การพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย

Development of Cyber Security Legal Measures for Insurance Company

ปัญม์ณิสาธ์ องค์ปรัชญากุล[1]
Pannisa Ongprachayakul

Received: December 15, 2023
Revised: January 19, 2024
Accepted: January 25, 2024

บทคัดย่อ

บทความวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาความเป็นมาและสภาพปัญหา แนวคิด ทฤษฎี การรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย 2) ศึกษาองค์กรและกฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย และ 3) เสนอแนะแนวทางการพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย วิธีดำเนินการวิจัย การวิจัยเชิงคุณภาพ แบบการวิจัยเอกสาร ผลการวิจัย พบว่า 1) อาชญากรรมด้านไซเบอร์เกิดขึ้นเริ่มมีการพัฒนาใช้คอมพิวเตอร์และการสื่อสารทางอินเตอร์เน็ตในประเทศทั่วโลกรวมทั้งประเทศไทย ปัญหาภัยไซเบอร์ในธุรกิจประกันภัยเกิดจากอาชญากรไซเบอร์หรือความผิดพลาดทุจริตของบุคลากรของบริษัทประกันภัยและกลุ่มเครือข่ายในธุรกิจประกันภัย แนวคิดหลักการมาตรการทางกฎหมาย หลักการมาตรการทางจริยธรรม และแนวคิดรูปแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ ซึ่งเป็นระบบสถาปัตยกรรมที่มีขั้นตอนการตรวจสอบการเข้าระบบอย่างเข้มงวด นำมาใช้บูรณาการเป็นแนวทางการพัฒนาเรื่องนี้ได้ 2) กฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย พบว่า มีกฎหมายและยุทธศาสตร์ชาติที่เกี่ยวข้อง 7 ฉบับ องค์กรที่เกี่ยวข้องกับการประกันภัย 6 องค์กร และ 3) สำนักงาน

[1] มหาวิทยาลัยเกริก; Krirk University
Corresponding author, e-mail: pantip2ong@gmail.com

คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) แก้ไขเพิ่มเติมประกาศให้สอดคล้องกับการกำกับบริษัทประกันภัย และออกประกาศใหม่ใช้กำกับควบคุมตัวแทนประกันภัย นายหน้าประกันภัย อย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ องค์กรที่เกี่ยวข้องกับการประกันภัย 6 องค์กร กำหนดนโยบาย แผนงาน กฎ ระเบียบ กติกา บริหารจัดการ การอบรม การตรวจสอบภายใน บริษัทและตัวบุคคลร่วมกันอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์

คำสำคัญ: ความปลอดภัย, ไซเบอร์, บริษัทประกันภัย, มาตรการทางกฎหมาย

Abstract

The objectives of this research article were 1) to study the background and rationale, concepts, and theories of cyber security related to insurance company; 2) to study organizations and laws related to cyber security of insurance company; and 3) to suggest guidelines to develop cyber security legal measures for insurance company. This was a qualitative research using document research. The results of the research found that 1) cybercrime has occurred with the development of computers and internet communications in countries all over the world, including Thailand. Cyber threats in the insurance business were caused by cybercriminals or fraudulent mistakes by insurance company personnel and insurance network groups. Concepts, principles, legal measures, principles of ethical measures and the concept of a strict security system based on zero trust which was an architectural system with strict login verification procedures can be used and integrated as a guideline for developing this matter. 2) cyber security laws for insurance company found that there were 7 related national laws and strategies, 6 insurance related organizations; and 3) the Office of the Insurance Commission (OIC) amended has announced this to be in line with insurance company supervision and issued new announcements to control insurance agents, insurance brokers strictly based on zero trust. Six insurance-related organizations set policies, plans, rules, regulations, management, training, and internal audits. Companies and individuals worked together strictly on the basis of zero trust.

Keywords: Security, Cyber, Insurance Company, Legal Measure

บทนำ

แนวโน้มภัยคุกคามทางไซเบอร์ทั่วโลกขยายตัวเพิ่มขึ้นกว่าหนึ่งเท่าตัวนับตั้งแต่เกิดการแพร่ระบาดของเชื้อไวรัสโควิด-19 ตามปริมาณการใช้งานออนไลน์ของธุรกิจและผู้ใช้งานที่สูงขึ้น โดยส่วนหนึ่งเป็นผลมาจากการทำงานระยะไกล (Remote Working) รวมถึงหลายองค์กรมีการปรับเปลี่ยนรูปแบบการดำเนินธุรกิจไปสู่ดิจิทัลมากขึ้น องค์กรทั่วโลกกำลังเผชิญกับภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเติบโตตามปริมาณการใช้งานออนไลน์ที่เพิ่มขึ้นเช่นกัน (พันธ์ศักดิ์ เสตเสถียร, 2564) ในครึ่งแรกของปี 2023 การโจมตีทางไซเบอร์ที่พุ่งเป้าไปที่หน่วยงานภาครัฐเพิ่มมากขึ้น จากรายงาน Atlas VPN มีเหตุการณ์การโจมตีทางไซเบอร์ที่สำคัญ ที่มุ่งเป้าไปที่หน่วยงานของรัฐ 49 เหตุการณ์สำคัญ เพิ่มขึ้นถึง 11% จากช่วงเวลาเดียวกันของปีก่อน การโจมตีดังกล่าวได้ส่งผลกระทบต่อหน่วยงานของรัฐในอย่างน้อย 27 ประเทศทั่วโลก (CYBER ELITE CO. LTD, 2566)

บริษัท CNA Financial ซึ่งเป็นบริษัทประกันภัยที่ใหญ่ที่สุดแห่งหนึ่งของสหรัฐอเมริกา ได้รับรายงานว่าได้รับผลกระทบจาก Sophisticated Ransomware เมื่อวันที่ 21 มีนาคม 2021 การโจมตีทางไซเบอร์ทำให้พนักงาน และส่วนบริการลูกค้าของบริษัทต้องหยุดดำเนินงานเป็นเวลาสามวันเพื่อป้องกันความเสียหายเพิ่มเติม บริษัทประกันภัยได้โพสต์ข้อความบนเว็บไซต์เพื่อแจ้งให้ประชาชนทราบว่า “ยังคงมีการโจมตีด้านความปลอดภัยทางไซเบอร์ที่ซับซ้อน การโจมตีทางไซเบอร์ทำให้เครือข่ายหยุดชะงักและส่งผลกระทบต่อระบบ CNA บางระบบรวมถึงอีเมลขององค์กร” และกังวลว่าข้อมูลของผู้ถือกรมธรรม์จะรั่วไหลหลังจากการโจมตีทางไซเบอร์ CNA Financial ยังไม่ได้แจ้งผู้ที่อาจเป็นเหยื่อ เนื่องจากยังไม่สามารถระบุได้ว่าผู้โจมตีขโมยข้อมูลใดไปบ้าง (Wizberry Mobile Security Co.th, 2021)

ในช่วงสามปีที่ผ่านมา สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ). ได้ดำเนินการร่วมกับหน่วยงานกำกับในภาคการเงิน ได้แก่ ธนาคารแห่งประเทศไทย (ธปท.) และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) ในการจัดกิจกรรมทดสอบความพร้อมเพื่อรับมือภัยคุกคามทางไซเบอร์ระดับภาคการเงิน (Financial Sector Cyber Drill) เพื่อสร้างกระบวนการและทดสอบความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ที่ครอบคลุมทั้งในด้านการตอบสนอง (Response) ต่อภัยคุกคามการกู้คืนระบบ (Recovery) และมาตรการเยียวยาต่อผู้ที่ได้รับผลกระทบ รวมถึงการพัฒนาแนวทางในการรับมือได้อย่างเหมาะสมกับลักษณะความซับซ้อนของการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจ และได้จัดกิจกรรมซ้อมรับมือภัยคุกคามทางไซเบอร์สำหรับธุรกิจประกันภัย (Insurance Sector Cyber Drill) เมื่อช่วงปลายปี 2563 เพื่อทดสอบความพร้อมในการรับมือเหตุการณ์ถูกโจมตีทางไซเบอร์ของสำนักงาน

คปภ. และบริษัทประกันภัย ให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น โดยมีบริษัทประกันชีวิตเข้าร่วมกิจกรรมซ้อมรับมือภัยคุกคามทางไซเบอร์ จำนวน 22 บริษัท และบริษัทประกันวินาศภัยเข้าร่วมกิจกรรม จำนวน 52 บริษัท คิดเป็นร้อยละ 94 ของบริษัทประกันภัยทั้งหมด ทั้งนี้ สำนักงาน คปภ. ได้สร้างมาตรฐานของการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยออกประกาศ คปภ. เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต/ประกันวินาศภัย พ.ศ. 2563 รวมถึงแนวปฏิบัติ เรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของบริษัทประกันชีวิต/ประกันวินาศภัย พ.ศ. 2564 ที่มุ่งหวังให้บริษัทประกันภัยมีความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ (สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย, 2564)

เมื่อวันที่ 15 กรกฎาคม 2566 ตำรวจไซเบอร์ได้ทำการจับกุมตัวนายผดุงเกียรติ สมสู่ ผู้ต้องหาตามหมายจับศาลจังหวัดภูเก็ต พร้อมทั้งของกลางโทรศัพท์มือถือ เครื่องคอมพิวเตอร์ สมุดบัญชีธนาคาร และอุปกรณ์จัดเก็บข้อมูล ผลการตรวจค้นพบฐานข้อมูลส่วนบุคคล และพบหลักฐานว่าผู้ต้องหาเป็นธุรการดูแลระบบหลังบ้านของเว็บการพนันออนไลน์ ผู้ต้องหาให้การรับสารภาพว่ามีความรู้ความเชี่ยวชาญด้านระบบคอมพิวเตอร์ เมื่อปีที่แล้วได้เริ่มทำเว็บพนันออนไลน์ จึงได้เริ่มทำการซื้อข้อมูลและรายชื่อลูกค้ามาจากสมาชิกในกลุ่มแอบพลิเคชั่นเฟซบุ๊ก จำนวน 2,000,000 รายชื่อ ราคา 8,000 บาท เพื่อนำมาใช้ทำการตลาดโฆษณาในเว็บไซต์พนันออนไลน์ที่ดูแลอยู่ ต่อมาได้เลิกทำเว็บไซต์พนันออนไลน์ แต่ได้เริ่มนำข้อมูลรายชื่อดังกล่าวมาประกาศขายในสื่อสังคมออนไลน์ต่าง ๆ ได้ประมาณปีกว่าแล้ว มีลูกค้าเข้ามาซื้อข้อมูล 15-20 รายต่อเดือน มีรายได้เฉลี่ยเดือนละประมาณ 50,000 บาท และได้ทราบว่าลูกค้าส่วนใหญ่ซื้อข้อมูลส่วนบุคคลดังกล่าวไปใช้ในการหลอกลวงเอาทรัพย์สินจากประชาชน (ไทยรัฐออนไลน์, 2566)

การโจมตีทางไซเบอร์นั้นเริ่มที่จะตรวจจับและป้องกันได้ยากขึ้น เมื่อยังไม่ปลอดภัยมากพอ ก็ต้องใช้วิธีแก้ไขปัญหาคือ Zero Trust ซึ่งเป็นการนำเอาโซลูชันป้องกันแบบเดิมมาพัฒนาเพิ่มเติม Perimeter-Less Security โดย Zero Trust คือโครงสร้างด้านความปลอดภัยที่ผู้ใช้ทุกรายหรืออุปกรณ์ทุกเครื่องจะต้องผ่านการรับรองและตรวจสอบก่อนจะเข้าถึงระบบ แอปพลิเคชันหรือทรัพย์สินต่างๆ ของบริษัทได้ เครื่องมือตอบสนองและตรวจจับช่องทางการเข้าถึงนี้มีการขับเคลื่อนด้วยระบบ AI จึงสามารถบล็อกและแยกอันตรายจากมัลแวร์และแรนซัมแวร์ได้ (บริษัท ริโก้ (ประเทศไทย) จำกัด, 2566)

ดังนั้น ผู้วิจัยจึงสนใจศึกษาการพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย เกี่ยวกับความเป็นมาและสภาพปัญหา แนวคิด ทฤษฎี องค์กรและกฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย เพื่อนำเสนอแนวทางการพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย อันจะเป็นประโยชน์ต่อสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยได้นำไปเป็นแนวทางในการออกกฎหมายกำกับบริษัทประกันภัยและกลุ่มเครือข่ายที่เกี่ยวข้อง และบริษัทประกันภัยได้นำไปเป็นแนวทางในการพัฒนาบริหารจัดการองค์กรภายในและกลุ่มเครือข่ายที่เกี่ยวข้องได้ อันจะเป็นประโยชน์ในการพัฒนาการป้องกันข้อมูลส่วนบุคคลของประชาชนและบริษัทประกันภัย ส่งผลดีให้สังคม เศรษฐกิจ และประเทศชาติพัฒนาได้อย่างมั่นคงและเจริญก้าวหน้าต่อไป

วัตถุประสงค์

1. เพื่อศึกษาความเป็นมาและสภาพปัญหา แนวคิด ทฤษฎี การรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย

2. เพื่อศึกษาองค์กรและกฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย

3. เพื่อเสนอแนะแนวทางการพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย

วิธีดำเนินการวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) แบบการวิจัยเอกสาร (Documentary Research) กำหนดขั้นตอนการวิจัยตามวัตถุประสงค์ดังนี้

ขั้นตอนที่ 1 เก็บรวบรวมข้อมูลเอกสาร เก็บรวบรวมข้อมูลปฐมภูมิและเอกสารทุติยภูมิจากแหล่งที่มาจาก เอกสารทางวิชาการ หนังสือ งานวิจัย บทความวิชาการ บทวิเคราะห์ เกี่ยวกับแนวคิด ทฤษฎี หลักการ กฎหมาย คำพิพากษาศาลฎีกา ข่าวสาร ค่าสถิติ และเอกสารเผยแพร่ทางสื่อออนไลน์ เว็บไซต์ของส่วนราชการและเอกชน เกี่ยวกับความเป็นมาและสภาพปัญหา แนวคิด ทฤษฎี องค์กรและกฎหมายการรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย

ขั้นตอนที่ 2 ศึกษาความเป็นมาและสภาพปัญหา แนวคิด ทฤษฎี การรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย ทำการจำแนกชนิดข้อมูลออกเป็น 3 กลุ่ม คือ กลุ่มที่ 1 ความเป็นมาและสภาพปัญหาการรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย กลุ่มที่ 2

สภาพปัญหาการรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย และกลุ่มที่ 3 แนวคิด ทฤษฎี การรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย

ขั้นตอนที่ 3 ศึกษาองค์กรและกฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย ทำการจำแนกชนิดข้อมูลออกเป็น 2 กลุ่ม คือ กลุ่มที่ 1 องค์กรที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย กลุ่มที่ 2 กฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย

ขั้นตอนที่ 4 ศึกษาแนวทางการพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย รวบรวมข้อมูลประเด็นหลักสำคัญจากขั้นตอนที่ 2-3 ทำการวิเคราะห์ข้อมูล ออกเป็น 2 กลุ่ม คือ กลุ่มที่ 1 พัฒนาหลักการมาตรการทางกฎหมาย (Hard Law) บูรณาการร่วมกับแนวคิดรูปแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ (Zero Trust Model) กลุ่มที่ 2 พัฒนาหลักการมาตรการทางจริยธรรม (Soft Law) บูรณาการร่วมกับแนวคิดรูปแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ (Zero Trust Model) และสังเคราะห์ออกมาเป็นการสรุปผลการวิจัย องค์ความรู้ใหม่ และข้อเสนอแนะ

สรุปผลการวิจัย

1. ผลการวิจัยความเป็นมาและสภาพปัญหา แนวคิด ทฤษฎี การรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย พบว่า

1.1 ความเป็นมาเกี่ยวกับความปลอดภัยไซเบอร์ พบว่า อาชญากรรมด้านไซเบอร์ (Cyber Crime) หมายถึง กิจกรรมที่ผิดกฎหมายใด ๆ ที่ใช้หรือรุกรานระบบและเครือข่ายคอมพิวเตอร์ รวมไปถึงอินเทอร์เน็ต (Capgemini, 2012) สถาบันที่มีความเชี่ยวชาญด้านความปลอดภัยของข้อมูลแห่งนี้ได้สรุปว่า ความเสียหายขององค์กรอันเกิดจากอาชญากรรมด้านไซเบอร์ยังคงมีแนวโน้มเพิ่มมากขึ้นทุกปี ซึ่งการโจมตีทางไซเบอร์มากกว่า 50% มีที่มาจาก 3 สาเหตุสำคัญ คือ 1) ภัยคุกคามที่เกิดขึ้นจากคนในหรือจากฝั่งผู้ให้บริการเอง (Maliciou Insiders) 2) ภัยคุกคามบนระบบเครือข่าย อันเป็นผลมาจากการได้รับโปรแกรมที่มีจุดประสงค์ทำให้เครื่องคอมพิวเตอร์หรือระบบโครงข่ายหยุดการทำงาน (Denial of Services) และ 3) การโจมตีบนเว็บ (Web-based Attacks) ซึ่งถือได้ว่าเป็นการโจมตีที่มีอัตราการเติบโตสูงมากในปัจจุบัน โดยการฝังมัลแวร์ (Malware) หรือโปรแกรมที่ไม่พึงประสงค์ผ่านทางช่องโหว่ของ Internet Browser โดยจะเข้าไปควบคุมการทำงานของโปรแกรม Internet Browser ให้เป็นไปตามความต้องการของผู้ประสงค์ร้าย

(Ponemon Institue, 2014) การโจมตีผ่านช่องทางการให้บริการคลาวด์ (Cloud) โดยใช้มัลแวร์ (Malware) หรือแรนซัมแวร์ มีแนวโน้มจะขยายตัวอย่างต่อเนื่องในอนาคต โดยการโจมตีมักเกิดขึ้นกับระบบใดระบบหนึ่งก่อน เช่น คอมพิวเตอร์ของพนักงานจากนั้นจึงลุกลามไปยังระบบหรือส่วนงานอื่น ๆ ก่อนที่จะมุ่งเป้าไปที่การโจรกรรมข้อมูล พบว่าผู้โจมตีมักแฝงตัวเข้ามาภายในเครือข่ายของบริษัทประมาณ 6 ถึง 18 เดือนก่อนเริ่มดำเนินการโจมตี โดยจะเริ่มสำรวจข้อมูลของเครือข่ายระบบคอมพิวเตอร์ และข้อมูลส่วนบุคคล เช่น ข้อมูลพนักงาน ข้อมูลคู่ค้า และวิธีการเปลี่ยนแปลงข้อมูลของผู้ใช้งาน (User Credentials) เป็นต้น หลังจากนั้นจึงสวมรอยเป็นคู่ค้า หรือพนักงานเพื่อหลอกให้มีการโอนเงินไปยังบัญชีที่ต้องการผ่านทางอีเมล วิธีการนี้เรียกว่า Business Email Compromise (BEC) (พันธ์ศักดิ์ เสตเสถียร, 2564) รูปแบบของภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในประเทศไทยมีลักษณะที่คล้ายคลึงกับที่พบในประเทศอื่น ๆ ทั่วโลก โดยไทยเซิร์ตได้จัดแยกประเภทของภัยคุกคามด้านไซเบอร์ออกเป็น 8 ประเภท คือ 1) ภัยคุกคามจากการฉ้อฉลหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) 2) ภัยคุกคามจากโปรแกรมที่ถูกพัฒนาขึ้นเพื่อให้เป็นอันตรายต่อระบบ (Malicious Code) 3) ภัยคุกคามจากการบุกรุก (Intrusion) 4) ภัยคุกคามจากความพยายามบุกรุก (Intrusion Attempts) 5) ภัยคุกคามจากการรวบรวมข้อมูล (Information Gathering) 6) ภัยคุกคามที่เกิดจากการใช้หรือเผยแพร่ข้อมูลที่ไม่เหมาะสมหรือไม่เป็นจริง (Abusive Content) 7) ภัยคุกคามต่อการพร้อมใช้ (Availability) 8) ภัยคุกคามประเภทอื่น ๆ (Other) (ฝ่ายวิจัยและสถิติ บริษัท รับประกันภัยต่อ จำกัด (มหาชน), 2558) จึงสรุปได้ว่า อาชญากรรมด้านไซเบอร์เกิดขึ้นตั้งแต่เริ่มมีการพัฒนาใช้คอมพิวเตอร์และการสื่อสารทางอินเตอร์เน็ตในประเทศทั่วโลกรวมทั้งประเทศไทยที่ขยายตัวเพิ่มขึ้นอย่างต่อเนื่อง โดยภัยไซเบอร์เกิดจากการโจมตีจากภายนอกและบุคคลากรภายในองค์กรเอง จึงได้มีการแบ่งประเภทภัยไซเบอร์ในรูปแบบของการถูกโจมตีเพื่อใช้เป็นข้อมูลในการป้องกันรักษาความปลอดภัยทางไซเบอร์

1.2 สภาพปัญหาภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย พบว่า อุตสาหกรรมประกันภัยถือเป็นแหล่งเก็บรวบรวม ประมวลผล และจัดการข้อมูลส่วนตัวที่ระบุตัวตนลูกค้าจำนวนมาก จึงทำให้อุตสาหกรรมประกันภัยกลายเป็นเป้าหมายหลักของอาชญากรรมทางไซเบอร์ ซึ่งความปลอดภัยทางไซเบอร์สำหรับอุตสาหกรรมประกันภัยนี้ ถือเป็นสิ่งสำคัญอันดับต้น ๆ ของฝ่ายไอที อาชญากรรมทางไซเบอร์ในธุรกิจประกันภัยถือว่าร้ายแรง ซึ่งเป็นทั้งอุปสรรคและโอกาสของบริษัทประกันภัย ซึ่งก่อให้เกิดความเสียหายทั้งในรูปแบบของค่าปรับ การสูญเสียลูกค้า และการเสื่อมเสียชื่อเสียง แต่ในอีกด้านหนึ่ง ความปลอดภัยทางไซเบอร์ก็เป็นธุรกิจที่กำลังเติบโตสำหรับบริษัทประกันภัย อาชญากรจากภายนอกไม่ใช่ภัยทางไซเบอร์เพียงอย่างเดียวที่เป็นอันตรายต่อธุรกิจ

ประกันภัย บริษัทยังคงต้องต่อสู้กับกระบวนการอื่น ๆ จาก “ฝีมือมนุษย์” อีกด้วย 2022 World Economic Forum ชี้ให้เห็นว่าการรั่วไหลของข้อมูลทางไซเบอร์กว่า 95% เกิดจากความผิดพลาดโดยมนุษย์ ช่วงประมาณเดือนกรกฎาคม พ.ศ. 2564 SEC มีรายงานว่า First American Insurance Corporation บริษัทประกันภัยสำหรับอสังหาริมทรัพย์ได้เปิดเผยข้อมูลส่วนตัวและข้อมูลทางการเงินของลูกค้ากว่า 800 ราย โดยไม่ได้ตั้งใจ ซึ่งข้อมูลเหล่านั้นประกอบไปด้วย เลขประกันสังคม เลขบัญชีธนาคาร ประวัติการจำนองอสังหาริมทรัพย์ ภาษี ใบเสร็จการโอนเงินต่างประเทศ และภาพใบอนุญาตขับขี่ (บริษัท ริโก้ (ประเทศไทย) จำกัด, 2566) เมื่อวันที่ 15 กรกฎาคม 2566 ตำรวจไซเบอร์ ได้ทำการจับกุมตัว นายผดุงเกียรติ สมสู่ ผู้ต้องหาตามหมายจับศาลจังหวัดภูเก็ต พร้อมของกลางโทรศัพท์มือถือ เครื่องคอมพิวเตอร์ สมุดบัญชีธนาคาร และอุปกรณ์จัดเก็บข้อมูล ผลการตรวจค้นพบฐานข้อมูลส่วนบุคคล และพบหลักฐานว่าผู้ต้องหาเป็นแอดมินดูแลระบบหลังบ้านของเว็บการพนันออนไลน์ ผู้ต้องหาให้การรับสารภาพว่าตนเริ่มทำเว็บพนันออนไลน์ ทำหน้าที่เป็นแอดมินดูแลระบบหลังบ้าน จึงได้เริ่มทำการซื้อข้อมูลและรายชื่อลูกค้ามาจากสมาชิกในกลุ่มเฟซบุ๊ก จำนวน 2,000,000 รายชื่อ ในราคา 8,000 บาท เพื่อนำมาใช้ทำการตลาดโฆษณาเว็บพนันออนไลน์ที่ตนดูแลอยู่ จากนั้นเดือนต่อมาตนได้เลิกทำเว็บพนันออนไลน์ แต่ได้เริ่มนำข้อมูลรายชื่อดังกล่าวมาประกาศขายในสื่อสังคมออนไลน์ต่าง ๆ ลูกค้าส่วนใหญ่ซื้อข้อมูลส่วนบุคคลดังกล่าวไปใช้ในการหลอกลวงเอาทรัพย์สินจากประชาชน ต่อมาวันที่ 6 พฤศจิกายน 2566 ตำรวจไซเบอร์ได้ขยายผลจับกุมผู้ต้องหานายพศิน อายุ 41 ปี โบรกเกอร์บริษัทประกันภัย ที่นำข้อมูลลูกค้าประกันไปขายให้มิจฉาชีพ และเมื่อวันที่ 18 พฤศจิกายน 2566 ตำรวจไซเบอร์ได้นำหมายค้นศาลอาญาธนบุรีที่ 584/2566 พร้อมหมายจับศาลอาญาที่ 212/2563 เข้าจับกุมตัวนายวีรทัศน์ อายุ 45 ปี พร้อมด้วยของกลางโทรศัพท์มือถือ 2 เครื่อง นายวีรทัศน์ยอมรับว่า หลังจากช่วงแพร่ระบาดโควิด คิดหาเงินทางลัดจากการขายข้อมูลจริง โดยมีรายได้เดือนละ 100,000 บาท ทั้งนี้ ข้อมูลส่วนบุคคลที่นำมาขายส่วนมากได้รับจากคนในวงการขายประกัน เนื่องจากก่อนหน้านี้เคยเป็นเจ้าหน้าที่ของบริษัทประกันภัย ทำงานในตำแหน่งซุปเปอร์ไวเซอร์ ได้ลาออกมาประมาณ 3 ปีแล้ว แต่ยังจัดเก็บข้อมูลลูกค้าอยู่ พร้อมรับว่าเป็นผู้โพสต์ขายฐานข้อมูลลูกค้าจริง โดยนำมาเปิดเผยโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูลก่อน จึงสรุปได้ว่า ปัญหาภัยไซเบอร์ในธุรกิจประกันภัยเกิดเพิ่มมากขึ้นอย่างต่อเนื่อง เพราะธุรกิจประกันภัยเป็นธุรกิจทางการเงินที่อาชญากรไซเบอร์สนใจโจมตีก่ออาชญากรรมข้อมูลของบริษัทประกันภัย และยังเกิดจากความผิดพลาดทุจริตจากบุคคลากรของบริษัทประกันภัยและกลุ่มเครือข่ายในธุรกิจประกันภัย เช่น ตัวแทนประกันภัย นายหน้าประกันภัย เป็นผู้ก่อภัยไซเบอร์กับบริษัทประกันภัยด้วย

1.3 แนวคิดและทฤษฎีการรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย พบว่า

1) หลักการมาตรการทางกฎหมาย (Hard Law) คือ กฎ ระเบียบ ข้อบังคับของรัฐ หรือปัญหาการบังคับใช้กฎหมาย ดังนั้น Hard Law in Corporate Governance คือ กฎหมายหรือระเบียบที่รัฐได้กำหนดขึ้นเพื่อจัดการหรือควบคุมดูแลการดำเนินธุรกิจให้เป็นที่เรียบร้อยและมีประสิทธิภาพ และองค์กรธุรกิจมีหน้าที่ต้องปฏิบัติตามหรือจัดการบริหารกิจการต่าง ๆ ตามที่กฎหมายกำหนด หากองค์กรธุรกิจฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนด องค์กรธุรกิจจำต้องรับผิดตามกฎหมายนั้น (กิตสุรณ สังขสุวรรณ์, 2562)

2) หลักการมาตรการทางจริยธรรม (Soft Law) คือ หลักจริยธรรมของผู้ประกอบธุรกิจ Soft Law จะเป็นการที่รัฐสนับสนุนให้กลุ่มผู้ประกอบการออกกฎกติกาหรือมาตรฐานของตนเองเพื่อให้เกิดบริการที่ดีบังคับการกันเอง Soft law เป็นการแสดงเจตจำนงของผู้ประกอบการที่จะถือปฏิบัติในการบริการ และตกลงกันสร้างกระบวนการแก้ไขปัญหาโดยสมัครใจ เพื่อให้เกิดการบริการที่ดีต้นทุนการบังคับใช้จึงไม่มากนัก เพราะมาจากการยอมตกลงปฏิบัติและผู้บริโภคก็จะไว้วางใจผู้ประกอบการที่แสดงตนว่าจะบริการอย่างมีมาตรฐาน ซึ่งกรณีเช่นนี้ Soft Law ก็จะเข้ามาเสริม Hard Law โดยผู้ประกอบการยินยอมกระทำการเพิ่มเติมไปจากข้อบังคับของกฎหมาย เพื่อให้ตนเองมีความสามารถในทางตลาดหรือแข่งขันมากขึ้น (ธรรมนิตย์ สุมันตกุล, 2549)

3) แนวคิดรูปแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ (Zero Trust Model) รัฐบาลสหรัฐอเมริการ่วมกับสำนักความมั่นคงโครงสร้างพื้นฐานและการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity and Infrastructure Security Agency-CISA) และสำนักบริหารงบประมาณ (Office of Management and Budget-OMB) ของสหรัฐอเมริกา ผลักดันให้หน่วยงานของรัฐนำแนวคิดการออกแบบมาตรการรักษาความมั่นคงปลอดภัยแบบ “Zero Trust” มาใช้ภายในกันยายน 2567 Zero Trust เป็นแนวคิดการออกแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ การเข้าถึงทรัพยากรบนระบบเครือข่ายคอมพิวเตอร์หรือการอนุญาตให้อุปกรณ์คอมพิวเตอร์เชื่อมต่อในเครือข่ายจะต้องผ่านการตรวจสอบ (Verify) อย่างเข้มงวดทั้งการเชื่อมต่อจากภายในสำนักงานหรือภายนอกสำนักงานและปฏิบัติในลักษณะเดียวกัน โดยหน่วยงานภาครัฐต้องประยุกต์ใช้สถาปัตยกรรมแบบ “Zero Trust” ซึ่งประกอบด้วย 5 เสาหลักการพัฒนามาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้ (1) การระบุยืนยันตัวตน (Identity) (2) อุปกรณ์ (Devices) (3) เครือข่าย (Networks) (4) แอปพลิเคชัน (Applications) 5) ข้อมูล (Data) (สำนักข่าวกรองแห่งชาติ, 2566) แม้ว่าการนำโมเดลการรักษา

ความปลอดภัยแบบ Zero Trust มาใช้อาจทำให้ต้องใช้เวลาและทรัพยากร เพราะเกี่ยวข้องกับการออกแบบสถาปัตยกรรมระบบเครือข่าย (Network Architecture) ขององค์กรให้มีความมั่นคงปลอดภัยตั้งแต่แรก หรือที่เรียกว่า Secure by Design แต่ก็คุ้มค่าที่องค์กรควรให้ความสำคัญ เพราะจะช่วยปกป้องข้อมูลและระบบงานต่าง ๆ ขององค์กรได้ (ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.), 2566)

ผู้วิจัยมีความเห็นว่า แนวคิดหลักการมาตรการทางกฎหมาย (Hard Law) หลักการมาตรการทางจริยธรรม (Soft Law)) และแนวคิดรูปแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ (Zero Trust Model) นำมาใช้บูรณาการเป็นแนวทางการพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัยได้

2. ผลการวิจัยองค์กรและกฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย พบว่า

2.1 กฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย พบว่า ประเทศไทยได้ให้ความสำคัญกับภัยคุกคามทางไซเบอร์ โดยออกกฎหมายและกำหนดเป้าหมายยุทธศาสตร์ชาติของภาครัฐในการพัฒนาประเทศอย่างยั่งยืน ดังนี้ 1) ยุทธศาสตร์ชาติ พ.ศ. 2561-2880 ยุทธศาสตร์ชาติด้านความมั่นคง 2) พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 3) พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 4) พระราชบัญญัติ ประกันวินาศภัย พ.ศ. 2535 5) พระราชบัญญัติ ประกันชีวิต พ.ศ.2535 6) ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ.2563 ซึ่งข้อ 5 ของประกาศดังกล่าวกำหนดให้บริษัทต้องมีหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท ดังต่อไปนี้ 1) การกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance) 2) การบริหารโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management) 3) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) 4) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) 5) การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance) 6) การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit) 7) การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) 8) การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ (Reporting) พร้อมกันนี้ได้ออก “ประกาศคณะกรรมการกำกับและส่งเสริม

การประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต พ.ศ.2563" ในวันเดียวกันซึ่งมีข้อความหลักเกณฑ์เดียวกันบังคับใช้กับบริษัทประกันชีวิต ซึ่งประกาศทั้งสองฉบับนี้มีมาจากการที่สายพัฒนามาตรฐานกำกับ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ได้จัดทำกรอบ "แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity)" เพื่อให้บริษัทประกันวินาศภัยและบริษัทประกันชีวิตนำไปบริหารจัดการภายในของบริษัท สรุปได้ว่ากฎหมายและยุทธศาสตร์ชาติทั้งเจ็ดฉบับดังกล่าวข้างต้นนี้เป็นกฎหมายที่ออกมาเพื่อกำกับควบคุมการรักษาความปลอดภัยทางไซเบอร์ ทั้งในระดับประเทศและระดับองค์กรภาครัฐและภาคเอกชนทางด้านธุรกิจประกันภัยด้วย

2.2 องค์กรที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย พบว่า องค์กรภาครัฐและภาคเอกชนที่กำกับและสนับสนุนบริษัทประกันภัยในการรักษาความปลอดภัยไซเบอร์ได้ ดังนี้ 1) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) 2) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) 3) สมาคมประกันวินาศภัยไทย 4) สมาคมประกันชีวิตไทย 5) สมาคมนายหน้าประกันภัยไทย 6) สมาคมตัวแทนประกันชีวิตและที่ปรึกษาทางการเงิน

3. ผลการวิจัยแนวทางการพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย พบว่า

3.1 พัฒนาหลักการมาตรการทางกฎหมาย (Hard Law) บูรณาการร่วมกับแนวคิดรูปแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ (Zero Trust Model) ตามที่สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ได้ออก ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ. 2563 และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต พ.ศ. 2563 ในการกำกับให้บริษัทประกันภัยบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ แต่เป็นการใช้บังคับกับบริษัทประกันภัยเท่านั้น และตาม "ข้อ 15 บริษัทต้องมีการบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (Human Resource Security) โดยบุคลากรที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีหลักเกณฑ์ในการคัดเลือกเพื่อบรรจุเป็นพนักงาน กฎระเบียบ หรือข้อบังคับ

ระหว่างการปฏิบัติงาน และการสิ้นสุดการปฏิบัติงาน” นั้นคือบริษัทประกันภัยต้องคัดเลือกควบคุมเฉพาะบุคลากรด้านเทคโนโลยีสารสนเทศเท่านั้น แต่ไม่ได้คัดเลือกควบคุมบุคลากรของบริษัททั้งหมด จึงเกิดปัญหาว่าบุคลากรของบริษัทประกันภัยยังมีการลักลอบนำข้อมูลส่วนบุคคลของลูกค้าและข้อมูลสำคัญของบริษัทออกไปใช้ในทางทุจริตและขายให้กับอาชญากรไซเบอร์ได้ และประกาศทั้งสองฉบับยังไม่ครอบคลุมถึงกลุ่มเครือข่ายของบริษัทประกันภัยด้วยคือ ตัวแทนประกันภัย นายหน้าประกันภัย จึงทำให้เกิดปัญหาที่มีจับกุมตัวแทนประกันภัยทุจริตขายข้อมูลส่วนบุคคลของลูกค้าดังกล่าว ซึ่งเป็นปัญหาต่อเนื่องที่ข้อมูลของบริษัทประกันภัยรั่วไหล ถือเป็นความผิดพลาดบกพร่อง เป็นช่องว่างและช่องโหว่ ให้อาชญากรไซเบอร์ได้ข้อมูลสำคัญของบริษัทไปก่ออาชญากรรมทางไซเบอร์

ดังนั้นจึงควรนำหลักการ Hard Law บูรณาการกับแนวคิด Zero Trust Model ซึ่งเป็นแนวคิดจะทำให้อาชญากรรมไซเบอร์หมดไปจากบริษัทประกันภัย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย จึงควรแก้ไขเพิ่มเติมประกาศทั้งสองฉบับดังกล่าวใน ข้อ 15 ให้ครอบคลุมการควบคุมบุคลากรทั้งหมดของบริษัท โดยแก้ไขเพิ่มเติมดังนี้ *“ข้อ 15 บริษัทต้องมีการบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (human resource security) โดยบุคลากรทั้งหมดที่ปฏิบัติงานและฝ่ายบริหาร ให้มีหลักเกณฑ์ในการคัดเลือกเพื่อบรรจุเป็นพนักงานกฎระเบียบ หรือข้อบังคับระหว่างการปฏิบัติงานและการสิ้นสุดการปฏิบัติงานตามหน้าที่และการใช้สารสนเทศของบริษัทด้วย”*

พร้อมกันนี้ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยควรดำเนินการยกร่างประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของนายหน้านิติบุคคลประกันชีวิต พ.ศ.... และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของนายหน้านิติบุคคลประกันวินาศภัย พ.ศ.... ซึ่งนายหน้านิติบุคคลประกันภัยส่วนใหญ่จดทะเบียนเป็นบริษัทจำกัด มีขนาดเล็กจนถึงขนาดใหญ่ จึงเห็นว่า ควรใช้หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท ดังต่อไปนี้ 1) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) 2) การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance) 3) การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) 4) การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ (Reporting) เป็นการเพียงพอในการบริหาร

จัดการรักษาความปลอดภัยไซเบอร์ในบริษัทนายหน้านิติบุคคล โดยนำกรอบ “แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity)” ที่เคยให้บริษัทประกันวินาศภัยและบริษัทประกันชีวิตนำไปบริหารจัดการภายในของบริษัท และแนวคิดรูปแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ (Zero Trust Model) มาเป็นต้นแบบในการร่างประกาศทั้งสองฉบับดังกล่าว

3.2 พัฒนาหลักการมาตรการทางจริยธรรม (Soft Law) บูรณาการร่วมกับแนวคิดรูปแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ (Zero Trust Model)

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ควรกำกับและส่งเสริมให้บริษัทประกันภัยปฏิบัติตาม ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ.2563 และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต พ.ศ.2563 อย่างโปร่งใสให้ปรากฏผลชัดเจนอย่างรวดเร็วและต่อเนื่อง

สมาคมประกันวินาศภัยไทย และสมาคมประกันชีวิตไทย ควรร่วมกับบริษัทประกันภัยนำประกาศทั้งสองฉบับมาใช้ในการกำหนดนโยบาย จัดทำแผนงาน กฎ ระเบียบ กติการ่วมกัน ในการบริหารจัดการทุกกระบวนการภายในบริษัทในการรักษาความปลอดภัยทางไซเบอร์ และเพิ่มเติมนโนบาย แผนงาน การบริหารจัดการ การอบรม การตรวจสอบ การติดต่อรับส่งข้อมูลข่าวสารระหว่างบริษัทกับกลุ่มเครือข่าย ตัวแทนประกันภัย นายหน้าประกันภัย ที่มีการป้องกันคุ้มครองข้อมูลไม่ให้รั่วไหลหรือมีช่องโหว่ออกจากบริษัทประกันภัย

สมาคมนายหน้าประกันภัยไทย และสมาคมตัวแทนประกันชีวิตและที่ปรึกษาทางการเงิน ควรร่วมกับตัวแทนประกันภัย และนายหน้าประกันภัย ในการกำหนดนโยบาย แผนงาน การบริหารจัดการ การอบรม การตรวจสอบภายในบริษัทและตัวบุคคล และการติดต่อรับส่งข้อมูลข่าวสารระหว่างกลุ่มเครือข่ายกับบริษัทประกันภัยในการรักษาความปลอดภัยทางไซเบอร์

อภิปรายผลการวิจัย

ความเป็นมาและสภาพปัญหา แนวคิด ทฤษฎี การรักษาความปลอดภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย พบว่า ความเป็นมาเกี่ยวกับความปลอดภัยไซเบอร์นั้น อาชญากรรมด้านไซเบอร์เกิดขึ้นตั้งแต่เริ่มมีการพัฒนาใช้คอมพิวเตอร์และการสื่อสารทางอินเตอร์เน็ตในประเทศทั่วโลกรวมทั้งประเทศไทยที่ขยายตัวเพิ่มขึ้นอย่างต่อเนื่อง โดยภัยไซเบอร์เกิดจากการโจมตีจากภายนอกและบุคคลากรภายในองค์กรเอง จึงได้มีการแบ่งประเภทภัยไซเบอร์ในรูปแบบของการถูกโจมตีเพื่อใช้เป็นข้อมูลในการป้องกันรักษาความปลอดภัยทางไซเบอร์ สภาพปัญหาภัยไซเบอร์ที่เกี่ยวกับบริษัทประกันภัย พบว่า ปัญหาภัยไซเบอร์ในธุรกิจประกันภัยเกิดเพิ่มมากขึ้นอย่างต่อเนื่อง เพราะธุรกิจประกันภัยเป็นธุรกิจทางการเงินที่อาชญากรไซเบอร์สนใจโจมตีก่ออาชญากรรมข้อมูลของบริษัทประกันภัย และยังเกิดจากความผิดพลาดหรือทุจริตจากบุคลากรของบริษัทประกันภัยและกลุ่มเครือข่ายในธุรกิจประกันภัย เช่น ตัวแทนประกันภัย นายหน้าประกันภัย เป็นผู้ก่อภัยไซเบอร์กับบริษัทประกันภัยด้วย สอดคล้องกับงานวิจัยของนริส อุไรพันธ์ และคณะ (2565) พบว่า วิสาหกิจขนาดกลางและขนาดย่อมที่ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ส่วนใหญ่ทำธุรกิจ ด้านการค้าปลีกและค้าส่ง มีระยะเวลาในการดำเนินธุรกิจ 4-9 ปี มีจำนวนพนักงานในองค์กร 6-10 คน และมีระดับตลาดที่ธุรกิจให้บริการดำเนินธุรกิจภายในประเทศ พนักงานที่มีพื้นฐานความรู้ทางด้านเทคโนโลยีสารสนเทศน้อยกว่า 50% มีการทำรายงานเมื่อโดนโจมตีให้กับทางบริษัทรับทราบแต่น้อยมาก กำลังดำเนินการสร้างแผนฉุกเฉินในการรับมือต่อเหตุการณ์การโจมตีทางไซเบอร์ และพนักงานไม่ทราบว่าบริษัทของตนเองมีโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เข้มงวด

องค์ความรู้ใหม่

การพัฒนามาตรการทางกฎหมายการรักษาความปลอดภัยไซเบอร์ของบริษัทประกันภัย มาตรการทางกฎหมาย Hard Law and Zero Trust Model

1. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) แก้ไขประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ.2563 และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต พ.ศ.2563 ข้อ 15. ดังนี้ *“ข้อ 15 บริษัทต้องมีการบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (human resource security) โดยบุคลากรทั้งหมดที่ปฏิบัติงานและฝ่าย*

บริหาร ให้มีหลักเกณฑ์ในการคัดเลือกเพื่อบรรจุเป็นพนักงาน กฎระเบียบ หรือข้อบังคับระหว่างการปฏิบัติงานและการสิ้นสุดการปฏิบัติงานตามหน้าที่และการใช้สารสนเทศของบริษัทด้วย”

2. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ควรดำเนินการยกร่างประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของนายหน้านิติบุคคลประกันชีวิต พ.ศ..... และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของนายหน้านิติบุคคลประกันวินาศภัย พ.ศ..... ใช้หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท ดังต่อไปนี้ 1) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) 2) การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance) 3) การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) 4) การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ (Reporting)

หลักการมาตรการทางจริยธรรม Soft Law and Zero Trust Model

1. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) กำกับและส่งเสริมให้บริษัทประกันภัยปฏิบัติตาม ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ.2563 และประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต พ.ศ.2563 อย่างโปร่งใสให้ปรากฏผลชัดเจนอย่างรวดเร็วและต่อเนื่อง

2. สมาคมประกันวินาศภัยไทย และสมาคมประกันชีวิตไทย ร่วมกับบริษัทประกันภัยนำประกาศทั้งสองฉบับมาใช้ในการกำหนดนโยบาย แผนงาน จัดทำกฎระเบียบกติการ่วมกัน ในการบริหารจัดการภายในบริษัทในการรักษาความปลอดภัยทางไซเบอร์ และเพิ่มเติมนโยบาย แผนงาน การบริหารจัดการ การอบรม การตรวจสอบ การติดต่อรับส่งข้อมูลข้อมูลข่าวสารระหว่างบริษัทกับกลุ่มเครือข่าย ตัวแทนประกันภัย นายหน้าประกันภัยที่มีการป้องกันคุ้มครองข้อมูลไม่ให้รั่วไหลหรือมีช่องโหว่ออกจากบริษัทประกันภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์

3. สมาคมนายหน้าประกันภัยไทย และสมาคมตัวแทนประกันชีวิตและที่ปรึกษาทางการเงิน ควรร่วมกับตัวแทนประกันภัย และนายหน้าประกันภัยในการกำหนดนโยบาย แผนงาน การบริหารจัดการ การอบรม การตรวจสอบภายในบริษัทและตัวบุคคล และการติดต่อรับส่งข้อมูลข้อมูลข่าวสารระหว่างกลุ่มเครือข่ายกับบริษัทประกันภัยในการรักษาความปลอดภัยทางไซเบอร์อย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์

ข้อเสนอแนะ

จากผลการวิจัย ผู้วิจัยมีข้อเสนอแนะ ดังนี้

ข้อเสนอแนะเชิงนโยบาย

1. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ควรนำหลักการ มาตรการทางกฎหมาย Hard Law and Zero Trust Model และหลักการมาตรการทางจริยธรรม Soft Law and Zero Trust Model มาพัฒนานโยบายการออกกฎหมายหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันประกันภัย ตัวแทนประกันภัยและนายหน้าประกันภัย ให้ทำการป้องกันอาชญากรรมทางไซเบอร์ในธุรกิจประกันภัยได้อย่างครบถ้วนทุกช่องทาง

2. สมาคมประกันวินาศภัยไทย สมาคมประกันชีวิตไทย สมาคมนายหน้าประกันภัยไทย และสมาคมตัวแทนประกันชีวิตและที่ปรึกษาทางการเงิน ควรนำหลักการมาตรการทางจริยธรรม Soft Law and Zero Trust Model มากำหนดนโยบาย แผนงาน กฎ ระเบียบ กติกาที่สำคัญและเร่งด่วนในการบริหารจัดการ การแก้ไข ป้องกัน การอบรม ตรวจสอบภายในเพื่อป้องกันอาชญากรรมทางไซเบอร์ของบริษัทและตัวบุคคลร่วมกันอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์

ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

1. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ควรทำการแก้ไขเพิ่มเติม ประกาศหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันภัยทั้งสองฉบับในข้อ 15

2. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ควรดำเนินการยกร่างประกาศประกาศหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของตัวแทนประกันภัย และนายหน้าประกันภัย

เอกสารอ้างอิง

กิตสุรณ สังขสุวรรณ์. (2562). การปกป้องคุ้มครองข้อมูลส่วนบุคคลในองค์กรธุรกิจ. *วารสารบริหารธุรกิจและการบัญชี มหาวิทยาลัยขอนแก่น, 3*(3), 95-108.

ไทยรัฐออนไลน์. (2566). *จับหนุ่มวิศวกร โพสต์ขายข้อมูลส่วนบุคคล ให้กลุ่มเว็บพนัน นับล้านรายชื่อ.* เข้าถึงได้จาก https://www.thairath.co.th/news/crime/2709740

ธรรมนิตย สุมันตกุล. (2549). *New Legislative Culture: Soft Law สำนักงานคณะกรรมการกฤษฎีกา*. เข้าถึงได้จาก https://www.krisdika.go.th/data/activity/act90.pdf

นริส อุไรพันธ์ และคณะ. (2565). ปัจจัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย. *วารสารสหวิทยาการเพื่อการพัฒนา*, *12*(1), 1-19.

บริษัท ริโก้ (ประเทศไทย) จำกัด. (2566). *ธุรกิจประกันภัย: เป้าหมายหลักของอาชญากรทางไซเบอร์*. เข้าถึงได้จาก https://www.ricoh.co.th/features/the-cybercriminals-target-of-choice-in-insurance-business

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.). (2566). *Zero Trust Model เกราะคุ้มกันภัยคุกคามไซเบอร์*. เข้าถึงได้จาก https://www.sec.or.th/TH/Template3/Articles/2566/010266.pdf

ฝ่ายวิจัยและสถิติ บริษัท รับประกันภัยต่อ จำกัด (มหาชน). (2558). ความเป็นไปได้ของการประกันภัยไซเบอร์ในประเทศไทย. *วารประกันภัย สมาคมประกันวินาศภัยไทย, 30*(129), 12-13.

พันธ์ศักดิ์ เสตเสถียร. (2564). *PwC ชี้การโจมตีทางไซเบอร์ทั่วโลกเพิ่มขึ้นกว่า 1 เท่าตัวหลังเกิดโควิด-19 แนะธุรกิจไทยทำประกันภัยไซเบอร์-ลงทุนระบบรักษาความปลอดภัยเพื่อป้องกันความเสี่ยง.* เข้าถึงได้จาก https://www.pwc.com/th/en/press-room / press-release/2021/press-release-18-08-21-th.html

สำนักข่าวกรองแห่งชาติ. (2566). *สหรัฐฯ เร่งผลักดันแนวคิดการรักษาความปลอดภัยระบบคอมพิวเตอร์แบบ Zero Trust.* เข้าถึงได้จาก https://www.nia.go.th/cybe /cyber page/534/

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย. (2564). *คปภ. สร้างภูมิคุ้มกันให้ธุรกิจประกันภัยรับมือภัยคุกคามทางไซเบอร์ เพื่อก้าวข้ามอุปสรรคการดำเนินธุรกิจภายใต้ "Digital Ecosystem".* เข้าถึงได้จาก https://www2.oic.or.th/th/consumer/news/releases/91864

Capgemini. (2012). *Using Insurance to Mitigate Cybercrime Risk*. Retrieved from https://www.capgemini.com/wpcontent/uploads/2017/07/Using_Insurance_to_Mitigate_Cybercrime_Risk.pdf

CYBER ELITE CO. LTD. (2566). *ภัยคุกคามทางไซเบอร์ที่มุ่งเป้าโจมตีหน่วยงานของรัฐเพิ่มขึ้นทั่วโลกในปี 2023*. เข้าถึงได้จาก https://www.cyberelite.co.th/blog/cyberattack-gov/

Ponemon Institue. (2014). *Global Report on the Cost of Cyber Crime*. Retrieved from https://www.ponemon.org/news-updates/blog/security/2014-global-report-on-the-cost-of-cyber-crime.html

Wizberry Mobile Security Co.th. (2021). *บริษัทรับประกันภัยทาง Cyber สหรัฐอเมริกาถูกโจมตีจากSophisticated Ransomware.* เข้าถึงได้จาก https://www.wizberry.biz/topics/insurance-vcyber-attack/