติการ หรือแม้แต่กระทั่งในด้านสิ่งแวดล้อมที่หลากหลาย ในฐานะของการเป็นกลยุทธ์ที่สำคัญทางด้านธุรกิจที่ซึ่งมีการปฏิบัติการ การจัดการความเสี่ยง จึงทำให้การคืนสภาพได้ของโซ่อุปทานดิจิทัล ได้กลายมาเป็นงานที่ท้าทาย ไม่เพียงแต่ในองค์กร หรือในโซ่อุปทาน แต่ยังเป็นไปในระดับโลกได้อีกด้วย ดังนั้นแล้วด้วยเหตุผลที่ เทคโนโลยีสารสนเทศและการสื่อสารที่มีการพัฒนาขึ้นอยู่เรื่อย ๆ เพื่อช่วยเหลือผู้จัดการโซ่อุปทาน ด้วยการพัฒนาเครื่องมือและบริการเพื่อที่จะนำมาใช้สำหรับการตรวจสอบการหยุดชะงัก สามารถที่จะสนับสนุนการสื่อสารและอำนวยความสะดวกในการฟื้นตัวอย่างรวดเร็วของโซ่อุปทาน บริษัทต่าง ๆ สามารถเตรียมความพร้อมสำหรับการโจมตีที่อาจเกิดขึ้นโดยการใช้เครื่องมือและเทคนิคสำหรับการจัดการความเสี่ยงของโซ่อุปทานที่เหมาะสม ทั้งนี้ก็เพื่อเป็นการลดโอกาสของการเกิดการบุกรุกและ เพื่อที่จะจัดการกับการหยุดชะงักใด ๆ ก่อนที่การโจมตีนั้นประสบความสำเร็จขึ้นได้ ในทุก ๆ ธุรกิจที่ขึ้นอยู่กับโซ่อุปทาน จำเป็นต้องที่จะต้องมีความต้องการที่จะสร้างการคืนสภาพได้ทางด้านไซเบอร์

จากการทบทวนวรรณกรรม พบว่า นักวิจัยและนักวิชาการได้ให้คำนิยามหรือคำจำกัดความของคำว่า การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) ไว้ดังตารางที่ 2.11 ดังต่อไปนี้

ตารางที่ 2.11 คำนิยามหรือคำจัดความของการคืนสภาพได้ทางไซเบอร์

แหล่งที่มา	**ความหมายของของการคืนสภาพได้ทางไซเบอร์**
ASIC (2015)	การคืนสภาพได้ทางไซเบอร์ คือ ความสามารถที่เตรียมพร้อมสำหรับตอบสนองและกู้คืนจากเหตุการณ์ที่ถูกโจมตีทางไซเบอร์ การคืนสภาพได้

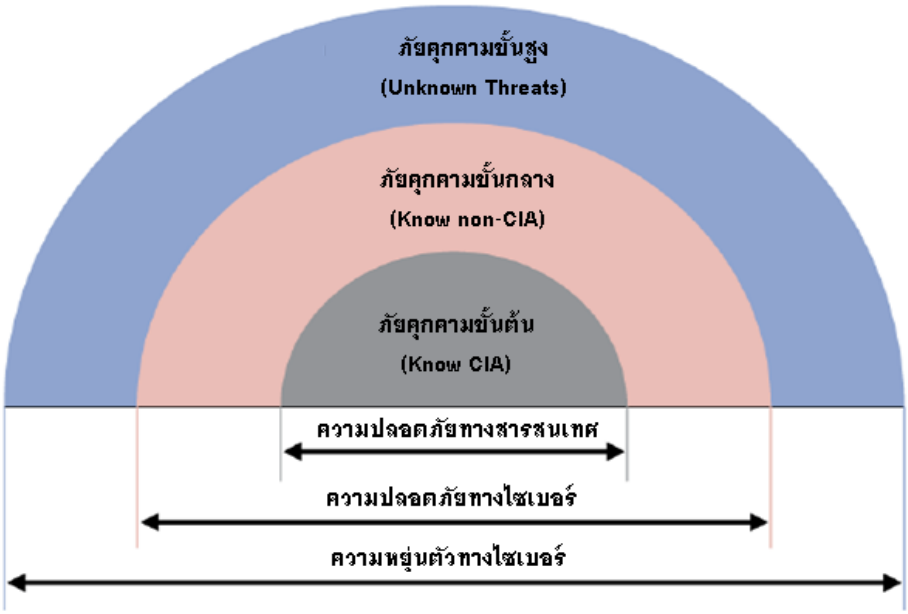
ตารางที่ 2.11 (ต่อ)

แหล่งที่มา	ความหมายของของการคืนสภาพได้ทางไซเบอร์
	ทางไซเบอร์นี้จะเป็นการกระทำที่มากกว่าการป้องกันและตอบสนองต่อการโจมตี กล่าวคือ จะต้องสามารถปรับตัวและกู้คืนได้จากเหตุการณ์
F. Bj. Rck (2015)	การคืนสภาพได้ทางไซเบอร์ คือ ความสามารถในการส่งมอบผลลัพธ์ที่ตั้งใจไว้อย่างต่อเนื่องแม้จะมีเหตุการณ์ที่ไม่พึงประสงค์เกิดขึ้นในโลกไซเบอร์ และคำนิยามนี้ได้มีการอธิบายไว้อย่างเป็นระบบและมีเหตุผลพื้นฐานในการสร้างกรอบของการคืนสภาพได้ทางไซเบอร์ได้มีการกำหนดและวิเคราะห์จากความแตกต่างกันระหว่างการคืนสภาพได้ทางไซเบอร์กับความมั่นคงปลอดภัยไซเบอร์
PPD-21 (2015)	การคืนสภาพได้ทางไซเบอร์ คือ ความสามารถในการเตรียมความพร้อมสำหรับปรับตัวสู่เงื่อนไขของการเปลี่ยนแปลง ทน และกู้คืนกลับได้อย่างรวดเร็วจากการหยุดชะงัก การคืนสภาพได้ดังกล่าวนี้จะประกอบไปด้วย ความสามารถในการทน และกู้คืนกลับมาจากการโจมตี อุบัติเหตุ หรือภัยธรรมชาติ ที่ทำให้เกิดภัยคุกคามขึ้น
Symantec (2014)	ภายใต้สภาวะแวดล้อมที่มีภัยคุกคามทางไซเบอร์เกิดขึ้น เทคนิคการรักษาความปลอดภัยแบบดั้งเดิมไม่สามารถใช้การ วิธีการดั้งเดิมไม่ว่าจะเป็นการเพิ่มสินค้าที่จุดอื่น หรือ รอให้มีการนำเอาเทคโนโลยีมาแก้ปัญหาแบบเดิมๆ จะไม่สามารถนำมาใช้ได้ ไม่มีองค์กรใดๆ สามารถที่จะมองข้ามผ่านเรื่องของการแจ้งเตือน การตรวจสอบถึงช่องโหว่อันจะเป็นผลเสียต่อองค์กร การนำเอานโยบายการรักษาความปลอดภัยไปใช้กับระบบทั้งหลาย รวมทั้งการเข้าถึงข้อมูลได้อย่างถูกต้องภายใต้การคุกคามทางด้านข้อมูลที่มีตัวอย่างให้เห็นได้ในระดับโลก เพื่อจัดการกับความท้าทายเหล่านี้ องค์กรต่างๆ จะต้องเปลี่ยนแนวทางในการรักษาความปลอดภัยของตนเองจากการป้องกันจากมัลแวร์ต่างๆ ไปเป็นการใช้วิธีที่เป็นไปได้และมีการคืนสภาพได้ ซึ่งก็คือ วิธีการของการคืนสภาพได้ทางไซเบอร์

จากคำนิยามหรือคำจัดความของการคืนสภาพได้ทางไซเบอร์ที่ผู้วิจัยได้ทำการศึกษามาเกี่ยวกับนั้น ผู้วิจัยได้สรุปถึงความหมายของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล คือ ความสามารถของโซ่อุปทานในการที่จะรักษาระดับของผลการดำเนินงานขององค์กรให้สามารถดำเนินต่อไปได้เมื่อต้องเผชิญกับภัยคุกคามทางไซเบอร์ หมายความว่า กิจกรรมต่าง ๆ ของโซ่อุปทานดิจิทัลจะต้องสามารถดำเนินงานต่อไปได้เมื่อได้รับการโจมตีทางไซเบอร์ โดยที่ระบบนั้นจะต้องทำการตรวจจับ (Detect) และตอบสนอง (React) ต่อการบุกรุกหรือโจมตีได้อย่างรวดเร็วและมีระบบ

จากประเด็นของคุกคามทางด้านไซเบอร์อันเป็นมาจากการใช้งานอินเทอร์เน็ตในปัจจุบันนั้น เราจะเห็นได้ว่าภัยคุกคามทางไซเบอร์มีการพัฒนาและก้าวหน้ามากขึ้นเรื่อย ๆ เป็นภัยคุกคามที่ไม่เคยพบมาก่อน หรือเรียกว่า Unknown Threats หรือ Zero-day Attacks (TechTalkThai, 2016) เป็นสิ่งที่บริษัททั้งหลายทั้งในประเทศไทยและต่างประเทศทั่วโลกบริษัทกำลังเผชิญ ซึ่งเมื่อบริษัทเหล่านี้ได้รับการโจมตีจากภัยคุกคามที่ไม่รู้จักนี้ บริษัทเหล่านั้นต้องเผชิญกับความสูญเสียมหาศาล การโจมตีจากภัยคุกคามที่ไม่รู้จักเหล่านี้แทบจะหาวิธีการที่จะนำมาใช้ในการป้องกันไม่ได้เลย เนื่องจากการโจมตีเหล่านั้นเป็นสิ่งที่ไม่เคยพบเห็นมาก่อนเป็นการโจมตีที่สามารถเกิดขึ้นด้วยวิธีการใหม่ ๆ ได้อยู่ตลอดเวลา การหาวิธีการในการดำเนินการป้องกันไม่ว่าจะด้วยวิธีใดก็ไม่สามารถที่จะรับมือจากการโจมตีที่เกิดขึ้นเหล่านี้ได้ แต่หนึ่งในวิธีป้องกันที่ดีที่สุดคงเป็น User Behavior Analytics หรือ Machine Learning (TechTalkThai, 2016) ซึ่งเป็นวิธีการที่เกิดจากการเรียนรู้พฤติกรรมจากการใช้งาน โดยถ้าพบเห็นสิ่งที่ผิดปกติก็ให้ทำการแจ้งเตือนหรือกักกันสิ่งเหล่านั้นออกจากระบบ แต่อย่างไรก็ตาม วิธีดังกล่าวนี้ก็ใช่ว่าวิธีที่จะใช้ในการตรวจจับและป้องกัน ภัยคุกคามที่ไม่เคยพบมาก่อนนี้ได้ 100% หรือได้ทันก่อนที่การโจมตีเหล่านั้นจะทำอันตรายระบบของบริษัทลงได้ ด้วยเหตุนี้ Information Security Forum (ISF) ซึ่งเป็นหน่วยงานอิสระที่มุ่งเน้นการพัฒนามาตรฐาน, คู่มือแนะนำ และ Best Practices เชิงเทคนิคทางด้านความมั่นคงปลอดภัยของข้อมูล ได้ทำการศึกษา และได้ทำการแบ่งภัยคุกคามและวิธีรับมือ โดยเหล่านี้จะเป็นแนวคิดสำหรับการที่จะจำแนกถึงภัยคุกคามและสิ่งที่จะมีผลกระทบต่อบริษัทและท้ายที่สุดต่อระบบโซ่อุปทาน

ดังนั้น องค์กรทั่วโลกต้องปรับกระบวนทัศน์ให้มีความสามารถในการปรับตัวเพื่อรองรับการเปลี่ยนแปลง และผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ และจากนำเสนอของ Information Security Forum (ISF) ได้อธิบายและแสดงถึงประเภทของภัยคุกคามและวิธีการรับมือ ซึ่งสามารถที่จะจำแนกออกไปได้เป็น 3 ขั้น ดังภาพประกอบที่ 2.5 ได้แก่



ภาพประกอบที่ 2.5 ประเภทของภัยคุกคามและการรับมือ (Information Security Forum (IFS))

1. **ขั้นต้น (Known CIA)** คือ ภัยคุกคามที่เป็นที่รู้จักที่ส่งผลกระทบต่อ CIA Triad ซึ่งประกอบด้วย Confidentiality, Integrity และ Availability การรับมือกับภัยคุกคามนี้เรียกว่า ความปลอดภัยทางสารสนเทศ (Information Security)

2. **ขั้นกลาง (Known non-CIA)** คือ ภัยคุกคามที่เป็นที่รู้จักที่ส่งผลกระทบต่อระบบอื่นนอกเหนือจาก CIA Triad เช่น Authentication, Authorization การรับมือกับภัยคุกคามนี้เรียกว่า ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

3. **ขั้นสูง (Unknown)** คือ ภัยคุกคามที่ไม่เคยพบมาก่อน ไม่สามารถทำนายได้ไม่ชัดเจน หรือไม่คาดคิดมาก่อน เช่น การโจมตีแบบ Zero-day การรับมือกับภัยคุกคามนี้เรียกว่า การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience)

จากภาพประกอบที่ 2.4 จะเห็นได้ว่า การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) จะมีความแตกต่างจาก ความปลอดภัยทางสารสนเทศ (Information Security) และ และความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) การคืนสภาพได้ทางไซเบอร์เป็นแนวคิดที่ไม่ได้มุ่งเพียงแค่เรื่องของการป้องกันตัวจากภัยคุกคามเท่านั้น แต่ลักษณะของการคืนสภาพได้ทางไซเบอร์นั้น จะต้องมีคุณลักษณะที่จะต้องมี “ความคงทน (Robustness)” และ “ความคล่องตัว (Agility)” ต่อการถูกโจมตี ซึ่งสอดคล้องกับคุณลักษณะของการคืนสภาพได้ที่มีอยู่ในการคืนสภาพได้ของโซ่อุปทาน ตามที่ได้แสดงไว้ในตารางที่ 2.9 ที่เกิดจากการศึกษาของ Wieland et al. (2013) กล่าวคือ

เมื่อโซ่อุปทานถูกโจมตีจากภัยคุกคามดังกล่าว ระบบจะต้องให้สามารถที่จะยังให้บริการในเชิงธุรกิจต่อไปได้ โดยที่ระบบนั้นจะต้องสามารถที่จะทำการตรวจจับการโจมตีเหล่านั้นได้อย่างรวดเร็ว สามารถบล็อกการโจมตี กักกันเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ ที่ใช้ในการทำงานที่กำลังตกเป็นเหยื่อไม่ให้แพร่กระจายการโจมตีหรือมัลแวร์เข้าสู่ระบบอื่นๆ และต้องสามารถที่ทำการจัดการคลีนให้เรียบร้อย เพื่อให้ระบบกลับสามารถกลับมาทำงานได้สมบูรณ์เป็นเหมือนเดิม Valikangas (2010) ได้ชี้ให้เห็นว่าความหยุ่นสามารถถูกนำไปปฏิบัติได้ทั้งในเชิงรุก (Proactive) และเชิงรับ (Reactive) โดยที่การปฏิบัติในเชิงรุกนั้นจะต้องมีการดำเนินการก่อนที่มีมันจะกลายเป็นสิ่งจำเป็นเมื่อเหตุการณ์ได้เกิดขึ้น และ การปฏิบัติในเชิงรับจะเป็นการกู้คืนกลับหลังจากที่เกิดเหตุการณ์อันวิกฤตเกิดขึ้น โดยจากแนวคิดของ Valikangas นี้ทำให้เราได้เห็นว่า การคืนสภาพได้นั้นจะต้องมีคุณสมบัติที่มีความสามารถได้ในทั้ง 2 ด้าน คือ ป้องกัน หรือ ต่อต้าน ต่อเหตุการณ์ใดๆ ที่จะเข้ามากระทบต่อระบบ และจะต้องสามารถที่จะกลับคืนสู่ระดับของการดำเนินงานและระยะเวลาที่สามารถยอมรับได้หลังจากที่ได้รับผลกระทบจากเหตุการณ์ดังกล่าว (ISO, 2010)

สำหรับโซ่อุปทานนั้น โซ่อุปทานที่มีความสามารถในการสร้างการคืนสภาพได้จะต้องเป็นโซ่อุปทานที่มีสถานะเดิมที่มีเสถียรภาพอย่างยั่งยืน หรือถ้าโซ่อุปทานนั้นได้ถูกเปลี่ยนไปเป็นสถานะใหม่ สถานะใหม่นี้ก็จะถูกทำให้สำเร็จลงได้ นั้นแสดงให้เห็นว่าความสามารถของโซ่อุปทานที่จะมีการคืนสภาพได้ได้นั้นจะต้องเป็นโซ่อุปทานที่ต้องสามารถที่จะรับมือได้ต่อการเปลี่ยนแปลงที่จะเกิดขึ้น (Wieland et al.,2013) เพื่อที่จะรับมือต่อการเปลี่ยนแปลงและออกจากสถานะที่ไม่เสถียรนั้น โดยทั่วไป ลักษณะของการที่จะเข้าไปเกี่ยวข้องกับสภาวะแวดล้อมก็จำเป็นที่จะต้องมีการรับมือทั้งในเชิงรุกและเชิงรับ (Chakravarthy, 1982) กลยุทธ์ในเชิงรับนั้นจะพบกับการเปลี่ยนแปลงของสภาวะแวดล้อม ซึ่งจะมีความเกี่ยวข้องกับการดำเนินการขององค์กร แต่ในทางตรงกันข้าม กลยุทธ์ในเชิงรุกนั้นจะถูกสร้างขึ้นมาจากการพยากรณ์และการป้องกัน (Lengnick-Hall and Beck, 2005)

สำหรับงานวิจัยนี้จะได้นำเอาแนวความคิดของที่ได้จากการศึกษาของ Wieland and Wallenburg (2012) จากผลการศึกษาได้กำหนดกลยุทธ์ไว้ 2 กลยุทธ์ที่เกี่ยวข้องกับความสามารถในการสร้างการคืนสภาพได้ โดยกลยุทธ์แรกคือ ความคล่องตัว (Agility) ” (Braunscheidel and Suresh, 2009; Swafford et al., 2006) และกลยุทธ์ที่ 2 คือ ความคงทน (Robustness) (Husdal, 2010; Meepetchdee and Shah, 2007) โดยที่ความคล่องตัว จะเป็นกลยุทธ์ในเชิงรับ (Braunscheidel and Suresh, 2009) และความคงทน ซึ่งเป็นกลยุทธ์ในเชิงรุก (Shukla et al., 2011)

ความคล่องตัว พิจารณาจากคำความหมายนั้น จะมีความหมายที่แสดงถึงความสามารถทางด้านรับ ไม่ว่าจะเป็นการแสดงปฏิกิริยาตอบโต้ (React) การตอบสนอง (Respond) การปรับตัว (Adapt) รวมไปถึงการกำหนดค่าใหม่ (Re-Configure) โดยทั้งหมดเป็นคำอธิบายที่แสดงให้เห็นถึงความสามารถที่จะอธิบายถึงผลที่เกิดจากการเปลี่ยนแปลงได้ จากการศึกษาของ Bakshi and Kleindorfer (2009) ได้แสดงให้เห็นว่า ความคล่องตัว คือประเด็นที่ต้องให้ความสนใจต่อการปรับตัวขึ้นมาของระบบอย่างรวดเร็วในสถานการณ์ที่ต้องเผชิญต่อการเปลี่ยนแปลงที่ไม่สามารถคาดเดาได้ ซึ่งจะเป็นประเด็นที่คล้ายกับการศึกษาของ Khan et al. (2009) ที่ชี้ให้เห็นว่า ความคล่องตัวของโซ่อุปทานคือความสามารถในการตอบสนองต่อความไม่แน่นอนของตลาดและต้องสามารถปรับตัวได้อย่างรวดเร็ว ซึ่งหลักในการคิดนี้จะมีความสอดคล้องกับแนวคิดของการผลิตที่ต้องการความคล่องตัวเช่นเดียวกัน โดยที่เมื่อมีการเปลี่ยนแปลงสถานะของการปฏิบัติงานที่มีผลมาจากการความไม่แน่นอน หรือแม้แต่ความต้องการสินค้าที่เปลี่ยนแปลงไปเมื่อมีการสั่งผลิตไปแล้ว (Narasimhan et al., 2006) โดยในงานวิจัยนี้ผู้วิจัยจึงได้ให้ความหมายของ ความคล่องตัวของโซ่อุปทาน หมายถึง ความสามารถของโซ่อุปทานในการที่จะตอบสนองต่อการเปลี่ยนแปลงได้อย่างรวดเร็ว โดยจะต้องสามารถที่จะปรับตัวกลับสู่สถานะเริ่มต้นก่อนการเปลี่ยนแปลงได้

ความคงทนของโซ่อุปทาน คือความสามารถของโซ่อุปทานในการที่จะดำเนินงานตามหน้าที่ต่อไป แม้ว่าจะมีความเสียหายบางอย่างเกิดขึ้นต่อโซ่อุปทาน (Meepetchdee and Shah, 2007) โดยยังจะต้องสามารถรักษาสถานะของโซ่อุปทานให้มีความเสถียรได้เหมือนกับก่อนที่มีการเปลี่ยนแปลง (Asbjørnslett, 2008) จะต้องสามารถทนทานได้มากกว่าการตอบสนอง (Husdal, 2010) จะต้องสามารถช่วยให้ ทนได้แต่แรงกระแทกได้มากกว่าการปรับตัวให้เข้ากับแรงกระแทก (Wallace and Choi, 2011) ด้วยเหตุนี้จึงเป็นเหตุผลว่าทำไมความคงทนของโซ่อุปทานจึงเป็นกลยุทธ์ในเชิงรุก ยิ่งไปกว่านั้นความคงทนของโซ่อุปทานยังจะสามารถดำเนินการได้ดีในทุกๆ สถานการณ์ (Harrison, 2005) โดยเฉพาะอย่างยิ่งเมื่อระบบหรือสภาวะแวดล้อมนั้นได้ตกอยู่ภายใต้การเปลี่ยนแปลงที่มีขนาดใหญ่ (Yan et al., 2000) ด้วยเหตุนี้ความคงทนจึงถูกมองว่าการดำเนินการในเชิงรุกของการเปลี่ยนแปลงที่จะเกิดขึ้น ดังนั้นแล้วสำหรับงานวิจัยนี้ผู้วิจัยจึงให้ความหมายสำหรับ ความคงทนของโซ่อุปทาน คือความสามารถของโซ่อุปทานในการที่ต่อต้านการเปลี่ยนแปลงโดยจะต้องไม่ไปกระทบต่อสถานะเริ่มต้นที่มีความเสถียรอยู่แล้ว

กล่าวโดยสรุป การรับมือจากภัยคุกคามด้วยวิธีการคืนสภาพได้ทางไซเบอร์ ก็คือแนวทางในการเตรียมความพร้อมเพื่อตรวจจับและตอบสนองต่อการถูกบุกรุกโจมตีได้อย่างรวดเร็วและมีระบบ จากแนวทางเดิมที่องค์กรต่างๆ นั้น จำเป็นต้องหาวิธีการในการป้องกันตัว

(Protective Security) จากภัยคุกคามต่างๆ โดยองค์กรเหล่านั้นจะต้องทำการปรับตัวจากการป้องกันแบบดั้งเดิมที่ทำอยู่ในปัจจุบัน ไปจะเปลี่ยนไปเป็น “การเตรียมความพร้อม (Responsive Security)” ให้พร้อมรับมือต่อภัยคุกคามที่ไม่เคยพบเห็นมาก่อน (TechTalkThai, 2016) ดังนั้น บริษัทต่างๆ จึงต้องลงทุนในความสามารถของโซ่อุปทานเพื่อที่จะได้เตรียมการเสริมสร้างความสามารถในการรับมือต่อการโจมตีทางไซเบอร์ หรือ การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) เพื่อป้องกันและเตรียมรับมือต่อภัยคุกคามที่อาจเกิดขึ้น เพราะว่าภัยคุกคามที่เกิดจากความเสี่ยงที่ไม่รู้จัก (Unknown Threats) นี้ จะเป็นภัยคุกคามที่สามารถเกิดขึ้นใหม่ได้อยู่ตลอดเวลา และบริษัทหรือองค์กรเองก็ไม่อาจจะคาดการหรือตรวจจับได้จนกว่าจะเกิดความเสียหายต่อองค์กร

2.6 การจัดการความต่อเนื่องทางธุรกิจ

ในปัจจุบัน การดำเนินธุรกิจให้ประสบความสำเร็จ นับเป็นสิ่งที่ท้าทายและยากขึ้นเรื่อยๆ ที่องค์กรหรือบริษัทต่างๆ ต้องเผชิญอยู่ในปัจจุบัน ไม่ว่าจะเป็นการแข่งขันที่เพิ่มสูงขึ้น ความซับซ้อนทางธุรกิจที่มากขึ้น หรือจะเป็นข้อกฎหมาย ระเบียบข้อบังคับต่างๆ ที่เข้มงวดมากขึ้น นอกจากนั้น ความไม่แน่นอนในเหตุการณ์ต่างๆ ไม่ว่าจะเป็นความผิดพลาดในการทำงาน อุบัติเหตุ ภัยพิบัติ หรือภัยคุกคามทางไซเบอร์ที่เกิดมาจากความก้าวหน้าทางด้านเทคโนโลยี สิ่งต่างๆ เหล่านี้ ล้วนส่งผลกระทบต่อการดำเนินธุรกิจ ในการดำเนินธุรกิจให้มีความต่อเนื่อง และประสบความสำเร็จตามเป้าหมายที่ตั้งไว้ ดังนั้นแนวความคิดเรื่องการจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) จึงได้รับการพัฒนาขึ้นมา เพื่อให้องค์กรหรือบริษัทต่างๆ สามารถที่จะรักษาความสามารถขององค์กรไว้ได้อย่างต่อเนื่อง ในสภาวะการณ์ที่เกิดเหตุการณ์ต่างๆ ที่จะทำให้เกิดความหยุดชะงักทางธุรกิจ (Business Disruption) ขึ้น

การเกิดภัยพิบัติทั้งทางธรรมชาติและด้วยฝีมือมนุษย์ในแต่ละครั้งนั้นสร้างความเสียหายมหาศาลแก่ชีวิตและทรัพย์สิน นอกจากนั้นยังสร้างความเสียหายอันใหญ่หลวงต่อภาคธุรกิจด้วยเช่นเดียวกัน บริษัททั้งหลายไม่ว่าจะมีขนาดเล็กหรือขนาดใหญ่หลายแห่งต้องสูญทุนและกำไร เสียภาพลักษณ์ รวมทั้งสูญเสียส่วนแบ่งทางธุรกิจ และหลายบริษัทต้องปิดกิจการไป แต่อย่างไรก็ตามบางบริษัทก็สามารถผ่านช่วงวิกฤตินี้ไปได้โดยได้รับความเสียหายเพียงเล็กน้อยซึ่งเกิดจากความพร้อมและประสิทธิภาพในการตอบสนองต่อภาวะวิกฤติของบริษัท ดังนั้นบริษัทต่างๆ จำเป็นต้องมีแผนสำรองทางธุรกิจที่ดีและมีประสิทธิผลที่จะช่วยให้การบริหารธุรกิจมีความต่อเนื่องและสูญเสียน้อยเมื่อต้องประสบภาวะวิกฤติ

2.6.1 แนวคิดของการจัดการความต่อเนื่องทางธุรกิจ

ความต่อเนื่องทางธุรกิจ (Business Continuity) หมายถึงขีดความสามารถทางกลยุทธ์ (Strategy) และยุทธวิธี (Tactical) ขององค์กรในการวางแผนและตอบสนองต่อเหตุการณ์ต่าง ๆ ที่ส่งผลต่อการหยุดชะงักทางธุรกิจ เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่องภายใต้ระดับที่สามารถยอมรับได้ การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)) หมายถึง กระบวนการจัดการแบบองค์รวม ในการระบุถึงภัยอันตรายและภัยคุกคามที่อาจจะเกิดขึ้นกับการดำเนินธุรกิจขององค์กร และผลกระทบที่มีต่อการดำเนินธุรกิจจากภัยอันตรายและภัยคุกคามนั้น ๆ รวมถึงการจัดเตรียมกรอบสำหรับการสร้างความยืดหยุ่นในขีดความสามารถขององค์กร ให้สามารถตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างมีประสิทธิผล เพื่อเป็นการปกป้องดูแลให้กับผู้มีส่วนได้เสีย ชื่อเสียงองค์กร ตราสินค้า และการดำเนินงานในการสร้างคุณค่าขององค์กร

ความจำเป็นที่จะต้องมีการจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) มีเหตุมาจากผลของการเกิดภัยพิบัติในแต่ละครั้งนอกจากจะสร้างความเสียหายมหาศาลแก่ชีวิตและทรัพย์สินแล้ว ยังรวมถึงได้สร้างความเสียหายต่อภาคธุรกิจด้วย โดยในบางธุรกิจสามารถผ่านช่วงวิกฤตนี้ไปได้ เนื่องจากมีแผนสำรองทางธุรกิจที่ดีและมีประสิทธิผลที่จะช่วยให้การบริหารธุรกิจมีความต่อเนื่องและสูญเสียน้อยเมื่อต้องประสบภาวะวิกฤติ โดยกระบวนการในการจัดการความต่อเนื่องทางธุรกิจ นั้นจะประกอบไปด้วย (กระทรวงพลังงาน, 2560)

1. แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plans (BCP)) คือเอกสารที่รวบรวมขั้นตอน และข้อมูลซึ่งทำให้องค์กรหรือบริษัท พร้อมที่จะนำไปใช้เมื่อเกิดเหตุฉุกเฉิน เพื่อให้สามารถดำเนินกิจกรรมหรือกระบวนการหลักในระดับที่กำหนดไว้ ซึ่งจะมีขั้นตอนในการจัดทำแผน 4 ขั้นตอน คือ 1) การวิเคราะห์ความเสี่ยงและผลกระทบต่อธุรกิจ เพื่อกำหนดวิธีการดำเนินการในสถานการณ์ฉุกเฉินซึ่งแตกต่างจากสถานการณ์ปกติ 2) การกำหนดแนวปฏิบัติเพื่อแก้ไขปัญหาที่เหมาะสมกับสถานการณ์ความเสี่ยง การกำหนดขั้นตอนงานที่ฉุกเฉิน วิธีปฏิบัติและแผนฟื้นฟูหลังผ่านพ้นวิกฤต 3) การทดสอบและประเมินในสถานการณ์จำลองตามความเสี่ยงและดำเนินการตามแผนนั้น และ 4) การนำไปปฏิบัติหลังจากผ่านการ ทดสอบและประเมินแล้ว (สำนักงานส่งเสริมรัฐวิสาหกิจขนาดกลางและขนาดย่อม, 2560)

2. แผนการจัดการอุบัติการณ์ฉุกเฉิน (Incident Management Plan (IMP)) คือแผนหรือแนวทางปฏิบัติที่กำหนดไว้เพื่อใช้เตรียมความพร้อมของระบบป้องกันและระงับเหตุฉุกเฉิน และผู้มีหน้าที่รับผิดชอบเมื่อเกิดเหตุฉุกเฉิน เช่น อัคคีภัย ภัยธรรมชาติ สารเคมีรั่วไหล การ

ก่อวินาศกรรม การโจมตีทางไซเบอร์ เป็นต้น ที่อาจเป็นเหตุให้เกิดอันตรายต่อชีวิต ทรัพย์สินและสิ่งแวดล้อม

โดยแผนความต่อเนื่องทางธุรกิจและแนวทางการปฏิบัติที่ได้รับการยอมรับจะต้องดำเนินการให้เป็นไปตามแนวทางดังต่อไปนี้ 1) นโยบายที่จะต้องทำให้เป็นที่รับรู้และเข้าใจอย่างถ่องแท้โดยจะต้องทำให้เป็นนโยบายพื้นฐานให้ได้ 2) การจัดทำแผนต่อเนื่องทางธุรกิจเพื่อรับมือภัยพิบัติโดยจะต้องมีการตรวจสอบความเสี่ยงจากภัยพิบัติ การประเมินผลกระทบ การประมาณการระยะหยุดให้บริการ และศักยภาพในการตอบสนอง รวมทั้งกำหนดได้ว่าสิ่งใดเป็นกิจกรรมที่มีความสำคัญ โดยจะต้องเลือกจัดลำดับความสำคัญบนพื้นฐานของการคำนวณเกี่ยวกับการหยุดชะงักของกิจการและความสามารถในการบูรณะฟื้นฟู

การจัดทำการจัดการความต่อเนื่องทางธุรกิจนั้น มีองค์ประกอบ 3 อย่างตามลำดับความสำคัญ ได้แก่ คน (People) สถานที่และอุปกรณ์ (Infrastructure) และแผน (Plans) โดยมีรายละเอียดโดยสังเขป ดังนี้

1. คน (People) เป็นองค์ประกอบที่สำคัญที่สุด โดยหลักการของ BCM นั้นต้องมีการกำหนดโครงสร้างองค์กรและบทบาทหน้าที่ของบุคลากร รวมทั้งสายบังคับบัญชาให้ชัดเจนเพื่อให้การใช้อำนาจตัดสินใจและการสื่อสารในช่วงวิกฤติมีประสิทธิภาพ นอกจากนั้นบุคลากรต้องได้รับการฝึกฝนแผนรวมทั้งร่างกายและจิตใจเพื่อให้ทำงานเป็นอันหนึ่งอันเดียวกัน (Teamwork) ในสภาวะวิกฤติให้ได้ นอกจากนั้นองค์กรควรกำหนดบุคลากรสำรองเพื่อการทำงานในสภาวะวิกฤติไว้ด้วย เช่น ทีมสนับสนุนการจัดการกรณีวิกฤติ ทีมกู้คืนทางธุรกิจ และทีมกู้คืนทางด้าน IT เป็นต้น

2. สถานที่และอุปกรณ์ (Infrastructure) เป็นองค์ประกอบที่สำคัญในระดับรองลงมา โดยสถานที่ตั้งสำรองในกรณีวิกฤตินั้นไม่ควรอยู่ใกล้สถานที่หลัก เช่น ศูนย์บัญชาการมากเกินไป และต้องมีอุปกรณ์การสื่อสารและ IT ที่ดีเพื่อให้การเข้าถึงข้อมูลสะดวกและรวดเร็วในช่วงที่เกิดวิกฤติการณ์รวมถึงต้องมีระบบการสำรองข้อมูลที่ดีด้วยโดยต้องจัดเก็บสำรองข้อมูลนอกสถานที่

3. แผน (Plans) เป็นองค์ประกอบที่สำคัญเป็นลำดับสุดท้าย โดยการจัดทำแผนต้องคำนึงถึงแผนที่มุ่งเน้นกระบวนการที่จำเป็นต้องปฏิบัติ เข้าใจง่าย กระชับ กำหนดบทบาทหน้าที่ชัดเจน และมีการประสานงานกับท้องถิ่น ภาครัฐ และหน่วยงานกำกับดูแล รวมทั้งต้องรวมแผนการเคลื่อนย้ายคนเป็นส่วนหนึ่งของ BCM ด้วย โดยแผนต่างๆเหล่านี้ต้องมีการทดสอบและปรับปรุงอย่างสม่ำเสมอ

2.6.2 มาตรฐานด้านการจัดการความต่อเนื่องทางธุรกิจ

แนวทางการจัดการความต่อเนื่องทางธุรกิจ มีวงจรการจัดการความต่อเนื่อง (BCM Life Cycle) ที่สำคัญคือ 1) การจัดการ โครงการจัดการความต่อเนื่องเป็นขั้นตอนการจัดทำกรอบนโยบาย โครงสร้างหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง 2) การศึกษาและทำความเข้าใจองค์กรผ่านการวิเคราะห์ผลกระทบทางธุรกิจและการประเมินความเสี่ยงที่เกี่ยวข้อง 3) การกำหนดกลยุทธ์ในการสร้างความต่อเนื่องทางธุรกิจ ได้แก่ กลยุทธ์การกู้คืนการดำเนินงาน และการกำหนดกลยุทธ์ด้านการจัดการทรัพยากรที่เหมาะสม ตามข้อมูลที่ได้รับจากการวิเคราะห์ผลกระทบทางธุรกิจ 4) การพัฒนาและเตรียมการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉิน ประกอบไปด้วย Incident Management Plans (IMP), Emergency/Crisis Management Plan (CMP), Business Continuity Plans (BCP) และ Recovery Plans (RP) และ 5) การทดสอบ ปรับปรุง และทบทวนแผน ได้แก่ การซ้อมแจ้งเหตุฉุกเฉินให้กับสมาชิกทีมงาน การประชุมแลกเปลี่ยนความคิดเห็นกับทุกหน่วยที่เกี่ยวข้องโดยจำลองสถานการณ์ขึ้นมา การทดสอบโดยจำลองสถานการณ์เสมือนจริง และการทดสอบเต็มรูปแบบและใกล้เคียงสถานการณ์จริงมากที่สุด (กิตติพงศ์ จิรวัสวงค์, 2012)

ปัจจุบันมีหลากหลายแนวทาง และมาตรฐานในการจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management) โดยแนวทางที่ได้รับการใช้อย่างแพร่หลาย ประกอบด้วย

2.6.2.1 มาตรฐาน BS25999

สถาบัน **BCI (Business Continuity Institute)** มีสำนักงานใหญ่อยู่ในประเทศอังกฤษ เป็นหน่วยงานที่กำหนดมาตรฐานในการทำ BCM และให้การรับรองผู้เชี่ยวชาญด้าน Business Continuity ทั่วโลกโดยมีสมาชิกกว่าสี่พันคนในกว่า 85 ประเทศ โดยสถาบัน BCI ได้อ้างอิงมาตรฐาน BCM จากสถาบัน BSI คือมาตรฐาน BS25999 ซึ่งเป็นมาตรฐานที่มาแทนที่มาตรฐาน PAS 56

มาตรฐาน BS25999 แบ่งออกได้เป็น 2 ส่วน ส่วนที่หนึ่งเรียกว่า “BS 25999-1:2006 -- Business Continuity Management. Code of Practice” เป็นแนวปฏิบัติที่ทาง BSI แนะนำให้ปฏิบัติแต่ไม่บังคับ สำหรับส่วนที่สองเรียกว่า “BS 25999-2:2007 --Specification for Business Continuity Management ” เป็นข้อกำหนดภาคบังคับที่ต้องปฏิบัติ เรียกว่า ระบบบริหารจัดการธุรกิจอย่างต่อเนื่อง “Business Continuity Management System หรือ BCMS” ซึ่งสามารถต่อยอดไปยังการรับรองมาตรฐานโดย Certification Body ซึ่งในขณะนี้มาตรฐาน BS 25999 นั้น accredit โดย LRQA และ BSI โดยในอนาคตอันใกล้คาดว่ามาตรฐาน BS 25999 จะกลายเป็นมาตรฐานนานาชาติ ISO/IEC ดังเช่น มาตรฐาน BS7799 กลายเป็นมาตรฐาน ISO/IEC 17799 และ ISO/IEC 270001 มาแล้ว เป็นต้น

ในปัจจุบันระบบสารสนเทศกลายเป็นหัวใจหลักของระบบธุรกิจแทบทุกระดับล้วนนำระบบสารสนเทศมาใช้ในองค์กรอย่างกว้างขวาง ไม่ว่าจะเป็นระบบ Web Site ขององค์กร, ระบบ Electronic Mail หรือ ระบบเฉพาะทางต่างๆ เช่น ระบบ Intranet, ระบบ Portal, ระบบ ERP, CRM และ SCM เป็นต้น ทำให้การใช้งานคอมพิวเตอร์ในการเข้าถึงข้อมูลองค์กรจึงกลายเป็นเรื่องที่พนักงานในองค์กรทุกคนคุ้นเคยและใช้ปฏิบัติงานอยู่ในชีวิตประจำวัน โดยอาศัยระบบสารสนเทศและระบบเครือข่ายถือเป็นโครงสร้างพื้นฐานในการทำงานของระบบต่างๆ ดังกล่าว

ปัญหาที่หลายองค์กรกำลังเผชิญอยู่ทั้งในอดีต ปัจจุบัน และอนาคต คือ ปัญหาระบบสารสนเทศไม่สามารถทำงานตามปกติ หรือ ปัญหาระบบสารสนเทศล่ม ยกตัวอย่าง เช่น หากพนักงานเข้าระบบไม่ได้ในช่วงระยะเวลาที่ระบบล่มอยู่ พนักงานก็ไม่สามารถเรียกข้อมูลต่างๆ ที่ถูกเก็บอยู่ในรูปของดิจิตอลฟอร์เมต (Digital Format) หรือ e – Document ออกมาได้ อีกทั้งลูกค้าก็ไม่สามารถเข้าถึงข้อมูลขององค์กร เช่น เข้าชม Web Site ขององค์กร หรือ ไม่สามารถส่งอิเล็กโทรนิคส์เมล์ได้ ยิ่งถ้าเป็นระบบของโรงพยาบาล, ระบบฝากถอนเงินของธนาคาร หรือ ระบบที่ใช้ในการควบคุมขนส่งมวลชน ตลอดจนระบบที่ใช้ในการควบคุมสาธารณูปโภค เช่น ไฟฟ้า, น้ำประปา เป็นต้น ล้วนเป็นระบบที่มีความสำคัญอย่างยิ่งยวด เป็นโครงสร้างพื้นฐานของประเทศ (Critical Infrastructure) ดังนั้น หากระบบดังกล่าวไม่สามารถใช้งานได้ การเข้าถึงข้อมูลที่อยู่ในระบบก็ไม่สามารถเข้าถึงได้ทันท่วงที ทำให้องค์กรไม่สามารถดำเนินธุรกิจธุรกรรมต่างๆได้ตามปกติ ส่งผลให้องค์กรเกิดความเสียหายได้

ตัวอย่างภัยคุกคามที่ทำให้ระบบล่ม ได้แก่ ภัยธรรมชาติ เช่น สึนามิ, พายุเฮอริเคน, น้ำท่วม หรือ ภัยจากมนุษย์ เช่น การก่อวินาศกรรม เช่น กรณี 911, การจราจล, การลอบวางเพลิง ก็ล้วนเป็นปัจจัยกระตุ้นให้ผู้บริหารองค์กรจำเป็นต้องให้ความสำคัญอย่างยิ่งยวดต่อระบบสารสนเทศที่เป็นกระดูกสันหลังในการดำเนินธุรกิจขององค์กร เพราะหากระบบเกิดปัญหา องค์กรก็ควรที่จะมีแผนฉุกเฉินในการทำให้ระบบสารสนเทศขององค์กรสามารถให้บริการได้อย่างไม่ติดขัดจนก่อให้เกิดความเสียหายแก่องค์กรทั้งทางตรงและทางอ้อม

มาตรฐาน BS25999 เป็นมาตรฐานทางด้านการบริหารความต่อเนื่องธุรกิจ (Business Continuity Management) ที่ได้รับการพัฒนาขึ้นมาจากมาตรฐาน PAS 56 ซึ่งเป็นมาตรฐานแรกของการบริหารความต่อเนื่องธุรกิจ โดย British Standard ทั้งนี้ มาตรฐาน BS 25999 ที่ประกาศใช้ออกมา จะมีทั้งหมด 2 ฉบับ ประกอบด้วย

1. BS 25999 – 1, Business Continuity Management Part 1 – Code of practices เป็นเอกสารที่ระบุถึงแนวปฏิบัติที่ดี และข้อเสนอแนะ สำหรับองค์กรที่ต้องการจะ

ดำเนินการ BCM ให้ได้อย่างมีประสิทธิผล ทั้งนี้ องค์กรสามารถเลือกใช้บางส่วน หรือทั้งหมดของเอกสารก็ได้ โดยมีการเผยแพร่เป็นทางการเมื่อเดือนพฤศจิกายน 2006

2. BS 25999-2, Business Continuity Management Part 2-Specification เอกสารนี้จะเป็นข้อกำหนดที่จะต้องปฏิบัติ โดยจะใช้สำหรับหน่วยงานทั้งภายใน และภายนอก รวมถึงหน่วยงานที่ให้การรับรอง (Certification bodies) เพื่อประเมินถึงความสามารถขององค์กร ในการดำเนินการให้สอดคล้องกับข้อกำหนดต่างๆ

2.6.2.2 มาตรฐาน ISO 22301

มาตรฐาน ISO 22301:2012 เป็นมาตรฐานสากลสำหรับการจัดการความต่อเนื่องทางธุรกิจ โดย International Organization for Standardization (ISO) ได้ประกาศเปิดตัวอย่างเป็นทางการมาตรฐาน ISO22301 “Societal Security-Business Continuity Management Systems” เมื่อวันที่ 15 พฤษภาคม 2555 (สำนักงานคณะกรรมการพัฒนาระบบราชการ ก.พ.ร., 2560) กรอบแนวทางการบริหารจัดการ BCM ตามมาตรฐาน ISO 22301:2012 มีองค์ประกอบที่เกี่ยวข้อง 6 องค์ประกอบหลัก หรือเรียกว่าเป็นวงจรบริหารจัดการความต่อเนื่องทางธุรกิจ (BCM Policy and Programme Management) ประกอบด้วย

1. การบริหารการจัดการความต่อเนื่องทางธุรกิจ (BCM Policy and Programme Management) หัวใจหรือองค์ประกอบหลักของการสร้างความต่อเนื่อง ก็คือ การจัดทำกรอบนโยบายและการบริหารจัดการโครงการ หรือการกำหนดโครงสร้างหน้าที่และความรับผิดชอบของบุคคลตั้งแต่ผู้บริหารระดับสูงลงมาถึงพนักงานระดับต่าง ๆ จัดตั้งทีมงานด้านการจัดการความต่อเนื่องทางธุรกิจ กำหนดตัวชี้วัด ผลการดำเนินงานของพนักงาน รวมถึงขั้นตอนการปรับระดับของเหตุการณ์ (Incident Escalation Process) วิธีบริหารโครงการ และการติดตามความพร้อมทั้งรายงานความคืบหน้า

2. การปลูกฝังการจัดการความต่อเนื่องทางธุรกิจให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร (Embedding BCM in The Organization’s Culture) เป็นขั้นตอนที่สำคัญประการหนึ่งในการทำให้ BCM ผสมกลมกลืนเข้าจนเป็นวัฒนธรรมองค์กร โดยเป็นเรื่องที่ต้องใช้เวลาและจิตวิทยาที่จะทำให้พนักงานทุกคนได้ซึมซาบและเข้าใจถึงความสำคัญของ BCM ตลอดจนบทบาทหน้าที่ที่ทุกคนพึงมี เพื่อให้ธุรกิจสามารถดำเนินต่อไปได้ในยามที่เกิดเหตุวิกฤต

3. การเข้าใจองค์กร (Understanding The Organization) เป็นกระบวนการทำความรู้จักกับองค์กร ซึ่งหมายถึง ความรู้และเข้าใจสภาพขององค์กรว่าจะรับผลกระทบทางธุรกิจหรือความเสี่ยงได้เท่าใด ผ่านวิธีการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis - BIA) และการประเมินความเสี่ยง (Risk Assessment - RA) เพื่อระบุความเร่งด่วนของกิจกรรมต่าง ๆ

และระดับความสามารถที่ต้องการ เพื่อนำไปเป็นข้อมูลในการจัดระดับความสำคัญของกระบวนงานและการกำหนดกลยุทธ์ในข้อต่อไป

4. การกำหนดกลยุทธ์ BCM (Determining BCM Strategy) คือ การกำหนดแนวทางในการตอบสนองต่อการหยุดชะงักของการดำเนินงานขององค์กร ได้แก่ กลยุทธ์กู้คืนการดำเนินงาน (Recovery Strategy) ซึ่งเป็นแผนที่ต้องจัดทำก่อนแผนฉุกเฉิน และกำหนดกลยุทธ์ด้านการจัดการทรัพยากรที่เหมาะสมตามข้อมูลที่ได้จาก BIA โดยต้องกำหนดในเรื่องบุคลากร (People) สถานที่ (Premise) เทคโนโลยี (Technology) ข้อมูล (Information) ผู้ผลิตสินค้าหรือผู้ให้บริการ (Supplier)

5. พัฒนา และจัดเตรียมวิธีการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉิน (Developing and Implementing a BCM Response) หลังจากที่ได้มีการกำหนดกลยุทธ์เรียบร้อยแล้ว ต้องจัดทำแผนงานเตรียมตอบสนองต่อภาวะฉุกเฉิน โดยให้เป็นไปตามกรอบยุทธศาสตร์ที่กำหนดไว้โดยจัดทำแผน 3 แผนดังต่อไปนี้

1) Incident Management Plans (IMP) เพื่อจัดการกับวิกฤติฉุกเฉินที่เกิดขึ้น

2) Business Continuity Plans (BCP) เพื่อบริหารธุรกิจอย่างต่อเนื่อง โดยมุ่งทำขั้นตอนงานที่ฉุกเฉินต่อธุรกิจ และใช้ทรัพยากรหลักอย่างเหมาะสมในจำนวนต่ำที่สุด พร้อมทั้งเตรียมแผนรับผลกระทบในสถานการณ์ที่แย่ที่สุด

3) Disaster Recovery Plans (DRP) หรือแผนกู้คืนธุรกิจหลังภัยพิบัติผ่านพ้นไป

6. ทดสอบ ปรับปรุง และทบทวนแผน (Exercising, Maintaining and Reviewing) เป็นขั้นตอนที่สำคัญเนื่องจากเป็นกระบวนการที่ทำให้แน่ใจได้ว่า BCM ที่ได้จัดทำขึ้นสามารถใช้ได้จริง รวมทั้งเพื่อเตรียมความพร้อม ตลอดจนตรวจสอบความสามารถของบุคลากรและประสิทธิภาพของแผนในการตอบสนองต่อวิกฤติการณ์ โดยรูปแบบอาจมีตั้งแต่ระดับง่ายไปหายาก ดังนี้

1) Call Tree คือ การซ้อมการแจ้งเหตุฉุกเฉินให้กับสมาชิกทีมงานที่เกี่ยวข้องตามผังรายชื่อทางโทรศัพท์

2) Tabletop Testing คือ การประชุมแลกเปลี่ยนความคิดเห็นกับทุกหน่วยที่เกี่ยวข้อง โดยจำลองโจทย์ สถานการณ์ขึ้นมา และลองนำแผน BCP มาพิจารณาว่าใช้ตอบโจทย์แต่ละขั้นตอนได้หรือไม่

3) Simulation คือ การทดสอบโดยจำลองสถานการณ์เสมือนจริง และลองใช้แผน BCP มา ประยุกต์ใช้

4) Full BCP Exercise คือ การทดสอบเต็มรูปแบบและใกล้เคียงสถานการณ์จริงมากที่สุด

ISO 22301 : 2012 Societal Security - Business Continuity Management Systems มาตรฐานการจัดการความต่อเนื่องทางธุรกิจ เป็นการจัดการความต่อเนื่องทางธุรกิจที่มีการบริหารจัดการแบบองค์รวม (Holistic Management) ในการชี้บ่งภัยคุกคามที่อาจจะเกิดขึ้น และผลกระทบจากภัยคุกคามดังกล่าวที่มีต่อการดำเนินธุรกิจขององค์กร และถ้าสิ่งนั้นเกิดขึ้นองค์กรต้องมีการจัดเตรียมกรอบการทำงาน ในการสร้างความยืดหยุ่นขององค์กรให้มีความสามารถในการตอบสนอง และปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสียหลัก ชื่อเสียง เครื่องหมายการค้า และกิจกรรมที่สร้างมูลค่าได้อย่างมีประสิทธิภาพ ระบบการรจัดการ (Management System) ที่เป็นมาตรฐานในฉบับนี้ได้ประยุกต์ใช้รูปแบบ “Plan-Do-Check-Act” (PDCA) ในการวางแผนจัดทำการนำไปปฏิบัติ การดำเนินการ การเฝ้าระวัง การทบทวน การคงรักษาไว้และการปรับปรุงประสิทธิผลอย่างต่อเนื่องของระบบการบริหารความต่อต่อเนื่องทางธุรกิจ โดยแต่ละขั้นตอนครอบคลุมกิจกรรมต่าง ๆ ดังนี้

1) Plan (Establish) เป็นการจัดทำนโยบายความต่อเนื่องทางธุรกิจ วัตถุประสงค์ เป้าหมาย การควบคุม กระบวนการ และขั้นตอนการปฏิบัติงานที่เกี่ยวข้อง เพื่อปรับปรุงความต่อเนื่องทางธุรกิจ เพื่อให้ได้ผลลัพธ์ที่สอดคล้องกับนโยบายและวัตถุประสงค์ขององค์กรโดยรวม

2) Do (Implement and operate) การนำไปปฏิบัติ และการดำเนินการตามนโยบายความต่อเนื่องทางธุรกิจ การควบคุม กระบวนการ และขั้นตอนการปฏิบัติงาน

3) Check (Monitor and review) การเฝ้าระวัง และทบทวนผลการดำเนินงานเปรียบเทียบกับนโยบายความต่อเนื่องทางธุรกิจ และวัตถุประสงค์ การรายงานผลการเฝ้าระวังต่อผู้บริหารเพื่อการทบทวน กำหนด และมอบหมายให้ดำเนินการเพื่อแก้ไขและปรับปรุง

4) Act (Maintain and improve) การคงรักษาไว้และปรับปรุงระบบการจัดการความต่อเนื่องทางธุรกิจ โดยการดำเนินการปฏิบัติการแก้ไขที่ขึ้นอยู่กับผลของการทบทวนฝ่ายบริหาร และการทบทวนขอบข่ายของระบบการบริหารความต่อเนื่องทางธุรกิจ และนโยบายความต่อเนื่องทางธุรกิจ และวัตถุประสงค์

ข้อกำหนดต่าง ๆ ในมาตรฐานเหล่านี้ จะใช้สำหรับการจัดทำ การนำไปปฏิบัติ การดำเนินการ การติดตามผล การทบทวน การดูแลรักษา และการปรับปรุงระบบบริหาร

ความต่อเนื่องธุรกิจขององค์กร โดยจะพิจารณาจากความเสี่ยงทางธุรกิจโดยรวมที่เกิดขึ้นกับองค์กร ซึ่งมาตรฐานนี้ สามารถนำไปประยุกต์ใช้ได้ทั่วทั้งองค์กร ในประเภท ขนาด และลักษณะต่าง ๆ ทางธุรกิจ โดยขอบเขตของการใช้ข้อกำหนดจะขึ้นอยู่กับสภาพแวดล้อมและความซับซ้อนขององค์กร ทั้งนี้ในการจัดการระบบการจัดการความต่อเนื่องทางธุรกิจให้เป็นไปอย่างมีประสิทธิผล จะต้องคำนึงถึง 1) การทำความเข้าใจในความต้องการของความต่อเนื่องทางธุรกิจ และการจัดทำนโยบาย และวัตถุประสงค์สำหรับความต่อเนื่องทางธุรกิจ 2) การนำไปปฏิบัติ และการควบคุมสำหรับการจัดการกับความเสี่ยงต่างๆ ที่มีต่อความต่อเนื่องในการดำเนินธุรกิจ 3) การติดตามผลและทบทวนผลการดำเนินงาน และความมีประสิทธิผลของระบบ และ 4) การปรับปรุงระบบอย่างต่อเนื่อง

ในมุมมองของมาตรฐาน ISO22301 : 2012 นี้ นอกจากการจัดการในสภาวะวิกฤต (Crisis Management) เพียงเพื่อป้องกันการหยุดชะงัก (Disruption) แล้วองค์กรต้องพิจารณาถึงความไม่แน่นอน และความเสี่ยงจากภัยคุกคามต่าง ๆ ซึ่งจะช่วยให้องค์กรมีระบบการบริหารความต่อเนื่องทางธุรกิจให้มีความสมบูรณ์ มีประสิทธิภาพและประสิทธิผล สามารถเกิดการจัดการความยั่งยืน (Sustainable Development) ขององค์กรได้อย่างแท้จริง โดยได้รับประโยชน์ดังนี้ 1) ปรับปรุงประสิทธิภาพของการบริหารจัดการแบบองค์รวมได้อย่างมีประสิทธิผล เกิดความต่อเนื่องของกระบวนการบริหารจัดการ 2) พัฒนาบุคลากรและองค์กรให้มีความสามารถ ในการคาดการณ์ (Anticipate) ประเมิน (Access) เตรียมการ (Prepare) ป้องกัน (Prevent) ตอบสนอง (Response) และฟื้นฟู (Recovery) ที่เกี่ยวข้องในการดำเนินธุรกิจอย่างต่อเนื่อง 3) สร้างขีดความสามารถที่ทำให้องค์กรเกิดความยืดหยุ่นในการบริหารจัดการ และ 4) สร้างภาพลักษณ์ที่ดีให้แก่ องค์กร

โดยสรุปแล้ว จะเห็นได้ว่าปัจจุบันการจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) มีความจำเป็นอย่างยิ่ง เนื่องจากการเกิดภัยพิบัติย่อมสร้างความเสียหายมหาศาลแก่ชีวิตและทรัพย์สิน การจัดการความต่อเนื่องทางธุรกิจ นอกจากจะมีแนวทาง BS25999 แล้ว ยังมีมาตรฐาน ISO 22301 ที่หน่วยงานสามารถพิจารณาและประยุกต์ใช้ในการจัดการและพัฒนาความต่อเนื่องได้ เพื่อเป็นมาตรฐานให้องค์กรมีการจัดการแบบองค์รวม บ่งชี้ภัยคุกคามต่อองค์กร และผลกระทบของภัยคุกคามนั้นต่อการดำเนินธุรกิจ และเป็นกรอบการสร้างขีดความสามารถให้องค์กรมีความยืดหยุ่น เพื่อตอบสนองและปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย ชื่อเสียง ภาพลักษณ์ และกิจกรรมที่สร้างมูลค่าที่มีประสิทธิผล ซึ่งมาตรฐานสำหรับการจัดการความต่อเนื่องทางธุรกิจนี้สามารถใช้ได้กับทุกองค์กร ทุกประเภท และทุกขนาด

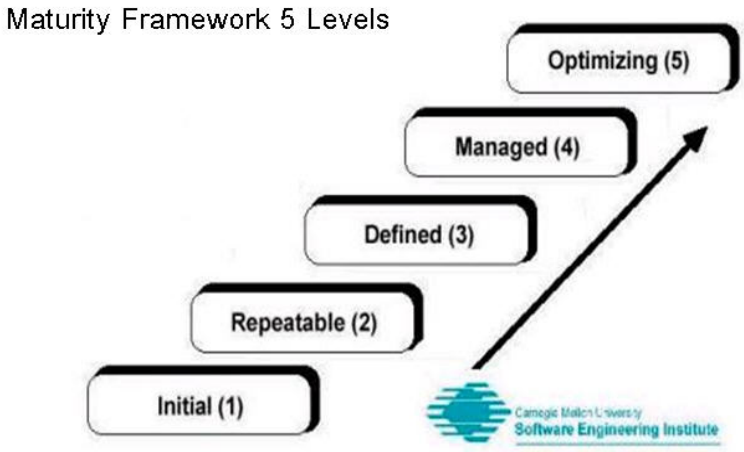
2.7 ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล

2.7.1 ตัวแบบวุฒิภาวะความสามารถ

ความหมายที่แท้จริงของคำว่าวุฒิภาวะ (Maturity) คือ ความสุกงอม ความเติบโตเต็มที่ (ripness) หมายถึง แนวคิดในการพัฒนาจากสถานะเริ่มต้นไปยังสถานะขั้นสูง โดยมีแนวคิดพื้นฐานที่อยู่เบื้องหลังสิ่งนี้คือ แนวคิดเกี่ยวกับวิวัฒนาการที่แสดงให้เห็นว่า เรื่องนั้น ๆ อาจมีการเปลี่ยนผ่านสถานะไปได้ในหลาย ๆ สถานะ ผ่านตัวกลางตัวหนึ่งจนถึงวุฒิภาวะ โดยทั่วไปอาจกล่าวได้ว่าคำจำกัดความของวุฒิภาวะ เป็นการรวมองค์ประกอบของการวิวัฒนาการหรือประสบการณ์มาจากแนวทางการปฏิบัติที่ดี (Good practice) ยิ่งไปกว่านั้นวุฒิภาวะยังต้องแสดงให้เห็นถึงกระบวนการที่เข้าใจกันเป็นอย่างดี ต้องมีการทำเอกสารเพื่อสนับสนุนแนวทางในการปฏิบัติและต้องมีการฝึกอบรม โดยที่องค์กรจะต้องสามารถนำไปใช้ได้อย่างสม่ำเสมอในทุก ๆ โครงการ มีการติดตามและปรับปรุงอย่างต่อเนื่องโดยผู้ใช้ (Fraser et al., 2002)

ตัวแบบวุฒิภาวะความสามารถ (Capability Maturity Model หรือ CMM) เรียกได้อีกอย่างหนึ่งว่า SW CMM (The Capability Maturity Model for Software) โดยที่ ตัวแบบ (Model) หมายถึง ตัวแบบ หรือ แบบจำลอง ซึ่งก็คือ ที่รวมขององค์ประกอบต่างๆ ที่ใช้บรรยายกระบวนการที่มีประสิทธิผล โดยกระบวนการที่นำมารวมไว้ในโมเดลนั้นได้รวมทั้งส่วนที่พิสูจน์จากประสบการณ์แล้วว่าใช้แล้วได้ผลจริง โดยจะได้นำเอาตัวแบบนี้ไปใช้เพื่อกำหนดลำดับความสำคัญและส่วนของขั้นตอนในการปรับปรุงกระบวนการทำงาน ช่วยให้เกิดความมั่นใจว่ากระบวนการจะมีความเสถียรและทำงานได้ถูกต้อง เพื่อเป็นแนวทางในการปรับปรุงกระบวนการของงาน, โครงการและหน่วยงานต่างๆ และเพื่อช่วยในการทำนายระดับของการปรับปรุงกระบวนการว่าดีขึ้นเพียงใด

Software Engineering Institute (SEI) ของมหาวิทยาลัยคาร์เนกี เมลลอน (Carnegie Mellon University) ได้พัฒนาต้นแบบวุฒิภาวะความสามารถ ซึ่งเป็นมาตรฐานที่กำหนดขึ้นเพื่อวัดความเชื่อมั่นและคุณภาพของกระบวนการพัฒนาซอฟต์แวร์ของบริษัทพัฒนาซอฟต์แวร์ (Software House) โดยมาตรฐานตัวแบบวุฒิภาวะความสามารถได้รวมเอาข้อดีของมาตรฐานการบริหารคุณภาพโดยรวม (Total Quality Management : TQM) มาปรับใช้กับการพัฒนาซอฟต์แวร์ (Software Development) โดยเฉพาะ จึงเป็นตัวแบบที่ใช้วัดความเชื่อมั่นและคุณภาพของกระบวนการพัฒนาซอฟต์แวร์ของบริษัทพัฒนาซอฟต์แวร์ที่มีอยู่ในปัจจุบัน มาตรฐานตัวแบบวุฒิภาวะความสามารถจัดเป็นมาตรฐานที่ได้รับความนิยมระดับสากลในเรื่องของซอฟต์แวร์ที่บริษัทพัฒนาซอฟต์แวร์ สามารถนำไปใช้ เพื่อเป็นแนวทางในการปรับปรุงกระบวนการพัฒนาซอฟต์แวร์ โดยมาตรฐานตัวแบบวุฒิภาวะได้แสดงไว้ตามภาพประกอบที่ 2.6



ภาพประกอบที่ 2.6 มาตรฐานของวุฒิภาวะความสามารถ 5 ระดับ

โดยความสามารถแบ่งระดับความสามารถในการพัฒนาซอฟต์แวร์ของบริษัทผู้พัฒนาซอฟต์แวร์ไว้ 5 ระดับ ดังนี้

1. ระดับเริ่มต้น (Initial Level) เป็นการพัฒนาเพียงด้านเดียว เป็นระดับที่บริษัทผู้พัฒนาซอฟต์แวร์ต้องอาศัยความสามารถของบุคลากรเพียงอย่างเดียว ลักษณะการทำงานไม่เป็นทางการมากนัก ยังไม่มีการควบคุมที่ดี ไม่มีการวางแผนงานที่เป็นระบบ จึงไม่สามารถประเมินคุณภาพของผลงานที่ได้ว่าจะมีคุณภาพดีหรือไม่ และซอฟต์แวร์ที่พัฒนาขึ้นส่วนใหญ่ไม่มีการนำไปพัฒนาต่อ

2. ระดับจัดทำโครงการเบื้องต้น (Repeatable Level) ในระดับนี้มีการนำการบริหารการจัดการโครงการเบื้องต้น (Basic Project Management) มาใช้ มีการวางแผนการทำงานอย่างเป็นระบบ มีการจัดทำเอกสาร และสามารถตรวจสอบได้ บริษัทผู้พัฒนาซอฟต์แวร์ที่สามารถเข้าสู่ระดับนี้ได้ จะสามารถพัฒนาซอฟต์แวร์ในแต่ละโครงการที่มีลักษณะแบบเดียวกันให้ประสบผลสำเร็จได้เช่นเดียวกับโครงการที่ทำสำเร็จไปแล้ว

3. ระดับที่มีการกำหนดขึ้นอย่างชัดเจน (Defined Level) ในระดับนี้เป็นการพัฒนาเพิ่มขึ้นจาก Repeatable Level การเข้าสู่ระดับบริษัทผู้พัฒนาซอฟต์แวร์จะต้องมีการกำหนดแนวทางในการปฏิบัติงานด้านการจัดทำเอกสารและกำหนดมาตรฐานในการปฏิบัติงาน ทั้งในส่วนของการบริหารโครงการ และด้านการพัฒนาซอฟต์แวร์ ได้อย่างเหมาะสม โดยมาตรฐานดังกล่าวต้องมีแนวปฏิบัติแบบเดียวกันทั้งองค์กร นั้นคือ องค์กรเริ่มมีระเบียบวิธีการปฏิบัติงานเป็นมาตรฐานของตนเอง

4. ระดับมีการจัดการ (Managed Level) เป็นการพัฒนาเพิ่มขึ้นจาก Defined Level ลักษณะการปฏิบัติในระดับนี้ผู้จัดทำต้องมีการรวบรวมข้อมูล รายละเอียดการปฏิบัติงานต่างๆ ที่เกิดขึ้นไว้ในรูปของสถิติ (Statistical Process Control) เพื่อนำข้อมูลนั้นมาใช้ในการศึกษาวิเคราะห์ผลการทำงาน สามารถวัดผล และควบคุมกระบวนการทางซอฟต์แวร์ได้

5. ระดับปรับปรุงให้เหมาะสมที่สุด (Optimizing Level) เป็นระดับที่ได้นำเอาหลักการจัดการคุณภาพ(Continuous Process Improvement) มาใช้ เพื่อป้องกันไม่ให้เกิดข้อบกพร่องในการปฏิบัติงาน และนำไปสู่การพัฒนาอย่างต่อเนื่อง รวมถึงเพื่อให้บริษัทผู้พัฒนาซอฟต์แวร์สามารถปรับเปลี่ยนตัวเองให้สอดคล้องกับการเปลี่ยนแปลงทางด้านเทคโนโลยีได้

2.7.2 ตัวแบบวุฒิภาวะความสามารถในการจัดการโซ่อุปทาน

แนวคิดของกระบวนการหรือวุฒิภาวะของความสามารถนั้นถูกนำไปใช้กับหลายๆ มุมมองในหลาย ๆ ด้านที่เกี่ยวข้องกับโซ่อุปทานมากขึ้น โดยสามารถนำมาใช้ได้ทั้งเป็น วิธีการประเมินผล และเป็นส่วนหนึ่งของการดำเนินการจัดทำกรอบแนวคิดสำหรับการปรับปรุง โดยทั่วไปแล้ว ตัวแบบวุฒิภาวะได้ถูกนำเสนอไว้ในกิจกรรมที่หลากหลาย ตัวอย่างเช่น การจัดการโซ่อุปทาน (SCM) ระบบการวางแผนทรัพยากรองค์กร (ERP) ความสัมพันธ์ของผู้จำหน่าย ประสิทธิภาพการวิจัยและพัฒนา การพัฒนาผลิตภัณฑ์ นวัตกรรม การออกแบบผลิตภัณฑ์ ความร่วมมือในการพัฒนาผลิตภัณฑ์และความน่าเชื่อถือของผลิตภัณฑ์ (Champlin, 2002) แนวคิดหลักของตัวแบบวุฒิภาวะ คือสิ่งที่อธิบายได้โดยทั่วไปในรูปประโยค เพียงไม่กี่ประโยค ที่สามารถบ่งบอกได้ถึงพฤติกรรมของบริษัทหรือองค์กรว่ามีระดับของวุฒิภาวะอยู่ที่ใด ด้วยตัวแบบวุฒิภาวะนี้บริษัทหรือองค์กรยังสามารถบอกได้ถึงระดับวุฒิภาวะในปัจจุบัน และสามารถที่พิจารณาเพื่อที่จะทำการพัฒนาที่มุ่งไปสู่การปฏิบัติขั้นสูงต่อไปได้

กระบวนการทางธุรกิจเป็นกระบวนการที่เกี่ยวข้องกับวิธีการ ทักษะ เครื่องมือ ทรัพยากรมนุษย์ และวัสดุขององค์กรที่แตกต่างกัน โดยที่องค์ประกอบเหล่านี้ต่างก็เป็นส่วนประกอบที่มีอิทธิพลอย่างมากต่อการพัฒนาอย่างยั่งยืนขององค์กร (Randeree et al., 2012) เพื่อที่จะให้เกิดสิ่งต่างๆ เหล่านี้เพื่อที่จะใช้ในการสนับสนุนองค์กรให้มีการดำเนินงานที่มีประสิทธิภาพนั้น องค์กรต่างๆ จำเป็นต้องที่จะพัฒนาในเรื่องของ ขั้นตอน (Stages), การปฏิสัมพันธ์ (Interactions) และการพึ่งพาซึ่งกันและกัน (Interdependency) ต่อกระบวนการทางธุรกิจต่างๆ ที่มีความหลากหลาย (Duffy, 2001) วุฒิภาวะ (Maturity) ของกระบวนการจะมีวงจรชีวิต (Lifecycle) และมันจะถูกนำมาใช้ในประเมินได้นั้นจะขึ้นอยู่กับกระบวนการที่ได้ถูกนิยาม, ได้ถูกจัดการ, ได้ถูกวัดและมีการเปลี่ยนแปลงในช่วงเวลาหนึ่งๆ (Randeree et al., 2012) วุฒิภาวะของกระบวนการสามารถวัดออกมาได้ด้วย ตัวแบบวุฒิภาวะ (Maturity models) ซึ่งจะต้องเป็น

กระบวนการที่มีการให้ความสำคัญไปที่เป้าหมายที่ต้องการจะประสบความสำเร็จนั้นจะต้องผ่านขั้นตอนที่เพิ่มขึ้น ดังนั้นตัวแบบวุฒิภาวะ จะเป็นตัวที่บ่งชี้ถึงวิธีการที่ถือว่าเป็นองค์ประกอบที่เกี่ยวข้องกับคำนิยาม, การประเมินผล, การจัดการและการควบคุมของกระบวนการทางธุรกิจต่างๆ (McCormack et al., 2008)

การวัดประสิทธิภาพในการดำเนินงานนั้นเป็นแนวคิดพื้นฐานในการจัดการกระบวนที่มีความสำคัญต่อองค์กรในการที่กำหนดและรักษาความได้เปรียบด้านการแข่งขันด้วยกระบวนการที่เหนือกว่า วิธีการวัดอันหลากหลายและเทคนิคในการเปรียบเทียบ (Benchmarking Techniques) ตัวอย่างเช่น Balanced Score-card, ตัวแบบ EVA และ มาตรฐาน ISO ได้เกิดขึ้นมาเมื่อกว่าทศวรรษในการที่จะช่วยฝ่ายบริหารในการประเมินความสามารถ (Capabilities) และข้อบกพร่อง (Shortcoming) และนอกจากนั้นแล้ว มันจะช่วยในการพัฒนากลยุทธ์เพื่อสนับสนุนต่อสภาวะการณ์ที่มีการแข่งขัน ซึ่งจุดเริ่มต้นของสิ่งเหล่านี้ส่วนมากจะเน้นไปที่การพัฒนาในเรื่องการวัดประสิทธิภาพในการดำเนินงานและควบคุมระบบสำหรับกระบวนการในระดับขององค์กร และได้รับความสำเร็จเป็นอย่างมากในการพัฒนากระบวนการในหลายๆ บริษัท

อย่างไรก็ตาม การล้ำหน้าทางด้านเทคโนโลยีได้นำมาซึ่งโอกาสใหม่ ๆ สำหรับการร่วมมือประสานงานกันระหว่างองค์กรภายใน และ ประสิทธิภาพที่มากขึ้นในโซ่อุปทาน แต่โชคก็ยังไม่เข้าข้างมากนัก เนื่องจากว่า มันยังมีเทคนิคหรือระเบียบวิธีที่จะนำมาใช้ในการวัดและการเปรียบเทียบที่เป็นระบบขององค์กรต่างๆ ภายในกระบวนการด้านโซ่อุปทาน ดังนั้นแล้ว ในการที่จะตอกย้ำไปในประเด็นเหล่านี้ จึงมีความประสงค์ที่จะพัฒนาและนิยามเทคนิคและระเบียบวิธีที่จะนำมาใช้ในการวัดประสิทธิภาพในการดำเนินงานของโซ่อุปทาน ซึ่งจะช่วยให้องค์การสามารถนำไปตอบคำถามเพื่อพัฒนา เครือข่ายในการเชื่อมโยงกันระหว่างองค์กรต่างๆ ในโซ่อุปทานในมากยิ่งขึ้น

จากองค์ความรู้ที่เกี่ยวกับกระบวนการธุรกิจและการจัดการกระบวนการธุรกิจ การควบคุมหรือการปรับปรุงกระบวนการคงจะเป็นระบบหรือเป็นขั้นตอนเพิ่มมากขึ้น ธุรกิจหรือแม้แต่ชีวิตเราเองก็ย่อมมีการพัฒนาเจริญเติบโต การจัดการขององค์กรธุรกิจนั้นเราคงไม่หวังผลกันแค่ผลลัพธ์ที่เกิดขึ้นในปัจจุบันเท่านั้น แต่คงจะต้องวัดเปรียบเทียบระหว่างอดีต ปัจจุบันและอนาคตในภาพรวมขององค์กรว่ามีระดับวุฒิภาวะ (Maturity Level) ของการพัฒนาองค์กรอย่างไรบ้าง เหมือนกับคนเราเองที่มีสภาพเป็นเด็ก วัยรุ่น ผู้ใหญ่ที่บรรลุนิติภาวะแล้ว สภาพของวุฒิภาวะ (Maturity) ของผู้ใหญ่หรือคนที่มีอายุมากและผ่านประสบการณ์มามากย่อมมีความสามารถในการตัดสินใจได้มากกว่า

แนวคิดเบื้องต้นของวุฒิภาวะ (Maturity) คือ การที่องค์กรต่าง ๆ ที่มีวุฒิภาวะหรือผ่านการดำเนินงานมาระยะหนึ่งแล้ว ได้ทำธุรกิจหรือดำเนินงานอย่างมีระบบ ในขณะที่องค์กรที่ยังมีวุฒิภาวะไม่สูงมากนักจะบรรลุผลสำเร็จในกิจกรรมขององค์กรโดยความสามารถส่วนตัวของแต่ละบุคคลโดยใช้แนวทางแบบการแก้ไขปัญหาแบบเฉพาะหน้าเสียเป็นส่วนใหญ่ ตำราบางเล่มก็ได้พยายามที่จะนิยามวุฒิภาวะให้ดูหนักแน่นขึ้นโดยการอธิบายในรูปแบบขององค์กรที่สามารถคาดการณ์ได้ (Predictability) สามารถควบคุมได้ และมีประสิทธิผล (Effectiveness)

ความสามารถในการคาดการณ์ได้จะหมายถึง การใช้เครื่องมือในการจัดตารางการทำงาน การใช้ระยะเวลาในการทำงาน และเป้าหมายนั้นตรงกันหรือไม่ องค์กรที่มีวุฒิภาวะไม่พอก็มักจะมีการสร้างตารางการทำงาน แต่ก็บ่อยครั้งการทำงานก็ไม่เป็นไปตามตารางหรือเป้าหมาย ทำให้พลาดเป้าหมายไปมาก ส่วนองค์กรที่มีวุฒิภาวะแล้วก็จะสร้างตารางการทำงานขึ้นมาเหมือนกันและก็จะพยายามดำเนินงานให้ได้ตามตาราง สำหรับการควบคุมนั้นจะหมายถึง ความสม่ำเสมอกับสิ่งที่องค์กรต้องการที่จะบรรลุเป้าหมายที่ตั้งไว้ครั้งแล้วครั้งเล่าด้วยความคลาดเคลื่อนเพียงเล็กน้อย ส่วนองค์กรที่ยังไม่บรรลุวุฒิภาวะก็จะไม่มีความมั่นใจในเป้าหมายว่าจะบรรลุผลสำเร็จหรือไม่ และอาจจะไม่แน่ใจระยะเวลาที่กำหนดไว้ในตารางการทำงาน 8 ช.ม. ในแต่ละวัน หรือแต่ละสัปดาห์นั้นจะเป็นไปตามที่กำหนดหรือไม่ ส่วนประสิทธิผลนั้นจะอ้างถึงการบรรลุผลสำเร็จที่ถูกต้องในลักษณะที่มีประสิทธิภาพ องค์กรที่มีวุฒิภาวะจะบรรลุเป้าหมายของตัวเองอย่างแม่นยำตามที่องค์กรได้ให้คำมั่นไว้ว่าจะต้องทำให้ได้ องค์กรที่ยังไม่มีวุฒิภาวะส่วนใหญ่แล้วจะบรรลุผลบ้างเป็นบางเป้าหมายไม่ใช่ทุกเป้าหมายที่ตั้งไว้ ยิ่งไปกว่านั้นต้นทุนและคุณภาพของงานอาจจะไม่เป็นไปตามที่ตั้งไว้ พูดในอีกแบบหนึ่งว่าองค์กรที่มีวุฒิภาวะสูงจะมีกระบวนการทำงานที่เป็นระบบ มีการจัดทำเอกสารในการดำเนินงาน ข้อมูลต่าง ๆ ที่ได้ถูกจัดเก็บจากอดีต จะนำมาเพื่อที่จะใช้ในการคาดการณ์สิ่งที่จะเกิดขึ้นเมื่อเหตุการณ์ในลักษณะเดียวกันนั้นเกิดขึ้นในอนาคตอีกครั้งหนึ่ง

หลายองค์กรยังไม่มีความคิดในเชิงกระบวนการ ในกรณีเหล่านั้นเราพบว่าองค์กรนั้น ๆ จะกำหนดวุฒิภาวะของหน่วยงานหรือฟังก์ชันการทำงานมากกว่า ถ้าเราพบว่าบริษัทผู้ผลิตรายหนึ่งอยู่ในระดับวุฒิภาวะที่ 1 นั้นหมายถึงกลุ่มของฟังก์ชันการทำงานในองค์กรไม่ได้ถูกพิจารณาคิดในรูปแบบของกระบวนการ และยังไม่มีความตั้งใจในการกำหนดการทำงานในรูปแบบของกระบวนการ แต่ในทางตรงกันข้ามองค์กรนั้นจะพึ่งพาการทำเป้าหมายและมาตรวัดที่ขึ้นอยู่กับฟังก์ชันการทำงานในหน่วยผลิตซึ่งไม่ใช่กระบวนการเฉพาะที่หน่วยผลิตหรือฟังก์ชันการทำงานนั้น ๆ มีส่วนร่วมอยู่ การที่องค์กรต่าง ๆ จะเคลื่อนตัวเองไประดับวุฒิภาวะที่สูงกว่าระดับที่ 1 จะต้องเผชิญหน้ากับการกำหนดขอบเขตขององค์กรที่เรากำลังมองในรูปแบบของกระบวนการต่าง ๆ ขององค์กร และมีความจำเป็นมีจะต้องมีมาตรฐานในการสื่อสารถึงกระบวนการต่าง ๆ

องค์กรต่าง ๆ นั้นก็มีแนวทางต่างกันในการอธิบายว่าองค์กรนั้นมีการจัดการอย่างไร คำอธิบายอย่างเดียว ตามปกติแล้วก็สามารถบอกได้ในเรื่องวุฒิภาวะขององค์กร องค์กรที่ไม่มีวุฒิภาวะเลย ก็จะมองตัวเองในรูปแบบของหน่วยงาน ฝ่าย และวาดผังองค์กรของตัวเองแบบเดิม ๆ ตามตำแหน่งงาน แผนกหรือฝ่าย และยึดติดที่ตัวบุคคล แต่องค์กรที่มีวุฒิภาวะสูงกว่าจะต้องคิดในรูปแบบกระบวนการซึ่งโดยปกติแล้วเราจะพูดกันถึงโซ่คุณค่า (Value Chain) หรือบางทีอาจจะใช้คำว่า “สายผลิตภัณฑ์” แนวคิดของการประเมินระดับวุฒิภาวะขององค์กรในลักษณะนี้ได้อ้างอิงแนวคิดและคำนิยามบางคำมาจาก CMM สำหรับการพัฒนาซอฟต์แวร์ และตีความอย่างไม่เป็นทางการ วิธีการนี้น่าจะเป็นแนวทางหนึ่งที่สามารถจะดำเนินตามกระบวนการทางธุรกิจได้ ถึงแม้จะยังไม่เป็นวีการที่เป็นทางการ หรือได้รับการยอมรับในวงการ หรือชุมชน การจัดการกระบวนธุรกิจ แต่สามารถทำให้มีขั้นตอนในการประเมินอย่างรวดเร็วขององค์กรได้

ถึงแม้ว่าจะมีการเสนอตัวแบบวุฒิภาวะการจัดการโซ่อุปทานที่หลากหลาย แต่สิ่งที่คล้ายกันของตัวแบบที่นำเสนอนั้น คือการมีคุณสมบัติร่วมกันในการกำหนดจำนวนมิติหรือพื้นที่กระบวนการในขั้นตอนที่ไม่ต่อเนื่องหลายระดับ หรือระดับของวุฒิภาวะพร้อมคำอธิบายของประสิทธิภาพของคุณลักษณะในระดับต่างๆ สิ่งนี้เกี่ยวข้องกับตัวแบบวุฒิภาวะที่ได้ถูกพัฒนาขึ้นมาแล้วทั้งหมดด้วยบริบทที่แตกต่างกัน การจำแนกประเภทของตัวแบบวุฒิภาวะการจัดการโซ่อุปทาน สามารถแบ่งออกเป็น 2 กลุ่มพื้นฐาน ทั้งสองกลุ่มสามารถกำหนดให้เป็นตารางวุฒิภาวะหรือกำหนดให้เป็นแบบสอบถามแบบคล้ายลิเคิร์ท (Likert) โดยที่แบบสอบถามแบบคล้ายลิเคิร์ทถือได้ว่าเป็นรูปแบบที่สมบูรณ์แบบ ถ้าได้มีการสร้างในลักษณะเฉพาะ ในกรณีนี้คำถามเป็นเพียงข้อความที่ง่าย ๆ ที่แสดงถึงวิธีปฏิบัติที่ดี และผู้ถูกขอให้ตอบคำถามเพียงแค่แสดงความคิดเห็นโดยให้คะแนน ที่ต้องมีความสัมพันธ์กับการดำเนินการขององค์กรในระดับ 1 ถึง n ซึ่งเทียบเท่ากับตารางวุฒิภาวะที่ได้อธิบายเฉพาะคุณลักษณะของแนวปฏิบัติระดับบนสุดเท่านั้น เราจะเรียกตัวแบบวุฒิภาวะของการจัดการโซ่อุปทานที่รวมวิธีการตอบแบบสอบถามเข้ากับคำจำกัดความของวุฒิภาวะดังที่กล่าวมาแล้วนั้น ว่าเป็นการกำหนดแบบลูกผสม โดยทั่วไปอาจมีคำอธิบายโดยรวมของระดับวุฒิภาวะ แต่ไม่มีคำอธิบายเพิ่มเติมสำหรับแต่ละกิจกรรม (Fraser et al., 2002)

2.7.3 ตัวแบบวุฒิภาวะความสามารถความมั่นคงปลอดภัยไซเบอร์

ด้วยโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ที่ทำให้วิถีการดำเนินชีวิตในปัจจุบัน ต้องประสบต่อความเสี่ยงเนื่องจากการโจมตีทางไซเบอร์มากขึ้น โครงสร้างพื้นฐานที่สำคัญเหล่านี้ถูกกำหนดให้เป็นสินทรัพย์ หรือเป็นระบบที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยและความเป็นอยู่ที่ดีของพลเมือง รวมถึงระบบสาธารณูปโภคที่ต้องมีการผลิตและจำหน่าย น้ำ ไฟฟ้า เชื้อเพลิงและเครือข่ายการสื่อสาร (Yusta et al., 2011) ดังนั้นหากเกิดการ

หยุดชะงักไปในโครงสร้างพื้นฐานที่สำคัญอย่างน้อยหนึ่งแห่ง ก็จะมีผลทำให้เกิดเป็นเป้าหมายของการโจมตีทางไซเบอร์ได้ทั้งสิ้น ทำให้เสียกำลังคนและต้นทุนเป็นจำนวนมากในการเข้าไปดูแลแก้ไข ยิ่งไปกว่านั้น เมื่อการเชื่อมต่อและปริมาณการไหลของข้อมูลเพิ่มขึ้น ย่อมเป็นโอกาสในการโจมตีทางไซเบอร์เพิ่มขึ้น (Dupont, 2013) จึงต้องทำให้ยิ่งต้องให้ความสำคัญกับความมั่นคงปลอดภัยมากขึ้นของโครงสร้างพื้นฐานที่สำคัญ ในการเตรียมระบบให้ทนต่อการโจมตีทางไซเบอร์ผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญต้องเผชิญกับการควบคุมและมาตรฐานมากมายและการใช้งานหลายอย่างไม่สมบูรณ์หรือไม่สอดคล้องกันซึ่งจะทำให้สภาพแวดล้อมของการคุกคามนั้นรุนแรงขึ้น และทำให้เกิดการรักษาความปลอดภัยที่ผิดพลาด (Chaplin & Akridge, 2005) เพื่อให้เกิดความปลอดภัยต่อโครงสร้างพื้นฐานที่สำคัญอย่างเหมาะสม และมีความพร้อมในการทนต่อภัยคุกคามทางไซเบอร์ ผู้ประกอบการจำเป็นต้องมีเครื่องมือนอกเหนือจากการควบคุมมาตรฐานในการทำให้เกิดความเชื่อมั่นต่อโครงสร้างพื้นฐานที่สำคัญดังกล่าว

ดังนั้นผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญจึงต้องจัดทำ ตัวแบบวุฒิภาวะความสามารถความมั่นคงปลอดภัยไซเบอร์ เพื่อนำมาใช้สำหรับการประเมินและรายงานความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ ตัวแบบวุฒิภาวะความสามารถความมั่นคงปลอดภัยไซเบอร์ สามารถที่จะพัฒนา ปรับปรุง วุฒิภาวะความสามารถและประสิทธิภาพของการควบคุมที่ใช้เพื่อความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐานที่สำคัญ ตัวแบบดังกล่าวจะสามารถใช้อธิบายลำดับของระดับวุฒิภาวะ ความพร้อม ความต้องการ รวมถึงการคาดการณ์ต่อสิ่งที่จะเกิดขึ้นต่อเหตุการณ์ที่ไม่คาดคิด (Becker et al.,2009) ซึ่งตามธรรมชาติของหลักการทั่ว ๆ ไปก็ควรที่จะมีการเรียงลำดับของเหตุการณ์ที่สามารถจะเกิดขึ้น และควรมีเกณฑ์ที่กำหนดขึ้นสำหรับการวัดหรือประเมินต่อสิ่งต่าง ๆ ที่จะเกิดขึ้น (Wendler, 2012) ตัวแบบวุฒิภาวะความสามารถความมั่นคงปลอดภัยไซเบอร์ ได้รับการพัฒนาเฉพาะกลุ่มอุตสาหกรรม แต่วิธีการในการนำไปใช้งานสามารถนำไปใช้ได้กับกระบวนการต่าง ๆ ที่มีวิธีการในการดำเนินงานที่แตกต่างกันทั่วโลกได้ อย่างเช่น ความร่วมมือระหว่างภาครัฐและเอกชนเป็นรูปแบบที่ใช้กันมากที่สุดในสหรัฐอเมริกาและแคนาดา ในขณะที่มีการออกกฎระเบียบที่สามารถพบได้ทั่วไปในยุโรป (Yusta et al., 2011)

การเพิ่มขึ้นถึงความตระหนักต่อภัยคุกคาม ต่อองค์ประกอบและกรอบการปฏิบัติตามกฎระเบียบทั้งในระดับรัฐบาลและระดับอุตสาหกรรม ได้สร้างความต้องการในการประเมินและรายงานความพร้อมของผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญโดยใช้ตัวแบบวุฒิภาวะความสามารถความมั่นคงปลอดภัยไซเบอร์ จากต้นกำเนิดที่มาจากอุตสาหกรรมซอฟต์แวร์ ทำให้ตัวแบบวุฒิภาวะความสามารถความมั่นคงปลอดภัยไซเบอร์ได้ถูกพัฒนาขึ้นมา เพียงเพื่อที่จะต้องการพัฒนา ปรับปรุง แนะนำ และเพิ่มขีดความสามารถต่อกระบวนการในการพัฒนาซอฟต์แวร์

(Wendler, 2012) โดยทั่วไปแล้วตัวแบบวุฒิภาวะความสามารถจะมี 2 องค์ประกอบ: 1) วิธีการวัดและอธิบายการพัฒนาต่อสิ่งต่าง ๆ ในลักษณะที่ต่อเนื่องกันซึ่งแสดงลำดับความก้าวหน้าแบบลำดับชั้น และ 2) เกณฑ์การวัดความสามารถของสิ่งต่าง ๆ เช่นเงื่อนไขกระบวนการหรือเป้าหมายของแอปพลิเคชัน

แนวคิดของตัวแบบวุฒิภาวะของความสามารถได้ถูกพัฒนาขยายไปถึงขอบเขตของความมั่นคงปลอดภัยไซเบอร์ และสามารถนำไปใช้กับการป้องกันโครงสร้างพื้นฐานที่สำคัญแทนที่จะมีรายการตรวจสอบที่เรียบง่ายอย่างที่เป็นมา ในปัจจุบันนี้ผู้จัดการต่าง ๆ จะได้มีมีเกณฑ์ที่ชัดเจนในการที่จะวัดความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ (Debreceny, 2006; Lahrmann et al., 2011; Siponen, 2002) โดยมีตัวแบบที่เปลี่ยนไปจากเดิม จาก International Organization for Standardization's Systems Security Engineering Capability Maturity Model (SSE-CMM), Citigroup's Information Security Evaluation Model (CITI-ISEM) และ Computer Emergency Response Team / CSO Online at Carnegie Mellon University (CERT/CSO) เปลี่ยนมาสู่แนวคิดในศตวรรษใหม่ที่มีแนวคิดที่มีความทันสมัยในปัจจุบัน เช่น International Organization for Standardization (ISO/IEC) standards, the National Institute of Standards and Technology (NIST) Cybersecurity framework, the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2), และ the U.S. Department of Homeland Security's NICE-CMM released in 2014 ตัวแบบวุฒิภาวะความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ทันสมัยเหล่านี้เป็นขั้นตอนสำหรับวิวัฒนาการสู่เส้นทางการพัฒนานโยบาย และกระบวนการเพื่อความมั่นคงปลอดภัยและการรายงานความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญ

The U.S. Department of Energy's C2M2 เป็นตัวแบบวุฒิภาวะความสามารถที่รวมเอา ES-C2M2 และ ONG-C2M2 มาไว้ด้วยกัน เป็นตัวแบบวุฒิภาวะและเครื่องมือประเมินผลเพื่ออำนวยความสะดวกในการเตรียมความพร้อม ต่องานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ประกอบการเครือข่ายการผลิตและจำหน่ายพลังงาน อย่างไรก็ตามเครื่องมือนี้ใช้เฉพาะกับภาคพลังงานเท่านั้น ซึ่งมีข้อจำกัด และการบังคับใช้

The U.S. Department of Homeland Security's NICECMM และ the Software Engineering Institute at Carnegie Mellon University มุ่งเน้นไปที่การพัฒนในส่วนของทีมงาน วุฒิภาวะของกระบวนการ และแนวทางในการปฏิบัติเพื่อการคืนสภาพได้ของการปฏิบัติการ เพื่อช่วยองค์กรให้มีความพร้อมด้านความปลอดภัยไซเบอร์ อย่างไรก็ตามในการดำเนินการยังไม่ได้เสนอแนวทางในการปฏิบัติที่ดีที่สุดในการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะ ยังต้องมีการเพิ่มเติมเกี่ยวกับกรอบแนวคิดเพื่อที่จะนำมาใช้กับตัวแบบดังกล่าวนี้

มาตรฐาน ISO ซึ่งครอบคลุม ในเรื่องของการรับรองอุปกรณ์ (ISO / IEC 15408) ระบบการจัดการความมั่นคงปลอดภัยของข้อมูล (ISO / IEC 27001) และกระบวนการวิศวกรรมความมั่นคงปลอดภัยของซอฟต์แวร์ (ISO / IEC 21827 หรือ SSE-CMM) เมื่อนำเอามาตรฐานเหล่านี้มาใช้ร่วมกันจะทำให้เกิดระบบที่สมบูรณ์ สำหรับความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร อย่างไรก็ตามการนำมาตรฐานจำนวนมากมีความซับซ้อน เสียเวลาและมีค่าใช้จ่ายที่เพิ่มขึ้น

กรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST คือชุดของกิจกรรมที่จะช่วยเหลือองค์กรในการพัฒนาความพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์ แม้ว่ากรอบการทำงานนี้จะแข็งแกร่ง แต่ก็ขึ้นอยู่กับผู้ให้บริการในการพัฒนาและปรับให้เข้ากับองค์กรนั้น ๆ ในการจัดการต่อช่องโหว่ที่เกิดขึ้น

ตัวแบบทั้งหมดที่ได้อธิบายไปนั้น ได้สรุปไว้ในตารางที่ 2.11 โดยเป็นการแนะนำสำหรับองค์กรในการจัดทำแผนความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยองค์กรต่าง ๆ จะได้เห็นถึงตัวแบบที่มีความสามารถในระดับสูงกว่ามาตรฐาน ISO ที่ซึ่งจะสามารถนำมาใช้ในการดำเนินการเพื่อรับมือต่อภัยคุกคามไซเบอร์ โดยข้อมูลที่ปรากฏในตารางได้ให้คำแนะนำที่เฉพาะเจาะจงมากขึ้น มีความซับซ้อนในการดำเนินการมากขึ้น ดังนั้นสำหรับผู้ประกอบการที่ต้องการเตรียมความพร้อมอย่างเพียงพอสำหรับการโจมตีทางไซเบอร์ จะได้ทราบข้อมูลถึงตัวแบบที่มีลักษณะเฉพาะเพื่อจะได้นำเอาไปใช้ตามความเหมาะสมขององค์กรของตนเองต่อไปได้

ตารางที่ 2.12 ตัวแบบวุฒิภาวะความสามารถความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานที่สำคัญ

ตัวแบบ	ผู้จัดทำ	จุดประสงค์
C2M2	U.S. Dept of Energy	การประเมินความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับองค์กรใด ๆ ซึ่งประกอบด้วยตัวแบบวุฒิภาวะและเครื่องมือประเมินผล
ES-C2M2	U.S. Dept of Energy	การปรับให้ C2M2 มีความเหมาะสมกับหน่วยงานด้านพลังงาน
ONG-C2M2	U.S. Dept of Energy	การปรับให้ C2M2 มีความเหมาะสมกับหน่วยงานด้านน้ำมันและก๊าซธรรมชาติ

ตารางที่ 2.12 (ต่อ)

ตัวแบบ	ผู้จัดทำ	จุดประสงค์
NICE-CMM	U.S. Dept of Homeland Security	กำหนดแนวทาง 3 ด้าน : กระบวนการและการวิเคราะห์, การกำกับแบบบูรณาการ, ผู้ปฏิบัติงานที่มีทักษะและเทคโนโลยีเพื่อการทีมงาน
CERT-RMM	CERT / SEI	กำหนดแนวทางการปฏิบัติขององค์กรเพื่อการคืนสภาพได้ในการปฏิบัติงาน ความมั่นคงปลอดภัย และความต่อเนื่องทางธุรกิจ
ISO/IEC 15408	ISO	เกณฑ์การรับรองความปลอดภัยของคอมพิวเตอร์
ISO/IEC 27001	ISO	Information Security Management System (ISMS) specification
ISO/IEC 21827 SEE-CMM	ISO	การประเมินกระบวนการวิศวกรรมความมั่นคงปลอดภัยของซอฟต์แวร์
NIST Cybersecurity Framework	NIST	กรอบสำหรับการพัฒนาโครงสร้างพื้นฐานที่สำคัญของรัฐบาลกลาง ผ่านชุดกิจกรรมที่ออกแบบมาเพื่อพัฒนาการดำเนินงานสำหรับผู้ประกอบการ

2.7.4 องค์ประกอบในการพัฒนาตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานเพื่อจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขนาดกลางและขนาดย่อม

ในงานวิจัยที่ผู้วิจัยนำเสนอในครั้งนี้ ผู้วิจัยมีวัตถุประสงค์ในการที่จะสร้างแนวทางเบื้องต้นในการพิจารณาถึงวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย ด้วยการประยุกต์ใช้แนวคิดของกรอบการทำงานด้านความปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) ร่วมกับมาตรฐานการจัดการความปลอดภัยของโซ่อุปทาน (ISO 28000) และมาตรฐานการจัดการความต่อเนื่องทางธุรกิจ (ISO

22301) เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในวิสาหกิจขาดกลางและขนาดย่อมในประเทศไทย สำหรับแนวทางในการกำหนดกรอบตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ จะแบ่งออกเป็น 2 ส่วนคือ

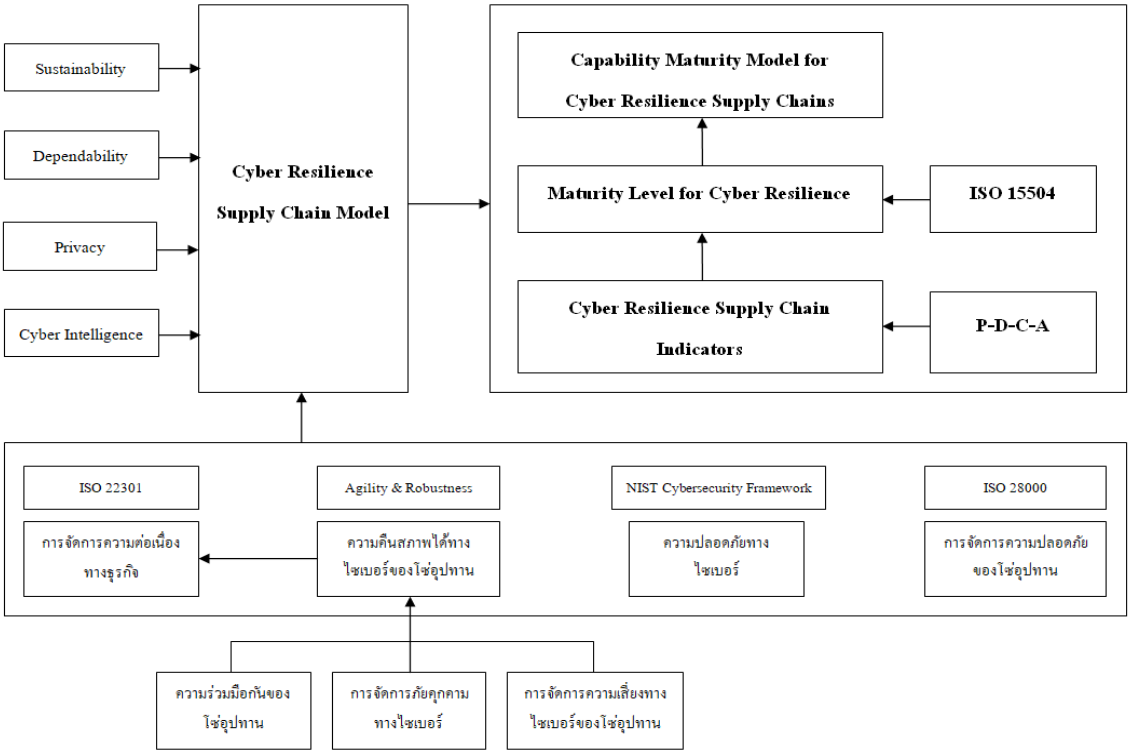
ส่วนที่ 1 : แนวทางการศึกษากรอบความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model)

ส่วนที่ 2 : แนวทางการศึกษาตัวชี้วัดของกรอบความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicators)

โดยรายละเอียดผู้วิจัยจะได้ทำการนำเสอไว้ดังต่อไปนี้

2.7.4.1 ส่วนที่ 1 : แนวทางการศึกษากรอบความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model)

แนวทางในการพัฒนากรอบความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยสามารถสรุปแนวคิดไว้ดังภาพประกอบที่ 2.7 ต่อไปนี้



ภาพประกอบที่ 2.7 แนวทางการพัฒนากรอบความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

จากรูปที่ 2.7 ผู้วิจัยขอสรุปผลการศึกษาแนวทางเพื่อการพัฒนากรอบความสามารถการคืนสภาพทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยมีรายละเอียดดังต่อนี้

1. การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilient Supply Chain)

การคืนสภาพได้ของโซ่อุปทานดิจิทัล ได้เป็นกลยุทธ์ที่มีบทบาทสำคัญในการสร้างความมั่นใจในการสร้างต่อเนื่องทางด้านธุรกิจและความน่าเชื่อถือในการบริหารต้นทุนที่มีประสิทธิภาพ การป้องกันหรือการกู้คืนจากสถานการณ์ใดๆ อันทำให้เกิดการหยุดชะงักนั้น จำเป็นต้องมีการเข้าถึงและการวิเคราะห์ข้อมูลจำนวนมาก ยิ่งไปกว่านั้นถ้าการคืนสภาพได้ของโซ่อุปทานจะต้องนำมาพิจารณาในบริบทที่มีผู้ที่มีส่วนได้ส่วนเสีย การปฏิบัติการ หรือแม้แต่กระทั่งในด้านสิ่งแวดล้อมที่หลากหลาย ในฐานะของการเป็นกลยุทธ์ที่สำคัญทางด้านธุรกิจที่ซึ่งมีการปฏิบัติการ การจัดการความเสี่ยง จึงทำให้การคืนสภาพได้ของโซ่อุปทานได้กลายมาเป็นงานที่ท้าทาย ไม่เพียงแต่ในองค์กร หรือในโซ่อุปทาน แต่ยังเป็นไปในระดับโลกได้อีกด้วย ดั้งนั้นแล้วด้วยเหตุผลนี้เทคโนโลยีสารสนเทศและการสื่อสารที่มีการพัฒนาขึ้นอยู่เรื่อยๆ เพื่อช่วยเหลือผู้จัดการโซ่อุปทาน ด้วยการพัฒนาเครื่องมือและบริการเพื่อที่จะนำมาใช้สำหรับการตรวจสอบการหยุดชะงัก สามารถที่จะสนับสนุนการสื่อสารและอำนวยความสะดวกในการฟื้นตัวอย่างรวดเร็วของโซ่อุปทาน บริษัทต่างๆ สามารถเตรียมความพร้อมสำหรับการโจมตีที่อาจเกิดขึ้นโดยการใช้เครื่องมือและเทคนิคสำหรับการจัดการความเสี่ยงของโซ่อุปทานที่เหมาะสม ทั้งนี้ก็เพื่อเป็นการลดโอกาสของการเกิดการบุกรุกและ เพื่อที่จะจัดการกับการหยุดชะงักใด ๆ ก่อนที่การโจมตีนั้นประสบความสำเร็จขึ้นได้ ในทุก ๆ ธุรกิจที่ขึ้นอยู่กับโซ่อุปทาน จำเป็นต้องที่จะต้องมีความต้องการที่จะสร้างการคืนสภาพได้ทางด้านไซเบอร์

จากการทบทวนวรรณกรรม พบว่า นักวิจัยและนักวิชาการได้ให้คำนิยามหรือคำจำกัดความของคำว่า การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) ตามที่ได้นำเสนอไว้ดังตารางที่ 2.9 นั้น จากคำนิยามหรือคำจัดความของการคืนสภาพได้ทางไซเบอร์ที่ผู้วิจัยได้ทำการศึกษามาทำให้ผู้วิจัยได้สรุปถึงความหมายของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน คือ ความสามารถของโซ่อุปทานในการที่จะรักษาระดับของผลการดำเนินงานขององค์กรให้สามารถดำเนินต่อไปได้เมื่อต้องเผชิญกับภัยคุกคามทางไซเบอร์ หมายความว่า กิจกรรมต่างๆ ของโซ่อุปทานจะต้องสามารถดำเนินงานต่อไปได้เมื่อได้รับการโจมตีทางไซเบอร์ โดยที่ระบบนั้นจะต้องทำการตรวจจับ (Detect) และตอบสนอง (React) ต่อการบุกรุกหรือโจมตีได้อย่างรวดเร็วและมีระบบ

การคืนสภาพได้ทางไซเบอร์เป็นแนวคิดที่ไม่ได้มุ่งเพียงแค่เรื่องของการป้องกันตัวจากภัยคุกคามเท่านั้น แต่ลักษณะของการคืนสภาพได้ทางไซเบอร์นั้น จะต้องมีคุณลักษณะที่จะต้องมี “ความคงทน (Robustness)” และ “ความคล่องตัว (Agility)” ต่อการถูกโจมตี จากการศึกษาของ Wieland et al. (2013) กล่าวคือ เมื่อโซ่อุปทานถูกโจมตีจากภัยคุกคามดังกล่าว ระบบจะต้องให้สามารถที่จะยังให้บริการในเชิงธุรกิจต่อไปได้ โดยที่ระบบนั้นจะต้องสามารถที่จะทำการตรวจจับการโจมตีเหล่านั้นได้อย่างรวดเร็ว สามารถบล็อกการโจมตี กักกันเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ ที่ใช้ในการทำงานที่กำลังตกเป็นเหยื่อไม่ให้แพร่กระจายการโจมตีหรือมัลแวร์เข้าสู่ระบบอื่นๆ และต้องสามารถที่ทำการจัดการคลีนให้เรียบร้อย เพื่อให้ระบบกลับสามารถกลับมาทำงานได้สมบูรณ์เป็นเหมือนเดิม Valikangas (2010) ได้ชี้ให้เห็นว่าความหยุ่นสามารถถูกนำไปปฏิบัติได้ทั้งในเชิงรุก (Proactive) และเชิงรับ (Reactive) โดยที่การปฏิบัติในเชิงรุกนั้นจะต้องมีการดำเนินการก่อนที่มีมันจะกลายเป็นสิ่งจำเป็นเมื่อเหตุการณ์ได้เกิดขึ้น และการปฏิบัติในเชิงรับจะเป็นการกู้คืนกลับหลังจากที่เกิดเหตุการณ์อันวิกฤตเกิดขึ้น โดยจากแนวคิดของ Valikangas นี้ทำให้เราได้เห็นว่า การคืนสภาพได้ นั้นจะต้องมีคุณสมบัติที่มีความสามารถได้ในทั้ง 2 ด้าน คือ ป้องกัน หรือ ต่อต้าน ต่อเหตุการณ์ใด ๆ ที่จะเข้ามากระทบต่อระบบ และจะต้องสามารถที่จะกลับคืนสู่ระดับของการดำเนินงานและระยะเวลาที่สามารถยอมรับได้หลังจากที่ได้รับผลกระทบจากเหตุการณ์ดังกล่าว (ISO, 2010)

สำหรับโซ่อุปทานนั้น โซ่อุปทานที่มีความสามารถในการสร้างการคืนสภาพได้ จะต้องเป็นโซ่อุปทานที่มีสถานะเดิมที่มีเสถียรภาพอย่างยั่งยืน หรือถ้าโซ่อุปทานนั้นได้ถูกเปลี่ยนไปเป็นสถานะใหม่ สถานะใหม่นี้ก็จะถูกทำให้สำเร็จลงได้ แสดงให้เห็นว่าความสามารถของโซ่อุปทานที่จะมีการคืนสภาพได้จะต้องเป็นโซ่อุปทานที่ต้องสามารถที่จะรับมือได้ต่อการเปลี่ยนแปลงที่จะเกิดขึ้น (Wieland et al.,2013) เพื่อที่จะรับมือต่อการเปลี่ยนแปลงและออกจากสถานะที่ไม่เสถียรนั้น โดยทั่วไปลักษณะของการที่จะเข้าไปเกี่ยวข้องกับสภาวะแวดล้อมก็จำเป็นที่จะต้องมีการรับมือทั้งในเชิงรุกและเชิงรับ (Chakravarthy, 1982) กลยุทธ์ในเชิงรับนั้นจะพบกับการเปลี่ยนแปลงของสภาวะแวดล้อม ซึ่งจะมีความเกี่ยวข้องกับการดำเนินการขององค์กร แต่ในทางตรงกันข้าม กลยุทธ์ในเชิงรุกนั้นจะถูกสร้างขึ้นมาจากการพยากรณ์และการป้องกัน (Lengnick-Hall and Beck, 2005)

สำหรับงานวิจัยนี้จะได้นำเอาแนวความคิดของที่ได้จากการศึกษาของ Wieland and Wallenburg (2012) จากผลการศึกษาได้กำหนดกลยุทธ์ไว้ 2 กลยุทธ์ที่เกี่ยวข้องกับความสามารถในการสร้างการคืนสภาพได้ โดยกลยุทธ์แรกคือ **“ความคล่องตัว (Agility)”** (Braunscheidel and Suresh, 2009; Swafford et al., 2006) และกลยุทธ์ที่ 2 คือ **“ความคงทน**

(Robustness)" (Husdal, 2010; Meepetchdee and Shah, 2007) โดยที่ความคล่องตัว จะเป็นกลยุทธ์ในเชิงรับ (Braunscheidel and Suresh, 2009) และความคงทน ซึ่งเป็นกลยุทธ์ในเชิงรุก (Shukla et al., 2011)

ความคล่องตัว พิจารณาจากคำความหมายนั้น จะมีความหมายที่แสดงถึงความสามารถทางด้านรับ ไม่ว่าจะเป็นการแสดงปฏิกิริยาตอบโต้ (React) การตอบสนอง (Respond) การปรับตัว (Adapt) รวมไปถึงการกำหนดค่าใหม่ (Re-Configure) โดยทั้งหมดเป็นคำอธิบายที่แสดงให้เห็นถึงความสามารถที่จะอธิบายถึงผลที่เกิดจากการเปลี่ยนแปลงได้ จากการศึกษาของ Bakshi and Kleindorfer (2009) ได้แสดงให้เห็นว่า ความคล่องตัว คือประเด็นที่ต้องให้ความสนใจต่อการปรับตัวขึ้นมาของระบบอย่างรวดเร็วในสถานการณ์ที่ต้องเผชิญต่อการเปลี่ยนแปลงที่ไม่สามารถคาดเดาได้ ซึ่งจะเป็นประเด็นที่คล้ายกับการศึกษาของ Khan et al. (2009) ที่ชี้ให้เห็นว่า ความคล่องตัวของโซ่อุปทานคือความสามารถในการตอบสนองต่อความไม่แน่นอนของตลาดและต้องสามารถปรับตัวได้อย่างรวดเร็ว ซึ่งหลักในการคิดนี้จะมีความสอดคล้องกับแนวคิดของการผลิตที่ต้องการความคล่องตัวเช่นเดียวกัน โดยที่เมื่อมีการเปลี่ยนแปลงสถานะของการปฏิบัติงานที่มีผลมาจากการความไม่แน่นอน หรือแม้แต่ความต้องการสินค้าที่เปลี่ยนแปลงไปเมื่อมีการสั่งผลิตไปแล้ว (Narasimhan et al., 2006) โดยในงานวิจัยนี้ผู้วิจัยจึงได้ให้ความหมายของ ความคล่องตัวของโซ่อุปทาน หมายถึง ความสามารถของโซ่อุปทานในการที่จะตอบสนองต่อการเปลี่ยนแปลงได้อย่างรวดเร็ว โดยจะต้องสามารถที่จะปรับตัวกลับสู่สถานะเริ่มต้นก่อนการเปลี่ยนแปลงได้

คงทนของโซ่อุปทาน คือความสามารถของโซ่อุปทานในการที่จะดำเนินงานตามหน้าที่ต่อไป แม้ว่าจะมีความเสียหายบางอย่างเกิดขึ้นต่อโซ่อุปทาน (Meepetchdee and Shah, 2007) โดยยังจะต้องสามารถรักษาสถานะของโซ่อุปทานให้มีความเสถียรได้เหมือนกับก่อนที่มีการเปลี่ยนแปลง (Asbjørnslett, 2008) จะต้องสามารถทนทานได้มากกว่าการตอบสนอง (Husdal, 2010) จะต้องสามารถช่วยให้ ทนได้แต่แรงกระแทกได้มากกว่าการปรับตัวให้เข้ากับแรงกระแทก (Wallace and Choi, 2011) ด้วยเหตุนี้จึงเป็นเหตุผลว่าทำไมความคงทนของโซ่อุปทานจึงเป็นกลยุทธ์ในเชิงรุก ยิ่งไปกว่านั้นความคงทนของโซ่อุปทานยังจะสามารถดำเนินการได้ดีในทุกๆ สถานการณ์ (Harrison, 2005) โดยเฉพาะอย่างยิ่งเมื่อระบบหรือสภาวะแวดล้อมนั้นได้ตกอยู่ภายใต้การเปลี่ยนแปลงที่มีขนาดใหญ่ (Yan et al., 2000) ด้วยเหตุนี้ความคงทนจึงถูกมองว่าการดำเนินการในเชิงรุกของการเปลี่ยนแปลงที่จะเกิดขึ้น ดังนั้นแล้วสำหรับงานวิจัยนี้ผู้วิจัยจึงให้ความหมายสำหรับ ความคงทนของโซ่อุปทาน คือความสามารถของโซ่

อุปทานในการที่ต่อต้านการเปลี่ยนแปลงโดยจะต้องไม่ไปกระทบต่อสถานะเริ่มต้นที่มีความเสถียรอยู่แล้ว

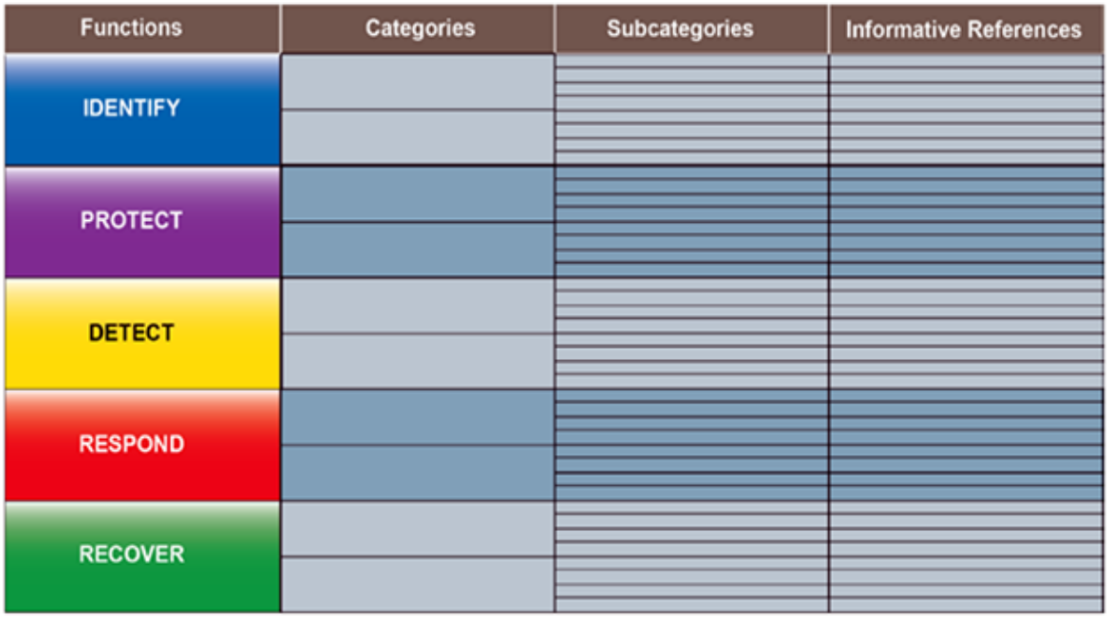
กล่าวโดยสรุป การรับมือจากภัยคุกคามด้วยวิธีการคืนสภาพได้ทางไซเบอร์ ก็คือแนวทางในการเตรียมความพร้อมเพื่อตรวจจับและตอบสนองต่อการถูกบุกรุกโจมตีได้อย่างรวดเร็วและมีระบบ จากแนวทางเดิมที่องค์กรต่างๆ นั้น จำเป็นต้องหาวิธีการในการป้องกันตัว (Protective Security) จากภัยคุกคามต่างๆ โดยองค์กรเหล่านั้นจะต้องทำการปรับตัวจากการป้องกันแบบดั้งเดิมที่ทำอยู่ในปัจจุบัน ไปจะเปลี่ยนไปเป็น “การเตรียมความพร้อม (Responsive Security)” ให้พร้อมรับมือต่อภัยคุกคามที่ไม่เคยพบเห็นมาก่อน (TechTalkThai, 2016) ดังนั้นบริษัทต่างๆ จึงต้องลงทุนในความสามารถของโซ่อุปทานเพื่อที่จะได้เตรียมการเสริมสร้างความสามารถในการรับมือต่อการโจมตีทางไซเบอร์ หรือ การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) เพื่อป้องกันและเตรียมรับมือต่อภัยคุกคามที่อาจเกิดขึ้น เพราะว่าภัยคุกคามที่เกิดจากความเสี่ยงที่ไม่รู้จัก (Unknown Threats) นี้ จะเป็นภัยคุกคามที่สามารถเกิดขึ้นใหม่ได้อยู่ตลอดเวลา และบริษัทหรือองค์กรเองก็ไม่อาจจะคาดการหรือตรวจจับได้จนกว่าจะเกิดความเสียหายต่อองค์กร

2. กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework)

แนวคิดสำคัญที่นำมาใช้ในการพัฒนากรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานที่นำมาใช้ในงานวิจัยนี้ ผู้วิจัยได้นำเอาหลักการของ **“NIST Cybersecurity Framework”** โดยหลักการนี้กำเนิดมาจากทางรัฐบาลของประเทศสหรัฐอเมริกาภายใต้การบริหารของประธานาธิบดี บารัค โอบามา ได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (NIST) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ที่สามารถครอบคลุมได้ทั้งในระดับนโยบาย การจัดการองค์กร และเทคโนโลยี เพื่อจัดการต่อความเสี่ยงไซเบอร์ที่มีผลกระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญได้อย่างเหมาะสม และมีแนวทางอย่างเป็นระบบเพื่อการจัดการความเสี่ยงทางไซเบอร์ได้อย่างมีประสิทธิภาพและประสิทธิผล

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นผลมาจากการศึกษาของ NIST มีที่มาจากการออกเอกสารฉบับหนึ่งที่เรียกว่า **“Cybersecurity Executive Order 13686 - Improving Critical Infrastructure Cybersecurity”** โดยประธานาธิบดี บารัค โอบามา เมื่อวันที่ 15 กุมภาพันธ์ พ.ศ. 2556 เป็นการกำหนดนโยบายเกี่ยวกับความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) มีการกำหนด

นโยบายในการแชร์ข้อมูล (Information Sharing) ระหว่างหน่วยงานของรัฐและเอกชน ซึ่งต่อมาได้มอบหมายให้ NIST จัดสัมมนา “Voluntary Cybersecurity Framework” เพื่อระดมความคิดจากทั้งหน่วยงานรัฐและเอกชนต่าง ๆ ซึ่งก่อให้เกิดความสำเร็จอย่างสัมฤทธิ์ผลจากการให้ความร่วมมืออย่างเต็มที่จากความเห็นของทุกภาคส่วน รวมกับกรอบการดำเนินงานตามมาตรฐานและแนวปฏิบัติที่ดี เพื่อปรับปรุงให้เป็น “National Cybersecurity Framework” ฉบับสมบูรณ์ โดยได้นำมาจัดทำเป็นกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ เรียกว่า “Framework for Improving Critical Infrastructure Cybersecurity” จากผลการศึกษาของ NIST ทำให้ได้ผลสรุปของ โครงสร้างองค์ประกอบของกรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ ที่สามารถสรุปได้ดังภาพประกอบที่ 2.8



ภาพประกอบที่ 2.8 องค์ประกอบของกรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์

ที่มา: “Framework core structure”, Framework for Improving Critical Infrastructure Cybersecurity, NIST, 12-Feb-2014

จากภาพประกอบที่ 2.8 สามารถอธิบายรายละเอียดขององค์ประกอบของกรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ได้ดังต่อไปนี้

1. **หน้าที่งาน (Functions)** เป็นกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภาพรวม ในเอกสารนี้ จำแนกเป็น 5 functions (IPDRR: Identify, Protect, Detect, Respond, Recover)

2. **กลุ่มงาน (Categories)** เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ อาทิ การจัดการทรัพย์สิน การควบคุมการเข้าถึง

3. กลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค และ/หรือกิจกรรมในการบริหารจัดการ

4. ข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทาง และแนวปฏิบัติ ที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม

โดยที่องค์ประกอบของกรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Framework Core Functions) สามารถแบ่งย่อยออกเป็นกรอบงานหลัก 5 หน้าที่งาน (functions) ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ได้แก่

1. การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ

2. การป้องกัน (Protect) เป็นการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี

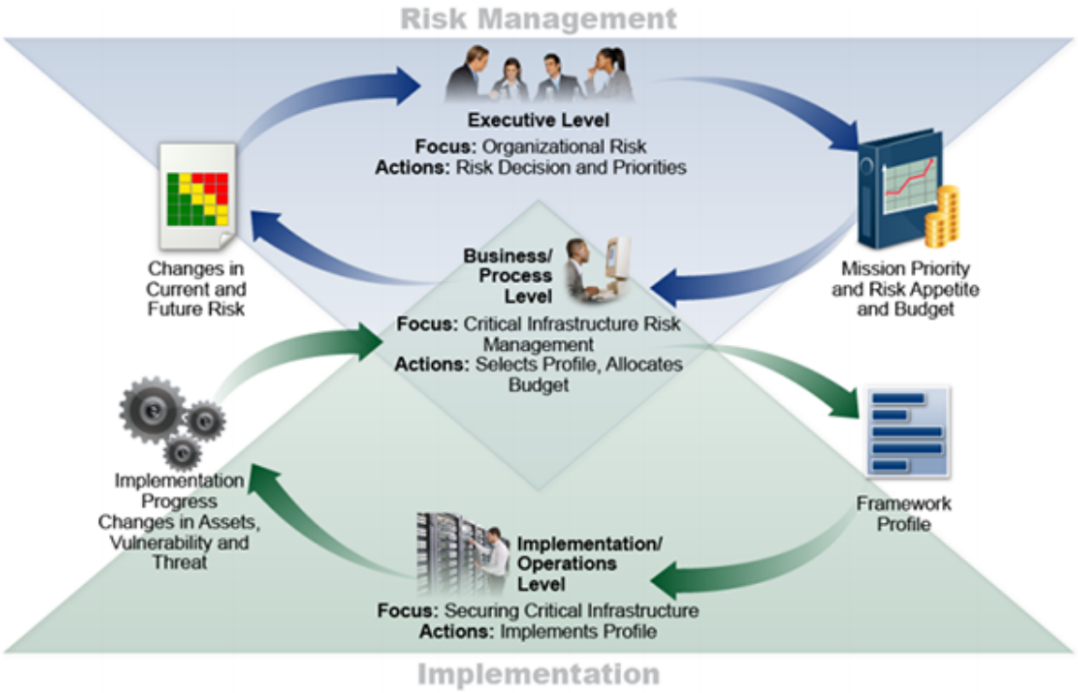
3. การตรวจจับ (Detect) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

4. การตอบสนอง (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

5. การคืนสภาพ (Recover) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงาน เพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด

การจะนำเอาหน้าที่งานทั้ง 5 ไปใช้ได้อย่างเหมาะสม องค์กรจะต้องทำการกำหนดผลลัพธ์ที่ต้องการ และกรอบปฏิบัติที่อ้างอิงสำหรับการดำเนินงานเพื่อให้สามารถบรรลุตามวัตถุประสงค์ของแต่ละอุตสาหกรรม/โครงสร้างพื้นฐาน ซึ่งจะช่วยให้องค์กรเข้าใจ และจัดทำโครงงานและระบบด้าน Cybersecurity ได้อย่างมีประสิทธิภาพมากขึ้น

วิธีการที่จะนำเอาแนวทางของ Cybersecurity Framework มาใช้ในองค์กร ควรจะต้องมีการพิจารณาถึงการไหลเวียนของข้อมูลและการตัดสินใจระดับต่าง ๆ ในองค์กร ได้แก่ ระดับบริหาร ระดับกระบวนการ/ธุรกิจ และระดับปฏิบัติการ โดยจำเป็นต้องมีการประสานงานกับส่วนงานต่าง ๆ ที่เกี่ยวข้องอย่างเหมาะสม แนวคิดการไหลเวียนของข้อมูลและการตัดสินใจในองค์กรตามกรอบ Cybersecurity Framework สามารถอธิบายได้ดังภาพประกอบที่ 2.9



ภาพประกอบที่ 2.9 แนวคิดการไหลของข้อมูลและการตัดสินใจในองค์กรตามกรอบ Cybersecurity Framework

ที่มา: “Notional Information and Decision Flows within an organization”, Framework for Improving Critical Infrastructure Cybersecurity, NIST, 12-Feb-2014.

จากภาพประกอบที่ 2.9 สามารถอธิบายได้ว่า ระดับบริหาร (Executive Level) แสดงถึงการส่งต่อข้อมูลที่เกี่ยวข้องกับการตัดสินใจในส่วนต่าง ๆ ในองค์กร โดยที่ระดับบริหาร (Executive Level) จะต้องทำการสื่อสารเกี่ยวกับเป้าหมายที่สำคัญต่าง ๆ ขององค์กร ทรัพยากรที่มี และที่นำมาใช้ได้ ตลอดจนความเสี่ยงที่กระทบองค์กรในระดับกระบวนการ จากนั้นระดับกระบวนการ (Business/Process Level) ก็จะนำข้อมูลจากระดับผู้บริหาร เพื่อใช้ในกระบวนการจัดการความเสี่ยง และประสานงานกับระดับปฏิบัติการ เพื่อจะสื่อสารความต้องการขององค์กร และทำการปฏิบัติการได้อย่างเหมาะสม และในสุดท้ายระดับปฏิบัติการ

(Implementation/Operation Level) จะต้องสื่อสารข้อมูลด้านความคืบหน้าของการปฏิบัติการกลับไปยังฝ่ายกระบวนการเพื่อจะประเมินผลกระทบ ซึ่งจะถูกรายงานกลับไปยังระดับบริหารเพื่อให้เห็นภาพรวมของการบริหารความเสี่ยง และฝ่ายปฏิบัติการก็จะนำข้อมูลดังกล่าวไปใช้เพื่อสร้างความตระหนักเกี่ยวกับผลกระทบของความเสี่ยงที่มีต่อองค์กร

กรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ได้มีประยุกต์และอ้างอิงกับมาตรฐาน ที่องค์กรส่วนใหญ่ได้ดำเนินการอยู่แล้ว อาทิ CCS CSC (Council on Cybersecurity: 20 Critical Security Controls), COBIT 5, ISA 62443-2-1:2009, ISO/IEC 27001:2013 และ NIST SP 800-53 Rev.4 รวมทั้งกรอบการดำเนินงานด้านไซเบอร์โดย NIST โดยโครงสร้างหลักของกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ (Framework Core) ตามกรอบการดำเนินงาน Cybersecurity Framework นี้ ยังสามารถแบ่งรายละเอียดลงไปในแต่ละหัวข้อของทั้ง 5 Function เพื่อเชื่อมโยงข้อมูลอ้างอิง (Informative references) ซึ่งได้แก่มาตรฐาน แนวปฏิบัติ หรือ ข้อกำหนดอื่นๆ ที่สามารถนำมาประยุกต์ใช้ในแต่ละ Function โดยไม่เพียงครอบคลุมการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระบบเทคโนโลยีสารสนเทศ แต่ยังมุ่งเน้นที่ระบบควบคุมอุตสาหกรรม (Industrial Control System: ICS) ซึ่งมีผลกระทบในวงกว้างมากกว่า ทำให้ผู้ใช้ในกลุ่มหน่วยงานระบบโครงสร้างพื้นฐานสำคัญจะได้รับประโยชน์อย่างเต็มที่ในการนำไปใช้งานได้

สำหรับงานวิจัยนี้ เนื่องด้วยผู้วิจัยได้ทำการศึกษา เพื่อที่จะทำการพัฒนาตัวแบบวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม นอกจากมาตรฐานที่มีอยู่ในกรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ จึงไม่อาจเพียงพอที่จะทำให้เกิดความสามารถสำหรับการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานเพื่อการจัดการความต่อเนื่องทางธุรกิจ ดังนั้น ผู้วิจัยจึงได้ทำการศึกษาในประเด็นเพิ่มเติม โดยมีรายละเอียดในหัวข้อถัดไป ดังต่อไปนี้

3. มาตรฐานความปลอดภัยของโซ่อุปทาน (ISO 28000)

ISO 28000 เป็นมาตรฐานสากลที่กำหนดข้อกำหนดของระบบการจัดการความปลอดภัยของโซ่อุปทานและจัดเตรียมรูปแบบการจัดการให้กับองค์กรที่ต้องการนำระบบนี้ไปใช้ มีจุดมุ่งหมายในการจัดการความเสี่ยงอย่างมีประสิทธิภาพโดยจัดกิจกรรมขององค์กรด้านความปลอดภัยของโซ่อุปทานภายใต้ระบบเดียวกับระบบการจัดการอื่น ๆ มาตรฐานใหม่ของระบบการจัดการให้กรอบที่ดึงดูดความสนใจไปยังจุดรักษาความปลอดภัยที่สำคัญในโซ่อุปทานให้กับองค์กรที่เชื่อมต่อในทางใดทางไปยังโซ่อุปทาน ในบริบทนี้โซ่อุปทานเป็นชุดของทรัพยากร

และกระบวนการที่เกี่ยวข้องกันเริ่มต้นด้วยการจัดหาวัตถุดิบและขยายผลิตภัณฑ์และบริการเพื่อเข้าถึงผู้ใช้ผ่านวิธีการขนส่งที่แตกต่างกัน การเงินรวมถึง แต่ไม่ จำกัด เพียงการจัดการข้อมูลการผลิตและโรงงานผลิต

การแข่งขันที่เพิ่มขึ้นด้วยผลกระทบของโลกาภิวัตน์จะเพิ่มความสำคัญที่ บริษัท จะต้องคำนึงถึงค่าใช้จ่ายการส่งมอบที่ตรงเวลาและคุณภาพ มาตรฐานนี้ให้กรอบใหม่ที่ดึงดูดความสนใจไปยังจุดรักษาความปลอดภัยที่สำคัญในโซ่อุปทานให้กับองค์กรที่เชื่อมต่อกับโซ่อุปทาน กรอบการทำงานนี้รวมถึง แต่ไม่ จำกัด เฉพาะด้านการเงินการผลิตการจัดการข้อมูลและการผลิต ในอีกด้านหนึ่งก็สนับสนุนองค์กรที่ดำเนินงานในทุกภาคอุตสาหกรรมในการประเมินและควบคุมความเสี่ยงด้านความปลอดภัยในขณะเดียวกันก็ลดผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามด้านความปลอดภัยและใช้หลักการจัดการพื้นฐานเช่นคุณภาพความปลอดภัยในการทำงานและการจัดการความพึงพอใจของลูกค้า ผลจากบทบาทและความสำคัญของโซ่อุปทาน ISO (The International Organization for Standardization) จึงได้ออกมาตรฐานสากล ISO/PAS 28000 ซึ่งเป็นมาตรฐานข้อกำหนดด้านการบริหารการรักษาความปลอดภัยของโซ่อุปทาน โดยประกาศใช้ครั้งแรกตั้งแต่ 15 พฤศจิกายน 2005

มาตรฐาน ISO/PAS 28000 จะกำหนดแนวทางสำหรับองค์กร ในการกำหนด นำไปปฏิบัติ ดูแลรักษาและปรับปรุงระบบการบริหารการรักษาความปลอดภัย รวมถึงลักษณะทางด้านการรักษาความปลอดภัย (Security Aspect) โดยมีเป้าหมายเพื่อรับประกันความปลอดภัยของโซ่อุปทาน ป้องกันบุคลากร สินค้า โครงสร้างพื้นฐานและอุปกรณ์ รวมถึงการขนส่ง การป้องกันอุบัติเหตุ และการป้องกันผลกระทบที่มีแนวโน้มที่จะเกิดขึ้น ทั้งนี้สามารถำไปประยุกต์ได้ในองค์กรระดับต่างๆ ทั้งขนาดเล็ก กลางและใหญ่ ทั้งในภาคอุตสาหกรรมการผลิต การบริการ การจัดเก็บและการขนส่ง การจัดจำหน่าย (รวมถึงถนน ทางรถไฟ ทางทะเลและทางอากาศ) และในขั้นตอนของการผลิตตลอดโซ่อุปทาน

ด้วยการใช้ระบบรักษาความปลอดภัยตาม IS0 28000 องค์กรจะเพิ่มความน่าเชื่อถือและความปลอดภัยที่มีตลอดโซ่อุปทาน ผลิตภัณฑ์ที่มีมูลค่าหรืออันตรายสูงสามารถขนส่งได้ทั่วโลกและเก็บไว้อย่างปลอดภัยมากขึ้น ช่วยลดความเสี่ยงด้านความปลอดภัยและทำให้มั่นใจได้ว่าการกระจายสินค้าและวัสดุจะเป็นไปอย่างรวดเร็วและปราศจากปัญหา ด้วยการผสมผสานแนวคิดในการบริหารกระบวนการของมาตรฐาน ISO 9001:2000 และมาตรฐาน ISO 14001:2004 รวมถึงแนวคิดการจัดการ PDCA (Plan-Do-Check-Act) รวมถึงข้อกำหนดในการปรับปรุงอย่างต่อเนื่อง และการบริหารความเสี่ยงในมาตรฐาน ISO 31000:2009

4. มาตรฐานระบบบริหารความต่อเนื่องทางธุรกิจ (ISO 22301)

ปัจจุบันความสนใจเกี่ยวกับการบริหารความต่อเนื่องทางธุรกิจได้เพิ่มสูงขึ้นอย่างมาก ซึ่งเป็นผลมาจากการเกิดภัยพิบัติ และภาวะฉุกเฉินขึ้นอย่างต่อเนื่อง และกระจายไปในทุก ๆ ส่วนทั่วโลก รวมถึงความรุนแรงที่ทำให้เกิดความเสียหายก็เพิ่มสูงขึ้นอย่างมากด้วย การเกิดภัยพิบัติในรูปแบบต่าง ๆ ทั้งที่เกิดขึ้นจากธรรมชาติ ไม่ว่าจะเป็นน้ำท่วม แผ่นดินไหว พายุ หรือที่เกิดขึ้นจากมนุษย์ เช่น ไฟป่า หรือโรคระบาด รวมไปถึงภาวะฉุกเฉินต่างๆ ที่เกิดขึ้นได้ทั้งจากการก่อการร้าย วินาศกรรม การจลาจล การชุมนุมทางการเมือง หรือการเสียหายที่เกิดจากอุปกรณ์ที่สำคัญ เช่น ไฟฟ้าดับ ระบบสาธารณูปโภคเสียหาย สิ่งต่าง ๆ เหล่านี้ เมื่อเกิดขึ้นล้วนส่งผลต่อการดำเนินงานขององค์กรที่อยู่ในบริเวณหรือพื้นที่ที่ได้รับผลกระทบจากเหตุการณ์ดังกล่าว เมื่อเกิดเหตุการณ์ขึ้นย่อมส่งผลกระทบที่สามารถสร้างความเสียหายต่อองค์กร ดังนั้นองค์กรต่าง ๆ จึงต้องหาแนวทางในการบริหารจัดการเพื่อให้เกิดผลเสียต่อองค์กรให้น้อยที่สุด แนวทางดังกล่าวเรียกว่า การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management)

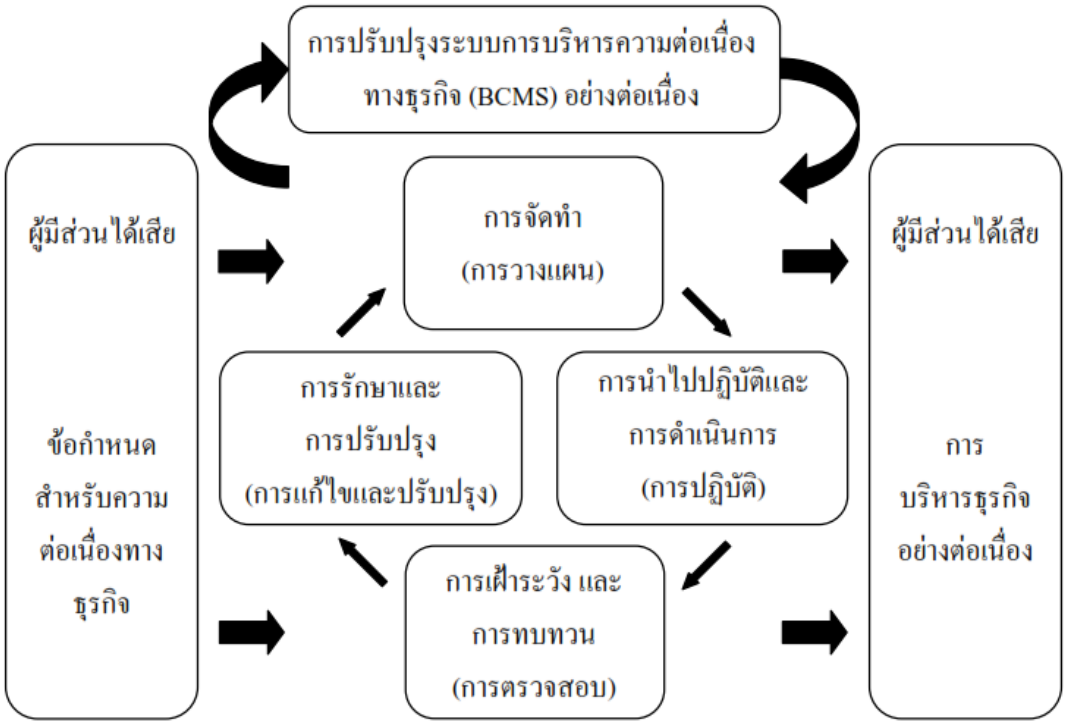
ความต่อเนื่องทางธุรกิจ (Business Continuity) หมายถึง ความสามารถทางกลยุทธ์และยุทธวิธีขององค์กรในการวางแผน และการรับมือกับอุบัติการณ์ และการหยุดชะงักทางธุรกิจ เพื่อให้เกิดความต่อเนื่องของการปฏิบัติการทางธุรกิจในระดับที่ยอมรับได้ โดยที่อุบัติการณ์ (Incident) หมายถึง สถานการณ์ที่อาจจะทำหรือนำไปสู่การหยุดชะงักทางธุรกิจ ความสูญเสีย ภาวะฉุกเฉิน หรือ ภาวะวิกฤต ด้วยเหตุนี้ผู้วิจัยสามารถกำหนดคำนิยามของ การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ว่าหมายถึง กระบวนการบริหารโดยองค์รวม ที่ระบุถึงภัยอันตรายที่อาจเกิดขึ้นกับองค์กร และผลกระทบของภัยอันตรายที่มีต่อการปฏิบัติการทางธุรกิจ รวมถึงให้แนวทางสำหรับการสร้างความยืดหยุ่นให้กับองค์กร สำหรับการตอบสนอง อย่างมีประสิทธิผลในการปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย ที่สำคัญ รวมถึงชื่อเสียง ตราสินค้า และกิจกรรมที่สร้างคุณค่า ดังนั้นการบริหารความต่อเนื่องทางธุรกิจ ประกอบด้วยการจัดการสำหรับ การฟื้นคืนสภาพ หรือความต่อเนื่องของกิจกรรมธุรกิจเมื่อเกิดการหยุดชะงักทางธุรกิจ และการบริหารโปรแกรมโดยรวมผ่านการฝึกอบรม การฝึกซ้อม และการทบทวน เพื่อให้มั่นใจว่าแผนความต่อเนื่องทาง ธุรกิจยังคงเป็นปัจจุบัน และทันสมัย

International Organization for Standardization (ISO) ซึ่ง เป็นองค์กรระหว่างประเทศที่รับผิดชอบในการจัดทำและเผยแพร่มาตรฐานสากลในด้านต่าง ๆ ได้มีการจัดทำมาตรฐานสากลเกี่ยวกับ ระบบบริหารความต่อเนื่องทางธุรกิจ เรียกว่า มาตรฐาน ISO 22301 ซึ่งประกาศใช้ เมื่อวันที่ 15 พฤษภาคม พ.ศ. 2555 เพื่อใช้เป็นแนวทางในการพัฒนา ระบบการบริหารความต่อเนื่องทางธุรกิจขององค์กรต่าง ๆ รวมถึง ใช้เป็นเกณฑ์ในการตรวจประเมิน เพื่อให้

การรองรับมาตรฐานดังกล่าว นอกเหนือจากมาตรฐาน ISO 22301 แล้ว ก่อนหน้านี้ได้มีมาตรฐานสากลที่เกี่ยวกับระบบบริหารความต่อเนื่องทางธุรกิจอีกหลายมาตรฐาน อาทิเช่น BS 25999 ของอังกฤษ หรือ AS 5050 ของออสเตรเลีย รวมถึงมาตรฐาน ISO อื่น ๆ ที่เกี่ยวกับการบริหาร ความต่อเนื่องทางธุรกิจ ทั้งที่ประกาศใช้แล้ว เช่น

- ISO 22320 (Societal Security – Emergency Management – Requirements for Incident Response)
- ISO/PAS 22399 (Societal Security – Guideline for Incident Preparedness and Operational Continuity Management)
- ISO/IEC 27031 (Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity)
- ISO/IEC 24762 (Information Technology – Security Techniques – Guidelines for Information and Communications Technology Disaster Recovery Services)
- ISO 22313 (Societal Security – Business Continuity Management Systems – Guidance)
- ISO 22390 (Societal Security – Guidelines for Execeises and Testing)

มาตรฐาน ISO 22301 มีการนำแนวทาง PDCA (Plan – Do – Check – Act) มาใช้ในการวางแผน การจัดทำ การนำไปใช้งาน การปฏิบัติการ การเฝ้าติดตาม การทบทวน การดูแลรักษา และการปรับปรุงประสิทธิผลอย่างต่อเนื่องกับระบบบริหารความต่อเนื่องทางธุรกิจขององค์การ ดังแสดงในภาพประกอบที่ 2.10 ที่แสดงให้เห็นถึงระบบบริหารความต่อเนื่องทางธุรกิจ (BCMs) จะมีการนำความต้องการด้านความต่อเนื่องทางธุรกิจจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง และผ่านการดำเนินการ รวมถึงกระบวนการที่จำเป็น เพื่อให้ได้ผลลัพธ์ออกมาเป็นความต่อเนื่องทางธุรกิจสอดคล้องตามความต้องการ



ภาพประกอบที่ 2.10 รูปแบบ PDCA ที่นำมาประยุกต์ใช้กับกระบวนการของระบบการบริหารความต่อเนื่องทางธุรกิจ

ที่มา: ประกาศกระทรวงอุตสาหกรรม ฉบับที่ 4563 (พ.ศ. 2556)

แนวทางของ PDCA ในระบบบริหารความต่อเนื่องทางธุรกิจ จะประกอบด้วย

1. **การวางแผน (Plan)** ประกอบด้วย การจัดทำนโยบายความต่อเนื่องทางธุรกิจ รวมถึงวัตถุประสงค์ เป้าหมาย การควบคุม กระบวนการ และขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการปรับปรุง ความต่อเนื่องทางธุรกิจ เพื่อให้ได้ผลลัพธ์ที่สอดคล้องกับนโยบายและวัตถุประสงค์โดยรวมขององค์กร

2. **การดำเนินการ (Do)** ประกอบด้วย การนำไปดำเนินการและการปฏิบัติการตามนโยบาย การควบคุมกระบวนการ และขั้นตอนการปฏิบัติงานด้านความต่อเนื่องทางธุรกิจตามที่ได้วางแผนไว้

3. **การเฝ้าติดตามและทบทวน (Check)** ประกอบด้วย การเฝ้าติดตาม และการทบทวนผลการดำเนินงาน เทียบกับนโยบายและวัตถุประสงค์ด้านความต่อเนื่องทางธุรกิจ การรายงานผลลัพธ์ เพื่อนำไปทบทวนโดยฝ่ายบริหาร

4. การดูแลรักษาและปรับปรุง (Act) ประกอบด้วย การดูแลรักษา และการปรับปรุงระบบบริหารความต่อเนื่องทางธุรกิจ โดยการปฏิบัติการแก้ไขจากผลลัพธ์ของการทบทวนโดยฝ่ายบริหาร และการประเมินขอบเขตของระบบ รวมถึงนโยบายและวัตถุประสงค์ทางธุรกิจ

5. ความเป็นส่วนบุคคล (Privacy)

โดยที่ปัจจุบันเทคโนโลยีมีความเจริญก้าวหน้าเป็นอย่างมากและได้ถูกนำมาใช้งานอย่างแพร่หลาย โดยมีเครือข่ายสื่อสารอินเตอร์เน็ตเป็นส่วนสำคัญในสังคมชีวิตประจำวันของมนุษย์ ทั้งนี้ไม่ว่าจะเพื่อใช้ในการติดต่อสื่อสาร การทำธุรกรรม การค้นคว้าหาข้อมูลหรือความรู้ การซื้อขายสินค้าหรือบริการ ซึ่งการทำรายการหรือธุรกรรมทั้งหลายบนโลกอินเทอร์เน็ต มักจะมีการเก็บข้อมูลส่วนบุคคลของผู้ที่เข้าใช้งาน โดยที่บุคคลผู้เข้าใช้งานไม่รู้ตัว ซึ่งข้อมูลดังกล่าวอาจมีผลกระทบต่อสิทธิในความเป็นอยู่ส่วนตัวของเจ้าของข้อมูลได้ หรือในบางกรณีที่มีการจัดเก็บข้อมูลส่วนบุคคลในรูปแบบของข้อมูลอิเล็กทรอนิกส์ จึงทำให้ข้อมูลเหล่านี้สามารถถ่ายโอนกันได้โดยสะดวก รวดเร็ว และปัจจุบันพบว่ามีการล่วงละเมิดสิทธิของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อนรำคาญหรืออเสียหายแก่เจ้าของข้อมูล ดังนั้นจึงได้มีความพยายามในการหาทางแก้ไขปัญหาข้างต้น โดยการกำหนดกฎเกณฑ์ กลไกหรือมาตรการกำกับดูแล เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

ความเป็นส่วนบุคคล (Privacy) เริ่มเป็นประเด็นร้อนที่หลาย ๆ คนสนใจ โดยเฉพาะอย่างยิ่งเมื่อเกิดเหตุการณ์ Data Breach และข้อมูลส่วนบุคคล (Data Privacy) ของตนเองถูกขโมยไปใช้ในทางที่ผิด ส่งผลให้ประเทศที่พัฒนาแล้วหลายแห่งมีการออกกฎหมายเพื่อคุ้มครองข้อมูลของผู้บริโภค โดยในปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย ซึ่งอาจต้องมีการรวบรวมจัดเก็บ ใช้หรือเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนตัว (Privacy Right) ของประชาชนที่ต้องได้รับการคุ้มครองอันจะทำให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์

ความหมายของข้อมูลส่วนบุคคล (Data Privacy)

โดยในปัจจุบันประเทศไทยได้มีการพูดถึงข้อมูลส่วนบุคคลอันเป็นสิทธิมนุษยชนขั้นพื้นฐานอย่างกว้างขวาง โดยผู้วิจัยได้ทำการรวบรวมความหมายของคำว่าข้อมูลส่วนบุคคล ที่ได้ให้ความหมายไว้ดังต่อไปนี้

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ได้กล่าวถึงไว้ในมาตรา 4 ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพและความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง และในมาตรา 35 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลาย ซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่ กรณีที่เป็นประโยชน์ต่อสาธารณะ บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตนทั้งนี้ตามกฎหมายบัญญัติ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้ความหมายของ “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรมบรรดาที่มีชื่อของบุคคลนั้นหรือมีหมายเลขรหัส หรือสิ่งอื่นที่ทำให้รู้ตัวบุคคลนั้น เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่ายและให้หมายรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

Samuel D. Warren และ Louis D. Brandeis (1890) ได้อธิบายถึงความเป็นส่วนตัว หมายถึง “สิทธิที่จะอยู่โดยลำพัง” (the right to be let alone) “ความเป็นส่วนตัว (Privacy)” เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ที่สังคมยุคใหม่ เกือบทุกประเทศให้ความสำคัญอย่างมาก ดังจะเห็นได้จากการรับรองหลักการดังกล่าวไว้ในรัฐธรรมนูญ หรือแม้บางประเทศจะไม่ได้บัญญัติรับรองไว้โดยตรงในรัฐธรรมนูญ แต่ก็ได้ตราบทบัญญัติรับรองไว้ในกฎหมาย เฉพาะ “ความเป็นส่วนตัว” ได้รวมถึงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นการตีความคำว่า “ความเป็นส่วนตัว” ในด้านการจัดการข้อมูลส่วนบุคคล ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) เป็นการให้ ความคุ้มครองข้อมูลส่วนบุคคล โดยการวางหลักเกณฑ์ เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล

นคร เสรีรักษ์ (2558) ได้ให้ความหมายของ ข้อมูลส่วนบุคคลว่าหมายถึง สิทธิในชีวิตและร่างกาย “เรื่องส่วนตัว” รัฐและบุคคลทั่วไปต้องเคารพและไม่ แทรกแซงและเป็นสิ่งบ่งชี้ศักดิ์ศรีความเป็นมนุษย์ สิทธิที่จะดำรงชีวิต กำหนดวิถีชีวิตของตัวเอง ความเป็นมนุษย์เป็นองค์รวมของข้อมูลส่วนบุคคลอีกมากมาย

การคุ้มครองข้อมูลส่วนบุคคลตามหลักสากล

1. การคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ ปัจจุบันได้มีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสาร มาประยุกต์ใช้ในการประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย เช่น การรวบรวม จัดเก็บ ใช้หรือเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานสำคัญในความเป็นส่วนตัวของประชาชนที่ต้องได้รับการคุ้มครองอันจะทำให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีกรอบในการคุ้มครองข้อมูลส่วนบุคคลที่นิยมในระดับสากลที่ถูกนำมาอ้างอิงเป็นแนวทางในการดำเนินการต่าง ๆ และประเทศไทยได้นำมาใช้เป็นแนวทางในการคุ้มครอง ข้อมูลส่วนบุคคลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ที่ต้องได้รับการคุ้มครองที่ เหมาะสมในทุกขั้นตอน ตั้งแต่ขั้นตอนการรวบรวม การเก็บรักษา และการเปิดเผย ข้อมูลส่วนบุคคล คือ กรอบในการคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (OECD: The Organization for Economic Cooperation and Development) ในเรื่อง Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data

2. การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของสหภาพยุโรป ว่าด้วยมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล ตามกฎหมายของสหภาพยุโรปว่าด้วยมาตรการคุ้มครองความเป็น ส่วนตัวของข้อมูลส่วนบุคคล “General Data Protection Regulation” หรือที่ เรียกว่า GDPR ซึ่งมีผลบังคับใช้วันที่ 25 พฤษภาคม พ.ศ. 2561 จึงอาจส่งผลกระทบต่อหน่วยงานต่าง ๆ ไม่ว่าภาครัฐ ภาคเอกชน หรือภาคธุรกิจที่มีการดำเนินการเกี่ยวกับการเก็บข้อมูลส่วนบุคคล หรือการให้บริการออนไลน์แก่บุคคลที่อยู่ในสหภาพยุโรป ดังนั้นการเตรียมความพร้อมและทำความเข้าใจกฎหมาย GDPR จึงมีความจำเป็นเพื่อส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจให้เทียบเท่ากับมาตรฐานสากลและป้องกันผลกระทบจากกฎหมายที่อาจเกิดขึ้น

หลักการสำคัญของ GDPR มีดังต่อไป

1. ข้อมูลส่วนบุคคล (Personal Data) ตามนิยามของ GDPR คือข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม รวมถึงข้อมูลที่นำมารวมกันแล้ว สามารถใช้ระบุอัตลักษณ์ของบุคคลได้ ตัวอย่างข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุล ที่อยู่ หมายเลขบัตรประจำตัว หมายเลข ID เพื่อใช้ในการโฆษณาในโทรศัพท์เคลื่อนที่ เวชระเบียน และข้อมูลสุขภาพอื่น ๆ ซึ่งสามารถใช้ระบุอัตลักษณ์ของผู้ป่วยได้ พฤติกรรมการบริโภคสินค้าหรือบริการ เป็นต้น

2. บทบาทของผู้เกี่ยวข้องกับการประมวลผลข้อมูล GDPR ได้กำหนดบทบาทของผู้เกี่ยวข้องกับการประมวลผลข้อมูลหลักไว้ ดังต่อไปนี้

2.1 ผู้ควบคุมข้อมูลส่วนบุคคล (Controller) คือ กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ซึ่งโดยส่วนมากจะเป็นผู้ขอความยินยอมจากเจ้าของข้อมูล เช่น ผู้ให้บริการเว็บไซต์ต่าง ๆ

2.2 ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor) คือ ผู้ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์และวิธีการของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งในทางปฏิบัติอาจเป็นบุคคลเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลก็ได้ทั้งนี้การประมวลผลข้อมูลตามกฎหมาย GDPR นั้นไม่ใช่เพียงแค่การวิเคราะห์หรือจัดการข้อมูลแบบทั่วไปเท่านั้น แต่ให้รวมถึงการบันทึกและจัดเก็บข้อมูลด้วย

2.3 เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ ผู้ที่เป็นเจ้าของข้อมูลต่าง ๆ เกี่ยวกับบุคคลนั้น อันสามารถระบุตัวบุคคลได้ไม่ว่าจะทางตรง หรือทางอ้อม เช่น ชื่อ-นามสกุล ที่อยู่ อาชีพ การศึกษา เวชระเบียนและข้อมูลสุขภาพ เป็นต้น

3. ขอบเขตการบังคับใช้โดยสังเขป คือ ตามกฎหมาย GDPR ได้กำหนดให้ “การประมวลผลข้อมูล” ในลักษณะต่อไปนี้ต้องอยู่ภายใต้ขอบเขตการบังคับใช้ของกฎหมาย GDPR ดังนี้

3.1 ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูล ส่วนบุคคลมีสถานประกอบการอยู่ภายในสหภาพยุโรป

3.2 ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูล ส่วนบุคคลไม่มีสถานประกอบการอยู่ภายในสหภาพยุโรป แต่การประมวลผลนั้น เกี่ยวข้องกับการเสนอสินค้าหรือบริการให้แก่บุคคลผู้พำนักในสหภาพยุโรป

3.3 ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูล ส่วนบุคคลไม่มีสถานประกอบการอยู่ภายในสหภาพยุโรป แต่การประมวลผลนั้นเกี่ยวข้องกับการเฝ้าสังเกตพฤติกรรมที่เกิดขึ้น ในสหภาพยุโรป ทั้งนี้หากมีการประมวลผลข้อมูลส่วนบุคคลนอกอาณาเขตของสหภาพยุโรปและประเทศนั้นมีผลผูกพันทางกฎหมายกับประเทศสหภาพยุโรป เช่น สนธิสัญญา จะตกอยู่ ภายใต้ขอบเขตการบังคับใช้ของ GDPR เช่นเดียวกัน

4. หลักการขอความยินยอม (Consent) เมื่อการประมวลผลข้อมูลส่วนบุคคลตกอยู่ภายใต้ขอบเขตการบังคับใช้กฎหมาย GDPR ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักพื้นฐานในการประมวลผลข้อมูลส่วนบุคคล เช่น ต้องประมวลผลข้อมูลโดยชอบด้วยกฎหมายเป็นธรรม และโปร่งใส ต่อเจ้าของข้อมูล ซึ่งการ

ประมวลผลข้อมูลจะชอบด้วยกฎหมายหรือไม่นั้นต้องพิจารณาจาก “ความยินยอม” ซึ่งเป็นหัวใจสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย GDPR นั้น การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลจะต้องเป็นไปตามหลักเกณฑ์ทั้ง 4 ประการ ดังต่อไปนี้

4.1 เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมอย่างเสรี หมายถึง เจ้าของข้อมูล มีทางเลือกในการตัดสินใจว่า จะให้หรือไม่ให้ข้อมูลส่วนใดบ้างและการไม่ให้ความยินยอมในส่วนนั้นต้องไม่ทำให้เกิดผลเสียแก่เจ้าของข้อมูลส่วนบุคคล

4.2 มีวัตถุประสงค์ที่เฉพาะเจาะจงในการขอความยินยอม หมายถึง การประมวลผลข้อมูลต้องเป็นไปเพื่อวัตถุประสงค์ที่แจ้งแก่เจ้าของข้อมูลส่วนบุคคลเท่านั้น

4.3 แจ้งการประมวลผลข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบ หมายถึง เจ้าของข้อมูลส่วนบุคคลต้องทราบแล้วว่าจะมีการประมวลผลนั้น ๆ ก่อนให้ความยินยอม

4.4 เจ้าของข้อมูลต้องแสดงความยินยอมอย่างไม่กำกวมหรือเป็นการแสดงออกโดยชัดเจน ต้องปราศจากความลังเลสงสัยในการตีความว่า เป็นการกระทำของเจ้าของข้อมูลหรือไม่ เช่น การกดอัพโหลดภาพบัตรประจำตัวประชาชน การลงลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น

5. หลักการออกแบบ (Privacy by Design) กฎหมาย GDPR กล่าวถึงหลักการออกแบบ คือ ฝ่ายผู้ควบคุมข้อมูลต้องคำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลตั้งแต่ ขั้นออกแบบ คงไว้ตลอดกระบวนการที่ตามมา ซึ่งสามารถประยุกต์ใช้ได้ทั้งในบริบทของการพัฒนาระบบผลิตภัณฑ์ บริการ แผนธุรกิจ เป็นต้น โดยเรื่อง Privacy by Design นี้มีอยู่ในกระบวนการทางวิศวกรรมบางสาขาและปฏิบัติกันมานานพอสมควรแล้ว แต่ไม่เคยมีการบัญญัติไว้เป็นกฎหมายแน่ชัดมาก่อนจนกระทั่งกฎหมาย GDPR มีผล บังคับใช้

6. ข่าวกรองทางไซเบอร์ (Cyber Intelligence)

ในอดีตที่ผ่านมาภายใต้สภาวะที่มีสงคราม ข่าวกรองทางด้านการทหารถือได้ว่าเป็นสิ่งจำเป็นยิ่ง ความน่าเชื่อถือและกลยุทธ์การรวบรวมข่าวกรองที่มีประสิทธิภาพเป็นปัจจัยในการตัดสินใจที่สำคัญต่อผลลัพธ์ของสถานการณ์การต่อสู้ จากการถอดรหัสปริศนาที่ซับซ้อนทั้งฝ่ายตรงข้ามและฝ่ายเดียวกัน ต้องกระทำด้วยวิธีการที่เหมาะสม เนื่องด้วยการดำเนินงานที่ซ่อนเร้นของสงคราม มีผลต่อเทคนิคการรวบรวมข่าวกรอง ทักษะการเข้ารหัสและวิธีการที่ใช้ในการถอดรหัส และเมื่อเวลาผ่านไปนั้นย่อมมีการเปลี่ยนแปลงไปอย่างมาก ยิ่งในสถานการณ์ที่มีการเปลี่ยนแปลทางด้านเทคโนโลยี เพื่อให้สอดคล้องกับสภาพที่เป็นอยู่และการเปลี่ยนแปลงไปทางด้านเทคโนโลยี จึงเป็นผลทำให้วิธีการติดตามวิเคราะห์และตอบโต้ภัยคุกคามความปลอดภัยทางดิจิทัลได้มีการพัฒนาขึ้นไปอย่างมากเช่นกัน

ในปัจจุบันไฟล์ข้อมูลได้มีการเข้ารหัสไว้อย่างซับซ้อน ซึ่งได้เข้ามาแทนที่ข้อความวิทยุ (Radio Message) ที่เข้ารหัส และยิ่งไปกว่านั้น เรื่องที่ยากยิ่งกว่าที่จะทำลายมาตรการรักษาความปลอดภัยที่ซับซ้อนต่อสิ่งที่เป็นอยู่ อย่างไรก็ตามแม้ว่าเทคโนโลยีขั้นสูงเหล่านี้ที่เข้ามา ซึ่งมีผลที่จะช่วยให้เกิดข้อผิดพลาดของมนุษย์ให้น้อยที่สุด แต่ในความเป็นจริงแล้วข้อผิดพลาดเหล่านั้นยังคงมีอยู่ ข้อผิดพลาดประการแรกอาจจะเกิดขึ้นแล้ว สำหรับหลาย ๆ คน คือการที่ไม่เข้าใจระดับและขนาดของภัยคุกคามที่อาจเกิดขึ้นนั้น ด้วยความล้มเหลวที่จะเข้าใจหรือตีความ ถึงความหมายของอาชญากรรมไซเบอร์และรูปแบบของการกระทำอย่างใกล้ชิด ความผิดพลาดประการที่ 2 คือความล้มเหลวในการตรวจสอบความปลอดภัยของข้อมูลในสื่อทุกประเภท ในสมัยก่อนเมื่อเกิดสงครามขึ้น ทุกคนก็จะพูดกันอยู่ในประเด็นที่ว่าจะทำอย่างไรให้สามารถอยู่รอดได้ภายใต้สภาวะสงคราม (Areless Talk Costs Lives) แต่ในปัจจุบันคำพูดเหล่าเปลี่ยนไป โดยจะมองถึงความปลอดภัยที่จะเกิดต่อธุรกิจตามมานั่นเอง (Careless Security Costs Business)

ภายใต้สภาพแวดล้อมที่เต็มไปด้วยดิจิทัลในปัจจุบัน ความปลอดภัยในเรื่องข้อมูลเป็นสิ่งที่ต้องตระหนักถึงเป็นอย่างมาก การหาแนวทางในการป้องกันต่อจุดอ่อนที่จะก่อให้เกิดช่องโหว่ในระบบได้นั้น ย่อมจะเป็นผลดีต่อการดำเนินการ และหนึ่งในวิธีการดังกล่าว คือ แนวทางในการหาข่าวกรองทางไซเบอร์ (Cyber Intelligence) ไม่ว่าระบบความปลอดภัยที่มีอยู่จะครอบคลุมแค่ไหน ความสามารถในการรักษาความปลอดภัยจะมีมากแค่ไหน สิ่งเหล่านี้ควรจะได้รับการป้องกันที่ดีขึ้นด้วยกลยุทธ์ที่เหมาะสม

ความหมายของข่าวกรองทางไซเบอร์ (Cyber Intelligence)

ข่าวกรอง (Intelligence) คือ ข่าวสารต่าง ๆ ที่มีความสำคัญด้านใดด้านหนึ่ง เช่น ความมั่นคง การเมือง ธุรกิจ ฯลฯ โดยมีการสืบค้น ตรวจสอบ วิเคราะห์ และพิสูจน์ว่าเป็นข่าวที่น่าเชื่อถือ เพื่อการปฏิบัติงานที่เกี่ยวข้อง โดยที่กระบวนการหาข่าวกรอง จะประกอบด้วย 1) การวางแผนและอำนวยการ 2) การสืบค้น รวบรวม และสอบถามจากแหล่งต่าง ๆ ซึ่งอาจจะเป็นความลับ 3) การวิเคราะห์ ตรวจสอบ และพิสูจน์ และ 4) การจัดทำรายงานและส่งให้ผู้เกี่ยวข้อง

ข่าวกรองทางไซเบอร์ (Cyber Intelligence) โดยคำนิยามของข่าวกรองทางไซเบอร์ ที่กระทรวงกลาโหมของสหรัฐอเมริกา ได้นิยามไว้ซึ่งมีความหมายดังต่อไปนี้

1. ผลผลิตที่เกิดมาจาก การรวบรวม การประมวลผล การบูรณาการ การประเมินผล การวิเคราะห์และการตีความข้อมูลที่พร้อมใช้งานซึ่งเป็นประเด็นเกี่ยวข้องกับต่างประเทศ กองกำลังของฝ่ายที่ไม่เป็นมิตรที่มีศักยภาพ หรือเป็นองค์ประกอบหรือพื้นที่ของการดำเนินงานจริงหรือที่อาจเกิดขึ้น

2. กิจกรรมที่ก่อให้เกิดผลดังกล่าว

3. องค์กรที่มีส่วนร่วมในกิจกรรมดังกล่าว

ถ้าพิจารณาในมุมมองทางด้านธุรกิจ สิ่งเหล่านี้สามารถแปลเป็นวิธีการที่องค์กรและบริษัท สามารถลดภัยคุกคามที่อาจมาจากผู้ไม่หวังดี ผ่านการรวบรวมข้อมูลและนำเอาข้อมูลที่ได้ซึ่งมีความเกี่ยวข้องกับความปลอดภัยไปใช้เพื่อการพัฒนาและใช้กลยุทธ์เพื่อปกป้องการดำเนินงานของสินทรัพย์ขององค์กรและบริษัท

ประเภทของข่าวกรอง

ได้มีการแบ่งประเภทของข่าวกรองไว้อย่างหลากหลาย โดยเฉพาะในกระบวนการทางธุรกิจที่ได้มีการประยุกต์ใช้ข่าวกรองทางไซเบอร์มาใช้งาน ดังตัวอย่างเช่น

1. HUMINT (Human Intelligence) คือ การส่งบุคคลลงพื้นที่เข้าไปหาข่าว เมื่อได้ข้อมูลดิบมา จะมีกระบวนการเพื่อให้ได้มาซึ่งข่าวกรองที่มีความน่าเชื่อถือมากขึ้น

2. OSINT (Open Source Intelligence) เป็นการนำเอา Cyber Intelligence มาใช้ในงานด้านการตลาด ที่ใช้กวาดข้อมูลในโลกออนไลน์จากแหล่งข้อมูลเปิดทั้งหลาย เช่น website, forums, social media ที่เปิด public และอื่นๆ แล้วนำมาประมวลผลเพื่อประโยชน์ในการทำ Brand monitoring เช่น ต้องการทราบว่าในขณะนี้โลกโซเชียลชอบสินค้าของบริษัทมากขนาดไหน เป็นต้น

นอกจากนี้ยังมีการแบ่งประเภทของข่าวกรองทางไซเบอร์ที่นำมาใช้ในงานด้านการทหาร ตัวอย่างเช่น

1. SIGINT (Signals Intelligence) คือ การใช้อุปกรณ์ดักรับดักฟังการสื่อสาร การตัดการสื่อสาร การแปลงข่าวสารให้มีข้อความที่เปลี่ยนไป ซึ่ง SIGINT ยังแบ่งออกได้เป็น 2 ชนิดย่อย ๆ คือ COMINT และ ELINT

2. GEOINT (Geospatial Intelligence) คือข่าวกรองทางด้านภูมิสารสนเทศ เป็นการนำเอาภาพถ่ายที่ได้จากถ่ายภาพบนเครื่องบินนำมาใช้สำหรับงานด้านการทหารเพื่อทราบลักษณะภูมิประเทศ

ในขณะที่แนวคิดด้านข่าวกรองทางไซเบอร์จะเกี่ยวข้องกับการตอบโต้และมาตรการทางการทหารที่ใช้โดยหน่วยงานของรัฐ แต่ในปัจจุบันนี้ได้มีการนำเอาแนวคิดนี้มาใช้เพื่อเพิ่มความสามารถในเรียนรู้และกำหนดองค์ความรู้เกี่ยวกับการทำธุรกิจ ยกตัวอย่างเช่น GEOINT มีแอปพลิเคชั่นในโลกของการเฝ้าระวังองค์กรและการรวบรวมหลักฐาน

รวมทั้งจัดหาความสามารถในการผูกกิจกรรมที่สงสัยว่ามีการฉ้อโกงให้กับสถานที่และเวลาที่สนับสนุนโดยหลักฐานภาพถ่าย ข้อมูลจะถูกรวบรวมด้วยวิธีการที่ได้มีการกำหนดกลยุทธ์ตามที่กำหนดไว้

เมื่อเวลาผ่านไปการสื่อสารทางโลกไซเบอร์เริ่มมีการแพร่หลายมากขึ้น มีข้อมูลที่ถูกส่งผ่านการสื่อสารในโลกไซเบอร์มากขึ้น ทั้งบนดินและใต้ดิน การสื่อสารของกลุ่มอาชญากร แฮกเกอร์ รวมทั้งผู้ก่อการร้ายก็มีมากขึ้น ยกตัวอย่างเช่น ISIS ใช้ Telegram ในการสื่อสารและสร้างสาวก ในมุมของหน่วยงานด้านความมั่นคง จึงมีความจำเป็นที่จะต้องสามารถหาข่าวจากโลกไซเบอร์เพื่อใช้ในการเตรียมตัวรับมือ ตัวอย่างที่ชัดเจนเช่น หากเรารู้ว่าผู้ก่อการร้ายใช้ช่องทางไซเบอร์ในการคุยกัน และเราสามารถได้ข่าวมาจากในนั้น เราคงสามารถหยุดการก่อการร้ายที่ลอนดอนได้ก่อนที่เหตุจะเกิด

กระบวนการข่าวกรองทางไซเบอร์

กระบวนการในการพัฒนากลยุทธ์ข่าวกรองทางไซเบอร์ที่มีประสิทธิภาพนั้นขึ้นอยู่กับขั้นตอนที่กล่าวไว้ข้างต้นว่า “ส่งผลให้เกิดผลผลิต” ซึ่งเป็น“ การรวบรวม การประมวลผล การบูรณาการ การประเมินผล การวิเคราะห์และการตีความ” จากข้อมูลที่เกี่ยวข้อง โดยพื้นฐานแล้วขั้นตอนเหล่านี้แสดงถึงวงจรของกระบวนการข่าวกรองทางไซเบอร์ โดยกระบวนการนั้นสามารถนำมาใช้เพื่อวัตถุประสงคค์ของการใช้ข่าวกรอง ที่นำไปใช้กับธุรกิจซึ่งสามารถดำเนินการได้ตามขั้นตอนดังต่อไปนี้

1. การวางแผนด้านข่าวกรอง (Intelligence planning)

ส่วนสำคัญของขั้นตอนนี้คือ การประเมินภัยคุกคาม ต้องสามารถระบุให้ได้ถึงจุดอ่อนของธุรกิจว่าอยู่ที่ใด และมีภัยคุกคามประเภทใดบ้างที่กำลังเผชิญ อาจเป็นการนำแนวทางบางอย่างง่าย ๆ เช่นเดียวกับการโจมตีมัลแวร์ผ่านอีเมล (E-mail phishing) การทำความเข้าใจสิ่งนี้เป็นสิ่งสำคัญในการกำหนดเป้าหมายและวัตถุประสงค์สำหรับการดำเนินงานข่าวกรองไซเบอร์ขององค์กร รวมไปถึงมาตรการตอบโต้ที่จะนำมาใช้

2. การรวบรวมข่าวกรอง (Intelligence collection)

ในขั้นตอนนี้จะเป็นการค้นหาหลักฐานในการโจมตี รูปแบบโจมตี รวมไปถึงแหล่งข้อมูลที่อาจจะถูกบันทึกไว้บนเซิร์ฟเวอร์หรือการถอดเสียงอีเมล วิธีการที่ซับซ้อนมากขึ้นอาจรวมถึงโปรแกรมการเฝ้าระวังพนักงานหรือซัพพลายเออร์ที่มีมากขึ้น ขอบเขตที่องค์กรอาชญากรรมที่ลักลอบนำเอาผลผลิตไปผลิตเป็นสินค้าลอกเลียนแบบ ดังนั้นบริษัทจึงต้องมีวิธีการในการเปิดเผย เฝ้าระวังและการรวบรวมข่าวกรอง

3. กระบวนการด้านข่างกรอง (Intelligence processing)

ข้อมูลที่รวบรวมจะมีหลายรูปแบบ จำเป็นต้องมี “มนุษย์” เพื่อให้เกิดกระบวนการในการประมวลผลวิเคราะห์และตีความ การบันทึกของเซิร์ฟเวอร์ต้องมีข้อมูลหลายประเภทตั้งแต่ผู้ใช้ไปจนถึงประเภทของ "ผู้ใช้งาน" ที่เข้าถึงระบบ การแยกข้อมูลที่เกี่ยวข้องมีความสำคัญต่อการประมวลผลข้อมูลอย่างมีประสิทธิภาพ

4. การส่งมอบ (Distribution)

กระบวนการง่ายๆในการเผยแพร่ข้อมูลที่เกี่ยวข้องและต่อมาทำให้แน่ใจว่าผู้ที่จำเป็นต้องรู้

5. การทบทวน (Review)

บางครั้งมันเป็นไปไม่ได้ที่จะสร้างความพึงพอใจให้กับผู้มีส่วนได้ส่วนเสียทั้งหมดที่เกี่ยวข้องกับการดำเนินงานที่ปลอดภัยของธุรกิจ ดังนั้นจึงเป็นเรื่องสำคัญที่จะต้องตรวจสอบให้แน่ใจว่า “ผลผลิต” ที่คุณส่งมอบตรงกับความต้องการของผู้บริโภค

7. ความยั่งยืนของโซ่อุปทาน (Supply Chain Sustainability)

แนวคิดการสร้างความยั่งยืนขององค์กร (Corporate Sustainability) เป็นกระบวนทัศน์ที่สำคัญยิ่งในการบริหารจัดการองค์กรธุรกิจสมัยใหม่ แนวคิดนี้เสนอว่า การเติบโตและผลกำไร (Corporate Growth and Profitability) ขององค์กรเป็นสิ่งสำคัญ แต่ขณะเดียวกันหากจะให้ธุรกิจดำเนินไปอย่างยั่งยืน ธุรกิจจำเป็นต้องมีเป้าหมายเชิงสังคมที่เกี่ยวข้องกับการพัฒนาอย่างยั่งยืนด้วย (Sustainable Development) เป้าหมายดังกล่าว เช่น การปกป้องสิ่งแวดล้อม การสร้างความเสมอภาคและความเป็นธรรมทางสังคม การพัฒนาเศรษฐกิจที่ส่งเสริมการกระจายรายได้ เป็นต้น กล่าวอีกนัยหนึ่ง กิจกรรมทางเศรษฐกิจของธุรกิจนั้นสามารถตอบสนองความต้องการของคนรุ่นปัจจุบัน แต่ขณะเดียวกัน ก็ต้องไม่ส่งผลร้ายต่อชีวิตความเป็นอยู่ของคนรุ่นต่อไป กิจกรรมของธุรกิจนั้นคำนึงถึงการกระจายผลประโยชน์แก่คนในสังคมอย่างเสมอภาคกัน (Fairness) กิจกรรมของธุรกิจนั้นต้องมีส่วนส่งเสริมสภาวะความเป็นอยู่ที่ดี (Wellbeing) ของคนในสังคม และยกระดับคุณภาพชีวิตของคนในสังคมไม่ทางตรงก็ทางอ้อม

หากกล่าวเจาะจงถึงกลุ่มคนในสังคมที่ธุรกิจควรมีส่วนร่วมรับผิดชอบโดยตรง คนกลุ่มนี้ได้แก่ ผู้มีส่วนได้ส่วนเสียกลุ่มต่าง ๆ (Stakeholders) ยิ่งธุรกิจสามารถสร้างความสัมพันธ์ที่ดีกับกลุ่มผู้มีส่วนได้ส่วนเสียผ่านการสร้างความเชื่อถือไว้ใจ ความเคารพซึ่งกันและกัน และการมีส่วนร่วม ได้มากเท่าใด ธุรกิจนั้นก็จะยิ่งได้รับการยอมรับจากสังคมและจะสามารถดำเนินไปได้อย่างต่อเนื่องมากยิ่งขึ้น ผู้มีส่วนได้เสียเหล่านี้คือผู้ที่สามารถสร้างผลกระทบโดยตรงต่อธุรกิจ หรือผู้ที่รับผลกระทบโดยตรงจากธุรกิจนั้น ซึ่งครอบคลุมไม่เพียงแต่ผู้ถือหุ้น แต่

รวมถึงพนักงาน ลูกค้า คู่ค้าต่าง ๆ รวมตลอดจนถึง ชุมชนที่อยู่แวดล้อมที่ตั้งของธุรกิจนั้น ผู้มีส่วนได้ส่วนเสียแต่ละกลุ่มอาจจะมีเป้าหมาย ความต้องการ ที่แตกต่างกัน ตัวอย่างเช่น ผู้ถือหุ้นและผู้ลงทุนจะสนใจที่ผลตอบแทนจากสิ่งที่ลงทุนไปกับธุรกิจ พนักงานย่อมต้องการการทำงานที่ให้โอกาสก้าวหน้าในการทำงาน ผลตอบแทนที่เป็นธรรม และความมั่นคงในงาน ส่วนลูกค้าหรือผู้บริโภคก็ต้องการได้สินค้าหรือบริการที่มีคุณภาพในราคาที่เป็นธรรมและเหมาะสม ขณะที่ชุมชนไม่เพียงต้องการธุรกิจที่สร้างงานสร้างรายได้ให้ชุมชน แต่ยังต้องการธุรกิจที่รับผิดชอบต่อชุมชนไม่สร้างมลภาวะหรือก่อผลกระทบเชิงลบต่อชีวิตความเป็นอยู่ของชุมชน หลายธุรกิจได้พยายามสร้างการมีส่วนร่วมกับชุมชน (Engagement) และทำให้ชุมชนมีส่วนร่วมในกิจกรรมต่าง ๆ ที่ธุรกิจนั้นจัดขึ้น

อย่างไรก็ดี แม้ความต้องการของแต่ละกลุ่มผู้มีส่วนได้ส่วนเสียจะแตกต่างกัน แต่ก็เป็นที่ยอมรับกันว่า แต่ละกลุ่มต่างมีความต้องการพื้นฐานร่วมกันในแง่ของความต้องการด้านการปกป้องรักษาสิ่งแวดล้อม การเติบโตของธุรกิจความคู่ไปกับการเพิ่มโอกาสในการทำงานและการส่งเสริมการกระจายรายได้ รวมทั้งการสร้างความเสมอภาคและความเป็นธรรมทางสังคมธุรกิจใดที่ละเมิดเป้าหมายเหล่านี้มักจะประสบปัญหาถูกต่อต้านจากผู้มีส่วนได้ส่วนเสีย เป็นเหตุให้ไม่สามารถดำเนินกิจการได้อย่างราบรื่นและต่อเนื่อง ในทางตรงกันข้าม ธุรกิจที่สามารถตอบสนองความต้องการพื้นฐานของผู้มีส่วนได้ส่วนเสียที่กล่าวไปข้างต้น และสามารถตอบสนองความต้องการเฉพาะของผู้มีส่วนได้ส่วนเสียรายกลุ่มอย่างเจาะจงได้ จะช่วยรักษาและเพิ่มพูนสัมพันธภาพอันดีระหว่างธุรกิจและผู้มีส่วนได้ส่วนเสียกลุ่มต่าง ๆ ทำให้ธุรกิจนั้นไม่เพียงแต่บรรลุเป้าหมายของธุรกิจ แต่ยังช่วยให้ธุรกิจสามารถดำเนินการไปอย่างต่อเนื่องและยั่งยืนได้

การวัดความสำเร็จของธุรกิจในกระบวนทัศน์ใหม่นี้จะมีความหมายที่กว้างไกลกว่าเพียงผลสำเร็จทางธุรกิจในแง่ของรายได้และผลกำไร แต่จะรวมถึงตัวชี้วัดอื่น ๆ ที่สะท้อนความยั่งยืนของธุรกิจเข้าไปด้วย อาทิ ความพึงพอใจของพนักงาน อัตราการลาออกของพนักงาน ความพึงพอใจของคู่ค้า ความพึงพอใจของชุมชน สัดส่วนของการสนับสนุนชุมชนต่อยอดขายสินค้าหรือบริการ สัดส่วนการใช้ทรัพยากรธรรมชาติต่อหน่วยของสินค้าที่ผลิตออกมา อัตราการปล่อยของเสียหรือมลพิษอันเนื่องจากการผลิตต่อการผลิตหนึ่งหน่วย เป็นต้น กระแสเรื่องของการรับผิดชอบต่อสังคม (Corporate Social Responsibility) ที่กำลังได้รับความสนใจจากธุรกิจต่าง ๆ ในประเทศไทยขณะนี้ เป็นตัวอย่างหนึ่งของกระแสการสร้างธุรกิจให้ยั่งยืน การเพิ่มจำนวนของธุรกิจที่ดำเนินกิจกรรมเพื่อสังคมในระยะ 4-5 ปีที่ผ่านมา เป็นตัวชี้ว่า แนวโน้มทิศทางของการทำธุรกิจในอนาคตจะเป็นไปในทิศทางที่ ธุรกิจจะให้ความสนใจกับความยั่งยืนขององค์กรมากขึ้นผ่านการเข้าไปมีส่วนร่วมรับผิดชอบและส่งเสริมการพัฒนาสังคม องค์กรธุรกิจใดที่

เข้าใจทิศทางนี้ และปรับตัวได้ก่อน ย่อมเป็นการวางรากฐานเพื่อความยั่งยืนขององค์กรในอนาคตได้เป็นอย่างดี

กระบวนการในการขับเคลื่อนธุรกิจสู่ความยั่งยืน จะประกอบไปด้วยกระบวนการหลัก ๆ 5 กระบวนการดังต่อไปนี้

1. การวิเคราะห์บริบทและประเด็นด้านความยั่งยืนขององค์กร (Context)

1.1 การศึกษาและทำความเข้าใจบริบทองค์กร (Context analysis) ธุรกิจจำเป็นต้องเข้าใจบริบทหรือตัวตนขององค์กรก่อนเป็นลำดับแรก โดยศึกษาและวิเคราะห์จากวิสัยทัศน์ พันธกิจ วัฒนธรรมองค์กร กลยุทธ์และแผนธุรกิจ ความเสี่ยงและโอกาสของธุรกิจ ซึ่งจะช่วยให้มองเห็นประเด็นที่องค์กรควรให้ความสำคัญและบริหารจัดการอย่างมีประสิทธิภาพ เพื่อสนับสนุนให้ธุรกิจสามารถเติบโตอย่างเข้มแข็งในระยะยาว

1.2 การระบุและวิเคราะห์ผู้มีส่วนได้เสีย พร้อมกำหนดวิธีการมีส่วนร่วม (Stakeholder engagement) ธุรกิจควรวิเคราะห์ความสัมพันธ์กับผู้มีส่วนได้เสียขององค์กรด้วยเพื่อให้สะท้อนบริบทการดำเนินงานของธุรกิจอย่างครอบคลุม โดยมีขั้นตอนดังนี้

- องค์กรควรระบุได้ว่าในการดำเนินธุรกิจตลอดห่วงโซ่คุณค่า องค์กรมีความเกี่ยวข้องกับผู้มีส่วนได้เสียทั้งในทางตรงและ / หรือทางอ้อมกลุ่มใด เช่น คณะกรรมการ พนักงาน ลูกค้า คู่ค้า ชุมชน หน่วยงานกำกับดูแล สังคม เป็นต้น
- วิเคราะห์ประเด็นที่ผู้มีส่วนได้เสียมีผลกระทบและมีความคาดหวังต่อองค์กร และประเด็นที่องค์กรมีผลกระทบและมีความคาดหวังต่อผู้มีส่วนได้เสีย ซึ่งธุรกิจควรให้ความสำคัญและดำเนินการเพิ่มผลกระทบเชิงบวกและลดผลกระทบเชิงลบ เพื่อรักษาขีดความสามารถในการแข่งขันและพัฒนาศักยภาพในการเติบโตของธุรกิจในระยะยาว
- กำหนดวิธีการมีส่วนร่วมกับผู้มีส่วนได้เสียแต่ละกลุ่ม เพื่อให้สามารถสื่อสารและจัดการประเด็นดังกล่าวได้อย่างมีประสิทธิผล ซึ่งผู้มีส่วนได้เสียแต่ละกลุ่มอาจมีช่องทางการเข้าถึงหรือรูปแบบการมีส่วนร่วมที่แตกต่างกัน

1.3 การกำหนดและจัดลำดับประเด็นสำคัญด้านความยั่งยืน (Materiality analysis) ธุรกิจควรวิเคราะห์ความสัมพันธ์กับผู้มีส่วนได้เสียขององค์กรด้วยเพื่อให้สะท้อนบริบทการดำเนินงานของธุรกิจอย่างครอบคลุม โดยมีขั้นตอนดังนี้

- คัดเลือกและกำหนดประเด็นสำคัญด้านความยั่งยืน จากประเด็นผลกระทบที่ทั้งธุรกิจและผู้มีส่วนได้เสียให้ความสำคัญ

- ประเมินระดับความรุนแรงของผลกระทบจากประเด็นด้านความยั่งยืนที่กำหนดขึ้น และจัดลำดับความสำคัญของประเด็นดังกล่าว เพื่อให้เห็นถึงความสำคัญและความจำเป็นเร่งด่วนในการบริหารจัดการประเด็นสำคัญด้านความยั่งยืนแต่ละประเด็น

เมื่อองค์กรสามารถจัดลำดับประเด็นสำคัญด้านความยั่งยืน จะช่วยให้สามารถวิเคราะห์ได้ว่าประเด็นใดเป็นประเด็นสำคัญด้านความยั่งยืนขององค์กร เพื่อนำไปสู่การพิจารณาแนวทางการบริหารจัดการแต่ละประเด็นอย่างเหมาะสมต่อไป อย่างไรก็ดี ประเด็นสำคัญด้านความยั่งยืนสามารถอาจเปลี่ยนแปลงไปหรือเปลี่ยนลำดับความสำคัญเมื่อบริบทองค์กรหรือผู้มีส่วนได้เสียเปลี่ยนไป ดังนั้นจึงควรทบทวนอย่างสม่ำเสมอ

2. การกำหนดนโยบายด้านความยั่งยืน (Policy)

2.1 การกำหนดนโยบายด้านความยั่งยืนในระดับองค์กร และกำหนดเป้าหมายในการบริหารจัดการความยั่งยืนในระดับองค์กร (Commitment) เมื่อได้ประเด็นสำคัญด้านความยั่งยืนขององค์กรแล้ว ธุรกิจควรกำหนดนโยบายและเป้าหมายด้านความยั่งยืนในระดับองค์กรออกมาเป็นลายลักษณ์อักษรและประกาศให้ผู้มีส่วนได้เสียรับทราบ เพื่อแสดงเจตนารมณ์และความมุ่งมั่นในการพัฒนาและขับเคลื่อนธุรกิจสู่ความยั่งยืน ซึ่งโดยส่วนใหญ่คณะกรรมการบริษัทหรือผู้บริหารสูงสุด จะเป็นผู้ประกาศนโยบายและเป้าหมายในระดับองค์กรเพื่อสร้างความชัดเจนกับผู้มีส่วนได้เสียทุกกลุ่มว่าองค์กรมีหลักการ กรอบความคิด ทิศทาง และเป้าหมายว่าจะดำเนินธุรกิจไปในทิศทางใด ซึ่งเป็นประโยชน์ต่อการสร้างความเข้าใจและการมีส่วนร่วมจากผู้มีส่วนได้เสีย โดยเฉพาะอย่างยิ่งพนักงานในองค์กร ให้มีแนวคิดและการดำเนินงานในทิศทางที่สอดคล้องกันกับนโยบายและเป้าหมายด้านความยั่งยืนขององค์กร

2.2 การกำหนดผู้รับผิดชอบและบทบาทหน้าที่ในการขับเคลื่อนประเด็นสำคัญด้านความยั่งยืนแต่ละประเด็น เพื่อให้เกิดการทำงานที่เชื่อมโยงกัน (Team set up) ธุรกิจควรกำหนดผู้รับผิดชอบและบทบาทหน้าที่ที่ชัดเจนในการขับเคลื่อนประเด็นสำคัญด้านความยั่งยืนแต่ละประเด็น อีกทั้งควรสื่อสารให้ผู้บริหาร พนักงานและผู้มีส่วนได้เสียที่เกี่ยวข้องได้รับทราบ เพื่อให้เกิดการทำงานที่เชื่อมโยงกันอย่างเป็นบูรณาการ เพราะการขับเคลื่อนองค์กรสู่ความยั่งยืนเป็นเรื่องที่เกี่ยวข้องกับทุกคนในองค์กร อย่างไรก็ดีการกำหนดผู้รับผิดชอบและบทบาทหน้าที่นี้ไม่มีวิธีดำเนินการแบบตายตัว ขึ้นอยู่กับโครงสร้างและบริบทของแต่ละองค์กร ซึ่งองค์กรสามารถพิจารณาได้ตามความเหมาะสม

3. การกำหนดกลยุทธ์ด้านความยั่งยืนขององค์กร (Strategy)

3.1 การกำหนดกรอบหรือกลยุทธ์ด้านการพัฒนาธุรกิจอย่างยั่งยืน (Sustainable Development Framework) ธุรกิจควรกำหนดกรอบการดำเนินงานหรือกลยุทธ์ในการพัฒนาธุรกิจอย่างยั่งยืนให้สอดคล้องกับนโยบายและนำไปสู่การบรรลุเป้าหมายในการบริหารจัดการความยั่งยืนที่กำหนด โดยทั่วไปการกำหนดกรอบการพัฒนาธุรกิจอย่างยั่งยืนขององค์กรมักเชื่อมโยงการกำกับดูแลกิจการที่ดี และการพัฒนาธุรกิจในมิติเศรษฐกิจ สังคม และสิ่งแวดล้อมเข้าไว้ด้วยกัน และสิ่งสำคัญคือควรเชื่อมโยงกรอบการดำเนินงานด้านความยั่งยืนเข้ากับความสามารถทางการเงินขององค์กร ทั้งนี้ โดยทั่วไปกรอบการพัฒนาความยั่งยืนของธุรกิจมักมองในระยะยาว จึงมักไม่เปลี่ยนแปลงทุกปี ยกเว้นในกรณีที่องค์กรมีบริบทหรือการบริหารจัดการองค์กรที่เปลี่ยนแปลงไป

3.2 การกำหนดแผนงานด้านความยั่งยืน (Sustainable Development Initiative) ธุรกิจควรกำหนดแผนปฏิบัติการหรือแผนงาน (Initiative) ด้านความยั่งยืนในระยะสั้น ระยะกลาง และระยะยาว เพื่อให้เห็นว่าธุรกิจจะดำเนินงานในแต่ละประเด็นสำคัญด้านความยั่งยืนอย่างไร ซึ่งควรสอดคล้องกับนโยบายและเป้าหมายด้านความยั่งยืนในระดับองค์กรที่กำหนด นอกจากนี้ ธุรกิจควรกำหนดเงื่อนเวลา แนวทางการดำเนินงานที่ชัดเจน และตัวชี้วัดที่สะท้อนผลการดำเนินงานได้ทั้งในเชิงผลลัพธ์แบบ output และ outcome เพื่อให้ผู้รับผิดชอบมีกรอบการทำงานที่ชัดเจน ที่สำคัญคือเพื่อสะท้อนให้เห็นถึงคุณค่าหรือมูลค่าที่ธุรกิจสามารถสร้างได้จากแผนงานด้านความยั่งยืน

4. การขับเคลื่อนความยั่งยืนไปสู่การปฏิบัติ (Implement)

4.1 เครื่องมือที่ใช้ในการขับเคลื่อนความยั่งยืนในองค์กร (PDCA) Plan, Do, Check, Act (PDCA) Cycle เป็นหนึ่งในเครื่องมือที่องค์กรสามารถนำมาใช้ในการพัฒนาและขับเคลื่อนแผนงานด้านความยั่งยืนของธุรกิจ เนื่องจากการนำแผนงานด้านความยั่งยืนไปปฏิบัติมีกระบวนการดำเนินงานไม่แตกต่างจากการนำแผนธุรกิจไปปฏิบัติ ซึ่งจำเป็นต้องมีการดำเนินงานอย่างเป็นระบบและมีการพัฒนาต่อเนื่อง โดยเริ่มต้นจากการวางแผนอย่างเหมาะสม จากนั้นจึงดำเนินการตามแผน ซึ่งควรมีการเฝ้าติดตามการดำเนินงานเป็นระยะ รวมถึงมีการตรวจสอบผลการดำเนินงาน วิเคราะห์จุดอ่อนและจุดแข็งของการดำเนินงาน และสรุปบทเรียนที่ได้หลังจบโครงการ เพื่อเพิ่มประสิทธิภาพและยกระดับการดำเนินงานได้อย่างต่อเนื่อง

5. การเปิดเผยข้อมูลด้านความยั่งยืน (Disclose)

5.1 การรวบรวมและวางระบบจัดเก็บข้อมูลด้านความยั่งยืน ธุรกิจควรมีกระบวนการจัดเก็บและรวบรวมข้อมูลผลการดำเนินงานด้านความยั่งยืน เนื่องจากการ

เปิดเผยข้อมูลถือเป็นกระบวนการที่ธุรกิจควรทำอย่างสม่ำเสมอและต่อเนื่อง พร้อมทั้งควรกำหนดผู้เกี่ยวข้องที่รับผิดชอบหรือดูแลข้อมูลแต่ละส่วนอย่างชัดเจน รวมถึงองค์กรควรมีการตรวจสอบความถูกต้องของแนวทาง วิธีการวัด และวิธีการเก็บรวบรวมข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าข้อมูลมีคุณภาพ ได้มาตรฐานและเชื่อถือได้ หรืออาจมีการสอบทานข้อมูลหรือรับรองคุณภาพของข้อมูลโดยหน่วยงานภายนอกเพิ่มเติมด้วย

5.2 การวิเคราะห์และประเมินผลข้อมูลด้านความยั่งยืน (Evaluate) เมื่อมีการจัดเก็บและรวบรวมข้อมูลผลการดำเนินงานด้านความยั่งยืนแล้ว ธุรกิจควรนำข้อมูลผลการดำเนินงานด้านความยั่งยืนที่รวบรวมไว้มาวิเคราะห์และประเมินผลการดำเนินงานโดยเปรียบเทียบกับเป้าหมายตามตัวชี้วัดที่กำหนดไว้ล่วงหน้า ซึ่งมักเป็นตัวชี้วัดในเชิงคุณภาพหรือเชิงปริมาณที่สะท้อนผลกระทบหรือผลลัพธ์ที่เกิดขึ้น เพื่อให้สามารถประเมินได้ว่าผลการดำเนินงานของบริษัทเป็นไปตามเป้าหมายหรือไม่

5.3 การรายงานผลการดำเนินงานด้านความยั่งยืนต่อผู้มีส่วนได้เสีย (Communicate) ธุรกิจควรเปิดเผยและสื่อสารผลการดำเนินงานด้านความยั่งยืนต่อผู้มีส่วนได้เสีย เพื่อสร้างความเข้าใจและการรับรู้เกี่ยวกับการดำเนินงานของบริษัท ซึ่งอาจนำไปสู่การสร้างคุณค่าและ/หรือมูลค่าให้แก่ธุรกิจได้ โดยการรายงานข้อมูลด้านความยั่งยืนให้มีความโปร่งใสและน่าเชื่อถือ บริษัทควรนำเสนอข้อมูลที่สะท้อนทั้งผลสำเร็จและความล้มเหลวของแผนงาน (ถ้ามี) โดยธุรกิจสามารถรายงานถึงความพยายามในการบริหารจัดการและดำเนินงานตามแผนงาน และยอมรับว่าอะไรคือปัจจัยที่ส่งผลกระทบให้บริษัทไม่สามารถบรรลุผลได้ตามเป้าหมายที่ตั้งไว้ เพื่อให้ผู้มีส่วนได้เสียเข้าใจและเห็นถึงผลการดำเนินงานที่แท้จริงของบริษัท

5.4 การติดตาม ทบทวน และวางแผนเพื่อพัฒนาผลการดำเนินงาน อย่างต่อเนื่อง (Review) ธุรกิจควรนำข้อมูลที่ได้จากการวิเคราะห์และประเมินผลมาติดตามทบทวนว่าอะไรเป็นจุดเด่นที่บริษัทสามารถดำเนินการได้ดี หรืออะไรเป็นข้อปรับปรุงที่บริษัทควรพัฒนาการดำเนินงานให้ดียิ่งขึ้น และวางแผนพัฒนาการดำเนินงานด้านความยั่งยืนอย่างต่อเนื่อง

8. ความน่าเชื่อถือของโซ่อุปทาน (Dependability of Supply Chain)

การป้องกันและความอยู่รอดของระบบข้อมูลที่ซับซ้อน ได้กลายเป็นปัญหาระดับชาติและระดับโลกที่ต้องจัดลำดับความสำคัญอยู่ในขั้นสูงสุด (John, 2000) และมากไปกว่านั้นบุคคลและองค์กรกำลังพัฒนาหรือจัดหาระบบคอมพิวเตอร์ที่ซับซ้อนซึ่งพวกเขาต้องการบริการที่ต้องพึ่งพาอย่างมากไม่ว่าจะเป็นให้บริการเครื่องจ่ายเงินสด ควบคุมกลุ่มดาวเทียม เครื่องบิน โรงงานนิวเคลียร์หรืออุปกรณ์การรักษาด้วยรังสีหรือเพื่อรักษาความลับของฐานข้อมูลที่

สำคัญ แตกต่างกันไปสถานการณ์โดยมุ่งเน้นที่คุณสมบัติที่แตกต่างของบริการดังกล่าว - เช่นตามเวลาจริงโดยเฉลี่ยการตอบสนองที่สำเร็จโอกาสในการสร้างผลลัพธ์ที่ต้องการความสามารถในการหลีกเลี่ยงความล้มเหลวนั้นอาจเป็นความหายนะต่อสภาพแวดล้อมของระบบหรือระดับของการบุกรุกโดยเจตนาป้องกันไม่ให้เกิด แนวคิดเรื่องความเชื่อถือได้นั้นเป็นวิธีการที่สะดวกมากในการจัดทำสิ่งต่าง ๆ เหล่านี้ความกังวลภายในกรอบแนวคิดเดียวเป้าหมายของเราคือการนำเสนอภาพรวมโดยย่อเกี่ยวกับแนวคิดเทคนิคและเครื่องมือที่มีวิวัฒนาการที่ผ่านมาสี่สิบปีในด้านการคำนวณที่เชื่อถือได้และการยอมรับข้อผิดพลาด

2.7.4.2 ส่วนที่ 2 : แนวทางการศึกษาตัวชี้วัดของกรอบความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicators)

หลักในการกำหนดตัวชี้วัดของกรอบความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ในการกำหนดตัวชี้วัดเพื่อใช้เป็นแนวทางในการบรรลุถึงระดับความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยได้ใช้หลักการทำงานของวงล้อเดมิ่ง (The Deming Cycle) หรือ วัฏจักรวางแผน-ทำ-ตรวจสอบ-ปฏิบัติ (Plan-Do-Check-Act Cycle) อ้างใน ณัฏพันธ์ เขจรนันท์ (2549) ซึ่งวงล้อเดมิ่ง จะช่วยให้ การทำงานสามารถพัฒนาคุณภาพของงานอย่างต่อเนื่องโดยพิจารณาลดหรือกำจัดกิจกรรมที่ไม่ก่อให้เกิดประโยชน์ออกจากการปฏิบัติงาน โดยแยกงานที่ไม่ก่อให้เกิดคุณค่า (No Value) ออกจากงานที่สร้างคุณค่าให้แก่ผลิตภัณฑ์หรือบริการ ซึ่งจะช่วยให้กระบวนการปฏิบัติงานมีความกระชับและพัฒนาขึ้นอย่างต่อเนื่อง โดยแนวทางสำหรับการทำงานของวงจรเดมิ่งประกอบด้วย

1. **การวางแผน (Plan)** เป็นการกำหนดแผนงานที่สามารถประเมินความก้าวหน้าของงานได้อย่างเป็นรูปธรรม

2. **การทำ (Do)** เป็นการดำเนินการตามแผนติดตาม และตรวจสอบความก้าวหน้าของกระบวนการ โดยเก็บรวบรวมข้อมูลตามระยะเวลาที่กำหนดเพื่อเป็นหลักฐานในการวิเคราะห์

3. **การตรวจสอบ (Check)** เป็นการตรวจสอบข้อมูลการดำเนินงานว่าจะสามารถบรรลุตามแผนที่กำหนดไว้หรือไม่ เพื่อพิจารณาปรับแผนหรือหยุดโครงการถ้าเกิดความไม่สอดคล้องระหว่างความเป็นจริงกับความต้องการ

4. **การปฏิบัติ (Act)** เป็นการตรวจสอบกระบวนการและจัดทำเอกสารเพื่อนำแผนงานทีที่พัฒนาจนประสบความสำเร็จ ไปเป็นแนวทางและมาตรฐานในการปฏิบัติงานต่อไป ทำให้มีการพัฒนาคุณภาพของงานอย่างต่อเนื่อง

2.8 วิสาหกิจขนาดกลางและขนาดย่อม

สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.) ได้จัดทำแผนการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม ฉบับที่ 3 พ.ศ.2555-2559 และผ่านความเห็นชอบจากคณะรัฐมนตรีเมื่อวันที่ 3 พฤษภาคม พ.ศ. 2554 แล้วนั้น ซึ่งมีการกำหนด ยุทธศาสตร์ กลยุทธ์ สำหรับให้หน่วยงานที่เกี่ยวข้องกับการส่งเสริมและพัฒนา SMEs นำไปประกอบการจัดทำยุทธศาสตร์และแผนปฏิบัติการฯที่เกี่ยวข้องกับการส่งเสริมและพัฒนา SMEs ที่เกิดจากการบูรณาการเชื่อมโยงร่วมกันระหว่างหน่วยงานต่าง ๆ โดยมีการกำหนดยุทธศาสตร์การส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม ฉบับที่ 3 พ.ศ. 2555- 2559 ดังนี้

ยุทธศาสตร์ที่ 1 สนับสนุนปัจจัยแวดล้อมให้เอื้อต่อการดำเนินธุรกิจวิสาหกิจขนาดกลางและขนาดย่อมไทย

ยุทธศาสตร์ที่ 2 เสริมสร้างขีดความสามารถในการแข่งขันของวิสาหกิจขนาดกลางและขนาดย่อมไทย

ยุทธศาสตร์ที่ 3 ส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อมไทยให้โตอย่างสมดุลตามศักยภาพของพื้นที่

ยุทธศาสตร์ที่ 4 เสริมสร้างศักยภาพของวิสาหกิจขนาดกลางและขนาดย่อมไทยให้เชื่อมโยงกับเศรษฐกิจระหว่างประเทศ

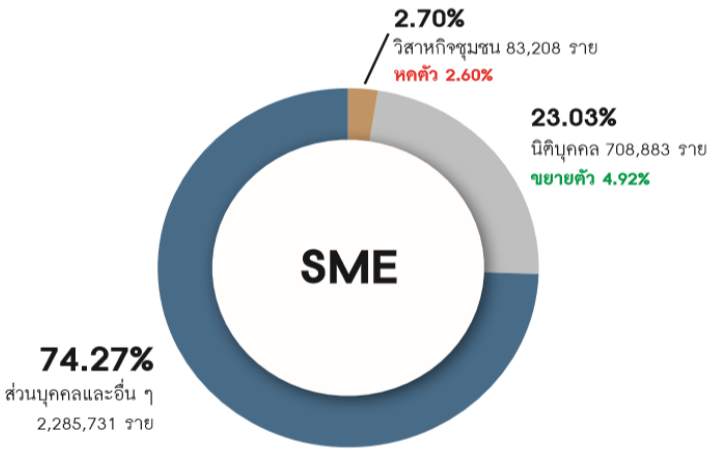
เนื่องจากวิสาหกิจ ตาม พ.ร.บ.ส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม พ.ศ. 2543 ครอบคลุมถึง กิจการผลิตสินค้า กิจการให้บริการ กิจการค้าส่ง กิจการค้าปลีก หรือกิจการอื่นตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ซึ่งในแต่ละสาขามีลักษณะการดำเนินธุรกิจ ประสบปัญหาและข้อจำกัดที่แตกต่างกัน การส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม จึงมีความจำเป็นต้องทราบสภาพปัญหาและผลกระทบในแต่ละสาขา สำหรับเป็นข้อมูลประกอบการกำหนดแนวทางการพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมให้เหมาะสม ดังนั้น เพื่อให้ทราบศักยภาพและขีดความสามารถ ของผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม ในแต่ละสาขาเพิ่มเติม รวมทั้งเพื่อให้มีแผนยุทธศาสตร์นโยบายการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อมในสาขาเป้าหมายที่สอดรับกับนโยบายของรัฐบาล แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 11 และแผนการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม ฉบับที่ 3 พ.ศ. 2555-2559 สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม จึงได้จัดทำโครงการ “การจัดทำยุทธศาสตร์และแผนปฏิบัติการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อมสาขาสารสนเทศ/ดิจิทัลคอนเท้นท์” ซึ่งจะมีส่วนสำคัญให้แผนการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม ฉบับที่ 3 พ.ศ. 2555-2559 มีความชัดเจนและบรรลุเป้าหมายที่กำหนดไว้

2.8.1 ข้อมูลจำนวนวิสาหกิจขนาดกลางและขนาดย่อม

สถิติจำนวนวิสาหกิจขนาดกลางและขนาดย่อมในปี 2561 โดยจำแนกขนาดด้วยจำนวนการจ้างงาน หรือสินทรัพย์ถาวร (ไม่รวมที่ดิน) ตามที่กำหนดในกฎกระทรวงฯ ปี 2545 สามารถแบ่งออกเป็น 3 กลุ่มตามประเภทการจัดตั้งหรือการจดทะเบียน คือ 1) สถิติจำนวนวิสาหกิจที่เป็นนิติบุคคล ซึ่งประมวลข้อมูลจากกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ 2) สถิติจำนวนวิสาหกิจที่เป็นส่วนบุคคล และอื่น ๆ (กลุ่มแม่บ้าน สหกรณ์) นั้น เป็นฐานข้อมูลที่ประมวลจากการสำมะโนธุรกิจการค้าและอุตสาหกรรม ปี 2561 โดยสำนักงานสถิติแห่งชาติ ซึ่งสำนักงานสถิติแห่งชาติจะใช้เป็นฐานข้อมูลหลัก ตั้งแต่ปี 2559 - 2563 หรือจนกว่าจะมีการสำมะโนธุรกิจครั้งใหม่ 3) สถิติจำนวนวิสาหกิจที่เป็นวิสาหกิจชุมชน ประมวลข้อมูลจากกรมส่งเสริมการเกษตร ซึ่งเป็นข้อมูลการจดทะเบียนของวิสาหกิจชุมชนทั่วประเทศ สำหรับสถิติการจ้างงานวิสาหกิจ ขนาดกลางและขนาดย่อมนั้น ได้รับข้อมูลสถิติจำนวนการจ้างงานของสำนักงานประกันสังคม

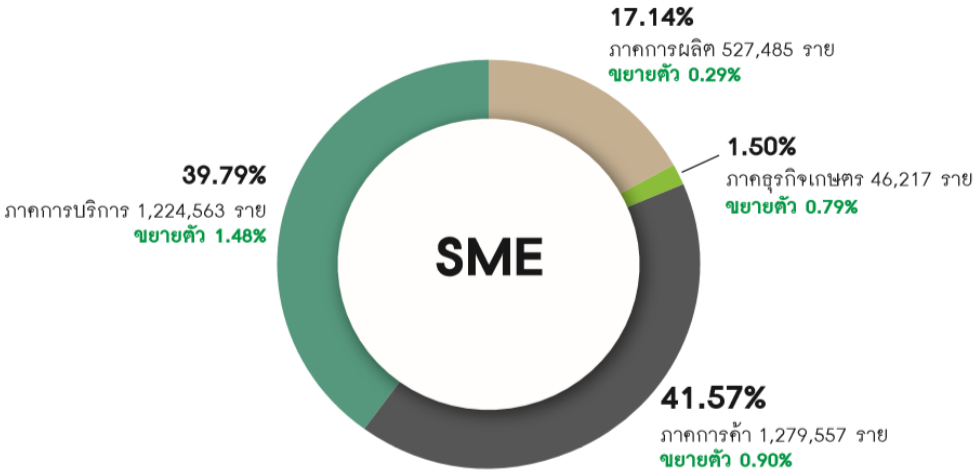
เมื่อพิจารณาตามกลุ่มธุรกิจ ที่กระจายตัวตามขนาดวิสาหกิจ ปี 2561 พบว่าวิสาหกิจขนาดกลางและขนาดย่อม (SME) มีจำนวน ทั้งสิ้น 3,077,822 ราย มีอัตราการขยายตัวร้อยละ 1.02 เมื่อเทียบกับวิสาหกิจขนาดกลางและขนาดย่อมในปีที่ผ่านมา คิดเป็นสัดส่วน ร้อยละ 99.79 ของจำนวนวิสาหกิจทั้งประเทศ โดยเป็นวิสาหกิจขนาดย่อม (SE) จำนวนทั้งสิ้น 3,063,651 ราย คิดเป็นสัดส่วนร้อยละ 99.49 ของจำนวนวิสาหกิจทั้งประเทศ เป็นวิสาหกิจขนาดกลาง จำนวน 14,171 ราย คิดเป็นสัดส่วนร้อยละ 0.32

เมื่อพิจารณาถึงจำนวน SME ที่จำแนกตามประเภทการจัดตั้งปี 2561 นั้น สามารถจำแนกได้ 3 ประเภท ได้แก่ นิติบุคคล มีจำนวน 708,883 ราย คิดเป็นสัดส่วนร้อยละ 23.03 ของจำนวน SME รวมทั้งประเทศ ส่วนบุคคลและอื่น ๆ มีจำนวน 2,285,731 ราย คิดเป็นสัดส่วน ร้อยละ 74.27 ของจำนวน SME รวมทั้งประเทศ และวิสาหกิจชุมชน มีจำนวน 83,208 ราย คิดเป็นสัดส่วนร้อยละ 2.70 ของจำนวน SME รวมทั้งประเทศ ดังภาพประกอบที่ 2.11 โดยมีรายละเอียด ดังนี้



ภาพประกอบที่ 2.11 จำนวนวิสาหกิจขนาดกลางและขนาดย่อม จำแนกตามประเภทการจัดตั้ง ปี 2561 (ที่มา : สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม)

เมื่อพิจารณาสัดส่วนภาพรวมของวิสาหกิจขนาดกลางและขนาดย่อม จำแนกตามกลุ่มธุรกิจ พบว่า อยู่ในกลุ่มภาคการค้ามากที่สุด มีจำนวนทั้งสิ้น 1,279,557 ราย คิดเป็นสัดส่วนร้อยละ 41.57 ของจำนวน SME ทั้งประเทศ รองลงมาอยู่ในภาคการบริการ มีจำนวน 1,224,563 ราย คิดเป็นสัดส่วนร้อยละ 39.79 ในภาคการผลิต มีจำนวน 527,485 ราย คิดเป็นสัดส่วนร้อยละ 17.14 และภาคธุรกิจเกษตร 46,217 ราย คิดเป็นสัดส่วนร้อยละ 1.50 โดยรายละเอียดของสัดส่วนของวิสาหกิจขนาดกลางและขนาดย่อมจำแนกตามกลุ่มธุรกิจ แสดงดังภาพประกอบที่ 2.12



ภาพประกอบที่ 2.12 จำนวนวิสาหกิจขนาดกลางและขนาดย่อม จำแนกตามกลุ่มธุรกิจ ปี 2561 (ที่มา : สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม)

2.8.2 ความสำคัญวิสาหกิจขนาดกลางและขนาดย่อม ต่อระบบเศรษฐกิจไทย

ในยุคที่ทุกชีวิตทั่วโลกได้กลายเป็นส่วนหนึ่งของ “จักรวาลดิจิทัล” ชีวิตยุคใหม่เริ่มต้นขึ้นโดยมีเครื่องคอมพิวเตอร์และอุปกรณ์มือถือต่าง ๆ ที่เชื่อมโยงเข้าสู่เครือข่ายอินเทอร์เน็ต เป็นปราการด่านแรกของการดำเนินชีวิตในทุกวัน ผู้คนจำนวนไม่น้อยได้ “สร้าง” และ “ใช้” ข้อมูลดิจิทัล (Digital Content) จำนวนมหาศาลผ่านเทคโนโลยีหลากหลาย จนทำให้การขยายตัวของข้อมูลบนเครือข่ายอินเทอร์เน็ตเติบโตขึ้นอย่างรวดเร็ว และ คงไม่มีใครปฏิเสธได้ว่าเทคโนโลยีสารสนเทศเข้ามามีบทบาทในชีวิตประจำวัน และนับวันยิ่งทวีความรุนแรงมากขึ้นเรื่อย ๆ ไม่ว่าจะเป็นการเข้าถึงข้อมูลต่าง ๆ ที่ผ่านทางอินเทอร์เน็ต ซึ่งปัจจุบันเป็นที่นิยมอย่างกว้างขวางและแพร่หลายเนื่องจากสะดวกและรวดเร็ว

ด้วยปริมาณของอุปกรณ์ดิจิทัลและแอปพลิเคชันรูปแบบใหม่ที่เพิ่มมากขึ้น จำนวนข้อมูลส่วนบุคคล (Personal Data) ที่มีการเรียกร้องให้ป้อนเข้าระบบก็ยิ่งมีปริมาณเพิ่มมากขึ้น ซึ่งสามารถนำไปสู่ปัญหาเรื่อง Privacy ได้ง่ายดาย ยิ่งกว่านั้นคือ เพื่อหลีกเลี่ยงการเกิดปัญหาดังกล่าว ซอฟต์แวร์และบริการจำนวนมากได้มีการสร้างขึ้นเพื่อปิดบังตัวตน (Anonymity) ในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเครื่องมือเหล่านี้ได้ถูกอาชญากรไซเบอร์นำมาใช้เพื่ออำพรางตัวเองด้วยเช่นเดียวกัน ดังนั้น สิ่งที่เป็นความท้าทายอย่างที่สุดในเวลานี้อย่างหนึ่งคือ เราจะสร้างสมดุลของการรักษาความเป็นส่วนตัว และการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปพร้อมกันได้อย่างไร (ศาสตราจารย์พิเศษ ดร. สุรเกียรติ์ เสถียรไทย, 2558)

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน) (SIPA) และพันธมิตรได้จัดทำตัวเลขประมาณการตลาดเทคโนโลยีสารสนเทศและการสื่อสาร ของปี พ.ศ. 2555 และจัดให้มีการสำรวจตลาดของประเทศไทยประจำปี พ.ศ. 2554 โดยตลาดเทคโนโลยีสารสนเทศและการสื่อสารที่ทำการสำรวจประกอบด้วย

1. ตลาดคอมพิวเตอร์ฮาร์ดแวร์ (Computer Hardware) ซึ่งประกอบด้วย กลุ่มซิสเท็ม (System) กลุ่มคอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) และกลุ่มอุปกรณ์ ต่อพ่วง (Peripheral)

2. ตลาดสื่อสาร (Communications) ซึ่งประกอบด้วย ตลาดอุปกรณ์สื่อสาร (Communication Equipment) และตลาดบริการสื่อสาร (Communication Service)

3. ตลาดซอฟต์แวร์ และบริการซอฟต์แวร์ ซึ่งประกอบด้วย
   3.1 Enterprise Software
   3.2 Mobile Application Software (ไม่รวมซอฟต์แวร์เกมบนโทรศัพท์เคลื่อนที่)
   3.3 Embedded System Software (ไม่รวมซอฟต์แวร์ที่อยู่ในอุปกรณ์สื่อสารขนาดเล็ก เช่น โทรศัพท์เคลื่อนที่)
   3.4 ซอฟต์แวร์กลุ่มอื่นๆ (ไม่รวมซอฟต์แวร์เกม) เช่น ซอฟต์แวร์เพื่อการศึกษาและซอฟต์แวร์เชิงวิศวกรรม เป็นต้น ขณะที่ตลาดบริการซอฟต์แวร์ได้แยกการสำรวจออกจากบริการ IT อื่นๆ โดยแบ่งเป็น 6 กลุ่มหลักได้แก่
      3.4.1 Software Maintenance Services
      3.4.2 Service and Application Hosting
      3.4.3 Software as a Service (SaaS)
      3.4.4 Software Services Outsourcing
      3.4.5 Software Related Training and Education
      3.4.6 บริการซอฟต์แวร์อื่นๆ (Software and Software Services)

จากแนวโน้มการใช้งานอินเทอร์เน็ตบรอดแบนด์ทั้งแบบใช้สายและแบบไร้สายขยายตัวมากขึ้น ส่งผลให้ความต้องการอุปกรณ์ที่รองรับการใช้งานอินเทอร์เน็ตเพิ่มสูงขึ้น นอกจากนี้การลงทุนทางด้านเทคโนโลยีสารสนเทศ ของภาครัฐและภาคเอกชนยังคงมีอย่างต่อเนื่องและการเติบโตของอุปกรณ์คอมพิวเตอร์ฮาร์ดแวร์ซึ่งมีราคาต่อหน่วยลดลงทุกปี นอกจากนี้ด้านเทคโนโลยีที่นำมาประยุกต์ใช้ร่วมกันได้ทั้งเทคโนโลยีเสมือนจริง หรือเวอร์ชวลไลเซชั่น ระบบการประมวลผลแบบคลาวด์ หรือคลาวด์คอมพิวติ้ง การนำทรัพยากรฮาร์ดแวร์และซอฟต์แวร์มาแบ่งปันกันใช้งานในลักษณะการบริการ (SaaS : Software as a Service) เป็นต้น

ที่กล่าวมาทั้งหมดนี้ทำให้เห็นถึง ความสำคัญของธุรกิจทางด้านเทคโนโลยีสารสนเทศ รวมไปถึงการดำเนินธุรกรรมทางดิจิทัลต่าง ๆ ที่ยังมีช่องทางให้กับผู้ที่ต้องการจะลงทุน วิสาหกิจขนาดกลางและขนาดย่อม จึงเป็นกลุ่มของผู้ประกอบการที่ยังต้องได้รับการสนับสนุนจากทางภาครัฐในการหาผู้ประกอบการมาดำเนินธุรกิจทางด้านนี้

2.8.3 แนวทางการสนับสนุนวิสาหกิจขนาดกลางและขนาดย่อม ภายในประเทศ

จากการศึกษาวิจัยของ International Data Corporation (IDC) พบว่าแรงขับเคลื่อนหลัก 4 ประการ ที่เป็นปัจจัยสำคัญที่ส่งผลต่อการเจริญเติบโตในอุตสาหกรรมเทคโนโลยีสารสนเทศของประเทศไทยในปี พ.ศ.2556 นี้ ได้แก่ (1) คลาวด์ (Cloud) (2) โมบิลิตี้ (Mobility) (3) โซเชียลบิซิเนส (SocialBusiness) และ (4) บิ๊กดาต้า (Big data) เนื่องจากสภาพเศรษฐกิจและความต้องการของผู้บริโภคเปลี่ยนไป และนอกจากนี้มีการคาดการณ์ถึงแนวโน้มสำคัญ 10 ประการที่จะส่งผลกระทบมากที่สุดต่อทิศทางของอุตสาหกรรมเทคโนโลยีสารสนเทศของประเทศไทยดังต่อไปนี้

2.8.3.1 การใช้จ่ายทางด้านเทคโนโลยีสารสนเทศของประเทศไทย

การใช้จ่ายและการลงทุนด้านเทคโนโลยีสารสนเทศในปี พ.ศ. 2556 ยังคงเติบโตอย่างแข็งแกร่งแม้ว่าจะถูกท้าทายจากเทคโนโลยีใหม่ๆ โดยจะได้รับแรงหนุนจากตลาดในกลุ่มองค์กร (Enterprise market) เพิ่มมากขึ้นกว่าปีที่ผ่านมา และได้รับอานิสงส์จากกลุ่มผู้บริโภค (Consumer market) โดย 3 กลุ่มหลักที่ยังคงใช้จ่ายด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องได้แก่ ธุรกิจการเงินการธนาคาร ธุรกิจโทรคมนาคม และกลุ่มงานภาครัฐ จะเห็นได้จากการลงทุนด้านโซลูชั่นอย่างต่อเนื่อง โดยการใช้จ่ายด้านฮาร์ดแวร์ยังคงเป็นส่วนประกอบหลัก อย่างไรก็ตามกลุ่มองค์กรเองยังต้องเผชิญกับการรับเอาเทคโนโลยีใหม่ๆ เข้ามาประยุกต์ใช้ได้แก่ บิ๊กดาต้า และอานาไลติก (Big data and analytic) หรือเทคโนโลยีคลาวด์ ขณะที่ภาครัฐเองก็มีการลงทุนอย่างต่อเนื่องด้านระบบสารสนเทศที่จะติดต่อกับโครงการ Government Cloud (G-cloud) และ Government Information Network (GIN) เพื่อให้สอดคล้องกับแผนสมาร์ทไทยแลนด์ (Smart Thailand) นอกจากนี้การเติบโตด้านเทคโนโลยีสารสนเทศในปีนี้ยังได้รับปัจจัยหนุนจากการลงทุนด้าน โครงข่าย 3G และโครงสร้างพื้นฐานทางโทรคมนาคมอย่างต่อเนื่องอีกด้วย มูลค่าตลาดรวมเทคโนโลยี สารสนเทศทั้งหมดของไทยจะสามารถเติบโตได้ไม่ต่ำกว่าร้อยละ 9.8 ไปสู่ระดับ 21 พันล้านเหรียญสหรัฐฯได้ โดยมูลค่าการใช้จ่ายเฉพาะด้านเทคโนโลยีสารสนเทศจะอยู่ที่ประมาณ 12.5 พันล้านเหรียญสหรัฐฯ ในปีนี้

2.8.3.2 การบริการข้อมูลไร้สายของธุรกิจด้านโทรคมนาคม

มูลค่าตลาดการสื่อสารและโทรคมนาคมของประเทศไทยในปี พ.ศ. 2556 ว่าบริการด้านข้อมูลไร้สายยังคงมีการเติบโตที่สดใส เนื่องจากการให้บริการข้อมูลผ่านโครงข่ายไร้สาย (Wireless network) จากผู้ให้บริการหลักที่มีปริมาณความต้องการสูงขึ้นอย่างต่อเนื่อง ประกอบกับบริการข้อมูลผ่านโครงข่าย 3G อย่างเต็มรูปแบบที่จะเกิดขึ้นในช่วงปลายไตรมาสที่ 2 เป็นต้นไป คาดว่าการเติบโตในปีนี้จะสูงกว่าร้อยละ 14 โดยมีมูลค่าตลาดไม่ต่ำกว่า 1.7 พันล้านเหรียญสหรัฐฯ

นอกจากนี้ การเติบโตของอุปกรณ์ประเภทสมาร์ทดีไวซ์ ยังถือเป็นแรงกระตุ้นหลักให้ปริมาณความต้องการใช้ข้อมูลผ่านโครงข่ายไร้สายให้สูงขึ้นอีกด้วย

2.8.3.3 รูปแบบใหม่ของการให้บริการเทคโนโลยีสารสนเทศแบบครบวงจรจากกลุ่มผู้ประกอบการ

ในตลาดเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทยไม่สามารถปฏิเสธได้ว่า บริการด้านสารสนเทศ (IT Services) ถือเป็นหนึ่งในองค์ประกอบหลักที่มีการใช้จ่ายเป็นอันดับที่ 2 รองจากการใช้จ่ายด้านฮาร์ดแวร์และอุปกรณ์ด้านการเครือข่าย (IT hardware and networking system) และสามารถใช้เป็นหนึ่งในตัวชี้วัดหลักในการประเมินความเป็นมืออาชีพ รวมถึงความสามารถในการให้บริการจากฝั่งผู้ประกอบการด้านการให้บริการติดตั้งระบบแบบครบวงจร (IT Services Provider and System Integrator) รูปแบบการให้บริการในปีนี้จะเปลี่ยนจากกลุ่มงานบริการที่ผูกติดกับอุปกรณ์มาสู่รูปแบบการนำเสนอบริการที่เน้นคุณค่าของกระบวนการทางธุรกิจและตอบโจทย์ทางธุรกิจมากขึ้นโดยลดความสำคัญของการให้บริการแบบบำรุงรักษาระบบทั่วไปลง เนื่องจากการแข่งขันที่รุนแรงในตลาดและไม่คุ้มค่ากับการลงทุนดังนั้น การสร้างมูลค่าในการให้บริการใหม่ๆ

ดังกล่าวจะส่งผลดีต่อทั้งผู้ให้บริการเองในแง่ของการสร้างมูลค่าเพิ่มในการให้บริการ ตัวอย่างโมเดลของรูปแบบการให้บริการแบบใหม่นั้น รวมถึง Outsourcing 3.0 การดำเนินกลยุทธ์การให้บริการบริหารจัดการอุปกรณ์ที่มาจากผู้ผลิตและสภาพแวดล้อมในการใช้งานที่ต่างกัน (Multi-vendors management service) หรือแม้กระทั่งการนำเสนอบริการดูแลระบบแบบเหมารวมทั้งอุปกรณ์ โดยที่ลูกค้าองค์กรสามารถเรียกใช้บริการได้ตามความจำเป็น เป็นต้น ในปี พ.ศ. 2556 นี้ มูลค่าตลาดบริการด้านสารสนเทศในประเทศไทยจะเติบโตได้ถึงร้อยละ 14.2 และมีมูลค่าไม่ต่ำกว่า 1.8 พันล้านเหรียญสหรัฐฯ

2.8.3.4 การอิ่มตัวของการเจริญเติบโตของคอมพิวเตอร์ส่วนบุคคล

เครื่องคอมพิวเตอร์ส่วนบุคคลหรือเดสก์ท็อป และเครื่องคอมพิวเตอร์ส่วนบุคคลแบบพกพกหรือแล็ปท็อป เคยเป็นผลิตภัณฑ์ส่วนบุคคลที่มียอดขายเติบโตอย่างต่อเนื่องมาเป็นเวลาช้านาน แต่ในทุกวันนี้จะต้องหลีกทางให้กับอุปกรณ์พกพาที่เกิดใหม่ทั้งสมาร์ทโฟนและแท็บเล็ต ไอดีซีเชื่อว่าตั้งแต่ปี พ.ศ. 2556 เป็นต้นไป ตลาดคอมพิวเตอร์ส่วนบุคคลในประเทศไทยจะขยายตัวอย่างยากลำบากโดยการเติบโตของตลาดคอมพิวเตอร์ส่วนบุคคลตั้งแต่ปี พ.ศ. 2556 นั้นมีแนวโน้มที่จะเติบโตอย่างแข็งแกร่งเหมือนในปีที่ผ่านมา และอาจจะถึงการเติบโตแบบติดลบอย่างต่อเนื่อง ส่งผลให้ผู้ผลิตและผู้จำหน่ายคอมพิวเตอร์ส่วนบุคคลต้องปรับตัวใช้กลยุทธ์ใหม่ๆ เพื่อ

รักษาฐานตลาดเดิมของตนไว้ซึ่งคาดการณ์ตลาดคอมพิวเตอร์ส่วนบุคคลของประเทศไทยในปี พ.ศ. 2556 จะขยายตัวน้อยกว่าร้อยละ 4 โดยมียอดจัดส่งเพียงแค่ 4 ล้านเครื่องเท่านั้น

2.8.3.5 Mobile OS ตลาดสมาร์ทโฟนและแท็บเล็ตที่เติบโต

ความนิยมที่เพิ่มมากขึ้นเรื่อยๆ ของสมาร์ทโฟนและแท็บเล็ตได้ทำให้ตลาดของดีไวซ์เหล่านี้เติบโตอย่างก้าวกระโดด ซึ่งคาดการณ์ว่าด้วยแรงซื้อที่ปรับตัวเพิ่มขึ้นอย่างต่อเนื่อง ประกอบกับความพร้อมของการให้บริการ 3G จะทำให้ตลาดสมาร์ทโฟนในปี พ.ศ. 2556 มีแนวโน้มที่จะขยายตัวได้สูงถึงร้อยละ 40 ด้วยยอดจัดส่งทั้งหมด 7.3 ล้านเครื่อง ส่วนตลาดแท็บเล็ตเองก็มีแนวโน้มที่จะเติบโตในอัตราใกล้เคียงกัน ซึ่งหมายถึงยอดจัดส่งทั้งหมดไม่ต่ำกว่า 3.5 ล้านเครื่องในปีนี้ ด้วยกำลังซื้อที่เพิ่มสูงขึ้นนี้มาพร้อมกับการแข่งขันที่เข้มข้นขึ้นในหมู่ผู้ผลิตและผู้จำหน่าย โดยเฉพาะอย่างยิ่ง เมื่อผู้บริโภคให้ความสำคัญกับการเลือกระบบปฏิบัติการมากกว่าจะมองที่ความสามารถของฮาร์ดแวร์เพียงประการเดียว ในปี พ.ศ.2556 เชื่อว่าระบบปฏิบัติการไอโอเอส (iOS) และแอนดรอยด์ (Android) จะต้องแข่งขันกันอย่างดุเดือดเพื่อขึ้นเป็นอันดับหนึ่งในใจของผู้บริโภค ส่วนระบบปฏิบัติการที่เกิดใหม่อย่างวินโดวส์โฟน 8 (Windows Phone 8) และแบล็กเบอร์รี 10 (Blackberry 10) จำเป็นจะต้องทุ่มสุดตัวเพื่อหาพื้นที่ในตลาดเพื่อรองรับการเติบโตในอนาคต โดยแต่ละระบบปฏิบัติการก็ต้องประสบกับความท้าทายที่แตกต่างกันไอโอเอสจำเป็นต้องปกป้องฐานผู้บริโภคเดิม ในขณะที่แอนดรอยด์และวินโดวส์จำเป็นต้องรุกเพื่อดึงส่วนแบ่งตลาดจากไอโอเอสมากขึ้น ส่วนแบล็กเบอร์รีต้องพยายามกลับเข้าสู่ตลาดอีกครั้งเพื่อเป็นทางเลือกที่ 3รองจากระบบปฏิบัติการยอดนิยมอย่างไอโอเอสและแอนดรอยด์ ไอดีซีเชื่อว่าการแข่งขันที่สูงขึ้นนี้จะทำให้ผู้บริโภคได้รับประโยชน์ในแง่ของความหลากหลายของสินค้าและราคาที่ปรับตัวลดลง ในขณะที่ผู้ผลิตจำเป็นต้องวางกลยุทธ์ใหม่ๆ ควบคู่ไปกับการเพิ่มความร่วมมือกับผู้จำหน่ายในประเทศเพื่อแย่งชิงส่วนแบ่งตลาด

2.8.3.6 ความนิยมของสมาร์ดิไวท์ (Smart devices) เป็นแรงกระตุ้นให้เกิดการใช้งาน Digital Content

กระแสความนิยมของสมาร์ทดีไวซ์ หรืออุปกรณ์อัจฉริยะ ไม่ว่าจะเป็นโทรศัพท์เคลื่อนที่ สมาร์ทโฟนหรืออุปกรณ์พกพาแบบแท็บเล็ต ได้ส่งผลต่อการใช้งานสื่อ Digital Content ที่หลากหลาย ไม่ว่าจะเป็น Content แอพพลิเคชั่นทางด้านธุรกิจ ด้านสันทนาการ ไปจนถึง Content แอพพลิเคชั่นที่เกี่ยวข้องกับไลฟ์สไตล์ของแต่ละบุคคล จากผลการศึกษา Consumerscape 360 ระดับภูมิภาคเอเชียแปซิฟิก ของ พ.ศ. 2555 ที่ผ่านมาพบว่า ทั้งกลุ่มผู้ใช้งานโทรศัพท์เคลื่อนที่สมาร์ทโฟนและแท็บเล็ตกว่าร้อยละ 55 นิยมดาวน์โหลด Content แอพพลิเคชั่นประเภทเกมมากเป็นอันดับหนึ่ง รองลงมาคือ แอพพลิเคชั่น ประเภทโซเชียลเน็ตเวิร์ก และเพลง เป็นอันดับที่สอง

และสาม ในขณะที่ Content แอพพลิเคชั่นด้าน การเดินทาง และการถ่ายรูปได้รับความนิยมน้อยที่สุด ซึ่งสอดคล้องกับความนิยมของผู้ใช้งานสมาร์ทดีไวซ์ ในประเทศไทยที่พบว่า ส่วนใหญ่นิยมใช้งาน Content แอพพลิเคชั่นประเภทโซเชียลเน็ตเวิร์กเป็นลำดับต้นๆ ซึ่งความนิยมนี้ได้ส่งผลต่อการเติบโตของปริมาณการใช้ข้อมูลจากผู้บริโภคและองค์กร

2.8.3.7 Consumerization to personal ecosystem สภาพแวดล้อมส่วนบุคคลผ่านสมาร์ทดิไวท์

กระแสการใช้งานอุปกรณ์ประมวลผลส่วนบุคคลโดยเฉพาะสมาร์ทดีไวซ์เข้ามาเป็นส่วนหนึ่งของกระบวนการทำงานในองค์กรนั้น ถือว่าได้รับความนิยมอย่างสูง หลายองค์กรเองได้กำหนดนโยบายการนำอุปกรณ์ส่วนตัวเหล่านี้มาติดต่อกับระบบสารสนเทศขององค์กรได้อย่างดีเยี่ยม และมีส่วนช่วยในการเพิ่มศักยภาพในการทำงานที่ยืดหยุ่นและทันต่อการสนองตอบทางธุรกิจมากขึ้น ในปี พ.ศ. 2556 นี้แนวคิดการประยุกต์การใช้งานในลักษณะ Consumerization กลายเป็นแรงกระตุ้นให้ผู้ใช้งานส่วนบุคคลหรือผู้บริโภค (consumer / personal user) ได้ใช้สมาร์ทดีไวซ์เพื่อการจัดการภาระงานและกิจกรรมส่วนบุคคลอันหลากหลาย ตัวอย่างที่เห็นได้ชัดเจน ได้แก่ โทรศัพท์สมาร์ทโฟน 1 เครื่องสามารถเป็นได้ทั้งอุปกรณ์จดบันทึก อุปกรณ์สื่อสารทั้งข้อมูลและเสียง ฟังเพลง แลกเปลี่ยนประสบการณ์การใช้งานหรือการเข้าถึงข้อมูลมัลติมีเดียในชีวิตประจำวัน เป็นต้น นอกจากนี้ผู้บริโภคเองยังได้มองหาอุปกรณ์เสริมตัวที่สองหรือพยายามสร้างสภาพแวดล้อมที่เหมาะสมสำหรับตนเองเพื่ออำนวยความสะดวกหรือสนับสนุนการทำงาน หรือเชื่อมต่ออุปกรณ์แต่ละประเภทเข้าด้วยกัน เพื่อแลกเปลี่ยนข้อมูลภายใต้สภาพแวดล้อมที่สามารถควบคุมได้จากเจ้าของอุปกรณ์เหล่านี้ อาทิ การฝากข้อมูลหรือการหาพื้นที่ออนไลน์ในการเก็บหรือสำรองข้อมูล (Online –virtual storage) ส่วนบุคคลเพื่อประโยชน์ในการแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์สมาร์ทดีไวซ์ประเภทต่างๆ ที่ตนเองครอบครองอยู่ หรือแม้กระทั่งการหาพื้นที่เสมือนในการแบ่งปันข้อมูลระหว่างผู้ใช้งานในกลุ่มเดียวกัน ตัวอย่างที่เห็นได้ชัดเจนที่สุดได้แก่ การสร้างเครือข่ายระหว่างอุปกรณ์ต่างๆ กับระบบคลาวน์ เพื่อประโยชน์ในการสำรองและถ่ายเทข้อมูล หรือการส่งข้อมูลระหว่างเครื่องเล่นมัลติมีเดียโดยผ่านช่องทางบลูทูธเพื่อเก็บเป็นโปรไฟล์ส่วนบุคคล พฤติกรรมต่างๆ เหล่านี้จะเป็นกิจกรรมที่เกิดขึ้นเป็นปรกติในชีวิตประจำวันสำหรับผู้ใช้สมาร์ทดีไวซ์ในปี พ.ศ. 2556

2.8.3.8 การเติบโตของคลาวด์ในประเทศยังคงเป็นไปอย่างต่อเนื่อง

แม้ว่าสถานการณ์การประยุกต์ใช้เทคโนโลยีคลาวด์ รวมถึงบริการคลาวด์ภายในประเทศยังคงเป็นไปค่อนข้างช้า เนื่องมาจากความกังวล 2 ประการ ได้แก่ ระบบรักษาความปลอดภัยในการใช้งานและความปลอดภัยของข้อมูล จะเป็นปัจจัยหลักในการเลี่ยงจากกการใช้งาน

คลาวด์เต็มรูปแบบ อย่างไรก็ตามการให้บริการคลาวด์ยังคงเกิดขึ้นในประเทศต่อไป โดยรูปแบบจะเป็นการให้บริการในลักษณะPublic Cloud มากขึ้น นอกจากนี้โครงการการลงทุนระบบคลาวด์ภาครัฐฯ หรือ Government Cloudที่จะนำมาเป็นส่วนเทคโนโลยีหลักในการให้บริการภาครัฐฯ เองก็เป็นแรงผลักดันอีกประการหนึ่งที่จะช่วยกระตุ้นส่งเสริมให้เกิดความมั่นใจในการใช้งานเทคโนโลยีประเภทนี้ ส่วนรูปแบบการใช้งานของคลาวน์ในประเทศในปีนี้จะมุ่งเน้นไปที่ Application-as-a-Service (AaaS) ได้แก่ แอพพลิเคชั่นด้าน Collaboration และ Productivities เป็นหลัก

2.8.3.9 การตอบรับจากกลุ่มองค์กรต่อความต้องการโซลูชั่นที่ผนวกกับโครงสร้างพื้นฐานด้านสารสนเทศ

กระแสของ Converged solution เริ่มมีให้เห็นอย่างชัดเจนมากขึ้นในธุรกิจสารสนเทศ และผู้ใช้งานระดับองค์กรได้ตระหนักถึงประโยชน์ของการปรับให้ converged solution เหล่านี้ ผู้ให้บริการระบบจึงมีความพยายามที่จะนำเสนอ consolidated solution เพื่อความสะดวกในการบริหารจัดการและควบคุมทรัพยากรด้านไอที โดยโครงสร้างพื้นฐานด้านสารสนเทศนั้นกำลังก้าวไปไกลกว่าเพียงแค่ระบบเน็ตเวิร์กเพียงอย่างเดียว บรรดาผู้ผลิตอุปกรณ์เครื่องแม่ข่าย อุปกรณ์การจัดเก็บข้อมูลอุปกรณ์เน็ตเวิร์กและซอฟต์แวร์ต่างก็พยายามนำเสนอโซลูชั่นแบบหนึ่งเดียวที่ได้รวมเอาโซลูชั่นปลีกย่อยตั้งแต่ระดับโครงสร้างพื้นฐานไปจนถึงแอพพลิเคชั่นซึ่งสามารถสร้างประสบการณ์ใหม่ๆ ให้กับผู้ใช้งานระดับองค์กร ด้วยระดับการแข่งขันที่เพิ่มสูงขึ้น ประกอบกับความต้องการของกลุ่มลูกค้าองค์กรในการปกป้องโครงสร้างพื้นฐานด้านสารสนเทศของตนจากสถานการณ์ที่ไม่คาดคิด ได้กดดันให้ผู้ผลิตอุปกรณ์ต่างๆ ต้องนำเสนอโซลูชั่นที่สามารถทำงานประสานร่วมกันอย่างมีประสิทธิภาพสูงสุดและพร้อมที่จะตอบสนองต่อความต้องการอันหลากหลายขององค์กรต่างๆ ซึ่งมีการคาดการณ์ว่า ตลาดระบบโครงสร้างพื้นฐานจะขยายตัวได้ประมาณร้อยละ 11 ในปี พ.ศ. 2556 โดยมีจุดเด่นที่สำคัญคือการผนวกระบบรักษาความปลอดภัยเข้าไปเป็นหนึ่งโซลูชั่นที่จะนำเสนอให้กับกลุ่มลูกค้าองค์กร

2.8.3.10 ระบบการจัดการและวิเคราะห์ข้อมูลขนาดใหญ่ (Big data and analysis)

บิ๊กดาต้า ได้มีส่วนสำคัญในการผลักดันให้เกิดการลงทุนด้านสารสนเทศในช่วงที่ผ่านมา และได้กลายเป็นหัวข้อสามัญที่เหล่าองค์กรต่างๆ ต้องหยิบยกขึ้นมาอภิปรายอยู่เสมอๆ ผู้ผลิตสินค้าและบริการด้านสารสนเทศก็มีส่วนในการสร้างความตระหนักถึงการมาถึง และการใช้ประโยชน์จากบิ๊กดาต้า อนึ่งความต้องการที่จะใช้ระบบการวิเคราะห์ข้อมูลขั้นสูงและซับซ้อน เริ่มเกิดขึ้นในองค์กรขนาดใหญ่ และองค์กรขนาดกลางได้เริ่มพิจารณาถึงประเด็นนี้ด้วยเช่นกัน ระบบการวิเคราะห์ข้อมูลขั้นสูงและซับซ้อนจะกลายเป็นกลไกสำคัญในกระบวนการ

บริหารจัดการระบบฐานข้อมูลเพื่อให้องค์กรสามารถใช้ประโยชน์จากข้อมูลให้ได้สูงสุด กระบวนการคอนซูเมอร์ไรเซชันของสมาร์ทโฟนและแท็บเล็ต ประกอบกับการที่องค์กรต่างๆ ได้อนุญาตให้พนักงานเข้าถึงแอพพลิเคชั่นผ่านอุปกรณ์สื่อสารเคลื่อนที่ ได้ทำให้เชื่อว่าตลาด Information Management Analytics จะสามารถเติบโตได้ถึงร้อยละ 12 ในปี พ.ศ. 2556

2.8.4 ความมั่นคงปลอดภัยทางไซเบอร์กับวิสาหกิจขนาดและขนาดย่อม

จากการสำรวจของ CERT 2013 US State of Cybercrime Survey (2014) ในประเด็นอาชญากรรมทางไซเบอร์ (Cybercrime) ในสหรัฐอเมริกา พบว่าวิสาหกิจขนาดกลางและขนาดย่อมได้ถูกการคุกคามการโจมตีทางไซเบอร์แบบโดยไม่รู้ตัว โดยช่องโหว่จะมาจากการใช้วิธีการด้านไอทีที่หลากหลาย แนวโน้มความเสี่ยงด้านไอทีที่พบมากที่สุดในขณะนี้คือการใช้อุปกรณ์มือถือ รวมไปถึงการย้ายที่จัดเก็บข้อมูลไปยังคลาวด์ การทำข้อมูลให้เป็นดิจิทัลแล้วย้ายไปยังเทคโนโลยีสมาร์กริต (Smartgrid) Watchguard.com (2015) ได้จัดทำรายงานเพื่อนำเสนอถึงภัยคุกคามทางไซเบอร์ที่เป็นอันตรายต่อ SMEs ของสหรัฐอเมริกา โดยที่ WatchGuard ได้ทำการสำรวจจากลูกค้าที่ส่วนใหญ่เป็น SMEs โดยที่ WatchGuard ได้ตรวจสอบถึงภัยคุกคามทางไซเบอร์ที่มีผลต่อความปลอดภัยด้านเครือข่ายที่เกิดขึ้นใหม่ทุกวัน โดยให้ความสำคัญกับปัญหาที่ส่งผลกระทบต่อ SMEs แนวทางของ WatchGuard สร้างรายงานที่เป็นประโยชน์เกี่ยวกับภัยคุกคามความปลอดภัยทางไซเบอร์ ทำให้ทราบถึงผลกระทบทางด้านลบที่เกิดต่อความปลอดภัยทางไซเบอร์ของลูกค้า ที่มุ่งเน้นไปการโจมตีข้อมูลในธุรกิจ SMEs นอกจากนี้ยังพบอีกว่ายังไม่มีหลักฐานใด ๆ ที่สามารถบอกได้ถึงรายชื่อ SMEs ที่ต้องประสบกับปัญหาภัยคุกคามทางไซเบอร์โดยเฉพาะ และจากรายงาน “The Verizon Data Breach Report 2014” Verizon. (2014) ซึ่งวิเคราะห์การรั่วไหลของข้อมูลที่มีมากกว่า 1,300 กรณี ทำให้ได้รับการยืนยันและชี้ให้เห็นถึงภัยคุกคามด้านความปลอดภัยที่คล้ายกัน นอกจากในรายงานยังแสดงให้เห็นอีกว่า การละเมิดข้อมูลที่เป็นภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น ไม่ได้ขึ้นอยู่กับภัยคุกคามที่มีผลต่อความปลอดภัยทางไซเบอร์ของ SME เท่านั้น ยังมาจากข้อมูลที่รวบรวมได้จาก 50 องค์กรความมั่นคงปลอดภัยทางไซเบอร์ในระดับชาติหรือระดับนานาชาติ และจากกลุ่มตัวอย่างที่มีอยู่อย่างจำกัด รายงานอาชญากรรมทางไซเบอร์หลายฉบับเช่น 2015 Cost of Cyber Crime Study: United Kingdom (Ponemon Institute, 2015) กล่าวถึงความถี่ของการเกิดอาชญากรรมไซเบอร์และการสูญเสียทางการเงินที่เกี่ยวข้อง ในรายงานได้กล่าวถึงเหตุการณ์ที่เกิดขึ้นแต่ไม่ได้ระบุถึงสาเหตุของการเกิดการโจมตี นอกจาก WatchGuard ยังได้อธิบายถึงมาตรการป้องกันที่จำเป็นที่เกี่ยวข้องกับภัยคุกคามเหล่านี้ รวมถึงโซลูชันเชิงพาณิชย์และซอฟต์แวร์ที่จัดทำขึ้น ภัยคุกคามด้านความปลอดภัยทางไซเบอร์ที่ WatchGuard [10] ยังถูก

ตรวจสอบจากแหล่งต่าง ๆ / เอกสารนำเสนอภาพที่สมบูรณ์ของภัยคุกคามและส่งผลกระทบต่อทรัพย์สินทางด้านไอทีของ

2.8.5 การศึกษาที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ของวิสาหกิจขนาดกลางและขนาดย่อม

2.8.5.1 ภัยคุกคามทางไซเบอร์ที่มีต่อวิสาหกิจขนาดกลางและขนาดย่อม

จากการศึกษาทำให้ผู้วิจัยพบว่าปัญหาภัยคุกคามทางไซเบอร์ที่วิสาหกิจขนาดกลางและขนาดย่อมต้องประสบในสถานการณ์ปัจจุบันจะมาจาก 2 สาเหตุหลัก ๆ ได้แก่

1. อุปกรณ์ส่วนตัวมาใช้งาน (Bring Your Own Devices: BYOD)

จากความพร้อมเนื่องจากการใช้งานของอินเทอร์เน็ต 3G/4G และความก้าวหน้าที่เกี่ยวกับอุปกรณ์การสื่อสาร ได้แก่แล็ปท็อป แท็บเล็ต สมาร์ตโฟน และอื่น ๆ ประกอบกับการพัฒนาขึ้นของอุปกรณ์เหล่านั้นที่สามารถทำการเคลื่อนย้ายไปในทุกแห่งทุกที่ได้อย่างสะดวกสบายมากขึ้นเพื่อให้เกิดความคล่องตัวในการใช้งานสำหรับอุปกรณ์ดังกล่าว แนวโน้มความคล่องตัวคือ BYOD (นำอุปกรณ์มาเอง) ซึ่งหมายถึงพนักงานใช้อุปกรณ์ของตัวเองในช่วงเวลาทำงาน โดยในปัจจุบัน คำว่า “เทคโนโลยีของคุณที่นำมาเอง” (BYOT) ก็จะถูกนำมาใช้แทนที่คำว่า “นำอุปกรณ์ของคุณมาเอง” (BYOD) ซึ่งโดยทั่วไปจะมีทั้งฮาร์ดแวร์และซอฟต์แวร์

BYOD (หรือ BYOT) กลายเป็นเรื่องธรรมดาไปแล้วในหลาย ๆ ธุรกิจ จากการสำรวจของซิสโก้ที่เป็นผู้เชี่ยวชาญด้านไอทีและธุรกิจในสหรัฐอเมริกา โดยการสอบถามด้วยแบบสอบถามจากผู้ที่เกี่ยวข้อง 600 คน ผู้ตอบแบบสอบถามร้อยละ 95 กล่าวว่าองค์กรของพวกเขาอนุญาตให้พนักงานใช้อุปกรณ์ของตนเองในที่ทำงานได้ Cisco (2015) การสำรวจเดียวกันนั้นนำไปสู่การประเมินว่าพนักงาน โดยเฉลี่ยที่มีพื้นฐานด้านเทคนิคใช้อุปกรณ์ที่เชื่อมต่อในที่ทำงานอยู่ในระดับสูง และจำนวนอุปกรณ์ที่เชื่อมต่อต่อพนักงานคาดว่าจะเพิ่มขึ้นในอนาคต และจากการสำรวจระบุว่าในยุโรปพบว่ามีบริษัทจำนวนมากขึ้นที่ยอมให้ BYOD Computer World, UK. (2015) อย่างไรก็ตามยังมีความกังวลเกี่ยวกับปัญหาด้านความปลอดภัยที่เกิดขึ้นจากพนักงานที่เชื่อมต่ออุปกรณ์ส่วนบุคคลกับทรัพยากรของบริษัท

นอกจากนั้นยังพบอีกว่า BYOD เป็นภัยคุกคามที่สามารถนำความเสี่ยงที่สำคัญบางอย่างมาสู่องค์กรหรือบริษัทได้ ภัยคุกคามใน BYOD ที่ปฏิเสธไม่ได้ก็คือ พนักงานหรือคนในองค์กรนั่นเอง จากการทบทวนวรรณกรรมพบว่าพนักงานที่ได้รับอนุญาตให้ใช้ระบบหรือสิ่งอำนวยความสะดวกของบริษัท Neumann, P. G. (2016) จากการศึกษาของ Kelly, B.B., (2016); Magklaras, GB et al., (2012) ได้ชี้ให้เห็นถึงภัยคุกคามทางไซเบอร์ที่มาจากการใช้ข้อมูล

ภายในในบริษัท โดยที่คนวงในอาจเป็นภัยคุกคามต่อองค์กรเนื่องจากการไม่รู้ตัวของเขา/เธอที่จะกระทำความผิดพลาดทั้งเจตนาหรือไม่เจตนาก็ตาม (Durgin, M., 2017; Lee, J., and Lee, Y. ,2016) จากการสำรวจของ CSI/FBI Gordon, L. et al., (2016) ซึ่งจัดทำขึ้นในหมู่ผู้ประกอบการรักษาความปลอดภัยทางคอมพิวเตอร์ 616 คนในสหรัฐอเมริกา พบว่า 64% ของผู้ตอบแบบสอบมีการสูญเสียที่เกี่ยวข้องกับความปลอดภัยของข้อมูลเกิดขึ้นเนื่องจากการกระทำของบุคคลภายใน ตัวอย่างเช่น บุคคลภายในอาจก่อให้เกิดภัยคุกคามความปลอดภัยด้านไอทีโดยการเรียกจดหมายขยะเปิดไฟล์แนบอีเมลที่ติดไวรัสหรือยกเลิกการป้องกันการคุกคามด้านความปลอดภัยข้อมูลที่ไม่มีนัยสำคัญ Besnard, D. & Arief, B. (2017) และจากรายงานของนอร์ตัน 2018 (Norton Report, 2018) ซึ่งทำการสำรวจในกลุ่มตัวอย่างของผู้ใหญ่ออนไลน์ 13,022 รายจาก 24 ประเทศ พบว่า

- 49% ใช้อุปกรณ์ส่วนตัว (พีซี แล็ปท็อป สมาร์ตโฟนและแท็บเล็ต) สำหรับกิจกรรมที่เกี่ยวข้องกับการทำงาน
- เกือบครึ่งหนึ่งไม่ได้ใช้ข้อควรระวังพื้นฐานด้านความปลอดภัยทางไซเบอร์ เช่นรหัสผ่านและซอฟต์แวร์ความปลอดภัย มีผู้ใช้สมาร์ตโฟนเพียง 26% เท่านั้นที่มีซอฟต์แวร์รักษาความปลอดภัยมือถือที่มีการป้องกันขั้นสูงว่า และ57% ไม่ทราบหรือว่ามีโซลูชั่นรักษาความปลอดภัยทางไซเบอร์มือถือนั้น ๆ ของตน
- 27% สูญเสียอุปกรณ์พกพาหรือถูกขโมย

ผู้ใช้อุปกรณ์พกพา (สมาร์ทโฟนแล็ปท็อปและแท็บเล็ต) มีแนวโน้มที่จะใช้คุณสมบัติและแอปของอุปกรณ์มากขึ้น (Smith, A., 2016) สำหรับการใช้คุณสมบัติของอุปกรณ์พนักงานสามารถเชื่อมต่ออุปกรณ์ส่วนบุคคลกับเครือข่ายหรือเครื่องที่ไม่รู้จักหรือไม่ปลอดภัย (อาจเป็นแบบมีสายหรือไร้สาย) และอาจติดไวรัสมัลแวร์หรือสคริปต์ที่เป็นอันตราย เมื่ออุปกรณ์เชื่อมต่อกับเครือข่ายของบริษัท การเชื่อมต่อนี้สามารถเปิดเส้นทางสำหรับมัลแวร์สปายแวร์ไวรัสหรือสคริปต์เพื่อโยกย้ายจากอุปกรณ์ส่วนบุคคลไปยังเครื่องของบริษัท และผ่านเครือข่ายของบริษัท ซึ่งแสดงให้เห็นว่าอุปกรณ์ส่วนบุคคลเพียงชิ้นเดียวเท่านั้นที่สามารถส่งผลกระทบต่อโครงสร้างพื้นฐานด้านไอทีทั้งหมดของ บริษัท ในอีกทางหนึ่งสามารถบันทึกข้อมูลสำคัญบนอุปกรณ์ส่วนตัวได้ สิ่งนี้สามารถกระทำได้แม้กระทั่งในรูปแบบของสิ่งที่แนบมากับอีเมลที่ดึงมาในอุปกรณ์ ข้อมูลนี้อาจรวมถึงข้อมูลลูกค้าส่วนตัวและข้อมูลบริษัทที่เป็นกรรมสิทธิ์ หรือแม้แต่การที่อุปกรณ์ถูกขโมยไปซึ่งก็อาจจะมีข้อมูลของบริษัทติดไปด้วยโดยอาจจะนำไปสู่การเปิดเผยข้อมูลที่อาจส่งผลเสียให้กับบริษัทตามมาได้ Paul Ruggiero, J.F. (2017).

2. การประมวลผลแบบคลาว์ (Cloud Computing)

การพัฒนาล่าสุดของการประมวลผลแบบคลาวด์ได้เข้าไปปรับปรุงและเปลี่ยนแปลงโครงสร้างพื้นฐานด้านไอทีของบริษัทต่าง ๆ อย่างสิ้นเชิง โดยจะเปลี่ยนการเก็บข้อมูลหรือประมวลผลบนคอมพิวเตอร์ของตัวเอง แต่เทคโนโลยีการประมวลผลคลาวด์ได้เก็บข้อมูลและซอฟต์แวร์บนเซิร์ฟเวอร์ระยะไกลและให้ลูกค้าสามารถเข้าถึงได้ผ่านทางอินเทอร์เน็ต นอกจากนี้ผู้ใช้ไม่ได้เป็นเจ้าของเทคโนโลยีที่ใช้ บริษัทที่ให้บริการเป็นเจ้าของฮาร์ดแวร์และซอฟต์แวร์ทั้งหมด ลูกค้าจะต้องชำระค่าบริการเท่านั้น ซึ่งแน่นอนว่าค่าใช้จ่ายย่อมน้อยกว่าการเป็นเจ้าของโครงสร้างพื้นฐานด้านไอทีทั้งหมดที่ให้บริการ

การประมวลผลแบบคลาวด์เป็นประโยชน์มากสำหรับ SMEs ในการแก้ปัญหางบประมาณที่ไม่เพียงพอทางด้าน ตัวอย่างของบริการคลาวด์สำหรับผู้ใช้ทั่วไป ได้แก่ เว็บเมลแอปพลิเคชัน วิกิพีเดีย (wikipedia) และ ดร้อปบ๊อกซ์ (Dropbox) ผู้ให้บริการคลาวด์ที่รู้จักกันดี คือ กูเกิ้ล (Google) อเมซอน (Amazon) และ ยะฮู (Yahoo) ซึ่งได้สร้างโครงสร้างพื้นฐานขนาดใหญ่เพื่อรองรับการคำนวณและการจัดเก็บในลักษณะที่ปรับขนาดได้ Azarnik, A. et al., (2012)

แบบจำลองทางด้านคลาวด์นี้มีประโยชน์ทั่วไปมากมาย ลูกค้าสามารถปรับเปลี่ยนความสามารถในการคำนวณ เช่นเวลาเซิร์ฟเวอร์และที่เก็บข้อมูลเครือข่ายโดยอัตโนมัติโดยไม่มีการโต้ตอบใด ๆ กับผู้ให้บริการในการบริการตนเองตามความต้องการ ลูกค้ายังสามารถใช้คลาวด์ด้วยอินเทอร์เน็ตและเข้าถึงอุปกรณ์มาตรฐาน เช่น โทรศัพท์มือถือ แล็ปท็อป และพีดีเอ ซึ่งให้ความสามารถในการเข้าถึงเครือข่ายในวงกว้าง สำหรับด้านของผู้ให้บริการ การรวมทรัพยากรเป็นไปได้ที่จัดเก็บและทรัพยากรการคำนวณบนคลาวด์สามารถจัดสรรให้กับลูกค้าหลายคนตามความต้องการด้วยทรัพยากรทางกายภาพและเสมือนที่แตกต่างกัน การใช้ทรัพยากรคลาวด์สามารถตรวจสอบวัดและรายงานโดยผู้ให้บริการและลูกค้าเพื่อความโปร่งใส NIST. (2019)

จากการสำรวจทางเศรษฐศาสตร์ของ Stewardship Economics Group. (2016) พบว่า SMEs ที่มียอดขายต่อปีค่อนข้างต่ำกำลังใช้การประมวลผลแบบคลาวด์มากกว่ากลุ่ม SMEs ที่มีระดับการหมุนเวียนสูงกว่า การประมวลผลแบบคลาวด์ นำเสนอฟังก์ชั่นการใช้งานทั้งหมดของบริการเทคโนโลยีสารสนเทศในปัจจุบันและลดค่าใช้จ่ายในการดำเนินงานของ SMEs ไปเป็นอย่างมาก ด้วยบริการทางด้านไอทีที่ทันสมัยที่จะสามารถช่วยผู้ประกอบการ SMEs ให้สามารถลดค่าใช้จ่ายและเวลาในการทำงานลงไปได้ Azarnik, A. et al., (2012)

แต่ถึงกระนั้นก็ตามการประมวลแบบคลาวด์ก็เป็นสาเหตุที่ทำให้เกิดภัยคุกคามทางด้านไซเบอร์ตามได้อีกด้วย แม้ว่าเทคโนโลยีการประมวลผลแบบคลาวด์จะมีข้อดีหลายประการ แต่ความเสี่ยงที่เกี่ยวข้องกับการประมวลผลแบบคลาวด์ก็นั้นค่อนข้างสูงตามมา

เช่นกัน SMEs ที่สนใจจะใช้งานเทคโนโลยีการประมวลผลแบบคลาวด์ก็ต้องพิจารณาถึงมาตรการในการรักษาความมั่นคงปลอดภัยการประมวลผลแบบคลาวด์ด้วย โดยจะต้องพิจารณาถึงแนวทางในการจัดการความเสี่ยงความไซเบอร์ตามมาอีกด้วย (Stewardship Economics Group., 2016) เพราะแน่นอนว่าการนำเอาข้อมูลของบริษัทไปเก็บไว้ที่คลาวด์นั้นย่อมมีความเสี่ยงเกิดขึ้นมาได้เช่นเดียวกัน รวมไปถึงเรื่องการลักลอบขโมยทรัพย์สินทางปัญญาซอฟต์แวร์ที่เป็นกรรมสิทธิ์และข้อมูลลับที่สำคัญ (Aron R. et al., 2012; Chen Y., 2009; Clemons E. K., 2017; Walden E. A., (2015)

การรุกล้ำเกิดขึ้นเมื่อผู้ให้บริการคลาวด์ใช้ข้อมูลและทรัพยากรของผู้ใช้บริการที่ผิดสัญญา ด้วยวิธีนี้ผู้ให้บริการคลาวด์สามารถเปิดเผยข้อมูลการออกแบบหรือกลยุทธ์ของลูกค้าของ SME การรุกล้ำยังสามารถนำไปสู่การใช้ข้อมูลส่วนตัวในทางที่ผิด ตัวอย่างเช่นหากฐานข้อมูลลูกค้าของ SME ที่จัดเก็บในระบบคลาวด์ถูกบุกรุก อาจนำไปสู่การเปิดเผยข้อมูลส่วนบุคคลของลูกค้าและในกรณีที่เลวร้ายที่สุดอาจนำไปสู่การขโมยข้อมูลส่วนบุคคลอย่างสมบูรณ์ (Kristof, K., 2016; McCoy K. (2017) ดังนั้นในขณะที่ที่เก็บข้อมูลบนคลาวด์ทำให้ง่ายต่อการบันทึกและแชร์ไฟล์และลดค่าใช้จ่ายด้านไอที แต่ยังทำให้เกิดช่องโหว่ด้านความปลอดภัยด้านไอทีมากขึ้นตามไปด้วย

โดยสรุปภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้กับ SMEs ไม่ว่าจะเป็นภัยคุกคามที่มาจากการประมวลผลแบบคลาวด์ และการนำเอาอุปกรณ์มาใช้เองนั้นยิ่งนับวันจะมีความรุนแรงมากยิ่งขึ้น แต่การแก้ไขก็ยังสามารถแก้ไขได้โดยการบังคับใช้นโยบายบางประการเกี่ยวกับพฤติกรรมของพนักงานในการใช้เทคโนโลยีเหล่านี้ ตัวอย่างเช่นภัยคุกคามที่จากการนำเอาอุปกรณ์ส่วนตัวมาใช้งานนั้นขึ้นอยู่กับกิจกรรมของผู้ใช้ที่มีความเป็นส่วนตัว ดังนั้นการบังคับใช้นโยบายเกี่ยวกับวิธีการใช้อุปกรณ์ส่วนบุคคลที่มีข้อมูลสำคัญทางการสามารถแก้ไขปัญหาได้ นอกจากนี้ภัยคุกคามทางไซเบอร์ก็จะมาจากการใช้งานในระบบการประมวลผลแบบคลาวด์เพราะความไวของข้อมูลที่สามารถรั่วไหลออกมา หากมีวิธีปฏิบัติทั่วไปเล็กน้อยเกี่ยวกับการบันทึกข้อมูลในระบบคลาวด์ในลักษณะที่ปลอดภัยภัยคุกคามนี้สามารถบรรเทาได้

จากความไม่ปลอดภัยจากภัยคุกคามทางไซเบอร์ที่มาจากสาเหตุดังที่ได้กล่าวไว้ข้างต้น มีผลทำให้ SMES มีความเสี่ยงต่อการเกิดเหตุการณ์ความปลอดภัยสูงในโลกไซเบอร์ ธุรกิจทุกขนาดต้องเตรียมพร้อมสำหรับภัยคุกคามเหล่านี้ เนื่องจากนี้ยังมีการวิจัยเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับด้าน SMEs อยู่น้อยมาก ยอ่มมีผลทำให้มีแนวทางในการรับมือด้วยความคาดหวังเพียงเล็กน้อยเกี่ยวกับสถานการณ์ความปลอดภัยของ SMEs ในปัจจุบัน

2.9 สรุป

ในบทที่ 2 ได้นำเสนอแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับ กรอบแนวคิดในการวิจัย ผู้วิจัยได้ศึกษารวม 5 หัวข้อหลัก ได้แก่ 1) ภัยคุกคามทางไซเบอร์ ซึ่งได้พิจารณาถึงความสำคัญของภัยคุกคามทางไซเบอร์ และผลที่จะทำให้เกิดความเสียหายต่อโซ่อุปทาน 2) การคืนสภาพได้ของโซ่อุปทาน เพื่อใช้เป็นฐานความรู้เกี่ยวกับ การพัฒนากรอบแนวคิดสำหรับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน 3) ตัวแบบวุฒิภาวะความสามารถเพื่อนำไปสร้างระดับวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน 4) ปัจจัยเหตุที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานที่ประกอบด้วย ความร่วมมือกันของโซ่อุปทาน การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน และสมรรถนะของโซ่อุปทาน และ 5) ผลของความสามารถในการสร้างการคืนสภาพได้ทางด้านไซเบอร์ โดยทั้งหมดผู้วิจัยได้ทำการศึกษาจากกลุ่มผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม สาขาสารสนเทศ/ดิจิทัลคอนเท้นท์ ที่รัฐบาลให้การสนับสนุนโดยมีเงื่อนไขของการดำเนินธุรกิจภายใต้สภาวะแวดล้อมที่เป็น IT-Base สำหรับวิธีการ ดำเนินการวิจัยจะนำเสนอในบทที่ 3 ต่อไป