บทความวิจัย

โมเดลสมการเชิงโครงสร้าง เพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย

นริส อุไรพันธ์* และ ธรนี มณีศรี
วิทยาลัยโลจิสติกส์และซัพพลายเชน มหาวิทยาลัยศรีปทุม
ประสงค์ ปราณีตพลกรัง
คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 06 2807 5550 อีเมล: naris080515@yahoo.com DOI: 10.14416/j.kmutnb.2020.02.004
รับเมื่อ 9 กันยายน 2562 แก้ไขเมื่อ 31 ตุลาคม 2562 ตอบรับเมื่อ 21 พฤศจิกายน 2562 เผยแพร่ออนไลน์ 11 กุมภาพันธ์ 2563

บทคัดย่อ

การวิจัยครั้งมีวัตถุประสงค์เพื่อ 1) ศึกษาปัจจัยที่จะส่งผลต่อการคืนสภาพได้ทางด้านไซเบอร์ของดิจิทัลซัพพลายเชน 2) วิเคราะห์ความสัมพันธ์โครงสร้างเชิงสาเหตุของปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางด้านไซเบอร์ของดิจิทัลซัพพลายเชน ด้วยวิธีการวิจัยเชิงปริมาณ ตัวอย่างที่ใช้ในศึกษา ได้แก่ วิสาหกิจขนาดกลางและขนาดย่อม (เอสเอ็มอี) จำนวน 400 ราย จากทั้งหมด 3,077,822 รายในประเทศไทย ผู้วิจัยทำการเก็บรวบรวมข้อมูลด้วยแบบสอบถาม โดยแจกแบบสอบถามเอสเอ็มอีละ 5 ฉบับ ผลการตอบแบบสอบถามกลับคิดเป็นร้อยละ 93.20 วิเคราะห์ข้อมูลด้วยการวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis; CFA) และการวิเคราะห์โมเดลสมการเชิงโครงสร้าง (Structural Equation Modeling; SEM) ผลการวิจัยพบว่า 1) ความร่วมมือกันของดิจิทัลซัพพลายเชน (Path Coefficient = 0.11) การจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชน (Path Coefficient = 0.03) และการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน (Path Coefficient = 0.83) เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน และมีอิทธิพลทางอ้อมต่อการจัดการความต่อเนื่องทางธุรกิจผ่านการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน 2) ความร่วมมือกันของดิจิทัลซัพพลายเชน (Path Coefficient = 0.39) และการจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชน (Path Coefficient = 0.59) เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน และ 3) การคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน (Path Coefficient = 0.98) เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการจัดการความต่อเนื่องทางธุรกิจ โดยสรุปแล้ว การคืนสภาพได้ทางไซเบอร์เป็นสภาวะที่องค์กรมีความทนทาน คล่องตัว มีความสามารถในการรับมือและฟื้นฟูกลับคืนสู่สภาพปกติได้อย่างเร็วที่สุดหลังจากการถูกโจมตีทางไซเบอร์

คำสำคัญ: ภัยคุกคามทางไซเบอร์ การคืนสภาพได้ทางไซเบอร์ ดิจิทัลซัพพลายเชน วิสาหกิจขนาดกลางและขนาดย่อม

การอ้างอิงบทความ: นริส อุไรพันธ์ ธรนี มณีศรี และ ประสงค์ ปราณีตพลกรัง, "โมเดลสมการเชิงโครงสร้าง เพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, (2563). DOI: 10.14416/j.kmutnb.2020.02.004

Research Article

Structural Equation Modeling for Analysis of Factors Affecting the Cyber Resilience in Digital Supply Chain for Small and Medium-sized Enterprises

Naris Uraipan* and Tharinee Manisri
College of Logistics and Supply Chain, Sripatum University, Bangkok, Thailand
Prasong Praneetpolgrang
School of Information Technology, Sripatum University, Bangkok, Thailand

* Corresponding Author, Tel. 06 2807 5550, E–mail: naris080515@yahoo.com
DOI: 10.14416/j.kmutnb.2020.02.004
Received 9 September 2019; Revised 31 October 2019; Accepted 21 November 2019; Published online: 11 February 2020

Abstract

This study aims to 1) study factors affecting the cyber resilience in digital supply chain and 2) analyze the casual model of factors that affecting the cyber resilience in digital supply chain. The research is carry out by the quantitative research methods with sample of 400 from 3,077,822 of Small and Medium-sized Enterprises (SMEs) in Thailand. The researcher collected data using questionnaire and distributed 5 questionnaires per SME. The questionnaires were returned to the response rate at 93.20%. Data was analyzed by Confirmatory Factor Analysis (CFA), and Structural Equation Modeling (SEM). The research found that 1) digital supply chain collaboration (Path Coefficient = 0.11), cyber threat management (Path Coefficient = 0.03) and digital supply chain risk management (Path Coefficient = 0.83) had direct and positive influence to cyber resilience in digital supply chain and had indirect to business continuity management through cyber resilience in digital supply chain, 2) digital supply chain collaboration (Path Coefficient = 0.39) and cyber threat management (Path Coefficient = 0.59) had direct and positive influence to digital supply chain risk management, and 3) cyber resilience in digital supply chain (Path Coefficient = 0.98) has direct and positive to business continuity management. In summary, cyber resilience is a state in which the organizations are robust, agile, capable of coping and recovering to the normal state as soon as possible after cyber attack.

Keywords: Cyber Threat, Cyber Resilience, Digital Supply Chain, Small and Medium-sized Enterprises

Please cite this article in press as: N. Uraipan, T. Manisri, and P. Praneetpolgrang, "Structural equation modeling for analysis of factors affecting the cyber resilience in digital supply chain for small and medium-sized enterprises," *The Journal of KMUTNB*, (2020), (in Thai). DOI: 10.14416/j.kmutnb.2020.02.004

1. บทนำ

จากการเปลี่ยนแปลงทางเทคโนโลยี ส่งผลให้ธุรกิจทั้งหลายเปลี่ยนแปลงตามไปด้วย สมรรถนะในการแข่งขัน การทำธุรกิจออนไลน์ รวมถึงแลกเปลี่ยนข้อมูลทางการค้ากับพันธมิตรด้วยเอกสารอิเล็กทรอนิกส์มีผลให้การจัดการโซ่อุปทาน (Supply Chain Management) ได้รับผลกระทบจากการเปลี่ยนแปลงในครั้งนี้ การเผชิญกับความท้าทายใหม่ๆ จึงกลายเป็นทางออกของแผนการเติบโตของอุตสาหกรรม ทำให้เกิดธุรกรรมต่างๆ ภายใต้ดิจิทัลซัพพลายเชน (Digital Supply Chain) เพิ่มขึ้นตามไปด้วยสิ่งที่ตามมาคือ ภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่เกิดขึ้นในปัจจุบัน ซึ่งได้ส่งผลกระทบต่อดิจิทัลซัพพลายเชนและทำให้เกิดปัญหาต่อโซ่อุปทาน โลกภัยคุกคามทางไซเบอร์เกิดได้ทั้งภายในโซ่อุปทานและระหว่างโซ่อุปทาน ไม่ว่าจะเป็นมัลแวร์ที่แฝงตัวในโฆษณาอีเมล (Malvertising) และการโจมตีทางไซเบอร์ไปยังช่องโหว่ (Vulnerability) กลายมาเป็นภัยคุกคามที่ท้าทายความน่าเชื่อถือในระบบโซ่อุปทานและแนวทางปฏิบัติที่เหมาะสม [1]

การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) เป็นสภาวะที่องค์กรมีความทนทานนั่นคือต้องมีความคล่องตัว (Agility) และคงทน (Robustness) [2], [3] ต่อภัยคุกคามทางไซเบอร์ที่เคยพบหรืออาจไม่เคยพบมาก่อนเป็นแนวทางในการเตรียมความพร้อมขององค์กรให้สามารถป้องกันและตรวจจับการบุกรุกโจมตีทางไซเบอร์ก่อนที่จะส่งผลเสียต่อองค์กร และถ้าการบุกรุกโจมตีได้ก่อเกิดปัญหาขึ้นต่อองค์กรแล้ว องค์กรควรจะมีความสามารถในการตอบสนองต่อการถูกโจมตีได้อย่างรวดเร็ว เป็นทราบกันว่าการโจมตีทางไซเบอร์ได้เกิดขึ้นมานานหลายปีแล้วเพียงแต่อาจจะไม่มีความรุนแรงเท่าในปัจจุบัน และด้วยการโจมตีที่เพิ่มขึ้น เป็นผลมาจากการขาดความพร้อมซึ่งเป็นปัญหาสำคัญที่จำเป็นต้องได้รับการจัดการดูแลอย่างจริงจังจากรายงานภัยคุกคามด้านความปลอดภัยบนอินเทอร์เน็ต (Internet Security Threat Report; ISTR) ฉบับที่ 20 ของไซแมนเทค (Nasdaq; SYMC) เปิดเผยว่าธุรกิจขนาดกลางและขนาดใหญ่ในประเทศไทยได้ลงทุนด้านไอทีไปค่อนข้างมาก ซึ่งต่างกับธุรกิจกลุ่มวิสาหกิจขนาดกลางและขนาดย่อม ซึ่งมีมูลค่าการค้าสูงถึง 43% ของจีดีพีของประเทศ นั้นที่ส่วนใหญ่ยังไม่ได้พัฒนาไปในทิศทางที่กล่าวข้างต้น ประกอบกับการเพิ่มขึ้นของความเสี่ยงที่เกิดมาจากภัยคุกคามทางไซเบอร์นี้เป็นผลมาจากการขาดความพร้อม จึงเป็นปัญหาสำคัญที่จำเป็นต้องได้รับการจัดการดูแลอย่างจริงจัง

จากข้อมูลที่กล่าวมาข้างต้น ทำให้ผู้วิจัยมีความสนใจที่จะศึกษาถึงปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนสำหรับธุรกิจหรือวิสาหกิจขนาดกลางและขนาดย่อม (เอสเอ็มอี) ในประเทศไทย เพื่อให้เอสเอ็มอีได้เตรียมความพร้อมและทำการปรับปรุงระบบในการปกป้องธุรกิจจากภัยคุกคามทางไซเบอร์ เอสเอ็มอีต้องระมัดระวังต่อภัยคุกคามทางไซเบอร์ทั้งในรูปแบบเดิมและรูปแบบใหม่ที่จะเข้ามา โดยจะต้องดำเนินการให้ครอบคลุมในทุกระบบและทุกกลุ่มเอสเอ็มอีในการสร้างแนวทางในการป้องกัน และรับมือต่อภัยคุกคามทางไซเบอร์เหล่านั้น

1.1 ภัยคุกคามทางไซเบอร์ (Cyber Threat)

ภัยคุกคามทางไซเบอร์ เป็นเรื่องที่บริษัทหรือหน่วยงานต่างๆ ทั้งภาครัฐและเอกชนกำลังเผชิญอยู่ โดยภัยคุกคามทางไซเบอร์เป็นสิ่งที่เกิดขึ้นเพื่อสร้างความเสียหายให้กับระบบคอมพิวเตอร์ที่เกิดขึ้นในปัจจุบัน จุดมุ่งหมายในการโจมตีส่วนใหญ่มุ่งไปใน 3 ลักษณะ คือการนำความลับไปเปิดเผย (Data Confidentiality) การเปลี่ยนแปลงข้อมูล (Data Integrity) และการทำให้ระบบหยุดบริการหรือไม่สามารถใช้งานได้ (System Availability) [4]

1.2 การจัดการความเสี่ยงของโซ่อุปทาน (Supply Chain Risk Management)

จากการศึกษาของ Christopher และ Peck [5] ได้ให้ข้อเสนอแนะว่า วิธีที่ดีที่สุดในการจัดการกับความเสี่ยงในคือการเพิ่มความเชื่อมั่นในโซ่อุปทานซึ่งจะเกิดขึ้นได้ก็ต่อเมื่อโซ่อุปทานจะมีความสามารถในการเปลี่ยนสภาพคืนกลับสู่สภาวะปกติจากการที่ต้องเผชิญกับการเปลี่ยนแปลงที่ส่งผลกระทบต่อการดำเนินงาน

1.3 การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน (Supply Chain Cyber Resilience)

สภาเศรษฐกิจโลก (World Economic Forum; WEF) ได้นิยามความหมายของคำว่า การคืนสภาพได้ทางไซเบอร์ ไว้ว่า ความสามารถของระบบและองค์กรในการทนต่อเหตุการณ์ที่เกิดขึ้นในโลกไซเบอร์ โดยวัดจากผลรวมระหว่างเวลาเฉลี่ยในการล้มเหลวกับเวลาเฉลี่ยในการกู้คืน

Windelberg [6] ได้ศึกษาถึงความเสี่ยงในโลกไซเบอร์ที่เกี่ยวข้องกับซัพพลายเออร์จำนวนมาก เนื่องจากไม่ได้มีการเข้มงวดในการทำงานจึ่งทำให้เกิดความเสี่ยงในการดำเนินงานต่อองค์กรต่อผู้ใช้ปลายทางและต่อสังคมและพบอีกว่าความน่าเชื่อถือเป็นสิ่งสำคัญต่อการจัดการความเสี่ยงในโซ่อุปทานโดยความซื่อสัตย์ และความปลอดภัยเป็นประเด็นที่รองลงมารวมถึงการกำหนดนโยบายสำหรับการจัดการความเสี่ยงในโซ่อุปทานที่เป็นไปได้ยาก

Ali และคณะ [7] ได้ศึกษาโดยพบว่า การกำหนดให้ได้มาซึ่งการคืนสภาพได้ของโซ่อุปทานต้องประกอบไปด้วยองค์ประกอบหลักๆ 3 ประการ ได้แก่ ขั้นตอนกลยุทธ์และความสามารถในการสร้างการคืนสภาพโดยความสามารถในสร้างการคืนสภาพได้จะประกอบไปด้วย ความสามารถในการคาดการณ์ปรับตัวตอบสนองการกู้คืนและเรียนรู้โดยได้ทำการระบุองค์ประกอบสำคัญ 13 ข้อ และแนวทางปฏิบัติด้านการบริหาร 84 ข้อ ที่จะสนับสนุนบริษัทต่างๆ เพื่อให้บรรลุความสามารถทั้ง 5 ประการ เพื่อเชื่อมโยงกับกลยุทธ์และขั้นตอนของกรอบแนวคิดในการสร้างการคืนสภาพได้ของโซ่อุปทานต่อไป

Parkinson และคณะ [8] พบว่าอุปกรณ์คอมพิวเตอร์ในเครือข่ายทั้งหมดที่มีการเชื่อมต่อเข้าหากันจะส่งผลให้มีความเสี่ยงสูงขึ้น จากการโจมตีด้านความมั่นคงปลอดภัยไซเบอร์ประกอบกับระบบอัตโนมัติที่เพิ่มขึ้นก็เป็นผลทำให้เกิดความเสี่ยงสูงขึ้น โดยการเพิ่มโอกาสให้ฝ่ายตรงข้ามในการโจมตีที่ประสบความสำเร็จ ทั้งนี้การโจมตีส่วนใหญ่จะมาจากช่องโหว่ ที่มีจากฝ่ายตรงข้ามที่เป็นมิตร (แฮ็กเกอร์หมวกสีขาว) นอกจากนั้น ยังพบว่ามีความเหลื่อมล้ำในเรื่องความรู้ความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ ควรให้ความสำคัญกับการพัฒนาเพื่อลดความเสี่ยงและความเหลื่อมล้ำด้านความมั่นคงปลอดภัยไซเบอร์ในภาคอุตสาหกรรมที่มีการเชื่อมต่อกันผ่านระบบเครือข่าย

ณัฏภัทรศญา [9] ได้ศึกษาพบว่า กลยุทธ์ที่มีความเหมาะสมสำหรับการประยุกต์ใช้งานตามปกติในโซ่อุปทานอุตสาหกรรมคอมพิวเตอร์ในประเทศไทย ที่มีอิทธิพลทางตรง คือ กลยุทธ์ความหยุ่นตัวทางอ้อมคือกลยุทธ์ความคล่องตัว โดยความคล่องตัวมีความสัมพันธ์ทางตรงกับความหยุ่นตัวและความคล่องตัว และความหยุ่นตัวใช้งานพร้อมกันแบบคู่ขนาน จะส่งผลในเชิงบวกอย่างมากต่อผลการดำเนินงานของบริษัท

2. วิธีการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงปริมาณ เนื่องจากต้องทำการวิเคราะห์ปัจจัยที่เกี่ยวข้องกับตัวแปรและใช้วิธีการทางสถิติช่วยวิเคราะห์ผล ทั้งนี้ผู้วิจัยได้ทำการศึกษาตัวแปรที่เกี่ยวข้องซึ่งประกอบด้วย ตัวแปรแฝงภายนอก (Exogenous Variables) และตัวแปรแฝงภายใน (Endogenous Variables) โดยมีรายละเอียดดังต่อไปนี้

ตัวแปรแฝงภายนอก ประกอบด้วยปัจจัย 3 ด้าน ได้แก่ ความร่วมมือกันของโซ่อุปทาน ปัญหาภัยคุกคามทางไซเบอร์ และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน โดยสถานะในแต่ละปัจจัยประกอบด้วยตัวแปรที่สังเกตได้หรือตัวชี้วัด ดังต่อไปนี้

1. ความร่วมมือกันของโซ่อุปทาน ประกอบด้วยตัวแปรที่สังเกตได้ 4 ตัวแปร ได้แก่ การแบ่งปันข้อมูลร่วมกัน ความไว้ใจ ความร่วมมือกันในการสื่อสาร และการสร้างความรู้ร่วมกัน

2. การจัดการภัยคุกคามทางไซเบอร์ ประกอบด้วยตัวแปรที่สังเกตได้ 3 ตัวแปร ได้แก่ แรงจูงใจในการโจมตีทางไซเบอร์จากภายนอก ช่องโหว่ของดำเนินงานภายใน และการรับมือต่อภัยคุกคามทางไซเบอร์

3. การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน ประกอบด้วยตัวแปรที่สังเกตได้ 3 ตัวแปร ได้แก่ บุคลากร กระบวนการ และเทคโนโลยี

ตัวแปรแฝงภายใน ประกอบด้วยปัจจัย 2 ด้าน ได้แก่

การคืนสภาพได้ทางไซเบอร์ของดิจิทัลชัพพลายเชน และการจัดการความต่อเนื่องทางธุรกิจโดยสถานะในแต่ละปัจจัยประกอบด้วยตัวแปรที่สังเกตได้หรือตัวชี้วัด ดังต่อไปนี้

1. การคืนสภาพได้ทางไซเบอร์ของดิจิทัลชัพพลายเชน ประกอบด้วยตัวแปรที่สังเกตได้ 2 ตัวแปร ได้แก่ ความคล่องตัว และความทนทาน

2. การจัดการความต่อเนื่องทางธุรกิจ ประกอบด้วยตัวแปรที่สังเกตได้ 4 ตัวแปร ได้แก่ แผนความต่อเนื่องทางธุรกิจ แผนกู้คืนภัยพิบัติ การจัดการวิกฤต และการจัดการเหตุฉุกเฉิน

โดยปัจจัยทั้งหมดจะได้ใช้ด้วยการใช้มาตรวัดของลิเคิร์ท 5 ระดับ (Five-point Likert-type Scale Ranging) ประชากรที่ศึกษาในการวิจัยเชิงปริมาณ ได้แก่ ผู้ประกอบการในวิสาหกิจขนาดกลางและขนาดย่อม โดยข้อมูล ณ ปี พ.ศ. 2561 มีจำนวนทั้งสิ้น 3,077,822 บริษัท ผู้วิจัยได้กำหนดตัวอย่าง โดยใช้เกณฑ์สำหรับการเลือกตัวอย่างในการวิเคราะห์โมเดลสมการเชิงโครงสร้าง (SEM) เท่ากับ 20 เท่าของจำนวนพารามิเตอร์ [10] โดยจำนวนพารามิเตอร์ในโมเดลได้ 16 พารามิเตอร์ ทำให้ได้ขนาดตัวอย่างเท่ากับ 320 บริษัท และเพื่อป้องกันแบบสอบถามที่ไม่สมบูรณ์ ผู้วิจัยได้เพิ่มจำนวนบริษัทเป็น 400 บริษัท โดยแจกแบบสอบถามเพื่อให้ผู้ตอบแบบสอบถามบริษัทละ 5 ฉบับ ซึ่งทำให้ได้จำนวนแบบสอบถามรวมทั้งสิ้น 2,000 ฉบับ และ โดยได้รับผลการตอบแบบสอบถามมาเป็นจำนวนทั้งสิ้น 1,864 ฉบับ มีอัตราการตอบกลับ (Response Rate) เท่ากับ 93.2% ดังแสดงในตารางที่ 1

การศึกษาวิจัยผู้วิจัยได้ใช้เครื่องมือเป็นแบบสอบถาม โดยหาคุณภาพของแบบสอบถาม ด้วยการหาค่าความเที่ยงตรง (Validity) โดยส่งให้ผู้เชี่ยวชาญ ที่มีความรู้ความเข้าใจเฉพาะด้าน จำนวน 5 ท่าน ตามเทคนิค Item Objective Congruence (IOC) โดยข้อคำถามมีค่า IOC มากกว่า 0.5 [11] และทุกข้อนำมาทดสอบความเชื่อถือได้ (Reliability) โดยทดลองใช้ (Try-out) กับกลุ่มที่มีลักษณะคล้ายคลึงกับกลุ่มตัวอย่าง จำนวน 30 คน เพื่อตรวจสอบสัมประสิทธิ์แอลฟาของครอนบาค (Conbach's Alpha Coefficient – α Coefficient) ซึ่งค่าสัมประสิทธิ์ของความเชื่อมั่นที่คำนวณมากกว่า 0.7 แสดงได้ว่าเครื่องมือแบบสอบถามมีความน่าเชื่อถือ [12]

ตารางที่ 1 การเลือกสุ่มตัวอย่างจากตัวเลขรายงานสถานการณ์ SME ปี 2561

จำนวนวิสาหกิจขนาดกลางและขนาดย่อม ปี พ.ศ. 2561	จำนวน (บริษัท)	สัดส่วนการเลือกสุ่มตัวอย่าง (%)	จำนวนตัวอย่าง (บริษัท)	บริษัทละ (คน)	รวมจำนวน (ฉบับ)
ภาคการค้า	1,279,557	41.57%	166	5	830
ภาคการบริการ	1,224,563	39.79%	159	5	795
ภาคการผลิต	527,485	17.14%	69	5	345
ภาคธุรกิจเกษตร	46,217	1.50%	6	5	30
รวมทั้งสิ้น	3,077,822	100.00%	400	-	2,000

ที่มา: สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (2561)

3. ผลการวิจัย

ผลการศึกษาระดับปัจจัยที่จะส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลชัพพลายเชน สำหรับวิสาหกิจขนาดกลางและขนาดย่อมสรุปได้ ดังตารางที่ 2

ตารางที่ 2 ระดับปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลชัพพลายเชน

ปัจจัย	$\bar{x}$	S.D.	แปลความ
1. ด้านความร่วมมือกันของโซ่อุปทาน	3.70	0.86	มาก
2. ด้านการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทาน	3.52	0.92	มาก
3. ด้านการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทาน	3.72	0.85	มาก
4. การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน	3.67	0.86	มาก
5. การจัดการความต่อเนื่องทางธุรกิจ	3.68	0.86	มาก

ผลการตรวจสอบความเหมาะสมของข้อมูลก่อนนำไปวิเคราะห์โมเดลสมการเชิงโครงสร้าง พบว่า มีตัวแปรที่สังเกต

ได้ 16 ตัวแปรทุกคู่ จำนวน 120 คู่ ส่วนใหญ่มีค่าไม่เกิน 0.80 ความสัมพันธ์ดังกล่าว แสดงให้เห็นว่าตัวแปรที่สังเกตได้มีระดับความสัมพันธ์ไม่สูงมากนัก จึงไม่เกิดปัญหาภาวะเส้นตรงร่วมเชิงพหุ (Multicollineartiry) และตัวแปรที่สังเกตได้ทั้งหมดอยู่บนองค์ประกอบร่วมกัน ดังนั้นจึงมีความเหมาะสมที่จะนำไปวิเคราะห์โมเดลสมการเชิงโครงสร้าง (Structure Equation Model; SEM) [13]

เมื่อพิจารณาค่าสถิติ Bartlett's Test of Sphericity พบว่ามีค่าเท่ากับ 32389.482, df = 120, p = 0.000 และเมทริกซ์สัมประสิทธิ์สหสัมพันธ์ไม่เป็นเมทริกซ์เอกลักษณ์ (Indentity Matrix) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.01 ตัวแปรมีความสัมพันธ์กันอย่างเพียงพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้สอดคล้องกับผลการวิเคราะห์ Kaiser-Mayer-Olkin (KMO) ซึ่งมีค่าใกล้ 1 (0.975) สอดคล้องกลมกลืนกับโมเดลการวิจัยกับข้อมูลเชิงประจักษ์เนื่องจากค่าดัชนีมีค่า 0.80 ขึ้นไปแสดงว่าข้อมูลเหมาะสมที่จะทำการวิเคราะห์องค์ประกอบ (Factor Analysis) ดีมากโดยผลการตรวจสอบความเหมาะสมของข้อมูลแสดงได้ดังตารางที่ 3

ผลการศึกษาความสัมพันธ์โครงสร้างเชิงสาเหตุของปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน สำหรับวิสาหกิจขนาดกลางและขนาดย่อมด้วยการวิเคราะห์อิทธิพลของตัวแปรเชิงสาเหตุที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนสำหรับวิสาหกิจขนาดกลางและขนาดย่อม นั้นได้ผลแสดงไว้ ดังตารางที่ 4

ตารางที่ 3 ผลการตรวจสอบความเหมาะสมของข้อมูลด้วยการวิเคราะห์ค่าสหสัมพันธ์แบบเพียร์สันระหว่างตัวแปรที่สังเกตได้

Factors	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	Y1	Y2	Y3	Y4	Y5	Y6
X1	1															
X2	0.797**	1														
X3	0.804**	0.826**	1													
X4	0.771**	0.794**	0.785**	1												
X5	0.430**	0.399**	0.374**	0.429**	1											
X6	0.652**	0.637**	0.630**	0.665**	0.446**	1										
X7	0.681**	0.654**	0.671**	0.644**	0.365**	0.660**	1									
X8	0.764**	0.748**	0.762**	0.764**	0.418**	0.672**	0.724**	1								
X9	0.694**	0.685**	0.724**	0.669**	0.342**	0.625**	0.683**	0.805**	1							
X10	0.677**	0.699**	0.700**	0.726**	0.408**	0.635**	0.652**	0.764**	0.729**	1						
Y1	0.738**	0.741**	0.736**	0.754**	0.445**	0.661**	0.695**	0.803**	0.751**	0.795**	1					
Y2	0.701**	0.734**	0.720**	0.748**	0.447**	0.647**	0.662**	0.776**	0.712**	0.808**	0.855**	1				
Y3	0.705**	0.715**	0.729**	0.722**	0.410**	0.625**	0.663**	0.781**	0.772**	0.765**	0.823**	0.829**	1			
Y4	0.688**	0.675**	0.713**	0.624**	0.336**	0.574**	0.690**	0.761**	0.764**	0.682**	0.756**	0.714**	0.803**	1		
Y5	0.669**	0.673**	0.673**	0.660**	0.386**	0.606**	0.641**	0.733**	0.727**	0.702**	0.750**	0.767**	0.776**	0.770**	1	
Y6	0.650**	0.690**	0.688**	0.724**	0.426**	0.615**	0.645**	0.750**	0.700**	0.751**	0.795**	0.808**	0.787**	0.722**	0.769**	1
Means	3.69**	3.73**	3.70	3.68	3.50	3.54	3.54	3.71	3.75	3.65	3.70	3.66	3.70	3.73	3.65	3.63
S.D.	0.77**	0.70	0.72	0.77	0.8	0.77	0.74	0.73	0.72	0.78	0.76	0.73	0.72	0.74	0.73	0.80

**Cometion is significant at the 0.01 level (2-tailed), Kaiser-Mayer-Olkin Measure of Sampling Adequacy (KMO) = 0.975, Bartlett's Test of Sphericity = 32389.482, df = 120, sig = 0.00

หมายเหตุ: นัยสำคัญที่ระดับ *$p < 0.01$

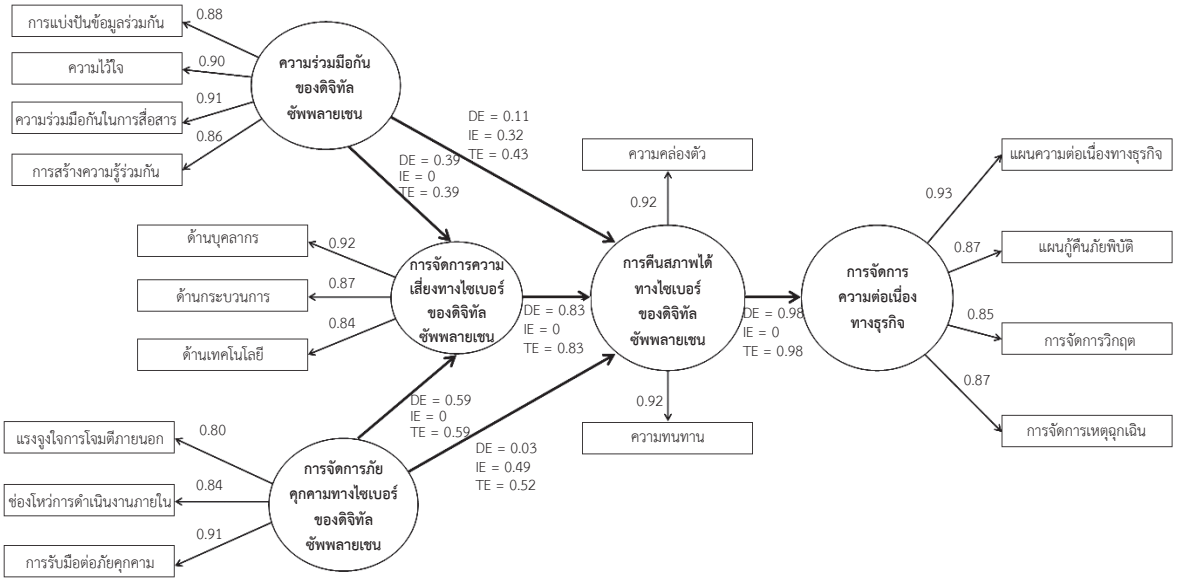
ผลการทดสอบความสอดคล้องของโมเดลสมการเชิงโครงสร้างของปัจจัยที่ตัวแปรเชิงสาเหตุ ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนและการจัดการความต่อเนื่องทางธุรกิจสำหรับวิสาหกิจขนาดกลางและขนาดย่อม โดยภาพรวมตามสมมติฐานกับข้อมูลเชิงประจักษ์ ซึ่งพิจารณาค่าสถิติประเมินความกลมกลืนของโมเดลกับข้อมูลเชิงประจักษ์ พบว่า โมเดลมีความสอดคล้องด้วยค่า χ^2/df= 1.391(41.740/30= 1.391) เป็นไปตามเกณฑ์กำหนดไว้คือ ควรมีค่าน้อยกว่า 2 นอกจากนี้ ผลการวิเคราะห์ค่า GFI และ AGFI มีค่าเท่ากับ 0.997 และ 0.987 ตามลำดับซึ่งมีค่าเข้าใกล้หนึ่งผ่านเกณฑ์ที่กำหนดไว้ว่า ควรมีค่ามากกว่า 0.95 ที่ระดับความเชื่อมั่น 99 และค่า RMSEA เท่ากับ 0.014 มีค่าเท่ากับศูนย์ซึ่งผ่านเกณฑ์ที่กำหนดว่าควรมีค่าน้อยกว่า 0.05 แสดงให้เห็นว่าโมเดลการวิจัยที่พัฒนาขึ้นสอดคล้องกับข้อมูลเชิงประจักษ์ ดังแสดงไว้ในรูปที่ 1 นั้นคือ

1. ความร่วมมือกันของดิจิทัลซัพพลายเชน มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน มีอิทธิพลทางตรงและทางอ้อมเชิงบวกต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน และมีอิทธิพลทางอ้อมเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจ

ตารางที่ 4 การวิเคราะห์ค่าสัมประสิทธิ์ของตัวแปรเชิงสาเหตุของการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนและการจัดการความต่อเนื่องทางธุรกิจ

ปัจจัยเหตุ	**ความร่วมมือกันของดิจิทัลซัพพลายเชน (SCC)**			**ปัญหาภัยคุกคามทางไซเบอร์ ของดิจิทัลซัพพลายเชน (CBT)**			**การจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน (CBR)**			**การคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน (CRS)**		
ปัจจัยผล	**TE**	**DE**	**IE**	**TE**	**DE**	**IE**	**TE**	**DE**	**IE**	**TE**	**DE**	**IE**
การจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน (CBR)	0.394	0.394	-	0.590	0.590	-	-	-	-	-	-	-
การคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน (CRS)	0.431	0.106	0.325	0.515	0.027	0.488	0.827	0.827	-			
การจัดการความต่อเนื่องทางธุรกิจ (BCM)	0.424	-	0.424	0.506	-	0.506	0.813	-	0.813	0.983	0.983	-
ค่าสถิติไคว์-สแควร์ = 41.740, df = 30, *p*-value = 0.075, GFI = 0.997, AGFI = 0.987, RMR = 0.003, RMSEA = 0.014												
ตัวแปรเหตุ	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10		
ความเที่ยง	0.782	0.815	0.831	0.748	0.272	0.616	0.704	0.838	0.749	0.709		
ตัวแปรผล	Y1	Y2	Y3	Y4	Y5	Y6						
ความเที่ยง	0.855	0.852	0.831	0.769	0.723	0.758						
สมการโครงสร้างของตัวแปร				CBR	CRS	BCM						
R-Square				0.913	0.902	0.967						
เมทริกซ์สหสัมพันธ์ระหว่างตัวแปรแฝง												
ตัวแปรแฝง	SCC		CBT		CBR		CRS		BCM			
SCC	1.000											
CBT	0.882		1.000									
CBR	0.914		0.937		1.000							
CRS	0.885		0.895		0.948		1.000					
BCM	0.870		0.880		0.933		0.983		1.000			

หมายเหตุ: $p < 0.01$ DE คืออิทธิพลทางตรง IE คืออิทธิพลทางอ้อม TE คืออิทธิพลรวม X1 = การแบ่งปันข้อมูลร่วมกัน X2 = การไว้ใจ X3 = ความร่วมมือกันในการสื่อสาร X4 = การสร้างความรู้ร่วมกัน X5 = แรงจูงใจจากภายนอก X6 = ช่องโหว่ภายใน X7 = การรับมือภัยคุกคาม X8 = บุคลากร X9 = กระบวนการ X10 = เทคโนโลยี Y1 = ความคล่องตัว Y2 = ความทนทาน Y3 = แผนความต่อเนื่อง Y4 = แผนกู้คืน Y5 = การจัดการวิกฤต Y6 = การจัดการเหตุฉุกเฉิน



รูปที่ 1 โมเดลปัจจัยเชิงโครงสร้างที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน สำหรับวิสาหกิจขนาดกลางและขนาดย่อม

2. การจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชนมีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน มีอิทธิพลทางตรงเชิงลบและทางอ้อมเชิงบวกต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน และมีอิทธิพลทางอ้อมเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจ

3. การจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชนมีอิทธิพลทางตรงเชิงบวกต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน และมีอิทธิพลทางอ้อมเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจ

4. การคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนมีอิทธิพลทางตรงเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจ

ผลการศึกษาโมเดลปัจจัยเชิงโครงสร้างที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน สำหรับวิสาหกิจขนาดกลางและขนาดย่อม แสดงดังไว้ในรูปที่ 1 พบว่า

1. ปัจจัยความร่วมมือกันของดิจิทัลซัพพลายเชน (Path Coefficient = 0.11) ปัจจัยการจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชน (Path Coefficient = 0.03) และปัจจัยการการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน (Path Coefficient = 0.83) เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน

2. ปัจจัยความร่วมมือกันของดิจิทัลซัพพลายเชน (Path Coefficient = 0.39) และปัจจัยการจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชน (Path Coefficient = 0.59) เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน

3. ปัจจัยการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน (Path Coefficient = 0.98) เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการจัดการความต่อเนื่องทางธุรกิจ

4. อภิปรายและสรุป

ความร่วมมือกันของดิจิทัลซัพพลายเชน มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน ซึ่งสอดคล้องกับผลการศึกษาของ Banomyong [14] ที่พบว่าความร่วมมือทางด้านเทคโนโลยีไม่ได้มองแต่ในเรื่องของการ

เปลี่ยนแปลงทางด้านวัฒนธรรมเท่านั้น จำเป็นต้องตระหนักถึงการไว้วางใจซึ่งกันและตลอดจนการแบ่งปันข้อมูลร่วมกัน ด้วยรวมไปถึงต้องหันมาสนใจต่อการดำเนินงานภายใน เพื่อที่จะได้รับมือกับการทำงานที่จะต้องติดต่อกับองค์กรที่อยู่ภายนอก เพราะข้อมูลที่เป็นความลับของบริษัทที่เพิ่มขึ้นจะทำให้เกิดการรั่วไหลของความรู้และการรั่วไหลของข้อมูลมากขึ้น

การจัดการภัยคุกคามทางไซเบอร์ มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน ซึ่งสอดคล้องกับงานวิจัยของ Hassell และคณะ [15] ที่พัฒนาชุดเครื่องมือในการสร้างแบบจำลองการป้องกันภัยคุกคามและช่องโหว่ทางไซเบอร์ เพื่อใช้ในการประเมินระบบและเครือข่ายเพื่อการพัฒนาให้เกิดการคืนสภาพได้ทางไซเบอร์ โดยในงานวิจัยได้มุ่งเน้นศึกษาถึงการนำเอาผลที่เกิดจากการภัยคุกคามและช่องโหว่มาเพื่อเป็นกระบวนการเริ่มต้นในการออกแบบและพัฒนาวิธีการในการรับมือ โดยการสร้างตัวชี้วัดที่จะนำมาใช้ในการประเมินผลที่จะเกิดขึ้นต่อการคืนสภาพได้ของระบบเพื่อให้การออกแบบและการกำหนดค่าของขีดความสามารถของระบบในการรองรับการทำงานในสภาพไซเบอร์อย่างเหมาะสมสำหรับระบบและเครือข่ายต่อไปได้

การจัดการความเสี่ยงทางไซเบอร์ มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน ซึ่งสอดคล้องกับงานวิจัยของ Tupa และคณะ [16] การทำงานภายใต้โครงสร้างพื้นฐานด้านไอทีที่ซับซ้อน ความเสี่ยงอาจเกิดขึ้นได้ซึ่งเป็นผลมาจากว่าการทำงานร่วมกันระหว่างคน กระบวนการ และเทคโนโลยี ที่ได้กลายเป็นเครือข่ายที่มีความซับซ้อนมากขึ้น

การคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน มีอิทธิพลโดยตรงต่อการจัดการความต่อเนื่องทางธุรกิจ ซึ่งสอดคล้องกับ Urciuoli [17] ทำการศึกษาโดยพบว่ากลยุทธ์การจัดการความเสี่ยงและการคืนสภาพได้ของดิจิทัลซัพพลายเชน มีบทบาทสำคัญในการสร้างความมั่นใจในความการจัดการความต่อเนื่องทางธุรกิจ และความน่าเชื่อถือในลักษณะของการประหยัดต้นทุน การป้องกันหรือการกู้คืนจากการหยุดชะงักของระบบ ต้องการการเข้าถึงและการวิเคราะห์ข้อมูลจำนวนมากๆ ดังนั้น จากการที่มีผลประโยชน์สำหรับผู้ที่มีส่วนได้ส่วนเสียจากการดำเนินงานและบริบทด้านต่าง ๆ ที่เกี่ยวกับดิจิทัลซัพพลายเชน จึงต้องทำการคืนสภาพได้ทางไซเบอร์อันเป็นสิ่งที่ท้าทายในการสร้างความต่อเนื่องทางธุรกิจต่อดิจิทัลซัพพลายเชน

จากผลการศึกษาโมเดลปัจจัยตัวแปรเชิงสาเหตุที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน พบว่า ความร่วมมือกันของดิจิทัลซัพพลายเชน การจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชน และการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน เป็นปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน รวมไปถึงความร่วมมือกันของดิจิทัลซัพพลายเชน และการจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชน เป็นปัจจัยที่มีผลต่อการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน อีกทั้งการคืนสภาพได้ทางไซเบอร์ของดิจทัลซัพพลายเชนยังเป็นปัจจัยที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจ

ข้อเสนอแนะในการวิจัยครั้งต่อไป

1) ควรให้มีการศึกษาถึงแนวทางและร่วมเร่งขับเคลื่อนดำเนินการเปลี่ยนผ่านทางดิจิทัล (Digital Transformation) ของเอสเอ็มอีโดยคำนึงถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์

2) ควรพัฒนาระดับวุฒิภาวะความสามารถสำหรับสร้างการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลในเอสเอ็มอี

3) ควรให้มีการนำผลการวิจัยนี้ไปขยายผลหรือปรับใช้กับภาคธุรกิจของแต่ละประเภทของเอสเอ็มอี ซึ่งจะมีบริบทหรือคุณลักษณะที่แตกต่างกันออกไป

เอกสารอ้างอิง

[1] Trend Micro Incorporated. (2015, May). *Bad ads and zero-days: Reemerging threats challenge trust in supply chains and best practices*. [Online]. Available: https:// www.trendmicro.com/vinfo/kr/security/research-and-analysis/threat-reports/roundup/bad-ads-and-zero-

days-reemerging-threats-challenge-trust-in-supply-chains-and-best-practices

[2] P. M. Swafford, S. Ghosh, and N. Murthy, "The antecedents of supply chain agility of afirm: Scale development and model testing," *Journal of Operations Management*, vol. 24, no. 2, pp. 170–188, 2006.

[3] Y. Meepetchdee and N. Shah, "Logistical network design with robustness and complexity considerations," *International Journal of Physical Distribution & Logistics Management*, vol. 37, no.3, pp. 201–222, 2007.

[4] A. Luma, B. Abazi, B. Selimi, and M. Hamiti, "Comparision of maturity model frameworks in information security and their implementtation," in *Proceedings International Conf on Engineering Technologies (ICENTE'18)*, Konya, Turkey, 2018, pp.102–104.

[5] M. Christopher and H. Peck, "Building the resilient supply chain," *The International Journal of Logistics Management*, vol. 15, no. 2, pp. 1–13, 2004.

[6] M. Windelberg, "Objectives for managing cyber supply chain risk," *International Journal of Critical Infrastructure Protection*, vol. 12, pp. 4–11, 2016.

[7] A. Ali, A. Mahfouz, and A. Arisha, "Analysing supply chain resilience: Integrating the constructs in a concept mapping frame-work via a systematic literature review," *Supply Chain Management*, vol. 22, no. 1, pp. 16–39, 2017.

[8] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, 2017.

[9] N. Setthachotsombat, V. U-on, and R. Kaewthammachai, "Supply chain agility and supply chain resilience: An implementation for supply chainof computer industry in Thailand," *Academic Journal Phranakhon Rajabhat University*, vol. 8, no.1, pp. 116–127, 2017.

[10] J. F. Hair, W. C. Black, B. J.Babin, and R. E. Anderson, *Multivariate Data Analysis A Global Perspective*, 7th ed., Pearson, 2010.

[11] S. Karnchanawasri, *Applied Statistics for Behavioral Research*, 3rd ed., Bangkok: Chulalongkron University Press, (2002) (in Thai).

[12] L. Petchroj and A. Chamniprasas, *Research Methodology*. Bangkok: Pimdeekarnpim, 2002 (in Thai).

[13] B. M. Byrne, *Structural Equation Modeling with AMOS*, 2nd ed., Taylor & Francis Group, (2010).

[14] R. Banomyong, "Collaboration in supply chain management: A resilience perspective," International Transport Forum Discussion Paper, no. 2018–22, 2018.

[15] S. Hassell, P. Beraud, A. Cruz, and G. Ganga, "Evaluating network cyber resiliency methods using cyber threat, vulnerability and defense modeling and simulation," presented at MILCOM 2012–2012 IEEE Military Communications Conference, 29 Oct.–1 Nov., 2012.

[16] J. Tupa, J. Simota, and F. Steiner, "Aspects of risk management implementation for Industry 4.0," *Procedia Manufacturing*, vol. 11, pp. 1223–1230, 2017.

[17] L. Urciuoli. "Cyber resilience: A strategic approach for supply chain management," *Technology Innovation Management* Review, vol. 5, no. 4, 2013.