

การเปิดรับสื่อ ทศนคติ และพฤติกรรมการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน)¹

กนกพร พานิชสมบัติ² และคันธริรา ฉายาวงศ์³

บทคัดย่อ

การวิจัยเรื่อง “การเปิดรับสื่อ ทศนคติ และพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน)” มีวัตถุประสงค์เพื่อศึกษาการเปิดรับสื่อภายในองค์กร ทศนคติ และพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน ปตท. รวมทั้งศึกษาความแตกต่างของการเปิดรับสื่อภายในองค์กรจำแนกตามลักษณะทางประชากร ตลอดจนศึกษาความสัมพันธ์ระหว่างการเปิดรับสื่อภายในองค์กรกับทศนคติ และความสัมพันธ์ระหว่างทศนคติกับพฤติกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ โดยใช้วิธีวิจัยเชิงสำรวจด้วยการเก็บข้อมูลด้วยแบบสอบถามออนไลน์จากพนักงานบริษัท ปตท. จำกัด (มหาชน) จำนวน 361 คน

ผลการวิจัยพบว่า กลุ่มตัวอย่างมีการเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยรวมอยู่ในระดับมาก มีค่าเฉลี่ยเท่ากับ 4.06 โดยสื่อกิจกรรมมีค่าเฉลี่ยสูงสุด รองลงมา คือ สื่อสิ่งพิมพ์ สื่อบุคคล และสื่อดิจิทัล ตามลำดับ ด้านทศนคติพบว่าอยู่ในระดับมากที่สุด มี

¹ วันที่รับบทความ 19 มิ.ย.69 / แก้ไขบทความ 23 มิ.ย.69 / ตอบรับบทความ 26 มิ.ย.69

² นักศึกษาระดับปริญญาโท คณะวารสารศาสตร์และสื่อสารมวลชน มหาวิทยาลัยธรรมศาสตร์

³ ผู้ช่วยศาสตราจารย์ ดร. คณะวารสารศาสตร์และสื่อสารมวลชน มหาวิทยาลัยธรรมศาสตร์

ค่าเฉลี่ยเท่ากับ 4.56 และด้านพฤติกรรมพบว่าอยู่ในระดับมากที่สุด มีค่าเฉลี่ยเท่ากับ 4.73

ผลการทดสอบสมมติฐานพบว่า พนักงานที่มีเพศ อายุ ระดับการศึกษา อายุงาน และพื้นที่ปฏิบัติงานแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 นอกจากนี้ การเปิดรับสื่อภายในองค์กรมีความสัมพันธ์เชิงบวกในระดับน้อยกับทัศนคติอย่างมีนัยสำคัญทางสถิติ โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.278 และทัศนคติมีความสัมพันธ์เชิงบวกกับพฤติกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.612 ผลการวิจัยสะท้อนว่าการสื่อสารภายในองค์กร โดยเฉพาะสื่อกิจกรรมและการใช้สื่อหลายประเภทอย่างเหมาะสม มีบทบาทสำคัญต่อการส่งเสริมทัศนคติและพฤติกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน

คำสำคัญ: การเปิดรับสื่อ, ทัศนคติ, พฤติกรรม, ความมั่นคงปลอดภัยทางไซเบอร์

Media Exposure, Attitudes, and Cybersecurity Behavior of Employees at PTT Public Company Limited

Kanokporn panichsombat⁴ and Kantira Chayawong⁵

ABSTRACT

The research titled “Media Exposure, Attitudes, and Cybersecurity Behavior of Employees of PTT Public Company Limited” aimed to study employees’ media exposure, attitudes, and behavior regarding cybersecurity. The study also examined differences in internal organizational media exposure classified by demographic characteristics, as well as the relationship between internal organizational media exposure and attitudes, and the relationship between attitudes and cybersecurity behavior. This study employed a quantitative survey research design. Data were collected through an online questionnaire from 361 employees of PTT Public Company Limited.

The findings revealed that the overall level of employees’ exposure to internal organizational media related to cybersecurity was at a high level, with a mean score of 4.06. Activity-based media had the highest mean score, followed by print media, personal media, and digital media, respectively. In

⁴ Master’s Student, Faculty of Journalism and Mass Communication, Thammasat University

⁵ Assistant Professor, Ph.D., Faculty of Journalism and Mass Communication, Thammasat University

terms of attitudes, the overall level was at a very high level, with a mean score of 4.56. Similarly, cybersecurity behavior was also reported at a very high level, with a mean score of 4.73.

The hypothesis testing results showed that employees with different genders, ages, educational levels, lengths of employment, and work locations had significantly different levels of exposure to internal organizational media at the 0.05 significance level. In addition, internal organizational media exposure had a low positive relationship with attitudes at a statistically significant level, with a correlation coefficient of 0.278. Attitudes were also positively related to cybersecurity behaviors, with a correlation coefficient of 0.612. The results indicate that internal organizational communication, particularly activity-based media and the appropriate use of multiple types of media, plays an important role in promoting employees' attitudes and behavior regarding cybersecurity.

Keywords: Media exposure, Attitudes, Behavior, Cybersecurity

ที่มาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีดิจิทัลและระบบสารสนเทศมีบทบาทสำคัญต่อการดำเนินงานขององค์กรทั้งภาครัฐและภาคเอกชน โดยเฉพาะองค์กรขนาดใหญ่ที่ต้องอาศัยระบบดิจิทัลในการบริหารจัดการข้อมูล การติดต่อสื่อสาร การให้บริการ และการสนับสนุนกระบวนการทำงาน อย่างไรก็ตาม การพึ่งพาระบบดิจิทัลที่เพิ่มขึ้นทำให้องค์กรต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ในหลายลักษณะ เช่น การเจาะระบบเพื่อเข้าถึงข้อมูลสำคัญ การขโมยรหัสหรือข้อมูลส่วนบุคคล การเผยแพร่ข้อมูลที่บิดเบือน การทำลายความน่าเชื่อถือขององค์กร รวมถึงการรบกวนหรือทำลายระบบคอมพิวเตอร์และอุปกรณ์ดิจิทัล ซึ่งภัยคุกคามเหล่านี้อาจส่งผลกระทบต่อได้ตั้งแต่ระดับบุคคล องค์กร เศรษฐกิจ ไปจนถึงโครงสร้างพื้นฐานสำคัญของประเทศ (สุธาเทพ รุณเรศ, 2561 อ้างถึงใน มาริสา จันเกตุ, 2566) ดังนั้น ความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นประเด็นที่องค์กรต้องให้ความสำคัญทั้งในด้านเทคโนโลยี การบริหารความเสี่ยง และการสร้างความตระหนักรู้ของบุคลากรภายในองค์กร

ในระดับสากล รายงาน Global Cybersecurity Outlook 2026 ของ World Economic Forum ระบุว่า ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศทั่วโลกกว่าร้อยละ 94 เห็นว่าเทคโนโลยีปัญญาประดิษฐ์ (AI) จะเป็นปัจจัยสำคัญที่ส่งผลกระทบต่อภูมิทัศน์ความมั่นคงปลอดภัยทางไซเบอร์ในอนาคต ขณะที่ร้อยละ 87 มองว่าความเสี่ยงด้าน AI เป็นภัยคุกคามที่เติบโตเร็วที่สุดในปัจจุบัน นอกจากนี้ รายงาน Allianz Risk Barometer 2026 ยังระบุว่า Cyber Incidents เป็นความเสี่ยงทางธุรกิจอันดับหนึ่งของโลก สะท้อนให้เห็นว่าภัยคุกคามทางไซเบอร์เป็นประเด็นสำคัญที่องค์กรทั่วโลกต้องให้ความสำคัญอย่างจริงจัง

สำหรับประเทศไทย ภัยคุกคามทางไซเบอร์มีแนวโน้มเพิ่มขึ้นและส่งผลกระทบต่อทั้งหน่วยงานภาครัฐ ภาคธุรกิจ และประชาชน โดยสถิติภัยคุกคามทางไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2569 พบว่าภัยที่พบบ่อย ได้แก่ การพยายามบุกรุกระบบ การละเมิดความมั่นคงของข้อมูล และการฉ้อโกงทางดิจิทัล สถานการณ์ดังกล่าวสะท้อนว่า ความมั่นคงปลอดภัยทางไซเบอร์ไม่ใช่เพียงปัญหาทางเทคนิค แต่เป็นประเด็นด้านการบริหารจัดการข้อมูล ความต่อเนื่องในการดำเนินงาน และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย ทั้งยังสอดคล้องกับทิศทางของประเทศไทยที่มีการกำหนดกรอบกฎหมายและนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้หน่วยงานและองค์กรต่าง ๆ สามารถป้องกัน รับมือ และลดผลกระทบจากภัยคุกคามได้อย่างเป็นระบบ

ด้วยเหตุนี้ บริษัท ปตท. จำกัด (มหาชน) ในฐานะองค์กรพลังงานของประเทศที่มีบทบาทสำคัญต่อระบบเศรษฐกิจและความมั่นคงด้านพลังงาน จึงมีการนำเทคโนโลยีดิจิทัลมาใช้สนับสนุนการดำเนินงานในหลายมิติ ส่งผลให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์กลายเป็นประเด็นสำคัญที่ต้องให้ความสำคัญควบคู่กับการดำเนินธุรกิจ ทั้งในด้านการบริหารจัดการข้อมูล การดำเนินงาน และการให้บริการ โดย ปตท. ได้กำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งดำเนินการตามแผนปฏิบัติการดิจิทัล พ.ศ. 2568–2572 เพื่อเสริมสร้างความปลอดภัยของระบบสารสนเทศและพัฒนาความตระหนักรู้ด้านไซเบอร์ให้แก่พนักงานทุกระดับผ่านช่องทางต่าง ๆ เช่น สื่อบุคคล สื่อสิ่งพิมพ์ สื่อดิจิทัล และกิจกรรมภายในองค์กร

ในด้านการเปิดรับสื่อมีองค์ประกอบเลือกเปิดรับ เลือกรับรู้ ตีความ และจดจำข้อมูลตามความสนใจ ประสบการณ์ ความเชื่อ และทัศนคติของ

ตนเอง (Klapper, 1960) ขณะเดียวกัน ด้านลักษณะทางประชากร เช่น เพศ อายุ ระดับการศึกษา อาชีพ และพื้นที่ปฏิบัติงาน ก็เป็นตัวแปรที่มีความเกี่ยวข้องกับรูปแบบการรับรู้และการเปิดรับสื่อของพนักงานแต่ละกลุ่มด้วยเช่นกัน (ประม สตะเวทิน, 2546 อ้างถึงใน วาทีณี เจริญพงษ์, 2565)

นอกจากนี้ ทักษะก็ยังเป็นปัจจัยสำคัญที่สะท้อนความเชื่อ ความคิดเห็น และการรับรู้ของพนักงานต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งอาจส่งผลต่อการตัดสินใจและการปฏิบัติตามแนวทางด้านความปลอดภัยขององค์กร ขณะที่พฤติกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นผลลัพธ์ที่แสดงออกผ่านการปฏิบัติงานจริงของพนักงาน ดังนั้น การศึกษาการเปิดรับสื่อภายในองค์กรควบคู่กับทัศนคติและพฤติกรรม จึงมีความสำคัญต่อการทำความเข้าใจว่าการสื่อสารภายในองค์กรสามารถส่งเสริมให้พนักงานเกิดความรู้ ความเข้าใจ ความตระหนัก และนำไปสู่การปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์ได้มากน้อยเพียงใด

ด้วยเหตุนี้ ผู้วิจัยจึงสนใจศึกษาการเปิดรับสื่อภายในองค์กร ทักษะ และพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน) เพื่อศึกษาระดับการเปิดรับสื่อ ทักษะ และพฤติกรรม รวมถึงเปรียบเทียบการเปิดรับสื่อจำแนกตามลักษณะทางประชากร และศึกษาความสัมพันธ์ระหว่างการเปิดรับสื่อกับทัศนคติ และความสัมพันธ์ระหว่างทัศนคติกับพฤติกรรม ทั้งนี้ ผลการวิจัยสามารถนำไปใช้เป็นแนวทางในการพัฒนาการสื่อสารภายในองค์กรให้เหมาะสมกับพนักงานแต่ละกลุ่ม และส่งเสริมพฤติกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ให้สอดคล้องกับบริบทของ ปตท. ได้อย่างมีประสิทธิภาพมากยิ่งขึ้นด้วยเหตุนี้ ผู้วิจัยจึงสนใจศึกษาการเปิดรับสื่อภายในองค์กร ทักษะ และพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด

(มหาชน) เพื่อศึกษาว่าพนักงานมีการเปิดรับสื่อด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับใด มีทัศนคติและพฤติกรรมต่อประเด็นดังกล่าวอย่างไร รวมถึงการเปิดรับสื่อมีความสัมพันธ์กับทัศนคติหรือไม่ และทัศนคติมีความสัมพันธ์กับพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์หรือไม่ โดยมุ่งหวังว่าผลการวิจัยจะสามารถนำไปใช้ในการพัฒนาการสื่อสารภายในองค์กรให้เหมาะสมกับพนักงานแต่ละกลุ่ม และส่งเสริมให้พนักงานมีความเข้าใจ ทัศนคติที่ดี และพฤติกรรมที่สอดคล้องกับแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาระดับการเปิดรับสื่อภายในองค์กร ทัศนคติ และพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน)
2. เพื่อเปรียบเทียบการเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน) จำแนกตามลักษณะทางประชากร
3. เพื่อศึกษาความสัมพันธ์ระหว่างการเปิดรับสื่อภายในองค์กรกับทัศนคติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน)
4. เพื่อศึกษาความสัมพันธ์ระหว่างทัศนคติกับพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน)

การทบทวนวรรณกรรม

การวิจัยเรื่องการเปิดรับสื่อภายในองค์กร ทักษะคิด และพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานบริษัท ปตท. จำกัด (มหาชน)

แนวคิดลักษณะทางประชากร อธิบายว่า บุคคลที่มีลักษณะพื้นฐานแตกต่างกัน เช่น เพศ อายุ ระดับการศึกษา อายุงาน และพื้นที่ปฏิบัติงาน อาจมีความสนใจ ประสบการณ์ การรับรู้ การตีความ และการตอบสนองต่อข่าวสารแตกต่างกัน กิติมา สุรสนธิ (2548) อธิบายว่า ปัจจัยด้านประชากรมีส่วนเกี่ยวข้องกับการรับรู้และการทำความเข้าใจสารของแต่ละบุคคล ขณะที่ ประมะ สตะเวทิน (2546 อ้างถึงใน ณัฐธาดา ศรีไพโรจน์, 2566) อธิบายว่า การวิเคราะห์ผู้รับสารจำนวนมากควรจำแนกตามลักษณะทางประชากรศาสตร์ เนื่องจากผู้รับสารแต่ละกลุ่มมีพื้นฐาน ประสบการณ์ และความสนใจแตกต่างกัน

สำหรับการวิจัยครั้งนี้ ลักษณะทางประชากรศาสตร์จึงถูกนำมาใช้เปรียบเทียบในการเปิดรับสื่อภายในองค์กรด้านความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน โดยจำแนกตามเพศ อายุ ระดับการศึกษา อายุงาน และพื้นที่ปฏิบัติงาน ซึ่งสะท้อนบริบทของ ปตท. ที่มีพนักงานปฏิบัติงานในพื้นที่และลักษณะงานที่หลากหลาย

แนวคิดการเลือกเปิดรับข่าวสาร (Selective Exposure Theory)

อธิบายว่า บุคคลไม่ได้เปิดรับข่าวสารทุกประเภทอย่างเท่าเทียมกัน แต่จะมีกระบวนการคัดเลือกข่าวสารตามความสนใจ ความต้องการ ประสบการณ์ ความเชื่อ และทัศนคติของตนเอง (ประมะ สตะเวทิน, 2546 อ้างถึงใน อภิษฎา เวชกิจ, 2567) โดยกระบวนการดังกล่าวประกอบด้วย 4 ขั้นตอน ได้แก่

1. การเลือกเปิดรับ (Selective Exposure) คือ การเลือกช่องทางหรือแหล่งข่าวสารที่ตนสนใจ ค้นเคย หรือเห็นว่ามีประโยชน์ต่อการดำเนินชีวิต

2. การเลือกให้ความสนใจ (Selective Attention) คือ การให้ความสนใจกับข้อมูลที่สอดคล้องกับความคิด ความเชื่อ หรือความสนใจของตน และมีกลไกเลือกข้อมูลที่ขัดแย้งกับความเชื่อเดิม
3. การเลือกรับรู้และตีความหมาย (Selective Perception and Interpretation) คือ การรับรู้และตีความข้อมูลตามประสบการณ์ ความรู้ ความเชื่อ และบริบทของแต่ละบุคคล ทำให้บุคคลอาจตีความสารเดียวกันแตกต่างกันได้
4. การเลือกจดจำ (Selective Retention) คือ การจดจำข้อมูลที่สอดคล้องกับความสนใจ ความเชื่อ และทัศนคติของตน ขณะที่ข้อมูลที่ไม่สอดคล้องอาจถูกลืมหรือให้ความสำคัญน้อยกว่า

ดังนั้น แนวคิดการเลือกเปิดรับข่าวสารสามารถอธิบายได้ว่า บุคคลจะมีการคัดเลือก เปิดรับ รับรู้ ตีความ และจดจำข้อมูลแตกต่างกันตามความสนใจ ความต้องการ ประสบการณ์ และบริบทของตนเอง ส่งผลให้แม้ได้รับข่าวสารเดียวกัน แต่ผู้รับสารแต่ละคนอาจมีระดับการรับรู้และความเข้าใจแตกต่างกันได้ แนวคิดดังกล่าวจึงสามารถนำมาใช้อธิบายการเปิดรับสื่อภายในองค์กรของพนักงานที่มีลักษณะทางประชากรแตกต่างกัน ซึ่งอาจส่งผลต่อการรับรู้ข้อมูลด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทัศนคติ และพฤติกรรมการปฏิบัติตามแนวทางด้านความปลอดภัยขององค์กร

แนวคิดการสื่อสารภายในองค์กร Grunig&Hunt (1984 อ้างถึงใน ญัฐชดา วิจิตรจามรี, 2554) อธิบายว่าการสื่อสารภายในองค์กรมีความสัมพันธ์กับโครงสร้างขององค์กร ช่วยอธิบายบทบาทของสื่อภายในองค์กรในฐานะเครื่องมือถ่ายทอดนโยบาย ข่าวสาร และแนวปฏิบัติไปยังบุคลากร เพื่อให้เกิดความเข้าใจร่วมกันและสนับสนุนการดำเนินงานขององค์กรให้เป็นไปในทิศทางเดียวกัน

สำหรับการวิจัยครั้งนี้ ผู้วิจัยจำแนกสื่อภายในองค์กรออกเป็น 4 ประเภท ได้แก่ สื่อบุคคล สื่อสิ่งพิมพ์ สื่อดิจิทัล และกิจกรรม เนื่องจากครอบคลุมทั้งการสื่อสารผ่านบุคคล การสื่อสารผ่านเอกสาร การสื่อสารผ่านเทคโนโลยี และการสื่อสารที่ส่งเสริมการมีส่วนร่วมของพนักงาน

แนวคิดด้านทัศนคติ

ธงชัย สันติวงษ์ (2535) อธิบายว่า ทัศนคติเป็นแนวโน้มของบุคคลในการประเมินสิ่งใดสิ่งหนึ่งในทางบวกหรือทางลบ และมีผลต่อแนวโน้มในการตอบสนองต่อสิ่งนั้น และอรรพรรณ ปิลันธน์โอวาท (2554) อธิบายว่า ทัศนคติเป็นตัวเชื่อมโยงระหว่างการเรียนรู้ ความคิด ความรู้สึก และพฤติกรรมของบุคคล อีกทั้งทัศนคดียังเกิดจากประสบการณ์ การเรียนรู้ ความเชื่อ ค่านิยม และการติดต่อสื่อสารกับบุคคลอื่น ดังนั้น ในบริบทของ ปตท. ทัศนคติด้านความมั่นคงปลอดภัยทางไซเบอร์จึงสะท้อนว่าพนักงานเห็นความสำคัญยอมรับ และพร้อมปฏิบัติตามแนวทางด้านความปลอดภัยขององค์กรเพียงใด

แนวคิดด้านพฤติกรรม

พฤติกรรมเป็นการแสดงออกของบุคคลทั้งในรูปของการกระทำที่สังเกตได้และการตอบสนองที่เกิดจากกระบวนการคิดภายใน โดยพฤติกรรมของบุคคลส่วนใหญ่มีพื้นฐานมาจากความรู้ ความเข้าใจ และทัศนคติที่มีต่อเรื่องนั้น ๆ (สุรพงษ์ โสธนเสถียร, 2533) กล่าวคือ เมื่อบุคคลมีความรู้และทัศนคติเชิงบวกต่อสิ่งใด ย่อมมีแนวโน้มแสดงพฤติกรรมที่สอดคล้องกับความเชื่อและทัศนคติดังกล่าว

นอกจากนี้ Ajzen (2003 อ้างถึงใน อรรพรรณ ปิลันธน์โอวาท, 2554) ได้อธิบายไว้ในทฤษฎีพฤติกรรมที่วางแผนไว้ (Theory of Planned Behavior: TPB) ว่า การแสดงพฤติกรรมของบุคคลได้รับอิทธิพลจาก 3 องค์ประกอบสำคัญ ได้แก่ ทัศนคติต่อพฤติกรรม การคล้อยตามกลุ่มอ้างอิง

และการรับรู้ความสามารถในการควบคุมพฤติกรรม โดยบุคคลที่มีทัศนคติเชิงบวกต่อพฤติกรรม เห็นว่าบุคคลรอบข้างให้ความสำคัญ และเชื่อว่าตนเองสามารถปฏิบัติพฤติกรรมนั้นได้ จะมีแนวโน้มแสดงพฤติกรรมดังกล่าวมากขึ้น

ในบริบทของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พฤติกรรมหมายถึง การปฏิบัติตามแนวทางด้านความปลอดภัยขององค์กร เช่น การรักษาความลับของข้อมูล การใช้งานรหัสผ่านอย่างปลอดภัย การระมัดระวังภัยคุกคามทางไซเบอร์ และการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ การแสดงพฤติกรรมดังกล่าวเกิดขึ้นจากการที่พนักงานมีความรู้ ความเข้าใจ ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์ และมีทัศนคติเชิงบวกต่อการปฏิบัติตามแนวทางขององค์กร (Bulgurcu et al., 2010; Cavusoglu et al., 2009 อ้างถึงใน สุพิชฌา อาจวงจิต, 2557)

ดังนั้น ผู้วิจัยจึงนำแนวคิดเกี่ยวกับพฤติกรรม มาใช้เป็นกรอบในการอธิบายพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน โดยคาดว่าพนักงานที่มีทัศนคติเชิงบวกต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จะมีแนวโน้มปฏิบัติตามแนวทางด้านความปลอดภัยขององค์กรในระดับที่สูงขึ้น

งานวิจัยที่เกี่ยวข้อง

จากการทบทวนงานวิจัยที่เกี่ยวข้อง พบว่างานวิจัยหลายเรื่องสะท้อนบทบาทของการสื่อสารภายในองค์กร ทัศนคติ และพฤติกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์

มาริสา จันเกตุ (2566) ศึกษากระบวนการวางแผนการสื่อสารเพื่อบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของบริษัท ปตท. จำกัด (มหาชน) พบว่า ปตท. มีการบริหารความเสี่ยงด้านไซเบอร์อย่างเป็น

ระบบ และมีการวางแผนการสื่อสารเพื่อสร้างความตระหนักรู้แก่พนักงานผ่านหลายช่องทาง เช่น เอกสาร ประกาศ ข่าวประชาสัมพันธ์ การอบรม และกิจกรรม Phishing Test Campaign งานวิจัยดังกล่าวสะท้อนว่า การสื่อสารด้าน Cybersecurity จำเป็นต้องอาศัยการวางแผนอย่างเป็นระบบ เพื่อให้พนักงานเกิดความรู้ ความเข้าใจ และตระหนักถึงบทบาทของตนเองในการลดความเสี่ยงทางไซเบอร์ขององค์กร

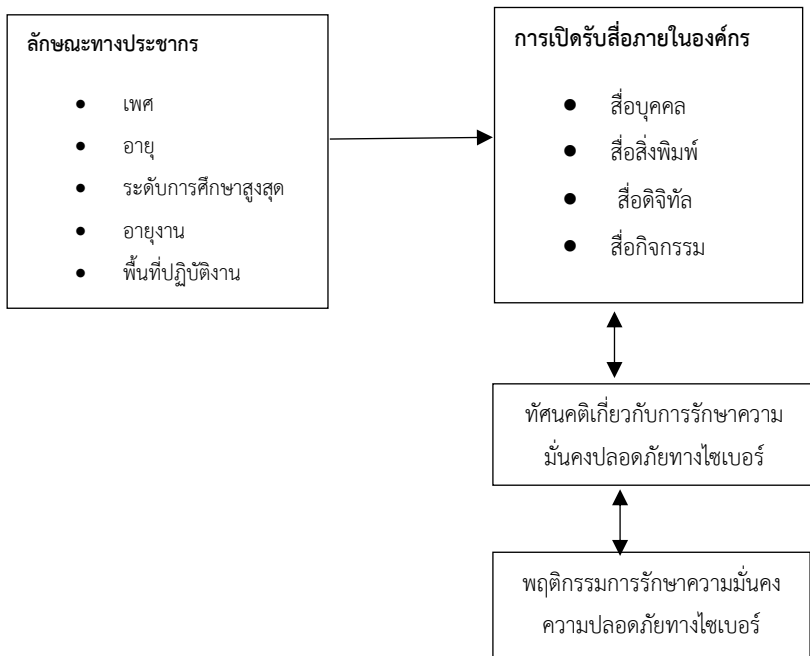
อภิญา รัตนารักษ์ (2559) ศึกษาปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผลการวิจัยพบว่า การรับรู้ภัยคุกคาม ความเชื่อในความสามารถของตนเอง การคล้อยตามกลุ่มอ้างอิง ทัศนคติ การรับรู้ความรับผิดชอบ และการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย มีอิทธิพลต่อความตั้งใจและพฤติกรรมในการปฏิบัติตามนโยบายขององค์กร ผลการศึกษานี้ชี้ให้เห็นว่า พฤติกรรมด้านความมั่นคงปลอดภัยของพนักงานไม่ได้เกิดจากกฎระเบียบเพียงอย่างเดียว แต่เกี่ยวข้องกับ การรับรู้ ความเชื่อ ทัศนคติ และความตระหนักของบุคลากรด้วย

วาทีณี เจริญพงษ์ (2565) ศึกษาการเปิดรับข่าวสาร ทัศนคติ และแนวโน้มการมีส่วนร่วมต่อการเปลี่ยนผ่านสู่ดิจิทัลของพนักงานบริษัท พีทีที โกลบอล เคมิคอล จำกัด (มหาชน) พบว่า พนักงานมีการเปิดรับข่าวสารผ่านสื่ออิเล็กทรอนิกส์ในระดับมาก โดยเฉพาะอีเมล ซึ่งเป็นช่องทางที่มีการเปิดรับมากที่สุด อีกทั้งการเปิดรับข่าวสารยังมีความสัมพันธ์กับทัศนคติและแนวโน้มการมีส่วนร่วมของพนักงาน งานวิจัยดังกล่าวสอดคล้องกับการศึกษาครั้งนี้ เนื่องจากสะท้อนว่า การสื่อสารภายในองค์กรผ่านช่องทางที่เหมาะสมสามารถสนับสนุนให้พนักงานเกิดความเข้าใจ ทัศนคติที่ดี และการมีส่วนร่วมต่อประเด็นสำคัญขององค์กรได้

คณิศนันต์ ทองคำ (2561) ศึกษาปัจจัยที่ส่งผลต่อความตั้งใจของพนักงานในการปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร พบว่า การฝึกอบรมและการให้ความรู้ขององค์กรมีผลต่อความตั้งใจในการปฏิบัติตามนโยบาย นอกจากนี้ ทัศนคติ การคล้อยตามกลุ่มอ้างอิง พฤติกรรมด้านความมั่นคงปลอดภัย และการตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ล้วนส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายขององค์กร งานวิจัยนี้สะท้อนว่า การสร้างความรู้ ความตระหนัก และทัศนคติที่ดีมีส่วนสำคัญต่อการส่งเสริมให้พนักงานปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยสารสนเทศ

วฤณ ประเสริฐศร (2559) ศึกษาการเปิดรับ ความต้องการสื่อและข้อมูลข่าวสาร และความพึงพอใจที่ได้รับจากการเข้าร่วมกิจกรรมฝึกอบรมในโครงการพัฒนาบุคลากร พบว่า กลุ่มตัวอย่างมีการเปิดรับสื่ออิเล็กทรอนิกส์ในระดับมาก โดยเปิดรับผ่านอีเมลมากที่สุด รองลงมา คือ สื่อบุคคล ได้แก่ หัวหน้างานและเพื่อนร่วมงาน อีกทั้งยังพบว่ากลุ่มตัวอย่างต้องการข้อมูลข่าวสารที่มีประโยชน์ต่อการทำงานและสามารถนำความรู้จากการฝึกอบรมไปประยุกต์ใช้ได้จริง งานวิจัยนี้สอดคล้องกับการศึกษาค้นคว้านี้ เนื่องจากแสดงให้เห็นว่า สื่ออิเล็กทรอนิกส์ สื่อบุคคล และกิจกรรมฝึกอบรมเป็นช่องทางสำคัญที่ช่วยสนับสนุนการรับรู้ ความเข้าใจ และการนำความรู้ไปใช้ในการทำงานของพนักงาน

กรอบแนวคิดการวิจัย



วิธีการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ ใช้วิธีวิจัยเชิงสำรวจ โดยเก็บรวบรวมข้อมูลด้วยแบบสอบถามออนไลน์จากพนักงาน บริษัท ปตท. จำกัด (มหาชน) ประชากรที่ใช้ในการวิจัย คือ พนักงานบริษัท ปตท. จำกัด (มหาชน) จำนวน 3,640 คน (รายงานประจำปี ปตท., 2569) ผู้วิจัยกำหนดขนาดกลุ่มตัวอย่างโดยใช้สูตรของ Yamane ที่ระดับความเชื่อมั่นร้อยละ 95 ได้กลุ่มตัวอย่างจำนวน 361 คน โดยใช้การสุ่มตัวอย่างใช้วิธีการสุ่มแบบโควตา (Quota Sampling) ซึ่งกำหนดสัดส่วนกลุ่มตัวอย่างตามพื้นที่ปฏิบัติงาน

เพื่อให้กลุ่มตัวอย่างครอบคลุมพนักงานในพื้นที่กรุงเทพมหานครและ
ปริมณฑล ต่างจังหวัด และต่างประเทศ ดังนี้

ตารางที่ 1

แสดงจำนวนกลุ่มตัวอย่าง ระบุด้วยวิธีการเลือกแบบโควตาจำแนกตาม
สัดส่วนพื้นที่ปฏิบัติงานพนักงานบริษัท ปตท. จำกัด (มหาชน)

พื้นที่ปฏิบัติงาน	จำนวน พนักงาน (N)	สัดส่วน (%)	กลุ่มตัวอย่าง (n)
กรุงเทพมหานคร	2,244	61.50	222
ต่างจังหวัด	1,364	37.67	136
ต่างประเทศ	32	0.83	3
รวม	3,640	100	361

เครื่องมือที่ใช้ในการวิจัย คือ แบบสอบถาม โดยนำผลการทดลองใช้
แบบสอบถามมาวิเคราะห์หาค่าความเชื่อถือได้ของเครื่องมือ โดยใช้ค่า
สัมประสิทธิ์แอลฟาของครอนบาค หรือ Cronbach's Alpha Coefficient เพื่อ
พิจารณาความสอดคล้องภายในของข้อความในแต่ละด้าน ได้แก่ การเปิดรับสื่อ
ภายในองค์กร ทัศนคติด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์ และ
พฤติกรรมด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์ โดยกำหนด
เกณฑ์การยอมรับค่าความเชื่อถือได้ไว้ที่ไม่ต่ำกว่า 0.70 ซึ่งถือว่าแบบสอบถามมี
ความเชื่อถือได้ในระดับที่ยอมรับได้

ตารางที่ 2

แสดงผลการทดสอบความเชื่อถือได้ของแบบสอบถาม ดังนี้

แบบสอบถาม	ค่าสัมประสิทธิ์แอลฟา
การเปิดรับสื่อภายในองค์กรด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์	0.893
ทัศนคติด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์	0.936
พฤติกรรมด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์	0.914

การวิเคราะห์ข้อมูลใช้สถิติเชิงพรรณนา ได้แก่ ค่าความถี่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน เพื่ออธิบายลักษณะทางประชากรของกลุ่มตัวอย่าง ระดับการเปิดรับสื่อภายในองค์กร ทัศนคติ และพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานบริษัท ปตท. จำกัด (มหาชน) ส่วนการทดสอบสมมติฐานใช้สถิติเชิงอนุมาน ได้แก่ การทดสอบค่าที่ การวิเคราะห์ความแปรปรวนทางเดียว และค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน เพื่อเปรียบเทียบการเปิดรับสื่อภายในองค์กรจำแนกตามลักษณะทางประชากร และวิเคราะห์ความสัมพันธ์ระหว่างการเปิดรับสื่อภายในองค์กรกับทัศนคติ รวมถึงความสัมพันธ์ระหว่างทัศนคติกับพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยกำหนดระดับนัยสำคัญทางสถิติที่ระดับ 0.05

ผลการวิจัย

ลักษณะทางประชากร

ผู้ตอบแบบสอบถามจำนวน 361 คน ซึ่งเป็นพนักงานบริษัท ปตท. จำกัด (มหาชน) พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง (ร้อยละ 51.80) ขณะที่เพศชายมีสัดส่วนใกล้เคียงกัน (ร้อยละ 48.20) ด้านอายุ พบว่า กลุ่มอายุ 36–45 ปี มีสัดส่วนมากที่สุด (ร้อยละ 36.84) รองลงมา คือ อายุ 46–55 ปี (ร้อยละ 36.29) และอายุ 26–35 ปี (ร้อยละ 19.67) ขณะที่กลุ่มอายุ 18–25 ปี มีสัดส่วนน้อยที่สุด (ร้อยละ 1.39)

ด้านระดับการศึกษา พบว่า กลุ่มตัวอย่างส่วนใหญ่มีระดับการศึกษาสูงกว่าปริญญาตรี (ร้อยละ 65.93) รองลงมา คือ ระดับปริญญาตรี (ร้อยละ 29.92) และต่ำกว่าปริญญาตรี (ร้อยละ 4.16) ตามลำดับ สำหรับอายุงาน พบว่า กลุ่มตัวอย่างส่วนใหญ่มีอายุงาน 11–15 ปี (ร้อยละ 50.42) รองลงมา คือ อายุงาน 5–10 ปี (ร้อยละ 31.58) ขณะที่กลุ่มอายุงานมากกว่า 20 ปี มีสัดส่วนน้อยที่สุด (ร้อยละ 1.39)

เมื่อพิจารณาพื้นที่ปฏิบัติงาน พบว่า กลุ่มตัวอย่างส่วนใหญ่ปฏิบัติงานในกรุงเทพมหานครและปริมณฑล (ร้อยละ 61.50) รองลงมา คือ ต่างจังหวัด (ร้อยละ 37.67) และต่างประเทศ (ร้อยละ 0.83)

ผลการศึกษาสะท้อนให้เห็นว่า กลุ่มตัวอย่างส่วนใหญ่เป็นพนักงานวัยทำงานที่มีประสบการณ์ในการปฏิบัติงานในระดับหนึ่ง และมีระดับการศึกษาค่อนข้างสูง ซึ่งสอดคล้องกับลักษณะของบุคลากรในองค์กรขนาดใหญ่ที่มีการดำเนินงานด้านเทคโนโลยีและระบบสารสนเทศอย่างต่อเนื่อง โดยลักษณะทางประชากรดังกล่าวเป็นปัจจัยสำคัญที่เกี่ยวข้องกับการรับรู้ การเข้าถึง ข้อมูลข่าวสาร และการเปิดรับสื่อภายในองค์กร ซึ่งเป็นประเด็นที่นำไปสู่

การศึกษาความแตกต่างของการเปิดรับสื่อภายในองค์กรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

การเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ตารางที่ 3

แสดงค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของการเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จำแนกตามประเภทสื่อ

ประเภทสื่อ	ค่าเฉลี่ย ($\bar{x}$)	S.D.	ความหมาย
สื่อบุคคล	3.98	0.46	มาก
สื่อสิ่งพิมพ์	4.09	0.53	มาก
สื่อดิจิทัล	3.95	0.39	มาก
กิจกรรม	4.21	0.47	มากที่สุด
รวม	4.06	0.38	มาก

จากตารางที่ 3 พบว่า กลุ่มตัวอย่างมีการเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน) โดยรวมอยู่ในระดับมาก มีค่าเฉลี่ยเท่ากับ 4.06 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.38

เมื่อพิจารณาเป็นรายประเภทสื่อ พบว่า ประเภทสื่อที่มีค่าเฉลี่ยสูงที่สุด คือ สื่อประเภทกิจกรรม มีค่าเฉลี่ยเท่ากับ 4.21 อยู่ในระดับมากที่สุด รองลงมา คือ สื่อสิ่งพิมพ์ มีค่าเฉลี่ยเท่ากับ 4.09 อยู่ในระดับมาก สื่อบุคคล มีค่าเฉลี่ยเท่ากับ 3.98 อยู่ในระดับมาก และสื่อดิจิทัล มีค่าเฉลี่ยเท่ากับ 3.95 อยู่ในระดับมาก ตามลำดับ

ดังนั้น การสื่อสารด้านความมั่นคงปลอดภัยทางไซเบอร์ควรใช้สื่อแบบผสมผสาน โดยคำนึงถึงวัตถุประสงค์ของสาร ความซับซ้อนของเนื้อหา และความแตกต่างของพนักงานแต่ละกลุ่ม เพื่อให้การสื่อสารสามารถสร้างการรับรู้ ความเข้าใจ ทักษะที่ดี และพฤติกรรมการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ

ทัศนคติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ตารางที่ 4

แสดงค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐานของระดับทัศนคติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน)

ทัศนคติด้านการรักษาความมั่นคง ความปลอดภัยทางไซเบอร์	ค่าเฉลี่ย ($\bar{x}$)	S.D.	ระดับ ทัศนคติ
การรักษาความมั่นคงความปลอดภัยทางไซเบอร์เป็นเรื่องจำเป็นต่อการดำเนินงานของ ปตท.	4.57	0.52	เชิงบวก
การสื่อสารด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์ที่ชัดเจนช่วยให้พนักงานปฏิบัติงานได้ปลอดภัยมากขึ้น	4.56	0.51	เชิงบวก
การปฏิบัติตามแนวทางด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์เป็นสิ่งสำคัญสำหรับพนักงานทุกคน	4.51	0.52	เชิงบวก
นโยบายหรือข้อกำหนดด้านการรักษาความมั่นคงความปลอดภัยทาง	4.46	0.52	เชิงบวก

ทัศนคติด้านการรักษาความมั่นคง ความปลอดภัยทางไซเบอร์	ค่าเฉลี่ย ($\bar{x}$)	S.D.	ระดับ ทัศนคติ
ไซเบอร์ของ ปตท. สามารถนำไป ปฏิบัติได้จริงในการทำงาน			
การรักษาความมั่นคงความปลอดภัย ทางไซเบอร์เป็นส่วนหนึ่งของค่านิยม และความรับผิดชอบของพนักงาน ปตท.	4.51	0.54	เชิงบวก
ความเต็มใจที่จะให้ความร่วมมือใน การปฏิบัติตามแนวทางด้านการ รักษาความมั่นคงความปลอดภัยทาง ไซเบอร์ขององค์กร	4.63	0.49	เชิงบวก
การละเลยแนวทางด้านการรักษา ความมั่นคงความปลอดภัยทางไซ เบอร์อาจก่อให้เกิดผลกระทบรุนแรง ต่อองค์กร	4.66	0.50	เชิงบวก
รวม	4.56	0.42	เชิงบวก

จากตารางที่ 4 พบว่า พนักงานบริษัท ปตท. จำกัด (มหาชน) มีทัศนคติต่อการรักษาความมั่นคงความปลอดภัยทางไซเบอร์โดยรวมอยู่ในระดับเชิงบวก มีค่าเฉลี่ย 4.56 เมื่อพิจารณาเป็นรายข้อ พบว่า ข้อที่มีค่าเฉลี่ยสูงสุด คือ การละเลยแนวทางด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์อาจก่อให้เกิดผลกระทบรุนแรงต่อองค์กร มีค่าเฉลี่ย 4.66 รองลงมา คือ ความเต็มใจที่จะให้ความร่วมมือในการปฏิบัติตามแนวทางด้านการรักษา

ความมั่นคงความปลอดภัยทางไซเบอร์ขององค์กร มีค่าเฉลี่ย 4.63 และการรักษาความมั่นคงความปลอดภัยทางไซเบอร์เป็นเรื่องจำเป็นต่อการดำเนินงานของ ปตท. มีค่าเฉลี่ย 4.57 ตามลำดับ ขณะที่ข้อที่มีค่าเฉลี่ยต่ำที่สุด คือ นโยบายหรือข้อกำหนดด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์ของ ปตท. สามารถนำไปปฏิบัติได้จริงในการทำงาน มีค่าเฉลี่ย 4.46 แต่ยังคงอยู่ในระดับเชิงบวกเช่นกัน

พฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ตารางที่ 5

แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของระดับพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน)

จำแนกตามรายด้าน

ด้านพฤติกรรม	ค่าเฉลี่ย ($\bar{x}$)	ค่าเบี่ยงเบน มาตรฐาน	ระดับ พฤติกรรม
ด้านที่ 1 การบริหารจัดการและ ควบคุมการเข้าถึงระบบ สารสนเทศ	4.70	0.45	มากที่สุด
ด้านที่ 2 การใช้งานเครื่อง คอมพิวเตอร์และอุปกรณ์พกพา	4.73	0.42	มากที่สุด
ด้านที่ 3 การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์	4.75	0.42	มากที่สุด
ด้านที่ 4 การใช้จดหมาย อิเล็กทรอนิกส์	4.72	0.44	มากที่สุด

ด้านพฤติกรรม	ค่าเฉลี่ย ($\bar{x}$)	ค่าเบี่ยงเบน มาตรฐาน	ระดับ พฤติกรรม
ด้านที่ 5 การบริหารจัดการ ข้อมูลและบริการดิจิทัลของ องค์กร	4.74	0.44	มากที่สุด
รวม	4.73	0.40	มากที่สุด

จากตารางที่ 5 พบว่า พนักงานบริษัท ปตท. จำกัด (มหาชน) มีพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยรวมอยู่ในระดับมากที่สุด มีค่าเฉลี่ย 4.73 และค่าเบี่ยงเบนมาตรฐาน 0.40 เมื่อพิจารณารายด้าน พบว่า ทุกด้านอยู่ในระดับมากที่สุด โดยด้านที่มีค่าเฉลี่ยสูงที่สุด คือ การใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์ มีค่าเฉลี่ย 4.75 รองลงมา คือ การบริหารจัดการข้อมูลและบริการดิจิทัลขององค์กร มีค่าเฉลี่ย 4.74 และ การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์พกพา มีค่าเฉลี่ย 4.73 ขณะที่ด้านการบริหารจัดการและควบคุมการเข้าถึงระบบสารสนเทศมีค่าเฉลี่ยต่ำที่สุด คือ 4.70 แต่ยังคงอยู่ในระดับมากที่สุดเช่นกัน.

ผลดังกล่าวแสดงให้เห็นว่า พนักงานมีแนวโน้มปฏิบัติตามแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรในระดับสูง โดยเฉพาะพฤติกรรมที่เกี่ยวข้องกับการใช้งานอินเทอร์เน็ต เครือข่ายสังคมออนไลน์ การดูแลข้อมูล และการใช้งานอุปกรณ์ดิจิทัล ซึ่งเป็นพฤติกรรมที่เกี่ยวข้องกับความเสี่ยงทางไซเบอร์ในชีวิตการทำงานประจำวันโดยตรง

ผลการวิจัยนี้สามารถอธิบายได้ว่า การที่พนักงานมีพฤติกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับมากที่สุด อาจเป็นผลจากการที่องค์กรมีนโยบาย แนวปฏิบัติ และการสื่อสารภายในองค์กรด้านความมั่นคง

ปลอดภัยทางไซเบอร์อย่างต่อเนื่อง ทำให้พนักงานตระหนักถึงบทบาทของตนเองในการป้องกันความเสี่ยง และสามารถนำแนวทางดังกล่าวไปใช้ในการทำงานจริงได้

ตารางที่ 6

แสดงความสัมพันธ์ระหว่างการเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงความปลอดภัยทางไซเบอร์กับทัศนคติของพนักงานบริษัท ปตท. จำกัด (มหาชน)

ความสัมพันธ์ระหว่าง	ระดับความสัมพันธ์ (r)	Sig.	ระดับความสัมพันธ์
การเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงความปลอดภัยทางไซเบอร์กับทัศนคติด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์	0.278	<.001	ทางบวกในระดับน้อย

ระดับนัยสำคัญ 0.05

จากตารางที่ 6 ผลความสัมพันธ์ระหว่างการเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงความปลอดภัยทางไซเบอร์กับทัศนคติของพนักงานบริษัท ปตท. จำกัด (มหาชน) เมื่อพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ พบว่า ค่า r เท่ากับ 0.278 เป็นความสัมพันธ์ทางบวกในระดับน้อย แสดงให้เห็นว่า ตัวแปรทั้งสองมีความสัมพันธ์ไปในทิศทางเดียวกัน กล่าวคือ พนักงานที่มีการเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความ

มันคงปลอดภัยทางไซเบอร์มากขึ้น มีแนวโน้มที่จะมีทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในทิศทางที่ดีขึ้นตามไปด้วย

ตารางที่ 7

แสดงความสัมพันธ์ระหว่างทัศนคติกับพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน)

ความสัมพันธ์ระหว่าง	Pearson Correlation (r)	Sig.	ระดับ ความสัมพันธ์
ทัศนคติกับพฤติกรรมด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์	0.612	<.001	สูง

ระดับนัยสำคัญ 0.05

จากตารางที่ 7 ผลการทดสอบสมมติฐานเกี่ยวกับความสัมพันธ์ระหว่างทัศนคติกับพฤติกรรมด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน) พบว่า ค่าสัมประสิทธิ์สหสัมพันธ์เท่ากับ 0.612 และค่า Sig. น้อยกว่า .001 ซึ่งน้อยกว่าระดับนัยสำคัญทางสถิติที่ 0.05 หมายความว่า ทัศนคติมีความสัมพันธ์กับพฤติกรรมด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์ของพนักงาน บริษัท ปตท. จำกัด (มหาชน) อย่างมีนัยสำคัญทางสถิติที่ 0.05

เมื่อพิจารณาค่าสัมประสิทธิ์สหสัมพันธ์ พบว่า ค่า r เท่ากับ 0.612 เป็นความสัมพันธ์ทางบวกในระดับสูงแสดงให้เห็นว่าตัวแปรทั้งสองมีความสัมพันธ์ไปในทิศทางเดียวกัน กล่าวคือ พนักงานที่มีทัศนคติเกี่ยวกับการ

รักษาความมั่นคงความปลอดภัยทางไซเบอร์สูงขึ้น มีแนวโน้มที่จะมีพฤติกรรมด้านการรักษาความมั่นคงความปลอดภัยทางไซเบอร์สูงขึ้นเช่นกัน

ผลการทดสอบสมมติฐาน

ตารางที่ 8

สรุปผลการทดสอบสมมติฐาน

สมมติฐาน	ค่าสถิติ	Sig.	ผลการทดสอบ
สมมติฐานที่ 1			พบว่ายอมรับสมมติฐานทุกข้อ
สมมติฐานย่อยที่ 1.1 เพศแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน	$t = -2.082$	0.038	ยอมรับสมมติฐาน
สมมติฐานย่อยที่ 1.2 อายุแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน	$F = 3.831$	0.005	ยอมรับสมมติฐาน
สมมติฐานย่อยที่ 1.3 ระดับการศึกษาแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน	$F = 9.943$	$< .001$	ยอมรับสมมติฐาน
สมมติฐานย่อยที่ 1.4 อายุงานแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน	$F = 2.453$	0.046	ยอมรับสมมติฐาน

สมมติฐาน	ค่าสถิติ	Sig.	ผลการทดสอบ
สมมติฐานย่อยที่ 1.5 พื้นที่ปฏิบัติงานแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน	$F = 9.682$	$< .001$	ยอมรับสมมติฐาน
สมมติฐานที่ 2 การเปิดรับสื่อภายในองค์กรมีความสัมพันธ์กับทัศนคติ	$r = 0.278$	$< .001$	ยอมรับสมมติฐาน
สมมติฐานที่ 3 ทัศนคติมีความสัมพันธ์กับพฤติกรรม	$r = 0.612$	$< .001$	ยอมรับสมมติฐาน

หมายเหตุ: * $p < .05$, ** $p < .01$, *** $p < .001$

อภิปรายผลการวิจัย

ผลการทดสอบสมมติฐานที่ 1 พบว่า พนักงานบริษัท ปตท. จำกัด (มหาชน) ที่มีลักษณะทางประชากรแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงความปลอดภัยทางไซเบอร์แตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยสามารถสรุปผลการทดสอบสมมติฐานย่อยได้ดังนี้

สมมติฐานย่อยที่ 1.1 เพศแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน พบว่า พนักงานเพศหญิงมีค่าเฉลี่ยการเปิดรับสื่อสูงกว่าเพศชายเล็กน้อย ผลดังกล่าวอาจสะท้อนว่า เพศเป็นปัจจัยหนึ่งที่เกี่ยวข้องกับรูปแบบการติดตามข้อมูลข่าวสาร ความสนใจ และการให้ความสำคัญต่อข้อมูลภายในองค์กร โดยพนักงานเพศหญิงในกลุ่มตัวอย่างมีแนวโน้มติดตาม รับรู้

หรือใส่ใจรายละเอียดของข่าวสารภายในองค์กรที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์มากกว่าเพศชายในบางประเด็น

สอดคล้องกับงานวิจัยของ นันทินี พิศวิลัย (2558) เพศหญิงมีแนวโน้มและความต้องการในการส่งและรับข่าวสารมากกว่าเพศชาย และสามารถล้อยตามง่ายกว่าเพศชาย ทำให้เพศหญิงมีแนวโน้มว่าจะเปิดรับสื่อและได้รับอิทธิพลจากสื่อมากกว่าเพศชาย ดังนั้น ผลดังกล่าวความแตกต่างด้านเพศ สามารถนำมาใช้ในการออกแบบการสื่อสารด้านความมั่นคงปลอดภัยทางไซเบอร์ให้เข้าถึงพนักงานทุกกลุ่มมากขึ้น โดยเฉพาะกลุ่มที่มีการเปิดรับต่ำกว่า อาจเพิ่มรูปแบบการสื่อสารที่เชื่อมโยงกับสถานการณ์การทำงานจริงเหมาะสมกับบริบทการทำงาน

สมมติฐานย่อยที่ 1.2 อายุแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน พบว่า กลุ่มอายุ 56–60 ปี มีค่าเฉลี่ยการเปิดรับสื่อสูงที่สุด ผลดังกล่าวอาจเนื่องมาจากพนักงานกลุ่มนี้มีประสบการณ์ในการทำงานมาก มีความคุ้นเคยกับระบบงานและวัฒนธรรมองค์กร รวมถึงให้ความสำคัญกับนโยบาย ข้อกำหนด และแนวปฏิบัติขององค์กรมากขึ้น ผลดังกล่าวสอดคล้องกับแนวคิดการเลือกเปิดรับข่าวสารของ ปรมะ สันติเวทิน (2546, อ้างถึงใน ณัฐธาดา ศรีไพโรจน์, 2566) ที่อธิบายว่า ผู้รับสารจะเลือกเปิดรับ เลือกรับรู้ และเลือกจดจำข่าวสารตามความสนใจ ประสบการณ์ ความต้องการ และทัศนคติของตนเอง อีกทั้งยังสามารถอภิปรายร่วมกับผลการศึกษาของ เสมอ นิมะเงิน (2566) ที่อธิบายว่ากลุ่มวัยต่าง ๆ มีลักษณะการติดตามข่าวสารแตกต่างกัน ดังนั้น การสื่อสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ ปตท. จึงควรปรับให้เหมาะสมกับพนักงานแต่ละช่วงวัย เช่น ใช้การอบรมและเอกสารทางการสำหรับกลุ่มที่ให้ความสำคัญกับความชัดเจนของนโยบาย ควบคู่กับสื่อดิจิทัลที่กระชับ เข้าใจง่าย และเข้าถึงได้สะดวกสำหรับพนักงานรุ่นใหม่

สมมติฐานย่อยที่ 1.3 ระดับการศึกษาแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน พบว่า พนักงานที่มีระดับการศึกษาสูงกว่าปริญญาตรี มีค่าเฉลี่ยการเปิดรับสื่อสูงกว่ากลุ่มอื่น ผลดังกล่าวอาจอธิบายได้ว่า ระดับการศึกษามีส่วนเกี่ยวข้องกับความสามารถในการทำความเข้าใจ วิเคราะห์ และตีความข้อมูลที่มีลักษณะเป็นนโยบาย มาตรการ หรือแนวปฏิบัติด้านเทคโนโลยีและความปลอดภัย ซึ่งสอดคล้องกับผลการศึกษาของ ชัชญา เรืองยศ (2563) ที่พบว่า ผู้ที่มีระดับการศึกษาสูงกว่ามีแนวโน้มได้เปรียบด้านการเปิดรับ การรับรู้ การวิเคราะห์ และการใช้ประโยชน์จากข้อมูลข่าวสาร เช่นเดียวกับผลการศึกษาของ คณิสันต์ ทองคำ (2561) ที่พบว่าระดับการศึกษา ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบาย ด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร โดยพบว่าค่าเฉลี่ยของกลุ่มต่ำกว่าปริญญาตรีมีค่าน้อยกว่ากลุ่มอื่น ดังนั้น การสื่อสารด้านความมั่นคงปลอดภัยทางไซเบอร์ของ ปตท. ควรออกแบบเนื้อหาให้มีความชัดเจน เข้าใจง่าย และเชื่อมโยงกับความเสี่ยง ผลกระทบ และแนวทางปฏิบัติที่เกี่ยวข้องกับงานจริง เพื่อให้พนักงานทุกระดับการศึกษาสามารถเข้าใจและนำไปใช้ได้เหมาะสม

สมมติฐานย่อยที่ 1.4 อายุงานแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน พบว่า กลุ่มอายุงาน 16–20 ปี มีค่าเฉลี่ยการเปิดรับสื่อสูงที่สุด ผลดังกล่าวสะท้อนว่า อายุงานอาจเกี่ยวข้องกับความสัมพันธ์ของการสื่อสาร วัฒนธรรมองค์กร และการรับรู้ความสำคัญของนโยบายภายในองค์กร ซึ่งสอดคล้องกับวาทีณี เจริญพงษ์ (2565) ที่พบว่า พนักงานที่มีอายุงานมากกว่ามีแนวโน้มเปิดรับข่าวสารภายในองค์กรสูงกว่าพนักงานที่มีอายุน้อยกว่า

สมมติฐานย่อยที่ 1.5 พื้นที่ปฏิบัติงานแตกต่างกัน มีการเปิดรับสื่อภายในองค์กรแตกต่างกัน พบว่า พนักงานในกรุงเทพมหานครและปริมณฑล

มีค่าเฉลี่ยการเปิดรับสื่อสูงกว่าพนักงานในต่างจังหวัดและต่างประเทศอย่างมีนัยสำคัญ ผลดังกล่าวมีความสำคัญต่อบริบทของ ปตท. เนื่องจากองค์กรมีทั้งสำนักงานใหญ่ พื้นที่ปฏิบัติการ และพื้นที่ทำงานที่กระจายตัว พนักงานในกรุงเทพมหานครและปริมณฑลอาจมีโอกาสเข้าถึงกิจกรรม สื่อบุคคล หรือการสื่อสารจากส่วนกลางได้มากกว่า ขณะที่พนักงานในต่างจังหวัดหรือต่างประเทศอาจมีข้อจำกัดด้านระยะทาง เวลา ลักษณะงาน หรือโอกาสในการเข้าร่วมกิจกรรม ในประเด็นดังกล่าวสอดคล้องกับผลการศึกษาของสุพานิ สฤกษ์วานิช (2552) ที่อธิบายว่า ความแตกต่างของหน่วยงาน ลักษณะงาน และบริบทการทำงานอาจเป็นอุปสรรคต่อการสื่อสารภายในองค์กร ดังนั้น การสื่อสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ ปตท. ควรออกแบบให้เข้าถึงพนักงานทุกพื้นที่อย่างเท่าเทียมมากขึ้น เช่น การอบรมออนไลน์ การจัดกิจกรรมเฉพาะพื้นที่ การใช้หัวหน้างานเป็นผู้ถ่ายทอดสาร และการพัฒนาสื่อดิจิทัลที่สามารถเข้าถึงได้จากทุกพื้นที่ปฏิบัติงาน

กล่าวโดยสรุปภาพรวมสมมติฐานที่ 1 ลักษณะทางประชากรและการเปิดรับสื่อในภาพรวม พบว่า พนักงานมีการเปิดรับสื่อด้านดิจิทัล ผ่านช่องทางอีเมลภายใน ปตท. และด้านกิจกรรม ผ่านช่องทางการอบรม Cyber Security ในระดับสูง ผลดังกล่าวแสดงให้เห็นว่า ช่องทางที่สอดคล้องกับพฤติกรรมการทำงานและเปิดโอกาสให้เกิดการเรียนรู้โดยตรงมีบทบาทต่อการรับรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน โดยอีเมลภายในเป็นช่องทางที่เข้าถึงง่าย รวดเร็ว และเหมาะกับการแจ้งข้อมูลนโยบาย หรือข้อควรระวังที่เกี่ยวข้องกับการทำงานประจำวัน ซึ่งสอดคล้องกับผลการศึกษาของวาทีนิ เจริญพงษ์ (2565) ที่พบว่า พนักงานมีแนวโน้มเปิดรับข่าวสารภายในองค์กรผ่านสื่อออนไลน์มากกว่าสื่อออฟไลน์ เนื่องจากเข้าถึงได้ง่ายและสอดคล้องกับพฤติกรรมการทำงานระยะไกลหรือ Work

from Home ในปัจจุบัน ขณะเดียวกัน กิจกรรมอบรม Cyber Security เป็นสื่อที่ช่วยเสริมการรับรู้ให้ลึกขึ้น เนื่องจากเปิดโอกาสให้พนักงานเรียนรู้ซักถาม แลกเปลี่ยนประสบการณ์ และเชื่อมโยงเนื้อหา กับสถานการณ์การทำงานจริง ซึ่งสอดคล้องกับงานวิจัยของวฤณ ประเสริฐศร (2559) ที่พบว่า การฝึกอบรมที่เปิดโอกาสให้พนักงานมีส่วนร่วมและแลกเปลี่ยนประสบการณ์ ช่วยส่งเสริมบรรยากาศการเรียนรู้และความเข้าใจได้ดียิ่งขึ้น

ดังนั้น พนักงานถือเป็นกลไกสำคัญในการขับเคลื่อนวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร หากพนักงานมีความเข้าใจ เห็นความสำคัญ และมีทัศนคติเชิงบวกต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ย่อมส่งผลให้เกิดพฤติกรรมการทำงานที่ปลอดภัยมากขึ้น

สมมติฐานที่ 2 ผลการวิจัยพบว่า การเปิดรับสื่อภายในองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีความสัมพันธ์เชิงบวกกับทัศนคติของพนักงานบริษัท ปตท. จำกัด (มหาชน) อย่างมีนัยสำคัญทางสถิติ แต่ความสัมพันธ์อยู่ในระดับน้อย ผลดังกล่าวสะท้อนว่า การเปิดรับสื่อภายในองค์กรมีบทบาทในการสนับสนุนการรับรู้ ความเข้าใจ และทัศนคติเชิงบวกของพนักงานต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ตาม ทัศนคติของพนักงานไม่ได้เกิดจากการเปิดรับสื่อภายในองค์กรเพียงปัจจัยเดียว แต่ยังสามารถได้รับอิทธิพลจากประสบการณ์ในการทำงาน ความรู้เดิม การเรียนรู้จากแหล่งข้อมูลภายนอก การรับรู้ความเสี่ยงทางไซเบอร์ การสนับสนุนจากผู้บังคับบัญชา วัฒนธรรมองค์กร และบริบทการทำงานของแต่ละบุคคล ผลดังกล่าวสอดคล้องกับแนวคิดด้านทัศนคติของอรวรรณ ปิรันธน์โอวาท (2554) ที่อธิบายว่า ทัศนคติเกิดจากการสะสมของข้อมูล ประสบการณ์ การเรียนรู้ ความเชื่อ และการรับรู้ในหลายบริบท

เมื่อพิจารณาในบริบทของ ปตท. ซึ่งเป็นองค์กรพลังงานขนาดใหญ่ที่มีการใช้ระบบสารสนเทศ ข้อมูลดิจิทัล และช่องทางการสื่อสารภายในองค์กรอย่างต่อเนื่อง การสื่อสารด้านความมั่นคงปลอดภัยทางไซเบอร์จึงควรมีบทบาทมากกว่าการแจ้งข้อมูลข่าวสาร แต่ควรเป็นกระบวนการสร้างความเข้าใจ ความตระหนักรู้ และการยอมรับต่อแนวทางด้านความปลอดภัยขององค์กร โดยเฉพาะการทำให้พนักงานเห็นว่า Cybersecurity เป็นเรื่องที่เกี่ยวข้องกับการทำงานของตนเองโดยตรง ไม่ใช่เพียงหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศเท่านั้น

ดังนั้น ปตท. ควรส่งเสริมการสื่อสารด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง ทั้งก่อน ระหว่าง และหลังการดำเนินกิจกรรมหรือโครงการที่เกี่ยวข้อง เช่น การอบรม Cyber Security กิจกรรมรณรงค์ การทดสอบ Phishing Test หรือการสื่อสารนโยบายด้านความปลอดภัย เพื่อให้พนักงานได้รับข้อมูลอย่างสม่ำเสมอ เข้าใจเหตุผลของมาตรการด้านความปลอดภัย และเห็นบทบาทของตนเองในการลดความเสี่ยงทางไซเบอร์ขององค์กร

กล่าวโดยสรุป ผลการวิจัยที่พบว่าความสัมพันธ์อยู่ในระดับน้อยชี้ให้เห็นว่า การสื่อสารด้านความมั่นคงปลอดภัยทางไซเบอร์ควรให้ความสำคัญกับคุณภาพของสาร รูปแบบการสื่อสาร และความสัมพันธ์กับผู้รับสารมากกว่าการเพิ่มปริมาณการสื่อสารเพียงอย่างเดียว โดยเนื้อหาควรมีความชัดเจน เข้าใจง่าย ทันต่อสถานการณ์ และเชื่อมโยงกับบทบาทหน้าที่ของพนักงานแต่ละกลุ่ม เพื่อให้การเปิดรับสื่อภายในองค์กรสามารถสนับสนุนทัศนคติเชิงบวกต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้น

สมมติฐานที่ 3 ผลการวิจัยพบว่า ทัศนคติมีความสัมพันธ์เชิงบวกกับพฤติกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานบริษัท ปตท. จำกัด (มหาชน) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยอยู่ใน

ระดับสูง ผลดังกล่าวสะท้อนว่า พนักงานที่มีทัศนคติเชิงบวกต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีแนวโน้มปฏิบัติตามแนวทางด้านความปลอดภัยขององค์กรในระดับสูงเช่นกัน

เมื่อพิจารณาผลการวิจัยด้านทัศนคติ พบว่า พนักงานมีทัศนคติโดยรวมอยู่ในระดับมากที่สุด โดยเฉพาะประเด็นที่ว่า การละเลยแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์อาจก่อให้เกิดผลกระทบรุนแรงต่อองค์กร และความเต็มใจให้ความร่วมมือในการปฏิบัติตามแนวทางขององค์กร ผลดังกล่าวแสดงให้เห็นว่า พนักงานตระหนักถึงความสำคัญของการรักษาข้อมูล ระบบสารสนเทศ และความต่อเนื่องในการดำเนินงานขององค์กร ขณะเดียวกัน ผลการวิจัยด้านพฤติกรรม พบว่า พนักงานมีพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยรวมอยู่ในระดับมากที่สุดเช่นกัน โดยเฉพาะด้านการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์ และด้านการบริหารจัดการข้อมูลและบริการดิจิทัลขององค์กร สะท้อนให้เห็นว่าพนักงานมีการปฏิบัติตามแนวทางด้านความปลอดภัยขององค์กรในระดับสูงผลดังกล่าวหมายความว่า พนักงานที่มีทัศนคติที่ดีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีแนวโน้มที่จะแสดงพฤติกรรมที่สอดคล้องกับแนวทางด้านความปลอดภัยขององค์กรในระดับที่สูงขึ้น ผลนี้มีความสำคัญ เนื่องจากชี้ให้เห็นว่าการสร้างทัศนคติที่ดีจะเป็นปัจจัยสำคัญที่สามารถเชื่อมโยงไปสู่พฤติกรรมการปฏิบัติงานที่ปลอดภัยของพนักงานได้

ผลการศึกษาดังกล่าวสอดคล้องกับแนวคิดของ Munn, (1971 อ้างถึงใน นริภา ลิ้มพิมพ์เพระ, 2558) ที่อธิบายว่า ทัศนคติเป็นความรู้สึก ความคิดเห็น หรือการประเมินของบุคคลที่มีต่อบุคคล เหตุการณ์ หรือสิ่งใดสิ่งหนึ่งในลักษณะของการยอมรับหรือปฏิเสธ ซึ่งส่งผลต่อการตอบสนองและการแสดงพฤติกรรมของบุคคล

ดังนั้น เมื่อพนักงานมีทัศนคติเชิงบวกต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เห็นถึงความสำคัญและผลกระทบที่อาจเกิดขึ้นจากการละเลยแนวปฏิบัติด้านความปลอดภัย ย่อมมีแนวโน้มที่จะปฏิบัติตามนโยบาย มาตรการ และแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรมากขึ้น ซึ่งนำไปสู่พฤติกรรมการทำงานที่ปลอดภัยและช่วยลดความเสี่ยงด้านไซเบอร์ขององค์กรได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะจากผลการวิจัย

1. องค์กรควรออกแบบการสื่อสารด้านความมั่นคงปลอดภัยทางไซเบอร์ให้เหมาะกับพนักงานแต่ละกลุ่ม เนื่องจากเพศ อายุ ระดับการศึกษา อายุงาน และพื้นที่ปฏิบัติงานที่แตกต่างกัน ทำให้การเปิดรับสื่อแตกต่างกัน
2. ควรให้ความสำคัญกับสื่อกิจกรรมควบคู่กับสื่อประเภทอื่น เนื่องจากสื่อกิจกรรมมีค่าเฉลี่ยการเปิดรับสูงที่สุด โดยควรเน้นกิจกรรมที่เชื่อมโยงกับสถานการณ์การทำงานจริง เช่น การอบรม การจำลองเหตุการณ์ และ Phishing Simulation
3. ควรพัฒนาคุณภาพของเนื้อหาการสื่อสารให้ชัดเจน เข้าใจง่าย ทันต่อสถานการณ์ และเชื่อมโยงกับบทบาทของพนักงาน เพราะการเปิดรับสื่อมีความสัมพันธ์กับทัศนคติในระดับน้อย
4. ควรส่งเสริมทัศนคติเชิงบวกต่อ Cybersecurity อย่างต่อเนื่อง เนื่องจากทัศนคติมีความสัมพันธ์กับพฤติกรรมในระดับสูง
5. ควรติดตามและประเมินผลการสื่อสารอย่างสม่ำเสมอ เพื่อนำผลไปปรับปรุงช่องทาง เนื้อหา และรูปแบบการสื่อสารให้เหมาะสมมากขึ้น

ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

1. ควรศึกษาการเปิดรับสื่อภายในองค์กรในระดับรายช่องทาง เช่น อีเมล อินเทอร์เน็ต แอปพลิเคชันภายในองค์กร ระบบ LMS การอบรม หัวหน้างาน หรือช่องทางสื่อสารอื่น ๆ เพื่อให้สามารถอธิบายรูปแบบการเปิดรับสื่อของพนักงานได้ละเอียดมากขึ้น
2. ควรศึกษาปัจจัยอื่นที่อาจเกี่ยวข้องกับทัศนคติและพฤติกรรม เช่น ความรู้ด้านไซเบอร์ การรับรู้ความเสี่ยง วัฒนธรรมองค์กร บทบาทหัวหน้างาน และประสบการณ์ภัยคุกคามไซเบอร์
3. การวิจัยเชิงคุณภาพเพิ่มเติม เช่น การสัมภาษณ์เชิงลึกหรือการสนทนากลุ่ม เพื่อทำความเข้าใจเหตุผล ประสิทธิภาพ ข้อจำกัด และมุมมองของพนักงานต่อการสื่อสารด้านความมั่นคงปลอดภัยทางไซเบอร์
4. ควรศึกษาประสิทธิผลของรูปแบบการสื่อสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เช่น การอบรมเชิงปฏิบัติการ การจำลองเหตุการณ์ การรณรงค์ผ่านสื่อดิจิทัล หรือการสื่อสารผ่านหัวหน้างาน เพื่อประเมินว่ารูปแบบใดสามารถส่งเสริมความรู้ ทัศนคติ และพฤติกรรมที่ปลอดภัย ในรายด้านเชิงลึก
5. ควรขยายขอบเขตการศึกษาไปยังบริษัทในกลุ่ม ปตท. องค์กรรัฐวิสาหกิจ หรือองค์กรโครงสร้างพื้นฐานสำคัญอื่น ๆ เพื่อเปรียบเทียบรูปแบบการสื่อสาร ทัศนคติ และพฤติกรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ในบริบทองค์กรที่แตกต่างกัน

รายการอ้างอิง

ภาษาไทย

- กิตติมา สุรสนธิ. (2548). *ความรู้ทางการสื่อสาร*. มหาวิทยาลัยธรรมศาสตร์.
- คณัสนันต์ ทองคำ. (2561). ปัจจัยที่ส่งผลต่อความตั้งใจของพนักงานในการปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศในองค์กร กรณีศึกษา: เทศบาลเมืองไร่ขิง [การค้นคว้าอิสระปริญญามหาบัณฑิต], มหาวิทยาลัยธรรมศาสตร์.
- ชัชชญา เรืองยศ, และแอนนา จุมพลเสถียร. (2565). การรู้เท่าทันสื่อสังคมออนไลน์ของผู้สูงวัย. *Media and Communication Inquiry*, 4(1), 144–169.
- ณัฐธาดา ศรีไพโรจน์, และโมไนยพล รณเวช. (2566). ความสัมพันธ์ระหว่างการเปิดรับสื่อออนไลน์ของธนาคารแห่งประเทศไทยกับความตระหนักเกี่ยวกับภัยทางการเงินของผู้บริโภค. *Media and Communication Inquiry*, 5(3), 113–148.
- ณัฐชуда วิจิตรจามรี. (2554). *การสื่อสารในองค์กร*. สำนักพิมพ์มหาวิทยาลัยเกษตรศาสตร์.
- ธงชัย สันติวงษ์. (2535). *พฤติกรรมผู้บริโภคทางการตลาด*. ไทยวัฒนาพานิช.
- นันท์น พิศวิสัย. (2558). *พฤติกรรม的开รับข่าวสารและความพึงพอใจของผู้ใช้เว็บไซต์ www.ginraidee.com ในเขตกรุงเทพมหานคร* [การค้นคว้าอิสระปริญญามหาบัณฑิต], มหาวิทยาลัยธรรมศาสตร์.
- นริภา ลิ้มพิมพ์เพระ. (2558). *ทัศนคติและพฤติกรรมการมีส่วนร่วมเกี่ยวกับโครงการความรับผิดชอบต่อสังคม (CSR) ของฝ่ายกิจการสังคมของผู้ปฏิบัติงานไฟฟ้าฝ่ายผลิตแห่งประเทศไทย* [การค้นคว้าอิสระปริญญามหาบัณฑิต], มหาวิทยาลัยธรรมศาสตร์.
- ปรมะ สตะเวทิน. (2546). *หลักนิเทศศาสตร์*. ภาพพิมพ์.

- บริษัท ปตท. จำกัด (มหาชน). (2568). แบบแสดงรายการข้อมูลประจำปี/รายงานประจำปี 2567 (แบบ 56-1 One Report).
- มาริสา จันเกตุ. (2566). กระบวนการวางแผนการสื่อสารเพื่อบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ของบริษัท ปตท. จำกัด (มหาชน) [การค้นคว้าอิสระปริญญามหาบัณฑิต], มหาวิทยาลัยธรรมศาสตร์.
- วาทีณี เจริญพงษ์. (2565). การเปิดรับข่าวสาร ทักษะคิด และแนวโน้มการมีส่วนร่วมต่อเรื่องการเปลี่ยนผ่านสู่ดิจิทัลของพนักงาน บริษัท พีทีที โกลบอล เคมิคอล จำกัด (มหาชน) [การค้นคว้าอิสระปริญญามหาบัณฑิต], มหาวิทยาลัยธรรมศาสตร์.
- วฤณ ประเสริฐสร. (2559). การเปิดรับ ความต้องการสื่อและข้อมูลข่าวสาร และความพึงพอใจที่ได้รับจากการเข้าร่วมกิจกรรมฝึกอบรมในโครงการพัฒนาบุคลากร [การค้นคว้าอิสระปริญญามหาบัณฑิต], มหาวิทยาลัยธรรมศาสตร์.
- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ. (2569). ข่าวสารภัยคุกคามทางไซเบอร์ [ชุดข้อมูล]. NCSA Open Data.
- สรารุช อนันตชาติ, และเนตรชนก พึ่งเกษม. (2550). การสื่อสารภายในองค์กร และการประชาสัมพันธ์. สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.
- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2567). รายงานประจำปี 2567.
- สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2568). สถิติภัยคุกคามทางไซเบอร์ 2568.
- สุพานี สฤษฏ์วานิช. (2552). พฤติกรรมองค์การสมัยใหม่: แนวคิดและทฤษฎี. โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์.
- สุรพงษ์ โสธนะเสถียร. (2533). การสื่อสารกับสังคม. สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

เสมอ นิ่มเงิน. (2563, 15 ธันวาคม). *Generation กับพฤติกรรมการรับข่าวสารผ่านสื่อต่างๆ*. กรมประชาสัมพันธ์.

อรรธรณ ปิลันธน์โอวาท. (2554). *การสื่อสารเพื่อการโน้มน้าวใจ*. สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

อภิญา รัตนารักษ์. (2559). *ปัจจัยที่ส่งเสริมให้พนักงานในองค์กรแสดงออกถึงพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ* [การค้นคว้าอิสระปริญญามหาบัณฑิต], มหาวิทยาลัยธรรมศาสตร์.

อภิญา เวชกิจ. (2567). *การเปิดรับข่าวสารออนไลน์ของกรมป้องกันและบรรเทาสาธารณภัยกับความพร้อมในการรับมือภัยพิบัติแผ่นดินไหวของคนวัยทำงานในกรุงเทพมหานคร* [การค้นคว้าอิสระปริญญามหาบัณฑิต], มหาวิทยาลัยธรรมศาสตร์.

ภาษาอังกฤษ

Allianz Commercial. (2025). *Allianz Risk Barometer 2025*.

Cybersecurity and Infrastructure Security Agency. (2026). *CISA's 2025 year in review: Driving security and resilience across critical infrastructure*.

European Union Agency for Cybersecurity. (2025). *ENISA Threat Landscape 2025*.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1).

World Economic Forum. (2025). *Global cybersecurity outlook 2025*.