การวิเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ

กิตติศักดิ์ จันทร์นิเวศน์[1*] และ ชัยวัฒน์ อุตตมากร[1]

[1]สาขาวิชาการบริหารเทคโนโลยี วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
*zkittisak@outlook.com

บทคัดย่อ

งานวิจัยในครั้งนี้มีวัตถุประสงค์เพื่อวิเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ เป็นงานวิจัยเชิงปริมาณ กลุ่มตัวอย่างที่ใช้ในการศึกษาคือพนักงานบริษัทกลุ่มน้ำมันและก๊าซในเขตพื้นที่จังหวัดกรุงเทพมหานคร ชลบุรี และระยอง จำนวน 500 คน สุ่มตัวอย่างแบบเจาะจง เครื่องมือที่ใช้ในการวิจัยคือแบบสอบถาม โดยมีการทดสอบความเที่ยงตรงเชิงเนื้อหา และความน่าเชื่อถือของแบบสอบถาม สำหรับการวิเคราะห์ข้อมูลใช้เทคนิคการวิเคราะห์องค์ประกอบเชิงสำรวจ เพื่อระบุองค์ประกอบร่วม และจัดกลุ่มองค์ประกอบใหม่

ผลการวิจัยพบว่าปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ ประกอบด้วย 3 ปัจจัย 8 กลุ่มองค์ประกอบ ได้แก่ ปัจจัยทัศนคติด้านการรักษาความมั่นคงปลอดภัย ประกอบไปด้วย 3 กลุ่มองค์ประกอบ คือ 1) ทัศนคติด้านปัญญา 2) ทัศนคติด้านอารมณ์ความรู้สึก และ 3) ทัศนคติด้านพฤติกรรม ปัจจัยด้านนโยบายขององค์กร ประกอบไปด้วย 3 องค์ประกอบ ได้แก่ 1) การข่มขู่ ยับยั้ง ลงโทษ 2) การตรวจสอบและประเมินผล และ 3) การฝึกอบรมและให้ความรู้ และ ปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ประกอบไปด้วย 2 องค์ประกอบ คือ 1) ความรู้ในการใช้งานระบบสารสนเทศ และ 2) ความรู้ความเข้าใจในการรักษาความปลอดภัยจากการคุกคามทางไซเบอร์

คำสำคัญ: นโยบายขององค์กร การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ความตั้งใจ

The Component of Factors Affecting Intention to Implement Corporate Cyber Security Policy in Oil and Gas Companies

Kittisak Channewes [1*] and Chaiwat Oottamakorn[1]

[1]Technology management College of innovation Thammasat University
* zkittisak@outlook.com

Abstract

The purpose of this study was to study the components of factors affecting intention to implement corporate cyber security policy in oil and gas companies. This study applied quantitative research methods, collect data from 500 employees of oil and gas companies in the areas of Bangkok, Chonburi and Rayong that were randomly selected by a purposive sampling, which is to collect data via online closed-ended questionnaire with content validity testing and the reliability. The data were analyzed using exploratory component analysis techniques to define complementary factors and regroup factors.

The result revealed that component analysis of factors affecting intention to implement corporate cyber security policy in oil and gas companies, consist of three factors and eighth components: three components of attitude toward information security is the cognitive component, the affective component and the behavioral component; three components of corporate policy is deterrence, analysis and evaluation and training; two components of knowledge of information security is known information system and known cyber threat & comprehension

Keywords: Corporate Policy, Cybersecurity, Intention

1. บทนำ

ในปัจจุบันความก้าวหน้าและอรรถประโยชน์ของเทคโนโลยีดิจิทัลได้ถูกนำมาใช้ในการบริหารจัดการงานต่าง ๆ ภายในองค์กรทุกภาคส่วน ทั้งภาครัฐและเอกชนมีการปรับเปลี่ยนระบบการดำเนินงานเข้าสู่ยุคดิจิทัลเพื่อเพิ่มประสิทธิภาพการทำงาน [1] ซึ่งทางรัฐบาลไทยได้กำหนดนโยบายแผนแม่บทหลักในการ พัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศระยะ 20 ปี (พ.ศ. 2561 – 2580) ให้มีการขับเคลื่อนประเทศสู่ความยั่งยืนโดย ใช้เทคโนโลยีดิจิทัล จึงมีการใช้ประโยชน์จากเทคโนโลยีดิจิทัลที่หลากหลายยิ่งขึ้น เช่น การใช้อินเทอร์เน็ตในการศึกษาหาความรู้ผ่านการเรียนออนไลน์ การใช้เพื่อความบันเทิง (เช่น ดูละครย้อนหลัง ดูหนัง หรือฟังเพลง) การเรียน การค้นคว้าหาความรู้หรือพัฒนาตนเอง (เช่น การเรียนภาษาอังกฤษออนไลน์) และการใช้เพื่อทำธุรกรรมทางการเงิน (เช่น การโอนหรือชำระเงินค่าสินค้าที่สั่งซื้อ ออนไลน์ผ่านอินเทอร์เน็ต) [2] ซึ่งจากการศึกษาลึกลงไปถึงรายละเอียดด้านเวลา พบว่า ประชากรชาวไทยมีการใช้เวลากับอินเทอร์เน็ต 9.06 ชั่วโมงต่อวัน ซึ่งแบ่งได้เป็นการใช้อินเทอร์เน็ตผ่านมือถือ 5.28 ชั่วโมงต่อวัน และ ใช้อินเทอร์เน็ตผ่านคอมพิวเตอร์ 3.38 ชั่วโมงต่อวัน อย่างไรก็ตาม

จากการที่ประชาชนสามารถเข้าถึงและใช้บริการ ด้านข้อมูลผ่านอินเทอร์เน็ตได้อย่างสะดวก รวดเร็ว ไม่จำกัดเวลาและสถานที่ ทำให้เกิดความสะดวกสบายในการบริหารจัดการ และการดำรงชีวิตเพิ่มขึ้น [3] แต่ขณะเดียวกันอาจมีการใช้อินเทอร์เน็ตที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ (Cyber Threats) ซึ่งเป็นภัยคุกคามที่ไร้พรหมแดน มีหลากหลายรูปแบบ เช่น การพยายามบุกรุกเข้าระบบ การโจมตีระบบการพัฒนาโปรแกรมที่ไม่พึงประสงค์ การเผยแพร่ข้อมูลที่ไม่เป็นความจริง โดยการสร้างเว็บไซต์ปลอมเพื่อการหลอกลวง เป็นต้น ซึ่งการละเมิดข้อมูลทำให้ธุรกิจต้องเสียค่าใช้จ่ายโดยเฉลี่ยประมาณ 3.7 ล้านดอลลาร์ และคาดว่าค่าใช้จ่ายทั้งหมดของอาชญากรรมไซเบอร์จะสูงถึง 6 ล้านล้านดอลลาร์ในปี 2564 วิธีการโจมตีทางไซเบอร์ที่เติบโตเร็วที่สุดคือผ่านแรนซัมแวร์ ซึ่งเป็นมัลแวร์ประเภทหนึ่งที่คาดว่าจะเพิ่มขึ้นอย่างต่อเนื่องในอีกไม่กี่ปีข้างหน้าแม้แต่ผู้ที่มีทักษะการเขียนโปรแกรมเพียงเล็กน้อยหรือไม่มีเลยก็สามารถทำการโจมตีการรักษาความปลอดภัยทางไซเบอร์เหล่านี้ได้ เนื่องจากส่วนหนึ่งมาจากชุดโจมตีแรนซัมแวร์ที่ได้มาอย่างง่ายดายบนดาร์กเว็บ (Techsauce, 2565)

จากการรวบรวมข้อมูลพบว่า ในปี 2563 ประเทศอเมริกาเสียจำนวนเงินค่าไถ่ที่เกิดจากการโจมตีทางอินเทอร์เน็ตมูลค่าเกือบ 350 ล้านดอลลาร์ของสกุลเงินดิจิทัล ซึ่งเพิ่มขึ้น 311% เมื่อเทียบกับปี 2562 จากการสรุปสถิติภัยคุกคามประจำปี 2564 จาก ศูนย์ปฏิบัติการ CSOC ของ NT cyfence ซึ่งเป็นศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ พบว่า ในปี 2564 นับได้ว่าเป็นปีแห่งเทคโนโลยีและ Cybersecurity ภัยคุกคามต่าง ๆ ได้เกิดขึ้นมากมายไม่ว่าจะเป็นการโจมตีทางไซเบอร์ (Cyber Attack) ข้อมูลลูกค้า/องค์กรหลุดสู่สาธารณะ (Data Breach) รวมถึงการละเมิดความเป็นส่วนตัว การหลอกลวงจากการฟิชชิ่ง (Phishing) หรือแม้แต่ช่องโหว่ Zero Day [5] จากรายงานปัญหาภัยคุกคามข้อมูลสารสนเทศที่เกิดขึ้นดังกล่าว ทำให้ทราบถึงต้นเหตุสำคัญที่ทำให้เกิดอาชญากรรมทางไซเบอร์มากที่สุด ที่มักจะเกิดจากการกระทำที่รู้เท่าไม่ถึงการณ์ของพนักงานในองค์กร [6] ซึ่งในปี 2564 เว็บไซต์ threatpost.com อ้างถึงผลงานวิจัยของ intezer บริษัทด้านความมั่นคงปลอดภัยไซเบอร์ เมื่อ 8 ก.ค. 2564 ว่า บริษัทน้ำมันและก๊าซธรรมชาติมักตกเป็นเป้าหมายหลักในการโจรกรรมข้อมูลทางไซเบอร์โดยใช้วิธีการโจมตีแบบหลอกลวงเฉพาะเจาะจง (Spear-Phishing) ในการใช้อีเมลที่แนบไฟล์อันตราย เมื่อผู้เปิดอีเมลมีการเปิดไฟล์แนบที่ส่งมาด้วยจะถูกมัลแวร์เข้าไปฝังไว้ในเครื่องทำให้แฮกเกอร์สามารถเข้ามาขโมยจากระยะไกล Remote Access Trojan (RATs) เป้าประสงค์ของมัลแวร์คือการเข้าไปขโมยข้อมูลที่สำคัญ เช่น ข้อมูลธนาคาร ข้อมูลเว็บบราวเซอร์ และ การจดบันทึกข้อมูลต่าง ๆ ขององค์กร [7]

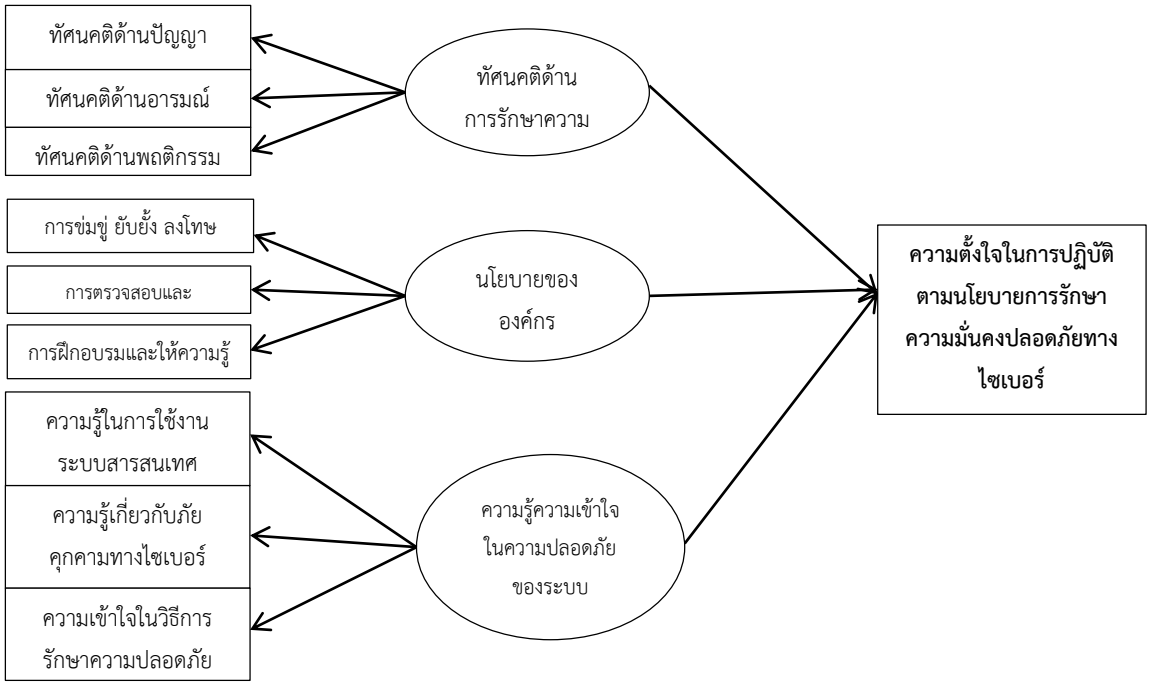
จากที่มาและความสำคัญข้างต้น ผู้วิจัยจึงมีความสนใจที่จะศึกษาองค์ประกอบขององค์ประกอบของปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ เพื่อนำผลการศึกษามาเสนอแนะ เป็นแนวทางในการสนับสนุนการลงทุน และพัฒนาบุคลากร สร้างระบบการความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพได้ต่อไป

2. วัตถุประสงค์ของการวิจัย

เพื่อวิเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ

3. กรอบแนวคิด

จากการทบทวนวรรณกรรมและเอกสารที่เกี่ยวข้องนำมาซึ่งกรอบแนวคิดได้ดังภาพที่ 1



ภาพที่ 1 กรอบแนวคิดในการวิจัย

4. การทบทวนวรรณกรรมและเอกสารที่เกี่ยวข้อง

ในงานวิจัยนี้ผู้วิจัยประยุกต์ใช้แนวคิดทฤษฎีที่เกี่ยวข้อง ดังนี้

4.1 ทัศนคติด้านการรักษาความมั่นคงปลอดภัย (Attitude toward information security) คือ การที่บุคคลมีความรู้สึกทั้งในแง่บวกและแง่ลบต่อการมีส่วนร่วมในการรักษาความมั่นคงปลอดภัย บุคคลสามารถรับรู้ทัศนคติที่มีต่อการรักษาความมั่นคงปลอดภัยได้จากสถานที่ บุคคล กิจกรรม หรือสิ่งต่าง ๆ ภายในองค์กร นักจิตวิทยา สนับสนุนการแบ่งทัศนคติออกเป็น 3 องค์ประกอบ [8] [9] คือ

1. องค์ประกอบด้านปัญญา (The Cognitive Component) คือ ส่วนที่เป็นความเชื่อของบุคคลที่เกี่ยวข้องกับการมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ หากบุคคลที่มีความรู้หรือคิดว่าการมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยนั้นดีจริงก็มักจะมีทัศนคติที่ดีต่อสิ่งนั้น แต่ถ้าหากรู้มาก่อนว่าไม่ดีก็จะมีทัศนคติที่ไม่ดีต่อสิ่งนั้น

2. องค์ประกอบด้านอารมณ์ ความรู้สึก (The Affective Component) คือ ส่วนที่เกี่ยวข้องกับอารมณ์ที่เกี่ยวเนื่องและต่อเนื่องกับการมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งจะมีผลแตกต่างกันไปตามบุคลิกภาพและค่านิยมของแต่ละบุคคล

3. องค์ประกอบด้านพฤติกรรม (The Behavioral Component) คือ การแสดงออกของบุคคลหนึ่งต่อการมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเป็นผลมาจากองค์ประกอบด้านปัญญา อารมณ์ และความรู้สึก

4.2 นโยบายขององค์กร (Corporate Policy) หมายถึง ลักษณะที่องค์กรระบุไว้อย่างกว่างขวางเพื่อให้องค์กรบรรลุเป้าหมายและวัตถุประสงค์อย่างมีประสิทธิภาพ ตลอดจนการกำหนดรูปแบบในการปฏิบัติการและการวางแผนควบคุมกลยุทธ์เพื่อให้การดำเนินงานขององค์กรประสบผลสำเร็จ [10]

1. การข่มขู่ ยับยั้ง ลงโทษ (Deterrence) หมายถึง กระบวนการในการลงโทษผู้กระทำผิดหรือผู้ฝ่าฝืนกฎแนวปฏิบัติขององค์กรจนก่อให้เกิดความเสี่ยงในการดำเนินงานขององค์กร เป็นนโยบายที่ทุกองค์กรจำเป็นต้องมี เพื่อข่มขวัญหรือป้องกันไม่ให้คนอื่นในองค์กรกระทำผิดแบบเดียวกัน เพราะเกรงกลัวต่อการถูกลงโทษ [11]

2. การตรวจสอบและประเมินผล (analysis and evaluation) หมายถึง กระบวนการพิจารณาทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ องค์กรตามรอบระยะเวลาที่กำหนดตามแผน และประเมินถึงผลลัพธ์ของการปฏิบัติงานเพื่อให้มั่นใจในความเหมาะสม ความเพียงพอของนโยบายองค์กร และ เพื่อประสิทธิผลที่มีอย่างต่อเนื่อง [12]

3. การฝึกอบรมและให้ความรู้ (Training) หมายถึง การฝึกอบรมและให้ ความรู้ด้านการรักษาความมั่นคงปลอดภัย ซึ่งเป็นสิ่งที่ต้องจัดทำ และจำเป็นสำหรับองค์กรในการ ดำเนินการฝึกอบรมการรักษาความมั่นคงปลอดภัย เพื่อให้พนักงานทราบถึงวิธีการรักษาความมั่นคง ปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร [13]

4.3 ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Knowledge of information security) หมายถึง การประยุกต์ใช้ความรู้เดิมและการทำความเข้าใจร่วมกัน หรืออธิบายเปรียบเทียบในหัวข้อประเด็นต่างๆได้อย่างมีเหตุผล ในเรื่องของระบบการรักษาความด้านเทคโนโลยีสารเทศ ซึ่งประกอบไปด้วย [14]

1. ความรู้ในการใช้งานระบบสารสนเทศ (Known information system) หมายถึง ความรู้ในการใช้งานระบบสารสนเทศอย่างถูกต้อง และนำความรู้ที่เก็บรวบรวมมาใช้ดัดแปลง อธิบาย เปรียบเทียบในเรื่องนั้นๆ ได้อย่างมีเหตุผล

2. ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ (Known cyber threat) หมายถึง ความรู้เกี่ยวกับรูปแบบต่างๆ ของภัยคุกคามทางไซเบอร์รวมถึงการรับรู้และเข้าใจถึงรูปแบบการโจมตีทางสารสนเทศที่อาจจะเกิดขึ้นได้

3. ความเข้าใจในวิธีการรักษาความปลอดภัย (Comprehension) หมายถึง ความเข้าใจในการป้องกันและแก้ไขเพื่อป้องกันการโจมตี อันจะก่อให้เกิดความเสียหายต่อข่าวสารข้อมูลที่บรรจุอยู่ในหน่วยความจำของระบบสารสนเทศ

จากการทบทวนวรรณกรรมงานวิจัยที่เกี่ยวข้อง ที่ Ameen et al. (2021) [15] ได้ทำการศึกษา การรักษาข้อมูลของลูกค้าให้ปลอดภัย: การศึกษาข้ามวัฒนธรรมเกี่ยวกับการปฏิบัติตามข้อกำหนดความปลอดภัยทางไซเบอร์ในหมู่พนักงาน Gen-Mobile พบว่า พนักงานที่มีทัศนคติที่ดีต่อการรักษาความปลอดภัยทางไซเบอร์ จะมีผลต่อการปฏิบัติตามข้อกำหนดในการรักษาความปลอดภัยทางไซเบอร์ที่ดียิ่งขึ้น อีกทั้งการศึกษาของ (Kweon et al., 2021) [16] ที่ได้ทำการศึกษา ประโยชน์ของการฝึกอบรมด้านความปลอดภัยข้อมูลและการศึกษาเกี่ยวกับเหตุการณ์ด้านความปลอดภัยในโลกไซเบอร์: หลักฐานเชิงประจักษ์ ยังพบว่า การมีความรู้ความเข้าใจในการรักษาความปลอดภัยจะช่วยให้องค์กรสามารถลดความเสี่ยงและลดผลกระทบจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อองค์กรได้ และการศึกษาของ (Li et al., 2019) [17] ที่ศึกษาเรื่อง อิทธิพลของการรับรู้นโยบายความปลอดภัยทางไซเบอร์ต่อพฤติกรรมความปลอดภัยทางไซเบอร์ของพนักงาน พบว่า เมื่อพนักงานทราบนโยบายและขั้นตอนการรักษาความปลอดภัยของข้อมูลของบริษัท พวกเขาก็จะมีความสามารถในการจัดการงานด้านความปลอดภัยทางไซเบอร์มากกว่าพนักงานที่ไม่ทราบนโยบายความปลอดภัยทางไซเบอร์ของบริษัทของตน จึงเป็นที่มาของการศึกษา

5. วิธีดำเนินการวิจัย

การวิจัยครั้งนี้ ใช้ระเบียบวิธีวิจัยเชิงปริมาณ (Quantitative Research) ซึ่งมีขั้นตอนดำเนินงานวิจัยดังนี้

5.1 ประชากรและกลุ่มตัวอย่าง กลุ่มตัวอย่างคือ พนักงานบริษัทกลุ่มน้ำมันและก๊าซ ในเขตพื้นที่จังหวัดกรุงเทพมหานคร ชลบุรี และระยอง มีการกำหนดขนาดตัวอย่างตามหลักเกณฑ์การกำหนดขนาดกลุ่มตัวอย่างของ Lindeman, Merenda และ and Gold (1980) [18] โดยการประมาณค่าพารามิเตอร์ด้วยวิธี Maximum Likelihoods ซึ่งการกำหนดกลุ่มตัวอย่างควรมีค่าประมาณ 20 เท่าของตัวแปรสังเกตได้จากงานวิจัย จึงกำหนดกลุ่มตัวอย่างเป็นจำนวน 500 ตัวอย่าง ซึ่งถือว่าไม่ต่ำกว่าจำนวนขั้นต่ำที่ควรศึกษา และใช้วิธีการสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling)

5.2 เรื่องมือที่ใช้ในการวิจัย เครื่องมือที่ใช้ในการวิจัยครั้งนี้ เป็นแบบสอบถามที่สร้างขึ้นตามวัตถุประสงค์ที่ตั้งไว้โดยแบ่งออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 ข้อคำถามเกี่ยวกับข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ประกอบไปด้วย 7 ข้อคำถาม ได้แก่ เพศ อายุ อายุงานในองค์กร ระดับการศึกษาสูงสุด รายได้ต่อเดือน แผนกที่ปฏิบัติงานอยู่ และ ระดับตำแหน่งงาน

ส่วนที่ 2 ข้อคำถามเกี่ยวกับปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ มีลักษณะแบบสอบถามเป็นแบบปลายปิดแบบมาตราส่วนประมาณค่า (Rating Scales) 5 ระดับของ Likert

ส่วนที่ 3 ข้อคำถามเกี่ยวกับความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่ม oil and gas มีลักษณะแบบสอบถามเป็นแบบปลายปิดแบบมาตราส่วนประมาณค่า (Rating Scales) 5 ระดับของ Likert

5.3 การทดสอบคุณภาพเครื่องมือ ในการทดสอบคุณภาพเครื่องมือที่ใช้ในการเก็บข้อมูลวิจัยครั้งนี้ ได้นำเอาเครื่องมือที่ใช้ในการวิจัยมาตรวจสอบความเที่ยงตรง (Validity) และความเชื่อมั่น (Reliability) ดังนี้

5.3.1 นำแบบสอบถามที่ได้ออกแบบให้ผู้เชี่ยวชาญที่มีความรู้ ความเชี่ยวชาญ หรือมีประสบการณ์ในการปฏิบัติงานด้านการรักษาความปลอดภัยทางไซเบอร์ จำนวน 5 คน ตรวจสอบความเที่ยงตรงของวัตถุประสงค์ เนื้อหา และภาษาที่ใช้ หลังจากนั้นนำข้อเสนอแนะของผู้เชี่ยวชาญมาปรับปรุงเนื้อหาข้อคำถามแต่ละข้อของแบบสอบถามให้มีความเหมาะสมตรงตามวัตถุประสงค์ของคำถามวิจัย โดยมีดัชนีความสอดคล้อง (IOC) อยู่ระหว่าง 0.60 – 1.00

5.3.2 การทดสอบหาค่าความเชื่อมั่น โดยคณะผู้วิจัยได้นำเอาแบบสอบถามที่ผ่านการตรวจจากผู้เชี่ยวชาญไปทำการทดสอบกับกลุ่มคล้ายตัวอย่าง จำนวน 30 ราย แล้วนำมาหาค่าความเชื่อมั่นโดยใช้สัมประสิทธิ์แอลฟาของครอนบาคเพื่อดูความเชื่อมั่นว่าอยู่ในระดับที่ยอมรับได้หรือไม่ โดยค่าสัมประสิทธิ์แอลฟาของครอนบาคของตัวแปรทัศนคติด้านการรักษาความมั่นคงปลอดภัย มีค่าเท่ากับ 0.756 ตัวแปรนโยบายขององค์กร มีค่าเท่ากับ .811 ตัวแปรความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ มีค่าเท่ากับ 0.882 ตัวแปรความตั้งใจ มีค่าเท่ากับ 0.886 และรวมทั้งแบบสอบถาม มีคำเท่ากับ 0.851

จากการทดสอบคุณภาพเครื่องมือในการเก็บข้อมูลนั้นผ่านเกณฑ์การทดสอบทั้ง 2 ข้อ

5.4 การเก็บรวบรวมข้อมูล ในการเก็บรวบรวมข้อมูล ผู้วิจัยทำการเก็บรวบรวมข้อมูลหลังจากปรับปรุงคุณภาพของแบบสอบถาม เก็บข้อมูลจากกลุ่มตัวอย่างจนครบตามจำนวน 500 ราย

5.5 ระยะเวลาในการเก็บข้อมูล ระยะเวลาในการเก็บข้อมูลในช่วงเดือนกันยายน 2565 – พฤศจิกายน 2565

5.6 การวิเคราะห์ข้อมูล ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยนำข้อมูลจากแบบสอบถามไปวิเคราะห์ข้อมูลด้วยคอมพิวเตอร์โดยใช้โปรแกรมสำเร็จรูป SPSS version 25 โดยใช้สถิติในการวิเคราะห์ข้อมูล ดังนี้

5.6.1 การวิเคราะห์ข้อมูลปัจจัยส่วนบุคคลของผู้ตอบแบบสอบถามโดยการหาค่าความถี่ (frequency) และค่าร้อยละ (percentage)

5.6.2 การวิเคราะห์ระดับทัศนคติด้านการรักษาความมั่นคงปลอดภัย นโยบายขององค์กร ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ และระดับความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร โดยใช้ค่าเฉลี่ย (mean) และส่วนเบี่ยงเบนมาตรฐาน (standard deviation) จากนั้นนำคะแนนเฉลี่ยมาแปลความหมาย

5.6.3 การวิเคราะห์องค์ประกอบของตัวแปรปัจจัยที่มีผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่ม oil and gas ผู้วิจัยใช้การวิเคราะห์ข้อมูลด้วยสถิติเชิงอนุมาน (Inferential Statistics) ด้วยเทคนิคการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) เพื่อวิเคราะห์หาองค์ประกอบร่วม (Common Factor) และจัดกลุ่มองค์ประกอบใหม่

6. ผลการวิจัย

1. ผู้ตอบแบบสอบถามจำนวน 500 คน พบว่า ส่วนใหญ่เป็นเพศชาย จำนวน 266 คน คิดเป็นร้อยละ 53.2 อายุระหว่างต่ำกว่า 30 ปี 279 คน คิดเป็นร้อยละ 55.8 อายุงานในองค์กรระหว่าง น้อยกว่า 3 ปี จำนวน 277 คนคิดเป็นร้อยละ 45.4 มีระดับการศึกษาปริญญาตรี จำนวน 424 คิดเป็นร้อยละ 84.8 ปฏิบัติงานอยู่ในแผนกผลิต/ควบคุมคุณภาพ จำนวน 78 คน คิดเป็นร้อยละ 15.6 ตำแหน่งงานระดับพนักงาน จำนวน 188 คิดเป็นร้อยละ 37.6

2. การวิเคราะห์องค์ประกอบเชิงสำรวจ (EFA) ใช้วิธีการสกัดองค์ประกอบด้วยวิธี Principal Components และการหมุนแกนด้วยวิธี Varimax ของกลุ่มปัจจัยทัศนคติด้านการรักษาความมั่นคงปลอดภัย (Attitude toward information security) จากผลการวิเคราะห์ พบว่า สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบเดิม คือ 3 องค์ประกอบ ได้แก่ 1) ทัศนคติด้านปัญญา (The Cognitive Component) 2) ทัศนคติด้านอารมณ์ความรู้สึก (The Affective Component) และ 3) ทัศนคติด้านพฤติกรรม (The Behavioral Component) ค่า KMO ได้ค่าเท่ากับ 0.683 และได้ค่า p-value เท่ากับ 0.00 สามารถอธิบายข้อมูลได้ร้อยละ 63.290 ทุกข้อคำถาม (ตัวแปร) มีค่า communalities มากกว่า 0.5 และ ค่า factor loading แสดงดังตารางที่ 1

ตารางที่ 1 แสดงค่า rotated factor matrix ของกลุ่มตัวแปรด้านปัจจัยทัศนคติด้านการรักษาความมั่นคงปลอดภัย (Attitude toward information security)

ข้อ	ข้อคำถาม (Item)	factor loading		
1	ท่านมีความเข้าใจในบทบาทหน้าที่ของพนักงานในการรักษาความปลอดภัยทางไซเบอร์ให้กับองค์กร			.750
2	ท่านสามารถดำเนินงานตามขั้นตอนการรักษาความปลอดภัยทางไซเบอร์ได้อย่างถูกต้อง			.802
3	ท่านคิดว่าการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งสำคัญต่อองค์กร			.758
4	ท่านมีความสุขเมื่อได้ปฏิบัติงานตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร		.747	
5	ท่านมีความภาคภูมิใจเมื่อท่านสามารถป้องกันไม่ให้ข้อมูลถูกโจรกรรมได้		.797	
6	ท่านมีความเต็มใจเป็นอย่างยิ่งที่จะช่วยรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กร		.807	
7	ท่านจะหลีกเลี่ยงการติดตั้งโปรแกรมอื่น ๆ ที่ไม่เกี่ยวข้องกับการปฏิบัติงานบนคอมพิวเตอร์ที่ท่านรับผิดชอบ	.812		
8	ท่านติดตั้งโปรแกรมสแกนไวรัสไว้ที่เครื่องคอมพิวเตอร์ของท่าน และทำการอัพเดตอยู่ตลอดเวลา	.781		
9	ท่านจะไม่เปิดอ่านไฟล์เอกสารที่แนบมากับอีเมล์หากเนื้อหาในอีเมล์นั้นดูน่าสงสัย	.843		

3. การวิเคราะห์องค์ประกอบเชิงสำรวจ (EFA) ใช้วิธีการสกัดองค์ประกอบด้วยวิธี Principal Components และการหมุนแกนด้วยวิธี Varimax ของกลุ่มปัจจัยด้านนโยบายขององค์กร (Corporate Policy) จากผลการวิเคราะห์ พบว่า สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบเดิม คือ 3 องค์ประกอบ ได้แก่ 1) การข่มขู่ ยับยั้ง ลงโทษ (Deterrence) 2) การตรวจสอบและประเมินผล (analysis and evaluation) และ 3) การฝึกอบรมและให้ความรู้ (Training) ค่า KMO ได้ค่าเท่ากับ 0.833 และได้ค่า p-value เท่ากับ 0.00 สามารถอธิบายข้อมูลได้ร้อยละ 72.040 ทุกข้อคำถาม (ตัวแปร) มีค่า communalities มากกว่า 0.5 และ ค่า factor loading แสดงดังตารางที่ 2

ตารางที่ 2 แสดงค่า rotated factor matrix ของกลุ่มตัวแปรด้านนโยบายขององค์กร (Corporate Policy)

ข้อ	ข้อคำถาม (Item)	factor loading		
1	หากท่านฝ่าฝืนกฎระเบียบที่องค์กรกำหนดและถูกจับได้ ท่านจะได้รับการลงโทษอย่างรุนแรงทันที		.839	
2	เมื่อท่านไม่ทำในสิ่งที่กำหนดไว้ในกฎระเบียบขององค์กรท่านมีแนวโน้มที่จะได้รับการลงโทษ		.833	
3	หัวหน้างานของท่านจะว่ากล่าวตักเตือนหรือกระทำการใด ๆ ซึ่งแสดงให้เห็นถึงความเข้มงวดในกฎระเบียบที่องค์กรกำหนดขึ้น		.861	
4	องค์กรของท่านจะลงโทษบุคคลที่นำทรัพยากรทางคอมพิวเตอร์ขององค์กรไปใช้เพื่อประโยชน์ส่วนตัว		.789	
5	องค์กรของท่านมีการจัดประชุมให้เข้าร่วมเพื่อหารือกับคณะทางานความมั่นคงปลอดภัยทางไซเบอร์อยู่เสมอ	.779		
6	องค์กรของท่านมีการตรวจสอบทรัพย์สินที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่ท่านรับผิดชอบอยู่อย่างสม่ำเสมอ	.828		
7	องค์กรของท่านมีการตรวจสอบแนวทางการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานอยู่เสมอ	.887		
8	องค์กรของท่านมีการประเมินเพื่อหาแนวทางการป้องกันภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ	.863		
9	องค์กรของท่านมีการทบทวน ติดตาม และตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง	.861		
10	องค์กรของท่านมีการให้ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กรอยู่เสมอ			.881
11	องค์กรของท่านมีการฝึกอบรมวิธีการใช้สารสนเทศอย่างปลอดภัย			.784
12	ท่านได้รับความรู้จากเพื่อนร่วมงานหรือหัวหน้างานในด้านการใช้งานระบบสารสนเทศที่ปลอดภัยอย่างเพียงพอ			.868

4. การวิเคราะห์องค์ประกอบเชิงสำรวจ (EFA) ใช้วิธีการสกัดองค์ประกอบด้วยวิธี Principal Components และการหมุนแกนด้วยวิธี Varimax ของกลุ่มปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Knowledge of information security) จากผลการวิเคราะห์ พบว่า สามารถจัดกลุ่มองค์ประกอบใหม่ได้ 2 องค์ประกอบ โดยองค์ประกอบแรก คือ ความรู้ในการใช้งานระบบสารสนเทศ (Known information system) โดยประกอบไปด้วยข้อคำถาม ทั้งหมด 2ข้อ ได้แก่ KIS1 และ KIS2 องค์ประกอบที่สอง คือ ความรู้ความเข้าใจในการรักษาความปลอดภัยจากการคุกคามทางไซเบอร์

(Known cyber threat & Comprehension) ประกอบไปด้วยข้อคำถาม ทั้งหมด 4 ข้อ ได้แก่ KCT1, KCT2, COM1 และ COM2 ค่า KMO ได้ค่าเท่ากับ 0.675 และได้ค่า p-value เท่ากับ 0.00 สามารถอธิบายข้อมูลได้ร้อยละ 68.454 ทุกข้อคำถาม (ตัวแปร) มีค่า communalities มากกว่า 0.5 และ ค่า factor loading แสดงดังตารางที่ 3

ตารางที่ 3 แสดงค่า rotated factor matrix ของกลุ่มตัวแปรด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Knowledge of information security)

ข้อ	ข้อคำถาม (Item)	factor loading	
1	ท่านคิดว่าเพื่อนร่วมงานของท่านมีอิทธิพลต่อการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรของท่าน		.894
2	ท่านคิดว่าหัวหน้างานของท่านมีอิทธิพลต่อการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรของท่าน		.886
3	เพื่อนร่วมงานของท่านจะให้การยอมรับท่านหากท่านปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรได้เป็นอย่างดี	.767	
4	หัวหน้างานของท่านจะให้การชื่นชมท่านหากท่านปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรได้เป็นอย่างดี	.812	
5	คนในองค์กรของท่านจะให้ความเคารพท่านเมื่อท่านสามารถปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรได้เป็นอย่างดี	.804	
6	การที่ท่านสามารถปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยขององค์กรได้เป็นอย่างดีจะทำให้ท่านได้รับการยอมรับจากหัวหน้างานภายในองค์กร	.783	

7. อภิปรายผล

ผลการวิจัยเคราะห์องค์ประกอบของปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในบริษัทกลุ่มน้ำมันและก๊าซ พบว่า

กลุ่มปัจจัยทัศนคติด้านการรักษาความมั่นคงปลอดภัย (Attitude toward information security) จากผลการวิเคราะห์ พบว่า สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบเดิม คือ 3 องค์ประกอบ ได้แก่ 1) ทัศนคติด้านปัญญา (The Cognitive Component) 2) ทัศนคติด้านอารมณ์ความรู้สึก (The Affective Component) และ 3) ทัศนคติด้านพฤติกรรม (The Behavioral Component) สอดคล้องกับ Krech et al. [8] และ Triandis [9] ที่ได้ทำการศึกษาและระบุว่า ทัศนคติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กรนั้น ประกอบไปด้วย 3 องค์ประกอบ ได้แก่ 1) องค์ประกอบด้านปัญญาที่เกิดจากความรู้หรือความคิดของบุคคลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร 2) องค์ประกอบด้านอารมณ์ ความรู้สึก จะมีผลแตกต่างกันไปตามบุคลิกภาพและค่านิยมของแต่ละบุคคล และ 3) องค์ประกอบด้านพฤติกรรม เป็นการแสดงออกของบุคคล ที่เป็นผลมาจากองค์ประกอบด้านปัญญา อารมณ์ และความรู้สึก โดยที่การศึกษาของ Ameen et al. (2021) [15] ยังได้กล่าวว่า พนักงานที่มีทัศนคติที่ดีต่อการรักษาความปลอดภัยทางไซเบอร์ จะมีผลต่อการปฏิบัติตามข้อกำหนดในการรักษาความปลอดภัยทางไซเบอร์ที่ดียิ่งขึ้นอีกด้วย

กลุ่มปัจจัยด้านนโยบายขององค์กร (Corporate Policy) จากผลการวิเคราะห์ พบว่า สามารถจัดกลุ่มองค์ประกอบได้ในรูปแบบเดิม คือ 3 องค์ประกอบ ได้แก่ 1) การข่มขู่ ยับยั้ง ลงโทษ (Deterrence) 2) การตรวจสอบและประเมินผล (analysis and evaluation) และ 3) การฝึกอบรมและให้ความรู้ (Training) สอดคล้องกับ Beccaria [11] ที่ได้กล่าวว่า การข่มขู่ ยับยั้ง ลงโทษผู้กระทำผิดหรือฝ่าฝืนกฎแนวปฏิบัติขององค์กรเป็นนโยบายที่ทุกองค์กรจำเป็นต้องมีเพื่อข่มขวัญหรือป้องกันไม่ให้คนอื่นในองค์กรกระทำผิดแบบเดียวกัน อีกทั้งยังสอดคล้องกับ Tyler [12] ที่ได้ระบุว่า การตรวจสอบและ

ประเมินผลเป็นนโยบายขององค์กรที่ใช้ในการพิจารณาทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรตามรอบระยะเวลาที่กำหนดตามแผนและประเมินถึงผลลัพธ์ของการปฏิบัติงานเพื่อให้มั่นใจในความเหมาะสมและความเพียงพอของนโยบายองค์กร และสอดคล้องกับ Gadzama et al. [13] ที่ได้กล่าวว่า นโยบายการฝึกอบรมและให้ความรู้ด้านการรักษาความมั่นคงปลอดภัยเป็นสิ่งที่ต้องจัดทำและจำเป็นสำหรับองค์กรในการดำเนินการฝึกอบรมการรักษาความมั่นคงปลอดภัยเพื่อให้พนักงานทราบถึงวิธีการรักษาความมั่นคง ปลอดภัยต่อการใช้ระบบสารสนเทศในองค์กร อีกทั้ง ผลการศึกษาของ Li et al., (2019) [17] ยังพบว่า เมื่อพนักงานทราบนโยบายและขั้นตอนการรักษาความปลอดภัยของข้อมูลของบริษัทพวกเขาก็จะมีความสามารถในการจัดการงานด้านความปลอดภัยทางไซเบอร์มากกว่าพนักงานที่ไม่ทราบนโยบายความปลอดภัยทางไซเบอร์ของบริษัทของตน

กลุ่มปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ (Knowledge of information security) จากผลการวิเคราะห์ พบว่า สามารถจัดกลุ่มองค์ประกอบใหม่ได้ 2 องค์ประกอบ คือ 1) ความรู้ในการใช้งานระบบสารสนเทศ (Known information system) และ 2) ความรู้ความเข้าใจในการรักษาความปลอดภัยจากการคุกคามทางไซเบอร์ (Known cyber threat & Comprehension) สอดคล้องกับ Son and Jeong [14] ที่ผลการวิจัยพบว่า ความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ประกอบไปด้วย ความรู้ในการใช้งานระบบสารสนเทศ และ ความรู้ความเข้าใจในการรักษาความปลอดภัยจากการคุกคามทางไซเบอร์ ส่งผลให้เกิดการประยุกต์ใช้ความรู้เดิมและการทำความเข้าใจร่วมกัน หรืออธิบายเปรียบเทียบในหัวข้อประเด็นต่าง ๆ ได้อย่างมีเหตุผล ในเรื่องของระบบการรักษาความด้านเทคโนโลยีสารเทศ อีกทั้ง ผลการศึกษาของ Kweon et al. (2021) [16] ยังพบว่า การมีความรู้ความเข้าใจในการรักษาความปลอดภัยจะช่วยให้องค์กรสามารถลดความเสี่ยงและลดผลกระทบจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อองค์กรได้

8. ข้อเสนอแนะ

8.1 ข้อเสนอแนะจากการวิจัย

8.1.1 ปัจจัยทัศนคติด้านการรักษาความมั่นคงปลอดภัย ประกอบไปด้วย 1) ทัศนคติด้านปัญญา 2) ทัศนคติด้านอารมณ์ความรู้สึก และ 3) ทัศนคติด้านพฤติกรรม ดังนั้น ผู้บริหาร หรือหัวหน้าฝ่ายที่มีความเกี่ยวข้องกับการรักษาความปลอดภัยและการอบรมพนักงานโดยกระตุ้นให้พนักงานเกิดทัศนคติทั้งในด้านปัญญา ความคิด อารมณ์ ความรู้สึก จนเกิดเป็นการแสดงพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างถูกต้องเหมาะสม ด้วยการฝึกอบรม การจัดสร้างนโยบายที่เคร่งครัด สร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์

8.1.2 ปัจจัยด้านนโยบายขององค์กร (Corporate Policy) ประกอบไปด้วย 1) การข่มขู่ ยับยั้ง ลงโทษ 2) การตรวจสอบและประเมินผล และ 3) การฝึกอบรมและให้ความรู้ ดังนั้น เพื่อให้พนักงานเกิดความตั้งใจในการรักษาความปลอดภัยทางไซเบอร์ขององค์กร ผู้บริหารและฝ่ายงานที่เกี่ยวข้องต้องมีการกำหนดนโยบายขององค์กรที่มุ่งเน้นให้ความสำคัญกับการข่มขู่ ยับยั้ง ลงโทษ พนักงานที่ฝ่าฝืนกฎระเบียบข้อบังคับอย่างเคร่งครัด อีกทั้งยังต้องหมั่นทำการตรวจสอบประเมินผลระดับการรักษาความปลอดภัยทางไซเบอร์ของพนักงานอยู่เสมอ เพื่อให้พนักงานพัฒนาระดับการรักษาความปลอดภัยของตนเอง และประเด็นสุดท้ายคือการให้ความสำคัญกับการฝึกอบรม และให้ความรู้แก่พนักงาน เพื่อให้ทราบถึงอันตรายและผลกระทบที่อาจเกิดขึ้นหากไม่รักษาความปลอดภัยทางไซเบอร์อย่างเคร่งครัด

8.1.3 ปัจจัยด้านความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ ประกอบไปด้วย 1) ความรู้ในการใช้งานระบบสารสนเทศ และ 2) ความรู้ความเข้าใจในการรักษาความปลอดภัยจากการคุกคามทางไซเบอร์ ดังนั้น ผู้บริหารและฝ่ายงานที่เกี่ยวข้องต้องมุ่งเน้นพัฒนากระบวนการสร้างความรู้ความเข้าใจในความปลอดภัยของระบบสารสนเทศ เพื่อให้เกิดการตระหนักถึงภัยอันตรายที่อาจเกิดขึ้นได้หากมีการฝ่าฝืนข้อบังคับ หรือไม่รักษาความปลอดภัย เพื่อให้พนักงานเกิดความระมัดระวังมากขึ้น

8.2 ข้อเสนแนะในงานวิจัยครั้งต่อไป

8.2.1 การศึกษาในครั้งนี้เป็นการศึกษาในบริบทพื้นที่จังหวัดกรุงเทพมหานคร ชลบุรี และระยอง ซึ่งยังเป็นข้อจำกัดในด้านพื้นที่ ที่อาจส่งผลให้ผลการศึกษาไม่ครอบคลุมได้ ดังนั้น การศึกษาในครั้งต่อไปควรศึกษาในเขตพื้นที่อื่นๆ เพื่อให้ผลการศึกษามีความหลากหลายมากขึ้น

8.2.2 การศึกษาครั้งต่อไปควรทำการทบทวนวรรณกรรมใหม่ ๆ เพิ่มเติม เพื่อค้นหาปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร เพื่อหาปัจจัยและองค์ประกอยอื่น ๆ ที่ส่งผลให้พนักงานปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรได้

9. เอกสารอ้างอิง

[1] Dutta, S., Geiger, T., & Lanvin, B. (2015). The global information technology report 2015. In *World Economic Forum,* 1(1), 80-85.

[2] Surachai Chatchalermpun and Therdpong Daengsi. (2020). CYBERSECURITY AWARENESS LEVEL IMPROVEMENT FOR EMPLOYEES IN ANORGANIZATION : A CASE OF PHISHING ATTACK SIMULATION. *Journal of Science and Technology Thonburi University*, 4(2), 1-11. (In Thai)

[3] Irfan, M., Putra, S. J., & Ramdhani, M. A. (2019, March). The readiness model of information technology implementation among universities in Indonesia. *In Journal of Physics: Conference Series*, 1175(1), 1-10.

[4] Techsauce. (2022). *Cyber Security of 2022 that organizations and consumers should not ignore*. Techsauce. https://techsauce.co/news/vmware-trend-cyber-security-2022/(In Thai)

[5] Cyfence. (2022). 2021 *Annual Threat Statistics Summary from NT cyfence CSOC Operations Center*. NT cyfence. https://www.cyfence.com/article/ntcyfence-csoc-summary-2021/(In Thai)

[6] Kanussanun Thongkum. (2018). *Factors Influencing Officer's Intention to abide by Information Security Policy: A Case Study of Rai Khing Town-municipality, Samphran District, Nakhon Pathom*. [Master of Science]. Thammasat University. (In Thai)

[7] National Intelligence Agency Thailand. (2022, June 2). *Energy infrastructure is a target for data theft*. Nia. https://www.nia.go.th/cyber/cyberpage/475/(In Thai)

[8] Krech, D., Crutchfield, R. S., & Ballachey, E. L. (1962). *Individual in society: A textbook of social psychology*. McGraw-Hill.

[9] Triandis, H. C. (1971). *Attitude and Attitude Change*. Wiley.

[10] Trang, S., & Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, 21, 1265-1284.

[11] Beccaria, C. (1764). *On crimes and punishments* (H. Paolucci, 1963, Trans.). Pearson Education Limited.

[12] Tyler, R. W. (1950). *Basic principles of curriculum and instruction*. University of Chicago Press. Wallace.

[13] Gadzama, G.B., Bawa, S.B., Ajinoma, Z., Saidu, M.M., Umar, A.S. (2014). Injection safety practices in a main referral hospital in northeastern Nigeria. *Nigerian Journal of Clinical Practice*,17(2), 134-139.

[14] Son, H. J., and Jeong, S. (2013). A Research on Security Awareness and Countermeasures for the Single Server. *International Journal of Security and Its Applications*, 7(6), 31-42.

[15] Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, 114, 106531.

[16] Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: an empirical evidence. *Information Systems Frontiers*, 23, 361-373.

[17] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13-24.

[18] Lindeman, R.H., Merenda, P.F., and Gold, R.Z. (1980). *Introduction to Bivariate and Multivariate Analysis.* Foreman and Company.