



ดุษฎีนิพนธ์

การศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศ
ของแพลตฟอร์มออนไลน์โดว่ยีน

A STUDY ON INFORMATION SYSTEM SECURITY MANAGEMENT
STRATEGIES OF THE DOUYIN ONLINE PLATFORM

LIU YIN

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

คณะนิติศาสตร์

มหาวิทยาลัยราชภัฏรำไพพรรณี

พ.ศ. 2568

การศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศ
ของแพลตฟอร์มออนไลน์ไต้หวัน

A STUDY ON INFORMATION SYSTEM SECURITY MANAGEMENT
STRATEGIES OF THE DOUYIN ONLINE PLATFORM

LIU YIN

เสนอต่อมหาวิทยาลัยราชภัฏรำไพพรรณี เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ลิขสิทธิ์เป็นของมหาวิทยาลัยราชภัฏรำไพพรรณี

พ.ศ. 2568



ใบรับรองคุณวุฒิ

เรื่อง

การศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศ
ของแพลตฟอร์มออนไลน์ไต้วยิน
A STUDY ON INFORMATION SYSTEM SECURITY MANAGEMENT
STRATEGIES OF THE DOUYIN ONLINE PLATFORM

LIU YIN

คณะกรรมการสอบคุณวุฒิ

ประธานสอบคุณวุฒิ

(ผู้ช่วยศาสตราจารย์ ดร.พจนา รุ่แก้ว)

ประธานที่ปรึกษา
คุณวุฒิ

(อาจารย์ ดร.พิพัฒน์ แก้วตาธนาวัฒนา)

กรรมการที่ปรึกษา
คุณวุฒิ

(ผู้ช่วยศาสตราจารย์ ดร.จำเริญ คังคะศรี)

กรรมการที่ปรึกษา
คุณวุฒิ

(อาจารย์ ดร. นิสกร ยินดีจันทร์)

กรรมการสอบ
คุณวุฒิ

(รองศาสตราจารย์ ดร. อภิวรรณ ศิรินนทนา)

ได้รับอนุมัติจากมหาวิทยาลัยราชภัฏรำไพพรรณีให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชาการจัดการนวัตกรรมการสื่อสาร

คณบดีคณะนิเทศศาสตร์

(อาจารย์ ดร.พิพัฒน์ แก้วตาธนาวัฒนา)

วันที่ 8 เดือน ธันวาคม พ.ศ. 2568

Liu Yin. (2568). การศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน. ดุษฎีนิพนธ์. ปร.ด. (การจัดการนวัตกรรมการสื่อสาร). จันทบุรี : มหาวิทยาลัยราชภัฏรำไพพรรณี. อาจารย์ที่ปรึกษาดุษฎีนิพนธ์หลัก : อาจารย์ ดร.สุริพัฒน์ แก้วตาชนวัฒนา, ปร.ด.

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์ 1) เพื่อศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน 2) เพื่อพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ใช้วิธีวิจัยแบบผสมผสานระหว่างการวิจัยเชิงปริมาณ (Quantitative) เก็บรวบรวมข้อมูลจากกลุ่มผู้ใช้แพลตฟอร์มออนไลน์ใน 4 ภูมิภาคของประเทศไทย ประกอบด้วย (1) ภาคตะวันออกเฉียงเหนือ (2) ภาคเหนือ (3) ภาคตะวันออก (4) ภาคใต้ มณฑลทางตั้ง จำนวน 400 คน ใช้สถิติที่ใช้ในการวิเคราะห์ข้อมูลคือการแจกแจงความถี่ ค่าร้อยละ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน ทดสอบสมมติฐานด้วยสถิติ T-test, F-test วิเคราะห์ค่าความแปรปรวนทางเดียว (One-Way ANOVA) และการวิจัยเชิงคุณภาพ (Qualitative research) โดยการสัมภาษณ์เชิงลึก (In-Depth Interview) เจ้าหน้าที่ภาครัฐ ผู้บริหาร และผู้พัฒนาแพลตฟอร์มออนไลน์ ที่มีหน้าที่กำกับดูแลความปลอดภัยระบบสารสนเทศ จำนวน 20 คน

ผลการวิจัยพบว่า 1) แพลตฟอร์มออนไลน์ไต้หวันมีกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน 5 กลยุทธ์ ดังนี้ (1) กลยุทธ์การกำหนดระบบการจัดการความปลอดภัยสารสนเทศ (2) กลยุทธ์การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศ (3) กลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัย (4) กลยุทธ์การพัฒนาบุคลากรด้านความปลอดภัยสารสนเทศ (5) กลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ 2) พบว่ารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ได้พัฒนามาจากการนำข้อมูลการวิจัยเชิงปริมาณและข้อมูลการวิจัยเชิงคุณภาพมาวิเคราะห์และสังเคราะห์ และนำมาพัฒนาปรับปรุงสร้างเป็น CIA Triad โมเดล “รูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน” โดยมีรูปแบบการจัดการที่สำคัญ 3 ประการ ได้แก่ การปกป้องข้อมูลให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น การปกป้องความถูกต้องครบถ้วนของข้อมูลสารสนเทศ และความพร้อมใช้งานของระบบสารสนเทศที่มีความปลอดภัย

คำสำคัญ : การพัฒนารูปแบบ, การจัดการความปลอดภัย, ระบบสารสนเทศ, แพลตฟอร์มออนไลน์

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

Liu Yin (2025). **A Study on Information System Security Management Strategies of the Douyin Online Platform.** Dissertation Ph.D. (Communication Innovation Management). Chanthaburi : Rambhai Barni Rajabhat University. Principal Dissertation Advisor : Dr. Puripat Keawtathanawatthana, Ph.D.

Abstract

This research aimed to; 1) study the information system security management strategies of the Toyin online platform, and 2) to develop an information system security management model for the Toyin online platform. The research employed a mixed-methods approach. Data were collected from users of the online platform in four regions of China, which included: (1) Eastern region, Shandong Province, (2) Northern region, Liaoning Province, (3) Western region, Sichuan Province, and (4) Southern region, Guangdong Province, totaling to 400 participants. The statistics used for data analysis included frequency distribution, percentage, mean, and standard deviation. Hypothesis testing was conducted using T-test and F-test, one-way ANOVA analysis, and in-depth interviews were conducted with 20 individuals, including government officials, executives, and online platform developers responsible for information system security oversight.

The findings indicated that 1) the Online Douyin platform had strategies for managing information system security on the platform, consisting of 5 strategies as follows: (1) Strategy for establishing an information security management system, (2) Strategy for setting information system security objectives, (3) Strategy for defining security governance policies, (4) Strategy for developing information security personnel, (5) Strategy for building user trust in the online platform. 2) It was found that the information security management model of the Toyin online platform was developed by analyzing and synthesizing quantitative and qualitative research data, and then further developed and improved to create the CIA Triad model: 'Information Security Management Model of the Toyin Online Platform.' The model had three key management aspects: protecting data to be accessible only to authorized individuals, ensuring the integrity and accuracy of information, and maintaining the availability of a secure information system.

Keywords : Model Development, Safety Management, Information Systems, Online Platforms

กิตติกรรมประกาศ

ดุษฎีนิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดีเนื่องจากได้รับความอนุเคราะห์จาก อาจารย์ ดร. ภูมิพัฒน์ แก้วตาธนาวัฒนา อาจารย์ที่ปรึกษาหลัก และผู้ช่วยศาสตราจารย์ ดร.จำเริญ คังคะศรี อาจารย์ ดร. นิสากร ยินดีจันทร์ อาจารย์ที่ปรึกษาร่วม ซึ่งเป็นผู้ควบคุมดูแลดุษฎีนิพนธ์ ที่ได้กรุณาแก้ไข ตรวจสอบข้อบกพร่อง ตลอดจนให้ข้อเสนอแนะที่เป็นประโยชน์ในการทำวิจัยครั้งนี้ด้วยความเอาใจใส่ อย่างดียิ่งตลอดการทำดุษฎีนิพนธ์นี้ พร้อมทั้ง ผู้ช่วยศาสตราจารย์ ดร.พจนา รูปแก้ว ประธานกรรมการ สอบดุษฎีนิพนธ์ และรองศาสตราจารย์ ดร.อภิวรรณ ศิรินันทนา กรรมการสอบดุษฎีนิพนธ์ ที่กรุณาให้ข้อเสนอแนะในการทำดุษฎีนิพนธ์จนสมบูรณ์ ขอขอบพระคุณทุกท่านเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบพระคุณผู้ทรงคุณวุฒิที่เป็นผู้ให้ข้อมูลสำคัญทั้ง 20 ท่าน ที่ให้ความอนุเคราะห์ในการให้ ข้อมูลเชิงลึก การวิเคราะห์ SWOT และการสนทนากลุ่ม ขอขอบคุณผู้ใช้แพลตฟอร์มออนไลน์ไต่ถามที่ให้ ความกรุณาผู้วิจัยได้เข้าไปศึกษาเก็บข้อมูลเชิงประจักษ์ยังสถานที่ทั้ง 4 มณฑล อีกทั้งขอขอบพระคุณพร อาจารย์ เจ้าหน้าที่คณะนิเทศศาสตร์ มหาวิทยาลัยราชภัฏรำไพพรรณีทุกท่านที่อำนวยความสะดวกให้ความช่วยเหลือในด้านต่าง ๆ สุดท้ายนี้ขอกราบขอบพระคุณบิดา มารดา ที่ให้กำเนิดและสั่งสอนจน ผู้ทำวิจัยเป็นคนดีเสมอมา ครู อาจารย์ทุกท่านที่มอบความรู้มาโดยตลอด ผู้บังคับบัญชา เพื่อนร่วมงาน ครอบครัว รวมไปถึงคนรอบข้างที่เป็นกำลังใจคอยช่วยเหลือเสมอ ซึ่งเป็นส่วนช่วยผลักดันให้ผู้วิจัยทำดุษฎี นิพนธ์นี้จนสำเร็จได้ด้วยดี

ผู้ทำวิจัยหวังเป็นอย่างยิ่งว่าดุษฎีนิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อผู้ที่สนใจ เพื่อเป็นแนวทางใน การศึกษาและพัฒนาต่อไป

Liu Yin

กันยายน 2568

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

สารบัญ

บทที่		หน้า
บทที่ 1	บทนำ	1
	1.1 ที่มาและความสำคัญของปัญหา	1
	1.2 ปัญหาการวิจัย	6
	1.3 วัตถุประสงค์การวิจัย	6
	1.4 ขอบเขตการวิจัย	6
	1.5 ประโยชน์ที่คาดว่าจะได้รับ	6
	1.6 นิยามศัพท์เฉพาะ	7
	1.7 กรอบแนวคิดการวิจัย	8
บทที่ 2	แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง	10
	2.1 แนวคิดทฤษฎีเกี่ยวกับการพัฒนา	10
	2.2 แนวคิดทฤษฎีเกี่ยวกับรูปแบบ	11
	2.3 แนวคิดทฤษฎีเกี่ยวกับการจัดการและการจัดการการสื่อสาร	20
	2.4 แนวคิดทฤษฎีเกี่ยวกับสารสนเทศเครือข่าย	33
	2.5 แนวคิดทฤษฎีเกี่ยวกับความปลอดภัยของข้อมูลเครือข่าย	49
	2.6 แนวคิดทฤษฎีเกี่ยวกับสื่อใหม่	54
	2.7 งานวิจัยที่เกี่ยวข้อง	62
บทที่ 3	ระเบียบวิธีวิจัย	65
	3.1 แนวทางการวิจัย	66
	3.2 การวิจัยเชิงปริมาณ	67
	3.3 การวิจัยเชิงคุณภาพ	72

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

สารบัญ (ต่อ)

บทที่	หน้า
บทที่ 4 ผลการวิเคราะห์ข้อมูล	76
4.1 ผลการวิเคราะห์ข้อมูล	76
4.2 การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของ แพลตฟอร์มออนไลน์ไต่สวน	98
บทที่ 5 สรุป อภิปรายผล และข้อเสนอแนะ	105
5.1 สรุปผลการวิจัย	105
5.2 อภิปรายผลการวิจัย	114
5.3 ข้อเสนอแนะการวิจัย	119
บรรณานุกรม	122
ภาคผนวก	134
ภาคผนวก ก. แบบสอบถาม	135
ประวัติย่อผู้วิจัย	141

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

สารบัญตาราง

ตารางที่	หน้า
ตารางที่ 3.1 แสดงตารางขั้นตอนการศึกษาวิจัยตามวัตถุประสงค์ของการวิจัย	65
ตารางที่ 3.2 ขนาดกลุ่มตัวอย่างในแต่ละระดับความคลาดเคลื่อน	67

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

สารบัญภาพ

ภาพที่	หน้า
ภาพที่ 1.1 กรอบแนวคิดการวิจัย	9
ภาพที่ 2.1 รูปแบบเชิงระบบและสถานการณ์ (System Contingency Model) ของ Brown and Moberg (1980)	15
ภาพที่ 2.2 กระบวนการจัดการขององรี ฟาโย	26
ภาพที่ 2.3 กระบวนการจัดการของกูลิคและเออร์วิก	27
ภาพที่ 2.4 กระบวนการของแฮโรลด์ คูนตซ์	28
ภาพที่ 2.5 กระบวนการบริหารของ ดร.เอ็ดเวิร์ด เดมิง	29
ภาพที่ 4.1 กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน	97
ภาพที่ 4.2 รูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน	103
ภาพที่ 5.1 รูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน	113

บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ด้วยการพัฒนาอย่างรวดเร็วของเทคโนโลยีอินเทอร์เน็ต ที่ก่อให้เกิดสื่อดิจิทัลจึงกลายเป็นช่องทางสำคัญในการเผยแพร่ข้อมูล (Li Lihe & Li Hong, 2022) โดยเฉพาะอย่างยิ่งในประเทศจีน รัฐบาลให้ความสำคัญอย่างยิ่งต่อการจัดการและกฎระเบียบของเศรษฐกิจดิจิทัลและมุ่งมั่นที่จะสร้างสภาพแวดล้อมเครือข่ายที่ปลอดภัยและมีประสิทธิภาพผู้กำหนดนโยบายควบคุมและชี้แนะการพัฒนาสื่อดิจิทัลอย่างเหมาะสมผ่านชุดนโยบายและกฎหมายระดับชาติ (Gao Jing, 2022) โดยเฉพาะสำหรับแพลตฟอร์มวิดีโอสั้น เช่น Douyin ฝ่ายบริหารไซเบอร์สเปซของจีนประกาศใช้มาตรการสำหรับการบริหารการบริการข้อมูลทางอินเทอร์เน็ต โดยเน้นความรับผิดชอบของผู้ให้บริการข้อมูลในการรับรองความถูกต้องและถูกต้องตามกฎหมายของเนื้อหาที่เผยแพร่ นโยบายนี้กำหนดให้ผู้ให้บริการข้อมูลเครือข่ายทุกรายลงทะเลเบียนด้วยชื่อจริงและห้ามเผยแพร่เนื้อหาที่ผิดกฎหมายโดยเด็ดขาด นอกจากนี้ สำหรับข้อมูลที่เกี่ยวข้องกับความมั่นคงของชาติและความปลอดภัยสาธารณะแพลตฟอร์มจะต้องรายงานต่อหน่วยงานภาครัฐที่เกี่ยวข้องทันทีและลบข้อมูลที่เกี่ยวข้องเพื่อให้แน่ใจว่าจะไม่ก่อให้เกิดผลกระทบทางสังคมขนาดใหญ่ จีนได้เสริมสร้างกรอบกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคล คือกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act : PIPL) มีผลบังคับใช้อย่างเป็นทางการในเดือนพฤศจิกายน 2564 กฎหมายนี้มีจุดมุ่งหมายเพื่อปกป้องความปลอดภัยของข้อมูลส่วนบุคคลของประชาชนที่ใช้อินเทอร์เน็ตเพื่อเป็นการป้องกันการรั่วไหลของข้อมูลและการละเมิด (Wang Liming & Ding Xiaodong, 2021) ตามกฎหมายนี้ทุกหน่วยงานที่เกี่ยวข้องกับการรวบรวมและประมวลผลข้อมูลส่วนบุคคลเหล่านี้ ต้องชี้แจงวัตถุประสงค์วิธีการ และขอบเขตของการประมวลผลข้อมูล และต้องไม่ทำการรวบรวมหรือใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากผู้ใช้ ทำให้เกิดข้อกำหนดที่สูงขึ้นสำหรับแพลตฟอร์มต่าง ๆ เช่น Douyin ในการจัดการข้อมูลของผู้ใช้ (Zhao Jinru, 2024) นอกจากนี้ สำหรับการจัดการเนื้อหาในโลกไซเบอร์ ประเทศจีนยังได้กำหนดกฎระเบียบการกำกับดูแลระบบนิเวศน์เนื้อหาในอินเทอร์เน็ต ซึ่งกำหนดให้ต้องเสริมสร้างกลไกการตรวจสอบเนื้อหาออนไลน์ให้เข้มแข็งและห้ามการแพร่กระจายของภาพอนาจาร ความรุนแรง การฉ้อโกง และข้อมูลผิดกฎหมายอื่น ๆ อย่างเคร่งครัด (ฟางหยู, 2563)

นโยบายนี้ยังเน้นย้ำถึงความสำคัญของการเสริมสร้างการประชาสัมพันธ์เชิงบวกและเผยแพร่ค่านิยมหลักสังคมนิยมของประเทศอย่างจริงจัง เพื่อให้แน่ใจว่าเนื้อหาที่มีอยู่ในสื่อออนไลน์มีความถูกต้องตามกฎหมายที่เกี่ยวข้องกับความปลอดภัยของข้อมูล กฎหมายความปลอดภัยของข้อมูลได้ประกาศใช้อย่างเป็นทางการในปี พ.ศ.2564 (2021) กฎหมายนี้มีข้อกำหนดด้านความปลอดภัยและมาตรการกำกับดูแลสำหรับกิจกรรมการประมวลผลข้อมูล และการป้องกันความเสี่ยงที่อาจเกิดขึ้นในกิจกรรมการสื่อสารข้อมูลอย่างชัดเจนและกำหนดให้องค์กรต่าง ๆ ต้องสร้างและปรับปรุงระบบการจัดการความปลอดภัยของข้อมูล และปรับปรุงความสามารถในการป้องกันความปลอดภัยของข้อมูล (Liu Guifeng et al., 2564)

นโยบายของจีนด้านความปลอดภัยของระบบข้อมูลของผู้ใช้อินเทอร์เน็ตได้มีการปรับปรุงอย่างต่อเนื่องเพื่อปรับให้เข้ากับความต้องการการพัฒนาในยุคดิจิทัล รัฐบาลจีนได้กำหนดข้อกำหนดที่ชัดเจนสำหรับการจัดการความปลอดภัยของข้อมูลของแพลตฟอร์มอินเทอร์เน็ตผ่านกฎหมายและข้อบังคับ โดยเฉพาะอย่างยิ่งแพลตฟอร์มวิดีโอสั้น เช่น Douyin โดยมีเป้าหมายเพื่อสร้างสภาพแวดล้อมข้อมูลออนไลน์ที่ปลอดภัยและเป็นระเบียบมากขึ้น ด้วยมาตรการเหล่านี้ความเสี่ยงด้านความปลอดภัยของข้อมูลในโลกไซเบอร์สามารถได้รับการจัดการและลดผลกระทบเชิงลบได้อย่างมีประสิทธิภาพตลอดจนสามารถปกป้องผลประโยชน์สาธารณะและความมั่นคงของชาติได้

ในฐานะแพลตฟอร์มออนไลน์ที่มีประสิทธิภาพในการแบ่งปันวิดีโอสั้นชั้นนำของจีนกลไกการเผยแพร่ข้อมูลของ Douyin มีประสิทธิภาพและเผยแพร่ได้กว้างขวาง (Liu Wanyi, 2022) แพลตฟอร์มดังกล่าวประสบความสำเร็จในการแพร่กระจายข้อมูลอย่างรวดเร็วและกว้างขวางผ่านระบบการแนะนำอัลกอริทึม การโต้ตอบกับผู้ใช้ และการสร้างเนื้อหาที่หลากหลาย (Liu Rushi, 2022) กลไกการสื่อสารหลักของ Douyin คือระบบการแนะนำตามอัลกอริทึมระบบนี้สามารถแนะนำเนื้อหาที่ผู้ใช้อาจสนใจได้อย่างชาญฉลาดโดยพิจารณาจากข้อมูล เช่น ประวัติการเข้าชมของผู้ใช้ พฤติกรรมเชิงโต้ตอบ เช่น การถูกใจ ความคิดเห็น และการแชร์ และเวลาในการดูวิดีโอ (Guo Kejing, 2020) คำแนะนำส่วนบุคคลประเภทนี้ช่วยเพิ่มการมีส่วนร่วมของผู้ใช้และความเหนียวแน่นของแพลตฟอร์มได้อย่างมาก ในขณะเดียวกันก็เร่งการแพร่กระจายของข้อมูลด้วย ตามสถิติ ผู้ใช้มากกว่าร้อยละ 70 เรียกดูเนื้อหาผ่านฟังก์ชัน การแนะนำสำหรับผู้ใช้ ซึ่งแสดงให้เห็นถึงความสำคัญของการแนะนำอัลกอริทึมในการเผยแพร่ข้อมูล Douyin (Li Xizi, 2020) การโต้ตอบของผู้ใช้ยังเป็นปัจจัยสำคัญในการส่งเสริมการเผยแพร่ข้อมูล Douyin (Zhao Yifan, 2022) ผู้ใช้ไม่เพียงสามารถโต้ตอบผ่านการกดไลค์ ความคิดเห็น และการแชร์แต่ยังเพิ่มการมองเห็นเนื้อหาของพวกเขาด้วยการเข้าร่วมในการทำทายโดยใช้เพลงยอดนิยมและแฮชแท็ก (Wang Fuchen, 2021) การโต้ตอบนี้ไม่เพียงแต่ปรับปรุงความรู้สึกของผู้ใช้ในการมีส่วนร่วมในเนื้อหา แต่ยังช่วยให้เนื้อหากลายเป็นที่นิยมอย่างรวดเร็วบนแพลตฟอร์ม ทำให้เกิดสิ่งที่เรียกว่าวิดีโอ ยอดนิยม และส่งเสริมการแพร่กระจายของข้อมูล ผู้สร้างเนื้อหาที่มีบทบาทสำคัญใน Douyin แพลตฟอร์มดังกล่าวสนับสนุนเนื้อหาต้นฉบับและสนับสนุนการผลิตเนื้อหาคุณภาพสูงผ่านสิ่งจูงใจ เช่น โปรแกรมรางวัลผู้สร้าง ผู้สร้างสามารถดึงดูดผู้ชมจำนวนมากได้อย่างรวดเร็วด้วยการผลิตวิดีโอที่เกี่ยวข้องอย่างใกล้ชิดกับเหตุการณ์ปัจจุบัน วัฒนธรรมสมัยนิยม หรือความสนใจของผู้ใช้ ตัวอย่างเช่น หัวข้อยอดนิยมบน Douyin เช่น เคล็ดลับชีวิต หรือ ทักษะการเรียน มักจะดึงดูดคลิกและความคิดเห็นนับล้านครั้ง ซึ่งแสดงให้เห็นถึงบทบาทของเนื้อหาคุณภาพสูงในการส่งเสริมการเผยแพร่ข้อมูล Douyin ยังได้ขยายขอบเขตของการเผยแพร่ข้อมูลผ่านการบูรณาการหลายแพลตฟอร์ม (Chen Qiang & Peng Yating, 2022) วิดีโอ Douyin จำนวนมากไม่เพียงแต่เผยแพร่อย่างกว้างขวางบนแพลตฟอร์มออนไลน์ Douyin เท่านั้นแต่ยังแพร่กระจายผ่านการแชร์ฟังก์ชันกับแพลตฟอร์มโซเชียลมีเดียอื่น ๆ เช่น Weibo และ WeChat นอกจากนี้ Douyin ยังได้ขยายอิทธิพลในตลาดต่างประเทศผ่านแอปพลิเคชัน TikTok ทำให้เนื้อหาสามารถเผยแพร่ข้ามวัฒนธรรมและพรมแดนได้ (Duan Peng, 2022) ด้วยกลไกข้างต้น Douyin ประสบ

ความสำเร็จในการสร้างแพลตฟอร์มเผยแพร่ข้อมูลเชิงโต้ตอบที่มีประสิทธิภาพซึ่งไม่เพียงตอบสนองความต้องการด้านความบันเทิงของผู้ใช้หลายร้อยล้านคนเท่านั้น แต่ยังกลายเป็นเครื่องมือเผยแพร่ข้อมูลทางสังคมที่สำคัญอีกด้วย

ในฐานะหนึ่งในแพลตฟอร์มวิดีโอสั้นที่ได้รับความนิยมมากที่สุดในโลกการเผยแพร่ข้อมูลของ Douyin มีอิทธิพลอย่างกว้างขวางและมีประสิทธิภาพสูง แต่ยังคงเผชิญกับปัญหาและความท้าทายหลายประการ โดยเฉพาะอย่างยิ่งในแง่ของการจัดการความปลอดภัยของข้อมูลความท้าทายของการกลั่นกรองเนื้อหาเป็นหนึ่งในปัญหาหลักที่ Douyin เผชิญอยู่เนื่องจากแพลตฟอร์มออนไลน์อื่น ๆ สร้างวิดีโอจำนวนมากทุกวัน แม้ว่าจะใช้เทคโนโลยีอัลกอริทึมขั้นสูงเพื่อช่วยในการตรวจสอบด้วยตนเอง แต่ก็ยังเป็นเรื่องยากที่จะตรวจสอบและกรองเนื้อหาที่ผิดกฎหมายทั้งหมดได้อย่างสมบูรณ์ (Chen Liangfei, 2021) ข้อมูลที่ไม่ถูกต้อง ข่าวลือ และแม้แต่เนื้อหาที่ผิดกฎหมาย บางครั้งอาจผ่านกลไกการกลั่นกรองและแพร่กระจายอย่างกว้างขวาง เช่น เนื้อหาที่ไม่เหมาะสมบางรายการมุ่งเป้าไปที่ผู้เยาว์หรือวิดีโอที่ละเมิดลิขสิทธิ์มักจะดึงดูดความสนใจของสาธารณชน แต่กลับสร้างปัญหาการรั่วไหลของความเป็นส่วนตัวที่รุนแรงมากขึ้นเช่นกัน (Zhang Meijie, 2023) แพลตฟอร์ม Douyin รวบรวมข้อมูลผู้ใช้งานจำนวนมาก รวมถึงข้อมูลตำแหน่ง ข้อมูลอุปกรณ์ พฤติกรรมการท่องเว็บ ฯลฯ หากข้อมูลนี้ไม่ได้รับการปกป้องอย่างเหมาะสม ข้อมูลดังกล่าวอาจถูกละเมิดหรือแฮ็กได้ง่าย ตามรายงานพบว่าแอปพลิเคชันอื่น ๆ บางตัวได้รับข้อมูลส่วนบุคคลจากผู้ใช้ Douyin ด้วยวิธีการที่ไม่เหมาะสมทำให้ผู้ใช้กังวลเกี่ยวกับความปลอดภัยของข้อมูลของตน นอกจากนี้ การแพร่กระจายของข้อมูลผ่าน Douyin ยังอาจนำไปสู่ความแตกแยกทางสังคม (Zhan Chengyu & Xu Mingjing, 2023) เนื่องจากเนื้อหาบนแพลตฟอร์มถูกกำหนดโดยคำแนะนำจากอัลกอริทึม และผู้ใช้อาจจะเห็นเฉพาะข้อมูลที่สอดคล้องกับมุมมองของตนเองเท่านั้นซึ่ง อาจทำให้ปรากฏการณ์ละเมิดข้อมูลหรือการกระทำผิดในสังคมรุนแรงขึ้นในระยะยาว ผลกระทบเชิงลบด้านข้อมูลนี้อาจส่งผลให้ผู้ใช้ไม่เข้าใจและไม่สามารถยอมรับมุมมองที่แตกต่างกันได้ ส่งผลให้เกิดความขัดแย้งทางสังคมรุนแรงขึ้น Douyin ยังอาจใช้เป็นเครื่องมือโฆษณาชวนเชื่อเมื่อเผยแพร่ข้อมูล องค์กรหรือบุคคลบางส่วนอาจใช้อิทธิพลของแพลตฟอร์มเพื่อจงใจเผยแพร่ข้อมูลที่ทำให้เข้าใจผิดหรือดำเนินการโฆษณาชวนเชื่อทางการเมืองซึ่งอาจเป็นภัยคุกคามต่อระเบียบสังคม และการตัดสินใจตามระบอบประชาธิปไตย แพลตฟอร์มจำเป็นต้องเสริมสร้างการกำกับดูแลการละเมิดที่อาจเกิดขึ้นนี้ และรับประกันความเป็นธรรมและความถูกต้องของการเผยแพร่ข้อมูล โดยตรงในฐานะแพลตฟอร์มเผยแพร่ข้อมูลที่มีประสิทธิภาพ Douyin ต้องเผชิญกับความท้าทายที่ค่อนข้างร้ายแรงในการจัดการความปลอดภัยของข้อมูลในขณะเดียวกันก็ให้ความบันเทิงและการแบ่งปันข้อมูลผู้ใช้บริการแพลตฟอร์มจำเป็นต้องปรับปรุงเทคโนโลยีและนโยบายอย่างต่อเนื่องเพื่อให้อย่างมั่นใจในความปลอดภัยและความถูกต้องของข้อมูลรวมถึงปกป้องความเป็นส่วนตัวและสิทธิ์ของผู้ใช้ในเวลาเดียวกันผู้ใช้ควรปรับปรุงความสามารถในการระบุข้อมูลของตนเอง ระวังภัยเกี่ยวกับเนื้อหาบนแพลตฟอร์ม และร่วมกันรักษาการพัฒนาสภาพแวดล้อมออนไลน์ให้ดีขึ้น

ในช่วงห้าปีที่ผ่านมา Douyin เป็นแอปพลิเคชันวิดีโอสั้น ๆ เติบโตอย่างต่อเนื่องทั่วโลก และอัตราการเติบโตของผู้ใช้ และกิจกรรมที่เผยแพร่ในแพลตฟอร์ม ก็แข่งขันแพลตฟอร์มโซเชียลมีเดียอื่น ๆ มาก

(Zheng, 2023) จากข้อมูลของ Sensor Tower Douyin และ TikTok เวอร์ชัน พบว่าในปี 2020 เพียงปีเดียวทั่วโลกมียอดดาวน์โหลดมากกว่า 2 พันล้านครั้ง และพบว่าตั้งแต่ปี 2561 (Huang, 2021) ในตลาดสหรัฐอเมริกา เอเชียตะวันออกเฉียงใต้ และยุโรป การเติบโตของ Douyin สูงมาก

เนื่องจากนโยบายรัฐบาลที่เข้มงวดทำให้การดาวน์โหลดเพื่อใช้งาน TikTok ในต่างประเทศทั่วโลกมีอัตราการเติบโตอย่างมีนัยที่น่าสนใจในปี 2023 มากถึง 75% (Ryu, 2024) อัตราการเติบโตนี้เร็วกว่าการเติบโตของ Facebook และ Instagram ในช่วงเวลาเดียวกันอย่างมาก ในแง่ของผู้ใช้งาน ตามรายงานของ App Annie ผู้ใช้งานรายเดือน (MAU) ของ Douyin จะสูงถึง 800 ล้านรายในปี 2566 เพิ่มขึ้นสองเท่าจาก 400 ล้านรายในปี 2562 (Lv, 2023) การเติบโตของผู้ใช้งาน Instagram ต่อเดือนเพิ่มขึ้นจาก 1 พันล้านเป็น 1.3 พันล้านคน ซึ่งเป็นอัตราการเติบโตยังน้อยกว่า Douyin มากสิ่งนี้สะท้อนให้เห็นถึงข้อได้เปรียบที่เป็นเอกลักษณ์ของ Douyin ในการดึงดูดและรักษาผู้ใช้ โดยเฉพาะในกลุ่มผู้ใช้งานอายุน้อย ในแง่ของการมีส่วนร่วมของผู้ใช้ Douyin ยังแสดงให้เห็นถึงความน่าดึงดูดที่เป็นเอกลักษณ์อีกด้วย ตามสถิติเวลาใช้งานเฉลี่ยต่อวันของผู้ใช้ Douyin คือมากกว่า 52 นาที ในขณะที่เวลาการใช้งานเฉลี่ยต่อวันของผู้ใช้ Instagram และ Facebook คือ 30 นาที และ 20 นาที ตามลำดับ (Roberts & David, 2023) ข้อมูลนี้แสดงให้เห็นว่า Douyin มีประสิทธิภาพมากขึ้นในการรักษาความเหนียวแน่นของผู้ใช้และเพิ่มการโต้ตอบของผู้ใช้ นอกจากนี้รายได้ของผู้สร้างเนื้อหายังเป็นจุดเด่นของ Douyin อีกด้วยจากการศึกษาเปรียบเทียบรายได้ของผู้สร้างเนื้อหาบน Douyin และ YouTube พบว่า Douyin มอบโอกาสในการสร้างรายได้และการสนับสนุนแพลตฟอร์มที่มากขึ้น ทำให้ผู้สร้างจำนวนมากชอบดำเนินการบนแพลตฟอร์ม Douyin (Huang & Ye, 2024) สิ่งนี้ไม่เพียงแต่ช่วยเพิ่มความหลากหลายของเนื้อหาบนแพลตฟอร์มแต่ยังส่งเสริมการผลิตเนื้อหาคุณภาพสูงมากขึ้นอีกด้วย Douyin ไม่เพียงแต่มีการเติบโตอย่างรวดเร็วของผู้ใช้งานทั่วโลกในช่วง 5 ปีที่ผ่านมาเท่านั้น แต่กิจกรรมและการมีส่วนร่วมของผู้ใช้งานยังสูงกว่าแพลตฟอร์มโซเชียลมีเดียกระแสหลักอื่น ๆ อย่างมากอีกด้วย แนวโน้มนี้แสดงให้เห็นว่า Douyin กลายเป็นกำลังที่ไม่อาจเพิกเฉยได้ในวงการสื่อดิจิทัลระดับโลก และยังทำให้เกิดข้อจำกัดที่สูงขึ้นสำหรับการจัดการความปลอดภัยของข้อมูลอีกด้วย

ในฐานะแพลตฟอร์มแบ่งปันวิดีโอสั้นชั้นนำของโลก ปัญหาด้านความปลอดภัยในการเผยแพร่ข้อมูลของ Douyin ไม่เพียงส่งผลกระทบเชิงบวกต่อผู้ใช้ส่วนใหญ่เท่านั้น แต่ยังส่งผลกระทบเชิงลบอย่างหลีกเลี่ยงไม่ได้ต่อผู้ใช้ที่มีหลากหลายกลุ่ม เช่น ผู้สร้างเนื้อหา ผู้เยาว์ และผู้ลงโฆษณา สำหรับผู้ใช้ทั่วไปปัญหาด้านความปลอดภัยของข้อมูลส่วนใหญ่จะเกิดจากการรั่วไหลของข้อมูลส่วนบุคคล การแพร่กระจายของเนื้อหาที่ทำให้เข้าใจผิด และการฉ้อโกงทางออนไลน์ ตามรายงานความปลอดภัยของข้อมูลโซเชียลมีเดียทั่วโลกปี 2023 ผู้ใช้ประมาณ 30% ประสบปัญหาด้านความปลอดภัยกับบัญชีโซเชียลมีเดีย เช่น การโจรกรรมบัญชีหรือการรั่วไหลของข้อมูลส่วนบุคคล (Senapati et al., 2023) ปัญหาดังกล่าวเกี่ยวข้องกับโดยตรงกับสิทธิ์ความเป็นส่วนตัวและความปลอดภัยของทรัพย์สินของผู้ใช้และเพิ่มความไม่ไว้วางใจของผู้ใช้ในแพลตฟอร์มสำหรับผู้สร้างเนื้อหา ความไม่มั่นคงของข้อมูลบนแพลตฟอร์ม Douyin อาจนำไปสู่การขโมยเนื้อหาต้นฉบับ ข้อพิพาทด้านลิขสิทธิ์และการสูญเสียรายได้ (Sengelmann, 2020) การสำรวจ

ผู้สร้างเนื้อหาทำเงินมากกว่า 40% พบว่า ผลงานของพวกเขาถูกคัดลอกหรือพิมพ์ซ้ำโดยไม่ได้รับอนุญาต สิ่งนี้ไม่เพียงละเมิดสิทธิ์ในทรัพย์สินทางปัญญาของผู้สร้างเท่านั้น แต่ยังส่งผลกระทบต่อความตั้งใจในการสร้างสรรค์และผลประโยชน์ทางเศรษฐกิจของพวกเขาด้วย สำหรับผู้เยาว์พวกเขาเสี่ยงต่อข้อมูลที่ไม่ปลอดภัยมากกว่าเนื่องจากขาดความสามารถในการระบุตัวตนที่จำเป็น (Seo, 2021) ซึ่งรวมถึงประเด็นต่าง ๆ เช่น การเปิดเผยเนื้อหาที่ไม่เหมาะสม การกลั่นแกล้งบนอินเทอร์เน็ต และการละเมิดความเป็นส่วนตัว ตามสถิติ ผู้ใช้ที่ยังไม่บรรลุนิติภาวะประมาณ 25% พบพฤติกรรมที่ไม่เป็นมิตรหรือการฉ้อโกงข้อมูลทางออนไลน์ (Paat & Markham, 2021) สถานการณ์นี้พบได้บ่อยโดยเฉพาะบนแพลตฟอร์มที่ไม่มีมาตรการกำกับดูแลที่มีประสิทธิภาพสำหรับผู้ลงโฆษณา ปัญหาด้านความปลอดภัยของข้อมูลอาจส่งผลให้ภาพลักษณ์ของแบรนด์เสียหายและผลตอบแทนจากการลงทุนลดลง หากเนื้อหาโฆษณาฝังอยู่กับข้อมูลที่เป็นอันตรายหรือเกี่ยวข้องกับเนื้อหาที่ไม่เหมาะสมอาจสร้างความน่ารังเกียจให้กับผู้บริโภคและส่งผลกระทบต่อชื่อเสียงของแบรนด์ การสำรวจผู้ลงโฆษณาระดับองค์กร พบว่าเกือบ 35% ของบริษัทได้ปรับเปลี่ยนหรือขัดขวางการโฆษณาเนื่องจากปัญหาด้านความปลอดภัยของข้อมูลบนแพลตฟอร์มโซเชียลมีเดีย การเผยแพร่ข้อมูล Douyin ที่ไม่ปลอดภัยส่งผลกระทบอย่างมากต่อคนหลายกลุ่ม ซึ่งผู้ใช้ทั่วไปและผู้เยาว์มีความเสี่ยงมากกว่าปกติ และมีความต้องการแพลตฟอร์มที่ไม่เพียงแต่เสริมสร้างมาตรการป้องกันทางเทคนิคเท่านั้นแต่ยังต้องปรับปรุงการรับรู้ด้านความปลอดภัยของข้อมูลของผู้ใช้และความสามารถในการป้องกันตนเอง เพื่อลดผลกระทบด้านลบของความไม่มั่นคงของข้อมูล

โต่วยีน (Douyin) ในฐานะแพลตฟอร์มแบ่งปันวิดีโอสั้นชั้นนำของโลกและเนื่องจากเนื้อหาบนแพลตฟอร์มถูกกำหนดโดยคำแนะนำจากอัลกอริทึมและผู้ใช้มักจะเห็นเฉพาะข้อมูลที่สอดคล้องกับมุมมองของตนเองเท่านั้น ผลกระทบเชิงลบด้านข้อมูลนี้อาจส่งผลให้ผู้ใช้ไม่เข้าใจและไม่สามารถยอมรับมุมมองที่แตกต่างกันได้ ส่งผลให้เกิดความขัดแย้งทางสังคมรุนแรงขึ้นและ Douyin ยังอาจถูกใช้เป็นเครื่องมือโฆษณาชวนเชื่อเพื่อเผยแพร่ข้อมูล องค์กรหรือบุคคลบางส่วนอาจใช้ข้อดีและอิทธิพลของแพลตฟอร์มเพื่อจูงใจเผยแพร่ข้อมูลที่ทำให้เข้าใจผิดหรือดำเนินการโฆษณาชวนเชื่อทางการเมืองซึ่งอาจเป็นภัยคุกคามต่อระเบียบสังคม และปัญหาด้านความปลอดภัยในการเผยแพร่ข้อมูลของ Douyin ไม่เพียงส่งผลกระทบเชิงบวกต่อผู้ใช้ส่วนใหญ่เท่านั้น แต่ยังส่งผลกระทบเชิงลบอย่างหลีกเลี่ยงไม่ได้ต่อผู้ใช้ที่มีหลากหลายกลุ่ม เช่น ผู้สร้างเนื้อหา ผู้เยาว์ และผู้ลงโฆษณา สำหรับผู้ใช้ทั่วไป ปัญหาด้านความปลอดภัยของข้อมูลส่วนใหญ่จะเกิดจากการรั่วไหลของข้อมูลส่วนบุคคล การแพร่กระจายของเนื้อหาที่ทำให้เข้าใจผิด และการฉ้อโกงทางออนไลน์ ตามรายงานความปลอดภัยของข้อมูลโซเชียลมีเดีย ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในทุกมิติของชีวิตประจำวัน ตั้งแต่การสื่อสารส่วนบุคคลไปจนถึงการทำธุรกรรมทางธุรกิจ ความสำคัญของการจัดการความปลอดภัยสารสนเทศ (Information Security Management) ได้เพิ่มขึ้นอย่างทวีคูณ แพลตฟอร์มออนไลน์และนวัตกรรมที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI) ได้นำมาซึ่งศักยภาพมหาศาลในการอำนวยความสะดวกและสร้างประโยชน์ทางเศรษฐกิจและสังคม แต่ในขณะเดียวกันก็ก่อให้เกิดความท้าทายใหม่ ๆ ในการจัดการกับภัยคุกคามทางไซเบอร์และการปกป้องข้อมูลส่วนบุคคลของ

ผู้ใช้ จากเหตุผลดังกล่าวผู้วิจัยจึงสนใจที่จะศึกษาการพัฒนาการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน (DouYin)

1.2 ปัญหาการวิจัย

1. กลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน (Douyin) เป็นอย่างไร
2. รูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน (Douyin) ควรเป็นการพัฒนารูปแบบการจัดการเพื่อความปลอดภัยระบบสารสนเทศอย่างไร

1.3 วัตถุประสงค์การวิจัย

1. เพื่อศึกษากลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน
2. การพัฒนารูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน

1.4 ขอบเขตการวิจัย

การพัฒนารูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน ครั้งนี้ ผู้วิจัยดำเนินการศึกษา ดังปรากฏรายละเอียดดังต่อไปนี้

1. ขอบเขตด้านเนื้อหา มุ่งศึกษากลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน และการพัฒนารูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน
2. ขอบเขตด้านประชากรที่ใช้ในการศึกษา คือ เจ้าหน้าที่ภาครัฐผู้กำกับดูแล ควบคุมการจัดการความปลอดภัยสื่อออนไลน์ ผู้บริหารแพลตฟอร์มออนไลน์ไต้ยีน บล็อกเกอร์ผู้พัฒนาแพลตฟอร์มไต้ยีน และผู้ใช้แพลตฟอร์มไต้ยีน
3. ขอบเขตด้านพื้นที่ ที่ใช้ในการศึกษาทั่วทั้ง 4 ภูมิภาคในประเทศจีน คือ 1) ภาคตะวันออก มณฑลซานตง 2) ภาคเหนือ มณฑลเหอหนาน 3) ภาคตะวันตก มณฑลเสฉวน 4) ภาคใต้ มณฑลกวางตุ้ง
4. ขอบเขตด้านเวลา ใช้เวลาในการเตรียมข้อมูล จัดลำดับข้อมูล พร้อมทั้งแจกแบบสอบถาม การสัมภาษณ์ และนำผลมาวิเคราะห์ข้อมูล ใช้ระยะเวลาการวิจัย เริ่มตั้งแต่วันที่ 4 มกราคม 2568 ถึง 30 สิงหาคม 2568

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ทราบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน เพื่อใช้เป็นแนวทางหลักในการดำเนินการส่งเสริมและพัฒนาการจัดการความปลอดภัยสารสนเทศ
2. ผลการวิจัยทำให้ผู้ที่มีส่วนเกี่ยวข้องทุกภาคส่วนของแพลตฟอร์มออนไลน์ไต้ยีนได้ทราบและสามารถนำหลักการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีนไปใช้ประโยชน์

3. สามารถนำผลการวิจัยไปกำหนดเป็นแนวทางหรือปรับใช้เกี่ยวกับการส่งเสริมหรือพัฒนาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยนได้อย่างมีประสิทธิภาพ

4. ผลของกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยน ซึ่งเป็นส่วนสำคัญที่ใช้เป็นแนวทางสนับสนุนและการป้องกันสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยนให้เกิดความปลอดภัยตามหลักกฎหมายและนโยบายภาครัฐ

5. ได้ผลการวิเคราะห์กลยุทธ์การจัดการสารสนเทศเพื่อความปลอดภัยของข้อมูล ซึ่งจะได้สารสนเทศของการพัฒนากลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยนเพื่อพัฒนาข้อมูลให้เกิดความปลอดภัยมากยิ่งขึ้น

6. ได้แนวทางในการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยน หน่วยงานทั้งภาครัฐ และภาคเอกชน หรือธุรกิจที่มีส่วนเกี่ยวข้องกับการสื่อสารออนไลน์ สามารถนำไปใช้ในการวางแผนส่งเสริมความปลอดภัยระบบสารสนเทศได้

7. ผู้ที่มีส่วนเกี่ยวข้องทุกภาคส่วนสามารถนำกลยุทธ์ วิธีการ รูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยน ไปใช้ประโยชน์ในพื้นที่ต่าง ๆ ในมณฑลอื่น ๆ ได้

8. หน่วยงานที่มีส่วนเกี่ยวข้องทุกภาคส่วน สามารถนำผลการศึกษาไปพัฒนาเป็นแผนในการจัดการความปลอดภัยสารสนเทศในสื่อออนไลน์ต่าง ๆ ให้มีมาตรฐานที่ดียิ่งขึ้นเป็นไปตามนโยบาย หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล

1.6 นิยามศัพท์เฉพาะ

การพัฒนา หมายถึง การจัดการการเปลี่ยนแปลงความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยนภายใต้นโยบายและกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้มีความปลอดภัยมากขึ้น เป็นไปในทางที่ดีที่ปลอดภัยกับระบบสารสนเทศสำหรับผู้พัฒนาแพลตฟอร์มออนไลน์และผู้ใช้แพลตฟอร์มออนไลน์โดยคำนึงถึงขั้นตอนการจัดการต่าง ๆ เพื่อยกระดับความปลอดภัยระบบสารสนเทศให้ดีขึ้น โดยมีการปรับปรุงพัฒนาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยนให้ดียิ่งขึ้นจนเป็นที่น่าเชื่อถือของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยน

กลยุทธ์การจัดการ หมายถึง ผู้บริหารแพลตฟอร์มออนไลน์ไต่ยนมีการกำหนดวิสัยทัศน์ ทิศทางภารกิจ และวัตถุประสงค์ของการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยนอย่างเป็นระบบ สามารถช่วยให้ผู้บริหารปรับตัวต่อนโยบายและกฎหมายคุ้มครองข้อมูลส่วนบุคคลของภาครัฐ และความต้องการด้านความปลอดภัยของผู้ใช้ เพื่อให้บรรลุเป้าหมายหรือวัตถุประสงค์ด้านความปลอดภัยระบบสารสนเทศที่ตั้งไว้

การจัดการความปลอดภัย หมายถึง การจัดการองค์รวมความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยนโดยมีการกำหนดนโยบายความปลอดภัยระบบสารสนเทศตามกฎหมายที่ว่าด้วยการกำหนดกฎข้อบังคับว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิใดบ้างเหนือข้อมูลนั้นๆ เป็นการวางแผนทางการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้งานแพลตฟอร์มออนไลน์ไต่ยนไม่ให้ถูกผู้พัฒนาแพลตฟอร์ม

ผู้ประกอบการค้าออนไลน์นำไปใช้ในทางที่ละเมิดสิทธิของผู้ใช้งานแพลตฟอร์มออนไลน์ไต่ยืนซึ่งเป็นเจ้าของข้อมูล พร้อมกำหนดหน้าที่ที่องค์กรผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลจะต้องกระทำเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในแพลตฟอร์มออนไลน์ไต่ยืน รวมถึงความรับผิดชอบในกรณีที่เกิดเหตุข้อมูลส่วนบุคคลของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนรั่วไหลด้วย

ระบบสารสนเทศ หมายถึง ระบบพื้นฐานของแพลตฟอร์มออนไลน์ไต่ยืนที่ใช้ในการจัดการความปลอดภัยของสารสนเทศที่เป็นข้อมูลองค์กร และข้อมูลส่วนบุคคลของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน ที่อยู่ในรูปแบบของการเก็บ (input) การประมวลผล (processing) เผยแพร่ (output) และมีส่วนจัดเก็บข้อมูล (storage) ซึ่งมีการจัดความความปลอดภัยระบบสารสนเทศ คือ ความปลอดภัยของฮาร์ดแวร์, ความปลอดภัยของซอฟต์แวร์, ความปลอดภัยของมนุษย์, ความปลอดภัยของกระบวนการ, ความปลอดภัยของข้อมูล, ความปลอดภัยของเครือข่าย Information System

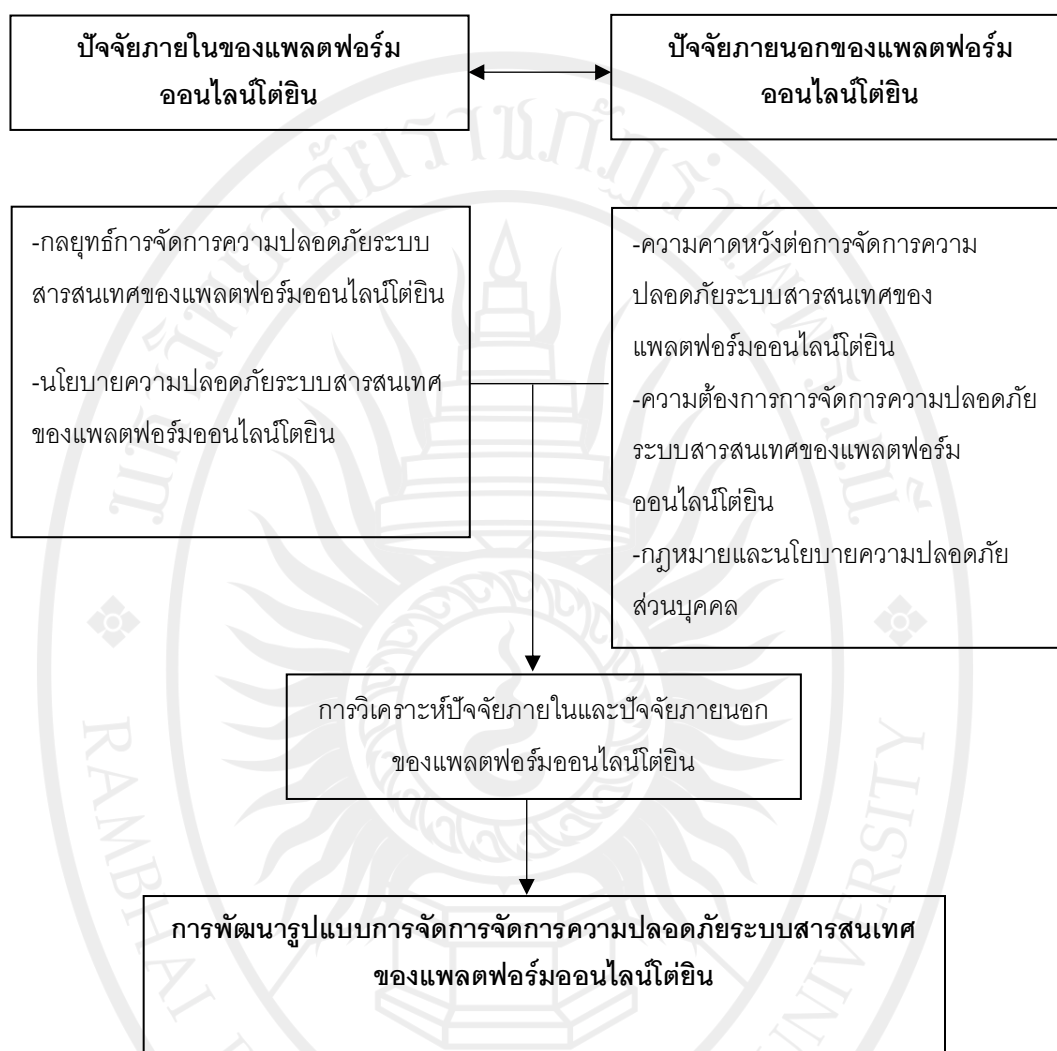
แพลตฟอร์มออนไลน์ไต่ยืน หมายถึง แพลตฟอร์มโซเชียลมีเดียที่เป็นวิดีโอสั้นที่ชาวจีนนิยมใช้ โดยแพลตฟอร์มออนไลน์ไต่ยืนสามารถสื่อสารเพื่อแสดงเนื้อหาวิดีโอสั้นจำนวนมากและมีความหลากหลายให้กับผู้ใช้แพลตฟอร์ม เพื่อตอบสนองความต้องการข้อมูลข่าวสารด้านต่าง ๆ ของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนที่มีการสื่อสารลักษณะส่วนบุคคล ความต้องการข้อมูลข่าวสารต่างๆ และเป็นเครื่องมือสร้างวิดีโอที่สะดวกสบายเพื่อให้ผู้ใช้แพลตฟอร์มสามารถถ่ายวิดีโอทุกประเภทได้อย่างง่ายดาย และใช้เอฟเฟกต์พิเศษ ฟิลเตอร์ และเพลงที่หลากหลายได้

รูปแบบการจัดการความปลอดภัย หมายถึง สิ่งที่แพลตฟอร์มออนไลน์ไต่ยืนสร้างขึ้นเพื่อผู้บริหารทุกระดับ และบุคลากรด้านการจัดการความปลอดภัยระบบสารสนเทศเห็นถึงองค์ประกอบสำคัญ ของการจัดการระบบสารสนเทศต่าง ๆ ของการบริหารความปลอดภัยให้บุคลากรทุกระดับเข้าใจได้ง่ายขึ้น เพื่อใช้เป็นแนวทางในการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนให้มีประสิทธิภาพมากขึ้น

1.7 กรอบแนวคิดการวิจัย

ผู้วิจัยได้ทำการทบทวนวรรณกรรมเกี่ยวกับแนวคิดและทฤษฎีความหวัง ความต้องการ การจัดการเชิงกลยุทธ์ การพัฒนา รูปแบบ ที่เกี่ยวข้องกับการพัฒนารูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน โดยสามารถกำหนดเป็นกรอบแนวคิดของการวิจัย ดังนี้

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี



ภาพ 1.1 กรอบแนวคิดการวิจัย

บทที่ 2

แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การศึกษาเรื่องนี้ ผู้วิจัยได้ทำการทบทวนวรรณกรรมจากเอกสารที่เป็นหนังสือ วารสารวิชาการ สื่ออิเล็กทรอนิกส์ เพื่อให้ได้แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องมาวิเคราะห์ สังเคราะห์ สร้างเป็นกรอบแนวคิดของการวิจัยที่จะใช้กระบวนการวิจัยเพื่อให้ได้ความรู้ ความจริงครอบคลุมในการตอบทุกคำถามของวัตถุประสงค์ในงานวิจัย โดยมีรายละเอียดต่าง ๆ ดังต่อไปนี้

- 2.1 แนวคิดทฤษฎีเกี่ยวกับการพัฒนา
- 2.2 แนวคิดทฤษฎีเกี่ยวกับรูปแบบ
- 2.3 แนวคิดทฤษฎีเกี่ยวกับการจัดการและการจัดการการสื่อสาร
- 2.4 แนวคิดทฤษฎีเกี่ยวกับสารสนเทศเครือข่าย
- 2.5 แนวคิดทฤษฎีเกี่ยวกับความปลอดภัยของข้อมูลเครือข่าย
- 2.6 แนวคิดทฤษฎีเกี่ยวกับสื่อใหม่
- 2.7 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดทฤษฎีเกี่ยวกับการพัฒนา

ความเป็นมาของแนวความคิดทางการพัฒนาประเทศ การพัฒนาเป็นคำที่มีความหมายไม่แน่นอน กล่าวก็คือ แฝงไปด้วยค่านิยม (Value-Laden) และดูเหมือนจะผูกพันกับวัฒนธรรม (Culture-Bound) การพัฒนาจึงมีความหมายแตกต่างกันมากมายขึ้นอยู่กับบุคคล สังคม วัฒนธรรม และกาลเวลา เป็นต้น อย่างไรก็ตามแนวความคิดของการพัฒนาโดยสรุปต่อไปนี้ แสดงให้เห็นถึงความเป็นมาของแนวความคิดแห่งการพัฒนา (มหาวิทยาลัยสุโขทัยธรรมมาธิราช, 2539 อ้างถึงใน สถาบันพระปกเกล้า, 2567)

1. แนวความคิดแบบวิวัฒนาการ (Evolution) นักสังคมศาสตร์ และ นักสังคมวิทยาในศตวรรษที่ 19 ใช้คำว่า การพัฒนาเพื่ออธิบายประวัติศาสตร์ของมนุษย์ (Human History) เพราะเชื่อว่า มนุษยชาติเคลื่อนย้ายจากภาวะหนึ่งไปสู่อีกภาวะหนึ่งที่สูงกว่า (Higher Stage) ในทิศทางเดียวกัน (Unidirectional) และการเคลื่อนย้ายดังกล่าวทำให้ชีวิตมนุษย์มีความอุดมสมบูรณ์ขึ้น มีความแตกต่างกันมากขึ้น ร่ำรวยขึ้น ทั้งทางวัตถุและวัฒนธรรม มีเหตุผลมากขึ้น ฯลฯ เป็นต้น โดยเหตุนี้ การพัฒนาจึงมีความหมายใกล้เคียงกับคำว่า ความก้าวหน้า (Progress) ซึ่งในบางครั้งมีการใช้คำทั้งสองแทนความหมายเดียวกัน

2. แนวความคิดแบบการเปลี่ยนแปลงทางสังคม (Social Change) นักสังคมศาสตร์ในศตวรรษที่ 20 เริ่มละทิ้งคำว่า การพัฒนาและความก้าวหน้า แล้วหันมาใช้คำว่า การเปลี่ยนแปลงทางสังคม (Social Change) เพราะมีความหมายเป็นกลางมากกว่าการพัฒนา คือ ไม่เกี่ยวข้องกับอดีตหรืออนาคตอันรุ่งโรจน์ แต่สนใจศึกษาการเปลี่ยนแปลงของปรากฏการณ์ (Phenomena) เช่น การจัดชนชั้นทางสังคม (Social

Stratification) เพื่อหาสาเหตุของการเปลี่ยนแปลง ไม่ว่าจะเป็นการเปลี่ยนแปลงภายในสังคม (Change in Society) หรือการเปลี่ยนแปลงทั้งสังคม (Change of Society)

3. แนวความคิดแบบเศรษฐศาสตร์ (Economic) แม้คำว่าการพัฒนาจะเลื่อนหายไปจากแนวความคิดทางสังคมศาสตร์ไปบ้าง แต่กลับได้รับความนิยมในทางเศรษฐศาสตร์ เพื่อใช้สำหรับจำแนกประเทศต่าง ๆ ตามดัชนีบ่งชี้ (Index) บางตัว เช่น รายได้ประชาชาติ กล่าวคือ มีการเรียกประเทศที่มีรายได้ประชาชาติสูงกว่าว่าเป็นประเทศพัฒนาแล้ว และเรียกประเทศที่มีรายได้ประชาชาติต่ำกว่าว่าด้อยพัฒนาหรือกำลังพัฒนา ดังนั้น การพัฒนาจึงหมายถึง การเพิ่มค่าของกลุ่มดัชนีบางตัวที่ชี้วัด จึงแทบจะมีความหมายเดียวกับคำว่า ความเป็นอุตสาหกรรม (Industrialization) ความทันสมัย (Modernization) หรือความเจริญทางเศรษฐกิจ (Economic Growth) การพัฒนาในที่นี้จึงมีความหมายแคบกว่าการเปลี่ยนแปลงทางสังคม

4. แนวความคิดแบบการปฏิบัติการทางสังคม (Social Action) การพัฒนาในระยะต่อมานั้นไม่เพียงจะเกี่ยวพันกับเศรษฐศาสตร์ ยังเกี่ยวพันกับการปฏิบัติการทางสังคมมากขึ้น เพราะทุกสังคมโดยเฉพาะฝ่ายรัฐบาลต่างเพียรพยายามปรับปรุงสถานการณ์ทางเศรษฐกิจและสังคม (Economic and Social Conditions) เช่น รายได้ประชาชาติ คุณภาพชีวิต ฯลฯ จึงได้วางแผนปฏิบัติการขึ้น เช่น การปฏิรูปที่ดิน การจัดตั้งองค์กรสหกรณ์ชนบท ฯลฯ เพื่อเพิ่มค่าดัชนีทางเศรษฐกิจสังคมและวัฒนธรรม (Socio-Economic and Cultural Index) ที่เลือกสรรไว้บางตัวดังนั้น การพัฒนาจึงเป็นผลของการปฏิบัติการทางสังคม

5. แนวความคิดแบบขัดแย้งทางสังคม (Social Conflict) เมื่อการพัฒนาเป็นผลของการปฏิบัติการทางสังคม ผลของการพัฒนาจึงก่อให้เกิดความตึงเครียด และความขัดแย้ง (Tension and Conflict) ขึ้น เช่น แบบแผนวัฒนธรรม สัดส่วนระหว่างอาชีพและจำนวนประชากร การทำงานในองค์กร การชนชั้นทางสังคม ฯลฯ เป็นต้น ความขัดแย้งทุกรูปแบบมีสหสัมพันธ์ต่อกัน (Interrelated) และมีผลกระทบ (Impact) ต่อกันมากน้อยต่างกัน แนวความคิดดังกล่าวนี้เป็นพื้นฐานของแนวความคิดในการพัฒนาประเทศแบบสังคมนิยม ที่ใช้ทฤษฎีว่าด้วยความขัดแย้งมาเปลี่ยนแปลงโครงสร้างและระบบสังคมเดิมเชื่อกันว่า การพัฒนาเป็นกระบวนการวิวัฒนาการตามธรรมชาติ ผู้สนใจจึงศึกษาประวัติศาสตร์ของมนุษยชาติ ต่อมาความสนใจหันมาทางการศึกษาปรากฏการณ์ของการเปลี่ยนแปลงทางสังคม และแนวความคิดทางเศรษฐศาสตร์เกี่ยวกับดัชนีบ่งชี้การพัฒนาในแง่ของรายได้ และผลผลิตของชาติก็เริ่มมีบทบาท และในที่สุดการศึกษาอย่างจริงจังในเชิงปฏิบัติของการพัฒนาจึงเกิดขึ้น เป็นการศึกษาถึงแนวความคิดเกี่ยวกับการปฏิบัติการทางสังคม และความขัดแย้งทางสังคม

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

2.2 แนวคิดทฤษฎีเกี่ยวกับรูปแบบ

2.2.1 ความหมายของรูปแบบ

รูปแบบเป็นสิ่งที่สร้างและพัฒนาขึ้นไว้เป็นแนวทางในการทำงานอย่างใดอย่างหนึ่ง มีนักวิชาการได้ให้ความหมายไว้ดังนี้

คัมภีร์ สุตแท้ (2553) กล่าวว่ารูปแบบ หมายถึง สิ่งที่สร้างหรือพัฒนาขึ้น แสดงให้เห็นถึงองค์ประกอบสำคัญของเรื่องให้เข้าใจง่ายขึ้น เพื่อใช้เป็นแนวทางในการดำเนินงานต่อไป

ปัญญา ทองนิล (2553) ได้กล่าวว่า รูปแบบหมายถึง โครงสร้างที่เกิดจากทฤษฎีประสบการณ์การคาดการณ์ นำเสนอในรูปแบบของข้อความหรือแผนผัง

ณัฐศักดิ์ จันทร์ผล (2552 : 125) รูปแบบ หมายถึง โครงสร้างโปรแกรม แบบจำลองหรือรูปแบบที่จำลองสภาพเป็นจริงที่สร้างขึ้นจากการลดทอนเวลาและเทศะ พิจารณามีสิ่งใดบ้างที่จะต้องนำมาศึกษาเพื่อใช้ทดแทนแนวคิดหรือปรากฏการณ์ใดปรากฏการณ์หนึ่ง โดยอธิบายความสัมพันธ์ขององค์ประกอบต่างๆของรูปแบบนั้นๆ

มาลี สิบกระส่าย (2552 : 108-109) รูปแบบมีสองลักษณะ คือ รูปแบบจำลองของสิ่งที่เป็นรูปธรรม เช่น ระบบการปฏิบัติงาน และรูปแบบจำลองของสิ่งเป็นแบบจำลองสิ่งที่เป็นนามธรรม เช่น เครื่องคอมพิวเตอร์ เป็นต้น รูปแบบอาจแสดงความสัมพันธ์ด้วยเส้นโยงแสดงในรูปแบบแผนภาพหรือเขียนในรูปสมการคณิตศาสตร์ หรือสมการพยากรณ์หรือเขียนเป็นข้อความ จำนวน หรือ ภาพ หรือ แผนภูมิหรือรูปสามมิติ

ทิตินา แคมมณี (2550) ได้กล่าวอธิบายความหมายของรูปแบบไว้ว่า รูปแบบ หมายถึงเครื่องมือทางความคิดที่บุคคลใช้ในการสืบสอบหาคำตอบ ความรู้ ความเข้าใจในปรากฏการณ์ที่เกิดขึ้น โดยสร้างมาจากความคิด ประสบการณ์ การใช้อุปมาอุปไมย หรือจากทฤษฎี หลักการต่างๆ และแสดงออกในลักษณะใดลักษณะหนึ่ง

Willer (1967 : 125) กล่าวว่า รูปแบบเป็นการสร้างมโนทัศน์(Conceptualization) เกี่ยวกับชุดปรากฏการณ์โดยอาศัยหลักการ (Rationale) ของระบบรูปนัย (Formal System) และมีจุดมุ่งหมายเพื่อการทำให้เกิดความกระจ่างของนิยาม ความสัมพันธ์และประพจน์ที่เกี่ยวข้อง

Procter (1978 : 174) ให้ความหมายของคำว่ารูปแบบไว้ใน Longman Dictionary of Contemporary English โดยสรุปแล้วจะมี 3 ลักษณะใหญ่ คือ Model หมายถึง สิ่งซึ่งเป็นแบบย่อส่วนของจริงความหมายนี้ตรงกับภาษาไทยว่า แบบจำลอง เช่น แบบจำลองของเรือดำน้ำ เป็นต้น Model ที่หมายถึงสิ่งของหรือคนหรือนำมาใช้เป็นแบบอย่างในการดำเนินการบางอย่างเช่น ครูแบบอย่าง นักเดินแบบ หรือแม่แบบในการวาดภาพศิลป์ เป็นต้น Model ที่หมายถึงแบบหรือรุ่นของผลิตภัณฑ์ต่าง ๆ เช่น เครื่องคอมพิวเตอร์รุ่น 864X เป็นต้น

Tosi and Carroll (1982 : 74) กล่าวไว้ว่า รูปแบบเป็นนามธรรมของจริงหรือภาพจำลองของสภาพการณ์อย่างใดอย่างหนึ่ง ซึ่งอาจจะมีตั้งแต่รูปแบบอย่างง่าย ๆ ไปจนถึงรูปแบบที่มีความสลับซับซ้อนมากๆ และมีทั้งรูปแบบทั้งกายภาพ (Physical Model) ที่เป็นแบบจำลองหอดูดาวแห่งชาติ แบบจำลองเครื่องบินขับไล่ เอฟ 16 เป็นต้นและรูปแบบเชิงลักษณะ (Qualitative Model) ที่ใช้อธิบายปรากฏการณ์ด้วยภาษาหรือสัญลักษณ์ เช่น รูปแบบเชิงระบบและตามสถานการณ์ (A System/Contingency Model) ของ Brown and Moberg (1980 : 56) และรูปแบบการควบคุมวิทยานิพนธ์ ของ บุญชม ศรีสะอาด (2548) เป็นต้น และรูปแบบการบริหารซึ่งกำลังศึกษาและพัฒนา รูปแบบเชิงคุณลักษณะ ซึ่งเป็นรูปแบบในความหมายโดยทั่วไปเมื่อกล่าวถึงคำนี้ในวงวิชาการ

Bardo and Hartman (1982 : 245) ได้กล่าวถึงรูปแบบในทางสังคมศาสตร์ไว้ว่า “เป็นชุดของข้อความเชิงนามธรรมเกี่ยวกับปรากฏการณ์ที่เราสนใจ เพื่อใช้ในการนิยามคุณลักษณะและ/หรือบรรยายคุณสมบัตินั้นๆ” Bardo และ Hartman อธิบายต่อไปว่ารูปแบบเป็นอะไรบางอย่างที่เราพัฒนาขึ้นมา เพื่อบรรยายคุณลักษณะที่สำคัญๆ ของปรากฏการณ์อย่างใดอย่างหนึ่ง เพื่อให้ง่ายต่อการทำความเข้าใจ รูปแบบจึงมิใช่การบรรยายหรืออธิบายปรากฏการณ์อย่างละเอียดทุกแง่มุม เพราะการทำเช่นนั้นจะทำให้รูปแบบมีความซับซ้อนและยุ่งยากเกินไปในการที่จะทำความเข้าใจซึ่งจะทำให้คุณค่าของรูปแบบนั้นด้อยลงไป ส่วนการที่จะจัดระบบรูปแบบหนึ่งๆ จะต้องมียาระเอียดมากน้อยเพียงใดจึงจะเหมาะสมและรูปแบบนั้นๆ ควรมีองค์ประกอบอะไรบ้าง ไม่ได้มีข้อกำหนดเป็นการตายตัว ทั้งนี้ก็แล้วแต่ปรากฏการณ์แต่ละอย่างและมีวัตถุประสงค์ของผู้สร้างรูปแบบที่ต้องการจะอธิบายปรากฏการณ์นั้นๆ อย่างไร

Stoner and Wankel (1986 : 44) ให้ทัศนะคิดว่ารูปแบบเป็นการจำลองความจริงของปรากฏการณ์เพื่อให้เราได้เข้าใจความสัมพันธ์ที่สลับซับซ้อนของปรากฏการณ์นั้นๆ ได้ง่ายขึ้น

Raj (1996 : 45) ได้ให้ความหมายของคำว่า รูปแบบ (Model) ในหนังสือ Encyclopedia of Psychology and Education ไว้ 2 ความหมายดังนี้ 1) รูปแบบ คือ รূปย่อของความจริงของปรากฏการณ์ซึ่งแสดงด้วย ข้อความ จำนวน ภาพ โดยการลดทอนเวลาและเทศะ ทำให้เข้าใจความจริงปรากฏการณ์ได้ดียิ่งขึ้น และ 2) รูปแบบ คือ ตัวแทนของการใช้แนวความคิดของโปรแกรมที่กำหนดเฉพาะโดยสรุปแล้ว รูปแบบหมายถึงแบบจำลองอย่างง่ายหรือย่อส่วน (Simplified Form) ของปรากฏการณ์ต่างๆ ที่ผู้เสนอรูปแบบดังกล่าวได้ศึกษาและพัฒนาขึ้นมาเพื่อแสดงหรืออธิบายปรากฏการณ์ให้เข้าใจได้ง่ายขึ้น หรือในบางกรณีอาจจะใช้ประโยชน์ในการทำนายปรากฏการณ์ที่จะเกิดขึ้น ตลอดจนอาจใช้เป็นแนวทางในการดำเนินการอย่างใดอย่างหนึ่งต่อไป

Good (2005 : 177) ในพจนานุกรมการศึกษาได้รวบรวมความหมายของรูปแบบเอาไว้ 4 ความหมาย คือ 1) เป็นแบบอย่างของสิ่งใดสิ่งหนึ่งเพื่อเป็นแนวทางในการสร้างหรือทำซ้ำ 2) เป็นตัวอย่างเพื่อเลียนแบบ เช่น ตัวอย่างในการออกเสียงภาษาต่างประเทศเพื่อให้ผู้เรียนได้เลียนแบบเป็นต้น 3) เป็นแผนภูมิหรือรูปสามมิติซึ่งเป็นตัวแทนของสิ่งใดสิ่งหนึ่งหรือหลักการหรือแนวคิด และ 4) เป็นชุดของปัจจัยตัวแปรที่มีความสัมพันธ์ซึ่งกันและกันซึ่งรวมตัวกันเป็นตัวประกอบและเป็นสัญลักษณ์ทางระบบสังคม อาจจะเขียนออกมาเป็นสูตรทางคณิตศาสตร์หรือบรรยายเป็นภาษาได้

Thinkexist (2008 : 1) ได้ให้ความหมายของคำว่า รูปแบบ (Model) ไว้ว่า เป็นแบบจำลองระบบปฏิบัติงาน หรือแบบแปลนของการก่อสร้างที่วาดไว้ล่วงหน้า หรือสิ่งของ ที่เป็นตัวแทนแสดงความคิดของสิ่งที่จะเกิดขึ้นในอนาคต หรือสิ่งที่เตรียมเอาไว้ล่วงหน้า อาร์ดิกชันนารี (Ardictionary. 2008 : 1) ได้นิยามความหมายของ Model ว่า หมายถึงแบบจำลองที่เป็นสัดส่วนหรือเป็นประเภทเดียวกันกับของจริงหรือสัญลักษณ์ของการเป็นตัวแทนสิ่งใดสิ่งหนึ่งที่คาดว่าจะเกิดในอนาคต หรือแบบแปลนของสิ่งที่เตรียมไว้

การให้ความหมายของรูปแบบ (Model) ในหนังสือ Encyclopedia of Psychology and Education ไว้ 2 ความหมายดังนี้ 1) รูปแบบ คือ รูปย่อของความจริงของปรากฏการณ์ ซึ่งแสดงด้วยข้อความ จำนวน หรือ ภาพ โดยการลดทอนเวลาและเทศะ ทำให้เข้าใจความจริงของปรากฏการณ์ได้ดียิ่งขึ้น และ 2) รูปแบบ คือ ตัวแทนของการใช้แนวความคิดของโปรแกรมที่กำหนดเฉพาะเรย์ (Rej. 1996 : 197) รูปแบบหมายถึงรูปย่อที่เลียนแบบความสัมพันธ์ของปรากฏการณ์ใดปรากฏการณ์หนึ่งโดยมีวัตถุประสงค์เพื่อช่วยจัดระบบความคิดในเรื่องนั้นให้ง่ายขึ้น

สารานุกรมสแตนฟอร์ดด้านปรัชญา (Stanford Encyclopedia of Philosophy. 2006 : 671) ได้ให้ความหมายของรูปแบบในลักษณะสอดคล้องกับการให้ความหมายของ Good ว่า รูปแบบเป็นระบบหรือโครงสร้างขึ้นมาจากทฤษฎีทั่วไป เพื่อพรรณนาและอธิบายปรากฏการณ์นั้นๆ

Husen and Postlethwaite (1994 : 3895) ได้ให้ความหมายว่า รูปแบบ คือ โครงสร้างที่ถูกนำเสนอเพื่อใช้วินิจฉัยความสัมพันธ์ระหว่างองค์ประกอบที่สร้างมาจากเหตุการณ์ การหยั่งรู้ด้วยวิธีการอุปมาอุปมัย หรือได้มาจากทฤษฎี รูปแบบจึงไม่ใช่ทฤษฎี

สรุปได้ว่า รูปแบบ หมายถึง โครงสร้างที่พัฒนาขึ้นจากทฤษฎี แสดงให้เห็นถึงการอธิบายองค์ประกอบสำคัญ ที่จำลองความจริงของปรากฏการณ์ เพื่อให้เข้าใจความสัมพันธ์ที่สลับซับซ้อนของปรากฏการณ์นั้นๆ ได้ง่ายขึ้น โดยนำเสนอในรูปแบบของข้อความหรือแผนผัง

2.2.2 องค์ประกอบของรูปแบบ

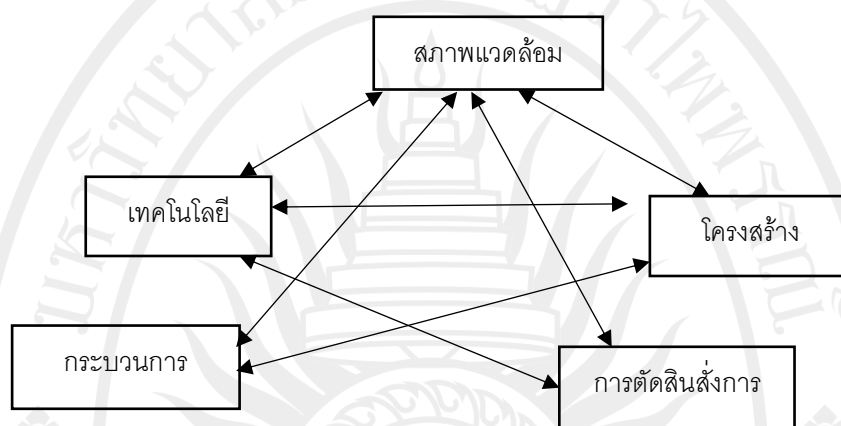
นักการศึกษาได้อธิบายถึงองค์ประกอบของรูปแบบได้ 4 องค์ประกอบ (Husen and Postlethwaite. 1994 : 3865; ทิศนา แฉมณี, 2550 : 220) ดังนี้

1. รูปแบบสามารถนำไปสู่การทำนายผลที่ตามมา สามารถสอบ/ สังเกตได้
2. มีความสัมพันธ์เชิงสาเหตุ อธิบายปรากฏการณ์เรื่องนั้นๆ/ปรากฏการณ์ใกล้เคียงสาเหตุที่กำลังศึกษาและอธิบายเรื่องที่กำลังศึกษา
3. รูปแบบช่วยจินตนาการสร้างความคิดรวบยอด ความสัมพันธ์ของสิ่งที่กำลังศึกษา/ช่วยสืบเสาะความรู้
4. รูปแบบมีความสัมพันธ์เชิงโครงสร้างมากกว่าความสัมพันธ์เชิงเชื่อมโยง

จากการศึกษาตัวอย่างของรูปแบบจากเอกสารที่เกี่ยวข้องต่างๆ พบว่า ไม่ปรากฏมีหลักเกณฑ์ตายตัวว่ารูปแบบนั้นต้องมีองค์ประกอบอะไรบ้างอย่างไร ส่วนใหญ่จะขึ้นอยู่กับลักษณะเฉพาะของปรากฏการณ์ที่ผู้สนใจดำเนินการศึกษา ส่วนการกำหนดองค์ประกอบรูปแบบในการศึกษาและการทำความเข้าใจเกี่ยวกับการจัดองค์การและการบริหารจัดการ (The Model of Organization and Management) ตามความคิดของ Brown and Moberg (1980 : 98) พบว่า Brown และ Moberg ได้สังเคราะห์รูปแบบขึ้นมาจากแนวคิดเชิงระบบ (System Approach) กับหลักการบริหารตามสถานการณ์ (Contingency Approach) และองค์ประกอบตามรูปแบบของ Brown และ Moberg ประกอบด้วย

สภาพแวดล้อม (Environment) เทคโนโลยี (Technology) โครงสร้าง (Structure) กระบวนการจัดการ (Management Process) และการตัดสินใจสั่งการ (Decision Making)

รูปแบบการศึกษาและการทำความเข้าใจเกี่ยวกับการจัดการองค์การและการบริหารของ Brown and Moberg (1980 : 17) มีลักษณะดังแผนภาพ



ภาพที่ 2.1 รูปแบบเชิงระบบและสถานการณ์ (System Contingency Model) ของ Brown and Moberg (1980)

สำหรับองค์ประกอบของรูปแบบการบริหารเท่าที่พบจากการศึกษาเอกสารที่เกี่ยวข้องพบว่า ส่วนใหญ่จะกล่าวถึง การจัดองค์การหรือโครงสร้างระบบบริหารและแนวทางในการดำเนินงานในภาระหน้าที่ (Function) ที่สำคัญ ๆ ในการบริหารงานขององค์กรนั้น ๆ เช่น การบริหารงานบุคลากร การบริหารงานการเงิน การบริหารงานวิชาการ เป็นต้น ซึ่งจะได้กล่าวถึงอีกครั้งหนึ่งในตอนที่ว่าด้วยการกำหนดองค์ประกอบในการกำหนดรูปแบบต่อไป

สรุปได้ว่า ในการกำหนดองค์ประกอบของรูปแบบไม่ปรากฏมีหลักเกณฑ์ตายตัวว่าจะประกอบด้วยอะไรบ้าง จำนวนเท่าใดมีโครงสร้างและความสัมพันธ์กันอย่างไร ขึ้นอยู่กับปรากฏการณ์ที่กำลังศึกษาหรือจะออกแบบแนวคิดทฤษฎีและหลักการพื้นฐานในการกำหนดรูปแบบนั้น ๆ เป็นหลัก

2.2.3 ประเภทของรูปแบบ

รูปแบบมีหลายประเภทด้วยกันซึ่งนักวิชาการด้านต่างๆก็ได้จัดแบ่งประเภทต่างกันไป สำหรับรูปแบบทางการศึกษาและสังคมศาสตร์นั้น (Keeves. 1988 : 565) แบ่งออกเป็น 4 ประเภท คือ

1. Analogue Model เป็นรูปแบบที่ใช้การอุปมาอุปมัยเทียบเคียงปรากฏการณ์ซึ่งเป็นรูปธรรมเพื่อสร้างความเข้าใจในปรากฏการณ์ที่เป็นนามธรรม เช่น รูปแบบในการทำนายจำนวนนักเรียนที่จะเข้าสู่ระบบโรงเรียน ซึ่งอนุมานแนวคิดมาจากการเปิดน้ำเข้าและปล่อยน้ำออกมาจากถัง นักเรียนที่จะ

เข้าสู่ระบบเปรียบเทียบได้กับน้ำที่เปิดออกจากถัง ดังนั้นนักเรียนที่คงอยู่ในระบบจึงเท่ากับนักเรียนที่เข้าสู่ระบบลบด้วยนักเรียนที่ออกจากระบบ เป็นต้น

2. Semantic Model เป็นรูปแบบที่ใช้ภาษาเป็นสื่อในการบรรยายหรืออธิบายปรากฏการณ์ที่ศึกษาด้วยภาษา แผนภูมิ หรือรูปภาพ เพื่อให้เห็นโครงสร้างทางความคิดองค์ประกอบ และความสัมพันธ์ขององค์ประกอบของปรากฏการณ์นั้นๆ เช่น รูปแบบการสอนของ (Joyce and Weil. 1985 : 41)

3. Mathematical Model เป็นรูปแบบที่ใช้สมการทางคณิตศาสตร์เป็นสื่อในการแสดงความสัมพันธ์ของตัวแปรต่างๆ รูปแบบประเภทนี้นิยมใช้กันทั้งในสาขาจิตวิทยาและศึกษาศาสตร์รวมทั้งการบริหารการศึกษาด้วย

4. Causal Model เป็นรูปแบบที่พัฒนามาจากเทคนิคที่เรียกว่า Path Analysis และหลักการสร้าง Semantic Model โดยการนำเอาตัวแปรต่าง ๆ มาสัมพันธ์กันเชิงเหตุผลที่เกิดขึ้น เช่น The Standard Deprivation Model ซึ่งเป็นรูปแบบที่แสดงความสัมพันธ์ระหว่างสภาพทางเศรษฐกิจสังคมของบิดา มารดา สภาพแวดล้อมทางการศึกษาที่บ้าน และระดับสติปัญญา ของเด็ก เป็นต้น

Schwirian (อ้างถึงใน Bardo and Hardman 1982 : 70-71) นักนิเวศวิทยาคนสำคัญ ได้แบ่งประเภทของรูปแบบด้วยการอธิบายลักษณะจากลักษณะของเมืองออกเป็นรูปแบบที่อธิบายโดยพื้นที่นั้นเป็นจุดมุ่งหมายในการบรรยายลักษณะของเมืองว่ามีลักษณะเช่นไร เช่น Concentric Zone Model และ Social Area Analysis Model เป็นต้น สำหรับรูปแบบที่ใช้อธิบายคุณลักษณะของประชากรเมืองนั้นเป็นรูปแบบที่เสนอความคิดในการอธิบายเกี่ยวกับลักษณะของประชากรเมืองต่างๆเช่น Residential Segregation Model เป็นต้น

Joyce and Weil (1985 : 74) ได้ศึกษาและจัดแบ่งประเภทของรูปแบบตามแนวคิดหลักการหรือทฤษฎี ซึ่งเป็นพื้นฐานในการพัฒนารูปแบบนั้นๆ และได้แบ่งกลุ่มรูปแบบการสอนไว้ 4 รูปแบบ คือ

1. Information Processing Models เป็นรูปแบบการสอนที่ยึดหลักความสามารถในการประมวลข้อมูลของผู้เรียนและแนวทางในการปรับปรุงวิธีการจัดเก็บข้อมูลให้มีประสิทธิภาพยิ่งขึ้น

2. Personal Models รูปแบบการสอนที่จัดไว้ในกลุ่มนี้ให้ความสำคัญกับ ปัจเจกบุคคลและการพัฒนาบุคคลเฉพาะราย โดยมุ่งเน้นกระบวนการที่แต่ละบุคคลจัดระบบปฏิบัติต่อสรรพสิ่ง (Reality)ทั้งหลาย

3. Social Interaction Models เป็นรูปแบบที่ให้ความสำคัญกับความสัมพันธ์ระหว่างบุคคลและบุคคลต่อสังคม

4. Behavior Models เป็นกลุ่มของรูปแบบการสอนที่ใช้องค์ความรู้ด้านพฤติกรรมศาสตร์เป็นหลักในการพัฒนารูปแบบ จุดเน้นที่สำคัญคือ การเปลี่ยนแปลงพฤติกรรมในการพัฒนารูปแบบ จุดเน้นที่สำคัญการเปลี่ยนแปลงพฤติกรรมที่สังเกตได้ของผู้เรียนมากกว่าการพัฒนาโครงสร้างจิตวิทยาและพฤติกรรมที่ไม่สามารถสังเกตได้

สไตเนอร์ (Steiner. 1988 : 148) รูปแบบแบ่งออกได้เป็น 2 ประเภทคือ 1) รูปแบบ เชิงปฏิบัติ (Practical Model or Model-of) รูปแบบเชิงทฤษฎี (Theoretical Model or Model-of) รูปแบบจำลองที่สร้างขึ้นจากกรอบความคิดที่มีทฤษฎีเป็นพื้นฐาน ด้วยทฤษฎีเองไม่ใช่รูปแบบหรือแบบจำลองเป็นตัวช่วยให้เกิดรูปแบบที่มีโครงสร้างต่างๆที่สัมพันธ์กัน

Bardo and Hartman (1982 : 141) นักนิเวศวิทยาที่สำคัญ ได้ให้ทัศนะที่น่าสนใจไว้อีกแนวหนึ่งซึ่งเป็นแนวคิดหรือทฤษฎีพื้นฐานในการกำหนดรูปแบบโดยแบ่งประเภทของรูปแบบด้วยการอธิบายลักษณะจากลักษณะจากลักษณะของเมืองออกเป็นรูปแบบที่อธิบายโดยลักษณะพื้นที่และรูปแบบที่อธิบายโดยลักษณะของประชากร รูปแบบที่ใช้ในการอธิบายพื้นที่นั้นมีจุดมุ่งหมายในการบรรยายลักษณะของเมืองว่าลักษณะอย่างไร เช่น Concentric Zone Model and Social Area Analysis model เป็นต้น สำหรับรูปแบบที่ใช้อธิบายโดยลักษณะของประชากรนั้น เป็นรูปแบบที่เสนอความคิดในการอธิบายเกี่ยวกับลักษณะของประชากรของเมืองต่าง ๆ เช่น Residential Segregation Model และ Group Location Model เป็นต้น

Steiner (1988 : 215) แบ่งรูปแบบออกได้เป็น 2 ประเภท คือ

1) รูปแบบเชิงปฏิบัติ (Practical Model or Model-of) รูปแบบประเภทนี้เป็นแบบจำลองทางกายภาพ เช่นจำลองหุ่นยนต์

2) รูปแบบเชิงทฤษฎี (Theoretical Model or Model-of) เป็นแบบจำลองที่สร้างขึ้นจากกรอบความคิดที่มีทฤษฎีเป็นพื้นฐาน ตัวทฤษฎีเองไม่ใช่รูปแบบหรือแบบจำลองเป็นตัวช่วยให้เกิดรูปแบบที่มีโครงสร้างต่าง ๆ ที่สัมพันธ์กัน

รูปแบบตามความคิดเห็นของ (Keeves. 1988 : 178) จำแนกออกได้เป็น 5 รูปแบบคือ

1) รูปแบบที่คล้าย (Analogue Models) คือ เป็นรูปแบบที่มีความสัมพันธ์กันระบบกายภาพมักเป็นรูปแบบที่ใช้ในวิทยาศาสตร์กายภาพเป็นรูปแบบที่นำไปใช้อุปมาอุปมัยกับสิ่งอื่นได้ เช่นรูปแบบจำลองระบบสุริยะที่เกิดขึ้นจริง ธนาครจำลองกับระบบธนาครที่เป็นจริงแบบจำลองการผลิตกับการผลิตจริง เป็นต้น

2) รูปแบบที่อธิบายความหมายหรือให้ความหมาย (Semantic Models) เป็นรูปแบบที่ใช้ภาษาในการบรรยายถึงลักษณะของรูปแบบชนิดนี้จะใช้วิธีการอุปมาอุปมัยในการพิจารณาด้วยภาษามากกว่าที่จะใช้วิธีอุปมาในการพิจารณาด้วยโครงสร้างภาพ

3) รูปแบบที่มีลักษณะเป็นแผนภูมิแบบแผน หรือโครงสร้าง (Schematic Models)

4) รูปแบบเชิงคณิตศาสตร์ (Mathematical Models) คือ เป็นรูปแบบที่กำหนดความสัมพันธ์ขององค์ประกอบในรูปสมการหรือฟังก์ชันทางคณิตศาสตร์

5) รูปแบบเชิงเหตุผล (Causal Models) คือ เป็นรูปแบบที่มีโครงสร้างเป็นสมการเชิงเส้นที่ประกอบด้วยตัวแปรสัมพันธ์กันเป็นเหตุเป็นผล มีการทดสอบสมมุติฐานผลของรูปแบบจากลักษณะการแบ่งประเภทของรูปแบบของนักวิชาการต่างๆที่กล่าวมาแล้วจะเห็นได้ว่าการแบ่งประเภทของรูปแบบตามแนวความคิดที่หนึ่งนั้นบอกให้ทราบถึงลักษณะการเขียนรูปแบบที่มีลักษณะส่วนการแบ่งประเภทของ

รูปแบบในแบบที่สองและสามนั้นเป็นการแบ่งประเภทของรูปแบบตามแนวพื้นฐานในการเสนอรูปแบบในการบรรยาย อธิบายปรากฏการณ์นั้นๆเป็นหลัก

สรุปได้ว่า รูปแบบมีหลายประเภทด้วยกันเป็นสิ่งที่สร้างและพัฒนาขึ้นของแต่ละสาขาก็มีรูปแบบที่แตกต่างกันออกไป เช่น รูปแบบทางการศึกษาและสังคมศาสตร์ ได้แบ่งออกเป็น รูปแบบที่ใช้ในการเปรียบเทียบกัน เทียบเคียงปรากฏการณ์ซึ่งเป็นรูปธรรมเพื่อสร้างความเข้าใจปรากฏการณ์ที่เป็นนามธรรม รูปแบบที่ใช้ภาษาสื่อในการขยายหรืออธิบายปรากฏการณ์ที่ศึกษาด้วยภาษา แผนภูมิ รูปภาพ รูปแบบที่ใช้สมการทางคณิตศาสตร์เป็นสื่อในการแสดงความสัมพันธ์ของตัวแปรต่างๆ และรูปแบบที่ใช้สมการทางคณิตศาสตร์เป็นสื่อในการแสดงความสัมพันธ์ของตัวแปรต่างๆ และรูปแบบที่นำเอา ตัวแปรต่างๆมาสัมพันธ์กันเชิงเหตุผลที่เกิดขึ้น เป็นต้น

2.2.4 คุณลักษณะของรูปแบบที่ดี

Keeves (1988 : 560) กล่าวว่า รูปแบบที่ใช้ประโยชน์ได้และมีคุณลักษณะของรูปแบบที่ดีควรมีข้อกำหนด (Requirement) 4 ประการ คือ

1. รูปแบบ ควรประกอบด้วยความสัมพันธ์อย่างมีโครงสร้าง (Structural Relationship) มากกว่าความสัมพันธ์ที่เกี่ยวข้องแบบรวมๆ (Associative Relationship)
2. รูปแบบ ควรใช้เป็นแนวทางในการพยากรณ์ผลที่จะเกิดขึ้น ซึ่งสามารถถูกตรวจสอบได้โดยการสังเกต ซึ่งเป็นไปได้ที่จะทดสอบรูปแบบพื้นฐานขอข้อมูลเชิงประจักษ์ได้
3. รูปแบบ ควรจะต้องระบุหรือชี้ให้เห็นถึงกลไกเชิงเหตุผลของเรื่องที่ศึกษา ดังนั้น นอกจากรูปแบบจะเป็นเครื่องมือในการพยากรณ์ได้ ควรใช้อธิบายปรากฏการณ์ได้ด้วย
4. รูปแบบ ควรเป็นเครื่องมือในการสร้างมโนทัศน์ใหม่และสร้างความสัมพันธ์ของตัวแปรในลักษณะใหม่ ซึ่งเป็นการขยายในเรื่องที่กำลังศึกษา

สรุปได้ว่า คุณลักษณะของรูปแบบที่ดีควรมีลักษณะ ดังนี้คือ ควรประกอบด้วยความสัมพันธ์อย่างมีโครงสร้าง ใช้เป็นแนวทางในการพยากรณ์ผลที่จะเกิดขึ้น จะต้องระบุหรือชี้ให้เห็นถึงกลไกเชิงเหตุผลของเรื่องที่ศึกษา ใช้อธิบายปรากฏการณ์ได้และเป็นเครื่องมือในการสร้างมโนทัศน์ใหม่และสร้างความสัมพันธ์ของตัวแปรในลักษณะใหม่

2.2.5 การตรวจสอบรูปแบบ

จุดมุ่งหมายที่สำคัญของการสร้างรูปแบบก็เพื่อทดสอบหรือตรวจสอบรูปแบบนั้นด้วยข้อมูลเชิงประจักษ์ การตรวจสอบรูปแบบมีหลายวิธี ซึ่งอาจใช้การวิเคราะห์จากหลักฐานเชิงคุณลักษณะ (Qualitative) และเชิงปริมาณ (Quantitative) โดยที่การตรวจสอบรูปแบบจากหลักฐานเชิงคุณลักษณะ อาจใช้ผู้เชี่ยวชาญเป็นผู้ตรวจสอบในโมเดลจากหลักฐานเชิงปริมาณใช้เทคนิคทางสถิติ ซึ่งการตรวจสอบรูปแบบควรตรวจสอบคุณลักษณะ 2 อย่าง คือ (อุทุมพร จามรมาน. 2541 : 23) คือ

1. การตรวจสอบความมากน้อยของความสัมพันธ์/ความเกี่ยวข้อง/เหตุผลระหว่าง ตัวแปร

2. การประมาณค่าพารามิเตอร์ของความสัมพันธ์ดังกล่าว ซึ่งการประมาณค่านี้สามารถประมาณข้ามกาลเวลา กลุ่มตัวอย่าง หรือสถานที่ได้ (Across Tim, Samples, Sites)

Eisner (1976 : 192-193) ได้เสนอแนวคิดการตรวจสอบโดยการใช้ผู้ทรงคุณวุฒิ ในบางเรื่องที่ต้องการความละเอียดอ่อนมากกว่าการวิจัยในเชิงปริมาณ โดยเชื่อว่าการรับรู้ที่เท่ากันนั้นเป็นคุณสมบัติพื้นฐานของผู้รู้ และได้เสนอแนวคิดการประเมินโดยผู้ทรงคุณวุฒิไว้ดังนี้

1) การประเมินโดยแนวทางนี้ มิได้เน้นผลสัมฤทธิ์ของเป้าหมายหรือวัตถุประสงค์ตามรูปแบบรูปแบบการประเมินแบบอิงเป้าหมาย (Goal-Based Models) การตอบสนองปัญหาและความต้องการของผู้เกี่ยวข้องตามรูปแบบการประเมินแบบสนองตอบ (Responsive Models) หรือกระบวนการวิเคราะห์วิจารณ์อย่างลึกซึ้งเฉพาะในประเด็นที่นำมาพิจารณา ซึ่งไม่จำเป็นต้องเกี่ยวข้องกับวัตถุประสงค์หรือผู้ที่มีส่วนเกี่ยวข้องกับการตัดสินใจเสมอไป แต่อาจจะผสมผสานปัจจัยในการพิจารณาต่างๆ เข้าด้วยกัน ตามวิจรรย์านของผู้ทรงคุณวุฒิ เพื่อให้ได้ข้อสรุปเกี่ยวกับคุณภาพ ประสิทธิภาพ หรือความเหมาะสมของสิ่งที่ทำการประเมิน

2) เป็นรูปแบบการประเมินที่เน้นความเชี่ยวชาญเฉพาะทาง (Specialization) ในเรื่องที่จะประเมิน โดยที่พัฒนามาจากรูปแบบการวิจารณ์งานศิลป์ (Art Criticism) ที่มีความละเอียดลึกซึ้งและต้องอาศัยผู้เชี่ยวชาญระดับสูงมาเป็นผู้วิจัย เนื่องจากการวัดคุณค่าไม่อาจประเมินด้วยเครื่องวัดใดๆ และต้องใช้ความรู้ความสามารถของผู้ประเมินอย่างแท้จริง ต่อมาได้มีการนำแนวคิดนี้มาประยุกต์ใช้ในทางการศึกษาระดับสูงในวงการอุดมศึกษามากขึ้นในสาขาเฉพาะที่ต้องอาศัยผู้รู้ ผู้เล่นในเรื่องนั้นจริงๆ มาเป็นผู้ประเมินผล ทั้งนี้เพราะองค์ความรู้เฉพาะสาขานั้นผู้ที่ศึกษาเรื่องนั้นจริงๆ จึงจะทราบและเข้าใจอย่างลึกซึ้ง

3) รูปแบบที่ใช้บุคคล คือ ผู้ทรงคุณวุฒิเป็นเครื่องมือในการประเมิน โดยใช้ความเชื่อถือว่าผู้ทรงคุณวุฒินั้นเที่ยงธรรมและมีดุลพินิจที่ดี ทั้งนี้มาตรฐานและเกณฑ์พิจารณาต่างๆ นั้น จะเกิดขึ้นจากประสบการณ์และความชำนาญของผู้ทรงคุณวุฒินั่นเอง

4) เป็นรูปแบบที่ยอมให้ความยืดหยุ่นในกระบวนการทำงานของผู้ทรงคุณวุฒิตามอัธยาศัยและความถนัดของแต่ละคน นับตั้งแต่การกำหนดประเด็นสำคัญที่พิจารณา การบ่งชี้ข้อมูลที่ต้องการ การเก็บรวบรวม การประมวล การวินิจฉัยข้อมูล ตลอดจนวิธีการนำเสนอ

ทั้งนี้ การเลือกผู้ทรงคุณวุฒิจะเน้นที่สถานภาพทางวิชาชีพ ประสบการณ์และการเป็นที่เชื่อถือ (High Credit) ของวิชาชีพนั้นเป็นสำคัญ

สรุปได้ว่า การตรวจสอบรูปแบบอาจใช้การวิเคราะห์จากหลักฐานเชิงคุณลักษณะ และเชิงปริมาณ โดยควรตรวจสอบคุณลักษณะ 2 อย่าง คือ ตรวจสอบระดับความสัมพันธ์ความสัมพันธ์ของตัวแปรและการประมาณค่าของความสัมพันธ์ นอกจากนี้ ยังมีการตรวจสอบโดยการประเมินจากผู้ทรงคุณวุฒิตามวิจรรย์านของผู้ทรงคุณวุฒิ เพื่อให้ได้ข้อสรุปเกี่ยวกับคุณภาพ ประสิทธิภาพ หรือความเหมาะสมของสิ่งที่ทำการประเมิน เป็นการประเมินที่เน้นความเชี่ยวชาญเฉพาะทาง

2.3 แนวคิดทฤษฎีเกี่ยวกับการจัดการและการจัดการการสื่อสาร

การจัดการ (Management) หรืออาจจะเรียกว่า การบริหาร (Administration) หมายถึง ชุดของหน้าที่ต่าง ๆ ที่กำหนดทิศทางในการใช้ประโยชน์จากทรัพยากรทั้งหลายอย่างมีประสิทธิภาพและประสิทธิผล เพื่อให้บรรลุเป้าหมายขององค์กร การใช้ทรัพยากรอย่างมีประสิทธิภาพ (Efficient) หมายถึง การใช้ทรัพยากรอย่างเฉลียวฉลาด และคุ้มค่า ส่วนการใช้ทรัพยากรอย่างมีประสิทธิภาพ (Effective) หมายถึงการตัดสินใจอย่างถูกต้อง และมีการปฏิบัติการได้สำเร็จตามแผนที่กำหนดไว้ ดังนั้น ผลสำเร็จของการจัดการต้องมีทั้งประสิทธิภาพและประสิทธิผลควบคู่กันไป (Griffin, 1997)

พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2542 ให้ความหมาย การจัดการ (Management) หมายถึง การสั่งการ ควบคุมงาน ดำเนินงาน และนอกจากนี้ได้นักวิชาการท่านอื่นได้ให้คำนิยามความหมายของ การจัดการซึ่งมีความหมายที่แตกต่างกันออกไปดังต่อไปนี้

ไซมอน (Simon, 1965 : 4) ให้ความหมายว่า การทำงานของบุคคลตั้งแต่ 2 คนขึ้นไปร่วมกันปฏิบัติงานเพื่อให้บรรลุวัตถุประสงค์ร่วมกัน

รูและเบอร์ (Rue and Byars, 2002 อ้างใน สาคร สุขศรีวงศ์, 2550) กล่าวว่าไว้ว่า การจัดการ คือ รูปแบบของงานซึ่งเกี่ยวข้องกับการประสานทรัพยากรต่าง ๆ ขององค์กร อันได้แก่ ที่ดิน แรงงาน และทุน เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

คุนตซ์ และไซริล (Koontz and Cyril, 1972 : 43) ให้ความหมายว่า การจัดการ หมายถึง การดำเนินงานให้บรรลุวัตถุประสงค์ที่ตั้งไว้โดยอาศัยปัจจัยทั้งหลาย ได้แก่ คน เงิน วัสดุสิ่งของซึ่งนับว่าเป็นอุปกรณ์ของการจัดการนั้น ๆ

เดล (Dale, 1968 : 43) ได้กล่าวไว้ว่า การจัดการ คือ กระบวนการจัดหน่วยงานและการใช้ทรัพยากรต่าง ๆ ให้บรรลุวัตถุประสงค์ที่กำหนดไว้ล่วงหน้า

สมยศ นาวิการ (2536 : 23) กล่าวว่าไว้ว่า กระบวนการจัดการว่าเป็นกิจกรรมของการบริหารที่สำคัญ 4 อย่าง คือ การวางแผน การจัดองค์การ การสั่งการ และการควบคุม

สุรัสวดี ราชกุลชัย (2543 : 3) กล่าวว่าไว้ว่า “การบริหาร” (Administration) และ “การจัดการ” (Management) มีความหมายแตกต่างกันเล็กน้อย โดยการบริหารจะสนใจและสัมพันธ์กับการกำหนดนโยบายไปลงมือปฏิบัติ นักวิชาการบางท่านให้ความเห็นว่าการบริหารใช้ในภาครัฐส่วนการจัดการใช้ในภาคเอกชน อย่างไรก็ตาม ในตำราหรือหนังสือส่วนใหญ่ทั้ง 2 คำนี้มีความหมายไม่แตกต่างกัน สามารถใช้แทนกันได้และเป็นที่ยอมรับโดยทั่วไป

ณัฐพันธ์ เขจรนันท์ และฉัตรยาพร เสมอใจ (2547) กล่าวถึง การจัดการ (Management) ว่าเป็นการจัดโครงสร้าง การจัดระบบงาน การรวมกลุ่มกิจกรรม การกำหนดขอบเขตหน้าที่ ความสำเร็จ รับผิดชอบ การมอบหมายงานให้ผู้ใต้บังคับบัญชาแต่ละคน เพื่อที่จะปฏิบัติงานให้สอดคล้องกันและบรรลุ

เป้าหมายที่กำหนดไว้ โดยจัดการระบบ (System) ระเบียบ (Order) และความสัมพันธ์ (Relationship) ในหน่วยงานหรือองค์กร

การจัดการ (Management) หมายถึง กระบวนการที่ผู้จัดการทำงานร่วมกันและโดยอาศัยพนักงานและทรัพยากรอื่น โดยใช้การวางแผน (Planning) การจัดองค์การ (Organizing) การนำ (Leading) และการควบคุม (Controlling) เพื่อให้การดำเนินงานบรรลุเป้าหมายองค์การอย่างมีประสิทธิภาพและประสิทธิผลภายใต้สภาพแวดล้อมที่เปลี่ยนแปลงหัวใจสำคัญของการจัดการ คือ การใช้ทรัพยากรอย่างมีประสิทธิภาพและประสิทธิผล

ดิน ปรัชญพฤทธิ (2551 : 8) การบริหารเป็นกระบวนการ โดยหมายถึง กระบวนการนำเอาการตัดสินใจและนโยบายไปปฏิบัติ ส่วนการบริหารรัฐกิจ หมายถึง เกี่ยวข้องกับการเอานโยบายสาธารณะไปปฏิบัติ

วิโรจน์ สารรัตน์ (2555 : 1) กล่าวว่า การบริหาร หมายถึง กระบวนการดำเนินงานเพื่อให้บรรลุจุดหมายขององค์การอย่างมีประสิทธิภาพ โดยอาศัยหน้าที่ในการบริหาร ได้แก่ การวางแผน (Planning) การจัดองค์การ (Organizing) การชี้นำ (Leading) และการควบคุมองค์การ (Controlling)

จากความหมายที่ได้มีนักวิชาการและหน่วยงานต่าง ๆ นิยามไว้เกี่ยวกับการจัดการ สามารถสรุปได้ว่า การจัดการคือ การจัดการโครงสร้าง ชุดของหน้าที่ต่าง ๆ แนวทางที่ใช้ทรัพยากรทางการบริหาร เช่น คน เงิน วัสดุอุปกรณ์ อย่างมีประสิทธิภาพและประสิทธิผล สามารถบรรลุผลสำเร็จตามวัตถุประสงค์ ด้วยความพยายามร่วมกันของกลุ่มบุคคล หรือเป็นกระบวนการบริหาร ที่มีการบูรณาการระหว่างคนกับงานโดยมีการวางแผนการจัดโครงสร้างองค์การ การเป็นผู้นำและการควบคุมที่มีประสิทธิภาพ ที่ทำให้องค์การดำรงอยู่และเกิดสัมฤทธิ์ผลตามเป้าหมายที่กำหนดไว้

โดยทั่วไปแล้วการจัดการมักใช้ควบคู่กับคำว่าการบริหาร หรือเรียกว่า การบริหารจัดการ เนื่องจากทั้งการบริหารและการจัดการมีความคล้ายคลึงกัน เป็นกระบวนการในการดำเนินงานเพื่อให้บรรลุเป้าหมาย การบริหาร (Administration) นิยมใช้กับการบริหารราชการหรือการจัดการเกี่ยวกับนโยบาย การจัดการ (Management) นิยมใช้กับการบริหารธุรกิจเอกชนหรือการดำเนินการตามนโยบายที่กำหนดไว้ อย่างไรก็ตามคำว่า การบริหารกับคำว่า การจัดการใช้แทนกันได้มีความหมายเหมือนกัน การจัดการ (Management) และการบริหาร (Administration) มีสิ่งที่เหมือนกันคือมีเป้าหมายเหมือนกันคือทำให้บรรลุเป้าหมายขององค์การอย่างมีประสิทธิภาพและประสิทธิผล (สมคิด บางโม, 2538 : 60) ความสำคัญของการจัดการ ดังนี้

1. การจัดการมีผลต่อความสำเร็จขององค์การ แม้จะเป็นสิ่งที่ไม่สามารถมองเห็นได้แต่สามารถวัดและประเมินผลได้ การจัดการทำให้การใช้ทรัพยากรมีความคุ้มค่าและเกิดประสิทธิผลในการผลิต กระบวนการทำงานหรือการจัดการมีความสำคัญต่อองค์การ เพราะทุกขั้นตอนมีผลต่อความสำเร็จที่จะทำให้เกิดและช่วยให้องค์การธุรกิจสามารถดำเนินการต่อไปได้ นอกจากนี้กระบวนการจัดการยังเป็นทั้งศาสตร์

และศิลป์ที่ต้องรู้จักนำมาประยุกต์ใช้ให้เกิดประโยชน์ เนื่องจากแต่ละองค์กรมีปัจจัยความสำเร็จที่แตกต่างกัน

2. การจัดองค์กรเป็นสิ่งที่ช่วยสนับสนุนความสำเร็จขององค์กร องค์กรทุกองค์กรจะต้องมีทั้งประสิทธิภาพและประสิทธิผลในการทำงาน จะขาดอย่างใดอย่างหนึ่งไม่ได้ ซึ่งประสิทธิภาพนั้น จะกล่าวถึงในเรื่องของใช้ทรัพยากรอย่างคุ้มค่า เพื่อให้องค์กรบรรลุเป้าหมายตามที่กำหนดไว้ ซึ่งบางครั้งอาจไม่บรรลุวัตถุประสงค์ขององค์กร ส่วนในเรื่องของประสิทธิผล กล่าวได้ว่าเป็น ความพยายามขององค์กรในการทำให้งานบรรลุตามวัตถุประสงค์ขององค์กรคือ ประสิทธิผล ซึ่งการที่จะเกิดประสิทธิผลได้นั้น เราไม่ได้มองในมุมของการใช้ทรัพยากรหรือคำนึงถึง การใช้ทรัพยากรให้คุ้มค่า แต่เราจะเน้นไปที่จะทำอย่างไร ให้องค์กรบรรลุวัตถุประสงค์ตามที่ได้ตั้งไว้ ซึ่งการจัดองค์กรนั้น เหมือนเป็นการกำหนดว่าจะทำอย่างไร เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

นรินทร์ แจ่มจำรัส (2549 : 46) ได้เสนอความสำคัญของการจัดการไว้ดังนี้

1. การจัดองค์กรเป็นสิ่งที่ช่วยสนับสนุนความสำเร็จขององค์กร เนื่องจากการจัดองค์กรเป็นงานที่ผู้บริหารใช้เป็นเครื่องมือในการกำหนดว่าใครจะทำอะไร ใครจะอยู่แผนกไหน ใครจะต้องรับผิดชอบ และรายงานต่อใคร ซึ่งการจัดองค์กรนั้นเหมือนเป็นการกำหนดว่าจะทำอย่างไร เพื่อให้บรรลุวัตถุประสงค์ขององค์กร โดยการจัดองค์กรนั้นยังรวมถึงกลไกการประสานงาน เนื่องด้วยในองค์กรหนึ่ง ๆ จะต้องมีการแบ่งงานและประสานงานกันเพื่อให้งานสำเร็จลุล่วง

2. เพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการดำเนินงาน เนื่องจากองค์กรทุกองค์กรจะต้องมีทั้งประสิทธิภาพและประสิทธิผลในการทำงาน จะขาดอย่างใดอย่างหนึ่งไม่ได้ ซึ่งประสิทธิภาพนั้น จะกล่าวถึงในเรื่องของใช้ทรัพยากรอย่างคุ้มค่า เพื่อให้องค์กรบรรลุเป้าหมายตามที่กำหนดไว้ ซึ่งบางครั้งอาจไม่บรรลุวัตถุประสงค์ขององค์กร ส่วนในเรื่องของประสิทธิผลกล่าวได้ว่าเป็นความพยายามขององค์กรในการทำให้งานบรรลุตามวัตถุประสงค์ขององค์กรคือ ประสิทธิภาพ ซึ่งการที่จะเกิดประสิทธิผลได้นั้น เราไม่ได้มองในมุมของการใช้ทรัพยากรหรือคำนึงถึงการใช้ทรัพยากรให้คุ้มค่า แต่เราจะเน้นไปที่จะทำอย่างไร ให้องค์กรบรรลุวัตถุประสงค์ตามที่ได้ตั้งไว้

3. ช่วยลดการทำงานที่ซ้ำซ้อนกัน เนื่องจากการจัดองค์กรเป็นการกำหนดว่าในองค์กรใด องค์กรหนึ่งควรแบ่งออกเป็นกี่แผนก เมื่อมีการแบ่งแผนกได้แล้วในขั้นตอนต่อไปจะเป็นเรื่องของ การกำหนดอำนาจหน้าที่และความรับผิดชอบ เช่น ใครอยู่แผนกไหน หน้าที่งานคืออะไร ใครเป็นผู้รับผิดชอบ หรือใครคือผู้บังคับบัญชาในแผนกนั้น ผลดีก็คือ ผู้บริหารสามารถมอบหมายงานได้ง่ายขึ้น

4. การจัดการองค์กรที่ดีช่วยให้ผู้ปฏิบัติงานได้ทำงานตามความถนัดหรือตามความเหมาะสม เช่น จากการจัดองค์กรจะต้องมีการแบ่งแผนกงาน และจัดคนลงไปทำงานในแต่ละแผนก ซึ่งการจัดคนไปในแต่ละแผนกนั้น ผู้บริหารต้องคำนึงถึงความรู้ ความสามารถและประสบการณ์เพื่อในการจัดคนให้

เหมาะสมกับงาน ถ้าผู้บริหารสามารถจัดคนให้เหมาะสมกับงานองค์กรก็จะได้ประโยชน์สูงสุดจากการทำงานของพวกเขาเหล่านั้น

นอกจากนี้ วรพจน์ บุษราคัมวดี (2552) ยังกล่าวถึงความสำคัญของการจัดการไว้ ดังนี้

1. ทำให้การดำเนินงานตามเป้าหมาย วัตถุประสงค์ขององค์กรเป็นไปอย่างมีประสิทธิภาพ (Effectiveness) และประสิทธิภาพ (Efficiency) การกำหนดเป้าหมายชัดเจน ประเมินผลดำเนินงานได้ และทำงานอย่างมีประสิทธิภาพมุ่งสู่การบริหารเพื่อต้นทุนที่ต่ำกว่า (Low cost) ดีกว่า (Better quality) เร็วกว่า (Higher speed) บริการที่ดีกว่า (Better service)

2. ในมุมมองของนักเศรษฐศาสตร์ การจัดการที่ดีจะช่วยลดค่าใช้จ่ายให้ต่ำสุด (Lowest cost) และผลตอบแทนให้ได้สูงสุด (Highest benefit)

3. การจัดการเป็นไปเพื่อให้สอดคล้องและปรับตัวต่อการเปลี่ยนแปลงของสภาพแวดล้อมโดยเฉพาะในยุคโลกาภิวัตน์ การจัดการต้องมีการจัดโครงสร้าง (Structure) และการออกแบบ (Design) ให้สอดคล้องต่อการเปลี่ยนแปลงของสภาพแวดล้อม

4. การจัดการก่อให้เกิดการอบรมขัดเกลาทางสังคม (Socialization) เพราะการปฏิบัติงานในองค์กรจะมีสถาบันหล่อหลอม อบรม สั่งสอน ขัดเกลา ให้มีบุคลากรที่เป็นไปตามเป้าหมายที่กำหนดไว้

5. การจัดการจะช่วยให้องค์กรมุ่งสู่บริหารจัดการงานอย่างเป็นระบบ ทำให้องค์กรไปสู่ความสำเร็จและมุ่งสู่ความเป็นเลิศได้

6. เกิดเป็นแนวคิดหรือพาราไดม์ใหม่เกี่ยวกับการจัดการว่าแปรเปลี่ยนไปตามยุคใหม่ ที่แปรเปลี่ยนไปตามบริบท (Context) ทางสังคม เศรษฐกิจ การเมือง เทคโนโลยี รวมทั้งสภาพแวดล้อมของงาน (Task environment)

การจัดการนั้นเป็นสิ่งสำคัญอย่างยิ่งในองค์กร เหตุผลคือประสิทธิภาพการทำงานขององค์กรส่วนใหญ่จะเปลี่ยนแปลงได้นั้นขึ้นอยู่กับการบริหารจัดการองค์กร ให้บรรลุเป้าหมายตาม ความต้องการ นั้น ต้องใช้กลยุทธ์การบริหารจัดการที่สอดคล้องกับองค์กรนั้น ๆ เนื่องจากบริบทมีการเปลี่ยนแปลงอย่างรวดเร็ว จึงจำเป็นต้องสร้างองค์กรให้แข็งแกร่งขึ้น เพื่อเพิ่มผลผลิต การจัดการ ฝึกอบรมทรัพยากรมนุษย์ และจัดทำแผนงานการจัดการองค์กรที่มีประสิทธิภาพก็จะทำให้องค์กรดำเนินงานได้อย่างราบรื่นมีประสิทธิภาพตามเป้าหมายที่ตั้งไว้

ปัจจัยสิ่งแวดล้อมที่มีอิทธิพลต่อการจัดการ การจัดการและการบริหารในปัจจุบันนี้อาจพบกับอุปสรรคต่าง ๆ มากมายซึ่งอุปสรรคเหล่านี้อาจจะเป็นปัจจัยที่ส่งผลกระทบต่อระบบการจัดการและการบริหารปัจจัยเหล่านี้บางปัจจัยเป็นปัจจัยไม่สามารถควบคุมได้ ดังนั้นถ้าต้องการให้ระบบการบริหารและการจัดการมีประสิทธิภาพและประสิทธิผล ควรต้องทำความเข้าใจและหาทางแก้ไข ดังนั้นเราจึงควรหันกลับมามองว่าปัจจัยที่มีอิทธิพลต่อการจัดการนั้นมีอะไรบ้าง ซึ่งโดยทั่วไปปัจจัยที่มีอิทธิพลต่อการจัดการแบ่งออกได้เป็น 2 ปัจจัยใหญ่ ดังนี้

องค์กรที่จะได้เปรียบในการแข่งขันและสามารถดำเนินกิจกรรมได้อย่างยั่งยืน จะต้องรู้เท่าทัน การเปลี่ยนแปลงของสภาพแวดล้อม (พิชาย รัตนดิลก ณ ภูเก็ต, 2552 : 78 – 88) ได้แบ่งสิ่งแวดล้อมที่มี อิทธิพลต่อการจัดการขององค์กรเป็น 2 ประเภท คือ

1. สิ่งแวดล้อมทั่วไป (General environment)

สิ่งแวดล้อมทั่วไป หมายถึง สิ่งแวดล้อมที่มีผลกระทบทางอ้อมต่อการปฏิบัติงาน ประจำวันขององค์กร สิ่งแวดล้อมทั่วไปประกอบด้วย รัฐ สังคมและวัฒนธรรม เงื่อนไขทางเศรษฐกิจ เทคโนโลยี แหล่งทรัพยากรด้านการเงิน และสถานการณ์ระหว่างประเทศ

2. สิ่งแวดล้อมเฉพาะ (Specific environment)

สิ่งแวดล้อมเฉพาะ หมายถึง สิ่งแวดล้อมซึ่งองค์กรมีปฏิสัมพันธ์โดยตรงหรือมีผลกระทบ ทางตรงต่อความสามารถขององค์กรในการดำเนินงานให้บรรลุเป้าหมาย สิ่งแวดล้อมเฉพาะ ได้แก่ 1) กลุ่ม อุตสาหกรรมซึ่งสะท้อนในเรื่องคู่แข่ง (Competitors) ภายในกลุ่มบริษัทเดียวกัน ถ้าเป็นหน่วยงานภาครัฐ ก็เช่น กลุ่มกระทรวงด้านสังคม มีหลายกรมที่ทำหน้าที่คล้ายกันและแข่งขันกัน อยู่ในที่แต่รุนแรงเท่า ภาคธุรกิจ 2) วัตถุดิบ หมายถึง กลุ่มที่จัดหาวัตถุดิบ (Supplies) ให้กับองค์กรและจัดจำหน่ายสินค้า 3) ทรัพยากรมนุษย์และกลุ่มสหภาพแรงงาน (Labor unions) 4) กลุ่มลูกค้าหรือผู้รับบริการ 5) หน่วยงาน และระเบียบ กฎหมายของราชการที่มีผลต่อการปฏิบัติโดยตรง

การจำแนกสิ่งแวดล้อมเป็นสิ่งแวดล้อมทั่วไปและสิ่งแวดล้อมเฉพาะนั้นไม่ใช่เป็นสิ่งตายตัว หรือมีขอบเขตแบ่งกันอย่างชัดเจนเสียทีเดียว เพราะในบางสถานการณ์และบางเวลาอาจมีความเหลื่อมล้ำ กันอยู่หรืออาจมีการสลับตำแหน่งกันได้ การจำแนกเช่นนี้เป็นเพียงกรอบที่ใช้เป็นแนวทางในการ วิเคราะห์ เพื่อทำให้มีจุดเน้นว่าในสถานการณ์และเวลาหนึ่งองค์กรให้ความสำคัญกับสิ่งแวดล้อมใดเป็นหลักและ สิ่งแวดล้อมใดเป็นรอง

กระบวนการจัดการ (Process of management) หมายถึง การกำหนดทิศทางของหน่วยงาน กลุ่มงาน หรือการดำเนินงานในหน้าที่ต่าง ๆ ให้ใช้ทรัพยากรทั้งหลายที่มีอยู่ในองค์การอย่างมี ประสิทธิภาพและประสิทธิผล การใช้ทรัพยากรอย่างมีประสิทธิภาพ (Efficient) ครอบคลุมถึง การใช้ ทรัพยากรได้อย่างเฉลียวฉลาด เหมาะสมและคุ้มค่า (Cost-effective) ส่วนการใช้ทรัพยากรอย่างมี ประสิทธิภาพ (Effective) นั้นหมายถึงการตัดสินใจได้อย่างถูกต้อง (Right decision) และมีการปฏิบัติการ สำเร็จตามแผนที่กำหนดไว้ เพื่อให้บรรลุถึงเป้าหมายขององค์กร

กระบวนการบริหารจัดการ เป็นกลไกและตัวประสานที่สำคัญที่สุดในการประมวล ผลักดัน และ กำกับให้ปัจจัยต่าง ๆ ที่เป็นทรัพยากรการจัดการประเภทต่าง ๆ สามารถดำเนินไปได้ โดยมีประสิทธิภาพ จนบรรลุเป้าหมายตามที่ต้องการ การเข้าใจถึงกระบวนการบริหารจัดการและ การฝึกฝนให้มีทักษะสูงขึ้น จะช่วยให้การบริหารงานมีประสิทธิภาพมากขึ้นได้

แมรี พาร์เกอร์ ฟอลเลท (Mary Parker Follet) ได้เสนอแนวคิดทางการบริหารจัดการให้เน้นตัวบุคคลโดยเห็นว่าความสำเร็จขององค์การขึ้นอยู่กับกลุ่มคนมากกว่าแต่ละบุคคล ผู้บริหารกับพนักงานควรเป็นส่วนส่วนกันในฐานะเป็นส่วนหนึ่งของกลุ่ม ผู้บริหารควรใช้ประสบการณ์และความรู้ จูงใจให้คนทำงานมากกว่าการใช้อำนาจตามตำแหน่งงาน (เสนาะ ตีเียว, 2546 : 46)

ฮอดเกตต์ (Hodgetts, อ้างถึงใน วิชัย รูปขำดี, 2542) มองกระบวนการจัดการภายใต้แนวคิดเชิงระบบว่า กระบวนการจัดการที่แท้จริง ก็คือการทำหน้าที่ของการจัดการ (Management function) ซึ่งมีบทบาทหน้าที่ของการจัดการภายใต้เรื่องที่สำคัญ 4 เรื่อง ได้แก่ 1) การวางแผนกำหนดทิศทางของหน่วยงาน (Planning the enterprises direction) 2) การจัดโครงสร้างองค์กรและบุคคล (Organizing and staffing the structure) 3) การอำนวยการเชิงการนำและการผลักดันบุคลากร (Leading and influencing the personnel) 4) การควบคุมในเชิงการปฏิบัติการ และในด้านทรัพยากร (Controlling organizational operations and resources)

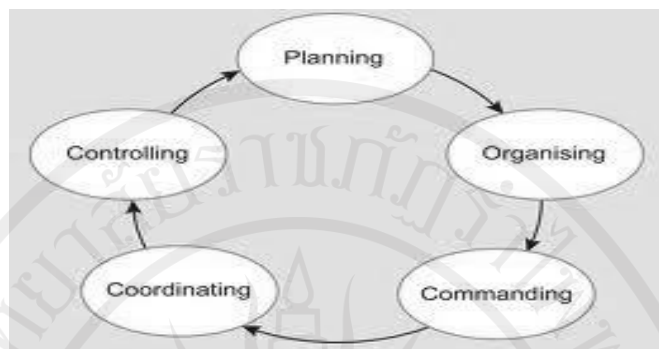
การบริหารจัดการ หมายถึง กระบวนการของการมุ่งสู่เป้าหมายขององค์การจากการทำงานร่วมกัน ซึ่งประกอบไปด้วยหน้าที่ หน้าที่คือการวางแผน ซึ่งเป็นขั้นตอนในการกำหนดวัตถุประสงค์และวิธีการปฏิบัติเพื่อให้บรรลุวัตถุประสงค์นั้น การจัดองค์กรจะเป็นขั้นตอนในการจัดบุคคลและทรัพยากรที่ใช้ในการทำงานเพื่อให้บรรลุจุดมุ่งหมายในการทำงาน การนำจะเป็นขั้นตอนที่จะสามารถทำงานให้บรรลุผลสำเร็จโดยการสร้างขวัญและกำลังใจผู้ใต้บังคับบัญชา การควบคุมจะเป็นการติดตามผลการทำงานและปรับปรุงแก้ไขเพื่อให้บรรลุผลที่ต้องการ (ศิริวรรณ เสรีรัตน์ และคณะ, 2545)

จากที่มีนักวิชาการหลายท่านได้ให้ความหมาย คำจำกัดความ นิยามของกระบวนการจัดการไว้สามารถได้ดังนี้ กระบวนการจัดการ (Process of management) คือ การวิเคราะห์ให้เห็นว่าผู้จัดการมีหน้าที่รับผิดชอบอะไรบ้าง มีงานอะไรจะต้องทำ และควรจะทำอย่างไรก่อนหลัง นับเป็นสิ่งสำคัญยิ่งสำหรับผู้จัดการที่จะได้ยึดเป็นหลักในการปฏิบัติงานเพื่อบรรลุเป้าหมายที่ตั้งไว้อย่างมีประสิทธิภาพ อาจกล่าวได้ว่าหัวใจของกระบวนการจัดการคือหน้าที่ของการบริหาร (Function of the executive) นั่นเอง แนวความคิดเรื่องกระบวนการจัดการซึ่งเป็นที่ยอมรับกันโดยทั่วไป มีดังนี้

1. กระบวนการจัดการของอองรี ฟาโย

เป็นบุคคลแรกที่วิเคราะห์ถึงองค์ประกอบมูลฐานการจัดการ 5 ประการ มีดังนี้

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี



ภาพที่ 2.2 กระบวนการจัดการขององรี ฟาโย ที่มา : แนวคิดและทฤษฎีการจัดการ, (2561)

1.1 การวางแผน (Planning) คือ การศึกษาข้อมูลในปัจจุบันและคาดการณ์ในอนาคต แล้ววางแผนเป้าหมายและแนวทางปฏิบัติไว้

1.2 การจัดการหน่วยงาน (Organizing) คือ การจัดการโครงสร้างของหน่วยงานหรือองค์การออกเป็นหน่วยงานย่อย ๆ กำหนดหน้าที่ความรับผิดชอบของหน่วยงาน การจัดสรรคนเข้าทำงานในตำแหน่งต่าง ๆ

1.3 การบังคับบัญชา (Commanding) คือ การสั่งให้คนทำงานตามที่มอบหมายงานให้ทำบังคับบัญชาพนักงานให้ทำงานตามภารกิจของหน่วยงาน

1.4 การประสานงาน (Coordinating) คือ การจัดระเบียบการทำงานไม่ให้ก้ำก่ายกันติดต่อประสานงานให้หน่วยงานย่อยต่าง ๆ ขององค์การ และประสานคนให้ทำงานโดยราบรื่น ไม่ให้ขัดแย้งกัน

2. กระบวนการจัดการของกูลิคและเออร์วิค

ได้นำหลักการจัดการของฟาโยมาปรับปรุงประยุกต์กับการบริหารจัดการระบบราชการได้เสนอแนะการจัดหน่วยงานในทำเนียบแก่ประธานาธิบดีสหรัฐอเมริกาเพื่อให้ตอบคำถามที่ว่า อะไรคืองานของประธานาธิบดีสหรัฐอเมริกา ในที่สุดก็ได้คำตอบสั้น ๆ คือ POSDCORB ซึ่งหมายถึงกระบวนการบริหาร 7 ประการดังนี้



ภาพที่ 2.3 กระบวนการจัดการของกูลิคและเออร์วิก ที่มา : Bovisualize, (2013)

2.1 Planning การวางแผนเป็นการวางแผนโครงการซึ่งเป็นการเตรียมการก่อนลงมือปฏิบัติ เพื่อให้การดำเนินการสามารถบรรลุเป้าหมายที่วางไว้อย่างมีประสิทธิภาพ

2.2 Organizing การจัดองค์การเป็นการกำหนดโครงสร้างขององค์การ โดยพิจารณาให้เหมาะสมกับงาน เช่น การแบ่งงาน (Division of work) เป็นกรม กอง หรือแผนก โดยอาศัยปริมาณงาน คุณภาพงาน หรือจัดตามลักษณะเฉพาะของงาน (Specialization)

2.3 Staffing การจัดบุคลากรปฏิบัติงานเป็นเรื่องที่เกี่ยวกับการบริหารทรัพยากรมนุษย์ในองค์การนั่นเอง ทั้งนี้เพื่อให้บุคลากรมาปฏิบัติงานอย่างมีประสิทธิภาพและสอดคล้องกับ การจัดแบ่งหน่วยงานที่กำหนดไว้

2.4 Directing การอำนวยการเป็นภาระกิจในการใช้ศิลปะในการบริหารงาน ไม่ว่าจะเป็นภาวะผู้นำ (Leadership) มนุษยสัมพันธ์ (Human relations) การจูงใจ (Motivation) และการตัดสินใจ (Decision making)

2.5 Coordinating การประสานงานเป็นการประสานให้ส่วนต่าง ๆ ของกระบวนการทำงานมีความต่อเนื่องกัน เพื่อให้การดำเนินงานเป็นไปด้วยความเรียบร้อย และราบรื่น

2.6 Reporting การรายงานเป็นกระบวนการและเทคนิคของการแจ้งให้ผู้บังคับบัญชาตามชั้นได้ทราบถึงผลการปฏิบัติงาน โดยที่มีความสัมพันธ์กับการติดต่อสื่อสาร (Communication) ในองค์การอยู่ด้วย

2.7 Budgeting งบประมาณเป็นภาระกิจที่เกี่ยวกับการวางแผนการทำบัญชี การควบคุมเกี่ยวกับการเงินและการคลัง

กระบวนการจัดการของกุ๊กและเออร์วิกเป็นที่ยอมรับของวงการทั่วไปอย่างกว้างขวาง รวมทั้งได้นำไปประยุกต์ในกิจการบริหารด้านต่าง ๆ ทั้งราชการและธุรกิจ นอกจากนั้น วงการวิชาการยังใช้อ้างอิงอยู่เสมอ

3. กระบวนการของแฮโรลด์ คูนตซ์ กำหนดขั้นตอนการจัดการไว้ 5 ขั้นตอน คือ POSDC ดังนี้



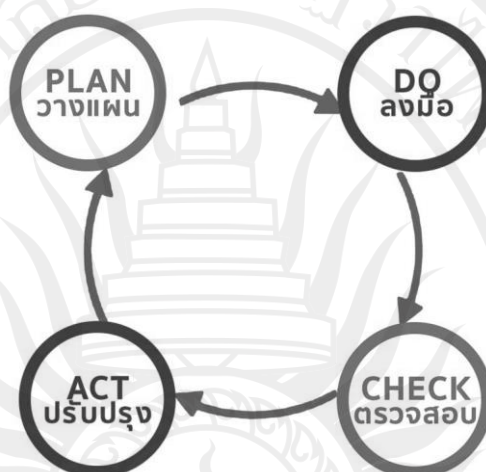
ภาพที่ 2.4 กระบวนการของแฮโรลด์ คูนตซ์

ที่มา : (ปริญญญา ธรรมเมือง และบุรินทร์ รุจจนพันธุ์, ม.ป.ป.)

- 3.1 Planning – การวางแผน
- 3.2 Organizing – การจัดองค์กร
- 3.3 Staffing – การจัดคนเข้าทำงาน
- 3.4 Directing – การอำนวยการ
- 3.5 Controlling – การควบคุมการทำงาน

4. กระบวนการจัดการตามแนวคิดปัจจุบัน หลังจากนี้ได้มีผู้เสนอกระบวนการจัดการหลายแนวคิด นักวิชาการทางการบริหารส่วนใหญ่ในปัจจุบันได้ศึกษาและวิเคราะห์แนวคิดทั้งหมดและสรุปว่า กระบวนการจัดการควรมีเพียง 4 ขั้นตอน คือ PODC (1) Planning การวางแผนงาน (2) Organizing การจัดองค์กร (3) Directing การอำนวยการหรือการชี้นำ และ (4) Controlling การควบคุมติดตามผลการทำงาน อย่างไรก็ตามไม่ว่าแนวคิดต่าง ๆ ในการจัดการจะมีกี่ขั้นตอน สารสำคัญยังคงมีรายละเอียดครอบคลุมเรื่องต่าง ๆ ในการจัดการทั้งหมดคล้ายคลึงกัน แล้วแต่การจัดหมวดหมู่ของแต่ละคนว่าจะมีกี่ขั้นตอนขึ้นอยู่กับผู้ปฏิบัติว่าจะนำเอาแนวคิดใดมาใช้กับองค์กรของตนให้เหมาะสม

5. กระบวนการบริหารของ ดร.เอ็ดเวิร์ด เดมिंग ได้ประยุกต์กระบวนการของ गुलิก และ เออร์วิกให้สั้นลง เรียกว่า วัฏจักรเดมिंग (Deming cycle) หรือ PDCA ซึ่งมี 4 ขั้นตอน ดังนี้ (สมคิด บางโม, 2558 : 71 - 72)



ภาพที่ 2.5 กระบวนการบริหารของ ดร.เอ็ดเวิร์ด เดมिंग
ที่มา : วิชาการรอบตัวเรา, (2564)

5.1 Plan คือ การกำหนดเป้าหมายจากปัญหา และสร้างออกมาเป็นแผน ในการดำเนินงาน เพื่อให้แผนงานประสบความสำเร็จ เพราะฉะนั้นในขั้นตอนนี้จะต้องกำหนดเป้าหมายให้ชัดเจนเสียก่อน และต้องกำหนดให้ครอบคลุมกระบวนการตั้งแต่เริ่มต้นไปจนถึงสิ้นสุดกระบวนการ เช่น มีปัญหาอะไรที่ควรแก้ไขหรือไม่ ใครเป็นผู้รับผิดชอบหรือเกี่ยวข้องบ้าง มีกระบวนการแก้ไขอย่างไร จากนั้นจัดทำเป็นแผนดำเนินงาน

5.2 Do คือ เป็นขั้นตอนของการลงมือปฏิบัติตามแผน โดยนำแผนดังกล่าวมาใช้ดำเนินการจริงเพื่อให้เห็นผลลัพธ์ หัวใจสำคัญของขั้นตอนนี้คือ การทดสอบเก็บข้อมูล ซึ่งเป็นการทดสอบแผนงานจากกระบวนการที่ก่อนหน้านี้เพื่อเก็บผลลัพธ์ โดยนำข้อมูลที่ได้มาพัฒนาเพิ่ม และใช้งานจริงภายหลัง เช่น หากธุรกิจการผลิตของคุณต้องการมีผลผลิตมากขึ้น และมีแผนจะปรับเปลี่ยนเครื่องจักรในโรงงานเพื่อให้มีผลผลิตที่เป็นไปตามเป้าหมายที่ได้วางไว้ คุณอาจเริ่มต้นจากการทดสอบกับเครื่องจักรเพียงเครื่องเดียวก่อนว่าสามารถให้ผลผลิตได้เท่าไร ใช้เวลานานแค่ไหน เป็นต้น หากเราทดสอบแล้วพบว่าตัวเลขการผลิตเป็นไปตามแผนก็สามารถดำเนินการในขั้นตอนต่อไปได้ หากไม่เป็นไปตามเป้าหมายจะมีแผนสำรองในการแก้ไขปัญหาอย่างไร เป็นต้น

5.3 Check คือ ขั้นตอนในการตรวจสอบ เพื่อหาช่องทางการพัฒนากระบวนการให้มีประสิทธิภาพมากยิ่งขึ้น และพิจารณาผลลัพธ์ในขั้นตอนลงมือปฏิบัติว่าสามารถทำให้เป้าหมาย ที่วางแผนไว้แต่แรกเป็นจริงได้หรือไม่ หากเป็นไปตามแผนที่ได้กำหนดไว้ ก็สามารถไปสู่ขั้นตอนต่อไปได้เลย แต่ถ้าไม่ประสบความสำเร็จ ก็จะต้องนำข้อมูลมาวิเคราะห์เพื่อหาสาเหตุของปัญหา ในขั้นตอนที่ 1 – 3 ใหม่ จนกว่าจะประสบความสำเร็จหรือผ่านตัวชี้วัดที่ได้กำหนดไว้

5.4 Act คือ ขั้นตอนของการดำเนินการปรับปรุงแก้ไข เพื่อให้กระบวนการต่าง ๆ ดีขึ้น เมื่อเราได้วางแผน ทดสอบลงมือทำตามกระบวนการ ขั้นตอนต่อมาก็คือ การนำมาปรับปรุงแก้ไขเพื่อนำไปสู่การปฏิบัติจริง ส่วนใหญ่พบว่าเหตุที่ทำให้วงจร PDCA ไปไม่ถึงความสำเร็จ เนื่องจากมีข้อจำกัดทางด้านทรัพยากร เช่น บุคคล เงินทุน เวลา ทักษะ และอื่น ๆ อีกมากมาย ซึ่งปัญหาเหล่านี้ควรจะต้องแก้ไขและพัฒนาไปเรื่อย ๆ เพื่อทำซ้ำจนหาวิธีการที่มีประสิทธิภาพมากยิ่งขึ้น

PDCA มีกระบวนการที่เรียบง่าย ไม่ว่าใครก็สามารถทำความเข้าใจกระบวนการนี้ได้ และสามารถนำไปปฏิบัติได้จริง ทำให้ตัดสินใจได้ง่ายขึ้น เนื่องจากการวางแผนและกำหนดเป้าหมายที่ชัดเจน ลดความเสี่ยงในการจัดการ มีการแนะนำให้ทำในโครงการเล็ก ๆ ก่อน หากมีข้อผิดพลาดเกิดขึ้นสามารถควบคุมสถานการณ์ได้ง่ายกว่าโครงการขนาดใหญ่ นอกจากนี้ในโครงการขนาดเล็กสามารถแก้ไขปัญหาได้ดีกว่าทำให้ลดความเสี่ยงในแง่ของการจัดการได้ดีกว่านั่นเอง

แต่ก็มีข้อเสียสำหรับการนำ PDCA มาใช้อยู่บ้าง เช่น ไม่เหมาะกับการแก้ไขปัญหา ที่เร่งด่วน แม้ว่า PDCA จะเป็นวงจรที่เรียบง่ายแต่ก็ไม่ใช่ว่าเรื่องง่าย เพราะเป็นวงจรที่มีการปรับปรุงกระบวนการเป็นขั้นตอนเล็ก ๆ อาจเกิดความล่าช้าจึงไม่เหมาะกับโครงการเร่งด่วน ขณะเดียวกันต้องอาศัยความรับผิดชอบในระยะยาว เพราะอาจไม่ได้ทำเพียงครั้งเดียวแล้วเสร็จสิ้นหากแต่เป็นกระบวนการต่อเนื่อง ดังนั้น การทำให้งานเป็นไปอย่างมีประสิทธิภาพในระยะยาวจึงต้องอาศัยความร่วมมือจากคนในองค์กร เริ่มตั้งแต่ผู้บริหารไปจนถึงระดับผู้ปฏิบัติการ หากปราศจากความรับผิดชอบวงจรนี้อาจทำให้งานไม่มีประสิทธิภาพ

5. ทรัพยากรในการบริหารจัดการ

การที่องค์กรได้นำสิ่งที่เป็นทรัพยากรการบริหารจัดการมาสนับสนุนการดำเนินงาน เพื่อให้เกิดการขับเคลื่อนกระบวนการบริหาร และนำไปสู่การบรรลุวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ ดังนี้

วิลเลียม ที. กรีนวูด (William T. Greenwood, 1965 : 33) ได้กล่าวว่า ทรัพยากรทางการบริหาร มีความสำคัญและจำเป็นต่อการบริหารงานให้ประสบความสำเร็จได้ด้วยดี และช่วยให้การทำงานบรรลุผลสัมฤทธิ์ได้อย่างมีคุณภาพ โดยมีองค์ประกอบอย่างน้อย 7 ประการ คือ คน (Man) เงิน (Money) วัสดุ สิ่งของ (Material) อำนาจหน้าที่ (Authority) เวลา (Time) กำลังใจในการทำงาน (Will) ความสะดวกต่าง ๆ (Facilities)

วิช วิษณุภาวรรณ (2551 : 47) ได้กล่าวว่า ในการบริหารจัดการเพื่อให้การปฏิบัติงานบรรลุผลสำเร็จได้นั้น จะเกี่ยวข้องกับปัจจัยต่าง ๆ ดังนี้ (1) การบริหารคน (Man) (2) การบริหารเงิน (Money) (3) การบริหารวัสดุอุปกรณ์ (Material) (4) การบริหารงานทั่วไป (Management) (5) การบริหารการให้บริการประชาชน (Market) (6) การบริหารคุณธรรม (Morality) (7) การบริหารข้อมูล (Message) (8) การบริหารเวลา (Minute) และ (9) การบริหารการวัดผล (Measurement)

หวน พินธุพันธ์ (2549 : 15) ได้กล่าวถึงทรัพยากรว่า เป็นสิ่งที่เป็นตัวกลางที่ช่วยในการดำเนินงานขององค์การให้บรรลุผลสำเร็จ โดยทรัพยากรในการบริหารที่สำคัญคือ 4 Ms ได้แก่ คน (Man) เงิน (Money) วัสดุสิ่งของ (Materials) และการจัดการ (Management)

สมคิด บางโม (2545 : 61) กล่าวว่า ทรัพยากรในการบริหาร หมายถึง วัตถุและเครื่องใช้ต่าง ๆ เพื่อประกอบการดำเนินงานตามภารกิจให้บรรลุผลสำเร็จ โดยทรัพยากรในการบริหาร ได้แก่ มนุษย์ (Man) เงิน (Money) วัสดุอุปกรณ์ (Material) และความสามารถในการจัดการ (Management) เครื่องจักร (Machine) และตลาด (Market) ซึ่งหมายถึงปฏิสัมพันธ์ต่อผู้รับบริการหรือผู้ที่ได้รับผลกระทบจากภารกิจขององค์การ

จากที่กล่าวมาสรุปได้ว่าทรัพยากรการบริหาร หมายถึง การนำปัจจัยต่าง ๆ ขององค์การ ที่เกี่ยวข้อง และตรงประเด็น มาใช้ในการกำหนดแนวทางการวางแผน การจัดการ และการควบคุมกำกับดูแล ด้วยการใช้ศาสตร์และศิลปะ เพื่อสนับสนุนให้การดำเนินงานบรรลุวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพตรงตามเป้าหมายขององค์การที่วางไว้

จากการศึกษาทฤษฎีการจัดการ ทำให้ทราบว่า การจัดการ คือ การทำงานร่วมกันของคนในองค์กร โดยมีเป้าหมายและวัตถุประสงค์ไปในทิศทางเดียวกัน โดยอาศัยกระบวนการวางแผน การบริหารจัดการองค์กรมาปรับใช้ มีการแบ่งอำนาจหน้าที่ในการดำเนินตามขอบเขตงานที่ได้รับมอบหมาย โดยอาศัยทรัพยากรไม่ว่าจะเป็น คน เงิน วัสดุ อุปกรณ์ เครื่องจักร รวมไปถึงเทคโนโลยี มาใช้เพื่อการดำเนินงานขององค์กรได้อย่างราบรื่น การบริหารจัดการจะช่วยให้การดำเนินงานขององค์กรบรรลุเป้าหมายอย่างมีประสิทธิภาพและประสิทธิผล

ผู้วิจัยจึงได้นำเอาข้อมูลที่ศึกษามาประยุกต์ใช้เป็นกรอบแนวทางในการวิจัยการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยื่น ในเรื่องที่เกี่ยวข้องกับการจัดการทั้งภายนอกและภายในองค์กร ซึ่งจะส่งผลถึงการบริหารจัดการความปลอดภัยระบบสารสนเทศให้มีประสิทธิภาพสำเร็จตามวัตถุประสงค์ที่วางไว้ได้อย่างเหมาะสม ซึ่งเป็นปัจจัยที่มีความสำคัญเป็นอย่างมากในการบริหารจัดการแพลตฟอร์มออนไลน์ไต่ยื่นด้านความปลอดภัยระบบสารสนเทศ

2.3.1 แนวคิดทฤษฎีเกี่ยวกับการจัดการการสื่อสาร

ทฤษฎีการจัดการการสื่อสารมุ่งเน้นการวิจัยเกี่ยวกับการจัดระเบียบการวางแผนและการควบคุมข้อมูลและกิจกรรมการสื่อสารทฤษฎีนี้สนับสนุนว่ากิจกรรมการสื่อสารต้องมีการจัดการและกำกับดูแล

อย่างเป็นระบบเพื่อการสื่อสารอย่างมีประสิทธิภาพและก่อให้เกิดการตอบสนองที่ต้องการซึ่งรวมถึงการระบุกลุ่มเป้าหมายการกำหนดวัตถุประสงค์ในการสื่อสารที่ชัดเจนการเลือกสื่อที่เหมาะสมการกำหนดกลยุทธ์เนื้อหาและการติดตามและประเมินผลการสื่อสารการจัดการการสื่อสารยังเกี่ยวข้องกับวิธีการสร้างสมดุลของทรัพยากรเวลาและงบประมาณและวิธีการปรับกลยุทธ์ในสภาพแวดล้อมทางสังคมวัฒนธรรมและเทคโนโลยีที่เปลี่ยนแปลงได้ขณะที่โลกาภิวัตน์ดิจิทัลและโซเชียลมีเดียเติบโตขึ้นทฤษฎีการจัดการการสื่อสารก็พัฒนาขึ้นเรื่อย ๆ โดยเน้นการมีส่วนร่วมมากขึ้นการโต้ตอบและการสื่อสารแบบสองทางกล่าวโดยสรุปทฤษฎีการจัดการการสื่อสาร (Communication Management Theory) เป็นกรอบการทำงานสำหรับองค์กรที่จะสามารถสื่อสารข้อมูลและค่านิยมขององค์กรได้อย่างมีประสิทธิภาพและประสิทธิผลเพื่อนำไปสู่การบรรลุเป้าหมายเชิงกลยุทธ์

2.3.2 แนวคิดการจัดการการสื่อสาร

การจัดการการสื่อสารเป็นระบบที่เป็นอิสระและครอบคลุมไม่จำกัดเฉพาะการไหลของข้อมูลภายในองค์กรเท่านั้นแต่ยังรวมถึงการแลกเปลี่ยนข้อมูลระหว่างองค์กรและสภาพแวดล้อมภายนอก (Wang Hui Jun et al. 2010) ระบบนี้ผ่านการวางแผน การดำเนินการ การตรวจสอบและการแก้ไขอย่างละเอียดและเป็นระบบเพื่อให้มั่นใจว่าข้อมูลจะถูกส่งผ่านหลายช่องทางและแพลตฟอร์มอย่างถูกต้องและมีประสิทธิภาพรูปแบบการจัดการนี้ไม่เพียงแต่เป็นองค์กรและการจัดเรียงการส่งข้อมูลเท่านั้นแต่ยังรวมถึงการวิจัยและพัฒนาและการส่งเสริมคำสั่งและนโยบายการสื่อสารใหม่ที่เกี่ยวข้องกับองค์กรเฉพาะโครงสร้างเครือข่าย หรือเทคโนโลยีการสื่อสาร

ในทางปฏิบัติของการจัดการการสื่อสารการพัฒนาเชิงกลยุทธ์ของโปรแกรมการสื่อสารองค์กรมีความสำคัญหลัก (XuKe, 2019) สิ่งนี้ไม่เพียงเกี่ยวข้องกับความปลอดภัยในการสื่อสารภายในองค์กรเท่านั้นแต่ยังเป็นตัวกำหนดคุณภาพของความสัมพันธ์ขององค์กรกับโลกภายนอกโดยเฉพาะอย่างยิ่งลูกค้าคู่ค้าและบุคคลอื่นที่เกี่ยวข้องดังนั้นยุทธศาสตร์การสื่อสารองค์กรจึงควรมีหลายมิติรอบด้านเพื่อให้การส่งข้อมูลมีความถูกต้องและมีประสิทธิภาพ

การออกแบบแนวทางการสื่อสารทั้งภายในและภายนอกก็เป็นส่วนสำคัญในการจัดการการสื่อสารนโยบายการสื่อสารภายในช่วยให้อุตสาหกรรมเข้าใจว่าการสื่อสารระหว่างพนักงานระหว่างพนักงานและผู้บริหารเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพขณะที่แนวทางการสื่อสารภายนอกทำหน้าที่ควบคุมการแลกเปลี่ยนข้อมูลข่าวสารขององค์กรกับโลกภายนอกรวมถึงแต่ไม่จำกัดเฉพาะสื่อสัมพันธ์การประชาสัมพันธ์และการมีปฏิสัมพันธ์กับแพลตฟอร์มโซเชียลออนไลน์ (Zhu Zhilin 2022)

การจัดการการไหลของข้อมูลยิ่งเป็นภารกิจสำคัญในการจัดการการสื่อสารซึ่งไม่ได้หมายถึงรวมถึงการสื่อสารแบบตัวต่อตัวแบบดั้งเดิมอีเมลการรายงาน ฯลฯ แต่ยังคงครอบคลุมช่องทางการสื่อสารรูปแบบใหม่ๆ เช่น การสื่อสารออนไลน์โซเชียลมีเดีย เป็นต้น โดยเฉพาะอย่างยิ่งภายใต้กระแส Digital Network การจัดการการสื่อสารออนไลน์อย่างมีประสิทธิภาพจึงกลายเป็นภารกิจสำคัญ

การสื่อสารและการจัดการมีความสัมพันธ์ที่ใกล้ชิดและซับซ้อนการเผยแพร่ไม่ได้เป็นเพียงกระบวนการแลกเปลี่ยนข้อมูลเท่านั้นแต่เป็นการแลกเปลี่ยนข้อมูลที่เป็นระเบียบและมีเป้าหมายซึ่งมี

ความสำคัญอย่างยิ่งในระดับการจัดการ (ซุนเจี้ยนลี่และจางเฉียนหนาน 2020) ผู้บริหารไม่เพียงแต่ต้องสื่อสารข้อมูลที่ชัดเจนเป็นรูปธรรมให้กับผู้ใต้บังคับบัญชาเท่านั้นแต่ยังต้องได้รับข้อเสนอแนะจากพนักงานเพื่อนำไปสู่การตัดสินใจที่มีประสิทธิภาพมากขึ้น การสื่อสารจึงมีบทบาทในการบริหารจัดการอย่างไม้อาจทดแทนได้ การสื่อสารมีสถานะที่ขาดไม่ได้ในการจัดการโครงการและเป็นกุญแจสำคัญในการทำให้แน่ใจว่าโครงการสามารถดำเนินการได้อย่างมีประสิทธิภาพและราบรื่นทุกขั้นตอน ตั้งแต่เริ่มต้นจนถึงขั้นสุดท้าย (Shen Guanglong & Qu Feiyu, 2004) หากไม่มีระบบการจัดการการสื่อสารที่ดีและมีประสิทธิภาพขั้นตอนต่าง ๆ ของการพัฒนาโครงการอาจเผชิญกับความยากลำบากและความท้าทายต่าง ๆ นั้นการสร้างกลไกการสื่อสารที่ดีเพื่อให้แน่ใจว่าข้อมูลสามารถเผยแพร่ได้อย่างมีประสิทธิภาพภายในองค์กรและแม้กระทั่งข้ามองค์กรจึงเป็นสิ่งจำเป็นสำหรับโครงการที่ประสบความสำเร็จ

สรุปการจัดการการสื่อสารเป็นระบบที่ซับซ้อนแต่มีความสำคัญอย่างยิ่งซึ่งเกี่ยวข้องกับทุกแง่มุมตั้งแต่การวางแผนกลยุทธ์ไปจนถึงการปฏิบัติจริงจากการสื่อสารภายในไปจนถึงการสื่อสารภายนอกการจัดการการสื่อสารอย่างเป็นระบบและมีมาตรฐานเท่านั้นที่จะช่วยให้มั่นใจได้ว่าข้อมูลจะถูกส่งผ่านอย่างถูกต้องและมีประสิทธิภาพในสภาพแวดล้อมที่ซับซ้อนและเปลี่ยนแปลงได้ซึ่งจะช่วยผลักดันองค์กรหรือโครงการไปสู่ความสำเร็จ

2.4 แนวคิดทฤษฎีเกี่ยวกับสารสนเทศเครือข่าย

2.4.1 ความหมายและการพัฒนาการของทฤษฎีสารสนเทศเครือข่าย

ทฤษฎีสารสนเทศเครือข่ายเป็นการขยายและการประยุกต์ทฤษฎีสารสนเทศในเครือข่ายการสื่อสาร มีวัตถุประสงค์เพื่อศึกษาวิธีการส่งข้อมูลอย่างมีประสิทธิภาพสูงสุดผ่านเครือข่าย แตกต่างจากทฤษฎีสารสนเทศแบบดั้งเดิม ทฤษฎีข้อมูลเครือข่ายมุ่งเน้นไปที่การสื่อสารแบบหลายจุดต่อหลายจุดในเครือข่ายที่ซับซ้อน ไม่ใช่แค่การสื่อสารแบบช่องทางเดียว El Gamal และ Kim, (2011) วัตถุประสงค์ของทฤษฎีข้อมูลเครือข่ายประกอบด้วยกระบวนการส่งข้อมูลระหว่างโหนด การเพิ่มประสิทธิภาพความจุช่องสัญญาณในเครือข่าย การสื่อสารแบบหลายผู้รับ การเข้ารหัสเครือข่าย ฯลฯ การใช้งานครอบคลุมสถานการณ์ที่หลากหลายในเครือข่ายการสื่อสารสมัยใหม่ เช่น การสื่อสารไร้สาย อินเทอร์เน็ตของสรรพสิ่ง (IoT) การสื่อสารผ่านดาวเทียม เป็นต้น โดยเฉพาะอย่างยิ่งในสภาพแวดล้อมการสื่อสารที่มีผู้ใช้หลายราย ทฤษฎีข้อมูลเครือข่ายมีบทบาทสำคัญในการปรับกลยุทธ์การเข้ารหัสและถอดรหัสให้เหมาะสมเพื่อปรับปรุงประสิทธิภาพและความคงทนของการส่งข้อมูล (Cover & Thomas, 2012)

รากฐานของทฤษฎีข้อมูลเครือข่ายสามารถย้อนกลับไปถึงทฤษฎีข้อมูลที่เสนอโดยแชนนอนในปี 1948 ซึ่งเป็นรากฐานสำคัญของการสื่อสารและการประมวลผลข้อมูลสมัยใหม่ (แชนนอน, 1948) ทฤษฎีข้อมูลของแชนนอนมุ่งเน้นไปที่การเข้ารหัสและถอดรหัสช่องทางเดียว โดยมีวัตถุประสงค์เพื่อศึกษาวิธีการส่งข้อมูลที่มีข้อผิดพลาดน้อยที่สุดและมีประสิทธิภาพสูงสุด บนพื้นฐานนี้ ในช่วงปลายทศวรรษ 1970 Cover และนักวิชาการคนอื่น ๆ ได้เสนอทฤษฎีของช่องสัญญาณที่มีผู้ใช้หลายราย และเริ่มให้ความสนใจกับปัญหาความจุของช่องสัญญาณในระบบที่มีผู้ใช้หลายราย (Cover, 1972)

เข้าสู่ศตวรรษที่ 21 ด้วยการพัฒนาอย่างรวดเร็วของการสื่อสารไร้สายและเทคโนโลยีอินเทอร์เน็ต โมเดลช่องทางเดียวแบบดั้งเดิมไม่สามารถตอบสนองความต้องการการสื่อสารเครือข่ายที่ซับซ้อนมากขึ้นอีกต่อไป เพื่อรับมือกับความท้าทายนี้ ทฤษฎีข้อมูลเครือข่ายได้รับการพัฒนาอย่างค่อยเป็นค่อยไป โดยประยุกต์ทฤษฎีคลาสสิกของแชนนอนกับสถานการณ์การสื่อสารแบบหลายจุด ครอบคลุมโครงสร้างการสื่อสารที่ซับซ้อน เช่น มัลติคาสต์ ช่องสัญญาณรีเลย์ และช่องสัญญาณรบกวน (Tse & Viswanath, 2005) ในช่วงไม่กี่ปีที่ผ่านมา ด้วยการเพิ่มขึ้นของเทคโนโลยี เช่น Internet of Things (IoT) และ 5G ความสำคัญของทฤษฎีข้อมูลเครือข่ายก็เพิ่มขึ้นอีก และนักวิชาการก็เริ่มมุ่งเน้นไปที่วิธีการบรรลุการส่งข้อมูลที่มีประสิทธิภาพและมีเวลาแฝงต่ำในรูปแบบที่แตกต่างกัน เครือข่าย (Lee et al., 2019)

โดยเฉพาะอย่างยิ่งหลังจากปี 2019 ได้มีการศึกษาการประยุกต์ใช้ทฤษฎีข้อมูลเครือข่ายในการสื่อสารไร้สายและ Internet of Things อย่างกว้างขวาง ตัวอย่างเช่น Lee, Kim และ Choi (2020) ศึกษาบทบาทของการเข้ารหัสเครือข่ายใน IoT ที่ต่างกัน และเสนอรูปแบบการส่งข้อมูลแบบหลายผู้รับใหม่ที่ปรับปรุงประสิทธิภาพและความเสถียรของเครือข่ายอย่างมีนัยสำคัญ ในทำนองเดียวกัน Zhou และคณะ (2021) ศึกษาการประยุกต์ใช้ทฤษฎีข้อมูลในเครือข่าย 6G และเสนอโมเดลความจุช่องสัญญาณใหม่ที่เหมาะสมกับสภาพแวดล้อม 6G เพื่อเพิ่มประสิทธิภาพการสื่อสารของเครือข่ายในอนาคต (Zhou et al., 2021)

นอกจากนี้ ทฤษฎีข้อมูลควอนตัมจะค่อย ๆ บูรณาการเข้ากับทฤษฎีข้อมูลเครือข่ายเพื่อศึกษาวิธีปรับปรุงความทนทานของการส่งข้อมูลในสภาพแวดล้อมการสื่อสารควอนตัม (Wang & Luo, 2022) แนวโน้มการพัฒนาล่าสุดในทฤษฎีข้อมูลเครือข่ายยังรวมถึงการประยุกต์ใช้การเรียนรู้เชิงลึกและปัญญาประดิษฐ์ในการเพิ่มประสิทธิภาพเครือข่าย ตัวอย่างเช่น Chen และคณะ (2023) สำรวจการประยุกต์ใช้การเรียนรู้เชิงลึกในการประมาณความจุช่องสัญญาณเครือข่ายและปรับกลยุทธ์การจัดสรรช่องสัญญาณที่มีผู้ใช้หลายรายให้เหมาะสมโดยการฝึกอบรมโครงข่ายประสาทเทียม ผลการวิจัยเหล่านี้แสดงให้เห็นว่าทฤษฎีข้อมูลเครือข่ายสมัยใหม่ไม่เพียงแต่สืบทอดแนวคิดหลักของทฤษฎีแชนนอนเท่านั้น แต่ยังดูดซับเทคโนโลยีใหม่ๆ อย่างต่อเนื่องเพื่อรับมือกับสภาพแวดล้อมเครือข่ายที่ซับซ้อนในปัจจุบัน จึงให้การสนับสนุนทางทฤษฎีสำหรับการพัฒนาเครือข่ายการสื่อสารขนาดใหญ่ในอนาคต (เฉิน และคณะ 2023)

โดยสรุป ประวัติการพัฒนากทฤษฎีข้อมูลเครือข่ายได้ขยายจากทฤษฎีข้อมูลช่องทางเดียวแบบคลาสสิกไปสู่สถานการณ์เครือข่ายที่มีผู้ใช้หลายรายและหลายช่องทางที่ซับซ้อน ในช่วงไม่กี่ปีที่ผ่านมา ได้มีการรวมเข้ากับข้อมูลควอนตัม ปัญญาประดิษฐ์ และเทคโนโลยีอื่น ๆ ค่อย ๆ สร้างกรอบทฤษฎีหลายระดับ ด้วยทฤษฎีนี้ นักวิชาการยังคงสำรวจวิธีปรับปรุงประสิทธิภาพและความน่าเชื่อถือของการส่งข้อมูลในเครือข่ายการสื่อสารที่กำลังพัฒนา เพื่อรับมือกับความท้าทายต่างๆ ในเครือข่ายการสื่อสารสมัยใหม่

2.4.2 ทฤษฎีพื้นฐานและแนวคิดหลักข้อมูลเครือข่าย

ทฤษฎีสารสนเทศแชนนอนเป็นรากฐานสำคัญของทฤษฎีข้อมูลเครือข่าย โดยกำหนดกรอบทางทฤษฎีของการส่งข้อมูลสมัยใหม่โดยการกำหนดแนวคิด เช่น ปริมาณข้อมูลและความจุของช่องสัญญาณ

(แชนนอน, 1948) ทฤษฎีของแชนนอนเป็นพื้นฐานสำหรับการศึกษาว่าข้อมูลถูกส่งผ่านช่องทางใดโดยมีข้อผิดพลาดน้อยที่สุดและมีประสิทธิภาพสูงสุด (Cover & Thomas, 2012) ความจุของช่องสัญญาณถูกกำหนดให้เป็นจำนวนข้อมูลสูงสุดที่สามารถส่งได้อย่างน่าเชื่อถือภายใต้สภาวะสัญญาณรบกวนที่กำหนด แนวคิดนี้ส่งผลโดยตรงต่อการประยุกต์ใช้ทฤษฎีข้อมูลเครือข่ายในสภาพแวดล้อมที่มีผู้ใช้หลายรายและหลายช่องสัญญาณ (Tse & Viswanath, 2005)

ในช่วงไม่กี่ปีที่ผ่านมา สถานะของทฤษฎีข้อมูลแชนนอนในทฤษฎีข้อมูลเครือข่ายได้รับการพัฒนาเพิ่มเติม ตัวอย่างเช่น (Chowdhury และ Gursoy, 2019) ขยายรูปแบบการส่งข้อมูลของ Shannon เพื่อรองรับช่องสัญญาณหลายอินพุตหลายเอาต์พุต (MIMO) ในเครือข่ายไร้สาย การศึกษาเหล่านี้วางรากฐานสำหรับการรับรองประสิทธิภาพการรับส่งข้อมูลในสภาพแวดล้อมที่ซับซ้อน (Chowdhury & Gursoy, 2019) นอกจากนี้ การประมวลผลสัญญาณรบกวนในทฤษฎีของแชนนอนยังเป็นส่วนสำคัญของระบบการสื่อสารสมัยใหม่ โดยเฉพาะอย่างยิ่งในการสื่อสารความถี่สูงสมัยใหม่ วิธีการประมวลผลสัญญาณรบกวนของช่องสัญญาณอย่างมีประสิทธิภาพเพื่อปรับปรุงคุณภาพการสื่อสารยังคงเป็นแนวทางการวิจัยที่สำคัญ (Li & Liu, 2020)

หลักการเข้ารหัสและถอดรหัสเป็นเนื้อหาหลักในทฤษฎีข้อมูลเครือข่าย จุดประสงค์คือเพื่อเข้ารหัสข้อมูลด้วยวิธีที่เหมาะสมเพื่อให้สามารถส่งผ่านช่องทางที่ไม่เหมาะสมได้อย่างมีประสิทธิภาพ และเพื่อกู้คืนข้อมูลต้นฉบับผ่านการถอดรหัส (El Gamal & Kim, 2011) วัตถุประสงค์ของการเข้ารหัสช่องสัญญาณ คือการเพิ่มข้อมูลที่ซ้ำซ้อนเพื่อรับมือกับข้อผิดพลาดที่อาจเกิดขึ้นระหว่างการสื่อสาร ในขณะที่การบีบอัดข้อมูลมีเป้าหมายเพื่อลดปริมาณข้อมูลที่ส่งเพื่อปรับปรุงประสิทธิภาพ ในช่วงไม่กี่ปีที่ผ่านมา การเข้ารหัสเครือข่ายได้กลายเป็นทิศทางการวิจัยใหม่ ด้วยการดำเนินการเข้ารหัสแบบไดนามิกในเครือข่าย ไม่เพียงแต่ปรับปรุงประสิทธิภาพการส่งข้อมูล แต่ยังช่วยเพิ่มความแข็งแกร่งของเครือข่ายด้วย (Fragouli & Soljanin, 2007)

การวิจัยล่าสุดแสดงให้เห็นว่าการประยุกต์ใช้วิธีการเรียนรู้เชิงลึกในการเข้ารหัสและถอดรหัสมีแนวโน้มในวงกว้าง Kang และคณะ (2021) เสนอรูปแบบการเข้ารหัสตามการเรียนรู้เชิงลึกที่ปรับปรุงความจุของช่องสัญญาณและความแม่นยำในการถอดรหัสในสภาพแวดล้อมที่มีผู้ใช้หลายคนอย่างมีนัยสำคัญ (Kang et al., 2021) นอกจากนี้ การประยุกต์ใช้การเข้ารหัสแบบไดนามิกใน Internet of Things (IoT) ยังดึงดูดความสนใจอย่างมาก โดยใช้วิธีการเข้ารหัสที่ยืดหยุ่นเพื่อรับมือกับความต้องการการสื่อสารที่เปลี่ยนแปลงไปในเครือข่ายเซ็นเซอร์ (Zhu et al., 2023) ความจุของเครือข่ายเป็นแนวคิดหลักในทฤษฎีข้อมูลเครือข่าย ซึ่งใช้ในการวัดจำนวนข้อมูลสูงสุดที่เครือข่ายสามารถส่งผ่านได้อย่างน่าเชื่อถือภายใต้สภาวะที่ต่างกัน การวิเคราะห์ความจุของเครือข่ายเกี่ยวข้องกับหลายแง่มุม รวมถึงปัญหาการไหลสูงสุด ทฤษฎีบทการตัดขั้นต่ำ และปริมาณงานของเครือข่าย (Ford & Fulkerson, 1962) ปัญหาการไหลสูงสุดมีจุดมุ่งหมายเพื่อกำหนดการไหลของข้อมูลสูงสุดจากโหนดต้นทางไปยังโหนดปลายทางในเครือข่าย ในขณะที่ทฤษฎีบท min-cut ใช้เพื่อระบุชุดขอบที่สามารถยอพาร์ติชันเครือข่ายให้เล็กที่สุดได้ จึงกำหนดความจุคอขวดของเครือข่าย

ในช่วงไม่กี่ปีที่ผ่านมา การวิจัยเกี่ยวกับความจุของเครือข่ายได้ให้ความสำคัญกับปัญหาการปรับให้เหมาะสมในเครือข่ายขนาดใหญ่มากขึ้น ตัวอย่างเช่น Chen และคณะ (2022) ศึกษาความจุของเครือข่ายในสภาพแวดล้อม 6G และเสนอรูปแบบการส่งข้อมูลแบบหลายผู้รับใหม่เพื่อรับมือกับความต้องการของผู้ใช้ขนาดใหญ่ในเครือข่ายที่ต่างกัน (Chen et al., 2022) ในทำนองเดียวกัน Liu และ Huang (2023) ศึกษาการประยุกต์ใช้ทฤษฎีข้อมูลควอนตัมในการวิเคราะห์ความจุของเครือข่ายเพื่อปรับปรุงประสิทธิภาพการส่งผ่านของเครือข่ายผ่านสถานะซ้อนทับของควอนตัมและสถานะที่พันกัน (Liu & Huang, 2023) การศึกษานี้ขยายแนวคิดเกี่ยวกับความจุของเครือข่ายและนำไปใช้กับเครือข่ายการสื่อสารที่ซับซ้อนสมัยใหม่

โดยสรุป ทฤษฎีข้อมูลแชนนอน หลักการเข้ารหัสและถอดรหัส และความจุของเครือข่ายถือเป็นรากฐานหลักของทฤษฎีข้อมูลเครือข่าย ตั้งแต่โมเดลการส่งข้อมูลของแชนนอนไปจนถึงการเรียนรู้เชิงลึกสมัยใหม่และการประยุกต์ใช้ข้อมูลควอนตัม ทฤษฎีข้อมูลเครือข่ายยังคงขยายและปรับปรุงอย่างต่อเนื่องเพื่อรับมือกับความต้องการด้านการสื่อสารที่เปลี่ยนแปลงไป ทฤษฎีและแนวคิดพื้นฐานเหล่านี้ไม่เพียงแต่ช่วยให้นักวิจัยมีกรอบการวิจัยที่สำคัญในทางทฤษฎีเท่านั้น แต่ยังใช้กันอย่างแพร่หลายในทางปฏิบัติในสาขาต่างๆ เช่น การสื่อสารไร้สายและ Internet of Things เพื่อเพิ่มประสิทธิภาพและความคงทนของการส่งข้อมูล

2.4.3 สถานการณ์การใช้งานข้อมูลเครือข่าย

ทฤษฎีข้อมูลเครือข่ายมีการใช้กันอย่างแพร่หลายในเครือข่ายการสื่อสารไร้สาย ครอบคลุมเครือข่ายโทรศัพท์เคลื่อนที่ Wi-Fi และเทคโนโลยีการสื่อสารไร้สายอื่น ๆ หนึ่งในแอปพลิเคชันหลักคือการเพิ่มประสิทธิภาพการจัดสรรทรัพยากรสเปกตรัม ปรับปรุงประสิทธิภาพการรับส่งข้อมูล และลดการรบกวนของช่องสัญญาณ ในเครือข่ายโทรศัพท์เคลื่อนที่ ทฤษฎีข้อมูลเครือข่ายถูกนำมาใช้เพื่อแก้ปัญหาการจัดการสัญญาณรบกวนในสภาพแวดล้อมที่มีผู้ใช้หลายคน โดยเฉพาะอย่างยิ่งเมื่อผู้ใช้หลายคนใช้คลื่นความถี่เดียวกันร่วมกัน เพื่อปรับปรุงประสิทธิภาพของระบบผ่านการจัดสรรช่องสัญญาณ การควบคุมพลังงาน และวิธีการอื่นๆ (Goldsmith & Wicker, 2005) . ในช่วงไม่กี่ปีที่ผ่านมา การเพิ่มขึ้นของ 5G และเทคโนโลยี 6G ในอนาคตได้เน้นย้ำถึงความสำคัญของทฤษฎีข้อมูลเครือข่ายในการสื่อสารไร้สาย ตัวอย่างเช่น Yang และ Chen (2020) เสนอวิธีการจัดสรรทรัพยากรแบบไดนามิกตามทฤษฎีข้อมูลเครือข่าย เพื่อปรับปรุงการใช้คลื่นความถี่และประสบการณ์ผู้ใช้เครือข่าย 5G (Yang & Chen, 2020)

นอกจากนี้ การประยุกต์ใช้ทฤษฎีข้อมูลในเครือข่าย Wi-Fi ส่วนใหญ่จะสะท้อนให้เห็นในการปรับปรุงปริมาณงานและความน่าเชื่อถือในการส่งข้อมูล ตัวอย่างเช่น Zhang และคณะ (2021) ศึกษาการประยุกต์ใช้เทคโนโลยี MIMO (Multiple Input Multiple Output) ในเครือข่าย Wi-Fi และใช้ทฤษฎีข้อมูลเครือข่ายเพื่อออกแบบรูปแบบการเข้ารหัสช่องสัญญาณที่เหมาะสมที่สุด ซึ่งจะช่วยปรับปรุงประสิทธิภาพของเครือข่าย Wi-Fi ได้อย่างมาก ปริมาณงานและความครอบคลุม (Zhang et al., 2021) ผลการวิจัยเหล่านี้แสดงให้เห็นว่าการประยุกต์ใช้ทฤษฎีข้อมูลเครือข่ายในการสื่อสารไร้สายไม่เพียง

ปรับปรุงการใช้คลื่นความถี่เท่านั้น แต่ยังช่วยเพิ่มความทนทานของเครือข่ายและความพึงพอใจของผู้ใช้อีกด้วย

Internet of Things (IoT) เป็นอีกหนึ่งสถานการณ์การใช้งานที่สำคัญของเทคโนโลยีข้อมูลเครือข่าย ซึ่งส่วนใหญ่เกี่ยวข้องกับความปลอดภัยของข้อมูล การประมวลผลข้อมูล และการสื่อสารเครือข่าย เซ็นเซอร์ ใน Internet of Things เนื่องจากการเข้าถึงเซ็นเซอร์และอุปกรณ์จำนวนมาก การส่งและการประมวลผลข้อมูลอย่างมีประสิทธิภาพจึงกลายเป็นความท้าทายที่สำคัญ การประยุกต์ใช้เทคโนโลยีข้อมูลเครือข่ายใน Internet of Things มีเป้าหมายเพื่อให้เกิดการบีบอัดข้อมูล การส่งผ่าน และความปลอดภัยที่มีประสิทธิภาพ ตัวอย่างเช่น Khan et al. (2019) เสนอรูปแบบการส่งข้อมูล IoT โดยอิงจากการเข้ารหัสเครือข่าย ซึ่งจะช่วยลดความซ้ำซ้อนของข้อมูลผ่านการเข้ารหัสแบบไดนามิก ดังนั้นจึงปรับปรุงประสิทธิภาพการใช้พลังงานและประสิทธิภาพการส่งข้อมูลของเครือข่ายเซ็นเซอร์ได้อย่างมีประสิทธิภาพ (Khan et al., 2019)

ความปลอดภัยของ Internet of Things เป็นส่วนสำคัญของเทคโนโลยีข้อมูลเครือข่าย เมื่อจำนวนอุปกรณ์ IoT เพิ่มขึ้น ปัญหาด้านความปลอดภัยของข้อมูลและความเป็นส่วนตัวก็มีความสำคัญมากขึ้น Liu และ Wang (2021) ศึกษาวิธีการเข้ารหัสตามเทคโนโลยีข้อมูลเพื่อให้มั่นใจถึงความปลอดภัยของการส่งข้อมูลในสภาพแวดล้อม Internet of Things เพิ่มการรักษาความลับของข้อมูลโดยการเพิ่มประสิทธิภาพเอนโทรปีของข้อมูลและอัลกอริธึมการเข้ารหัส (Liu & Wang, 2021) แอปพลิเคชันเหล่านี้แสดงให้เห็นว่าเทคโนโลยีข้อมูลเครือข่ายสามารถรองรับการส่งข้อมูลในสภาพแวดล้อม IoT ขณะเดียวกันก็รับประกันความปลอดภัยของข้อมูลและความเป็นส่วนตัวได้อย่างไร

การประยุกต์ใช้เทคโนโลยีข้อมูลเครือข่ายในการสื่อสารผ่านดาวเทียมและเครือข่ายเซ็นเซอร์ก็มีความสำคัญอย่างยิ่งเช่นกัน ในการสื่อสารผ่านดาวเทียม เทคโนโลยีข้อมูลเครือข่ายถูกนำมาใช้เพื่อเพิ่มประสิทธิภาพการส่งข้อมูลระหว่างดาวเทียมและสถานีภาคพื้นดิน โดยเฉพาะอย่างยิ่งในกลุ่มดาวเทียมขนาดใหญ่ วิธีการบรรจุการรับส่งข้อมูลและกำหนดเวลาอย่างมีประสิทธิภาพกลายเป็นประเด็นสำคัญในช่วงไม่กี่ปีที่ผ่านมา Xu et al. (2022) ศึกษาโมเดลการเพิ่มประสิทธิภาพการสื่อสารผ่านดาวเทียมโดยใช้เทคโนโลยีข้อมูลเพื่อปรับปรุงประสิทธิภาพการสื่อสารและความน่าเชื่อถือของการเชื่อมโยงผ่านดาวเทียมผ่านวิธีการถ่ายถอดมัลติฮอปและการเข้ารหัสเครือข่าย (Xu et al., 2022)

ในเครือข่ายเซ็นเซอร์ การประยุกต์ใช้เทคโนโลยีข้อมูลเครือข่ายส่วนใหญ่จะสะท้อนให้เห็นในการปรับปรุงประสิทธิภาพการใช้พลังงานและความสามารถในการประมวลผลข้อมูลของเครือข่าย เครือข่ายเซ็นเซอร์มักจะประกอบด้วยโหนดที่ถูกจำกัดพลังงานจำนวนมาก ดังนั้นการส่งข้อมูลที่มีประสิทธิภาพจึงเป็นสิ่งสำคัญอย่างยิ่งในการยืดอายุการใช้งานเครือข่าย Zhou และ Li (2023) เสนอโครงการฟิวชั่นข้อมูลเครือข่ายเซ็นเซอร์ตามทฤษฎีสารสนเทศ ซึ่งปรับกลยุทธ์การเข้ารหัสแบบไดนามิกเพื่อลดภาระการสื่อสารระหว่างโหนดเซ็นเซอร์ จึงช่วยขยายเวลาการทำงานของเครือข่ายได้อย่างมีประสิทธิภาพ (Zhou & Li, 2023)

นอกจากนี้ การบีบอัดข้อมูลและการตรวจจับข้อผิดพลาดในเครือข่ายเซ็นเซอร์ยังถูกนำมาใช้ผ่าน ทฤษฎีข้อมูลเครือข่าย เพื่อให้มั่นใจในการส่งข้อมูลที่เชื่อถือได้ในสภาพแวดล้อมที่รุนแรง

โดยสรุป การประยุกต์ใช้ทฤษฎีข้อมูลเครือข่ายในเครือข่ายการสื่อสารไร้สาย อินเทอร์เน็ตของสรรพสิ่ง และเครือข่ายดาวเทียมและเซ็นเซอร์ ถือเป็นรากฐานทางทฤษฎีที่มั่นคงสำหรับความก้าวหน้าของเทคโนโลยีการสื่อสารสมัยใหม่ ด้วยการเพิ่มประสิทธิภาพทรัพยากรสเปกตรัม รับประกันความปลอดภัยของข้อมูล และการปรับปรุงประสิทธิภาพการใช้พลังงานของเครือข่ายเซ็นเซอร์ ทฤษฎีข้อมูลเครือข่ายได้ส่งเสริมการพัฒนาพื้นที่สำคัญเหล่านี้อย่างมีประสิทธิภาพ และตอบสนองความต้องการและความท้าทายด้านการสื่อสารที่เพิ่มขึ้น

2.4.3 ทฤษฎีความปลอดภัยของข้อมูล

แนวคิดพื้นฐานและคำจำกัดความของความปลอดภัยของข้อมูล ความปลอดภัยของข้อมูล หมายถึงการทำให้แน่ใจว่าข้อมูลและระบบได้รับการปกป้องจากการเข้าถึง การรั่วไหล การปลอมแปลง และการทำลายโดยไม่ได้รับอนุญาตระหว่างการจัดเก็บ การส่งผ่าน และการประมวลผล และเพื่อให้บรรลุเป้าหมายในการปกป้องการรักษาความลับ ความสมบูรณ์ และความพร้อมของข้อมูล (Stallings & Brown, 2020)

ในด้านวิชาการและการประยุกต์ใช้ในวงกว้าง หลักของความปลอดภัยของข้อมูลอยู่ที่การรักษาความปลอดภัยของข้อมูลในทุกขั้นตอนเพื่อป้องกันภัยคุกคามจากแหล่งข้อมูลทั้งภายนอกและภายใน การรักษาความปลอดภัยของข้อมูลประกอบด้วยกรอบการผสมผสานระหว่างวิธีการทางเทคนิค มาตรการการจัดการ และบรรทัดฐานด้านพฤติกรรมเพื่อให้บรรลุเป้าหมายการปกป้องระบบข้อมูล (Whitman & Mattord, 2021)

ความหมายแฝงของความปลอดภัยของข้อมูลสามารถเข้าใจได้ด้วยเป้าหมายหลัก 3 ประการ ได้แก่ การรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน ซึ่งเรียกอีกอย่างว่า "องค์ประกอบสามประการของ CIA" ของการรักษาความปลอดภัยข้อมูล (การรักษาความลับ ความสมบูรณ์ ความพร้อมใช้งาน) การรักษาความลับคือเพื่อให้แน่ใจว่าข้อมูลสามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น ความสมบูรณ์คือการป้องกันข้อมูลจากการดัดแปลงโดยไม่ได้รับอนุญาต ความพร้อมใช้งานคือเพื่อให้แน่ใจว่าผู้ใช้ที่ได้รับอนุญาตจะสามารถใช้ข้อมูลได้เมื่อจำเป็น (Peltier, 2019) นอกเหนือจากเป้าหมายหลักทั้งสามนี้แล้ว ความปลอดภัยของข้อมูลยังเกี่ยวข้องกับแง่มุมอื่น ๆ ด้วย เช่น การตรวจสอบตัวตน การไม่ปฏิเสธ และการควบคุมการเข้าถึง ซึ่งขยายขอบเขตความปลอดภัยของข้อมูลและทำให้เหมาะสมกับสถานการณ์การใช้งานที่หลากหลายมากขึ้น (Solms & Niekerk, 2016)

ในกระบวนการพัฒนาความปลอดภัยของข้อมูล ด้วยความก้าวหน้าของเทคโนโลยี ส่วนขยายที่กำลังขยายตัวเช่นกัน ความปลอดภัยของข้อมูลสมัยใหม่ไม่ได้จำกัดอยู่เพียงการปกป้องข้อมูลเพียงอย่างเดียว แต่ยังรวมถึงการปกป้องสภาพแวดล้อมของระบบ สิ่งอำนวยความสะดวกทางกายภาพ และสื่อการสื่อสารต่างๆ นอกจากนี้ ความปลอดภัยของข้อมูลยังเกี่ยวข้องกับอย่างใกล้ชิดกับโครงสร้างการกำกับดูแล

ขององค์กร ไม่เพียงแต่ปัญหาด้านเทคนิคเท่านั้น แต่ยังเกี่ยวข้องกับการประสานงานในระดับกฎหมาย การจัดการ และนโยบายด้วย (Ahmad et al., 2023)

แม้ว่าความปลอดภัยของข้อมูลจะซ้อนทับกับแนวคิดอื่นๆ ที่เกี่ยวข้อง เช่น ความปลอดภัยของเครือข่ายและความเป็นส่วนตัวของข้อมูล แต่ก็ยังมีคุณลักษณะเฉพาะของตัวเองอีกด้วย ความปลอดภัยของข้อมูลมุ่งเน้นไปที่การปกป้องทรัพยากรข้อมูลเป็นหลัก ในขณะที่ความปลอดภัยของเครือข่ายมุ่งเน้นไปที่การปกป้องความปลอดภัยของเครือข่ายทั้งหมดและสถาปัตยกรรม รวมถึงการป้องกันฮาร์ดแวร์ ซอฟต์แวร์ และสภาพแวดล้อมเครือข่าย (Tetrack & Williams, 2021) ทั้งสองมีความสัมพันธ์กันอย่างใกล้ชิด และความปลอดภัยทางไซเบอร์ถือเป็นส่วนหนึ่งของความปลอดภัยของข้อมูล โดยเฉพาะอย่างยิ่งเมื่อข้อมูลที่ส่งผ่านอินเทอร์เน็ตจำเป็นต้องได้รับการปกป้องความเป็นส่วนตัวของข้อมูลและความปลอดภัยของข้อมูลเป็นสองแนวคิดที่แยกกันไม่ออก ความเป็นส่วนตัวของข้อมูลส่วนใหญ่เน้นย้ำถึงวิธีการตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลจะไม่ถูกนำไปใช้ในทางที่ผิดหรือรั่วไหลเมื่อรวบรวม จัดเก็บ และใช้ และมุ่งเน้นไปที่ความถูกต้องตามกฎหมายและการปฏิบัติตามข้อกำหนดของข้อมูล (Wright & Raab, 2022) ในทางกลับกัน ความปลอดภัยของข้อมูลมุ่งเน้นไปที่การรับรองความปลอดภัยของข้อมูลผ่านวิธีการทางเทคนิคและกลไกการจัดการมากกว่า ดังนั้น จึงสามารถเข้าใจความสัมพันธ์ระหว่างความปลอดภัยของข้อมูลและความเป็นส่วนตัวของข้อมูลได้ เนื่องจากการบรรลุความเป็นส่วนตัวของข้อมูลจำเป็นต้องได้รับการสนับสนุนจากเทคโนโลยีความปลอดภัยของข้อมูล เพื่อปกป้องความปลอดภัยของข้อมูลที่ละเอียดอ่อน ตลอดจนวงจรชีวิตของข้อมูล (Kumar & Dhillon, 2020)

สรุปความสำคัญของความปลอดภัยของข้อมูลมีความสำคัญมากขึ้นเรื่อย ๆ ในขณะที่กระบวนการเปลี่ยนผ่านสู่ดิจิทัลมีการเร่งตัวเร็วขึ้น ไม่ว่าจะเป็นการปกป้องความเป็นส่วนตัวหรือการปกป้องความลับทางการค้าขององค์กร ความปลอดภัยของข้อมูลได้กลายเป็นรากฐานที่สำคัญในสังคมดิจิทัล ด้วยการทำความเข้าใจความหมายแฝงและส่วนขยาย ตลอดจนความสัมพันธ์กับความปลอดภัยของเครือข่ายและความเป็นส่วนตัวของข้อมูล เราจึงสามารถตอบสนองต่อความท้าทายด้านความปลอดภัยที่เปลี่ยนแปลงไปในยุคดิจิทัลได้ดีขึ้น

2.4.5 การพัฒนาความปลอดภัยของข้อมูล

กระบวนการพัฒนาความปลอดภัยของข้อมูลสามารถสืบทอดไปถึงขั้นเริ่มต้นของความต้องการในการปกป้องข้อมูล และผ่านขั้นตอนการพัฒนาที่สำคัญมากมายตั้งแต่แบบเดิม ๆ ไปจนถึงสมัยใหม่ ความปลอดภัยของข้อมูลในระยะเริ่มแรกมุ่งเน้นไปที่ความปลอดภัยทางกายภาพเป็นหลัก เนื่องจากการแพร่หลายของคอมพิวเตอร์และเครือข่าย ความปลอดภัยของข้อมูลจึงค่อย ๆ พัฒนาไปสู่สาขาหลายมิติและสหวิทยาการ (Whitman & Mattord, 2021) แนวคิดนี้จะแนะนำประวัติการพัฒนาความปลอดภัยของข้อมูล ครอบคลุมขั้นตอนหลักและคุณลักษณะของแต่ละขั้นตอน

การพัฒนาความปลอดภัยของข้อมูลสามารถแบ่งออกเป็นหลายขั้นตอนสำคัญ โดยแต่ละขั้นตอนมีข้อกำหนดด้านความปลอดภัยและคุณลักษณะทางเทคนิคเฉพาะของตัวเอง ความปลอดภัยของข้อมูลในระยะเริ่มแรกมุ่งเน้นไปที่การป้องกันทางกายภาพเป็นหลัก เช่น การปกป้องไฟล์และอุปกรณ์จากความ

เสียหายหรือการโจรกรรม (Stallings & Brown, 2020) ในช่วงเวลานี้ วิธีการหลักของการรักษาความปลอดภัยของข้อมูล คือเพื่อให้มั่นใจในความปลอดภัยของข้อมูลโดยการล็อกการเข้าถึงทางกายภาพ และจำกัดไม่ให้บุคลากรเข้าไปในพื้นที่ที่มีความละเอียดอ่อน

ด้วยการถือกำเนิดของคอมพิวเตอร์ ความปลอดภัยของข้อมูลได้เข้าสู่ขั้นตอนที่สอง ซึ่งก็คือ ขั้นตอนการรักษาความปลอดภัยคอมพิวเตอร์ ในขั้นตอนนี้ คอมพิวเตอร์จะค่อยๆ กลายเป็นเครื่องมือหลักในการจัดเก็บและประมวลผลข้อมูล ดังนั้นการปกป้องข้อมูลในคอมพิวเตอร์จากการเข้าถึงที่เป็นอันตราย จึงกลายเป็นประเด็นสำคัญ การรักษาความปลอดภัยของคอมพิวเตอร์ในยุคแรกเริ่มอาศัยการควบคุมการเข้าถึงและเทคโนโลยีการเข้ารหัสขั้นพื้นฐานเป็นหลัก (Kim & Solomon, 2019)

ในช่วงทศวรรษ 1990 อินเทอร์เน็ตแพร่หลายอย่างรวดเร็วได้นำความปลอดภัยของข้อมูลมาสู่ ขั้นตอนการรักษาความปลอดภัยเครือข่าย เนื่องจากเครือข่ายเปิดกว้างและเชื่อมโยงถึงกัน การส่งข้อมูลจึงมีความเปราะบางมากขึ้นและเสี่ยงต่อการโจมตีเครือข่ายต่างๆ เช่น การแฮ็กและการแพร่กระจายของไวรัส ในเวลานี้ เทคโนโลยี เช่น ไฟร์วอลล์ ระบบตรวจจับการบุกรุก (IDS) และเครือข่ายส่วนตัวเสมือน (VPN) เริ่มถูกนำมาใช้กันอย่างแพร่หลายเพื่อปกป้องความปลอดภัยของการส่งข้อมูลในเครือข่าย (Peltier, 2019)

เมื่อเข้าสู่ศตวรรษที่ 21 ความปลอดภัยของข้อมูลค่อยๆ พัฒนาไปสู่ระบบรักษาความปลอดภัยที่ครอบคลุมมากขึ้น ซึ่งเกี่ยวข้องกับหลายแง่มุม เช่น ความปลอดภัยของข้อมูล ความปลอดภัยของเครือข่าย และความปลอดภัยของแอปพลิเคชัน ด้วยการประยุกต์ใช้คลาวด์คอมพิวเตอร์ Internet of Things และเทคโนโลยีข้อมูลขนาดใหญ่อย่างกว้างขวาง ภัยคุกคามที่ความปลอดภัยของข้อมูลต้องเผชิญจึงมีความซับซ้อนและหลากหลายมากขึ้น และวิธีการป้องกันแบบดั้งเดิมไม่สามารถตอบสนองความต้องการของการปกป้องข้อมูลสมัยใหม่ได้อย่างเต็มที่อีกต่อไป (Ahmad et al. , 2023)

ดังนั้นการรักษาความปลอดภัยของข้อมูลสมัยใหม่จึงให้ความสำคัญกับการออกแบบสถาปัตยกรรมความปลอดภัยโดยรวมมากขึ้น รวมถึงการบริหารความเสี่ยง ข้อมูลภัยคุกคาม และการตรวจสอบความปลอดภัยอย่างต่อเนื่อง ขั้นตอนการพัฒนาความปลอดภัยของข้อมูลสามารถแบ่งออกเป็นขั้นตอนหลักได้ดังต่อไปนี้

ขั้นตอนการรักษาความปลอดภัยทางกายภาพมุ่งเน้นไปที่การป้องกันทางกายภาพและรับรองความปลอดภัยของข้อมูลโดยการควบคุมการเข้าถึงทางกายภาพของบุคลากร ในขั้นตอนนี้ วิธีการหลักได้แก่ การล็อกตู้เก็บเอกสารและการรักษาความปลอดภัยอุปกรณ์อำนวยความสะดวก (Stallings & Brown, 2020)

จุดเน้นของขั้นตอนการรักษาความปลอดภัยคอมพิวเตอร์คือการปกป้องข้อมูลในคอมพิวเตอร์จากการเข้าถึงและการดัดแปลงโดยไม่ได้รับอนุญาต ในขั้นตอนนี้ การควบคุมการเข้าถึง การตรวจสอบสิทธิ์ผู้ใช้ และการเข้ารหัสข้อมูล กลายเป็นวิธีการรักษาความปลอดภัยหลัก (Kim & Solomon, 2019)

ขั้นตอนการรักษาความปลอดภัยเครือข่ายมาพร้อมกับแอปพลิเคชันอินเทอร์เน็ตที่แพร่หลาย ซึ่งทำให้การส่งข้อมูลเผชิญกับภัยคุกคามมากขึ้นและการโจมตีเครือข่ายกลายเป็นความเสี่ยงหลัก เพื่อให้

มั่นใจถึงความปลอดภัยของข้อมูลในเครือข่าย เทคโนโลยี เช่น ไฟร์วอลล์, IDS และ VPN จึงถูกนำมาใช้กันอย่างแพร่หลายในขั้นตอนนี้ (Peltier, 2019)

ขั้นตอนการรักษาความปลอดภัยข้อมูลที่ครอบคลุม ด้วยการพัฒนาเทคโนโลยีใหม่ เช่น การประมวลผลแบบคลาวด์ ข้อมูลขนาดใหญ่ และอินเทอร์เน็ตของสรรพสิ่ง ความหมายแฝงและการขยายความปลอดภัยของข้อมูลยังคงขยายตัวอย่างต่อเนื่อง โดยต้องใช้มาตรการการจัดการความปลอดภัยที่ครอบคลุมมากขึ้น ในขั้นตอนนี้ การบริหารความเสี่ยง การออกแบบสถาปัตยกรรมความปลอดภัย ข้อมูลภัยคุกคาม การตรวจสอบอย่างต่อเนื่อง และวิธีการอื่นๆ กลายเป็นแกนหลักของการรักษาความปลอดภัยของข้อมูล (Ahmad et al., 2023)

แนวโน้มความปลอดภัยของข้อมูลในอนาคต ด้วยการพัฒนาเทคโนโลยีเกิดใหม่ เช่น ปัญญาประดิษฐ์ และคอมพิวเตอร์ควอนตัม ความปลอดภัยของข้อมูลก็มีการพัฒนาอย่างต่อเนื่องเช่นกัน ตัวอย่างเช่น การเกิดขึ้นของคอมพิวเตอร์ควอนตัมก่อให้เกิดความท้าทายต่อเทคโนโลยีการเข้ารหัสแบบดั้งเดิม ในขณะที่ปัญญาประดิษฐ์ใช้ในการตรวจจับและตอบสนองต่อภัยคุกคาม เพื่อปรับปรุงการประมวลผลเหตุการณ์ด้านความปลอดภัยโดยอัตโนมัติ (Kumar & Dhillon, 2020)

กล่าวโดยสรุป ประวัติการพัฒนากฎความปลอดภัยของข้อมูลสะท้อนให้เห็นถึงการพัฒนาอย่างต่อเนื่องของเทคโนโลยีสารสนเทศและความต้องการด้านความปลอดภัย ตั้งแต่การป้องกันทางกายภาพล้วนๆ ไปจนถึงการป้องกันรอบด้านที่เกี่ยวข้องกับเครือข่ายและข้อมูล ไปจนถึงระบบรักษาความปลอดภัยแบบครอบคลุมที่ทันสมัยซึ่งครอบคลุมหลายสาขา ความปลอดภัยของข้อมูลยังคงพัฒนาอย่างต่อเนื่องเพื่อตอบสนองต่อสภาพแวดล้อมภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา การทำความเข้าใจกระบวนการพัฒนานี้จะช่วยให้เราวางแผนและใช้กลยุทธ์การรักษาความปลอดภัยของข้อมูลได้ดีขึ้นในสภาพแวดล้อมดิจิทัลที่ซับซ้อนในปัจจุบัน

2.4.6 เป้าหมายความปลอดภัยของข้อมูล

เป้าหมายของการรักษาความปลอดภัยข้อมูลคือการปกป้องความปลอดภัยของระบบข้อมูลและข้อมูลและรับประกันการรักษาความลับ ความสมบูรณ์ และความพร้อมของข้อมูล เป้าหมายเหล่านี้มักเรียกว่าองค์ประกอบหลักสามประการของการรักษาความปลอดภัยข้อมูล (CIA สามองค์ประกอบ) นอกจากนี้ ด้วยการพัฒนาเทคโนโลยีสารสนเทศอย่างต่อเนื่อง เป้าหมายของความปลอดภัยของข้อมูลยังได้ขยายออกไปให้ครอบคลุมถึงการรับรองความถูกต้องของข้อมูลประจำตัว การไม่ปฏิเสธ และการควบคุมการเข้าถึง การทำความเข้าใจเป้าหมายเหล่านี้ช่วยพัฒนากลยุทธ์การรักษาความปลอดภัยของข้อมูลที่มีประสิทธิภาพในสถานการณ์การใช้งานต่างๆ (Stallings & Brown, 2020)

เป้าหมายหลักของความปลอดภัยของข้อมูล ได้แก่ การรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน การรักษาความลับหมายถึงการทำให้แน่ใจว่าข้อมูลสามารถเข้าถึงได้และใช้งานโดยบุคคลากรที่ได้รับอนุญาตเท่านั้น เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต (Kim & Solomon, 2019) การรักษาความลับมักเกิดขึ้นได้ด้วยเทคโนโลยีการเข้ารหัสและนโยบายการควบคุมการเข้าถึง เพื่อให้มั่นใจในความปลอดภัยของข้อมูลที่ละเอียดอ่อนระหว่างการส่งและการจัดเก็บ ด้วยการแบ่งปันข้อมูลอย่างกว้างขวาง

และการละเมิดข้อมูลบ่อยครั้ง การรักษาความลับจึงกลายเป็นเป้าหมายที่สำคัญที่สุดประการหนึ่งในความปลอดภัยของข้อมูล (Whitman & Mattord, 2021) ตัวอย่างเช่น บริษัทจำเป็นต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลของลูกค้าไม่รั่วไหลผ่านการจัดการสิทธิ์และการเข้ารหัสข้อมูลที่เข้มงวด ความสมบูรณ์หมายถึงการรับรองว่าข้อมูลจะไม่ถูกดัดแปลงหรือเสียหายโดยไม่ได้รับอนุญาตระหว่างการส่งและการจัดเก็บ เพื่อให้มั่นใจถึงความถูกต้องและความสม่ำเสมอของข้อมูล (Peltier, 2019)

ความสมบูรณ์ไม่เพียงแต่ต้องป้องกันไม่ให้ผู้โจมตีที่เป็นอันตรายแก้ไขข้อมูลเท่านั้น แต่ยังต้องป้องกันความเสียหายของข้อมูลเนื่องจากอุบัติเหตุหรือความล้มเหลวทางเทคนิคในระหว่างดำเนินการตามปกติอีกด้วย ตัวอย่างเช่น การใช้เทคโนโลยี เช่น ลายเซ็นดิจิทัลและฟังก์ชันแฮชสามารถตรวจสอบความสมบูรณ์ของข้อมูลและมั่นใจได้ว่าข้อมูลจะไม่ได้รับการแก้ไข (Stallings & Brown, 2020) ความพร้อมใช้งานหมายถึงการทำให้แน่ใจว่าระบบข้อมูลและข้อมูลสามารถเข้าถึงและใช้งานได้โดยผู้ใช้ที่ถูกต้องตามกฎหมายเมื่อจำเป็น (Ahmad et al., 2023) ไม่ว่าจะเป็นการหยุดทำงานของเซิร์ฟเวอร์ การโจมตีเครือข่าย (เช่น การโจมตี DDoS) หรือความล้มเหลวของฮาร์ดแวร์ ความพร้อมใช้งานของระบบจะได้รับผลกระทบ เพื่อให้มั่นใจว่ามีความพร้อมใช้งาน องค์กรมักจะต้องใช้มาตรการต่างๆ เช่น การสำรองข้อมูลซ้ำซ้อน ไฟร์วอลล์ และการปรับสมดุลโหลดเพื่อให้แน่ใจว่าระบบสามารถทำงานได้ตามปกติเมื่อเผชิญกับการโจมตีหรือความล้มเหลว (Kim & Solomon, 2019)

เป้าหมายที่เพิ่มขึ้นของการรักษาความปลอดภัยข้อมูล ได้แก่ การรับรองความถูกต้อง การไม่ปฏิเสธ และการควบคุมการเข้าถึง การรับรองความถูกต้องเป็นกระบวนการในการตรวจสอบตัวตนของผู้ใช้หรือระบบเพื่อให้แน่ใจว่าเฉพาะผู้ใช้ที่ถูกต้องเท่านั้นที่สามารถเข้าถึงระบบข้อมูลได้ (Kumar & Dhillon, 2020) วิธีการตรวจสอบสิทธิ์ทั่วไป ได้แก่ ชื่อผู้ใช้และรหัสผ่าน ข้อมูลชีวภาพ (เช่น ลายนิ้วมือและการจดจำใบหน้า) และการตรวจสอบสิทธิ์แบบหลายปัจจัย (MFA) การรับรองความถูกต้องมีบทบาทสำคัญในการรักษาความปลอดภัยของข้อมูล โดยเฉพาะอย่างยิ่งในการปกป้องข้อมูลที่ละเอียดอ่อนและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การไม่ปฏิเสธหมายถึงการรับรองว่าผู้ส่งหรือผู้รับข้อมูลไม่สามารถปฏิเสธได้ว่าพวกเขาได้ส่งหรือรับข้อมูล ซึ่งเป็นสิ่งสำคัญมากในการป้องกันการฉ้อโกงในการทำธุรกรรม (Solms & Niekerk, 2020) ลายเซ็นดิจิทัลและการประทับเวลาเป็นเทคโนโลยีทั่วไปในการไม่ปฏิเสธ ซึ่งสามารถให้หลักฐานที่มีประสิทธิภาพเพื่อให้แน่ใจว่าทั้งสองฝ่ายที่สื่อสารกันมีหน้าที่รับผิดชอบในการส่งข้อมูล นี่เป็นสิ่งสำคัญอย่างยิ่งสำหรับด้านต่างๆ เช่น อีคอมเมิร์ซและธุรกรรมทางการเงิน การควบคุมการเข้าถึงหมายถึงการจำกัดและการจัดการการเข้าถึงทรัพยากรระบบเพื่อให้แน่ใจว่าเฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลหรือทรัพยากรระบบที่เฉพาะเจาะจง (Whitman & Mattord, 2021)

โดยทั่วไปนโยบายการควบคุมการเข้าถึงจะรวมถึงการควบคุมการเข้าถึงตามบทบาท (RBAC), การควบคุมการเข้าถึงแบบบังคับ (MAC) และการควบคุมการเข้าถึงตามดุลยพินิจ (DAC) ด้วยการใช้การควบคุมการเข้าถึงที่มีประสิทธิภาพ การรั่วไหลของข้อมูลหรือการทำลายที่เกิดจากความประมาทเลินเล่อของบุคลากรหรือพฤติกรรมที่เป็นอันตรายจะลดลง

เป้าหมายของการรักษาความปลอดภัยข้อมูลไม่ได้้อย่างโดดเดี่ยว แต่มีอยู่โดยรวม การรักษาความปลอดภัย และความสมบูรณ์ และความพร้อมใช้งานเป็นหัวใจหลักของความปลอดภัยของข้อมูล และการตรวจสอบตัวตน การไม่ปฏิเสธ และการควบคุมการเข้าถึงให้การสนับสนุนและการรับประกันสำหรับแกนหลักนี้ (Ahmad et al., 2023) เป้าหมายเหล่านี้เชื่อมโยงถึงกันและเสริมกำลังร่วมกัน และร่วมกันสร้างระบบรักษาความปลอดภัยข้อมูลที่ครอบคลุม ตัวอย่างเช่น การผสมผสานการรักษาความปลอดภัยและการตรวจสอบตัวตนสามารถรับประกันได้ว่ามีเพียงผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้ ในขณะที่การผสมผสานระหว่างความสมบูรณ์และการไม่ปฏิเสธสามารถรับประกันความถูกต้องของข้อมูลและเป็นหลักฐานยืนยันความถูกต้องตามกฎหมายของการส่งข้อมูล

สรุปด้วยการพัฒนาเทคโนโลยีสารสนเทศอย่างต่อเนื่อง ภัยคุกคามต่อความปลอดภัยของข้อมูลก็มีการพัฒนาอย่างต่อเนื่อง ดังนั้นเป้าหมายของความปลอดภัยของข้อมูลจึงต้องมีการปรับเปลี่ยนและขยายอย่างต่อเนื่อง ด้วยการทำความเข้าใจและบรรลุเป้าหมายด้านความปลอดภัยเหล่านี้ องค์กรและบุคคลจึงสามารถปกป้องทรัพยากรข้อมูลได้ดีขึ้น และรับประกันการรักษาความปลอดภัย ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลในสภาพแวดล้อมที่หลากหลาย

2.4.7 เทคโนโลยีและวิธีการหลักในการรักษาความปลอดภัยข้อมูลเครือข่าย

เทคโนโลยีและวิธีการรักษาความปลอดภัยข้อมูลได้รับการออกแบบมาเพื่อปกป้องระบบข้อมูลจากภัยคุกคามต่างๆ และรับประกันการรักษาความปลอดภัย ความสมบูรณ์ และความพร้อมของข้อมูล เทคโนโลยีความปลอดภัยของข้อมูลหลัก ได้แก่ เทคโนโลยีการเข้ารหัส กลไกการรับรองความถูกต้องและการตรวจสอบตัวตน ไฟร์วอลล์ ระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS) เทคโนโลยีเหล่านี้เสริมซึ่งกันและกันและรวมกันเป็นระบบป้องกันความปลอดภัยของข้อมูล (Stallings & Brown, 2020) เทคโนโลยีการเข้ารหัสเป็นหนึ่งในวิธีการพื้นฐานและใช้กันอย่างแพร่หลายในการรักษาความปลอดภัยข้อมูล วัตถุประสงค์หลักคือเพื่อให้แน่ใจว่าข้อมูลเป็นความลับโดยการแปลงข้อความธรรมดาเป็นไซเฟอร์เท็กซ์ เทคโนโลยีการเข้ารหัสแบ่งออกเป็นสองวิธี: การเข้ารหัสแบบสมมาตรและการเข้ารหัสแบบอสมมาตร

การเข้ารหัสแบบสมมาตรเป็นเทคนิคที่ใช้คีย์เดียวในการเข้ารหัสและถอดรหัส และมีประสิทธิภาพในการคำนวณ อัลกอริธึมการเข้ารหัสแบบสมมาตรทั่วไป ได้แก่ Advanced Encryption Standard (AES) และ Data Encryption Standard (DES) (Kim & Solomon, 2019) ข้อดีของการเข้ารหัสแบบสมมาตรคือมีความรวดเร็วและเหมาะสำหรับการเข้ารหัสข้อมูลจำนวนมากอย่างรวดเร็ว แต่ปัญหาหลักคือการกระจายและการจัดการคีย์ การประนีประนอมที่สำคัญอาจส่งผลให้เกิดความสมบูรณ์และการรักษาความปลอดภัยของข้อมูลที่ถูกบุกรุก (Peltier, 2019)

การเข้ารหัสแบบอสมมาตรใช้คีย์คู่หนึ่ง: คีย์สาธารณะและคีย์ส่วนตัว โดยคีย์สาธารณะใช้สำหรับการเข้ารหัส และใช้คีย์ส่วนตัวสำหรับการถอดรหัส วิธีนี้จะแก้ปัญหาการกระจายคีย์ในการเข้ารหัสแบบสมมาตรได้อย่างมีประสิทธิภาพ อัลกอริธึมการเข้ารหัสแบบอสมมาตรทั่วไป ได้แก่ RSA และการเข้ารหัสแบบเส้นโค้งวงรี (ECC) (Stallings & Brown, 2020) ข้อได้เปรียบหลักของการเข้ารหัสแบบอสมมาตรคือ

ความปลอดภัยที่ได้รับการปรับปรุง แต่เนื่องจากความซับซ้อนในการคำนวณสูง จึงมักจะใช้เพื่อเข้ารหัสข้อมูลจำนวนเล็กน้อยหรือแลกเปลี่ยนคีย์สมมาตรเท่านั้น (Kumar & Dhillon, 2020)

กลไกการรับรองความถูกต้องและการตรวจสอบตัวตนเป็นวิธีการสำคัญเพื่อให้แน่ใจว่าระบบข้อมูลสามารถเข้าถึงได้โดยผู้ใช้ที่ได้รับอนุญาตเท่านั้น การตรวจสอบตัวตนทำให้มั่นใจได้ว่าเฉพาะผู้ใช้ที่ถูกต้องเท่านั้นที่สามารถเข้าถึงทรัพยากรระบบโดยการตรวจสอบตัวตนของผู้ใช้ วิธีการตรวจสอบตัวตนทั่วไป ได้แก่ การพิสูจน์ตัวตนด้วยรหัสผ่าน การพิสูจน์ตัวตนด้วยชีวมาตร (เช่น ลายนิ้วมือและการจดจำใบหน้า) และการตรวจสอบสิทธิ์แบบหลายปัจจัย (MFA) ซึ่งรวมวิธีการพิสูจน์ตัวตนหลายวิธีเพื่อเพิ่มความปลอดภัย (Ahmad et al., 2023)

Solms & Niekerk, 2020) การตรวจสอบรหัสผ่านเป็นวิธีการตรวจสอบสิทธิ์ขั้นพื้นฐานที่สุด แต่การรักษาความปลอดภัยนั้นไม่จำกัด เนื่องจากรหัสผ่านถูกถอดรหัสหรือถูกขโมยได้ง่าย การรับรองความถูกต้องด้วยไบโอเมตริกซ์ใช้คุณลักษณะไบโอเมตริกซ์เฉพาะตัวของผู้ใช้ในการยืนยันตัวตน เช่น ลายนิ้วมือ ม่านตา หรือลักษณะใบหน้า วิธีนี้มีความปลอดภัยมากกว่า แต่มีค่าใช้จ่ายค่อนข้างสูง (Whitman & Mattord, 2021) การรับรองความถูกต้องแบบหลายปัจจัยรวมวิธีการรับรองความถูกต้องอย่างน้อยสองวิธี เช่น รหัสผ่านและรหัสยืนยันทาง SMS ซึ่งสามารถปรับปรุงการรักษาความปลอดภัยของระบบได้อย่างมีประสิทธิภาพ และป้องกันความเสี่ยงที่เกิดจากความล้มเหลวของวิธีการรับรองความถูกต้องวิธีเดียว (Solms & Niekerk, 2020)

ไฟร์วอลล์เป็นแนวป้องกันแรกในการปกป้องความปลอดภัยของขอบเขตเครือข่าย บทบาทของพวกเขาคือการตรวจสอบและควบคุมการรับส่งข้อมูลที่เข้าและออกจากเครือข่าย ไฟร์วอลล์สามารถกรองแพ็กเก็ตข้อมูลเครือข่ายตามกฎที่กำหนดไว้ล่วงหน้าเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและการโจมตีเครือข่ายที่อาจเกิดขึ้น (Kim & Solomon, 2019) โดยปกติไฟร์วอลล์จะใช้เพื่อแยกเครือข่ายภายในออกจากเครือข่ายภายนอกเพื่อให้แน่ใจว่าเครือข่ายภายในได้รับการปกป้องจากภัยคุกคามภายนอก ระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS) เป็นเครื่องมือสำคัญในการรับรองความปลอดภัยของเครือข่ายเพิ่มเติม หน้าที่หลักของ IDS คือการตรวจสอบการรับส่งข้อมูลเครือข่ายและกิจกรรมของระบบ ตรวจสอบว่ามีพฤติกรรมที่น่าสงสัยหรือรูปแบบการโจมตีที่ทราบหรือไม่ และออกการแจ้งเตือนไปยังผู้ดูแลระบบ (Stallings & Brown, 2020) ในทางตรงกันข้าม IPS ไม่เพียงตรวจจับการโจมตีเท่านั้น แต่ยังใช้มาตรการเชิงรุกเพื่อป้องกันการโจมตี เช่น การปล่อยแพ็กเก็ตที่เป็นอันตรายหรือการบล็อกการเชื่อมต่อของผู้โจมตี (Peltier, 2019)

การรวมกันของ IDS และ IPS สามารถปรับปรุงความปลอดภัยโดยรวมของระบบได้อย่างมีประสิทธิภาพ IDS มีหน้าที่ในการตรวจจับและออกการแจ้งเตือน ในขณะที่ IPS สามารถตอบสนองได้ทันทีและดำเนินการเพื่อป้องกันการขยายการโจมตีเพิ่มเติม (Ahmad et al., 2023) นอกจากนี้ ไฟร์วอลล์สมัยใหม่มักจะรวมเข้ากับ IDS และ IPS เพื่อสร้างระบบการจัดการภัยคุกคามแบบครบวงจร (UTM) เพื่อให้การป้องกันที่ครอบคลุมมากขึ้น

สรุปการประยุกต์ใช้เทคโนโลยีความปลอดภัยของข้อมูลอย่างครอบคลุม เช่น เทคโนโลยีการเข้ารหัส กลไกการตรวจสอบสิทธิ์ ไฟร์วอลล์ IDS และ IPS สามารถตอบสนองภัยคุกคามด้านความปลอดภัยที่เปลี่ยนแปลงตลอดเวลาได้อย่างมีประสิทธิภาพ เทคโนโลยีแต่ละอย่างมีการมุ่งเน้นในตัวเอง ซึ่งสามารถปกป้องความลับและความสมบูรณ์ของข้อมูล ทำให้มั่นใจได้ว่าเฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงทรัพยากรระบบ และใช้มาตรการตอบสนองทันเวลาเมื่อตรวจพบภัยคุกคาม (Whitman & Mattord, 2021) ด้วยการปรับใช้ที่เหมาะสมและการจัดการที่มีประสิทธิภาพของเทคโนโลยีเหล่านี้ องค์การต่าง ๆ จะสามารถสร้างแนวป้องกันการรักษาความปลอดภัยของข้อมูลที่แข็งแกร่งเพื่อปกป้องทรัพย์สินข้อมูลจากการโจมตีและภัยคุกคามต่างๆ

2.4.8 ความเสี่ยงและภัยคุกคามด้านความปลอดภัยของข้อมูล

ความเสี่ยงและภัยคุกคามด้านความปลอดภัยของข้อมูลถือเป็นความท้าทายที่ระบบสารสนเทศต้องเผชิญซึ่งไม่สามารถมองข้ามได้ ด้วยการพัฒนาเทคโนโลยีสารสนเทศ ภัยคุกคามและการโจมตีรูปแบบต่างๆ ยังคงเกิดขึ้น ซึ่งส่งผลกระทบร้ายแรงต่อการรักษาความลับ ความสมบูรณ์ และความพร้อมของข้อมูล เพื่อต่อสู้กับภัยคุกคามเหล่านี้อย่างมีประสิทธิภาพ การจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลจึงมีความสำคัญ บทความนี้จะแนะนำภัยคุกคามด้านความปลอดภัยของข้อมูลทั่วไป วิธีการและขั้นตอนการจัดการความเสี่ยง (Stallings & Brown, 2020)

ภัยคุกคามทั่วไปต่อความปลอดภัยของข้อมูล ได้แก่ มัลแวร์ การโจมตีทางไซเบอร์ และวิศวกรรมสังคม มัลแวร์หมายถึงโปรแกรมที่เป็นอันตรายซึ่งออกแบบมาเพื่อสร้างความเสียหายให้กับระบบคอมพิวเตอร์ ขโมยข้อมูลที่ละเอียดอ่อน หรือเข้าถึงระบบโดยไม่ได้รับอนุญาต รวมถึงไวรัส เวิร์ม ม้าโทรจัน แรนซัมแวร์ ฯลฯ (Kim & Solomon, 2019) ไวรัสและเวิร์มจะจำลองตัวเองและแพร่กระจายไปยังระบบอื่นๆ ในขณะที่ม้าโทรจันมักจะซ่อนอยู่ในซอฟต์แวร์ที่ถูกต้องตามกฎหมายเพื่อรวบรวมข้อมูลผู้ใช้อย่างเงียบๆ หรือควบคุมการทำงานของระบบ ในช่วงไม่กี่ปีที่ผ่านมา ภัยคุกคามของแรนซัมแวร์มีความโดดเด่นเป็นพิเศษ โดยผู้โจมตีเข้ารหัสข้อมูลของเหยื่อและเรียกค่าไถ่เพื่อกู้คืนการเข้าถึง (Ahmad et al., 2023)

การโจมตีเครือข่ายประกอบด้วย การโจมตีแบบปฏิเสธการให้บริการ (DDoS) แบบกระจาย การโจมตีแบบแมนอินเดอะมิดเดิล (MITM) การโจมตีแบบฟิชชิง ฯลฯ โดยมีวัตถุประสงค์เพื่อรบกวนการสื่อสารเครือข่าย การขโมยข้อมูล หรือป้องกันการดำเนินงานตามปกติของบริการ (วิทแมนและแมตต์ฟอร์ด, 2021) การโจมตี DDoS ครอบครองทรัพยากรระบบเป้าหมายผ่านการร้องขอจำนวนมาก ทำให้ไม่สามารถให้บริการแก่ผู้ใช้ที่ถูกต้องตามกฎหมายได้ การโจมตีแบบแทรกกลางจะขโมยข้อมูลที่ละเอียดอ่อนโดยการสกัดกั้นและแก้ไขข้อมูลการสื่อสาร ในขณะที่การโจมตีแบบฟิชชิงทำให้ผู้ใช้เปิดเผยข้อมูลส่วนบุคคลผ่านอีเมลหรือเว็บไซต์ที่ปลอมตัวเป็นเอนทิตีที่เชื่อถือได้ (Kumar & Dhillon, 2020)

วิศวกรรมสังคมเป็นวิธีการโจมตีที่ใช้การจัดการทางจิตวิทยาเพื่อฉ้อโกงข้อมูลส่วนบุคคล โดยมักจะใช้ประโยชน์จากความไว้วางใจและอารมณ์ของมนุษย์เพื่อให้ได้ข้อมูลที่ละเอียดอ่อน (Peltier, 2019) การโจมตีทางวิศวกรรมสังคมทั่วไป ได้แก่ การฉ้อโกงทางโทรศัพท์ ฟิชชิง การแอบอ้างตัวตน ฯลฯ ผู้โจมตี

อาจสร้างทำเป็นเจ้าหน้าที่สนับสนุนทางเทคนิคหรือพนักงานภายในบริษัทเพื่อฉ้อโกงข้อมูลรับรองการเข้าสู่ระบบของผู้ใช้หรือข้อมูลที่ละเอียดอ่อนอื่น ๆ วิศวกรรมสังคมมีอัตราความสำเร็จที่สูงกว่าเนื่องจากต้องอาศัยช่องโหว่ของมนุษย์มากกว่าช่องโหว่ทางเทคโนโลยี (Solms & Niekerk, 2020)

วัตถุประสงค์ของการบริหารความเสี่ยงด้านความปลอดภัยของข้อมูลคือเพื่อระบุ ประเมิน และตอบสนองต่อภัยคุกคามด้านความปลอดภัยต่างๆ ที่อาจมีอยู่ในระบบข้อมูล ซึ่งจะช่วยลดผลกระทบของความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นกับองค์กร การบริหารความเสี่ยงมักประกอบด้วยขั้นตอนต่อไปนี ประการแรกคือการระบุความเสี่ยงซึ่งมีจุดมุ่งหมายเพื่อค้นหาแหล่งความเสี่ยงต่างๆ ที่อาจคุกคามความปลอดภัยของระบบข้อมูล (Ahmad et al., 2023) โดยทั่วไปกระบวนการนี้เกี่ยวข้องกับการระบุทรัพย์สินของระบบและการวิเคราะห์ภัยคุกคามและช่องโหว่ที่อาจเกิดขึ้น ตัวอย่างเช่น ผ่านรายการสินทรัพย์และการประเมินความปลอดภัย องค์กรสามารถระบุได้ว่าสินทรัพย์ใดมีแนวโน้มที่จะถูกโจมตีมากที่สุดและภัยคุกคามเฉพาะที่สินทรัพย์เหล่านั้นเผชิญ

ถัดไปคือการประเมินความเสี่ยง ซึ่งเป็นการวิเคราะห์ความเสี่ยงที่ระบุเพื่อพิจารณาผลกระทบที่อาจเกิดขึ้นต่อองค์กร (Whitman & Mattord, 2021) โดยทั่วไปกระบวนการประเมินจะเกี่ยวข้องกับการประเมินความเสี่ยงในเชิงคุณภาพและเชิงปริมาณเพื่อกำหนดความรุนแรงและความเป็นไปได้ ผลลัพธ์ของการประเมินความเสี่ยงมักจะใช้เพื่อช่วยให้องค์กรพิจารณาว่าภัยคุกคามใดที่ต้องจัดลำดับความสำคัญ เช่น โดยใช้เมทริกซ์ความเสี่ยงเพื่อประเมินความรุนแรงและความน่าจะเป็นของการเกิดภัยคุกคามต่างๆ เพื่อพิจารณาว่าความเสี่ยงใดที่ต้องดำเนินการทันที (Stallings & Brown, 2020) .

ขั้นตอนที่สามคือการตอบสนองความเสี่ยง ซึ่งเป็นกระบวนการดำเนินการมาตรการเพื่อลดความเสี่ยงซึ่งโดยปกติจะรวมถึงการหลีกเลี่ยงความเสี่ยง การลดความเสี่ยง การแบ่งปันความเสี่ยง และการยอมรับความเสี่ยง (Kumar & Dhillon, 2020) วิธีทั่วไปในการลดความเสี่ยง ได้แก่ การใช้การควบคุมทางเทคนิค เช่น การเข้ารหัส การควบคุมการเข้าถึง ไฟร์วอลล์ ฯลฯ เพื่อลดความเสี่ยงหรือผลกระทบของความเสี่ยงสำหรับความเสี่ยงที่หลีกเลี่ยงไม่ได้ องค์กรสามารถแบ่งปันความเสี่ยงโดยการซื้อประกันภัย หรือเลือกที่จะยอมรับความเสี่ยงเมื่อผลกระทบจากความเสี่ยงมีน้อย

สุดท้ายมีการติดตามและทบทวนความเสี่ยง การจัดการความเสี่ยงเป็นกระบวนการต่อเนื่องที่ต้องมีการติดตามและทบทวนความเสี่ยงที่มีอยู่ตลอดจนภัยคุกคามที่เกิดขึ้นใหม่อย่างต่อเนื่อง (Peltier, 2019) ด้วยการทบทวนนโยบายและการควบคุมด้านความปลอดภัยอย่างสม่ำเสมอ องค์กรสามารถมั่นใจได้ว่าโปรแกรมการจัดการความเสี่ยงของตนยังคงมีประสิทธิภาพและปรับเปลี่ยนตามสถานการณ์ที่เปลี่ยนแปลง ตัวอย่างเช่น ภัยคุกคามทางไซเบอร์ใหม่ๆ หรือการเปลี่ยนแปลงกระบวนการภายในอาจต้องมีการประเมินและปรับปรุงกลยุทธ์การบริหารความเสี่ยงที่มีอยู่ (Solms & Niekerk, 2020)

การจัดการความเสี่ยงด้านความปลอดภัยของข้อมูลและการป้องกันภัยคุกคามเป็นส่วนสำคัญในการปกป้องระบบข้อมูลและข้อมูล ภัยคุกคาม เช่น มัลแวร์ การโจมตีทางไซเบอร์ และวิศวกรรมสังคมก่อให้เกิดความเสี่ยงที่สำคัญต่อความปลอดภัยของข้อมูล และด้วยแนวทางการจัดการความเสี่ยงที่เป็นระบบ องค์กรต่างๆ จึงสามารถระบุและตอบสนองต่อภัยคุกคามเหล่านี้ได้อย่างมีประสิทธิภาพ ด้วยการ

ระบุความเสี่ยง การประเมิน การตอบสนอง และการติดตามอย่างต่อเนื่อง องค์กรต่างๆ สามารถสร้างระบบป้องกันความปลอดภัยของข้อมูลแบบไดนามิกเพื่อปกป้องทรัพย์สินข้อมูลของตนได้ดีขึ้นในสภาพแวดล้อมภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว (Whitman & Mattord, 2021)

2.4.9 แนวทางปฏิบัติและการประยุกต์ใช้ความปลอดภัยของข้อมูล

การปฏิบัติและการประยุกต์ใช้ความปลอดภัยของข้อมูลถือเป็นสิ่งสำคัญในสังคมยุคใหม่ โดยเฉพาะอย่างยิ่งในระดับองค์กรและส่วนบุคคล ธุรกิจปกป้องข้อมูลที่ละเอียดอ่อนโดยการใช้นโยบายการรักษาความปลอดภัยของข้อมูลและการควบคุมการเข้าถึง ในขณะที่บุคคลจำเป็นต้องใช้นโยบายการป้องกันที่เหมาะสมเพื่อรักษาข้อมูลของตนเองให้ปลอดภัย (Stallings & Brown, 2020)

ในองค์กร แนวปฏิบัติด้านความปลอดภัยของข้อมูลมุ่งเน้นไปที่สองด้านเป็นหลัก: ความปลอดภัยของข้อมูลองค์กรและการควบคุมการเข้าถึง หัวใจสำคัญของการรักษาความปลอดภัยของข้อมูลองค์กรคือการปกป้องข้อมูลทางธุรกิจที่ละเอียดอ่อน ข้อมูลลูกค้า และทรัพย์สินทางปัญญาจากการเข้าถึงโดยไม่ได้รับอนุญาตและการโจมตีที่อาจเกิดขึ้น ด้วยเหตุนี้ องค์กรต่างๆ มักจะใช้กลยุทธ์การปกป้องข้อมูลแบบหลายชั้น เช่น การเข้ารหัส การสำรองข้อมูล และการแบ่งส่วนข้อมูล (Kim & Solomon, 2019) การเข้ารหัสข้อมูลเป็นวิธีการสำคัญในการรับรองความลับและความสมบูรณ์ของข้อมูลที่ละเอียดอ่อนในระหว่างการส่งและจัดเก็บข้อมูล ในขณะที่การสำรองข้อมูลสามารถป้องกันข้อมูลสูญหายเนื่องจากความล้มเหลวของฮาร์ดแวร์หรือการโจมตีของแรนซัมแวร์ (Whitman & Mattord, 2021) นอกจากนี้ เทคโนโลยีการแบ่งส่วนข้อมูลจะจัดเก็บข้อมูลไว้ในตำแหน่งที่แตกต่างกัน ซึ่งช่วยลดความเสี่ยงของการโจมตีแบบจุดเดียว

การควบคุมการเข้าถึงเป็นอีกมาตรการที่สำคัญในการรักษาความปลอดภัยข้อมูลขององค์กร วัตถุประสงค์คือเพื่อให้แน่ใจว่าเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงทรัพยากรระบบและข้อมูลที่ละเอียดอ่อนได้ นโยบายการควบคุมการเข้าถึงมักจะรวมถึงการควบคุมการเข้าถึงตามบทบาท (RBAC) การควบคุมการเข้าถึงตามดุลยพินิจ (DAC) และการควบคุมการเข้าถึงแบบบังคับ (MAC) (Peltier, 2019) RBAC ให้สิทธิ์การเข้าถึงในระดับต่างๆ ตามตำแหน่งและความรับผิดชอบของพนักงาน ซึ่งช่วยลดความเสี่ยงของการรั่วไหลของข้อมูลอันเนื่องมาจากข้อผิดพลาดของมนุษย์หรือพฤติกรรมที่เป็นอันตราย เพื่อเสริมความแข็งแกร่งให้กับการควบคุมการเข้าถึง องค์กรต่างๆ ยังนำการรับรองความถูกต้องแบบหลายปัจจัย (MFA) มาใช้ ซึ่งรวมปัจจัยการตรวจสอบหลายประการ (เช่น รหัสผ่าน ลายนิ้วมือ และรหัสยืนยันทาง SMS) เพื่อรับรองความถูกต้องของข้อมูลประจำตัวผู้ใช้ (Ahmad et al., 2023)

การกั้นช่องโหว่เป็นวิธีการที่ใช้กันทั่วไป โดยมีเป้าหมายเพื่อค้นหาช่องโหว่ด้านความปลอดภัยในระบบและซ่อมแซมทันที ซึ่งจะเป็นการปรับปรุงระดับความปลอดภัยโดยรวม นอกจากนี้ การฝึกอบรมการตระหนักรู้ด้านความปลอดภัยของข้อมูลสำหรับพนักงานไม่สามารถละเลยได้ เนื่องจากปัจจัยด้านมนุษย์เป็นหนึ่งในจุดอ่อนที่สุดของความปลอดภัยของข้อมูล (Kumar & Dhillon, 2020) ด้วยการฝึกอบรมด้านความปลอดภัยเป็นประจำ พนักงานสามารถเข้าใจถึงความสำคัญของความปลอดภัยของข้อมูลได้ดีขึ้น และเรียนรู้วิธีระบุและป้องกันภัยคุกคามทั่วไป เช่น การโจมตีทางวิศวกรรมสังคม

ในระดับบุคคล หลักปฏิบัติด้านความปลอดภัยของข้อมูลสะท้อนให้เห็นเป็นหลักในการปกป้องข้อมูลที่ละเอียดอ่อนส่วนบุคคล และหลีกเลี่ยงการรั่วไหลของข้อมูลและความเสี่ยงที่ไม่จำเป็น ชั้นแรกบุคคลจำเป็นต้องใช้รหัสผ่านที่รัดกุมและเปลี่ยนรหัสผ่านเป็นประจำ รหัสผ่านที่รัดกุมควรมีตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษเพื่อเพิ่มความยากในการถอดรหัส (Whitman & Mattord, 2021) นอกจากนี้ บุคคลทั่วไปยังสามารถใช้เครื่องมือการจัดการรหัสผ่านเพื่อสร้างและจัดการรหัสผ่านที่ซับซ้อน ซึ่งจะช่วยลดความเสี่ยงในการใช้รหัสผ่านซ้ำ

การตรวจสอบสิทธิ์แบบหลายปัจจัย (MFA) ยังเป็นหนึ่งในมาตรการที่มีประสิทธิภาพในการปกป้องความปลอดภัยของข้อมูลส่วนบุคคล เพิ่มความปลอดภัยของบัญชีโดยการรวมรหัสผ่านและวิธีการยืนยันอื่น ๆ (เช่น รหัสยืนยันโทรศัพท์มือถือหรือข้อมูลชีวภาพ) (Solms & Niekerk, 2020) . วิธีนี้สามารถป้องกันปัญหาการบุกรุกบัญชีที่เกิดจากการรั่วไหลของรหัสผ่านได้อย่างมีประสิทธิภาพ สำหรับบัญชีที่เกี่ยวข้องกับข้อมูลที่ละเอียดอ่อน (เช่น ธนาคารและโซเชียลมีเดีย) การเปิดใช้งาน MFA เป็นหนึ่งในแนวทางปฏิบัติที่ดีที่สุดในการรับรองความปลอดภัยของข้อมูล

บุคคลควรดูแลปกป้องข้อมูลส่วนตัวของตนเอง โดยเฉพาะอย่างยิ่งเมื่อใช้โซเชียลมีเดียและบริการออนไลน์ บริการออนไลน์จำนวนมากรวบรวมข้อมูลส่วนบุคคลของผู้ใช้ ดังนั้นบุคคลจึงต้องเข้าใจนโยบายความเป็นส่วนตัวส่วนตัวของข้อมูลของแพลตฟอร์มเหล่านี้ เพื่อลดการเปิดเผยข้อมูลที่ละเอียดอ่อนให้เหลือน้อยที่สุด (Kim & Solomon, 2019) นอกจากนี้ เมื่อเข้าถึงข้อมูลที่ละเอียดอ่อนบนเครือข่าย Wi-Fi สาธารณะ การใช้เครือข่ายส่วนตัวเสมือน (VPN) สามารถเข้ารหัสการส่งข้อมูลและป้องกันไม่ให้ผู้โจมตีดักจับและขโมยได้

นอกจากนี้ บุคคลทั่วไปควรระวังฟิชชิ่งและการโจมตีทางวิศวกรรมสังคมอื่นๆ ฟิชชิ่งมักจะเกี่ยวข้องกับการหลอกผู้ใช้ให้คลิกลิงก์ที่เป็นอันตรายหรือให้ข้อมูลที่ละเอียดอ่อนผ่านอีเมลหรือข้อความที่ปลอมตัวเป็นองค์กรที่ถูกกฎหมาย (Peltier, 2019) เพื่อป้องกันการโจมตีดังกล่าว บุคคลควรระมัดระวังตรวจสอบตัวตนของผู้ส่งอย่างรอบคอบ และไม่คลิกลิงก์ที่ไม่รู้จักหรือดาวน์โหลดไฟล์แนบโดยง่าย การติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัสเป็นประจำยังเป็นวิธีการป้องกันที่มีประสิทธิภาพ และสามารถช่วยตรวจจับและบล็อกการบุกรุกของมัลแวร์ได้

โดยสรุป แนวทางปฏิบัติและการประยุกต์ใช้ความปลอดภัยของข้อมูล ไม่ว่าจะเป็นในระดับองค์กรหรือระดับบุคคล มีหลายชั้น และต้องได้รับการดูแลและอัปเดตอย่างต่อเนื่อง ธุรกิจต่างๆ รักษาข้อมูลของตนให้ปลอดภัยโดยใช้มาตรการต่างๆ เช่น ความปลอดภัยของข้อมูลและการควบคุมการเข้าถึง ในขณะที่บุคคลต่างๆ ปกป้องข้อมูลของตนด้วยรหัสผ่านที่รัดกุม การตรวจสอบสิทธิ์แบบหลายปัจจัย และการใช้บริการออนไลน์อย่างระมัดระวัง ในยุคที่เทคโนโลยีสารสนเทศมีการพัฒนาอย่างรวดเร็วภัยคุกคามด้านความปลอดภัยของข้อมูลก็เปลี่ยนแปลงอยู่ตลอดเวลา ดังนั้นจึงจำเป็นอย่างยิ่งที่ต้องใช้มาตรการรักษาความปลอดภัยเชิงรุกและรักษาความตระหนักรู้ด้านความปลอดภัยของข้อมูล (Stallings & Brown, 2020)

2.5 แนวคิดทฤษฎีเกี่ยวกับความปลอดภัยของข้อมูลเครือข่าย

ทฤษฎีความปลอดภัยของข้อมูลเครือข่ายมุ่งเน้นไปที่วิธีการป้องกันเครือข่ายคอมพิวเตอร์และระบบข้อมูลจากการเข้าถึงที่ผิดกฎหมายการทำลายการปลอมแปลงหรือการรั่วไหลที่ไม่ได้รับอนุญาต ครอบคลุมหลายสาขารวมถึงการเข้ารหัสการตรวจสอบสิทธิ์การควบคุมการเข้าถึงการตรวจจับการบุกรุกและโปรโตคอลความปลอดภัยเป็นต้นภายใต้กรอบทฤษฎีนี้ความปลอดภัยไม่ใช่แค่การป้องกันการโจมตีจากภายนอกแต่ยังรวมถึงการป้องกันระบบจากภัยคุกคามภายในเช่นพนักงานที่เป็นอันตรายหรือซอฟต์แวร์ที่มีข้อบกพร่องการเข้ารหัสให้การเข้ารหัสและการตรวจสอบความสมบูรณ์ของข้อมูลปกป้องความเป็นส่วนตัวและความถูกต้องของข้อมูลเมื่อส่งและจัดเก็บการตรวจสอบสิทธิ์และการควบคุมการเข้าถึงเพื่อให้แน่ใจว่ามีเพียงผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงและแก้ไขทรัพยากรได้ระบบตรวจจับการบุกรุกจะตรวจสอบกิจกรรมเครือข่ายอย่างต่อเนื่องตรวจจับและตอบสนองต่อพฤติกรรมที่ผิดปกติ โปรโตคอลการรักษาความปลอดภัยเช่น SSL / TLS มีช่องทางที่ปลอดภัยสำหรับการโต้ตอบออนไลน์รับประกันความลับและความสมบูรณ์ของการส่งข้อมูลทฤษฎีความปลอดภัยของข้อมูลทางไซเบอร์ให้ชุดเครื่องมือที่ครอบคลุมและกลยุทธ์ที่จะช่วยป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่หลากหลายเพื่อให้มั่นใจว่าทรัพยากรข้อมูลมีความปลอดภัยและสมบูรณ์

2.5.1 แนวคิดด้านความปลอดภัยของข้อมูลไซเบอร์

ความปลอดภัยของข้อมูลเครือข่าย(เรียกว่าความปลอดภัยของข้อมูลเครือข่ายคอมพิวเตอร์)เป็นหลักความคิดที่ครอบคลุมซึ่งมุ่งเน้นไม่เพียงแต่การปกป้องข้อมูลที่เก็บไว้ในฮาร์ดแวร์คอมพิวเตอร์แต่ยังครอบคลุมความปลอดภัยของข้อมูลในขั้นตอนการส่ง (Jing Jiwu, 2022)เพื่อให้ถูกต้องยิ่งขึ้นแนวคิดนี้ถูกสร้างขึ้นร่วมกันโดยองค์ประกอบหลักสองประการคือความปลอดภัยของโหนดเครือข่ายและระดับการป้องกันของการเชื่อมโยงการสื่อสารส่งผลให้เกิดสภาพแวดล้อมเครือข่ายที่ครอบคลุมและป้องกันดังแสดงในรูปด้านล่าง



ดังนั้น Cyber Information Security จึงเข้าใจได้ว่าเป็นแบบจำลองการรักษาความปลอดภัยที่ครอบคลุมซึ่งรวมองค์ประกอบหลักสองอย่างคือความปลอดภัยในการสื่อสารและความปลอดภัยของโฮสต์ (HuangWei et al. 2020) ในการใช้งานจริงกลยุทธ์ความปลอดภัยทางไซเบอร์มักจะเน้นสองประการ: หนึ่งคือกลไกการป้องกันแบบคงที่ของระบบ สองคือกลยุทธ์ความปลอดภัยของส่วนประกอบต่างๆของระบบในกระบวนการปฏิสัมพันธ์แบบไดนามิก อย่างหลังมีความสำคัญเป็นพิเศษ

ในสภาพแวดล้อมเครือข่ายเป้าหมายที่อาจถูกโจมตีประกอบด้วยสามด้านหลัก: ฮาร์ดแวร์ ซอฟต์แวร์และข้อมูล (Ghahghah et al. 2021) ทั้งสามด้านนี้ไม่เพียงแต่เป็นเนื้อหาหลักของการรักษาความปลอดภัยของโฮสต์เท่านั้นแต่ยังแสดงถึงองค์ประกอบพื้นฐานของความปลอดภัยของโหนดเครือข่าย ดังนั้นจึงเป็นทิศทางที่กลยุทธ์การรักษาความปลอดภัยทางไซเบอร์ต้องพิจารณามากที่สุด

จากมุมมองที่แตกต่างกันความปลอดภัยของข้อมูลเครือข่ายสามารถแบ่งออกเป็นสองประเภทหลักของความปลอดภัยของผู้ให้บริการข้อมูลและความปลอดภัยของเนื้อหาข้อมูล ผู้ให้บริการข้อมูลส่วนใหญ่หมายถึงแพลตฟอร์มทางกายภาพสำหรับการจัดเก็บการประมวลผลและการส่งข้อมูล เช่น ระบบคอมพิวเตอร์สายเคเบิลใยแก้วนำแสงและคลื่นแม่เหล็กไฟฟ้า เป็นต้น ปัญหาด้านความปลอดภัยส่วนใหญ่เกี่ยวข้องกับความเสี่ยงของความเสียหายทางกายภาพการรั่วไหลของแม่เหล็กไฟฟ้าการตัดการสื่อสารและการดักฟังที่ผู้ให้บริการอาจได้รับ (Win Jinying & Jin Kai, 2022) ในขณะที่ความปลอดภัยของเนื้อหาข้อมูลมุ่งเน้นไปที่ความเสียหายการรั่วไหลและการสูญเสียข้อมูลที่สามารถได้รับในระหว่างการจัดเก็บการประมวลผลและการส่งผ่านซึ่งเกี่ยวข้องโดยตรงกับการรักษาความลับความสมบูรณ์และความพร้อมใช้งานของข้อมูล (Ho Daiju 2021)

เป้าหมายสูงสุดของการรักษาความปลอดภัยข้อมูลไซเบอร์โดยทั่วไปคือการรับประกันความลับ ความสมบูรณ์และความพร้อมของข้อมูล (Li Hui, 2021) วรรณกรรมวิจัยบางฉบับยังเพิ่มปัจจัยอื่นๆเช่น ความน่าเชื่อถือความถูกต้องการไม่สามารถปฏิเสธได้และการตรวจสอบได้การรักษาความลับช่วยให้มั่นใจได้ว่าข้อมูลจะไม่ถูกเข้าถึงโดยผู้ใช้หรือบุคคลที่ไม่ได้รับอนุญาตและการรับประกันความสมบูรณ์ของข้อมูลจะไม่ถูกแก้ไขหรือถูกทำลายโดยไม่ได้รับอนุญาตในระหว่างการส่งหรือจัดเก็บในขณะที่ความพร้อมใช้งานช่วยให้มั่นใจได้ว่าข้อมูลจะถูกเข้าถึงและใช้โดยผู้ใช้หรือระบบที่ได้รับอนุญาตอย่างถูกต้องตามกฎหมาย

สรุปความปลอดภัยของข้อมูลเครือข่ายเป็นชุดของกลยุทธ์และมาตรการรักษาความปลอดภัยที่ออกแบบมาอย่างเป็นระเบียบโดยมีวัตถุประสงค์เพื่อรักษาความลับความสมบูรณ์และความพร้อมใช้งานของข้อมูลในสภาพแวดล้อมเครือข่ายซึ่งรวมถึงการสร้างเชื่อมั่นว่าข้อมูลจะสามารถไปถึงจุดหมายปลายทางได้อย่างถูกต้องและถูกต้องหลังจากการส่งผ่านเครือข่ายในขณะเดียวกันก็มั่นใจว่ามีเพียงผู้ใช้หรือระบบที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลนี้ได้เพื่อให้บรรลุเป้าหมายนี้ส่วนประกอบเครือข่ายทั้งหมดจำเป็นต้องมีฟังก์ชันความปลอดภัยที่จำเป็นตามความต้องการ

2.5.2 ความปลอดภัยของข้อมูลเครือข่าย

2.5.2.1 ภัยคุกคามทางไซเบอร์

ในด้านการรักษาความปลอดภัยของข้อมูลทางไซเบอร์แหล่งภัยคุกคามหลักสามารถแบ่งออกเป็นการโจมตีที่เป็นอันตรายช่องโหว่ด้านความปลอดภัยข้อบกพร่องของซอฟต์แวร์และปัญหาโครงสร้าง (HoWenhai&Xinjiajia,2019) ประเภทของบุคคลที่เกี่ยวข้อง ได้แก่ผู้จัดการผู้ใช้และผู้มีอำนาจตัดสินใจภายในระบบเจ้าหน้าที่พัฒนาและบำรุงรักษาระบบผู้ตรวจสอบบัญชีผู้ตรวจสอบและนักข่าวที่มีบทบาทพิเศษแฮกเกอร์หรือกลุ่มโจมตีภายนอกคู่แข่งทางธุรกิจองค์กรก่อการร้ายทางไซเบอร์และองค์กรในระดับในแง่ของวิธีการโจมตีที่เฉพาะเจาะจงวิธีการทั่วไปได้แก่การโจมตีโดยปฏิเสธบริการ (DOS) การปฏิเสธธุรกรรมที่ไม่ได้รับการรับรอง การปลอมตัวตนของผู้ใช้ที่ถูกกฎหมาย การเปลี่ยนแปลงข้อมูลการเล่นข้อมูลการดักฟังเครือข่ายและการบุกรุกของไวรัส ฯลฯ (Dong Yi & Wang Anqi, 2021) ผู้โจมตีมักใช้วิธีการทางเทคนิค เช่น บัฟเฟอร์ล้น ที่อยู่ IP ปลอม และใช้ซอฟต์แวร์ "แบ็คดอร์" ในการโจมตี

สาเหตุพื้นฐานของภัยคุกคามอาจเกิดจากพฤติกรรมโดยเจตนาของมนุษย์ความผิดพลาดในการดำเนินงานโดยไม่ได้ตั้งใจ หรือภัยพิบัติทางธรรมชาติ (เซียหลัวผิง 2021)โดยเฉพาะเครื่องมือโจมตีแฮกเกอร์มักจะใช้ประโยชน์จากสแกนเนอร์ (เช่น Nessus, Nmap ฯลฯ) sniffers เครือข่าย เช่น Sniffit, Sunsniff ฯลฯ รหัสผ่าน cracker เช่น John โทรจัน ระเบิดอีเมล เช่น Nimingxin, QuickFyre ฯลฯ และไวรัสคอมพิวเตอร์ เช่น หนอน เป็นต้น (ฉางเยียน, 2021) Network Sniffer ถือได้ว่าเป็นอุปกรณ์ดักฟังทางอิเล็กทรอนิกส์ที่ออกแบบมาเป็นพิเศษเพื่อจับข้อมูลที่ส่งบนเครือข่ายมักจะซ่อนอยู่ในคอมพิวเตอร์เป้าหมายอย่างเงียบ ๆ เพื่อให้ผู้โจมตีสามารถควบคุมคอมพิวเตอร์ได้จากระยะไกลอีเมลระเบิดทำให้กล่องจดหมายและทรัพยากรเครือข่ายหมดลงโดยการส่งสแปมจำนวนมากด้วยการวิเคราะห์หลายมิติและหลายระดับนี้จะสามารถทำความเข้าใจความซับซ้อนและความหลากหลายของภัยคุกคามทางไซเบอร์ได้อย่างครอบคลุมมากขึ้นและให้คำแนะนำที่แม่นยำยิ่งขึ้นสำหรับการป้องกันความปลอดภัยของข้อมูลทางไซเบอร์

2.5.2.2 กลไกและบริการรักษาความปลอดภัยข้อมูลที่มีอยู่

ในการจัดการความปลอดภัยของข้อมูลเครือข่ายกลไกการรักษาความปลอดภัยหลักและบริการรวมถึงการรับรองความถูกต้อง(Authentication)การรักษาความลับของข้อมูล (Confidentiality) ความสมบูรณ์ของข้อมูล (Integrity) การควบคุมการเข้าถึง (Access Control) และการไม่ปฏิเสธ (Nonrepudiation)กลไกความปลอดภัยเหล่านี้ถือเป็นโครงสร้างพื้นฐานสำหรับการใช้นโยบายความปลอดภัย (Dubojet et al. 2020)

กลไกการระบุตัวตนมีวัตถุประสงค์สองประการ : ประการแรกคือการยืนยันว่าตัวตนของผู้ส่งข้อมูลได้รับการรับรองตามกฎหมายเพื่อป้องกันการแอบอ้างชื่อหรือไม่ประการที่สองคือการรับประกันความถูกต้องและไม่ถูกเปลี่ยนแปลงซ้ำหรือล่าช้าของข้อมูลที่ส่งผ่าน ได้แก่ การบรรลุการรับรองความถูกต้องของข้อมูลและตัวตนสองครั้ง (Wang Jingjing 2021)

กลไกการรักษาความลับของข้อมูลถูกออกแบบมาเพื่อป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงหรือได้รับข้อมูลการแปลงข้อมูลดิบ(ข้อความที่ชัดเจน)เป็นข้อมูลที่เข้ารหัส(ข้อความลับ)ผ่านอัลกอริทึม

ทางคณิตศาสตร์ที่อนุญาตให้เฉพาะผู้ใช้ที่มีคีย์ถอดรหัสเท่านั้นที่สามารถเรียกคืนข้อความลับให้เป็นข้อมูลที่มีอยู่ (ปิ่นสิทธิ์, 2023)

กลไกการควบคุมการเข้าถึงคือ การกำหนดระดับการอนุญาตที่แตกต่างกันเพื่อกำหนดว่าผู้ใช้ที่มีตัวตนแตกต่างกันสามารถกระทำการเฉพาะใดได้บ้าง เช่น อ่าน เขียน ดำเนินการ ฯลฯ กลไกนี้สามารถจัดการการเข้าถึงของผู้ใช้ได้อย่างมีประสิทธิภาพและมั่นใจได้ว่าระบบสารสนเทศจะทำงานอย่างปลอดภัย (Gindchao, 2021)

กลไกทางเพศที่ไม่ปฏิเสธหรือกลไกการต่อต้านก็เพื่อให้แน่ใจว่าฝ่ายที่ทำธุรกรรมหรือการสื่อสารไม่สามารถปฏิเสธการกระทำหรือการทำธุรกรรมที่พวกเขากระทำได้ (หลีนา, 2021)

กลไกความปลอดภัยและบริการเหล่านี้ไม่เพียงแต่สอดคล้องกับความต้องการด้านความปลอดภัยที่เฉพาะเจาะจงเท่านั้นแต่ยังมักจะโต้ตอบและเสริมในกรอบความปลอดภัยที่ครอบคลุมซึ่งให้การรับประกันความปลอดภัยทางไซเบอร์หลายระดับและครอบคลุม

2.5.2.3 เครือข่ายความปลอดภัยของข้อมูล เทคโนโลยีหลัก

ในด้านของการรักษาความปลอดภัยของเครือข่ายข้อมูลกลไกการรักษาความปลอดภัยที่หลากหลายและบริการสามารถทำได้โดยวิธีการทางเทคนิคที่แตกต่างกันและวิธีการทางเทคนิคเหล่านี้อาจนำไปใช้กับกลยุทธ์ด้านความปลอดภัยที่หลากหลาย

โดยทั่วไปการรับรองความถูกต้องจะแบ่งออกเป็นสองประเภทหลัก:แบบจำลองความไว้วางใจจากบุคคลที่สามและแบบจำลองบนพื้นฐานของความไว้วางใจโดยตรงโซลูชันการรับรองความถูกต้องมีเป้าหมายหลักสามประการ:ปัจจัยความรู้ เช่น รหัสผ่าน ปัจจัยการเป็นเจ้าของ เช่น สมาร์ทการ์ดหรือ JavaCard และไบโอเมตริกซ์ เช่น การจดจำลายนิ้วมือหรือม่านตา เทคโนโลยีเฉพาะได้แก่การรับรองคีย์ลายเซ็นดิจิทัลตามฟังก์ชันแฮชและเทคโนโลยีไบโอเมตริกซ์ (Siong Tao, 2020)

การควบคุมการเข้าถึงครอบคลุมเทคโนโลยีที่หลากหลายเช่นการกรองแพ็คเกจบริการพร็อกซีเทคโนโลยีคอมพิวเตอร์เทคโนโลยีการตรวจสอบและเทคโนโลยีการเข้ารหัสลับในแง่ของความสมบูรณ์ของข้อมูล, วิธีการ เช่น การสำรองข้อมูล และการกู้คืนข้อมูลมักจะนำมาใช้ เป็นต้น

เทคโนโลยีการเข้ารหัสเป็นแกนหลักและพื้นฐานของการรักษาความปลอดภัยของข้อมูลสามารถแบ่งออกเป็นสองประเภทหลักของการเข้ารหัสซอฟต์แวร์และการเข้ารหัสฮาร์ดแวร์การเข้ารหัสคีย์แบบสมมาตร(เช่นDES,3DES,AES)และการเข้ารหัสคีย์แบบอสมมาตร เช่น RSA, DH, ECDH มีข้อดีและข้อเสียโดยเฉพาะอย่างยิ่งในสภาพแวดล้อมที่มีข้อมูลจำนวนมาก และโครงสร้างเครือข่ายที่ซับซ้อนการเข้ารหัสคีย์สมมาตรมักจะแพร่หลายมากขึ้นเพื่อปรับปรุงความปลอดภัยความยาวของคีย์ก็เพิ่มขึ้นเรื่อย ๆ ความยาวของคีย์ทั่วไปคือ 64 บิตและ 128 บิต (Wang Xiaolan, 2020)

การไม่ปฏิเสธมักกระทำผ่านเทคโนโลยี เช่น ลายเซ็นดิจิทัลนอกจากนี้ยังมีเทคโนโลยีและมาตรการรักษาความปลอดภัยอื่นอีกมากมายเช่นการประเมินผลการสแกนการวิเคราะห์ข้อมูลและการตรวจสอบการป้องกันไวรัสการจัดการความปลอดภัยและการตรวจจับความปลอดภัยทางไซเบอร์ (Chang Chunyan, 2021)

โปรแกรมความปลอดภัยทางไซเบอร์ที่ครอบคลุมโดยทั่วไปประกอบด้วยการรักษาความปลอดภัยทางกายภาพไฟร์วอลล์การประเมินความปลอดภัยของเครือข่ายและระบบการสแกนการจับและวิเคราะห์การไหลของข้อมูลการตรวจสอบความปลอดภัยแบบเรียลไทม์การสแกนช่องโหว่การตรวจจับและการตอบสนองต่อการบุกรุกและการป้องกันไวรัสและการเข้ารหัสข้อมูลความปลอดภัยโดยรวมของเครือข่ายจะเกิดขึ้นได้ก็ต่อเมื่อมีการใช้เทคโนโลยีและมาตรการที่หลากหลายเหล่านี้อย่างครอบคลุมและเหมาะสม

กลไกความปลอดภัยบริการและเทคโนโลยีเหล่านี้ไม่เพียงแต่สามารถตอบสนองต่อความต้องการด้านความปลอดภัยที่เฉพาะเจาะจงได้อย่างอิสระแต่ยังทำงานร่วมกันภายใต้กรอบการรักษาความปลอดภัยที่ครอบคลุมซึ่งให้การป้องกันหลายระดับและทุกด้าน

2.5.2.4 มาตรฐานความปลอดภัยหลักระดับและองค์กรเครือข่าย

กรอบทฤษฎีความมั่นคงทางไซเบอร์ในปัจจุบันยังไม่สุกงอมเต็มที่ทำให้เกิดปัญหาการขาดยุทธศาสตร์ความมั่นคงที่เป็นเอกภาพปัจจุบันทฤษฎีและมาตรฐานด้านความปลอดภัยที่สำคัญส่วนใหญ่รวมถึงแนวทางการจัดอันดับความปลอดภัยของเทคโนโลยีสารสนเทศของ CEC คู่มือเครือข่ายที่เชื่อถือได้ของ NCSC และ ISO7498-2 ของ ISO เป็นต้น (Jang Yuying, 2021)

ศูนย์ความปลอดภัยคอมพิวเตอร์แห่งชาติ (NCSC) ภายใต้กระทรวงกลาโหมสหรัฐฯ ได้พัฒนาชุดมาตรฐานความปลอดภัยทางไซเบอร์ที่เรียกว่า DoD 5200.28 STD หรือที่เรียกว่ามาตรฐานการประเมินระบบคอมพิวเตอร์ที่น่าเชื่อถือหรือ Orange Book มาตรฐานนี้แบ่งระดับความปลอดภัยทางไซเบอร์ตั้งแต่ระดับ D ถึงระดับ A1 ซึ่งแต่ละระดับสอดคล้องกับความปลอดภัยทางกายภาพที่แตกต่างกัน การรับรองผู้ใช้ความน่าเชื่อถือของระบบปฏิบัติการและความปลอดภัยของแอปพลิเคชัน ในแง่ของการเข้ารหัสข้อมูลสำนักงานมาตรฐานแห่งชาติของสหรัฐอเมริกาได้ออก "อัลกอริทึมมาตรฐานการเข้ารหัสข้อมูล (DES)" ในปี ค.ศ.1976 องค์การระหว่างประเทศเพื่อการมาตรฐาน (ISO) ยังได้จัดตั้งคณะกรรมการ SC27 ขึ้นในปี 1990 เพื่อรับผิดชอบในการพัฒนามาตรฐานความปลอดภัยของเทคโนโลยีสารสนเทศ นอกจากนี้ยังมีโปรโตคอลที่เกี่ยวข้องกับการเข้ารหัสที่หลากหลายเช่น PKCS, SSL, S-HTTP และอื่น ๆ

ในประเทศจีนส่วนใหญ่กำหนดมาตรฐานแห่งชาติที่สอดคล้องกันตามมาตรฐานสากลตัวอย่างเช่น GB178951999" แนวทางการแบ่งระดับการป้องกันความปลอดภัยของระบบข้อมูลคอมพิวเตอร์"

ซึ่งกำหนดโดยกระทรวงความมั่นคงสาธารณะ ซึ่งแบ่งความปลอดภัยของระบบข้อมูลออกเป็นห้าระดับและให้ตัวชี้วัดความปลอดภัยหลายระดับสำหรับระดับที่แตกต่างกัน (Chen wu et al. 2021) นอกจากนี้ยังมีองค์กรและมาตรฐานหลายแห่งทั่วโลกที่มีส่วนร่วมในการทำงานด้านความปลอดภัยของข้อมูลรวมถึงคณะกรรมการที่ปรึกษาด้านโทรเลขและโทรศัพท์ระหว่างประเทศ (CCITT) สมาคมวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (IEEE) และอื่น ๆ (Gong Jianhu, 2022)

โดยสรุปแล้วแม้ว่าประเทศต่าง ๆ และหลายองค์กรจะมีผลงานที่หลากหลายเกี่ยวกับมาตรฐานและโปรโตคอลด้านความปลอดภัยทางไซเบอร์ แต่โดยรวมแล้วยังขาดระบบทฤษฎีความปลอดภัยทางไซเบอร์ที่เป็นเอกภาพและสมบูรณ์แบบ ทั้งยังหมายถึงความจำเป็นในการบูรณาการเทคโนโลยีและมาตรการ

รักษาความปลอดภัยต่าง ๆ ในการสร้างเครือข่ายสารสนเทศเพื่อให้เกิดการป้องกันความปลอดภัยทางไซเบอร์อย่างครอบคลุม

ทฤษฎีความปลอดภัยของข้อมูลเครือข่ายศึกษาวิธีการป้องกันเครือข่ายและระบบข้อมูลจากการเข้าถึงที่ผิดกฎหมายและการทำลาย เช่น การเข้ารหัส, การตรวจสอบสิทธิ์ และการควบคุมการเข้าถึง เมื่อนำไปใช้กับการศึกษา เรื่องการจัดการความปลอดภัยของข้อมูลที่เผยแพร่โดยแพลตฟอร์มออนไลน์ Douyin จึงหมายถึงการรับประกันความเป็นส่วนตัวของข้อมูลผู้ใช้ ความถูกต้องและความสมบูรณ์ของเนื้อหาและการส่งข้อมูลอย่างปลอดภัยโดยเฉพาะอย่างยิ่ง Douyin อาจใช้การเข้ารหัสเพื่อเข้ารหัสข้อมูลผู้ใช้ ใช้กลไกการตรวจสอบความถูกต้องเพื่อให้แน่ใจว่ามีเพียงผู้ใช้ที่ถูกต้องตามกฎหมายเท่านั้นที่สามารถเข้าถึงบัญชีของตนได้และผ่านโปรโตคอลความปลอดภัยเพื่อปกป้องการถ่ายโอนข้อมูลเมื่อผู้ใช้อัปโหลดหรือดาวน์โหลดเนื้อหา ในขณะที่การตรวจสอบกิจกรรมที่ผิดปกติหรือเป็นอันตรายใด ๆ เพื่อรักษาความน่าเชื่อถือของแพลตฟอร์มและความไว้วางใจของผู้ใช้

2.6 แนวคิดทฤษฎีเกี่ยวกับสื่อใหม่

ทฤษฎีสื่อใหม่ได้สำรวจว่าเทคโนโลยีดิจิทัลและอินเทอร์เน็ตมีอิทธิพลต่อการผลิตและเผยแพร่วัฒนธรรมสังคมและศิลปะอย่างไร หัวใจสำคัญของความห่วงใยคือทำอย่างไรจึงจะเข้าใจและตีความลักษณะเฉพาะของสื่อใหม่ เช่น ปฏิสัมพันธ์ดิจิทัลไฮเบอร์ไลเซชันและเสมือนจริง สื่อใหม่เป็นมากกว่าสื่อเก่าในเวอร์ชันดิจิทัลแต่เป็นการนำเสนอวิธีการใหม่ในการสร้างสรรค์เผยแพร่และรับเนื้อหาตัวอย่าง เช่น การมีปฏิสัมพันธ์ช่วยให้ผู้ใช้มีส่วนร่วมในการสร้างสรรค์เนื้อหาไม่ใช่แค่ผู้บริโภคเท่านั้น เครือข่ายหมายความว่าข้อมูลสามารถแพร่กระจายได้ทันทีและทั่วโลกความเสมือนได้ท้าทายคำจำกัดความดั้งเดิมของความเป็นจริงและนิยามของทฤษฎีสื่อใหม่ยังศึกษาว่าเทคโนโลยีเหล่านี้มีอิทธิพลต่ออัตลักษณ์ของปัจเจกบุคคลโครงสร้างทางสังคมและความสัมพันธ์ทางอำนาจอย่างไรมันถูกออกแบบมาเพื่อเจาะลึกว่าการเปลี่ยนแปลงเหล่านี้สามารถปรับเปลี่ยนชีวิตประจำวันวิธีการสื่อสารและปฏิสัมพันธ์ทางสังคมของมนุษย์ได้อย่างไรในขณะเดียวกันก็คิดอย่างวิพากษ์วิจารณ์ถึงความเสี่ยงและความท้าทายที่อาจเกิดขึ้นจากเทคโนโลยีเหล่านี้ กล่าวโดยสรุป ทฤษฎีสื่อใหม่(New Media Theory) ได้ให้กรอบแนวคิดที่จะช่วยให้เข้าใจและรับมือกับความซับซ้อนและสภาพแวดล้อมของสื่อที่เปลี่ยนแปลงไปในยุคดิจิทัล

2.6.1 แนวคิดของสื่อใหม่

สื่อใหม่เป็นเทคโนโลยีการสื่อสารขั้นสูงไม่เพียงแต่ส่งเสริมการสื่อสารระหว่างผู้ใช้นั้น แต่ยังช่วยเพิ่มปฏิสัมพันธ์แบบไดนามิกระหว่างผู้ใช้และเนื้อหา (Weilu & Ding Fangzhou, 2013) สิ่งนี้ถือเป็นการเปลี่ยนแปลงขั้นพื้นฐานในวิธีการเผยแพร่ข้อมูล และความสำคัญของสื่อใหม่คือความสามารถในการขยายข้อจำกัดของสื่อแบบดั้งเดิมและให้แพลตฟอร์มที่มีประสิทธิภาพและครอบคลุมมากขึ้นสำหรับการแลกเปลี่ยนข้อมูลระหว่างบุคคลและส่วนรวม

ในช่วงกลางทศวรรษ 1990 แนวคิดของสื่อใหม่ค่อย ๆ เข้าสู่สายตาของสาธารณชนในฐานะกลยุทธการส่งเสริมธุรกิจโดยมีจุดประสงค์หลักเพื่อโปรโมตผลิตภัณฑ์ CD-ROM แบบโต้ตอบที่เกิดขึ้นใหม่ในเวลานั้น ซึ่งไม่เพียงแต่ใช้เพื่อความบันเทิงแต่ยังรวมถึงการศึกษา (JiaZhimei2012) ในช่วงเวลานั้น CDROM เป็นผู้ให้บริการที่ปฏิวัติวงการสื่อสารเนื่องจากความสามารถในการรวมข้อมูลต่าง ๆ เช่น วิดีโอ เสียงและข้อความ แต่ในปัจจุบันสิ่งเหล่านี้ถูกแทนที่ด้วยทรัพยากรที่สะดวกและหลากหลายมากขึ้นบนอินเทอร์เน็ต เทคโนโลยีสื่อใหม่ของ Web2.0 ครอบคลุมเครื่องมือสื่อสารที่เกี่ยวข้องกับเครือข่ายที่หลากหลายซึ่งรวมถึงบล็อกวิกิพีเดียเครือข่ายสังคมออนไลน์โลกเสมือนจริงและแพลตฟอร์มโซเชียลมีเดียที่หลากหลาย การเกิดขึ้นของแพลตฟอร์มเหล่านี้ไม่เพียงแต่ช่วยเสริมสร้างรูปแบบการนำเสนอข้อมูลเท่านั้นแต่ยังช่วยอำนวยความสะดวกในการสร้างเผยแพร่และแลกเปลี่ยนข้อมูลอย่างมากซึ่งนำไปสู่การขับเคลื่อนกระบวนการสารสนเทศทั่วโลก (Chai Wengou, 2015)

สื่อใหม่เป็นสื่อคอมพิวเตอร์ที่ใช้คอมพิวเตอร์และอินเทอร์เน็ตเป็นช่องทางหลักในการสื่อสาร สื่อใหม่มีปฏิสัมพันธ์ที่สูงขึ้นและขอบเขตการสื่อสารที่กว้างขึ้นเมื่อเทียบกับสื่อแบบดั้งเดิม ซึ่งส่วนใหญ่เป็นผลมาจากการพัฒนาอย่างรวดเร็วของเทคโนโลยีคอมพิวเตอร์ที่ทันสมัยและเทคโนโลยีเครือข่าย (DaisFu, 2012) ดังนั้นสื่อใหม่ไม่เพียงแต่เปลี่ยนวิธีที่เราเข้าถึงและประมวลผลข้อมูล แต่ยังได้นิยามใหม่ของสื่อเองในระดับหนึ่งสื่อไม่ได้ถูกแทนที่หรือซ้ำซ้อนกันในลักษณะที่ชัดเจนเป็นเส้นตรง แต่ในทางตรงกันข้ามกับมีปฏิสัมพันธ์และกลไกการตอบรับที่ซับซ้อนระหว่างสื่อเก่าและใหม่ ซึ่งเป็นผลมาจากความก้าวหน้าอย่างต่อเนื่องของเทคโนโลยีสารสนเทศและความหลากหลายของความต้องการของสังคมนั้นก็หมายความว่าสื่อใหม่ไม่ได้แทนที่สื่อดั้งเดิมอย่างง่าย ๆ แต่มีปฏิสัมพันธ์กับมันด้วยวิธีที่ซับซ้อนและหลากหลายมากขึ้นและผลักดันให้ปรับตัวและพัฒนาอย่างต่อเนื่อง (Feng Rui & Jinjing, 2007)

อย่างไรก็ตามต้องชัดเจนว่าไม่ใช่ทุกรายการวิทยุ โทรทัศน์ ภาพยนตร์ นิตยสารและหนังสือ จะเรียกว่าเป็นสื่อใหม่ได้เฉพาะเมื่อสื่อดั้งเดิมเหล่านี้รวมเข้ากับเทคโนโลยีใหม่ ๆ ที่สามารถสร้างดิจิทัลหรือมีลักษณะเชิงโต้ตอบได้สื่อเหล่านี้จึงจะถือว่าเป็นส่วนหนึ่งของสื่อใหม่นอกจากนี้ยังทำให้เกิดความท้าทายว่าจะนิยามและจัดหมวดหมู่สื่อใหม่อย่างไรให้ถูกต้อง รวมถึงจะประเมินความสัมพันธ์และผลกระทบที่เกิดขึ้นกับสื่อดั้งเดิมอย่างไร

สรุปแล้วสื่อใหม่ในฐานะเครื่องมือสื่อสารสมัยใหม่ที่รวมพลังคอมพิวเตอร์ที่สูงและการเชื่อมต่อที่กว้างขวางได้ส่งผลกระทบอย่างลึกซึ้งต่อวิธีการเข้าถึงการประมวลผลและการเผยแพร่ข้อมูลของเราไม่เพียงผลักดันให้สื่อดั้งเดิมพัฒนาไปในทิศทางที่มีปฏิสัมพันธ์และหลากหลายมากขึ้นแต่ยังส่งเสริมการไหลของข้อมูลและความรู้อย่างเสรีในระดับโลก

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

2.6.2 ประเภทของสื่อใหม่

ในสาขาการสื่อสาร สื่อการสื่อสารถูกกำหนดให้อยู่ระหว่างผู้ส่งและผู้รับเพื่อดำเนินการถ่ายทอดขยายและขยายสัญลักษณ์เฉพาะซึ่งส่วนใหญ่ประกอบด้วยองค์ประกอบหลักสามประการของวัตถุ สัญลักษณ์และข้อมูลทั้งสามพึ่งพาอาศัยกันและขาดสิ่งใดก็ไม่สามารถบรรลุการสื่อสารได้อย่างสมบูรณ์ใน

ความหมายกว้าง ๆ สื่อการสื่อสารใหม่เกี่ยวข้องกับเทคโนโลยีที่ใช้ดิจิทัลมีเดียเครือข่ายคอมพิวเตอร์ และการสื่อสารผ่านดาวเทียม รวมถึงเคเบิลทีวีดิจิทัลเครือข่ายทีวีวิทยุและโทรทัศน์ผ่านดาวเทียม สิ่งพิมพ์ทางอิเล็กทรอนิกส์และอินเทอร์เน็ต เป็นต้น ในความหมายที่แคบสื่อการสื่อสารใหม่หมายถึงสื่อที่ผุดขึ้นตามหลังสื่อแบบดั้งเดิม 3 แห่ง ได้แก่ หนังสือพิมพ์ วิทยุและโทรทัศน์ ซึ่งส่วนใหญ่ประกอบด้วยวิธีการสื่อสาร เช่น อินเทอร์เน็ต และเครือข่ายมือถือ เป็นต้น

ในโลกของสื่อใหม่สามารถแบ่งออกเป็น 4 ประเภทหลักตามเส้นทางการสื่อสาร

1) สื่อใหม่ที่ใช้อินเทอร์เน็ต

สื่อใหม่บนอินเทอร์เน็ต หมายถึง รูปแบบสื่อที่อาศัยเทคโนโลยีโปรโตคอลและโครงสร้างอินเทอร์เน็ตในการเผยแพร่ข้อมูลเป็นหลัก สื่อประเภทนี้รวมถึงแต่ไม่จำกัดเพียงบล็อก ซึ่งเป็นแพลตฟอร์มสำหรับบุคคลหรือกลุ่มบุคคลในการแสดงความคิดเห็นและแบ่งปันประสบการณ์ นิตยสารอิเล็กทรอนิกส์เป็นส่วนขยายแบบดิจิทัลของนิตยสารกระดาษแบบดั้งเดิม สามารถให้ผู้อ่านได้รับประสบการณ์การอ่านที่หลากหลายและโต้ตอบมากขึ้นวิดีโอออนไลน์ด้วยความสะดวกสบายและคุณสมบัติที่กำหนดเองได้สูง และได้ปรากฏตัวอย่างรวดเร็วในปีที่ผ่านมาเพื่อให้ผู้ใช้มีเนื้อหาประเภทต่าง ๆ กลุ่มและชุมชนเครือข่าย เป็นต้น เพื่อเป็นสถานที่แลกเปลี่ยนข้อมูลและความคิดเห็นเปิดโอกาสให้ผู้ใช้ได้มีปฏิสัมพันธ์และแลกเปลี่ยนกับผู้ใช้อื่นๆ อีกมากมาย

2) สื่อใหม่บนเครือข่ายการกระจายเสียงในระบบดิจิทัล

สื่อใหม่บนเครือข่ายวิทยุกระจายเสียงในระบบดิจิทัล โดยมุ่งเน้นว่าเทคโนโลยีดิจิทัลจะปรับปรุงและขยายการรับส่งสัญญาณวิทยุและโทรทัศน์แบบเดิมอย่างไร ทีวีดิจิทัลไม่เพียงแต่ให้ผู้ชมที่มีคุณภาพของภาพความละเอียดสูงขึ้นเท่านั้น แต่ยังแนะนำฟังก์ชันแบบโต้ตอบมากมายที่วีเคชั่นที่ใช้ความสามารถในการพกพาเพื่อให้ผู้ใช้สามารถรับชมรายการทีวีได้ทุกที่ ทำลายข้อจำกัดของพื้นที่

3) สื่อใหม่บนเครือข่ายไร้สาย

ด้วยการพัฒนาอย่างรวดเร็วของเทคโนโลยีมือถือสื่อใหม่ที่ใช้เครือข่ายไร้สายก็เพิ่มขึ้นอย่างรวดเร็วเช่นกันตัวอย่างเช่นทีวีบนมือถือและวิดีโอบนมือถือช่วยให้ผู้ใช้สามารถรับชมเนื้อหาในสถานะเคลื่อนที่ได้หนังสือพิมพ์โทรศัพท์มือถือให้วิธีการรับข้อมูลข่าวที่ทันเวลาและสะดวกแก่ผู้ใช้ส่วน SMS/MMS บนมือถือเป็นวิธีการส่งข้อความโต้ตอบแบบทันทีที่ใช้กันทั่วไปในชีวิตประจำวัน

4) สื่อใหม่ที่ผสานเครือข่ายเข้าด้วยกัน

Fusion Network รวมเทคโนโลยีเครือข่ายที่หลากหลายเพื่อให้บริการที่หลากหลาย ตัวอย่างเช่นบริการกระจายเสียงโทรทัศน์ (IPTV) บนพื้นฐานของโปรโตคอล IP ซึ่งไม่เพียงแต่เปลี่ยนนิสัยการรับชมโทรทัศน์แบบดั้งเดิมแต่ยังให้ผู้ใช้ทางเลือกที่สมบูรณ์มากขึ้น และเนื้อหาส่วนบุคคล ที่วีอาคารซึ่งมักจะติดตั้งในคอนโดมิเนียมหรืออาคารสำนักงานเพื่อให้บริการข้อมูลที่สะดวกสำหรับผู้อยู่อาศัยหรือพนักงาน ในด้านการสื่อสารร่วมสมัยสื่อใหม่ สามารถจำแนกตามลักษณะของสื่อการสื่อสาร ได้ดังนี้

1) เว็บสื่อใหม่ สื่อใหม่ทางอินเทอร์เน็ตส่วนใหญ่หมายถึงแพลตฟอร์มและวิธีการเผยแพร่ข้อมูลผ่านอินเทอร์เน็ตตัวอย่างเช่น พอร์ทัลไซต์ซึ่งเป็นทางเข้าข้อมูลหลักสำหรับชาวเน็ตรวบรวมเนื้อหา

ข่าวบริการและความบันเทิงมากมาย เครื่องมือค้นหาช่วยให้ผู้ใช้ค้นหาข้อมูลที่ต้องการได้อย่างมีประสิทธิภาพ ชุมชนเสมือนให้พื้นที่แก่ชาวเน็ตในการสื่อสารและแบ่งปัน อีเมลการส่งข้อความโต้ตอบแบบทันทีและห่วงโซ่การสนทนาเป็นวิธีหลักในการสื่อสารประจำวัน บล็อกพอดคาสต์ Weibo และ Viscer ทอนให้เห็นถึงพลังของการสร้างเนื้อหาส่วนบุคคลในระบบออนไลน์ แอนิเมชันและเกมนำเสนอวิธีการบันเทิงแบบดิจิทัลในนิตยสารออนไลน์ วิทย์และโทรทัศน์เป็นส่วนขยายดิจิทัลของสื่อดั้งเดิม ในขณะที่นักเก้ตส์ อินน์เกอร์ เปลี่ยนแขกและวิกเกอร์/วอล์คเกอร์ ฯลฯ แสดงถึงวิธีการมีส่วนร่วมและการทำงานร่วมกันที่เกิดขึ้นใหม่

2) สื่อโทรทัศน์รูปแบบใหม่ สื่อโทรทัศน์รูปแบบใหม่เน้นผลผลิตจากการผสมผสานเทคโนโลยีทีวีแบบดั้งเดิมเข้ากับเทคโนโลยีดิจิทัลสมัยใหม่ในจำนวนนี้ทีวีดิจิทัลทำให้ผู้ชมมีคุณภาพภาพที่สูงขึ้นและมีทางเลือกมากขึ้น IPTV เป็นบริการทีวีบนพื้นฐานของโปรโตคอล IP ซึ่งรวมลักษณะของอินเทอร์เน็ตและโทรทัศน์ ทีวีมือถือ ได้หลายข้อจำกัดของพื้นที่ในการดูทีวีแบบดั้งเดิมเพื่อให้ผู้ใช้สามารถดูได้ทุกที่ทุกเวลา ทีวีอาคารเป็นบริการทีวีสำหรับสถานที่เฉพาะเช่น อาคารหรืออาคารสำนักงาน

3) สื่อใหม่สำหรับโทรศัพท์มือถือ ด้วยการพัฒนาอย่างรวดเร็วของเทคโนโลยีการสื่อสารเคลื่อนที่ โทรศัพท์มือถือได้กลายเป็นเครื่องมือสำคัญในการเผยแพร่ข้อมูลข้อความ โทรศัพท์มือถือและ MMS เป็นวิธีการสื่อสารเคลื่อนที่ที่เก่าแก่ที่สุดหนังสือพิมพ์และสิ่งพิมพ์บนมือถือช่วยให้ผู้ใช้สามารถรับข้อมูลได้ตลอดเวลา ทีวีและวิทยุโทรศัพท์มือถือให้เนื้อหาความบันเทิงบนมือถือแก่ผู้ใช้ เกมมือถือและแอปก็ได้รับความนิยมมากขึ้นเรื่อยๆจากผู้ใช้นำเสนอคุณสมบัติและบริการที่หลากหลายให้กับผู้ใช้เคลื่อนที่เครือข่ายมือถือเป็นแอปพลิเคชันพิเศษที่สร้างขึ้นโดยแพลตฟอร์มหลักสำหรับผู้ใช้โทรศัพท์มือถือ

4) สื่อใหม่อื่น ๆ นอกจากสื่อสื่อสารที่กล่าวมาข้างต้นแล้วยังมีสื่อใหม่ที่มีลักษณะพิเศษที่ไม่ใช่สื่อกระแสหลัก ตัวอย่างเช่น สื่ออุโมงค์เป็นบริการข้อมูลสำหรับผู้คนในอุโมงค์ สื่อใหม่ริมถนนส่วนใหญ่ตั้งอยู่สองข้างทางเพื่อให้ข้อมูลหรือโฆษณาแก่ผู้ที่ผ่านไปมาสอบถามข้อมูลสื่อช่วยให้ประชาชนสามารถสอบถามข้อมูลต่าง ๆ สื่อใหม่อื่น ๆ ที่ข้ามยุครวมถึงรูปแบบการสื่อสารบางอย่างที่ยังอยู่ในช่วงเริ่มต้นของการสำรวจหรือเริ่มต้นในสาขาการศึกษาการสื่อสารสมัยใหม่สำหรับความหลากหลายของรูปแบบการสื่อสารที่แตกต่างกัน

5) โตยีน (Douyin) Douyin เวอร์ชันสากลชื่อ Douyin เป็นแอปแชร์วิดีโอสั้นที่ได้รับความนิยมไปทั่วโลก คุณลักษณะที่ใหญ่ที่สุดของแพลตฟอร์มนี้คือความคิดสร้างสรรค์และการโต้ตอบสูงทำให้ผู้ใช้มีพื้นที่ในการแสดงความคิดสร้างสรรค์ และค้นพบเนื้อหาที่สร้างสรรค์ ผู้ใช้สามารถสร้างวิดีโอสั้น ๆ บน แพลตฟอร์มออนไลน์ Douyin ครอบคลุมหลายสาขา เช่น การเต้นรำ การศึกษาเคล็ดลับชีวิต ฯลฯ วิดีโอเหล่านี้มักจะมีเพลงฟิลเตอร์และเอฟเฟกต์ภาพต่าง ๆ เพื่อให้ผู้ใช้ทั่วไปสามารถสร้างเนื้อหาที่น่าสนใจได้อย่างง่ายดาย อัลกอริทึมของ Douyin สามารถแนะนำเนื้อหาวิดีโอส่วนบุคคลตามความสนใจและการโต้ตอบของผู้ใช้ ทำให้ประสบการณ์ของแต่ละคนไม่เหมือนใคร นอกจากนี้ฟีดเจอร์โซเชียลของแพลตฟอร์มออนไลน์โตยีน เช่น การกดไลค์ความคิดเห็นและการแชร์ยังช่วยส่งเสริมการเผยแพร่เนื้อหาและปฏิสัมพันธ์ระหว่างผู้ใช้ทำให้ Douyin เป็นหนึ่งในแพลตฟอร์มโซเชียลมีเดียที่มีอิทธิพลมากที่สุดในปัจจุบัน

2.6.3 พัฒนาการทางประวัติศาสตร์ของสื่อใหม่

ในปี 1950 วิทยาศาสตร์คอมพิวเตอร์ ได้ก่อตัวเป็นสาขาข้ามศาสตร์ที่เริ่มขยายตัวเพิ่มมากขึ้น แนวโน้มนี้เป็นจุดเริ่มต้นของการผสมผสานที่ซับซ้อนระหว่างเทคโนโลยีและการแสดงออกทางวัฒนธรรม แต่จนถึงทศวรรษ 1980 การข้ามนี้จึงถูกนำมาใช้กันอย่างแพร่หลายอย่างแท้จริง อัลันเคย์ (Alan Kay) ได้สร้างสรรค์นวัตกรรมในการคำนวณคอมพิวเตอร์ส่วนบุคคลให้กับคนทั่วไปความคิดริเริ่มนี้เปิดบทใหม่ของ การมีปฏิสัมพันธ์ระหว่างบุคคลกับคอมพิวเตอร์ในขณะเดียวกันก็ยุติการผูกขาดทรัพยากรคอมพิวเตอร์โดยองค์กรขนาดใหญ่การเปลี่ยนแปลงนี้ไม่เพียงแต่เปลี่ยนขอบเขตของการประยุกต์ใช้วิทยาการคอมพิวเตอร์ เท่านั้นแต่ยังส่งผลสำคัญต่อโครงสร้างทางสังคมและชีวิตประจำวันของผู้คนด้วย (Manovich, 2003)

อย่างไรก็ตามในช่วงปลายทศวรรษ 1980 และต้นทศวรรษ 1990 เราได้สังเกตเห็นความสัมพันธ์ คู่ขนานระหว่างการเปลี่ยนแปลงทางสังคมที่แตกต่างกับการออกแบบคอมพิวเตอร์ แม้ว่าทั้งสองไม่ได้ เกี่ยวข้องโดยตรงกับความสัมพันธ์เชิงสาเหตุแต่จากแนวคิดและภูมิหลังของเวลาสงครามเย็นและการ เพิ่มขึ้นของเวิลด์ไวด์เว็บ (WWW) ดูเหมือนจะแสดงให้เห็นถึงความสัมพันธ์ที่สะท้อนซึ่งกันและกันใน ช่วงเวลาทางประวัติศาสตร์ที่เฉพาะเจาะจงนี้ ความตึงเครียดทางการเมืองระหว่างประเทศและการพัฒนา อย่างรวดเร็วของเทคโนโลยีสารสนเทศดูเหมือนจะบ่งบอกถึงการเปลี่ยนแปลงพื้นฐานบางอย่างใน โครงสร้างประชาคมโลก

เกี่ยวกับการพัฒนาทฤษฎีของสื่อมีนักวิชาการและนักปรัชญาที่มีอิทธิพลอย่างลึกซึ้งหลายคนใน ระยะนี้โดยเฉพาะ มาร์แชล แมคลูฮาน ที่เขียนไว้ในหนังสือของเขา "เข้าใจสื่อ : ส่วนขยายของมนุษย์" เขา ได้เสนอมุมมองที่ว่า "สื่อคือข้อมูล" โดยเน้นว่าสื่อและเทคโนโลยีเองไม่ใช่แค่ "เนื้อหา" ของพวกเขามี ผลกระทบต่อประสบการณ์ของมนุษย์ที่มีต่อโลก และสังคมอย่างไม่อาจมองข้ามได้มุมมองนี้ทำให้เกิดการ ตรวจสอบใหม่ว่าสื่อกับวัฒนธรรมสังคม และแม้แต่วิทยาส่วนบุคคลมีปฏิสัมพันธ์และหล่อหลอมอย่างไร จนถึงทศวรรษที่ 80 ของศตวรรษที่ 20 สื่อยังคงพึ่งพารูปแบบการพิมพ์และการออกอากาศแบบอนาล็อก แบบดั้งเดิมเป็นหลัก เช่น โทรทัศน์และวิทยุแต่ในช่วง 25 ปีที่ผ่านมา สื่อใหม่ที่ใช้เทคโนโลยีดิจิทัลเป็น พื้นฐานอย่างอินเทอร์เน็ตและวิดีโอเกมได้พัฒนาอย่างรวดเร็ว ควรสังเกตว่าสิ่งเหล่านี้เป็นเพียงยอดภูเขาน้ำแข็งของสื่อใหม่เท่านั้น ดิจิทัลไม่เพียงแต่สร้างรูปแบบใหม่ของสื่อเท่านั้นแต่ยังช่วยปรับปรุงและอัปเดต สื่อเก่าแบบดั้งเดิมไว้ด้วย เช่น การเกิดขึ้นของทีวีดิจิทัลและสิ่งพิมพ์ออนไลน์และแม้แต่วิทยาการพิมพ์ แบบดั้งเดิม ต่างก็ได้รับการปรับปรุงเนื่องจากซอฟต์แวร์ประมวลผลภาพ เช่น Adobe Photoshop และ เครื่องมือเผยแพร่เดสก์ท็อป

นักวิชาการ (Stalder, 1999) เชื่อว่าเทคโนโลยีดิจิทัลที่เกิดขึ้นใหม่เป็นการเปลี่ยนแปลงที่มี ศักยภาพและพื้นฐานในการควบคุมข้อมูลข่าวสาร ประสบการณ์และทรัพยากร มุมมองนี้สะท้อนให้เห็นถึง ข้อมูลเชิงลึกทางสังคมวิทยาว่านวัตกรรมทางเทคโนโลยีส่งผลกระทบต่อโครงสร้างอำนาจและการไหลเวียนของข้อมูลอย่างไรในขณะ (รัสเซล, 1991) เสนอว่าแม้ว่าสื่อใหม่จะมีศักยภาพมหาศาลในระดับ เทคโนโลยีแต่พลังทางเศรษฐกิจและสังคมก็มักมีบทบาทถ่วงดุลหรือแม้กระทั่งข้อจำกัดจากมุมมองของ

Neuman เรากำลังเห็นการก่อตัวของเครือข่ายอินเทอร์เน็ตทั่วโลกที่จะสร้างความสับสนหรือคลุมเครือเส้นแบ่งระหว่างบุคคลและการสื่อสารมวลชนและการสื่อสารสาธารณะและเอกชน

ในบริบทของการพัฒนานี้สื่อใหม่ไม่เพียงแต่เปลี่ยนความหมายทางสังคมและวัฒนธรรมของระยะห่างทางภูมิศาสตร์แต่ยังเพิ่มปริมาณและความเร็วของการสื่อสารให้โอกาสมากขึ้นในการโต้ตอบและช่วยให้ความหลากหลายของรูปแบบการสื่อสารที่เป็นอิสระเดิมเริ่มทับซ้อนและเชื่อมต่อกัน ดังนั้น NARAYANA (2021) จึงเห็นว่าสื่อใหม่โดยเฉพาะอินเทอร์เน็ตนำเสนอพื้นที่สาธารณะเป็นเสมือนบ้านหลังสมัยใหม่ที่เป็นประชาธิปไตย ซึ่งพลเมืองสามารถเข้าถึงข้อมูลข่าวสารอย่างเต็มที่และการอภิปรายเชิงโครงสร้างทางสังคมที่เท่าเทียมกัน อย่างไรก็ตามการประเมินในแง่ดีนี้ยังได้รับการวิพากษ์วิจารณ์อยู่บ้าง Herman & McChesney มองว่าการเพิ่มขึ้นของสื่อใหม่ยังอาจทำให้อิทธิพลระดับโลกของบริษัทโทรคมนาคมข้ามชาติเพียงไม่กี่แห่งเพิ่มมากขึ้น ปรากฏการณ์นี้จำเป็นต้องมีการวิจัยทางสังคมศาสตร์และการวิเคราะห์เชิงวิพากษ์ต่อไป

โดยสรุปผลกระทบที่อาจเกิดขึ้นและเป็นจริงจากเทคโนโลยีสื่อใหม่นั้นมีความซับซ้อนและหลายด้านทั้งด้านบวกและด้านลบดังนั้นการศึกษาสื่อใหม่จึงจำเป็นต้องหลุดพ้นจากหลุมพรางของการตัดสินใจทางเทคโนโลยีและมุ่งเน้นไปที่เครือข่ายทางสังคมที่ซับซ้อนซึ่งมีผลต่อการพัฒนาเทคโนโลยีการระดมทุนการนำไปปฏิบัติและทิศทางในอนาคตให้มากขึ้นขณะเดียวกันคนก็มีเวลาจำกัดในการบริโภคสื่อที่แตกต่างและการเกิดขึ้นของสื่อใหม่น่าจะส่งผลให้ผู้ชมหรือผู้อ่านสื่อดั้งเดิมลดลงซึ่งน่าจะเป็นประเด็นสำคัญในการศึกษาในอนาคตด้วย

2.6.4 อิทธิพลของสื่อใหม่

สื่อใหม่และความเป็นสากล สื่อใหม่ในฐานะพลังนำที่นำไปสู่กระบวนการโลกาภิวัตน์ผลักดันสังคมมนุษย์ไปสู่ทิศทางการพัฒนาที่เชื่อมโยงและซับซ้อนมากขึ้นในช่วงหลายสิบปีที่ผ่านมา สื่อใหม่ไม่เพียงแต่ประสบความสำเร็จในการรวมการสื่อสารระหว่างบุคคลแบบดั้งเดิม และการเข้าถึงการสื่อสารมวลชนแต่ยังช่วยให้บุคคลมีความสามารถในการควบคุมข้อมูลอย่างเท่าเทียมกันมากขึ้น ในด้านการสื่อสารระหว่างบุคคลและการสื่อสารมวลชน (Crosbie, 2002) รูปแบบปฏิสัมพันธ์แบบใหม่และวิธีการควบคุมข้อมูลได้ผลักดันการเปลี่ยนแปลงที่ครอบคลุมในทุกด้านของสังคมอย่างมาก

ดิจิทัลเป็นคุณลักษณะที่โดดเด่นที่สุดของสื่อใหม่ ทำให้การจับต้องไม่ได้ของข้อความสื่อเป็นไปได้ด้วยการเปลี่ยนข้อมูลจากรูปแบบอะนาล็อกเป็นรูปแบบดิจิทัล สื่อใหม่จะช่วยให้ข้อมูลสามารถดำเนินงานได้มากขึ้นและสามารถคำนวณได้ (Chen, 2012) สิ่งนี้ไม่เพียงช่วยเพิ่มประสิทธิภาพในการจัดเก็บและถ่ายโอนข้อมูลอย่างมากเท่านั้น แต่ยังช่วยให้สามารถดึงข้อมูลและดำเนินการได้มากในพื้นที่ที่จำกัด

สื่อใหม่แสดงให้เห็นถึงความสามารถในการผสมผสานที่แข็งแกร่ง ซึ่งเห็นได้ชัดโดยเฉพาะอย่างยิ่งในการเพิ่มขึ้นของอินเทอร์เน็ตไม่เพียงแต่รวมหลายสาขา เช่น การประมวลผลข้อมูลการสื่อสารสื่อการสื่อสารทางอิเล็กทรอนิกส์และคอมพิวเตอร์อิเล็กทรอนิกส์เท่านั้น แต่ยังส่งเสริมการหลอมรวมอุตสาหกรรม

ระหว่างพื้นที่เหล่านี้ (Flew, 2005) โดยเฉพาะการควมรวมกิจการและบูรณาการธุรกิจสื่อขนาดใหญ่อย่างต่อเนื่องเพื่อรองรับและตอบสนองต่อความต้องการของตลาดที่เปลี่ยนแปลงไปในบริบทสื่อใหม่และภายในอุตสาหกรรมสื่อ วัสดุผลิตภัณฑ์และบริการของสื่อต่าง ๆ ก็ได้รับการเชื่อมต่อและบูรณาการอย่างมากด้วยแรงผลักดันจากสื่อใหม่ ๆ ซึ่งเร่งก้าวของความหลากหลายและโลกาภิวัตน์ของอุตสาหกรรมสื่ออย่างไม่ต้องสงสัย

จากมุมมองของการมีปฏิสัมพันธ์สื่อใหม่ มีกลไกการโต้ตอบสองแบบที่ไม่เพียงแต่เปลี่ยนรูปแบบการปฏิสัมพันธ์ระหว่างผู้ใช้กับระบบสารสนเทศเท่านั้น แต่ยังเพิ่มประสิทธิภาพการใช้ทรัพยากรสารสนเทศอีกด้วย ในกระบวนการนี้ผู้ใช้สามารถมีอิสระในเนื้อหาและรูปแบบของข้อมูลอย่างไม่เคยปรากฏมาก่อนกล่าวคือ การมีปฏิสัมพันธ์ของสื่อใหม่ไม่เพียงแต่มีเงื่อนไขที่สะดวกต่อการดึงข้อมูลและการดำเนินงานในระดับเทคโนโลยีเท่านั้น แต่ยังส่งผลสำคัญต่อความซับซ้อนและความหลากหลายของการสื่อสารในสังคมมนุษย์อีกด้วย ด้วยการให้ผู้ใช้สามารถผลิตและผลิตซ้ำข้อมูลได้ด้วยตนเอง สื่อใหม่ได้แสดงให้เห็นถึงอิทธิพลทางสังคมที่แข็งแกร่งตลอดกระบวนการสื่อสารของมนุษย์

Hypertext เป็นคุณลักษณะที่สำคัญของสื่อใหม่ไปสู่การเกิดของศูนย์เครือข่ายการไหลของข้อมูลทั่วโลกและการเชื่อมต่อที่เป็นอิสระ (Lister et al., 2008) ปรากฏการณ์นี้ได้พลิกโฉมประสบการณ์ชีวิตของผู้คนในระดับโลกและขับเคลื่อนการเปลี่ยนแปลงในหลาย ๆ ด้าน เช่น กิจกรรมทางสังคมและเศรษฐกิจประเพณีวัฒนธรรมและวิธีการสื่อสาร จากข้อมูลของ Castells (2000) ที่กล่าวว่า Hypertext ไม่ได้เป็นเพียงคุณสมบัติทางเทคนิคเท่านั้น แต่ยังเป็นปัจจัยสำคัญในการขับเคลื่อนโลกาภิวัตน์และการเปลี่ยนแปลงทางสังคมในหลายมิติ เช่น วัฒนธรรม เศรษฐกิจ และสังคม

พื้นที่เสมือนจริงที่เกิดขึ้นจากสื่อใหม่ได้สร้างประสบการณ์เสมือนจริงและมุมมองความเป็นจริงแบบใหม่ให้กับผู้คน ไฮเบอร์สเปซที่ดูเหมือนนามธรรมนี้จริง ๆ แล้วมีผลกระทบในทางปฏิบัติมากมายรวมถึงแต่ไม่จำกัดเพียงขอบเขตที่คลุมเครือระหว่างความเป็นจริงและความเสมือนจริง การเปลี่ยนแปลงอัตลักษณ์ส่วนบุคคลหลาย ๆ อย่าง ตัวอย่างเช่น ในสภาพแวดล้อมของสื่อใหม่ผู้คนสามารถเปลี่ยนเพศ บุคลิกภาพ รูปลักษณ์และอาชีพของพวกเขาในอินเทอร์เน็ตได้ตามต้องการ การเพิ่มขึ้นของเสรีภาพนี้ ส่วนใหญ่ท้าทายแนวคิดดั้งเดิมของคนทั่วไปเกี่ยวกับความเป็นจริงและการรับรู้ตัวตน (โจนส์, 1995)

โลกาภิวัตน์เป็นปรากฏการณ์ทางสังคมหลายมิติและซับซ้อนที่สื่อใหม่เข้ามามีบทบาทเป็นตัวเร่งปฏิกิริยา Steger (2009) เชื่อว่าโลกาภิวัตน์ส่วนใหญ่เกี่ยวข้องกับการขยายตัวและการเสริมสร้างความสัมพันธ์ทางสังคมและจิตสำนึก ในเวลาทั่วโลกและในพื้นที่โลก นิยามนี้ไม่เพียงแต่แสดงให้เห็นว่าโลกาภิวัตน์เป็นกระบวนการขยายตัวอย่างต่อเนื่อง แต่ยังเน้นบทบาทของการรับรู้ทั่วโลก เมื่อโลกาภิวัตน์ได้สร้างประสบการณ์และการปฏิสัมพันธ์ที่ลึกซึ้งยิ่งขึ้น โลกทัศน์และมุมมองเชิงพื้นที่ของผู้คนก็เปลี่ยนไปเช่นกัน ก่อให้เกิดจิตสำนึกระดับโลก Waters (2013) กล่าวเพิ่มเติมว่าโลกาภิวัตน์คือข้อจำกัดทางภูมิศาสตร์เกี่ยวกับการจัดการทางสังคมและวัฒนธรรมค่อย ๆ หายไปและในขณะเดียวกันผู้คนก็ตระหนักถึง

กระบวนการนี้อย่างชัดเจนมากขึ้น แสดงให้เห็นว่าโลกาภิวัตน์ไม่ได้เป็นเพียงปรากฏการณ์ในระดับวัตถุเท่านั้นแต่ยังรวมถึงการเปลี่ยนแปลงในระดับจิตวิญญาณและจิตสำนึกด้วย

โลกาภิวัตน์เกิดขึ้นในระดับกิจกรรมทางสังคมที่แตกต่างกันซึ่งรวมถึงโลกทั้งใบประเทศเฉพาะอุตสาหกรรมหรือองค์กรเฉพาะและบุคคล (Govindarajan & Gupta, 1997) ซึ่งหมายความว่าโลกาภิวัตน์ไม่ได้สะท้อนให้เห็นเฉพาะในระดับมหภาคเท่านั้นแต่ยังรวมถึงในระดับจุลภาคและแม้กระทั่งระดับบุคคลหลายระดับนี้ทำให้โลกาภิวัตน์มีความซับซ้อนมากขึ้นและต้องมีการศึกษาและวิเคราะห์หลายมุม เฉิน (2005) ศึกษาพบว่าสื่อใหม่ผลักดันอิทธิพลโลกาภิวัตน์ให้แข็งแกร่ง ในห้าคุณลักษณะที่สำคัญคือ พลวัตสากล การเชื่อมต่อ การผสมผสานทางวัฒนธรรมและการเสริมสร้างความเข้มแข็งของแต่ละบุคคล ประการแรกโลกาภิวัตน์เป็นกระบวนการที่เต็มไปด้วยการเปลี่ยนแปลงแบบไดนามิก ซึ่งรวมถึงปฏิสัมพันธ์ที่ซับซ้อนระหว่างเอกลักษณ์ทางวัฒนธรรมและความหลากหลายทางวัฒนธรรมการโลคัลไลเซชันและความเป็นสากลวัตน์สะท้อนให้เห็นว่าโลกาภิวัตน์ไม่ใช่กระบวนการทิศทางเดียวแต่เป็นพหุนิยมและมีอิทธิพลต่อกัน ประการที่สองโลกาภิวัตน์มีลักษณะที่แพร่หลายเหมือนอากาศมีอิทธิพลต่อทุกแง่มุมของชีวิตเรา ตั้งแต่เศรษฐกิจวัฒนธรรมไปจนถึงวิถีชีวิต ประการที่สามโลกาภิวัตน์ได้สร้างเครือข่ายระดับโลกที่เชื่อมต่อกันอย่างใกล้ชิดซึ่งไม่เพียงแต่รวมถึงการแลกเปลี่ยนทางวัตถุเท่านั้นแต่ยังรวมถึงการไหลของข้อมูลแนวคิดและจิตสำนึกอย่างรวดเร็ว ประการที่สี่โลกาภิวัตน์ได้นำไปสู่การผสมผสานและการผสมผสานของวัฒนธรรมซึ่งแพร่กระจายอย่างรวดเร็วโดยเฉพาะอย่างยิ่งผ่านสื่อใหม่ทำลายขอบเขตของภูมิภาคและวัฒนธรรมในที่สุดโลกาภิวัตน์ได้ให้อิทธิพลแก่ปัจเจกบุคคลมากขึ้นผ่านแพลตฟอร์มสื่อใหม่และการเพิ่มอำนาจของปัจเจกบุคคลนี้ ในทางกลับกันก็ส่งเสริมการบรรลุความหลากหลายทั่วโลก คุณลักษณะทั้งห้านี้มีอิทธิพลต่อกันและกันและรวมกันเป็นปรากฏการณ์โลกาภิวัตน์ที่ซับซ้อนและหลากหลายมากขึ้น Chen (2000)

ด้วยแรงบันดาลใจและแรงผลักดันจากการเพิ่มขึ้นของสื่อใหม่ โลกาภิวัตน์มีผลกระทบอย่างลึกซึ้งในหลาย ๆ ด้านรวมถึงพลวัตวิภาษ ความเป็นสากล การเชื่อมต่อที่ครอบคลุมการผสมผสานทางวัฒนธรรมและพลังของแต่ละบุคคล ผลกระทบนี้ไม่เพียงแต่เปลี่ยนวิถีชีวิตและรูปแบบพฤติกรรมของผู้คนอย่างมากแต่ยังกำหนดจิตสำนึกของชุมชนใหม่และแม้กระทั่งปรับโครงสร้างพื้นฐานของสังคมมนุษย์ในระดับมหภาคมากขึ้นในบริบทนี้สื่อใหม่ผสมผสานกับโลกาภิวัตน์ก่อให้เกิดการเปลี่ยนแปลงทางสังคมอย่างลึกซึ้งผลกระทบของการผสมผสานของสื่อใหม่และโลกาภิวัตน์ปรากฏในห้ามิติที่ชัดเจน ได้แก่ การหดตัวของโลกการบีบอัดเวลาและพื้นที่ปฏิสัมพันธ์อย่างใกล้ชิดในทุกด้านของสังคมการเชื่อมต่อระดับโลกและการเร่งการแข่งขันและความร่วมมือในระดับภูมิภาคและระดับโลก (Chen & Starosta, 2000) ในบริบทที่กว้างขวางนี้ พบว่าขอบเขตดั้งเดิมของสังคมมนุษย์ในหลาย ๆ ด้านรวมถึงพื้นที่เวลาขอบเขตโครงสร้างภูมิศาสตร์ วิชาชีพค่านิยมและความเชื่อกำลังเปลี่ยนแปลงอย่างรวดเร็วการเปลี่ยนแปลงนี้กำลังเปลี่ยนไปสู่รูปแบบใหม่ของความเหมือนและการเชื่อมต่อที่สะท้อนผลกระทบอย่างลึกซึ้งจากโลกาภิวัตน์และสื่อใหม่

แม้ว่าจะมีการพึ่งพาอาศัยกันอย่างชัดเจนระหว่างสื่อใหม่และโลกาภิวัตน์แต่วิธีการเข้าใจความเชื่อมโยงที่เป็นรูปธรรมระหว่างคุณลักษณะห้าประการของสื่อใหม่(เช่นการแปลงเป็นดิจิทัลการหลอมรวมการโต้ตอบไฮเปอร์เท็กซ์ความเสมือนจริง)และคุณลักษณะที่เห็นได้ชัดห้าประการของโลกาภิวัตน์(เช่นพลวัตวิทยาศาสตร์การแทรกซึมทั่วไปการเชื่อมต่อที่ครอบคลุมการผสมทางวัฒนธรรมพลังส่วนบุคคล)ยังคงเป็นหัวข้อที่ควรค่าแก่การศึกษาเชิงลึกโดยนักวิชาการ (Chen & Starosta, 2000) ความสัมพันธ์เชิงปฏิสัมพันธ์ที่ซับซ้อนนี้เกี่ยวข้องกับการวิจัยหลายสาขารวมถึงสังคมวิทยาการสื่อสาร การศึกษาวัฒนธรรมและอื่นๆ แต่ละมิติอาจเปิดเผยว่าสื่อใหม่และโลกาภิวัตน์มีอิทธิพลต่อทุกแง่มุมของสังคมสมัยใหม่ร่วมกันอย่างไรแม้ว่าบทความนี้จะมุ่งเน้นไปที่ความสัมพันธ์ระหว่างสื่อใหม่และการสื่อสารข้ามวัฒนธรรมเป็นหลักแต่เราก็คะหนักคิดว่าหัวข้อการวิจัยนี้เป็นเพียงส่วนเล็กๆ ของพื้นที่การวิจัยที่กว้างขึ้น

สรุปการศึกษาแนวคิดเกี่ยวกับสื่อใหม่นี้เพื่อทำความเข้าใจพฤติกรรมของผู้ใช้ กลไกการเผยแพร่เนื้อหาและการปกป้องข้อมูล การใช้ทฤษฎีสื่อใหม่ในการศึกษานี้สามารถสร้างความตระหนักว่าพฤติกรรมการโต้ตอบซึ่งเป็นปฏิสัมพันธ์ของผู้ใช้แพลตฟอร์ม Douyin ที่เกี่ยวข้องกับความเสี่ยง เช่น การรั่วไหลของความเป็นส่วนตัวและการแพร่กระจายของข่าวปลอม ดังนั้นรูปแบบการจัดการความปลอดภัยของข้อมูลที่มีประสิทธิภาพจำเป็นต้องพิจารณาทั้งสามระดับของเทคโนโลยีระบบและการศึกษาเพื่อให้แน่ใจว่าข้อมูลที่ปลอดภัยและถูกต้องในสภาพแวดล้อมของสื่อใหม่

2.7 งานวิจัยที่เกี่ยวข้อง

Mirtschetal (2021) มีวัตถุประสงค์ในการศึกษาเพื่อเพิ่มพูนความรู้เกี่ยวกับการจัดการความปลอดภัยของข้อมูลในระดับบริษัทโดยเฉพาะเกี่ยวกับการดำเนินการตามมาตรฐานสากล ISO/IEC27001 จากการสำรวจบริษัทเยอรมัน 125 แห่งที่ได้รับการรับรองมาตรฐาน ISO/IEC27001 การศึกษานี้แสดงให้เห็นถึงแรงจูงใจในการนำ ISO/IEC27001 ไปใช้ผลกระทบที่ประสบและอุปสรรคที่เผชิญเมื่อพิจารณาถึงความแตกต่างในอัตราการนำไปใช้ระหว่างบริษัทในภาค ICT และที่ไม่ใช่ ICT การศึกษานี้จึงเน้นไปที่การเปลี่ยนแปลงที่เกี่ยวข้องกับอุตสาหกรรมเป็นพิเศษการศึกษานี้พิจารณาการนำมาตรฐานนี้ไปใช้ในฐานะนวัตกรรมเชิงป้องกันขององค์กรและใช้การสร้างแบบจำลองสมการโครงสร้างเพื่อตรวจสอบสาเหตุของอัตราการใช้มาตรฐานระบบการจัดการนี้ที่ค่อนข้างต่ำในกลุ่มบริษัทที่ไม่ใช่ภาค ICT จากผลการวิจัยการศึกษาครั้งนี้ให้คำแนะนำสำหรับผู้กำหนดนโยบาย หน่วยกำหนดมาตรฐาน และหน่วยรับรองเพื่อส่งเสริมความนิยมต่อการจัดการความปลอดภัยระบบสารสนเทศ

Topa & Karyda (2019) มีวัตถุประสงค์เพื่อสำรวจผลกระทบของปัจจัยกำหนดพฤติกรรมความปลอดภัยต่อการจัดการความปลอดภัยและเสนอการตอบสนองที่สามารถบูรณาการเข้ากับแนวทางปฏิบัติการจัดการความปลอดภัยในปัจจุบัน(รวมถึงแนวทางปฏิบัติที่เป็นไปตามมาตรฐานความปลอดภัยของข้อมูลที่น่ามาใช้อย่างกว้างขวาง ISO 27001, 27002, 27003 และ 27005) ด้วยการวิเคราะห์ที่ครอบคลุมของวรรณกรรมที่เกี่ยวข้อง ปัจจัยสำคัญที่มีอิทธิพลต่อพฤติกรรมความปลอดภัยของพนักงานและการปฏิบัติตามนโยบายความปลอดภัยของข้อมูล (ISP) ได้รับการระบุและปัจจัยเหล่านี้ถูกนำมาใช้ใน

การดำเนินการวิเคราะห์ช่องว่างของมาตรฐานความปลอดภัยของข้อมูลที่น่ามาใช้กันอย่างแพร่หลาย ระบุปัญหาที่ไม่ครอบคลุมหรือแก้ไขปัญหาก็ได้เพียงบางส่วนเท่านั้น การศึกษาพบว่า ปัจจัยที่มีอิทธิพลต่อพฤติกรรมการรักษาความปลอดภัยรวมถึงการมีส่วนร่วมของผู้บริหารระดับสูง การปรับให้เข้ากับลักษณะส่วนบุคคล การพิจารณาภูมิหลังทางวัฒนธรรม การส่งเสริมให้พนักงานปฏิบัติตามนิสัยและการพิจารณาค่าใช้จ่ายในการปฏิบัติตามข้อกำหนด มีเพียงเล็กน้อยหรือไม่มีเลยในมาตรฐานความปลอดภัยของข้อมูล ISO นอกจากนี้การศึกษานี้ยังให้แนวทางในการปรับปรุงแนวทางปฏิบัติในการจัดการความปลอดภัยเมื่อนำมาตรฐาน ISO ไปใช้ปฏิบัติการศึกษาไม่เพียงแต่วิเคราะห์บทบาทและผลกระทบของปัจจัยกำหนดพฤติกรรมความปลอดภัยเท่านั้น แต่ยังอภิปรายถึงความคลาดเคลื่อนและข้อค้นพบที่ขัดแย้งในวรรณกรรมที่เกี่ยวข้องให้การวิเคราะห์ช่องว่างของมาตรฐานความปลอดภัยของข้อมูลที่ใช้กันทั่วไปและเสนอแนวทางปฏิบัติในการจัดการความปลอดภัยที่ได้รับการปรับปรุงเกี่ยวกับวิธีการปรับปรุง ISP การปฏิบัติตามแนวทางที่กำหนดไว้

Chu & So (2020) ได้ทำการศึกษาเกี่ยวกับประเภทของพฤติกรรมการรักษาความปลอดภัยของข้อมูลของพนักงานที่ผิดจรรยาบรรณและผลกระทบต่อการรักษาระบบข้อมูลที่ยั่งยืนในที่ทำงานโดยมีวัตถุประสงค์เพื่อระบุและพัฒนาเครื่องมือที่เชื่อถือได้และถูกต้องเพื่อวัดปริมาณความปลอดภัยของข้อมูลของพนักงานที่ผิดจรรยาบรรณประเภทต่างๆ พฤติกรรมและสำรวจปัจจัยที่มีอิทธิพลต่อพฤติกรรมเหล่านี้และวิธีที่ปัจจัยเหล่านี้คาดการณ์ความเต็มใจของพนักงานในการรายงานเหตุการณ์ด้านความปลอดภัยของข้อมูลด้วยการใช้วิธีการวิจัยเชิงปริมาณการศึกษานี้เผยให้เห็นความสัมพันธ์ระหว่างความพยายามในการจัดการความปลอดภัยของข้อมูลกับพฤติกรรมด้านความปลอดภัยของข้อมูลที่ผิดจรรยาบรรณของพนักงานและสำรวจผลกระทบของโปรแกรมการรับรู้ด้านความปลอดภัยของข้อมูลและการรับรู้ถึงการลงโทษต่อพฤติกรรมที่ผิดจรรยาบรรณประเภทต่าง ๆ ผลการวิจัยระบุว่าพฤติกรรมการรักษาความปลอดภัยของข้อมูลที่ผิดจรรยาบรรณบางประเภทอาจส่งผลกระทบต่อความสมัครใจของพนักงานในการรายงานเหตุการณ์ด้านความปลอดภัยของข้อมูลการค้นพบนี้มีผลกระทบที่สำคัญต่อผู้จัดการในการพัฒนากฎและนโยบายด้านความปลอดภัยที่มีประสิทธิภาพมากขึ้นซึ่งเป็นกุญแจสำคัญในการรักษาความต่อเนื่องทางธุรกิจ

Stewart & Jurjens (2017) มุ่งหวังที่จะส่งเสริมให้ฝ่ายบริหารตระหนักว่าพนักงานมีบทบาทสำคัญในการจัดการความปลอดภัยของข้อมูลโดยเฉพาะอย่างยิ่งในองค์กรที่ข้อมูลเป็นทรัพย์สินที่มีค่าและปัญหาเหล่านี้จำเป็นต้องได้รับการแก้ไขอย่างมีประสิทธิภาพ การศึกษานี้ใช้วิธีการวัดที่ถูกต้องตามกรอบทฤษฎีวรรณกรรมที่มีอยู่เพื่อจัดทำแบบสอบถามและรวบรวมข้อมูลผ่านแบบสอบถามแบบภาคตัดขวางและมาตราส่วน Likert โดยอ้างอิงกับมาตราส่วนของ Witherspoon และคณะ (2013) การศึกษานี้เสนอหลักปฏิบัติในการปฏิบัติตามข้อกำหนดด้านความปลอดภัยของข้อมูลของหลักการ Nine-Five Circle (NFC) โดยใช้โปรแกรมสำเร็จรูปในการวิเคราะห์ข้อมูลและจากการสำรวจและผลการวิจัย 3 ครั้ง ซึ่งพบว่าพฤติกรรมของมนุษย์และปัญหาที่เกี่ยวข้องกับความปลอดภัยด้านไอที การจัดการความปลอดภัยของ

ข้อมูลการศึกษานี้ไม่เพียงแต่ช่วยในการหาการวิจัยเกี่ยวกับปัจจัยที่ส่งผลต่อการพัฒนาและการดำเนินการด้านการจัดการความมั่นคงปลอดภัยสารสนเทศแต่ยังเผยให้เห็นปัญหาที่แท้จริงที่นำไปสู่ข้อบกพร่องในการจัดการความมั่นคงปลอดภัยสารสนเทศโดยการให้ข้อมูลเชิงประจักษ์ให้คำแนะนำเชิงปฏิบัติแก่องค์กรในการกำหนดข้อมูล นโยบายการปฏิบัติตามข้อกำหนดด้านความปลอดภัย

Kim & Kim (2021) มีวัตถุประสงค์เพื่อตรวจสอบผลกระทบของปัจจัยด้านเทคนิค องค์กรและสิ่งแวดล้อม(กรอบงานTOE)ต่อความตั้งใจในการจัดการความปลอดภัยข้อมูลขององค์กรการเพิ่มประสิทธิภาพและความคงอยู่จากการสำรวจผู้เชี่ยวชาญในสาขาที่เกี่ยวข้องกับความปลอดภัยของข้อมูล การศึกษานี้รวบรวมและวิเคราะห์แบบสอบถาม 107 รายการผลการศึกษานี้ระบุว่าปัจจัยด้านองค์กรและสิ่งแวดล้อมมีผลกระทบอย่างมีนัยสำคัญต่อความตั้งใจของการจัดการความปลอดภัยของข้อมูลในขณะที่ปัจจัยทางเทคนิคและสิ่งแวดล้อมมีบทบาทสำคัญในการปรับปรุงการจัดการความปลอดภัยของข้อมูล นอกจากนี้ปัจจัยด้านสิ่งแวดล้อมยังได้รับการพิสูจน์แล้วว่าเป็นปัจจัยที่สำคัญที่สุดที่ส่งผลต่อการจัดการความปลอดภัยของข้อมูลขององค์กรการศึกษายังพบว่าการเสริมสร้างความเข้มแข็งของการจัดการความปลอดภัยของข้อมูลมีผลกระทบอย่างมีนัยสำคัญต่อความยั่งยืนมากกว่าความตั้งใจของการจัดการความปลอดภัยของข้อมูลงานวิจัยนี้ให้มุมมองและหลักฐานใหม่ๆสำหรับการทำความเข้าใจและปรับปรุงการจัดการความปลอดภัยของข้อมูลองค์กร

Kor & Metin (2021) การศึกษานี้เน้นย้ำถึงความสำคัญของพฤติกรรมการรักษาความปลอดภัยของข้อมูลส่วนบุคคลนอกเหนือจากมาตรการทางเทคนิคเมื่อใช้มาตรฐานการจัดการความปลอดภัยของข้อมูล ISO/IEC27001 วัตถุประสงค์ของการศึกษานี้คือเพื่อแสดงให้เห็นถึงบทบาทที่สำคัญของปัจจัยมนุษย์ในการรับรองความปลอดภัยของสินทรัพย์ข้อมูลขององค์กร นอกเหนือจากการควบคุมทางเทคนิคและระดับองค์กร การศึกษานี้ใช้วิธีการวิจัย เช่น การวัดความน่าเชื่อถือและการวิเคราะห์ปัจจัยยืนยันผ่านการสำรวจแบบสอบถามจำนวน 630 คนและการวิเคราะห์ข้อมูลผลการศึกษานี้สนับสนุนความน่าเชื่อถือของขนาดที่ใช้ในการศึกษาและพิสูจน์ว่าในกระบวนการดำเนินการของการจัดการความปลอดภัยของข้อมูล ISO/IEC27001 การใส่ใจกับพฤติกรรมด้านความปลอดภัยส่วนบุคคลเป็นสิ่งสำคัญ งานวิจัยนี้ไม่เพียงแต่ให้มุมมองใหม่เกี่ยวกับการจัดการความปลอดภัยของข้อมูลเท่านั้นแต่ยังให้คำแนะนำเชิงปฏิบัติที่สำคัญสำหรับองค์กรในการกำหนดและการนำนโยบายความปลอดภัยของข้อมูลไปใช้อีกด้วย

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

บทที่ 3 ระเบียบวิธีวิจัย

การศึกษาวิจัยเรื่องนี้ เป็นการศึกษาวิจัยซึ่งมีวัตถุประสงค์ เพื่อศึกษาศึกษากลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และการพัฒนารูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน โดยการศึกษาวิจัยในครั้งนี้ มีวิธีดำเนินการวิจัยเพื่อการพัฒนา (Research and development) มีรายละเอียด ดังนี้

ตารางที่ 3.1 แสดงตารางขั้นตอนการศึกษาวิจัยตามวัตถุประสงค์ของการวิจัย

วัตถุประสงค์การวิจัย	วิธีการวิจัย	แนวคิด/ทฤษฎี	วิธีการวิจัย	
			แหล่งข้อมูล	วิธีการเก็บรวบรวมข้อมูล
1. เพื่อศึกษาศึกษากลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน	-เชิงคุณภาพ -และเชิงปริมาณ	-ทฤษฎีความปลอดภัยของข้อมูลไซเบอร์ -ทฤษฎีสื่อใหม่ -ทฤษฎีการจัดการ - ทฤษฎีการจัดการการสื่อสาร -แนวคิดเกี่ยวกับกลยุทธ์	-บล็อกเกอร์ -ผู้บริหารระดับสูง -ผู้บริหารระดับกลาง -ผู้บริหารระดับปฏิบัติ -ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน	-สัมภาษณ์ -แบบสอบถาม
2. การพัฒนารูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน	เชิงคุณภาพ	-ทฤษฎีความปลอดภัยของข้อมูลไซเบอร์ - ทฤษฎีสื่อใหม่ -ทฤษฎีการจัดการการสื่อสาร -ทฤษฎีการจัดการนวัตกรรม -แนวคิดเกี่ยวกับรูปแบบ -แนวคิดเกี่ยวกับการพัฒนา	-บล็อกเกอร์ -ผู้บริหารระดับสูง -ผู้บริหารระดับกลาง -ผู้บริหารระดับปฏิบัติ	-การระดมสมอง -การประชุมกลุ่ม

3.1 แนวทางการวิจัย

การศึกษานี้เป็นการวิจัยประยุกต์ (Applied research) เป็นการวิจัยแบบผสมผสาน (mixed methods research) ระหว่างการวิจัยเชิงปริมาณ (Quantitative research) กับการวิจัยเชิงคุณภาพ (Qualitative research) โดยใช้วิธีการศึกษาจากเอกสาร และวิเคราะห์เอกสาร (Documentary Research) วิธีการสัมภาษณ์แบบเจาะลึก (In-Depth Interview) และใช้วิธีการสังเคราะห์ข้อมูลความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน โดยมีผู้บริหารระดับสูง ผู้บริหารระดับกลาง และผู้บริหารระดับปฏิบัติการ เจ้าหน้าที่ภาครัฐ บล็อกเกอร์ และผู้มีส่วนได้ส่วนเสีย เป็นหน่วยการวิเคราะห์ (Unit of Analysis) โดยข้อมูลที่รวบรวมได้จะนำไปวิเคราะห์ใน 2 รูปแบบ คือ 1) การวิเคราะห์เนื้อหา (Content Analysis) และ 2) การวิเคราะห์แบบอุปนัย (Analytic Induction) ซึ่งผู้วิจัยกำหนดระเบียบวิธีวิจัยสำหรับการศึกษา ตามวัตถุประสงค์ ในการเก็บรวบรวมข้อมูลเพื่อให้ได้คำตอบตามวัตถุประสงค์การวิจัยที่กำหนดไว้ และให้ได้ข้อมูลหลายส่วนครบถ้วนประกอบกัน ให้ได้ข้อมูลครบถ้วนทุกด้าน โดยการวิจัยแต่ละประเภทมีลักษณะดังนี้

1. การวิจัยเชิงปริมาณ (Quantitative Research) เพื่อเก็บรวบรวมข้อมูล และวิเคราะห์ถึงลักษณะข้อมูลส่วนบุคคล พฤติกรรมการใช้แพลตฟอร์มออนไลน์ไต้หวัน ความคาดหวังต่อการจัดการความปลอดภัยระบบสารสนเทศของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน และความต้องการความปลอดภัยระบบสารสนเทศของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน โดยใช้แบบสอบถาม (Questionnaire) เป็นเครื่องมือ ซึ่งรายละเอียดของประชากรและกลุ่มตัวอย่าง เครื่องมือที่ใช้ในการศึกษา ขั้นตอนการสร้างเครื่องมือวิธีเก็บรวบรวมข้อมูล การวิเคราะห์ข้อมูล และการอภิปรายผลการวิเคราะห์ จะได้กล่าวในลำดับต่อ ๆ ไป

2. การวิจัยเชิงคุณภาพ (Qualitative Research) ใช้วิธีศึกษาวิจัยดังนี้

- 1) การสัมภาษณ์แบบเจาะลึก (In-depth Interview) เพื่อศึกษากลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ผู้วิจัยใช้การสัมภาษณ์เชิงลึก เป็นการสัมภาษณ์ในรูปแบบที่ไม่เป็นทางการ โดยมีการใช้ประเด็น/แนวคำถามกว้างๆ เพื่อกระตุ้นให้คู่สนทนาเล่าเรื่องราวอย่างมีเป้าหมาย ผู้สัมภาษณ์มีปฏิสัมพันธ์กับผู้ถูกสัมภาษณ์ในลักษณะเป็นคู่สนทนา โดยมีการใช้ทักษะการสื่อสาร สร้างการสนทนาอย่างมีเป้าหมาย โดยผู้วิจัยมีการสัมภาษณ์บุคคลซึ่งเป็นแหล่งข้อมูลกลุ่มเป้าหมายที่ได้กำหนดไว้เป็นผู้ให้ข้อมูลหลัก (Key Informant) ที่เป็นตัวแทนจากผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้บริหารระดับปฏิบัติการ และบล็อกเกอร์ เจ้าหน้าที่หน่วยงานภาครัฐ ที่มีส่วนเกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ และผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวัน จำนวน 3 กลุ่ม ได้แก่ 1) หน่วยงานภาครัฐบาล/หน่วยงานในกำกับ 2) หน่วยงานภาคเอกชน 3) บล็อกเกอร์ที่มีความรู้เกี่ยวกับแพลตฟอร์มออนไลน์ไต้หวัน

- 2) การสังเคราะห์ (Synthesis) โดยวิธีการดังนี้ 1) นำผลข้อมูลจากการวิเคราะห์ข้อมูลเชิงปริมาณ เกี่ยวกับความคาดหวังด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และความต้องการด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน 2) นำผลจากการศึกษาเชิงคุณภาพด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) เกี่ยวกับประเด็นกลยุทธ์การ

จัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน มาหาข้อสรุปโดยการวิเคราะห์ SWOT เพื่อพัฒนาเป็นรูปแบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันเบื้องต้น

3) การระดมสมอง /focus group/ การประชุมกลุ่ม โดยนำข้อมูลจากการสังเคราะห์ (Synthesis) ข้อมูลจากข้อที่ 1 เกี่ยวกับความคาดหวังด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และความต้องการด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และข้อมูลจากข้อที่ 2 กลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน เพื่อยืนยันรูปแบบการพัฒนาการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

3.2 การวิจัยเชิงปริมาณ

3.2.1 ประชากร และกลุ่มตัวอย่าง

ประชากรที่ใช้ในการศึกษา คือ ประชาชนจีนที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันใน 4 ภูมิภาคของประเทศจีน คือ 1) ภาคตะวันออกมณฑลชานตง 2) ภาคเหนือมณฑลเหอหนาน 3) ภาคตะวันตกมณฑลเสฉวน 4) ภาคใต้มณฑลกวางตุ้ง ปัจจุบันมณฑลทั้ง 4 ภูมิภาคมีจำนวนประชากรรวมกันมากกว่า 220 ล้านคน ณ วันที่ 13 มีนาคม 22567 (สำนักงานการทะเบียนราษฎร กรุงปักกิ่ง, 2024)

กลุ่มตัวอย่างที่ใช้ในการศึกษาวิจัยครั้งนี้ คือ ตัวแทนของประชาชนชาวจีนที่อาศัยอยู่ใน 4 ภูมิภาคของประเทศจีน ทั้ง 4 มณฑล เนื่องจากมีจำนวนประชากรจำนวนมาก จึงใช้ตาราง Taro Yamana ที่คำนวณแบบสำเร็จรูปแล้วในแต่ละระดับความคลาดเคลื่อน ดังนี้

ตารางที่ 3.2 ขนาดกลุ่มตัวอย่างในแต่ละระดับความคลาดเคลื่อน

ขนาดประชากร (N)	ขนาดกลุ่มตัวอย่างในแต่ละระดับความคลาดเคลื่อน (e)					
	±1%	±2%	±3%	±4%	±5%	±10%
6000		1765	938	566	375	98
7000		1842	959	574	387	99
8000		1905	976	580	381	99
9000		1957	898	584	383	99
10000	5000	2000	1000	588	385	99
15000	6000	2143	1034	600	390	99
20000	6667	2222	1053	606	392	100
25000	7143	2273	1064	610	394	100
∞		2500	1111	625	400	100

ดังนั้นในการวิจัยนี้ ผู้วิจัยจึงได้กำหนดขนาดตัวอย่างไว้ ไม่น้อยกว่า 400 คน

3.2.2 วิธีการเลือกตัวอย่าง

วิธีการเลือกตัวอย่างของงานวิจัยนี้ โดยมีขั้นตอนดังนี้

ขั้นตอนที่ 1 กำหนดขนาดกลุ่มตัวอย่างจากตารางสูตรการคำนวณของทาโร ยามาเน่ (Taro Yamane) ที่ระดับความเชื่อมั่น 95% และค่าความคลาดเคลื่อนที่ 0.05 ได้จำนวนกลุ่มตัวอย่างจำนวน 400 คน (ตามที่ได้ดำเนินการแล้วในข้อ 3.2.1)

ขั้นตอนที่ 2 เลือกกลุ่มตัวอย่างที่เป็นประชาชนจีนที่ใช้แพลตฟอร์มออนไลน์ไต้ยีน ในพื้นที่ทั้ง 4 มณฑล คือ 1) มณฑลซานตง 2) มณฑลเหอหนาน 3) มณฑลเสฉวน 4) มณฑลกวางตุ้ง ที่ยินดีให้ความร่วมมือ

ขั้นตอนที่ 3 เลือกสุ่มตัวอย่างด้วยวิธีการคัดเลือกแบบตามสะดวก (Accident Sampling) โดยผู้วิจัยได้ออกไปแจกแบบสอบถามด้วยตนเอง ซึ่งกำหนดเป็นพื้นที่เขตเมืองที่ประชาชนอาศัยอยู่หนาแน่นทั้ง 4 มณฑล ที่ใช้แพลตฟอร์มออนไลน์ไต้ยีน

3.2.3 เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล

การศึกษานี้ได้ใช้แบบสอบถามเป็นเครื่องมือในการเก็บรวบรวมข้อมูล โดยสร้างจากการศึกษาแนวคิด ทฤษฎีที่เกี่ยวข้อง และเอกสารเกี่ยวกับการจัดการความปลอดภัยระบบสารสนเทศ ของแพลตฟอร์มสื่อออนไลน์ไต้ยีน แบบสอบถามประกอบด้วยคำถามปลายปิด (Closed-Ended) และคำถามปลายเปิด (Open-Ended) โดยแบ่งเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 ชุดคำถามเกี่ยวกับลักษณะข้อมูลส่วนบุคคลของผู้ใช้แพลตฟอร์มสื่อออนไลน์ไต้ยีน ได้แก่ เพศ อายุ อาชีพ รายได้ การศึกษา สถานภาพ เป็นคำถามแบบเลือกตอบ (Check List)

ส่วนที่ 2 ชุดคำถามเกี่ยวกับพฤติกรรมการใช้แพลตฟอร์มสื่อออนไลน์ไต้ยีน เป็นคำถามแบบเลือกตอบ (Check List)

ส่วนที่ 3 ชุดคำถามเกี่ยวกับความคาดหวังด้านการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อออนไลน์ไต้ยีน เป็นคำถามแบบมาตรวัดประเมินค่า ชนิดมาตราส่วนประเมินค่า 5 ระดับ (Rating Scale) ตามแบบของลิเคิร์ต (Likert's Rating Scale) ดังนี้

5 หมายถึง มีความคาดหวังด้านการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับมากที่สุด

4 หมายถึง มีความคาดหวังด้านการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับมาก

3 หมายถึง มีความคาดหวังด้านการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับปานกลาง

2 หมายถึง มีความคาดหวังด้านการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับน้อย

1 หมายถึง มีความคาดหวังด้านการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับน้อยที่สุด

ส่วนที่ 4 ชุดคำถามเกี่ยวกับความต้องการการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มสื่อออนไลน์ไต้ยีน เป็นคำถามแบบมาตรวัดประเมินค่า ชนิดมาตราส่วนประเมินค่า 5 ระดับ (Rating Scale) ตามแบบของลิเคิร์ต (Likert's Rating Scale) ดังนี้

- ที่สุด
- 5 หมายถึง มีความต้องการการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับมากที่สุด
- 4 หมายถึง มีความต้องการการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับมาก
- 3 หมายถึง มีความต้องการการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับปานกลาง
- 2 หมายถึง มีความต้องการการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับน้อย
- 1 หมายถึง มีความต้องการการจัดการความปลอดภัยระบบสารสนเทศอยู่ในระดับน้อยที่สุด
- ส่วนที่ 5 ข้อเสนอแนะของงานวิจัย เป็นแบบคำถามปลายเปิดเพื่อให้ประชาชนชาวจีนที่เป็นผู้แพลตฟอร์มสื่อออนไลน์ไต้หวัน ที่เป็นกลุ่มตัวอย่างได้ให้ความคิดเห็นอย่างอิสระ

3.2.4 การตรวจสอบคุณภาพเครื่องมือ

เมื่อสร้างแบบสอบถามตามแนวคิดและทฤษฎี การศึกษาผลงานที่เกี่ยวข้องเสร็จแล้วนำไปตรวจสอบคุณภาพเครื่องมือ การตรวจสอบคุณภาพของเครื่องมือ เป็นขั้นตอนหลังจากการสร้างเครื่องมือเรียบร้อยแล้ว ดังนั้นเพื่อความถูกต้อง ผู้วิจัยนำไปตรวจสอบเครื่องมือ (สุวิมล ติรกันนท์, 2543: 50) ตามขั้นตอน ดังนี้

1. การหาความตรงเชิงเนื้อหา (Content Validity) ผู้สอบถามได้นำแบบสอบถามเสนอต่ออาจารย์ที่ปรึกษาตรวจสอบในด้านความเที่ยงตรงของเนื้อหา รูปแบบของแบบสอบถาม (Format) ความเหมาะสมด้านภาษา (Wording) ความสมบูรณ์ของคำชี้แจง และความเหมาะสมของการใช้เวลาในการตอบแบบสอบถาม เมื่อรับเครื่องมือกลับคืนจากอาจารย์ที่ปรึกษาแล้วนำข้อแก้ไขทั้งหมดมาปรับปรุงแก้ไขให้สมบูรณ์ยิ่งขึ้นตามข้อเสนอแนะ

2. การหาความเที่ยงตรงของเนื้อหา และความเหมาะสมของภาษาที่ใช้ โดยในการทดสอบความเที่ยงตรงตามเนื้อหาได้ดำเนินการโดยให้ผู้เชี่ยวชาญพิจารณาถึงความสอดคล้องระหว่างวัตถุประสงค์ กับแบบสอบถามเป็นรายข้อ วิธีการพิจารณาแบบนี้จะเรียกว่า การหาค่าสัมประสิทธิ์ความสอดคล้อง (Index of Item – Objective Congruence : IOC) โดยมีสูตรการการคำนวณ ดังนี้

$$\text{สูตร} \quad ioc = \frac{\sum r}{n}$$

เมื่อ IOC คือ ความสอดคล้องระหว่างเนื้อหาในข้อคำถามกับวัตถุประสงค์

$\sum R$ คือ ผลรวมของคะแนนความคิดเห็นของผู้เชี่ยวชาญทั้งหมด

N คือ จำนวนผู้เชี่ยวชาญ

ด้วยการแปลความหมายของคะแนน ดังนี้

+1 ข้อคำถามวัดได้ตามวัตถุประสงค์การวิจัย

0 ข้อคำถามวัดได้ไม่ตรงตามวัตถุประสงค์การวิจัย

-1 ข้อคำถามวัดไม่ได้ เพราะไม่เกี่ยวข้องกับวัตถุประสงค์การวิจัย

การเลือกข้อคำถามที่ใช้ในการวิจัยด้วยค่า IOC โดยใช้เกณฑ์ค่ามากกว่าหรือเทียบเท่า 0.5 สำหรับค่าที่น้อยกว่า 0.5 นำมาปรับปรุงตามหรือตัดออกไปตามคำแนะนำของผู้เชี่ยวชาญ

ผู้เชี่ยวชาญในการตรวจสอบความเที่ยงตรงของเครื่องมือวิจัยมี 3 ท่าน ดังนี้

- | | |
|---|--|
| 1. รองศาสตราจารย์ ดร.อภิวรรณ ศิรินันทนา | ผู้ช่วยคณบดีคณะนิเทศศาสตร์
มหาวิทยาลัยราชภัฏรำไพพรรณี |
| 2. ผู้ช่วยศาสตราจารย์ ดร.เสาวนีย์ วรรณประภา | ผู้ช่วยคณบดีคณะนิเทศศาสตร์
มหาวิทยาลัยราชภัฏรำไพพรรณี |
| 3. รองศาสตราจารย์ ดร. สุภาภรณ์ ศรีดี | ประธานสาขาวิชานิเทศศาสตร์
มหาวิทยาลัยสุโขทัยธรรมมาธิราช |

การหาค่าความเที่ยงตรงของเนื้อหาและความเหมาะสมของภาษาที่ใช้ระหว่างข้อคำถามกับรูปแบบการดำเนินชีวิตและผลกระทบในครั้งนี้ ได้ค่า IOC มีค่าเท่ากับ 0.95 (ภาคผนวก ค.)

3. การหาความเชื่อถือได้ (Reliability) โดยนำแบบสอบถามที่ปรับปรุงแล้วไปทดลองใช้ (Try Out) กับประชากรที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันในพื้นที่ข้างเคียง จำนวน 30 คน แล้วนำมาวิเคราะห์ด้วยโปรแกรมสำเร็จรูปทางสถิติ วิเคราะห์หาค่าทดสอบความเที่ยงของแบบสอบถามและค่าความเชื่อมั่นของเครื่องมือ โดยการคำนวณหาค่าสัมประสิทธิ์แบบครอนบาค (Cronbach Alpha Coefficient) ซึ่งกำหนดว่าจะต้องได้ค่าสัมประสิทธิ์แอลฟาตั้งแต่ 0.75 ขึ้นไป จึงจะยอมรับว่ามีความเชื่อถือได้

4. การหาคุณภาพของเครื่องมือครั้งนี้ สามารถหาความเชื่อมั่นของเครื่องมือ ได้ค่าแอลฟาสัมประสิทธิ์ (α - Coefficient) ในชุดคำถามเกี่ยวกับลักษณะส่วนบุคคล พฤติกรรมการการใช้แพลตฟอร์มออนไลน์ไต้หวัน ความต้องการด้านการจัดการความปลอดภัยระบบสารสนเทศและความคาดหวังด้านการจัดการความปลอดภัยระบบสารสนเทศของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน มีค่าเท่ากับ 0.81 ดังนั้น แบบสอบถามชุดนี้จึงมีความน่าเชื่อถือในระดับสูง

5. นำเครื่องมือที่ทดลองใช้แล้วมาปรับแก้ให้สมบูรณ์ยิ่งขึ้นก่อนนำเครื่องมือไปเก็บรวบรวมข้อมูล
6. จัดพิมพ์เครื่องมือเป็นฉบับจริงและนำไปใช้เก็บรวบรวมข้อมูล

3.2.5 การเก็บรวบรวมข้อมูล

ในส่วนของคุณลักษณะข้อมูล สามารถจำแนกเป็น 2 ลักษณะ ดังนี้

1. ข้อมูลปฐมภูมิ (Primary Data) เป็นข้อมูลที่ได้จากการเก็บรวบรวมด้วยวิธีการเก็บข้อมูลภาคสนามจากประชาชนที่ใช้แพลตฟอร์มออนไลน์ไต้หวัน กลุ่มเป้าหมายที่ได้ตอบแบบสอบถามความต้องการ ความคาดหวังด้านการจัดการความปลอดภัยระบบสารสนเทศของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

2. ข้อมูลทุติยภูมิ (Secondary Data) เป็นข้อมูลที่ได้จากเอกสาร หนังสือ งานวิจัย บทความ ตลอดจนเอกสารอื่นๆ ที่เกี่ยวข้องกับกลยุทธ์ การจัดการ ความต้องการ ความคาดหวัง การพัฒนา และรูปแบบการพัฒนาความปลอดภัยระบบสารสนเทศ

ในการเก็บรวบรวมด้วยวิธีการเก็บข้อมูลจากผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ซึ่งเป็นเทคนิควิธีการที่ต้องใช้และคำนึงถึงในการรวบรวมข้อมูล ผู้วิจัยได้มีการวางแผนงานในการเก็บรวบรวมข้อมูล โดยเก็บรวบรวมข้อมูลจากผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ในพื้นที่กรุงเทพมหานคร 16 เขต ด้วยวิธีการเก็บข้อมูลจากแบบสอบถามตามสะดวก (ดำเนินการแล้วข้อ 3.2.2 วิธีการเลือกตัวอย่าง) ที่กำหนดไว้ให้เป็นตัวแทนผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน รวมจำนวน 400 ตัวอย่าง (คน) ซึ่งประกอบด้วยขั้นตอน

1) ให้มหาวิทยาลัยออกหนังสือขอความอนุเคราะห์และขออนุญาตผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ให้ผู้วิจัยเก็บข้อมูล

2) ให้คณะนิเทศศาสตร์ มหาวิทยาลัยราชภัฏรำไพพรรณี ประกาศแต่งตั้งผู้ช่วยวิจัยประจำพื้นที่แต่ละมณฑล และแต่งตั้งผู้ช่วยวิจัยแต่ละมณฑลละ 4 คน โดยมีผู้วิจัยเป็นหัวหน้าการวิจัย

3) ผู้วิจัยติดต่อประสานงานกับผู้เกี่ยวข้องในพื้นที่การวิจัยทั้ง 4 มณฑล และผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน กลุ่มตัวอย่างเพื่อนัดวัน และเวลาที่เหมาะสมในการแจกแบบสอบถาม

3.2.6 การวิเคราะห์ข้อมูล

หลังจากการรวบรวมแบบสอบถามทั้งหมดที่ผ่านการตอบแบบสอบถามเรียบร้อยแล้ว ผู้วิจัยนำแบบสอบถามทั้งหมดมาดำเนินการ ดังนี้

1. นำแบบสอบถามที่ได้จากการเก็บรวบรวมข้อมูลมาตรวจสอบความสมบูรณ์ก่อนนำไปวิเคราะห์

2. นำแบบสอบถามที่ถูกต้องเรียบร้อยแล้วมาลงรหัสเพื่อประมวลผลข้อมูล

3. นำข้อมูลที่ลงรหัสแล้วมาบันทึกโดยใช้เครื่องคอมพิวเตอร์เพื่อประมวลผลข้อมูล โปรแกรมสำเร็จรูป สำหรับวิเคราะห์ข้อมูลตามสมมติฐานที่ตั้งไว้

โดยเกณฑ์การคำนวณความกว้างของอันตรภาคชั้นมี ดังนี้

$$\begin{aligned} \text{ความกว้างของแต่ละอันตรภาคชั้น} &= \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}} \\ &= \frac{5-1}{5} = 0.8 \end{aligned}$$

ผู้วิจัยได้ดำเนินการแปลความหมายคะแนนเฉลี่ยที่ได้มาจัดระดับความสำคัญเป็น 5 ระดับ ดังนี้

ค่าเฉลี่ยระหว่าง 4.21 - 5.00 หมายถึง อยู่ในระดับมากที่สุด

ค่าเฉลี่ยระหว่าง 3.41 - 4.20 หมายถึง อยู่ในระดับมาก

ค่าเฉลี่ยระหว่าง 2.61 - 3.40 หมายถึง อยู่ในระดับปานกลาง

ค่าเฉลี่ยระหว่าง 1.81 - 2.60 หมายถึง อยู่ในระดับน้อย

ค่าเฉลี่ยระหว่าง 1.00 - 1.80 หมายถึง อยู่ในระดับน้อยที่สุด

3.2.7 สถิติที่ใช้ในการวิเคราะห์

สถิติที่ใช้ในการวิจัยและการวิเคราะห์ข้อมูลเชิงปริมาณ ได้แก่

1. ลักษณะทางประชากรของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน ใช้สถิติความถี่ (Frequency) และค่าร้อยละ (Percentage)
2. ความต้องการของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน เกี่ยวกับการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน ใช้สถิติค่าเฉลี่ย ($\bar{X}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.)
3. ความคาดหวังของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน เกี่ยวกับการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน ใช้สถิติค่าเฉลี่ย ($\bar{X}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.)
4. การทดสอบสมมติฐาน ใช้สถิติ T-test และ F-test เพื่อทดสอบความแตกต่างที่นัยสำคัญทางสถิติ 0.05

3.2.8 การนำเสนอข้อมูล

ผู้วิจัยได้ตรวจสอบความถูกต้อง และความสมบูรณ์ของคำตอบนำไปสู่การวิเคราะห์ข้อมูลด้วยโปรแกรมสำเร็จรูป เพื่อนำเสนอข้อมูลในลักษณะตารางแสดงผล และพรรณนาความตามเนื้อหาที่ได้วิเคราะห์

3.3 การวิจัยคุณภาพ (Qualitative Research)

การศึกษาในขั้นตอนนี้ ใช้วิธีการเชิงคุณภาพ (Qualitative method) โดยมีวิธีดำเนินการวิจัยดังต่อไปนี้

3.3.1 การสัมภาษณ์เชิงลึก (In-depth Interview)

ผู้ให้ข้อมูลสำคัญ หรือผู้ให้ข้อมูลหลัก (Key Informants) ในการสัมภาษณ์เชิงลึก (In-depth Interview) เพื่อให้ได้ข้อมูลเชิงลึกในมิติต่างๆ ที่มีความหลากหลาย โดยผู้วิจัยเลือกเก็บข้อมูลจากตัวแทนดังนี้

1. ภาครัฐ ประกอบด้วย เจ้าหน้าที่ที่ทำหน้าที่สนับสนุนงานนโยบาย และกฎหมายความปลอดภัยข้อมูลส่วนบุคคล การใช้แพลตฟอร์มออนไลน์ รวมทั้งสิ้นจำนวน 3 คน
2. ภาคเอกชน ประกอบด้วย ผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้บริหารระดับกลางปฏิบัติ และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต่ยืน จำนวน 7 คน

เนื่องจากขั้นตอนนี้เป็นารวิจัยเชิงคุณภาพ ผู้ให้ข้อมูลหลักเป็นผู้ที่มีส่วนเกี่ยวข้องในการกำกับดูแลและนโยบายและกฎหมายความปลอดภัยสารสนเทศ และผู้เกี่ยวข้องกับการใช้แพลตฟอร์มออนไลน์และพัฒนาแพลตฟอร์มออนไลน์ไต่ถาม ในพื้นที่ 4 มณฑล รวมทั้งหมด 10 คน ซึ่งได้มาจากการเลือกแบบเจาะจง (Purposive Sampling) อันเป็นการเลือกตัวอย่างผู้ให้ข้อมูลสำคัญที่ผู้วิจัยได้ดำเนินการพิจารณาเลือกผู้ให้สัมภาษณ์จากตัวแทนผู้มีส่วนเกี่ยวข้องกับการกำกับดูแลและนโยบายและกฎหมายความปลอดภัยระบบสารสนเทศ และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต่ถาม ที่มีบทบาทหน้าที่ในการกำกับดูแลนโยบายส่งเสริม/กฎหมายความปลอดภัยระบบสารสนเทศ ผู้เชี่ยวชาญด้านการบริหารจัดการการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ถาม เป็นเกณฑ์คัดเลือก

3.3.2 วิธีการคัดเลือกผู้ให้ข้อมูลสำคัญ

ใช้วิธีการเลือกแบบเจาะจง (Purposeful Selection) เป็นการเลือกแบบไม่มีโครงสร้างที่เคร่งครัด มีขั้นตอนและวิธีการดำเนินการที่ไม่ซับซ้อน จุดมุ่งหมายหลักของการเลือกตัวผู้ให้ข้อมูลหลักที่เป็นผู้ให้ข้อมูลสำคัญ แบบนี้ไม่ใช่เพื่อได้กลุ่มที่เป็นตัวแทน แต่เพื่อที่จะได้ตัวแทนที่เหมาะสมที่สุดเท่าที่จะเป็นไปได้ สำหรับแนวคิด จุดมุ่งหมาย และวัตถุประสงค์ของการศึกษา (ชาย โพธิ์สีตา, 2550) กลุ่มผู้ให้ข้อมูลสำคัญที่เลือกมีลักษณะเป็น “Information-rich case” คือ มีข้อมูลให้ศึกษาในระดับลึกได้มาก และสามารถสะท้อนความเป็นจริงได้ดีที่สุด ซึ่งจะมีความหมายต่อจุดมุ่งหมายหลักของการวิจัย เพื่อให้ได้ผู้ให้ข้อมูลสำคัญที่เหมาะสมกับจุดมุ่งหมายและวัตถุประสงค์ของการวิจัยมากที่สุด โดยมีกระบวนการในการเลือกผู้ให้ข้อมูลสำคัญ ดังนี้

1. ศึกษาข้อมูลจากสำนักงานที่เกี่ยวข้องกับการกำกับดูแลนโยบาย และกฎหมายความปลอดภัยระบบสารสนเทศในกรุงเทพฯ
2. ศึกษาข้อมูลจากบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต่ถาม และผู้บริหารแพลตฟอร์มออนไลน์ไต่ถาม
3. เลือกโดยยึดจุดมุ่งหมายเป็นหลัก โดยผู้ให้ข้อมูลสำคัญต้องเป็นผู้เชี่ยวชาญเกี่ยวกับการบริหารจัดการการความปลอดภัยระบบสารสนเทศแพลตฟอร์มออนไลน์ไต่ถามโดยตรง

3.3.3 เครื่องมือที่ใช้ในการวิจัยเชิงคุณภาพ

ผู้วิจัยได้ดำเนินการวิจัยตามระเบียบวิธีวิจัยเชิงคุณภาพ ผู้วิจัยเก็บรวบรวมข้อมูลคือ ใช้แนวคำถามในการสัมภาษณ์ (Interviewing)

โดยขั้นตอนการสร้างเครื่องมือ ผู้วิจัยสร้างเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเรื่องการพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ถาม ดังนี้

1. ศึกษาข้อมูลพื้นฐาน สภาพพื้นที่ บริบท สิ่งแวดล้อม การสื่อสาร หน่วยงานต่าง ๆ ที่อยู่ในเขตพื้นที่ 4 มณฑล

2. สร้างแนวคำถามในการสัมภาษณ์เพื่อใช้ในการสัมภาษณ์ข้อมูลกับผู้ให้ข้อมูลหลัก ในประเด็นด้านการสื่อสารออนไลน์ ด้านการส่งเสริมความปลอดภัยระบบสารสนเทศ ด้านการวางแผนพัฒนาความปลอดภัยระบบสารสนเทศและ ด้านกลยุทธ์การวางแผนพัฒนาความปลอดภัยระบบสารสนเทศ

3. นำแนวคำถามในการสัมภาษณ์ผ่านการตรวจสอบจากอาจารย์ที่ปรึกษาและแก้ไขปรับปรุงเรียบร้อยแล้ว

4. นำร่างแบบสัมภาษณ์เสนอต่อผู้เชี่ยวชาญด้านการสื่อสารออนไลน์ ด้านการบริหารและด้านการบริหารจัดการความปลอดภัยระบบสารสนเทศ 3 ท่าน คือ 1) รองศาสตราจารย์ ดร. อภิวรรณ ศิรินันทนา 2) รองศาสตราจารย์ ดร.สุภาภรณ์ ศรีดี 3) ผู้ช่วยศาสตราจารย์ ดร.เสาวนีย์ วรรณประภา เพื่อตรวจสอบและพิจารณาความถูกต้องเพื่อปรับปรุงและแก้ไขแนวคำถามในการสัมภาษณ์ แล้วนำเสนอต่อคณะกรรมการจริยธรรมการวิจัยในมนุษย์เพื่อพิจารณาอีกครั้ง เพื่อให้เกิดความสมบูรณ์ตามหลักจริยธรรมการวิจัยในมนุษย์

5. จัดพิมพ์แนวคำถามในการวิจัย และนำแนวคำถามในการวิจัยไปใช้ในการสัมภาษณ์กับกลุ่มผู้ให้ข้อมูลสำคัญต่อไป

3.3.4 การเก็บรวบรวมข้อมูล

การวิจัยครั้งนี้ ผู้วิจัยเป็นผู้เก็บข้อมูลด้วยตนเอง โดยการสัมภาษณ์ผู้ที่มีส่วนเกี่ยวข้อง โดยใช้การสัมภาษณ์แบบเปิดกว้างเป็นการสัมภาษณ์ไม่จำกัดคำตอบเพื่อให้ผู้ให้ข้อมูลหลักซึ่งเป็นผู้ให้ข้อมูลสำคัญตอบคำถามและแสดงความคิดเห็นได้อย่างอิสระ โดยใช้วิธีการเก็บข้อมูลดังนี้

1. การสัมภาษณ์แบบเจาะลึก (In-Depth interview) ใช้การสัมภาษณ์กับผู้ให้ข้อมูลสำคัญ โดยผู้วิจัยได้ทำการลงพื้นที่ทั้ง 4 มณฑล เพื่อไปพบกับกลุ่มผู้ให้ข้อมูลหลักและอธิบายถึงความสำคัญ ความสำคัญ วัตถุประสงค์และประโยชน์ของงานวิจัย อีกทั้งผู้วิจัยได้พูดคุยแบบเป็นกันเองและใช้ภาษาในการสื่อสารที่เข้าใจง่ายเพื่อให้เกิดความเข้าใจที่ตรงกัน นำไปสู่การสร้างความร่วมมือที่ดีในการให้ข้อมูลที่เป็นประโยชน์ต่อการดำเนินการวิจัย จากนั้นผู้วิจัยได้จัดทำตารางการนัดหมายผู้ให้ข้อมูลหลักเพื่อจะทำการสัมภาษณ์ข้อมูลกับกลุ่มผู้ให้ข้อมูลหลักในครั้งต่อไป

2. การวิเคราะห์ข้อมูล ผู้วิจัยจะทำการวิเคราะห์ข้อมูล โดยการวิเคราะห์แบบอุปมัย (Induction Analysis) จากการสัมภาษณ์แบบเจาะลึก (In-Depth Interview) และจากข้อมูลเชิงปริมาณเพื่อนำข้อมูลมาวิเคราะห์และตีความเพื่อสร้างข้อสรุป โดยอาจมีการแบ่งประเภทตามเนื้อหาของข้อมูลที่ได้จากการสัมภาษณ์แล้วเปรียบเทียบเนื้อหาประเภทต่าง ๆ เข้าด้วยกัน

3. การตรวจสอบข้อมูล ในการวิจัยครั้งนี้ผู้วิจัยใช้วิธีการตรวจสอบความน่าเชื่อถือของข้อมูลเพื่อให้เกิดความถูกต้องด้วยวิธีการตรวจสอบแบบสามเส้าด้านวิธีการรวบรวมข้อมูล (Methodological Triangulation) และตรวจสอบข้อมูลสามเส้าด้านแนวคิดทฤษฎี โดยการใช้ข้อมูลที่ได้จากเก็บรวบรวมข้อมูล คือ การสัมภาษณ์แบบเจาะลึก (In-Depth Interview) และการตรวจสอบความ

น่าเชื่อถือของข้อมูลโดยการอธิบายทบทวนข้อมูลหลังจากการสัมภาษณ์เสร็จอีก 1 ครั้ง และการตรวจสอบสามเส้าด้านวิธีการรวบรวมข้อมูล โดยการจัดหมวดหมู่ข้อมูลที่เหมือนกันไว้ในกลุ่มประเภทเดียวกัน และใช้ทฤษฎีทางการสื่อสาร คือ องค์ประกอบทางการสื่อสาร ได้แก่ ผู้ส่งสาร สาร สื่อ ผู้รับสาร ผลสะท้อนกลับ มาวิเคราะห์เชื่อมโยงข้อมูลที่ได้จากการสัมภาษณ์เพื่อเป็นการยืนยันความน่าเชื่อถือของข้อมูล

3.3.5 การนำเสนอข้อมูล

ผู้วิจัยมีการนำเสนอข้อมูลที่ได้จากการสรุปข้อมูลจากการรวบรวมข้อมูลและนำเสนอข้อมูลการวิจัยในรูปแบบเชิงพรรณนา (Descriptive Analysis) จากการสรุปผลการวิจัย อภิปรายผล ข้อเสนอแนะ และนำผลการวิจัยมาใช้ในการพัฒนาเป็น "การพัฒนาแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน" ต่อไป

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

บทที่ 4

ผลการวิเคราะห์ข้อมูล

การศึกษาเรื่อง “กลยุทธ์การพัฒนาการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน” ครั้งนี้มีวัตถุประสงค์ ดังนี้ 1) เพื่อศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน 2) การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน โดยผู้วิจัยขอเสนอผลการวิเคราะห์ข้อมูลตามวัตถุประสงค์ ดังนี้

4.1 ผลการวิเคราะห์ข้อมูล

4.1.1 กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน การศึกษาเรื่องการพัฒนาแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) เจ้าหน้าที่ภาครัฐ ผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้บริหารระดับปฏิบัติการ และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวัน ที่รับผิดชอบการส่งเสริมสนับสนุนหรือการพัฒนาความปลอดภัยระบบสารสนเทศเพื่อสร้างความปลอดภัยของข้อมูล และปกป้องการรั่วไหลของสารสนเทศส่วนบุคคลของแพลตฟอร์มออนไลน์ไต้หวันที่ส่งผลกระทบต่อความนิยมในการใช้แพลตฟอร์มออนไลน์ไต้หวันของประชาชนทั้งในประเทศจีน และประเทศต่าง ๆ ทั่วโลก จำนวน 20 คน ผลการศึกษาพบว่า แพลตฟอร์มออนไลน์ไต้หวัน มีการดำเนินการเชิงกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน 5 กลยุทธ์ ดังนี้

1. กลยุทธ์การกำหนดระบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน
2. กลยุทธ์การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน
3. กลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัยของแพลตฟอร์มออนไลน์ไต้หวัน
4. กลยุทธ์การพัฒนาบุคลากรด้านความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน
5. กลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

1. กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

ผลการศึกษาพบว่า แพลตฟอร์มออนไลน์ไต้หวัน มีการกำหนดการเข้าถึงข้อมูลในรูปของคณะกรรมการความปลอดภัย และสร้างคู่มือให้กับบุคลากรทุกระดับในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน และใช้ชื่อย่อเป็น (InfoSec) เพื่อใช้สื่อความหมายของระบบความปลอดภัยได้อย่างเข้าใจได้ง่ายและสามารถเรียกใช้ระบบได้อย่างสะดวก ระบบการจัดการความปลอดภัยของแพลตฟอร์มออนไลน์ไต้หวันเป็นการกำหนดลักษณะของการรักษาความปลอดภัยออกเป็นขั้นตอน และระบุเครื่องมือในการรักษาความปลอดภัยสารสนเทศที่ช่วยปกป้องข้อมูลสำคัญของ

องค์กรและลูกค้าในวงกว้าง ที่สามารถจับหรือแจ้งเตือนอย่างทันท่วงทีจากการใช้แพลตฟอร์มออนไลน์ไต่ยืนของกลุ่มลูกค้าในทางที่ผิด และการเข้าถึงระบบความปลอดภัยต้องมีระดับขั้นของการเข้าถึง เช่น การเข้าถึงระบบจะต้องเป็นผู้บริหารระดับสูง และเจ้าหน้าที่จะเข้าถึงระบบต้องได้รับการอนุญาตจากคณะกรรมการระบบของมูลของแพลตฟอร์มออนไลน์ไต่ยืน โดยผู้บริหารระดับปฏิบัติการไม่สามารถเข้าถึงระบบได้โดยไม่ได้รับอนุญาตจากคณะกรรมการบริหารแพลตฟอร์มออนไลน์ไต่ยืน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“ด้วยระบบของสื่อออนไลน์ที่รัฐบาลมีการกำหนดอย่างเคร่งครัดในการใช้สื่อออนไลน์เพื่อป้องกันอย่างสูงสุด เอกชนที่ต้องการประกอบอาชีพสื่อหรือพัฒนาสื่อใหม่ขึ้นมาต้องแต่งตั้งเป็นรูปคณะกรรมการที่มีเลขาธิการพรรคประชาชนจีนร่วมเป็นกรรมการ” (Jang dejun, สัมภาษณ์, 20 เมษายน 2568)

การรักษาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน แบ่งเป็นการรักษาความปลอดภัยทางกายภาพและสิ่งแวดล้อมของระบบสารสนเทศ คือมาตรการการควบคุมการเข้าถึงระบบ และการรักษาความปลอดภัยทางไซเบอร์ด้วยเทคโนโลยีของประเทศจีน เช่น ตัวกลางรักษาความปลอดภัยของการเข้าถึงระบบความปลอดภัย (CASB) ระบบเครื่องจับที่หลอกลวง การตรวจหาและการตอบสนองปลายทาง (EDR) และระบบการทดสอบความปลอดภัยสำหรับผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“ความปลอดภัยของเนื้อหาข้อมูลมุ่งเน้นไปที่ความเสียหายการรั่วไหลและการสูญเสียข้อมูลที่อาจได้รับในระหว่างการจัดเก็บการประมวลผลและการส่งผ่านซึ่งเกี่ยวข้องโดยตรงกับการรักษาความลับความสมบูรณ์และความพร้อมใช้งานของข้อมูล (Ju liuly, สัมภาษณ์, 17 เมษายน 2568)

การจัดการภาวะความปลอดภัยสารสนเทศ (Security) เป็นสิ่งจำเป็นที่แพลตฟอร์มออนไลน์ไต่ยืน และผู้พัฒนาระบบแพลตฟอร์มออนไลน์ไต่ยืนซึ่งเป็นพัฒนาการใช้งานในเทคโนโลยีสารสนเทศ ได้ให้ความสำคัญในรูปของข้อมูล ความปลอดภัยของข้อมูล (Data Security) เป็นสิ่งสำคัญสูงสุด การรักษาข้อมูลส่วนบุคคลและการนำไปใช้เป็นที่แพลตฟอร์มออนไลน์ไต่ยืนต้องตระหนัก โดยเมื่อใดมีสิ่งใดคุกคามภาวะความเป็นส่วนตัวของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน โดยมีวัตถุประสงค์เพื่อให้มีข้อมูลพร้อมใช้งาน (Availability) ข้อมูลมีความถูกต้อง (Integrity) รักษาความลับของข้อมูล (Secrecy) และลดความเสี่ยงต่าง ๆ (Risk Assessment) ที่อาจทำให้ข้อมูลเสียหาย ฐานข้อมูลขนาดใหญ่ที่รวบรวมข้อมูลของแพลตฟอร์มออนไลน์ไต่ยืน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“ผู้รับผิดชอบดูแลระบบควรจะทำการป้องกัน การควบคุมการเข้าถึงข้อมูลและป้องกันมิให้ผู้ที่ไม่เกี่ยวข้องเข้าถึงข้อมูล ความปลอดภัยของข้อมูลเป็นการป้องกันผู้ไม่มีสิทธิเข้าใช้หรือแก้ไขข้อมูล การ

ควบคุมความพร้อมกันในการเรียกใช้ข้อมูลเดียวกันรวมถึงการรักษาความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล โดยมีวัตถุประสงค์เพื่อให้มีข้อมูลพร้อมใช้งาน ข้อมูลมีความถูกต้อง รักษาความลับของข้อมูล และลดความเสี่ยงต่าง ๆ ที่อาจทำให้ข้อมูลรั่วไหล ส่งผลเสียต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน” (Sun Liguó, สัมภาษณ์, 30 มีนาคม 2568)

แพลตฟอร์มออนไลน์ไต้หวันเป็นเทคโนโลยีสารสนเทศที่ประชาชนจีนส่วนใหญ่ใช้ในชีวิตประจำวัน พบว่า แพลตฟอร์มออนไลน์ไต้หวันสามารถตอบสนองต่อการติดต่อสารกันระหว่างคนในครอบครัว เพื่อนร่วมงาน และการค้นหาข้อมูลโดยแพลตฟอร์มออนไลน์ไต้หวันได้ออกแบบมาเป็นเครื่องมือสำหรับใช้ค้นหาข้อมูล ซึ่งแพลตฟอร์มออนไลน์ไต้หวันค้นหาข้อมูลโดยผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันสามารถกรอกข้อมูลที่ต้องการค้นหา หรือใส่คำค้นหาต่าง ๆ ลงไปในช่องค้นหาที่อยู่ด้านบนแพลตฟอร์มออนไลน์ไต้หวัน เช่น การเลือกซื้อสินค้า ความบันเทิง อีกทั้งแพลตฟอร์มออนไลน์ไต้หวันยังสามารถเชื่อมต่อกันเป็นเครือข่ายหรือสร้างกลุ่มเฉพาะเพื่อการถ่ายทอดสดที่สามารถพัฒนาเป็นการค้าอิเล็กทรอนิกส์ จากผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันไปสู่ผู้บริโภคที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันได้ กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การพินิจอิเล็กทรอนิกส์ กำลังเป็นที่นิยมมากในหมู่ประชาชนด้วยความก้าวหน้าของอินเทอร์เน็ตทำให้ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน สามารถเป็นผู้ประกอบการได้ การขายค้าผ่านอินเทอร์เน็ตทำให้ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันขายสินค้าได้โดยตรง” (Guo Zengzhe, สัมภาษณ์, 30 มีนาคม 2568)

สรุป ระบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ได้ถูกกำหนดเป็นกลยุทธ์ด้านความปลอดภัยในยุคดิจิทัลเช่นปัจจุบันนี้ นวัตกรรมผ่านการใช้แพลตฟอร์มออนไลน์ไต้หวัน เพื่อเป็นช่องทางส่งผ่านข้อมูลขององค์กรที่พัฒนาแพลตฟอร์มออนไลน์ไต้หวัน ที่ขับเคลื่อนด้วยระบบอินเทอร์เน็ตและใช้ปัญญาประดิษฐ์ AI ก่อให้เกิดศักยภาพที่เป็นประโยชน์มากมายมหาศาลต่อการสื่อสารต่อสังคม ต่อเศรษฐกิจ อย่างไรก็ตามความพยายามในการรักษาความปลอดภัยระดับองค์กรของแพลตฟอร์มออนไลน์ไต้หวัน และจัดการกับภัยคุกคามทางไซเบอร์มีความท้าทายเพิ่มมากขึ้น ส่งผลให้ผู้บริหารทุกระดับของแพลตฟอร์มออนไลน์ไต้หวัน ผู้ดูแลและพัฒนาระบบแพลตฟอร์มออนไลน์ไต้หวัน จำเป็นต้องต้องสร้างสมดุลระหว่างความก้าวหน้าทางเทคโนโลยี และเทคโนโลยี AI นำเสนอผ่านแพลตฟอร์มออนไลน์ไต้หวัน กับความคาดหวังและความต้องการความปลอดภัยของระบบสารสนเทศของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ที่สำคัญในการรักษาความปลอดภัยข้อมูล แอปพลิเคชัน และผู้ใช้

2. กลยุทธ์การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

ผลการศึกษาพบว่า การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันในยุคดิจิทัลปัจจุบัน การจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ถือเป็นสิ่งสำคัญสำหรับแพลตฟอร์มออนไลน์ไต้หวันในการปกป้องข้อมูลที่ละเอียดอ่อน รักษาการปฏิบัติตามข้อกำหนดและรับรองความต่อเนื่องในการดำเนินงาน ด้วยความซับซ้อนและความถี่ของภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้น ผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน ใช้แนวทางเชิงรุกเพื่อระบุความไม่ปลอดภัย ประเมินความไม่ปลอดภัย และลดความเสี่ยงที่จะเกิดความไม่ปลอดภัยจากการใช้สารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างมีประสิทธิภาพ ด้วยการนำกรอบงานด้านความปลอดภัยทางไซเบอร์ที่แข็งแกร่ง เช่น กรอบงานด้านความปลอดภัยทางไซเบอร์ของ NIST หรือกรอบงาน ISO 27001 ซึ่งเป็นกรอบงานที่เป็นมาตรฐานระดับสากลที่ทั่วโลกยอมรับโดยนำมาใช้ในบทบาทของการกำหนดเป้าหมายความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ซึ่งเป็นกระบวนการสำคัญหลักในการรักษาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน โดยกำหนดให้เป็นแนวทางมาตรฐานในการจัดการภัยคุกคามอย่างเป็นระบบ กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“สิ่งสำคัญในการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ของแพลตฟอร์มออนไลน์ไต้หวัน รวมถึงกรอบการทำงานหลัก กระบวนการประเมินความเสี่ยงทางไซเบอร์ และแนวทางปฏิบัติที่ดีที่สุดใน การลดความเสี่ยง การทำความเข้าใจและนำมาตรฐานความปลอดภัยเหล่านี้ไปใช้ถือเป็นสิ่งสำคัญในการเสริมความแข็งแกร่งให้กับแพลตฟอร์มออนไลน์ไต้หวันในการรับมือกับการโจมตีทางไซเบอร์ที่อาจเกิดขึ้น” (Zhu Jiang, สัมภาษณ์, 28 เมษายน 2568)

การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน พบว่า เริ่มจากการประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ซึ่งผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน กำหนดให้เป็นแนวทางปฏิบัติว่าการประเมินความเสี่ยงทางไซเบอร์นั้นถือเป็นสิ่งสำคัญอันดับต้น ๆ ในการทำความเข้าใจความเสี่ยงต่อระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และให้ทุกหน่วยงานในองค์กรไต้หวันดำเนินมาตรการความปลอดภัยระบบสารสนเทศที่เคร่งครัด และมีความเหมาะสมเพื่อปกป้องระบบสารสนเทศ และพบว่า กระบวนการประเมินความเสี่ยงทางไซเบอร์นี้ของแพลตฟอร์มออนไลน์ไต้หวัน อยู่ในแผนที่กำหนดเป้าหมายความปลอดภัยไว้ว่าต้องดำเนินการตามระบบของการประเมินความเสี่ยงทางไซเบอร์ เพื่อใช้ประเมินอย่างเป็นระบบเพื่อแก้ไขปัญหาความปลอดภัยทางไซเบอร์ หรือช่วยบรรเทาภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ด้านล่างนี้คือขั้นตอนสำคัญในการประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์โดยละเอียด กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

“ขั้นตอนแรกในกระบวนการประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ของแพลตฟอร์มออนไลน์ไต้หวัน คือการระบุช่องโหว่ที่สำคัญขององค์กร รวมถึงฮาร์ดแวร์ ซอฟต์แวร์ ทรัพยากรทางปัญญา ข้อมูล เครือข่าย และบุคลากรที่จำเป็นต่อการดำเนินการจัดการความปลอดภัยสารสนเทศ” (Qui Yu, สัมภาษณ์ 23 มีนาคม 2568)

ปัจจุบันผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน มีการกำหนดเป้าหมายความปลอดภัยสารสนเทศอยู่ในแผนการบริหารความเสี่ยงทางไซเบอร์ ที่ใช้ในการบริหารสื่อสารไปถึงผู้บริหารทุกระดับรวมถึงระดับปฏิบัติการ การกำหนดเป้าหมายความปลอดภัยถือเป็นหัวใจสำคัญที่ช่วยกำหนดทิศทางการจัดการความปลอดภัยสารสนเทศที่ชัดเจน ช่วยให้แพลตฟอร์มออนไลน์ไต้หวัน สามารถสื่อสารกับกลุ่มเป้าหมายที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ได้อย่างตรงจุด และบรรลุเป้าหมายที่วางไว้ได้ คือผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน เกิดความเชื่อมั่นในความปลอดภัยของข้อมูลส่วนบุคคลของตนเอง กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“เพื่อให้แผนการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน สามารถสื่อสารสร้างผลลัพธ์ที่ดีที่สุดให้กับลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน จำเป็นต้องหลีกเลี่ยงข้อผิดพลาดที่อาจเกิดขึ้นในกระบวนการสื่อสารกับทุกคนในองค์กร ซึ่งจะช่วยให้กลยุทธ์การจัดการความปลอดภัยสารสนเทศสามารถตอบสนองต่อความต้องการของกลุ่มเป้าหมายได้อย่างมีประสิทธิภาพยิ่งขึ้น” (Li Shiyong, สัมภาษณ์ 28 กุมภาพันธ์ 2568)

กำหนดวัตถุประสงค์ของการเป้าหมายความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน พบว่า มีเป้าหมายความปลอดภัยที่ชัดเจน เช่น มาตรการแจ้งข้อมูล สร้างความเข้าใจในเรื่องความปลอดภัยของสารสนเทศของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ทำให้แพลตฟอร์มออนไลน์ไต้หวันเป็นที่ยอมรับในการเป็นแพลตฟอร์มการสื่อสารที่มีมาตรฐานการรักษาความปลอดภัยในระดับสากล และพบว่าการกำหนดเป้าหมายความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันนอกจากจะทำให้ผู้ใช้เกิดความเชื่อมั่นต่อระบบความปลอดภัยแล้ว ยังทำให้แพลตฟอร์มออนไลน์ไต้หวันสามารถรู้จักกลุ่มเป้าหมาย จากการระบุกลุ่มคนที่แพลตฟอร์มออนไลน์ไต้หวันต้องการสื่อสารด้วย เช่น ทีมงาน ลูกค้า หรือผู้ถือหุ้น เพื่อให้การสื่อสารมีความหมายและตอบโจทย์ธุรกิจของแพลตฟอร์มออนไลน์ไต้หวันได้เป็นอย่างดี กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“แพลตฟอร์มออนไลน์ไต้หวันเลือกช่องทางหรือรูปแบบการสื่อสารที่เป็นเป้าหมายความปลอดภัยของสารสนเทศ โดยเลือกวิธีที่เหมาะสมกับกลุ่มเป้าหมาย เช่น การใช้สื่อออนไลน์สำหรับกลุ่มลูกค้า หรือการประชุมภายในสำหรับพนักงาน เพื่อให้การสื่อสารเรื่องมาตรฐานความปลอดภัยของข้อมูลมีประสิทธิภาพและเข้าใจได้ง่าย” (Zhang Jianwei, สัมภาษณ์ 25 กุมภาพันธ์ 2568)

สรุป การจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศทางไซเบอร์ถือเป็นสิ่งสำคัญสำหรับแพลตฟอร์มออนไลน์ไต้หวัน ในการปกป้องข้อมูลที่ละเอียดอ่อนของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน การปฏิบัติตามข้อกำหนด และรับรองความต่อเนื่องในการดำเนินงาน ด้วยความซับซ้อนและความถี่ของภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้น ผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน จึงใช้แนวทางเชิงรุกเพื่อระบุนิ่วความปลอดภัย ประเมินความไม่ปลอดภัย และลดความเสี่ยงที่จะเกิดความปลอดภัยจากการใช้สารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างมีประสิทธิภาพ ด้วยการนำกรอบงานด้านความปลอดภัยทางไซเบอร์ที่เป็นมาตรฐานสากลที่ได้รับการยอมรับทั่วโลกมาใช้เพื่อรักษาความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างจริงจัง

3. กลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัยของแพลตฟอร์มออนไลน์ไต้หวัน

ผลการศึกษาพบว่า แพลตฟอร์มออนไลน์ไต้หวัน ซึ่งเป็นสื่อดิจิทัลได้กลายเป็นส่วนหนึ่งของชีวิตประจำวันของประชาชนชาวจีน ผู้ใช้งานแพลตฟอร์มออนไลน์ไต้หวัน ต้องเผชิญกับความท้าทายและความเสี่ยงจากการใช้แพลตฟอร์มออนไลน์ไต้หวัน เพิ่มมากขึ้นทั้งความน่าเชื่อถือของเนื้อหา การเผยแพร่ข้อมูลเท็จ บิดเบือน ข้อมูลที่ปลุกปั่นความรุนแรง ความเกลียดชัง การละเมิดสิทธิบุคคล ความโปร่งใส รวมไปถึงอิทธิพลของแพลตฟอร์มในการกำหนดการเข้าถึงเนื้อหา ปัญหาความปลอดภัยของแพลตฟอร์มออนไลน์ไต้หวัน ที่ประเทศจีนพยายามแก้ไขเพื่อคุ้มครองผู้ใช้งานดิจิทัล โดยออกกฎหมาย Digital Services Act เพื่อใช้เป็นแนวทางในการกำกับดูแลแพลตฟอร์มที่ชัดเจน โดยเน้นการคุ้มครองความปลอดภัยของผู้ใช้และเสริมสร้างความโปร่งใสในแพลตฟอร์มดิจิทัลต่าง ๆ กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“เมื่อสถานการณ์ด้านสื่อออนไลน์ทั่วโลกมีการขยับ แน่นนอนว่าแพลตฟอร์มออนไลน์ไต้หวันจะต้องขยับตามให้เท่าทันกับสถานการณ์ และภูมิทัศน์ของแพลตฟอร์มดิจิทัลที่เปลี่ยนแปลงไปในขณะเดียวกันจะต้องสร้างเครือข่ายความรู้ แลกเปลี่ยนประสบการณ์การกำกับดูแล รวมทั้งกำหนดแนวทางเพื่อส่งเสริมการบังคับใช้กฎหมายให้สอดคล้องกับบริบทของประเทศจีน” (Li Shiyou, สัมภาษณ์ 28 กุมภาพันธ์ 2568)

แพลตฟอร์มออนไลน์ไต้หวัน ซึ่งเป็นผู้พัฒนาแพลตฟอร์มออนไลน์ชั้นนำของจีน ร่วมกับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ของรัฐบาลจีนที่กำกับดูแลสื่อออนไลน์ ได้จัดงานแลกเปลี่ยน ถ่ายทอดองค์ความรู้ สร้างเครือข่ายเกี่ยวกับแนวทางกำกับดูแล และการบังคับใช้กฎหมายการกำกับดูแลบริการดิจิทัลในประเทศเพื่อลดความเสี่ยงต่อผู้ให้บริการดิจิทัล ภายใต้โครงการประเมินผลสัมฤทธิ์และวิเคราะห์ผลกระทบของกฎหมาย ซึ่งจัดขึ้นเป็นประจำทุกปี โดยมีผู้แทนหน่วยงานภาครัฐที่เกี่ยวข้องกับการกำกับดูแลแพลตฟอร์มดิจิทัล ภาคประชาสังคม และภาคเอกชนที่สนใจเข้าร่วม กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“ทางการจีนมีนโยบายที่เข้มงวดเกี่ยวกับสื่อทุกประเภทการกำหนดการควบคุมผลกระทบจากการใช้สื่อออนไลน์ยังมีความสำคัญเพราะสามารถแพร่กระจายข่าวสารได้อย่างรวดเร็วที่อาจส่งผลกระทบต่อสังคมโดยรวมมากกว่าสื่ออื่นๆ ในฐานะผู้บริหารไต้หวันจึงต้องมึนโยบายความคุมโดยการกำกับดูแลการใช้แพลตฟอร์มให้เป็นไปตามกฎหมายเป็นอย่างดี” (Qi Guannan, สัมภาษณ์, 24 เมษายน 2568)

รัฐบาลจีนมีกฎหมายกำกับดูแลสื่อสังคมออนไลน์โดยเฉพาะ และมีวิธีการความรับผิดชอบทางการละเมิดข้อกฎหมายที่ค่อนข้างเฉียบขาดในการกำกับดูแลเนื้อหาบนแพลตฟอร์ม โดยพบว่าในประเทศจีนมีการผลักดันให้แพลตฟอร์มต้องเปิดเผยนโยบายการกลั่นกรองเนื้อหา รวมทั้งให้แพลตฟอร์มมีช่องทางให้ผู้ใช้งานสามารถร้องเรียนเนื้อหาที่ผิดกฎหมายหรือเป็นอันตรายได้ และผู้ใช้งานสามารถโต้แย้งได้หากเนื้อหาถูกลบทิ้งโดยแพลตฟอร์ม และพบว่าห้ามแพลตฟอร์มจำกัดเนื้อหาหากเป็นการแสดงออกโดยสุจริตในทางสังคม วัฒนธรรม เศรษฐกิจ ฯลฯ ยกเว้นเรื่องการเมือง ดังนั้นแพลตฟอร์มออนไลน์ไต้หวัน จึงมีกฎระเบียบที่เป็นนโยบายในการกำกับดูแลความปลอดภัยที่ชัดเจนในการใช้แพลตฟอร์มออนไลน์ไต้หวัน ที่มุ่งปกป้องความปลอดภัยผู้ใช้งาน การปกป้องสิทธิขั้นพื้นฐานของบุคคล องค์กร โดยการการส่งเสริมความโปร่งใสและความรับผิดชอบของออนไลน์แพลตฟอร์มออนไลน์ไต้หวัน โดยให้ความสำคัญเป็นพิเศษกับการปกป้องข้อมูลเกี่ยวกับเด็กและเยาวชน และความโปร่งใสในการเสนอเนื้อหาผ่านแพลตฟอร์มออนไลน์ไต้หวัน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การสมัครใช้แพลตฟอร์มออนไลน์ไต้หวัน จะมีขั้นตอนบังคับให้ผู้สมัครต้องเข้าไปดูไปอ่านนโยบายของแพลตฟอร์มให้เข้าใจอย่างชัดเจนก่อนการสมัครใช้ว่ามีข้อกำหนดอะไรที่ทำได้ทำไม่ได้ และแพลตฟอร์มออนไลน์ไต้หวันยังระบุข้อความที่เป็นกฎหมายเรื่องความปลอดภัยของข้อมูลส่วนบุคคลอีกด้วย” (Zhang Jianwei, สัมภาษณ์ 25 กุมภาพันธ์ 2568)

การกำหนดนโยบายการกำกับดูแลความปลอดภัยของแพลตฟอร์มออนไลน์ไต้หวัน พบว่าเป็นประเด็นที่ได้รับความสนใจอย่างกว้างขวางจากผู้ใช้งานแพลตฟอร์มออนไลน์ คือบทบาทและอิทธิพลของแพลตฟอร์มออนไลน์ไต้หวันต่อผู้ใช้หลายพันล้านคนทั่วโลก ทั้งในการเพิ่มการมองเห็นของคอนเท้นท์และการจำกัดการมองเห็น และยังมีข้อถกเถียงถึงความรับผิดชอบของแพลตฟอร์มหากมีการเผยแพร่ข้อมูลเท็จว่าแพลตฟอร์มต้องรับผิดชอบด้วย อย่างไรก็ตามแพลตฟอร์มออนไลน์ไต้หวันที่ใช้อยู่ในหลายประเทศต่างมีกฎหมายเพื่อสร้างความโปร่งใสให้กับการตัดสินใจของบริหารแพลตฟอร์ม แต่การบังคับใช้กฎหมายความปลอดภัยทางไซเบอร์ยังคงเป็นเรื่องที่ท้าทาย รวมถึง

ความร่วมมือระหว่างประเทศมีความสำคัญต่อการแก้ไขปัญหาด้วยเช่นกัน เพราะเป็นเรื่องซับซ้อนเกินกว่าที่จะแก้ไขปัญหาได้โดยประเทศใดประเทศหนึ่ง ดังนั้นการแบ่งปันข้อมูล ความเชี่ยวชาญของบุคลากรร่วมกันจึงจะสร้างความปลอดภัยได้ และการดำเนินการจะให้เกิดประสิทธิภาพได้นั้นจะต้องอาศัยทรัพยากร รวมทั้งนวัตกรรม กรณีดังกล่าวยังสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“แพลตฟอร์มออนไลน์ต้องอาศัยความร่วมมือจากหลายฝ่ายทั้งในประเทศและต่างประเทศ และผู้เชี่ยวชาญด้านกฎหมายและเศรษฐกิจดิจิทัล นำเสนอแนวทางการพิจารณาการกำกับดูแลโดยมุ่งเน้นสร้างความสมดุลระหว่างนวัตกรรม และการกำหนดกฎเกณฑ์ ซึ่งการที่จะออกกฎหมายมากำกับแพลตฟอร์มนั้น จะต้องดูลักษณะของแพลตฟอร์ม และการบังคับใช้กฎหมายว่าสามารถทำได้จริงหรือไม่เป็นหลัก” (Wang Yuanyuan, สัมภาษณ์, 29 มีนาคม 2568)

สรุป หลักการและนโยบายของแพลตฟอร์มออนไลน์ไต้หวัน ตระหนักถึงการใช้สื่อสังคมออนไลน์ที่แพร่หลาย และผลกระทบที่อาจเกิดขึ้นทั้งประโยชน์และโทษ โดยเฉพาะหากมีการเผยแพร่ข้อมูลที่ไม่เหมาะสมออกสู่สาธารณะ ซึ่งอาจก่อให้เกิดความเสียหายต่อตนเอง ผู้อื่น และองค์กร นโยบายของแพลตฟอร์มออนไลน์ไต้หวัน จึงจัดทำขึ้นเพื่อให้การใช้แพลตฟอร์มออนไลน์ไต้หวันของประชาชน มีความเหมาะสม เป็นประโยชน์ และหลีกเลี่ยงผลกระทบต่อสังคม และการดำเนินงานของแพลตฟอร์มออนไลน์ไต้หวันในอนาคต

แพลตฟอร์มออนไลน์ไต้หวัน กำหนดนโยบายและแนวปฏิบัติที่เหมาะสมต่อการดำเนินงานตามวัตถุประสงค์ ปณิธาน พันธกิจ ของแพลตฟอร์ม โดยคำนึงถึงสิทธิและเสรีภาพอย่างมีขอบเขตในการแสดงความคิดเห็นของประชาชนผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

แพลตฟอร์มออนไลน์ไต้หวัน ส่งเสริมให้ใช้สื่อสังคมออนไลน์เพื่อการเรียนรู้ การแลกเปลี่ยนความรู้ การเสริมสร้างปฏิสัมพันธ์ทางสังคม วัฒนธรรม การท่องเที่ยว วิชาการ ฯลฯ และการเผยแพร่ข้อมูลหรือข้อคิดเห็นทางความคิดเชิงสร้างสรรค์ ที่ไม่ขัดต่อศีลธรรมอันดีของประชาชนจีน ธรรมเนียมปฏิบัติของสังคม

แพลตฟอร์มออนไลน์ไต้หวัน ไม่จำกัดสิทธิและเสรีภาพในการใช้สื่อแพลตฟอร์มออนไลน์ไต้หวัน แต่ผู้ใช้อาจต้องตระหนักถึงสถานภาพความเป็นประชาชนจีนที่มีหน้าที่ในการรักษาวินัย จรรยาบรรณ รวมถึงการรักษาเกียรติและความน่าเชื่อถือทั้งของตนเอง ของสถาบันทางสังคม และประเทศ

4. กลยุทธ์การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

ผลการศึกษาด้านการพัฒนาบุคลากรด้านความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน พบว่า การส่งเสริมความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ให้ประสบความสำเร็จได้นั้น ต้องให้ความสำคัญต่อการพัฒนาบุคลากรมีปฏิบัติงานด้านความปลอดภัยสารสนเทศที่เกี่ยวข้องในทุกระดับ ตั้งแต่เจ้าหน้าที่รัฐที่กำกับดูแลงานส่งเสริมพัฒนาความปลอดภัยระบบสารสนเทศของสื่อสังคม

ออนไลน์ ผู้บริหารแพลตฟอร์มออนไลน์ บล็อกเกอร์ และผู้พัฒนาแพลตฟอร์มออนไลน์ไต่ยน ซึ่งการศึกษาพบว่า การพัฒนาบุคลากรด้านการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยน เป็นกลไกสำคัญที่จะนำไปสู่ความสำเร็จในการพัฒนาระบบความปลอดภัยของข้อมูล ซึ่งหากแพลตฟอร์มออนไลน์ไต่ยน มีบุคลากรด้านความปลอดภัยระบบสารสนเทศแพลตฟอร์มออนไลน์ไต่ยน ที่มีศักยภาพ คุณภาพ และคุณธรรมจริยธรรมที่สูง จะเกิดผลดีและจะสามารถพัฒนาระบบความปลอดภัยระบบสารสนเทศให้เข้าไปสู่ความสามารถในการแข่งขันด้านการให้บริการแพลตฟอร์มออนไลน์ไต่ยนที่สูง เพื่อดึงดูดผู้ใช้แพลตฟอร์มออนไลน์ไต่ยนต่างๆ ทั้งภายในประเทศ และต่างประเทศที่ต้องการแพลตฟอร์มออนไลน์ไต่ยนที่ใช้งานง่าย สะดวกและมีระบบการรักษาความปลอดภัยระบบสารสนเทศให้สนใจและใช้แพลตฟอร์มออนไลน์ไต่ยน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยน ต้องทำเป็นกระบวนการที่มุ่งจะพัฒนาบุคลากรทุกระดับให้มีความรู้ด้านการรักษาความปลอดภัยระบบสารสนเทศ ทักษะการให้บริการที่มีคุณภาพ และทัศนคติที่ดีต่อการให้บริการต่อผู้ใช้แพลตฟอร์มออนไลน์ไต่ยนอย่างเหมาะสม เพื่อเพิ่มประสิทธิภาพในการทำงานด้านบริการความปลอดภัยระบบสารสนเทศ และให้มีความรู้สามารถปรับปรุง ดูแลระบบสารสนเทศเข้ากั้งงานด้านความปลอดภัยระบบสารสนเทศที่อาจเจอผู้ใช้แพลตฟอร์มออนไลน์ไต่ยนที่มีความหลากหลายทั้งอารมณ์ และความต้องการที่อาจเปลี่ยนแปลงไปมาได้ ส่งผลให้ลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต่ยนเกิดความประทับใจ” (Maynur, สัมภาษณ์, 28 เมษายน 2567)

กลยุทธ์การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยนพบว่า เป็นกระบวนการวางแผนให้เป็นไปตามกฎหมายความปลอดภัยสารสนเทศ และนโยบายด้านความปลอดภัยของระบบสารสนเทศที่กำหนดอย่างเป็นระบบของหน่วยงานภาครัฐโดยรัฐบาลกลางจีน ที่ให้ภาคเอกชนที่เป็นผู้ประกอบการแพลตฟอร์มออนไลน์ไต่ยน และผู้พัฒนาแพลตฟอร์มออนไลน์ไต่ยน ต้องทำการพัฒนาศักยภาพบุคลากรที่เกี่ยวข้องกับความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยน และแพลตฟอร์มออนไลน์ไต่ยนทุกประเภท ทุกระดับให้สูงขึ้น โดยอาศัยเทคโนโลยีสารสนเทศยุคใหม่ทำให้การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยน ได้อย่างสะดวกรวดเร็ว และพัฒนาได้อย่างกว้างขวางครอบคลุมทุกฟังก์ชันการใช้งานแพลตฟอร์มออนไลน์ไต่ยน ด้วยเทคโนโลยีสารสนเทศยุคใหม่ที่มีศักยภาพทำให้การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศสามารถดำเนินการพัฒนาได้อย่างต่อเนื่องและมีประสิทธิภาพเพราะสามารถพัฒนาบุคลากรด้านความปลอดภัยของระบบสารสนเทศในรูปแบบออนไลน์ และรูปแบบออนไซต์ที่บุคลากรสามารถเรียนรู้ พัฒนาได้ตลอดเวลา กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การพัฒนาคุณลักษณะบุคลากรด้านการท่องเที่ยวเชิงสร้างสรรค์ ต้องมุ่งเน้นด้านความรู้ บุคลากรต้องมีความรู้ความเข้าใจในมรดกทางวัฒนธรรม ทรัพยากรการท่องเที่ยวต่างๆ ของชุมชนทำให้สามารถปฏิบัติงานตามหน้าที่ที่กำหนดไว้ในบทบาทของบุคลากรด้านการท่องเที่ยว คือต้องมีความรู้ทั้งศาสตร์และศิลป์ทางด้านการท่องเที่ยวและบริการ และเข้าใจพฤติกรรมนักท่องเที่ยวที่หลากหลาย ประสพการณ์การทำงาน ความรู้รอบตัวทักษะการสื่อสารในงานทั้งการอ่าน การพูด และการเขียน การสื่อสารภาษาต่างประเทศ มีมนุษยสัมพันธ์ทำงานเป็นทีม มีไหวพริบ แก้ปัญหาเฉพาะหน้าได้ดี มีทัศนคติที่ดี ต้องมีใจรักงานบริการ มีความรักในชุมชนท้องถิ่นหรือองค์กรและเพื่อนร่วมงาน เพื่อการพัฒนาตนเอง ในการต่อยอดความได้เปรียบด้วยการบริการมีประสิทธิภาพ และได้มาตรฐานระดับสากล” (Jia Shixin, สัมภาษณ์, 29 เมษายน 2568)

ผู้ให้บริการแพลตฟอร์มออนไลน์โตύν โดยปกติแล้วถ้าต้องการใช้บริการออนไลน์จากแพลตฟอร์มออนไลน์โตύν ซึ่งความต้องการพื้นฐานของผู้ใช้บริการแพลตฟอร์มออนไลน์โตύν พบว่า ต้องการแพลตฟอร์มออนไลน์ที่จะใช้งาน ผู้ใช้สามารถทำได้ทันทีที่ต้องการ มีความเชื่อถือได้ ง่ายต่อการใช้และการเรียนรู้ มีบริการที่มีใช้แพร่หลาย รวดเร็ว และประหยัด เป็นต้น โดยปกติแพลตฟอร์มออนไลน์โตύνมีบริการเสริมอื่น ๆ อีก เช่น สามารถติดต่อได้ง่ายจากแพลตฟอร์มออนไลน์ที่อยู่ในโทรศัพท์ มีบริการคอลเซ็นเตอร์ที่คอยรับเรื่องราวเกี่ยวกับการแก้ไขปัญหาด้านความปลอดภัยหรือบริการอื่น ๆ ที่ผู้ใช้แพลตฟอร์มสามารถติดต่อได้ตลอด 24 ชั่วโมง และพบว่า บริการด้านความปลอดภัยของข้อมูลเหล่านี้เป็นกลยุทธ์การบริการพื้นฐานที่แพลตฟอร์มออนไลน์โตύνให้ความสำคัญเป็นอย่างมากและจะต้องมี กรณีดังกล่าวสอดคล้องกับให้สัมภาษณ์ที่ว่า

“แพลตฟอร์มออนไลน์โตύνมีการบริหารที่เป็นเอกชนภายใต้การกำกับของรัฐ เป็นกิจการประเภทธุรกิจที่เกี่ยวข้องกับข้อมูลลูกค้า ข้อมูลองค์กรที่เป็นลูกค้าของเรา การพัฒนาบุคลากรเป็นบทบาทที่ต้องส่งเสริมและพัฒนาทักษะการทำงานอยู่แล้วและยังต้องพัฒนาบุคคลด้านความปลอดภัยระบบสารสนเทศให้รู้ข้อกฎหมายที่เกี่ยวข้องและติดตามเทคโนโลยีสื่อสารตลอดเวลา” (Lu Yangjing สัมภาษณ์, 16 เมษายน 2568)

การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์โตύν จำเป็นต้องให้ความสำคัญกับนโยบาย และกฎหมายที่เกี่ยวข้องกับความปลอดภัยระบบสารสนเทศ และคำนึงถึงสิทธิส่วนบุคคลที่ต้องได้รับปกป้อง และป้องกันความเสียหายที่มีต่อองค์กร และประชาชนผู้ใช้แพลตฟอร์มออนไลน์โตύν นอกจากนี้การพัฒนาระบบสารสนเทศเพื่อความปลอดภัยยังควรให้ความสำคัญกับอุตสาหกรรมต่าง ๆ ที่มีส่วนสำคัญต่อการการพัฒนาแพลตฟอร์มออนไลน์โตύν และยักรวมถึงหน่วยงานภาครัฐ เอกชนและประชาชน ที่เป็นผู้มีส่วนได้ส่วนเสียที่สำคัญในการพัฒนาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์โตύν การพัฒนาบุคลากรซึ่งเป็นทรัพยากรสำคัญใน

การขับเคลื่อนงานด้านความปลอดภัยระบบสารสนเทศเพื่อสนับสนุนการดำเนินกิจกรรมทางธุรกิจของแพลตฟอร์มออนไลน์ไต้ยีน จำเป็นต้องเน้นในกระบวนการเกี่ยวกับการพัฒนาบุคลากรให้มีความรู้ความเข้าใจในสิทธิส่วนบุคคล นโยบายภาครัฐ กฎหมายที่เกี่ยวข้อง การสื่อสารข้อมูลผ่านสื่อออนไลน์ประเภทต่าง ๆ และปัจจัยอื่นๆ เพื่อให้บรรลุความสำเร็จในการพัฒนาด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน ดังนั้นการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศ จึงมีความสำคัญ พบว่า ของแพลตฟอร์มออนไลน์ไต้ยีนมีกลยุทธ์ในการกำหนดขอบเขตของการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศครอบคลุม 3 ส่วน ดังนี้

1) การฝึกอบรม (Training) เป็นแผนงานที่หน่วยงานภาครัฐ ภาคเอกชน และภาควิชาการ ซึ่งมีบทบาทหน้าที่หรือพันธกิจที่ต้องรับผิดชอบในการพัฒนาระบบสารสนเทศให้เกิดความปลอดภัยให้เกิดขึ้นในขอบเขตที่ต้องรับผิดชอบ โดยจัดขึ้นเพื่อส่งเสริมการเรียนรู้เพื่อพัฒนาบุคลากรที่กำลังปฏิบัติงานด้านความปลอดภัยระบบสารสนเทศอยู่ในปัจจุบัน และหน่วยงานภาครัฐเป็นผู้สนับสนุนให้เกิดการพัฒนาบุคลากร ให้กับแพลตฟอร์มออนไลน์ไต้ยีน โดยใช้บุคลากรภาควิชาการด้านนโยบาย และกฎหมายความปลอดภัยทางไซเบอร์ภายใต้หัวข้อหรือหลักสูตรความปลอดภัยระบบสารสนเทศของรัฐบาลจีน เพื่อใช้ฝึกอบรมให้ผู้ประกอบเจ้าของแพลตฟอร์ม และผู้พัฒนาแพลตฟอร์มออนไลน์ไต้ยีน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“มีการจัดการเรียนการสอนระบบสารสนเทศและการรักษาความปลอดภัย และการอบรมอยู่ในสถานศึกษาทั้งภาครัฐและภาคเอกชนซึ่งเป็นหลักสูตรที่ผู้บริหารผู้พัฒนาแพลตฟอร์มออนไลน์ไต้ยีนต้องพัฒนาและจัดให้มีบุคลากรด้านความปลอดภัยสารสนเทศ ซึ่งบางแห่งอาจจัดตั้งเป็นแผนกงานรับผิดชอบโดยตรงด้วยซ้ำ” (Nie Songtao, สัมภาษณ์, 18 เมษายน 2568)

2) การศึกษา (Education) เป็นกระบวนการที่หน่วยงานภาครัฐ ภาคเอกชนที่เกี่ยวข้องกับการส่งเสริมหรือพัฒนาบุคลากรด้านสารสนเทศให้มีความรู้อย่างลึกซึ้งผ่านกระบวนการศึกษาความปลอดภัยระบบสารสนเทศ ในการเตรียมการพัฒนาผู้ที่มาทำงานด้านความปลอดภัยระบบสารสนเทศให้มีความพร้อมด้านความรู้ ความสามารถ และทักษะเกี่ยวกับการจัดการความปลอดภัยระบบสารสนเทศและการสื่อสารในอนาคต การศึกษาการฝึกอบรมด้านความปลอดภัยระบบสารสนเทศและการสื่อสารนอกจากจะทำให้เกิดความรู้ในการนำมาใช้บริหารจัดการระบบสารสนเทศและการสื่อสารท่องเที่ยวและพัฒนาตนได้แล้ว สิ่งนี้ยังสามารถเป็นตัวกำหนดทิศทางของการพัฒนาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีนได้อีกด้วย เพราะหากมีการส่งเสริมการศึกษา การฝึกอบรมด้านความปลอดภัยระบบสารสนเทศและการสื่อสารไปในทิศทางที่ถูกต้อง ย่อมทำให้แพลตฟอร์มออนไลน์ไต้ยีน นั้นมีต้นทุนที่เป็นทรัพยากรมนุษย์ที่มีศักยภาพในการร่วมกันสร้างแพลตฟอร์มออนไลน์ไต้ยีนให้เป็นแพลตฟอร์มออนไลน์เชิงสร้างสรรค์ที่มีคุณภาพสูง กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การพัฒนาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีนต้องอาศัยทรัพยากรบุคคลที่เป็นปัจจัยสำคัญที่สุดต่อการพัฒนาองค์กรด้านการสื่อสารออนไลน์ ไปจนถึงการพัฒนา

สังคม และประเทศ การที่จะสร้างบุคลากรที่มีคุณภาพขึ้นมาในองค์กรไต้หวัน ในสังคมได้นั้น หนึ่งในปัจจัยสำคัญก็คือ การศึกษาสำหรับเยาวชน นักเรียน นักศึกษา การฝึกอบรมสำหรับบุคลากรวัยทำงานให้สามารถปฏิบัติงานได้ดียิ่งขึ้น เหล่านี้เองล้วนแต่ส่งผลดีต่อการพัฒนาระบบสารสนเทศและรักษาความปลอดภัยของระบบถ้ามีบุคลากรที่ได้รับการพัฒนา” (Wen Yaqing, สัมภาษณ์, 30 มีนาคม, 2568)

3) การพัฒนา (Development) เป็นขั้นตอนที่หน่วยงานภาครัฐ ภาคเอกชนและภาควิชาการ จัดขึ้นเพื่อให้เกิดการเรียนรู้และประสบการณ์แก่บุคลากรของแพลตฟอร์มออนไลน์ไต้หวันสำหรับการเรียนรู้สิ่งต่าง ๆ ที่เกี่ยวข้องกับการจัดการความปลอดภัยระบบสารสนเทศทั้งระบบ เป็นการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ขององค์การแพลตฟอร์มออนไลน์ไต้หวัน หรือหน่วยงานการพัฒนาความปลอดภัยระบบสารสนเทศทุกระดับในองค์กรของแพลตฟอร์มออนไลน์ไต้หวันได้เพิ่มพูนความรู้เชิงวิชาการด้านความปลอดภัยระบบสารสนเทศ เป็นการเปิดโอกาสให้บุคลากรของแพลตฟอร์มออนไลน์ไต้หวันได้พัฒนาความสามารถ และศักยภาพที่มีอยู่ออกมา กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การพัฒนาด้านความปลอดภัยระบบสารสนเทศให้ที่มีประสิทธิภาพ เกิดทักษะการให้บริการที่ดีของผู้ประกอบการแพลตฟอร์มออนไลน์ไต้หวัน เจ้าหน้าที่พนักงานด้านความปลอดภัยของแพลตฟอร์มออนไลน์ไต้หวันรับบทบาทหน้าที่ ประชาชนผู้ใช้บริการแพลตฟอร์มออนไลน์ไต้หวันในพื้นที่ต่างๆ ทั่วประเทศ จีน เข้าใจและทราบถึงประโยชน์ของการจัดการความปลอดภัยระบบสารสนเทศและมีส่วนร่วมในการรักษาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน วิธีการดังกล่าว เป็นกระบวนการดำเนินการให้การศึกษา อบรมอย่างเป็นระบบเพื่อให้เกิดการส่งเสริมและพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันที่ได้ผล” (Dong Zhenzhen, สัมภาษณ์, 22 เมษายน 2568)

การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศ มีการจัดการเรียนการสอนที่เป็นหลักสูตรอยู่ในสถานศึกษาของทั้งภาครัฐ และภาคเอกชน เป็นการส่งเสริมและการพัฒนาบุคลากรด้านระบบสารสนเทศให้มีความชำนาญในการแก้ไขปัญหาความไม่ปลอดภัยของระบบสารสนเทศ ส่งผลทำให้พนักงานเจ้าหน้าที่ของแพลตฟอร์มออนไลน์ไต้หวัน ที่เป็นผู้รับผิดชอบมีความรู้ มีความเข้าใจและเกิดทักษะเกี่ยวกับระบบการจัดการความปลอดภัยระบบสารสนเทศ และการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศโดยให้บุคลากรที่เกี่ยวข้องกับความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันมาศึกษาต่อ การอบรมระยะสั้น ระยะยาว อย่างต่อเนื่องเป็นวิธีการพัฒนากำลังคนด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันให้มีความรู้ ความเข้าใจ และเกิดทักษะเกี่ยวกับการจัดการความปลอดภัยระบบสารสนเทศ เช่น การวางแผน การจัดองค์กร การสั่งการ และการควบคุมงานด้านสารสนเทศและความปลอดภัยเพื่อให้เกิดการส่งเสริมและพัฒนาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันให้เป็นไปตามมาตรฐานและถูกต้องตามกฎหมายที่เกี่ยวข้อง กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศเป็นกลยุทธ์การดำเนินงานตามแนวคิดที่เห็นว่าบุคคลทั้งเก่าและบุคลากรใหม่ ต้องพัฒนาด้วยวิธีการศึกษา หรือฝึกอบรมเป็นสิ่งสำคัญ ที่จะให้การพัฒนาของแพลตฟอร์มออนไลน์โตขึ้นเป็นที่รู้จักและยอมรับของลูกค้าผู้ใช้แพลตฟอร์มออนไลน์โตขึ้นและผู้เกี่ยวข้อง การสร้างความรู้ ความเข้าใจจึงจำเป็น” (Lu Yangjing, สัมภาษณ์, 27 มีนาคม 2568)

การจัดการระบบสารสนเทศ และความปลอดภัยของข้อมูลในฐานข้อมูลขนาดใหญ่ของของแพลตฟอร์มออนไลน์โตขึ้น ในมิติของการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศ พบว่าส่งผลทำให้บุคลากรด้านการรักษาความปลอดภัยระบบสารสนเทศมีความรู้ความเข้าใจและตระหนักถึงคุณค่าและความสำคัญของปัจจัยที่เกี่ยวข้องกับฐานข้อมูลของของแพลตฟอร์มออนไลน์โตขึ้น ให้ประสบความสำเร็จ ส่งผลให้บุคลากรมีการตัดสินใจที่ถูกต้องรวดเร็วในการบริหารทรัพยากรข้อมูลต่าง ๆ ของของแพลตฟอร์มออนไลน์โตขึ้น ได้อย่างมีประสิทธิภาพ รวมทั้งการจัดสรรงบประมาณด้านความปลอดภัยระบบสารสนเทศที่มีอยู่อย่างจำกัดให้มีประสิทธิภาพและประสิทธิผลสูงสุด การบริหารค่าใช้จ่าย และการบริหารวัสดุอุปกรณ์กิจกรรมเหล่านี้ล้วนเป็นผลจากการพัฒนาบุคลากรทางด้านความปลอดภัยระบบสารสนเทศให้กลายเป็นกำลังสำคัญในการร่วมพัฒนาของแพลตฟอร์มออนไลน์โตขึ้นเชิงสร้างสรรค์ การพัฒนาบุคลากรมีบทบาทสำคัญต่อแพลตฟอร์มออนไลน์โตขึ้น หน่วยงานรัฐบาลที่เกี่ยวกับการรักษาระบบสารสนเทศ เพราะการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศมีผลทำให้สังคม วัฒนธรรม เศรษฐกิจ ชุมชน ท้องถิ่นมีความเข้มแข็ง และเจริญรุ่งเรืองด้วยสารสนเทศที่เป็นประโยชน์ต่อการพัฒนา ซึ่งแพลตฟอร์มออนไลน์โตขึ้น ต้องอาศัยบุคลากรที่ถูกพัฒนาแล้วให้เป็นผู้กระทำให้เกิดผลดีต่อการพัฒนาที่เกิดประโยชน์ต่อชุมชน ท้องถิ่น สังคม และประเทศชาติ กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การพัฒนาด้านความปลอดภัยระบบสารสนเทศด้วยวิธีการที่เชิงสร้างสรรค์มีผลต่อการพัฒนาธุรกิจแพลตฟอร์มออนไลน์โตขึ้นให้มีประสิทธิภาพ พนักงานด้านความปลอดภัยระบบสารสนเทศเกิดทักษะการให้รักษาระบบสารสนเทศให้มีความปลอดภัยที่ดีได้มาตรฐาน พนักงานรับบทบาทหน้าที่ และมีส่วนร่วมในการรักษาความปลอดภัยระบบสารสนเทศ วิธีการดังกล่าว เป็นกระบวนการดำเนินการให้การศึกษา อบรมอย่างเป็นระบบเพื่อให้เกิดการพัฒนาด้านความปลอดภัยระบบสารสนเทศที่ได้ผล” (Sun Ligu, สัมภาษณ์, 22 เมษายน 2568)

ปัจจุบันกระแสเรื่องของเศรษฐกิจสังคม และเทคโนโลยี และการแลกเปลี่ยนทางวัฒนธรรม ก่อให้เกิดความหิวหรือความต้องการความปลอดภัยของข้อมูลที่ผ่านแพลตฟอร์มออนไลน์ของแพลตฟอร์มออนไลน์โตขึ้น จึงจำเป็นต้องพัฒนากำลังคนด้านความปลอดภัยระบบสารสนเทศอย่างต่อเนื่อง มีทั้งการให้บุคลากรของแพลตฟอร์มออนไลน์โตขึ้น ลาศึกษาต่อ การอบรมระยะสั้น ระยะยาวมีขึ้นอย่างต่อเนื่องเพราะเป็นการพัฒนาคนให้มีความรู้เกี่ยวกับการระบบความปลอดภัยสารสนเทศเป็นการสื่อสารที่มีจุดมุ่งเน้นเพื่อให้เกิดการพัฒนาความเชื่อมั่นต่อแพลตฟอร์มออนไลน์โตขึ้น ที่ได้ผลดีและมีลักษณะที่ยั่งยืน เพื่อให้มีการพัฒนาด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์โตขึ้น ไปใน

ทิศทางที่ดีตลอดเวลา ต้องอาศัยทรัพยากรบุคคลที่เป็นปัจจัยสำคัญที่สุดต่อการพัฒนาองค์กรของแพลตฟอร์มออนไลน์ไต้หวัน ไปจนถึงการพัฒนาสังคม และประเทศ การที่จะสร้างบุคลากรที่มีคุณภาพขึ้นมาในองค์กรแพลตฟอร์มออนไลน์ไต้หวัน ประชาชนในสังคมจีนได้นั้น หนึ่งในปัจจัยสำคัญก็คือ การศึกษาสำหรับเยาวชน นักเรียน นักศึกษา การฝึกอบรมสำหรับบุคลากรวัยทำงานให้สามารถปฏิบัติงานได้ดียิ่งขึ้น ปัจจัยเหล่านี้ล้วนแต่ส่งผลดีต่อการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ถ้าบุคลากรได้รับการพัฒนาด้านความปลอดภัยระบบสารสนเทศ กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“การศึกษา การฝึกอบรมด้านการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน นอกจากจะทำให้เกิดความรู้ในการนำมาใช้บริหารจัดการความปลอดภัยระบบสารสนเทศและพัฒนาตนได้แล้ว ยังสามารถเป็นตัวกำหนดทิศทางของการพัฒนาการจัดการระบบสารสนเทศให้มีความปลอดภัยที่สูงขึ้นได้อีกด้วย ทั้งนี้หากแพลตฟอร์มออนไลน์ไต้หวัน มีการส่งเสริมการศึกษา การฝึกอบรมด้านการจัดการความปลอดภัยระบบสารสนเทศไปในทิศทางที่ถูกต้อง ย่อมทำให้แพลตฟอร์มออนไลน์ไต้หวัน มีต้นทุนที่เป็นทรัพยากรมนุษย์ที่มีศักยภาพในการร่วมกันสร้างระบบสารสนเทศที่มีความปลอดภัยที่ส่งผลต่อผู้ใช้งานแพลตฟอร์มออนไลน์ไต้หวันให้ก้าวไกล” (Qiao Zhi, สัมภาษณ์, 20 เมษายน 2568)

สรุป การพัฒนาเศรษฐกิจจีนในปัจจุบันอาศัยศักยภาพจากการสื่อสารที่สะดวกรวดเร็ว ในกิจการต่างๆ เศรษฐกิจในภาพรวมที่เติบโตได้อย่างยั่งยืนและมีเสถียรภาพในระยะยาวนั้น ควรให้ความสำคัญกับสถานการณ์ด้านต่าง ๆ และสาระสำคัญในประเด็นการพัฒนาทักษะ (Skills Development) การเตรียมแรงงานให้มีทักษะที่จำเป็นสำหรับทุกอุตสาหกรรม เพื่อให้บุคลากรที่เกี่ยวข้องกับอุตสาหกรรมสื่อสารทั้งภาครัฐ ภาคเอกชน มีความรู้ ความเข้าใจเกี่ยวกับสินค้าและบริการทางต้องอาศัยการสื่อสารผ่านแพลตฟอร์มออนไลน์ การจัดการด้านความปลอดภัยระบบสารสนเทศ ให้ประสบความสำเร็จ จึงเป็นกลยุทธ์ของแพลตฟอร์มออนไลน์ไต้หวัน ให้ความสำคัญกับการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศในทุกระดับ ในมิติของการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศ ทำให้บุคลากรด้านระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน มีความรู้ความเข้าใจและตระหนักถึงคุณค่าและความสำคัญของปัจจัยที่เกี่ยวข้องกับด้านการพัฒนาบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศทั้งระบบ พบว่า การส่งเสริมการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ให้ประสบความสำเร็จได้นั้น ต้องให้ความสำคัญต่อการพัฒนาบุคลากรด้านการจัดการระบบสารสนเทศในทุกๆ ระดับ ซึ่งการศึกษาพบว่า การพัฒนาบุคลากรด้านการจัดการระบบสารสนเทศเพื่อความปลอดภัยเป็นกลไกสำคัญของแพลตฟอร์มออนไลน์ไต้หวัน ที่จะนำไปสู่ความสำเร็จในการพัฒนาแพลตฟอร์มออนไลน์ไต้หวัน ซึ่งหากแพลตฟอร์มออนไลน์ไต้หวัน มีบุคลากรด้านการจัดการระบบสารสนเทศทั้งระบบที่มีศักยภาพ คุณภาพ และคุณธรรมจริยธรรมที่สูง จะเกิดผลดีและจะสามารถพัฒนาแพลตฟอร์มออนไลน์ไต้หวัน ให้เข้า

ไปสู่ความสามารถในการแข่งขันด้านการให้บริการของแพลตฟอร์มออนไลน์ที่สูง เพื่อดึงดูดลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ ทั้งภายในประเทศ และต่างประเทศที่ให้เลือกใช้บริการของแพลตฟอร์มออนไลน์ไต้หวัน

5. กลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

ผลการศึกษาพบว่า การสร้างเชื่อมั่นของลูกค้าของแพลตฟอร์มออนไลน์ไต้หวัน เป็นหนึ่งในกลยุทธ์สำคัญที่สุดที่จะนำไปสู่ความสำเร็จในระยะยาวภายใต้แบรนด์ธุรกิจของแพลตฟอร์มออนไลน์ไต้หวัน โดยเฉพาะอย่างยิ่งสำหรับผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันที่เป็นประชาชนธรรมดา และประกอบการธุรกิจ SME ที่ใช้แพลตฟอร์มออนไลน์ไต้หวัน เพื่อเป็นสื่อสังคมออนไลน์ในการส่งเสริมการตลาด พบว่า ความเชื่อมั่นของลูกค้าที่ใช้แพลตฟอร์มออนไลน์ของแพลตฟอร์มออนไลน์ไต้หวัน เป็นรากฐานของความสัมพันธ์ที่แน่นแฟ้นระหว่างแบรนด์ของแพลตฟอร์มออนไลน์ไต้หวัน และผู้บริโภค ซึ่งจะนำไปสู่ความเชื่อมั่นที่มีต่อแบรนด์ของแพลตฟอร์มออนไลน์ไต้หวัน ความเชื่อมั่นต่อแพลตฟอร์มออนไลน์ไต้หวัน ส่งผลให้เกิดการโฆษณาบอกต่อ และสามารถรายได้ที่เพิ่มขึ้นในระยะยาว การสร้างเชื่อมั่นให้กับลูกค้าของแพลตฟอร์มออนไลน์ไต้หวัน จึงเป็นสิ่งจำเป็นอย่างยิ่งสำหรับธุรกิจทุกประเภท ในโลกของการแข่งขันที่รุนแรงในปัจจุบัน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“ความเชื่อมั่น ถือเป็นสิ่งสำคัญที่ทุกธุรกิจต้องการได้รับจากผู้บริโภค โดยรายงานผลสำรวจ Voice of the Consumer Survey 2024 ของ PwC ที่ทำการศึกษาความคิดเห็นของผู้บริโภคผ่านแพลตฟอร์มออนไลน์ทั่วโลกจำนวนกว่า 20,000 ราย ใน 31 ประเทศที่นิยมใช้แพลตฟอร์มออนไลน์ไต้หวัน พบว่า ปัจจุบันช่องว่างระหว่างความเชื่อมั่นของผู้บริโภคที่มีต่อบริษัทผู้ขายสินค้าและบริการ กับความเชื่อมั่นที่บริษัทผู้ขายสินค้าและบริการคาดว่าจะได้รับนั้นขยายตัวกว้างมากขึ้น” (Feng Yaping, สัมภาษณ์ , 25 มีนาคม 2568)

ความเชื่อมั่นต่อแพลตฟอร์มออนไลน์ไต้หวัน พบว่า ความน่าเชื่อถือทุกด้านโดยเฉพาะความปลอดภัยระบบสารสนเทศและวิธีการสื่อสารกลายเป็นปัจจัยสำคัญที่มีผลต่อการตัดสินใจซื้อสินค้าจากผู้ประกอบการต่าง ๆ ผ่านแพลตฟอร์มออนไลน์ไต้หวัน โดยจากการสำรวจของ PwC พบว่า ผู้บริโภคที่เป็นผู้ใช้ของแพลตฟอร์มออนไลน์ไต้หวัน มากถึง 85% เคยได้รับบริการที่มีคุณภาพสูง สามารถตอบสนองต่อการใช้งานด้านต่าง ๆ ได้ดีจึงต้องการเลือกซื้อสินค้าผ่านแพลตฟอร์มออนไลน์ไต้หวัน ซึ่งผู้บริโภคกลุ่มนี้มีความพร้อมในการจ่ายสินค้าราคาสูงขึ้น โดยพวกเขายินดีจะจ่ายเพิ่มขึ้นถึง 9.7% จากราคาปกติสำหรับสินค้าที่ผ่านแพลตฟอร์มออนไลน์ไต้หวัน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“แพลตฟอร์มออนไลน์ไต้หวัน สร้างความน่าเชื่อถือของลูกค้าอยู่เสมอเราทำการสำรวจทุกปีถึงความต้องการของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันในแต่ละด้านและก็นำมาวางแผนเป็นแนวทางเพื่อพัฒนาให้

ตรงกับที่ลูกค้าต้องการ แพลตฟอร์มออนไลน์ไต่ยีนดำเนินการตามข้อมูลที่ได้รับส่งผลต่อความเชื่อมั่น” (Zhu Xincheg, สัมภาษณ์, 18 เมษายน 2568)

การใช้แพลตฟอร์มออนไลน์ไต่ยีน ในการทำตลาดอย่างมีชั้นเชิง พบว่า ผู้บริโภคเกือบครึ่งคือ 46% ที่ถูกสำรวจ กล่าวว่าตนใช้แพลตฟอร์มออนไลน์ไต่ยีน ในการจับจ่ายสินค้าและใช้เป็นแหล่งหาข้อมูล และรีวิวนสินค้าก่อนตัดสินใจซื้อ แต่ขณะเดียวกันแพลตฟอร์มออนไลน์ไต่ยีน ก็ยังเปิดโอกาสให้แสดงความกังวลด้านความปลอดภัยและความน่าเชื่อถือด้วย ดังนั้นแพลตฟอร์มออนไลน์ไต่ยีนจึงมุ่งเน้นไปที่การสร้างเนื้อหาที่น่าสนใจและน่าเชื่อถือ พร้อมจัดการกับความปลอดภัยของข้อมูลผู้บริโภคที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต่ยีน รวมถึงประเด็นอื่น ๆ เช่น คุณภาพของสินค้าและบริการ การปฏิสัมพันธ์กับพนักงาน และความคุ้มค่าของสินค้าผ่านแพลตฟอร์มออนไลน์ไต่ยีน ทั้งนี้ยังพบว่า ด้านความเชื่อมั่นถูกกำหนดเป็นกลยุทธ์การใช้แพลตฟอร์มออนไลน์ไต่ยีนถูกปรับให้เข้ากับกลุ่มเป้าหมาย มีการสร้างโฆษณาสำหรับเฉพาะบุคคล และสร้างความสัมพันธ์บนพื้นที่ดิจิทัลที่เหนือไปกว่าการทำให้แบรนด์ของแพลตฟอร์มออนไลน์ไต่ยีนเป็นที่รู้จัก กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“ผู้ใช้แพลตฟอร์มออนไลน์ไต่ยีนให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลของตน โดยต้องการความเชื่อมั่นว่าข้อมูลของตนจะไม่รั่วไหล ถึงวลถึงความปลอดภัยของข้อมูลจากการใช้งานโซเชียลมีเดีย แต่แม้ว่าจะมีความกังวลในเรื่องนี้ ผู้บริโภคเกือบครึ่งก็ยังดีที่จะให้ข้อมูลของพวกเขาถูกนำไปใช้เพื่อนำเสนอบริการและประสบการณ์เฉพาะบุคคล เช่น รายการส่งเสริมการขายต่าง ๆ หรือส่วนลดพิเศษ เป็นต้น ด้วยเหตุนี้แพลตฟอร์มออนไลน์ไต่ยีน จึงยกระดับกลยุทธ์การใช้งานข้อมูลและรักษาความเป็นส่วนตัวอย่างเต็มประสิทธิภาพ และมีความรับผิดชอบ ซึ่งรวมถึงการลงทุนในเทคโนโลยีด้านความปลอดภัย” (Dong Zhenzhen, สัมภาษณ์, 29 มีนาคม 2568)

แพลตฟอร์มออนไลน์ไต่ยีนสร้างความเชื่อมั่นโดยการสร้างประสบการณ์ที่คุ้มค่าให้กับลูกค้า พร้อมจัดการต้นทุนอย่างมีประสิทธิภาพ การกำหนดราคาที่ทำให้ความคุ้มค่า ถือเป็นอีกหนึ่งปัจจัยสำคัญที่ช่วยให้ลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต่ยีนตัดสินใจว่าแพลตฟอร์มออนไลน์ไต่ยีนนั้น ๆ จะได้รับความเชื่อมั่นจากผู้บริโภคสูงขึ้น และพบว่า ผู้บริโภคที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต่ยีน ที่ถูกสำรวจจะระบุว่า จะพิจารณาเปลี่ยนไปใช้สินค้าแบรนด์อื่นที่มีราคาเหมาะสมกว่าที่ขายอยู่ในแพลตฟอร์มออนไลน์ไต่ยีน ด้วยเหตุนี้แพลตฟอร์มออนไลน์ไต่ยีน จึงขอให้ผู้ประกอบการค้าผ่านสื่อแพลตฟอร์มออนไลน์ไต่ยีนต้องคำนึงถึงการกำหนดราคาสินค้าและบริการที่สัมพันธ์กับภาวะเศรษฐกิจ และเงินเฟ้อ รวมถึงมีกลยุทธ์ในการขายสินค้าและบริการผ่านแพลตฟอร์มออนไลน์ไต่ยีนที่หลากหลาย เพื่อสร้างประสบการณ์ที่ดีและทำให้ลูกค้ารู้สึกได้ถึงความคุ้มค่าที่ตนได้รับและเกิดความเชื่อมั่นต่อการค้าขายแพลตฟอร์มออนไลน์ไต่ยีน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“ผู้บริหารทุกระดับของแพลตฟอร์มออนไลน์ไต้หวันคำนึงถึงความเชื่อมั่นและความต้องการของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน จึงให้ความสำคัญกับความเชื่อมั่นของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน และเราพยายามทุกวิถีทางเพื่อให้เกิดความเชื่อมั่น” (...สัมภาษณ์ 17 มีนาคม 2568)

แพลตฟอร์มออนไลน์ไต้หวันมีการประยุกต์ใช้ AI ร่วมกับบุคลากรเพื่อสร้างความถูกต้องของข้อมูล ซึ่งเป็นส่วนในการสร้างความเชื่อมั่นเป็นอย่างมาก จากผลสำรวจพบว่า ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันซึ่งเป็นบริษัทยักษ์ใหญ่ แสดงความเห็นว่าตนไว้วางใจให้เทคโนโลยีปัญญาประดิษฐ์ (AI) ในการแนะนำข้อมูลสินค้าและบริการทั่วไป แต่ยังคงไม่มั่นใจในการใช้บริการที่มีความเสี่ยงสูง เช่น คำแนะนำด้านการเงินหรือการแพทย์ เป็นต้น แม้ปัจจุบันหลาย ๆ บริษัทจะได้นำ Gen AI และการเรียนรู้ของเครื่องจักร (Machine Learning) มาใช้ปรับปรุงประสิทธิภาพการทำงาน รวมถึงนำแชทบอตมาช่วยโต้ตอบกับลูกค้า แต่ก็ยังพบว่าผู้บริโภคผ่านแพลตฟอร์มออนไลน์ไต้หวัน ต้องการความช่วยเหลือจากบุคลากรของแพลตฟอร์มออนไลน์ไต้หวันในการให้บริการหรือตอบคำถามที่มีความซับซ้อน ดังนั้นแพลตฟอร์มออนไลน์ไต้หวันมีนโยบายซึ่งเป็นกลยุทธ์เพื่อสร้างความเชื่อมั่นต่อแพลตฟอร์มออนไลน์ไต้หวัน โดยการผสมผสานการใช้งาน AI เข้ากับการทำงานของพนักงานของแพลตฟอร์มออนไลน์ไต้หวันที่เป็นมนุษย์ เพื่อส่งมอบประสบการณ์ที่ดีและเฉพาะเจาะจงให้กับผู้บริโภคที่ใช้แพลตฟอร์มออนไลน์ไต้หวัน กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“ชื่อเสียงของแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน นับเป็นสิ่งจำเป็นต่อความสำเร็จในการทำธุรกิจออนไลน์ ดังนั้นการรู้สึกถึงความเชื่อใจในตัวแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน จะเป็นบันไดขั้นแรกๆ ที่ช่วยให้แบรนด์ของแพลตฟอร์มออนไลน์ไต้หวันมีชื่อเสียงเป็นที่รู้จัก ซึ่งไม่ใช่แค่คำพูดที่แบรนด์สื่อสารเพียงอย่างเดียว แต่มันคือความมั่นใจที่แบรนด์นั้นมอบให้กับลูกค้าที่สามารถทำได้จริง Brand Trust จึงเป็นเรื่องของการสร้างความสัมพันธ์อันดีระหว่างแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน และลูกค้า ที่ประกอบขึ้นมาจาก 3 ส่วนด้วยกัน ได้แก่ ความน่าเชื่อถือ (Credibility) ความน่าไว้วางใจ (Reliability) และความสนิทสนมคุ้นเคย (Intimacy)” (Qiu Yu, สัมภาษณ์ 30 เมษายน 2568)

สินค้าและบริการเป็นสิ่งที่สร้างรายได้ให้กับแบรนด์และธุรกิจของแพลตฟอร์มออนไลน์ไต้หวันพบว่า ความเชื่อใจในตัวแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน จะขึ้นได้จากการที่แบรนด์แพลตฟอร์มออนไลน์ไต้หวัน นำเสนอสินค้าหรือบริการที่มีคุณภาพเท่านั้น แม้ว่าแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน จะสื่อสารหรือโปรโมทคุณสมบัติของสินค้าหรือการให้บริการที่เป็นเลิศ แต่หากลูกค้าที่ใช้แพลตฟอร์มออนไลน์ไต้หวัน เมื่อมาสัมผัสด้วยตัวเองแล้วไม่ได้เป็นอย่างที่บอกไว้ในแพลตฟอร์มออนไลน์ไต้หวัน ก็ยากที่จะเกิดความไว้วางใจจนบางครั้งอาจทำให้แพลตฟอร์มออนไลน์ไต้หวันเสียลูกค้าไปก็ได้ และพบว่าความเชื่อมั่นต่อแพลตฟอร์มออนไลน์ไต้หวัน เกิดจากแพลตฟอร์มออนไลน์ไต้หวันมีความจริงใจ เสนอคุณค่าและความแท้จริงความแท้จริงผ่านแพลตฟอร์มออนไลน์ไต้หวัน เป็นข้อพิสูจน์แรกของความจริงใจ เพราะลูกค้าส่วนใหญ่ในยุคสมัยใหม่นี้ไม่ได้สนใจในเรื่องของคุณสมบัติหรือประโยชน์เพียงอย่างเดียว แต่ยังพบว่า

ยังอยากรู้ว่าแบรนด์หรือธุรกิจของแพลตฟอร์มออนไลน์ไต่ขึ้นคือใคร ซึ่งนั่นก็คือแบรนด์ของแพลตฟอร์มออนไลน์ไต่ขึ้นต้องมีคุณค่าและมีความแท้จริง ที่สะท้อนมาจากความเชื่อ วัฒนธรรม ความจริงใจในการทำธุรกิจ การยึดลูกค้าเป็นสำคัญ และถ่ายทอดผ่านแพลตฟอร์มออนไลน์ไต่ขึ้น ด้วยการเล่าเรื่องหรือบอกเล่าเรื่องราวต่าง ๆ (Storytelling) เพื่อให้ลูกค้าเกิดความเชื่อถือและเกิดความไว้วางใจในตัวแบรนด์แพลตฟอร์มออนไลน์ไต่ขึ้น (Brand Trust) กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“แพลตฟอร์มออนไลน์ไต่ขึ้น เน้นการสร้างความสัมพันธ์มากกว่าการขายเรื่องของความเชื่อใจ ไม่ได้เกิดกันง่าย ๆ เพียงชั่วข้ามคืน แต่ความเชื่อใจนั้นเกิดจากการสร้างความสัมพันธ์อันดีในระยะยาว การสร้างมิตรภาพดี ๆ จะมีพลังและส่งเสริมให้เกิดความรู้สึกที่ดีให้กับแบรนด์แพลตฟอร์มออนไลน์ไต่ขึ้น จนกลายเป็นความเชื่อจนสนิทใจที่ส่งผลดีต่อการทำธุรกิจได้ในระยะยาว” (Chen Che, สัมภาษณ์, 2 พฤษภาคม 2568)

ปัจจุบันโลกนี้สื่อสารกันด้วยระบบออนไลน์แพลตฟอร์มออนไลน์ไต่ขึ้นก็เป็นส่วนหนึ่งของระบบสารสนเทศและการสื่อสารยุคใหม่ที่เกิดขึ้น เพื่อตอบสนองต่อการสื่อสารยุคใหม่ สารสนเทศยุคใหม่เกิดประโยชน์ต่อการสื่อสารและสามารถตอบสนองต่อความต้องการทางสังคมอื่นๆ แต่ก็พบว่าการสื่อสารออนไลน์ผ่านแพลตฟอร์มต่าง ๆ ก็มักมีปัญหา และเต็มไปด้วยปัญหาต่าง ๆ ไม่เว้นแต่ละวัน แบรนด์สื่อสารออนไลน์ที่ดีจึงไม่ใช่นำการยึดเหนี่ยวเพื่อที่จะส่งผ่านข้อมูลการขายสินค้าหรือบริการ แต่หากแบรนด์ออนไลน์ต้องสามารถสร้างความเชื่อใจได้ด้วยการรับฟังและเสนอทางแก้ไขปัญหาลูกค้าได้ ก็จะทำให้การสร้างแบรนด์และธุรกิจของแพลตฟอร์มออนไลน์ไต่ขึ้นง่ายมากขึ้น ความช่วยเหลือเพื่อสร้างความเชื่อมั่นต่อแพลตฟอร์มออนไลน์ไต่ขึ้น พบว่า แพลตฟอร์มออนไลน์ไต่ขึ้นทำได้หลายรูปแบบ เช่น การรับฟัง การให้คำแนะนำ เสนอทางแก้ไข เป็นต้น กรณีดังกล่าวสอดคล้องกับคำให้สัมภาษณ์ที่ว่า

“มีหลากหลายสถิติบ่งบอกถึงความกังวลใจของลูกค้าในเรื่องของการเปิดเผย และการที่ข้อมูลส่วนตัวนั้นหลุดออกไปสู่สาธารณชน โดยเฉพาะเมื่อลูกค้ามีการทำธุรกรรมต่าง ๆ ร่วมกับแบรนด์แพลตฟอร์มออนไลน์ไต่ขึ้น ไม่ว่าจะเป็นการซื้อสินค้าหรือบริการ การติดต่อเพื่อพูดคุยกับแพลตฟอร์มออนไลน์ไต่ขึ้น ที่ต้องมีการเก็บข้อมูลของลูกค้า สิ่งต่าง ๆ เหล่านี้คือข้อกังวลใจที่หากแพลตฟอร์มออนไลน์ไต่ขึ้น สามารถให้คำมั่นสัญญาได้ว่าจะสามารถปกป้องและเก็บข้อมูลต่าง ๆ ของลูกค้าให้เป็นความลับได้ มีกระบวนการจัดเก็บที่ดีการป้องกันข้อมูลรั่วไหลที่ดี ก็จะสามารถสร้างความเชื่อใจแพลตฟอร์มออนไลน์ไต่ขึ้นได้มากขึ้นอีกหลายเท่า” (Nie Sungtao, สัมภาษณ์, 2 พฤษภาคม 2568)

สรุป แพลตฟอร์มออนไลน์ไต่ขึ้นสามารถสื่อสารเพื่ออธิบายในสิ่งที่แพลตฟอร์มออนไลน์ไต่ขึ้นทำในสิ่งที่ลูกค้าที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต่ขึ้นได้อย่างเข้าใจ พบว่า ความเชื่อมั่นและความมั่นใจของลูกค้าแพลตฟอร์มออนไลน์ไต่ขึ้นเชื่อใจในแบรนด์ของแพลตฟอร์มออนไลน์ไต่ขึ้น และพบว่า แพลตฟอร์มออนไลน์ไต่ขึ้นมีการสร้างความเชื่อมั่นให้กับผู้ใช้แพลตฟอร์มโดยการนำเสนอข่าว ข้อมูลที่มีการสื่อสารและสร้างภาพลักษณ์ (Brand Image) ที่ดีให้กับตัวแพลตฟอร์มออนไลน์ไต่ขึ้น ดังนั้นการจะสร้างความเชื่อใจให้กับแบรนด์แพลตฟอร์มออนไลน์ไต่ขึ้น (Brand Trust) ต้องสื่อสารอย่างตรงไปตรงมา และพร้อมให้ทุกคนตรวจสอบได้อยู่เสมอซึ่งเป็นวิธีการบริหารจัดการที่เหมาะสมกับยุคเทคโนโลยีดิจิทัลที่ทำให้เกิดความ

โปร่งใส่ทั้งภายในองค์กรและภายนอกองค์กร และพบว่า แพลตฟอร์มออนไลน์ไต้หวัน เป็นแบรนด์ที่สามารถสร้างความเชื่อมั่นและความไว้วางใจให้กับลูกค้า ด้วยการยืนยันยึดอยู่บนความถูกต้องของข้อมูลและคุณธรรมซึ่งก็คือความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันที่แสดงจุดยืนที่ชัดเจนในเรื่องของความเป็นธรรมในการทำธุรกิจสื่อสังคมออนไลน์แพลตฟอร์มออนไลน์ไต้หวัน และยังพบว่า แพลตฟอร์มออนไลน์ไต้หวันสามารถสร้างความเชื่อใจให้เกิดความรู้สึกดีทั้งกับตัวแบรนด์แพลตฟอร์มออนไลน์ไต้หวันรวมถึงสินค้าและบริการ จนกลุ่มคนผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันเหล่านั้นกลายเป็น Social Proof ที่ทรงพลัง ที่นำไปบอกต่อทั้งแบบปากต่อปาก (Word-of-Mouth) หรืออาจนำไปบอกต่อผ่านโซเชียล และยังพบว่า นอกจากนั้น Social Proof เกิดจากสิ่งที่แบรนด์แพลตฟอร์มออนไลน์ไต้หวันได้ดำเนินธุรกิจแพลตฟอร์มออนไลน์มาอย่างยาวนานและได้รับการันตีรางวัลแพลตฟอร์มออนไลน์ดีเด่นระดับโลก มีจำนวนลูกค้าที่ใช้งานแพลตฟอร์มออนไลน์ไต้หวันทั่วโลก รางวัลด้านคุณภาพดีเด่น และรางวัลด้านการบริการที่ดี เป็นต้น

2. ผลการวิเคราะห์ข้อมูลกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

เมื่อได้ตีความและเปรียบเทียบความคิดเห็นจากการสัมภาษณ์เชิงลึกของผู้บริหารระดับสูงระดับกลาง ระดับปฏิบัติการ และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวัน ข้อมูลกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน จำนวน 20 ท่าน แล้วนำมาสังเคราะห์พบว่า มีการแสดงแนวคิดเกี่ยวกับกลยุทธ์ความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ดังนี้

1. ระบบการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันได้ถูกกำหนดให้เป็นกลยุทธ์ด้านความปลอดภัย ในยุคดิจิทัลเช่นปัจจุบันนี้นวัตกรรมการสื่อสารผ่านการใช้แพลตฟอร์มออนไลน์ไต้หวัน เพื่อเป็นช่องทางส่งผ่านข้อมูลขององค์กรที่พัฒนาแพลตฟอร์มออนไลน์ไต้หวัน ที่ขับเคลื่อนด้วยระบบอินเทอร์เน็ตและใช้ปัญญาประดิษฐ์ AI ก่อให้เกิดศักยภาพที่เป็นประโยชน์มากมายมหาศาลต่อการสื่อสาร ต่อสังคม ต่อเศรษฐกิจ อย่างไรก็ตามความพยายามในการรักษาความปลอดภัยระดับองค์กรของแพลตฟอร์มออนไลน์ไต้หวัน และจัดการกับภัยคุกคามทางไซเบอร์มีความท้าทายเพิ่มมากขึ้น ส่งผลให้ผู้บริหารทุกระดับของแพลตฟอร์มออนไลน์ไต้หวัน ผู้ดูแลและพัฒนาระบบแพลตฟอร์มออนไลน์ไต้หวัน จำเป็นต้องต้องสร้างสมดุลระหว่างความก้าวหน้าทางเทคโนโลยี และเทคโนโลยี AI นำเสนอผ่านแพลตฟอร์มออนไลน์ไต้หวัน กับความคาดหวังและความต้องการความปลอดภัยของระบบสารสนเทศของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ที่สำคัญในการรักษาความปลอดภัยข้อมูล แอปพลิเคชัน และผู้ใช้

2. การจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศทางไซเบอร์ถือเป็นสิ่งสำคัญสำหรับแพลตฟอร์มออนไลน์ไต้หวัน ในการปกป้องข้อมูลที่ละเอียดอ่อนของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน การปฏิบัติตามข้อกำหนด และรับรองความต่อเนื่องในการดำเนินงาน ด้วยความซับซ้อนและความถี่ของภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้น ผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน จึงใช้กลยุทธ์เป็นแนวทางเชิงรุกเพื่อ

ระบุความไม่ปลอดภัย ประเมินความไม่ปลอดภัย และลดความเสี่ยงที่จะเกิดความปลอดภัยจากการใช้สารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนอย่างมีประสิทธิภาพ ด้วยการนำกรอบงานด้านความปลอดภัยทางไซเบอร์ที่เป็นมาตรฐานสากลที่ได้รับการยอมรับทั่วโลกมาใช้เพื่อรักษาความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนอย่างจริงจัง

3. หลักการและนโยบายของแพลตฟอร์มออนไลน์ไต่ยืน ตระหนักถึงการใช้สื่อสังคมออนไลน์ที่แพร่หลาย และผลกระทบที่อาจเกิดขึ้นทั้งประโยชน์และโทษ โดยเฉพาะหากมีการเผยแพร่ข้อมูลที่ไม่เหมาะสมออกสู่สาธารณะ ซึ่งอาจก่อให้เกิดความเสียหายต่อตนเอง ผู้อื่น และองค์กร นโยบายของแพลตฟอร์มออนไลน์ไต่ยืน จึงจัดทำขึ้นเพื่อให้การใช้แพลตฟอร์มออนไลน์ไต่ยืน มีความเหมาะสม เป็นประโยชน์ และหลีกเลี่ยงผลกระทบต่อสังคม และการดำเนินงานของแพลตฟอร์มออนไลน์ไต่ยืนในอนาคต

แพลตฟอร์มออนไลน์ไต่ยืน มีการกำหนดนโยบายและแนวปฏิบัติที่เหมาะสมต่อการดำเนินงานตามวัตถุประสงค์ ปณิธาน พันธกิจ ของแพลตฟอร์ม โดยคำนึงถึงสิทธิและเสรีภาพอย่างมีขอบเขตในการแสดงความคิดเห็นของผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนเป็นสำคัญ

มีการส่งเสริมให้ใช้สื่อสังคมออนไลน์ผ่านแพลตฟอร์มออนไลน์ไต่ยืน เพื่อการเรียนรู้ การแลกเปลี่ยนความรู้ การเสริมสร้างปฏิสัมพันธ์ทางสังคม วัฒนธรรม การท่องเที่ยว วิชาการ ฯลฯ และการเผยแพร่ข้อมูลหรือข้อคิดเห็นทางความคิดเชิงสร้างสรรค์ ที่ไม่ขัดต่อศีลธรรมอันดีของประชาชนจีน ธรรมเนียมปฏิบัติของสังคม

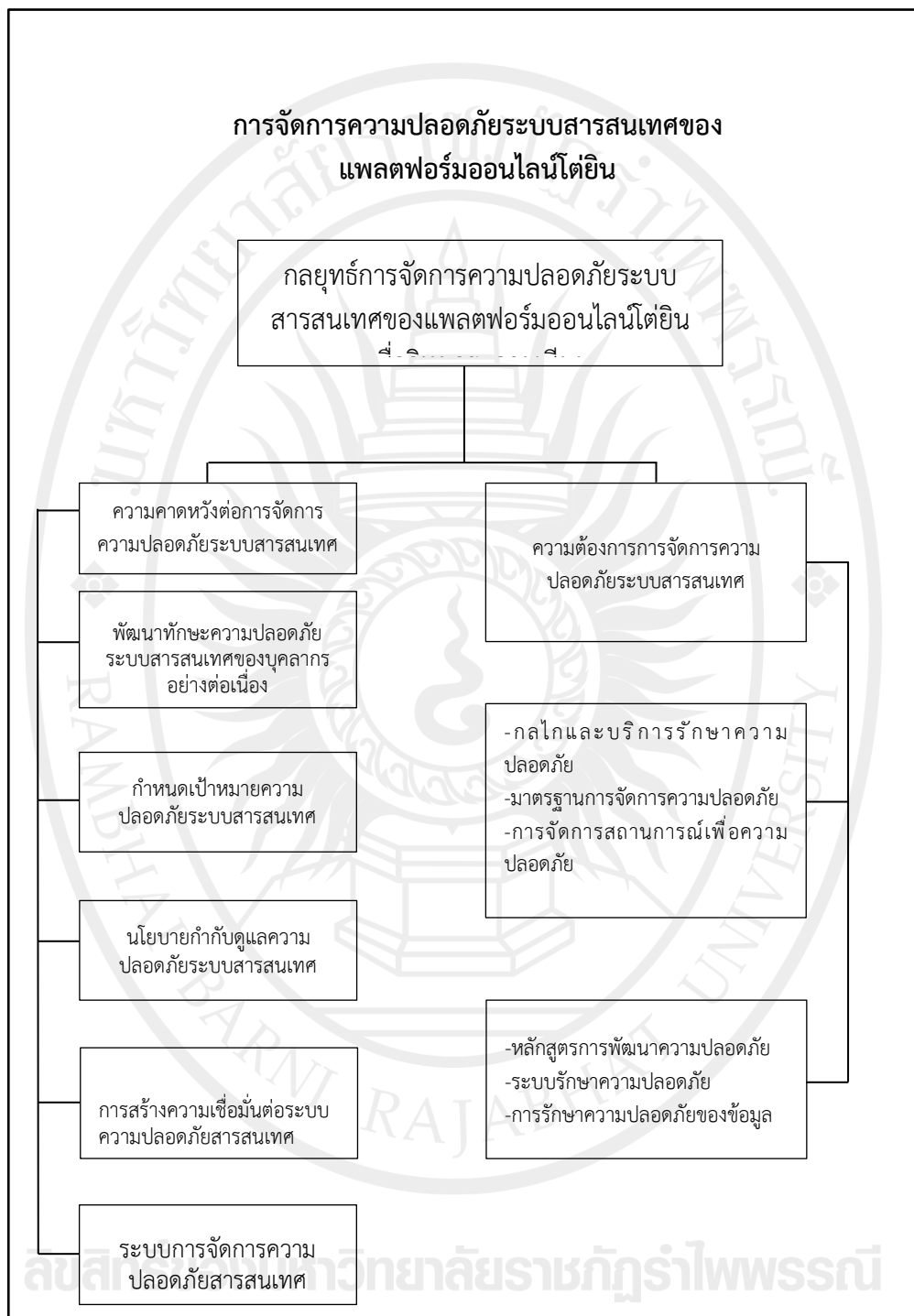
แพลตฟอร์มออนไลน์ไต่ยืน ไม่จำกัดสิทธิและเสรีภาพในการใช้สื่อแพลตฟอร์มออนไลน์ไต่ยืน แต่ผู้ใช้งานต้องตระหนักถึงสถานภาพความเป็นประชาชนจีนที่มีหน้าที่ในการรักษาวินัย จรรยาบรรณ รวมถึงการรักษาเกียรติและความน่าเชื่อถือทั้งของตนเอง ของสถาบันทางสังคม และประเทศ

4. แพลตฟอร์มออนไลน์ไต่ยืนคำนึงถึงและการเป็นส่วนหนึ่งในการพัฒนาเศรษฐกิจจีนในปัจจุบันที่ต้องอาศัยศักยภาพจากการสื่อสารที่สะดวกรวดเร็ว ในกิจการต่างๆ เศรษฐกิจในภาพรวมที่เติบโตได้อย่างยั่งยืนและมีเสถียรภาพในระยะยาวนั้น ควรให้ความสำคัญกับสถานการณ์ด้านต่าง ๆ และสาระสำคัญในประเด็นการพัฒนาทักษะ (Skills Development) การเตรียมแรงงานให้มีทักษะที่จำเป็นสำหรับทุกอุตสาหกรรม เพื่อให้บุคลากรที่เกี่ยวข้องกับอุตสาหกรรมทั้งภาครัฐ ภาคเอกชน มีความรู้ ความเข้าใจเกี่ยวกับสินค้าและบริการทางต้องอาศัยการสื่อสารผ่านแพลตฟอร์มออนไลน์ การจัดการด้านความปลอดภัยระบบสารสนเทศ ให้ประสบความสำเร็จ จึงเป็นกลยุทธ์ของแพลตฟอร์มออนไลน์ไต่ยืน ให้ความสำคัญกับการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศในทุกระดับ ในมิติของการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศ ทำให้บุคลากรด้านระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน มีความรู้ความเข้าใจและตระหนักถึงคุณค่าและความสำคัญของปัจจัยที่เกี่ยวข้องกับด้านการพัฒนาบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศทั้งระบบ พบว่า การส่งเสริมการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน ให้ประสบความสำเร็จได้นั้น ต้องให้ความสำคัญต่อการพัฒนาบุคลากรด้านการจัดการระบบสารสนเทศในทุกระดับ ซึ่งการศึกษาพบว่า การ

พัฒนาบุคลากรด้านการจัดการระบบสารสนเทศเพื่อความปลอดภัยเป็นกลไกสำคัญของแพลตฟอร์มออนไลน์ไต่ยืน ที่จะนำไปสู่ความสำเร็จในการพัฒนาแพลตฟอร์มออนไลน์ไต่ยืน ซึ่งหากแพลตฟอร์มออนไลน์ไต่ยืน มีบุคลากรด้านการจัดการระบบสารสนเทศทั้งระบบที่มีศักยภาพ คุณภาพ และคุณธรรม จริยธรรมที่สูง จะเกิดผลดีและจะสามารถพัฒนาแพลตฟอร์มออนไลน์ไต่ยืน ให้เข้าไปถึงความสามารถในการแข่งขันด้านการให้บริการของแพลตฟอร์มออนไลน์ไต่ยืน ที่สูง เพื่อดึงดูดลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน ทั้งภายในประเทศ และต่างประเทศที่ให้เลือกใช้บริการของแพลตฟอร์มออนไลน์ไต่ยืน

5. แพลตฟอร์มออนไลน์ไต่ยืนสามารถสื่อสารเพื่ออธิบายในสิ่งที่แพลตฟอร์มออนไลน์ไต่ยืนทำในสิ่งที่ลูกค้าที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนได้อย่างเข้าใจ เป็นการสร้างความเชื่อมั่นและความมั่นใจของลูกค้าแพลตฟอร์มออนไลน์ไต่ยืนเชื่อใจในแบรนด์ของแพลตฟอร์มออนไลน์ไต่ยืน และพบว่าแพลตฟอร์มออนไลน์ไต่ยืนมีการสร้างความเชื่อมั่นให้กับผู้ใช้แพลตฟอร์มโดยการนำเสนอข่าว ข้อมูลที่มีการสื่อสารและสร้างภาพลักษณ์ (Brand Image) ที่ดีให้กับตัวแพลตฟอร์มออนไลน์ไต่ยืน ดังนั้นการจะสร้างความเชื่อใจให้กับแบรนด์แพลตฟอร์มออนไลน์ไต่ยืน (Brand Trust) ต้องสื่อสารอย่างตรงไปตรงมา และพร้อมให้ทุกคนตรวจสอบได้อยู่เสมอซึ่งเป็นวิธีการบริหารจัดการที่เหมาะสมกับยุคเทคโนโลยีดิจิทัลที่ทำให้เกิดความโปร่งใสทั้งภายในองค์กรและภายนอกองค์กร และพบว่า แพลตฟอร์มออนไลน์ไต่ยืน เป็นแบรนด์ที่สามารถสร้างความเชื่อมั่นและความไว้วางใจให้กับลูกค้า ด้วยการยืนยันยึดอยู่บนความถูกต้องของข้อมูลและความยุติธรรมซึ่งก็คือความปลอดภัยของระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนที่แสดงจุดยืนที่ชัดเจนในเรื่องของความเป็นธรรมในการทำธุรกิจสื่อสังคมออนไลน์แพลตฟอร์มออนไลน์ไต่ยืน และยังพบว่า แพลตฟอร์มออนไลน์ไต่ยืนสามารถสร้างความเชื่อใจให้เกิดความรู้สึกดีทั้งกับตัวแบรนด์แพลตฟอร์มออนไลน์ไต่ยืนรวมไปถึงสินค้าและบริการ จนกลุ่มคนผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนเหล่านั้นกลายเป็น Social Proof ที่ทรงพลัง ที่นำไปบอกต่อทั้งแบบปากต่อปาก (Word-of-Mouth) หรืออาจนำไปบอกต่อผ่านโซเชียล และยังพบว่า นอกจากนั้น Social Proof เกิดจากสิ่งที่แบรนด์แพลตฟอร์มออนไลน์ไต่ยืนได้ดำเนินธุรกิจแพลตฟอร์มออนไลน์ไต่ยืนมาอย่างยาวนานและได้รับการันตีรางวัลแพลตฟอร์มออนไลน์ไต่ยืนดีเด่นระดับโลก มีจำนวนลูกค้าที่ใช้งานแพลตฟอร์มออนไลน์ไต่ยืนทั่วโลก รางวัลด้านคุณภาพดีเด่น และรางวัลด้านการบริการที่ดี เป็นต้น

การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน ดำเนินการภายใต้กรอบของกลยุทธ์หลัก 5 ประการที่ทำงานร่วมกันอย่างเป็นระบบ ผู้วิจัยได้สรุปเป็นแผนภาพกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน ตามผลการวิเคราะห์ข้อมูลเชิงคุณภาพด้านกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน โดยแสดงเป็นภาพที่ 4.1 ดังนี้



ภาพที่ 4.1 กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่สวน

4.2 การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ ยีน

การศึกษา การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน ด้วยการนำผลการวิเคราะห์จากการสัมภาษณ์เชิงลึก (In-depth Interview) ผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้บริหารระดับปฏิบัติการ และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต่ยีนที่รับผิดชอบการส่งเสริมสนับสนุนหรือการพัฒนาความปลอดภัยระบบสารสนเทศเพื่อสร้างความปลอดภัยของข้อมูล และปกป้องการรั่วไหลของสารสนเทศส่วนบุคคลของแพลตฟอร์มออนไลน์ไต่ยีนที่ส่งผลต่อความนิยมในการใช้แพลตฟอร์มออนไลน์ไต่ยีนของประชาชนทั้งในประเทศจีน และประเทศต่าง ๆ ทั่วโลก จำนวน 20 คน และผลการวิเคราะห์ข้อมูลเชิงปริมาณด้านความคาดหวังต่อการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน และความต้องการการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน โดยการเก็บรวบรวมข้อมูลจากผู้ใช้แพลตฟอร์มออนไลน์ไต่ยีนใน 4 ภูมิภาคของประเทศจีน คือ 1) ภาคตะวันออกมณฑลซานตง 2) ภาคเหนือมณฑลเหอหนาน 3) ภาคตะวันตกมณฑลเสฉวน 4) ภาคใต้มณฑลกวางตุ้ง จำนวน 400 คน จากนั้นทำการนำข้อมูลที่ได้จากการวิเคราะห์ผลการสัมภาษณ์เชิงลึก (In-depth Interview) และผลข้อมูลจากการวิเคราะห์เชิงปริมาณ มาสรุปเป็น จุดแข็ง จุดอ่อน โอกาส และอุปสรรคของการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน ด้วยเทคนิคการวิเคราะห์ SWOT เพื่อประเมิน จุดแข็ง จุดอ่อน โอกาส และอุปสรรค เพื่อพัฒนาเป็นรูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน โดยกลุ่มเป้าหมายที่เข้าร่วมระดมสมองจำนวน 20 คน และได้มีการประชุมสนทนากลุ่ม (Focus group) เพื่อพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน โดยใช้เทคนิคการวิเคราะห์ SWOT ในการประเมินจุดแข็ง (Strengths) จุดอ่อน (Weaknesses) โอกาส (Opportunities) และอุปสรรค (Threats) เพื่อกำหนดรูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน ที่เหมาะสมสำหรับแพลตฟอร์มออนไลน์ไต่ยีน ซึ่งผลการวิเคราะห์แบ่งออกเป็น 2 ส่วน ได้แก่

1. ผลการวิเคราะห์ จุดแข็ง จุดอ่อน โอกาส อุปสรรค ของแพลตฟอร์มออนไลน์ไต่ยีน และ
2. ผลการวิเคราะห์ข้อมูลการสนทนากลุ่ม (Focus group) การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน

ผลการศึกษาพบว่า

1. ผลการวิเคราะห์ข้อมูล จุดแข็ง จุดอ่อน โอกาส และอุปสรรค โดยภาพรวมของการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน สามารถสรุปได้ดังนี้

1) จุดแข็ง (Strengths)

การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน เป็นนโยบายที่ผู้บริหารทุกระดับ และผู้พัฒนาแพลตฟอร์มออนไลน์ไต่ยีน ให้ความสำคัญโดยมีการจัดตั้งหน่วยงานด้านความปลอดภัยระบบสารสนเทศ การพัฒนาบุคลากรด้านความปลอดภัยเป็นประจำเพื่อให้ทันต่อการเปลี่ยนของ

เทคโนโลยี และพฤติกรรมการเปิดรับข่าวสารของประชาชนผู้ใช้แพลตฟอร์ม หากเกิดปัญหาความไม่ปลอดภัยระบบสารสนเทศ จะมีระบบคัดกรองข้อมูลที่ได้มาตรฐาน ISO/IEC 27001 ที่เป็นมาตรฐานสากลที่ได้รับการยอมรับอย่างกว้างขวางที่สุดสำหรับการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System - ISMS) ซึ่งเป็นระบบที่ช่วยให้แพลตฟอร์มออนไลน์ไต่ยืนสามารถปกป้องข้อมูลสำคัญของตนได้อย่างเป็นระบบและมีประสิทธิภาพไม่ว่าจะเป็นข้อมูลลูกค้า ข้อมูลทางการเงิน หรือทรัพย์สินทางปัญญา ISO 27001 ช่วยสร้างระบบป้องกันสารสนเทศที่แข็งแกร่ง เพื่อป้องกันการรั่วไหล การสูญหาย หรือการถูกโจมตีทางไซเบอร์ ส่งผลให้ผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนเกิดความมั่นใจต่อระบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนและยังช่วยเพิ่มความน่าเชื่อถือ การได้รับการรับรอง ISO 27001 เป็นเครื่องยืนยันว่าแพลตฟอร์มออนไลน์ไต่ยืนให้ความสำคัญกับความปลอดภัยของข้อมูล ซึ่งสร้างความมั่นใจให้กับลูกค้า คู่ค้า และผู้มีส่วนได้เสีย ส่งผลให้แพลตฟอร์มออนไลน์ไต่ยืนได้เปรียบในการแข่งขัน ในตลาดที่ความปลอดภัยของข้อมูลเป็นปัจจัยสำคัญ ISO 27001 ช่วยให้องค์กรแพลตฟอร์มออนไลน์ไต่ยืนโดดเด่นและเป็นที่น่าเชื่อถือ และยังพบว่า แพลตฟอร์มออนไลน์ไต่ยืนปฏิบัติตามกฎหมายเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศของรัฐบาลจีนอย่างเคร่งครัด และแพลตฟอร์มออนไลน์ไต่ยืนยังได้ปฏิบัติตามข้อบังคับมาตรฐาน ISO 27001 ช่วยให้แพลตฟอร์มออนไลน์ไต่ยืนสามารถปฏิบัติตามข้อกำหนดด้านความปลอดภัยของข้อมูล เช่น GDPR (General Data Protection Regulation) ได้อย่างมีประสิทธิภาพ

2. จุดอ่อน (Weaknesses)

การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน พบว่า กระบวนการปฏิบัติงานบางส่วนของการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนยังเป็นแบบแมนนวลที่ใช้เวลานานเกินไปทำให้การระบุและตอบสนองต่อภัยคุกคามทางไซเบอร์เกิดความล่าช้า และเพิ่มค่าใช้จ่ายในการดำเนินงานการป้องกันความปลอดภัยระบบสารสนเทศในลักษณะเชิงรับที่ขาดการตรวจจับภัยคุกคามทางไซเบอร์เชิงรุก ส่งผลให้ผู้พัฒนาแพลตฟอร์ม และผู้ใช้แพลตฟอร์มเกิดเป็นความกังวลอันดับต้น ๆ ทั้งในประเทศจีนเอง และความกังวลเรื่องความปลอดภัยระบบสารสนเทศในระดับภูมิภาคต่างๆ ที่นิยมใช้แพลตฟอร์มออนไลน์ไต่ยืน และพบว่า แพลตฟอร์มออนไลน์ไต่ยืน มีบุคลากรที่มีทักษะด้านการจัดการความปลอดภัยสารสนเทศน้อย ไม่เพียงพอต่อการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน ซึ่งในปัจจุบันกำลังได้รับความนิยมมากทั้งภายในประเทศและต่างประเทศ ทำให้การบริหารจัดการระบบรักษาความปลอดภัยทางไซเบอร์เป็นไปอย่างยากลำบาก และยังพบว่า ความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนมีความซับซ้อนในการจัดการโซลูชันรักษาความปลอดภัยในแต่ละระดับที่แตกต่างกัน นำไปสู่ช่องว่างในการป้องกันความปลอดภัยระบบสารสนเทศ ส่งผลให้บุคลากรทำการกำหนดค่าความปลอดภัยที่อาจผิดพลาด และอาจจะเกิดความเสี่ยงความปลอดภัยของระบบสารสนเทศที่เพิ่มขึ้น

ผลการสำรวจจุดอ่อนด้านการบริหารจัดการความปลอดภัยทางไซเบอร์ระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน และการเตรียมพร้อมรับมือการถูกโจมตีทางไซเบอร์กับความท้าทายด้านความ

ปลอดภัยระบบสารสนเทศในอนาคตของแพลตฟอร์มออนไลน์ไต่ยืนในปัจจุบัน โดยข้อมูลการสัมภาษณ์ผู้บริหาร และผู้พัฒนาแพลตฟอร์มออนไลน์แพลตฟอร์มออนไลน์ไต่ยืนด้านกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศ และข้อมูลเชิงปริมาณด้านความคาดหวังต่อการจัดการความปลอดภัยระบบสารสนเทศและความต้องการการจัดการความปลอดภัยระบบสารสนเทศ พบว่า 98% ต้องการปรับปรุงระบบเพื่อเพิ่มการป้องกันสูงสุดถึงแม้ว่าข้อมูลจากผู้บริหารทุกระดับ และผู้พัฒนาแพลตฟอร์มออนไลน์ไต่ยืนเป็นผู้รับผิดชอบต่อการจัดการความปลอดภัยระบบสารสนเทศจะมีกลยุทธ์การจัดการด้านความปลอดภัยระบบสารสนเทศที่ครอบคลุม และผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนจะมีระดับความคาดหวัง และความต้องการการจัดการด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนจนอยู่ในระดับที่มีความเชื่อมั่นถึงการรักษาความปลอดภัยระบบสารสนเทศ ต่อระบบป้องกันภัยของแพลตฟอร์มออนไลน์ไต่ยืนในปัจจุบันที่สูง และมีเพียง 6% เท่านั้นที่แสดงความไม่เชื่อมั่นต่อมาตรการรักษาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน แต่ยังคงมีความคาดหวัง และต้องการระบบป้องกันภัยระบบสารสนเทศที่แข็งแกร่งมากขึ้นและปรับเปลี่ยนได้มากขึ้น

และยังพบว่า แพลตฟอร์มออนไลน์ไต่ยืนยังมีจุดอ่อนด้านกระบวนการจัดการความปลอดภัยแบบแมนนวลที่ก่อให้เกิดค่าใช้จ่ายในการดำเนินงานด้านความปลอดภัยระบบสารสนเทศที่เพิ่มขึ้น และเกิดความล่าช้าในการระบุและตอบสนองต่อภัยคุกคามทางไซเบอร์ ในขณะที่จุดที่สำคัญที่สุดคือการจัดการโซลูชันรักษาความปลอดภัยที่แตกต่างกันหลายโซลูชันของแพลตฟอร์มออนไลน์ไต่ยืน ทำให้เกิดช่องว่างในการครอบคลุม การกำหนดค่าที่ผิดพลาด และความเสี่ยงที่เพิ่มขึ้นจากการกำกับดูแลที่ผ่านมาที่รักษาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนต้องดิ้นรนเพื่อรักษาการป้องกันแบบบูรณาการและมีประสิทธิภาพในระบบที่หลากหลาย การแยกส่วนนี้ขัดขวางเวลาในการตอบสนองที่รวดเร็วและเพิ่มโอกาสในการมองข้ามช่องโหว่ ซึ่งท้ายที่สุดแล้วจะทำให้สถานะความปลอดภัยโดยรวมของของแพลตฟอร์มออนไลน์ไต่ยืนอ่อนแอลง

3) โอกาส (Opportunities)

การมาถึงของยุคดิจิทัลได้เปลี่ยนแปลงภูมิทัศน์ของการสื่อสารไปอย่างสิ้นเชิง จากการส่งจดหมายที่ต้องใช้เวลาหลายวันสู่การส่งข้อความถึงกันได้ในวันเดียวความเปลี่ยนแปลงนี้ไม่ได้จำกัดอยู่แค่ความเร็ว แต่ยังส่งผลกระทบอย่างลึกซึ้งต่อวิถีชีวิต การทำงาน และปฏิสัมพันธ์ทางสังคมของมนุษย์ นำมาซึ่งโอกาสที่เป็นประโยชน์นานัปการของแพลตฟอร์มออนไลน์ไต่ยืนที่พลิกการสื่อสารยุคดิจิทัลที่มากกว่าแค่การส่งข้อความ ด้วยการสร้างโอกาสให้กับแพลตฟอร์มออนไลน์ไต่ยืน ดังนี้

1. ประสิทธิภาพที่เหนือกว่า: ลดเวลา เพิ่มผลลัพธ์ ยุคดิจิทัลทำให้การสื่อสารรวดเร็วและมีประสิทธิภาพมากขึ้นอย่างเห็นได้ชัด การส่งอีเมล การประชุมออนไลน์ หรือการใช้แพลตฟอร์มการทำงานร่วมกัน ช่วยลดระยะเวลาและค่าใช้จ่ายในการเดินทาง ประชุม และแลกเปลี่ยนข้อมูล สิ่งนี้ช่วยให้แพลตฟอร์มออนไลน์ไต่ยืนสามารถตอบสนองต่อสถานการณ์ต่าง ๆ ได้อย่างทันท่วงที่ ตัดสินใจได้อย่างรวดเร็ว และทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

2. ชุมทรัพย์แห่งข้อมูล: เข้าถึงความรู้ได้ง่ายดาย อินเทอร์เน็ตเปรียบเสมือนห้องสมุดขนาดใหญ่ที่รวบรวมข้อมูลและความรู้จากทั่วทุกมุมโลกที่แพลตฟอร์มออนไลน์ไต่ยนสามารถเข้าถึงบทความวิจัย ข่าวสาร เทคนิคต่าง ๆ และข้อมูลอื่นๆ ที่จำเป็นต่อการเรียนรู้และการพัฒนาตนเองได้อย่างง่ายดาย เพียงแค่ปลายนิ้วสัมผัส ความสามารถในการเข้าถึงข้อมูลที่หลากหลายและทันสมัยนี้ช่วยให้แพลตฟอร์มออนไลน์ไต่ยนสามารถตัดสินใจได้อย่างชาญฉลาดและปรับตัวเข้ากับการเปลี่ยนแปลงได้อย่างรวดเร็ว

3. โลกไร้พรมแดน: การเชื่อมต่อข้ามวัฒนธรรมการสื่อสารยุคดิจิทัลช่วยลดอุปสรรคทางภูมิศาสตร์และวัฒนธรรมทำให้แพลตฟอร์มออนไลน์ไต่ยนสามารถเชื่อมต่อกับผู้คนจากทั่วโลก แลกเปลี่ยนความรู้ ความคิดเห็น และประสบการณ์ได้อย่างอิสระ การเชื่อมต่อนี้ส่งเสริมความเข้าใจอันดีระหว่างวัฒนธรรม สร้างความร่วมมือ และเปิดโอกาสให้เราได้เรียนรู้และเติบโตจากมุมมองที่หลากหลาย

4. สร้างเครือข่ายและโอกาส: เส้นทางสู่ความสำเร็จแพลตฟอร์มออนไลน์ไต่ยนซึ่งเป็นแพลตฟอร์มโซเชียลมีเดียและเครือข่ายออนไลน์ต่างๆ เป็นเครื่องมือที่ทรงพลังในการสร้างเครือข่าย การเชื่อมต่อกับผู้คนที่มีความสนใจร่วมกัน หรือแม้กระทั่งการค้นหาโอกาสทางธุรกิจและการเรียนรู้ การสร้างเครือข่ายเหล่านี้ไม่เพียงแต่ช่วยให้แพลตฟอร์มออนไลน์ไต่ยนได้รับคำแนะนำและการสนับสนุน แต่ยังเปิดโอกาสให้แพลตฟอร์มออนไลน์ไต่ยนได้แสดงศักยภาพและสร้างชื่อเสียงในวงการต่าง ๆ

5. กระจายโอกาสอย่างเท่าเทียม: เสียงของทุกคนมีความหมาย แพลตฟอร์มออนไลน์ไต่ยนในปัจจุบันซึ่งเป็นยุคดิจิทัลเปิดโอกาสให้ผู้คนจากทุกชนชั้น ทุกภูมิภาค และทุกความสามารถสามารถเข้าถึงข้อมูลและแสดงความคิดเห็นได้อย่างเท่าเทียมกัน แพลตฟอร์มออนไลน์ไต่ยน เป็นพื้นที่ให้กลุ่มคนที่ด้อยโอกาสสามารถแสดงพลัง สร้างความตระหนักรู้ และเรียกร้องสิทธิของตนเอง การกระจายโอกาสนี้ช่วยสร้างสังคมที่เท่าเทียมและยุติธรรมมากขึ้น

6. การเรียนรู้ตลอดชีวิต: พัฒนาตนเองอย่างต่อเนื่อง ด้วยแหล่งข้อมูลและความรู้มากมายที่เข้าถึงได้ง่าย แพลตฟอร์มออนไลน์ไต่ยนเป็นแพลตฟอร์มของการสื่อสารยุคดิจิทัลที่ช่วยส่งเสริมการเรียนรู้ตลอดชีวิต เราสามารถเรียนรู้ทักษะใหม่ ๆ ติดตามข่าวสารล่าสุด และพัฒนาตนเองอย่างต่อเนื่อง ไม่ว่าจะเป็นการเรียนคอร์สออนไลน์ การเข้าร่วมสัมมนาผ่านเว็บ หรือการอ่านบทความต่างๆ การเรียนรู้ตลอดชีวิตนี้ช่วยให้ประชาชนสามารถปรับตัวเข้ากับการเปลี่ยนแปลงของโลกได้อย่างรวดเร็วและประสบความสำเร็จในระยะยาว

4) อุปสรรค (Threats)

ปัญหาและอุปสรรคในการสื่อสาร : สร้างความเข้าใจที่ตรงกัน ฝ่าฟันอุปสรรคที่ขวางกั้น การสื่อสารเป็นหัวใจสำคัญของการอยู่ร่วมกันในสังคม ไม่ว่าจะเป็นในระดับบุคคล องค์กร หรือแม้แต่ว่าระดับประเทศ การสื่อสารที่มีประสิทธิภาพนำไปสู่ความเข้าใจอันดี ลดความขัดแย้ง และส่งเสริมความร่วมมือ แต่ในความเป็นจริงการสื่อสารไม่ใช่เรื่องง่ายเสมอไป ผู้สื่อสารมักเผชิญกับปัญหาและอุปสรรคต่างๆ ที่ขัดขวางการสื่อสารไม่ให้เป็นไปอย่างราบรื่น ปัญหาและอุปสรรคของแพลตฟอร์มออนไลน์ไต่ยนที่ใช้ในการสื่อสารนั้นมีอุปสรรค 5 รูปแบบดังนี้

1. อุปสรรคด้านภาษา: ภาษาเป็นเครื่องมือหลักในการสื่อสารผ่านแพลตฟอร์มออนไลน์ไต้หวัน ประเทศจีนมีความหลากหลายทางภาษา และมีความหลากหลายทางวัฒนธรรม ความแตกต่างทางภาษา วัฒนธรรม และภูมิหลังของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน อาจก่อให้เกิดความเข้าใจผิดในการสื่อสารผ่านแพลตฟอร์มออนไลน์ไต้หวัน คำศัพท์บางคำอาจมีความหมายแตกต่างกันในแต่ละบริบท หรือสำเนียงที่แตกต่างกันอาจทำให้การสื่อสารในแพลตฟอร์มออนไลน์ไต้หวันเป็นไปอย่างยากลำบาก

2. อุปสรรคด้านจิตใจ: อารมณ์ ความรู้สึก ทศนคติ และอคติส่วนตัว ล้วนมีผลต่อการรับรู้และการตีความสารผ่านแพลตฟอร์มออนไลน์ไต้หวัน หากผู้รับสารอยู่ในภาวะอารมณ์ที่ไม่ดี หรือมีอคติต่อผู้ส่งสารที่เป็นแพลตฟอร์มออนไลน์ไต้หวัน ก็อาจทำให้เกิดการตีความในแพลตฟอร์มออนไลน์ไต้หวันที่ผิดเพี้ยนไปจากความเป็นจริง

3. อุปสรรคด้านกายภาพ: สภาพแวดล้อมที่ไม่เอื้ออำนวย เช่น เสียงดังรบกวน แสงสว่างไม่เพียงพอ หรือระยะทางที่ห่างไกล ระบบอินเทอร์เน็ตที่ไม่ครอบคลุม ก็เป็นอุปสรรคสำคัญในการสื่อสารผ่านแพลตฟอร์มออนไลน์ไต้หวัน

4. อุปสรรคด้านเทคโนโลยี: แม้ว่าเทคโนโลยีแพลตฟอร์มออนไลน์ไต้หวันจะช่วยอำนวยความสะดวกในการสื่อสาร แต่ก็อาจเป็นอุปสรรคได้เช่นกัน ปัญหาด้านสัญญาณอินเทอร์เน็ต ระบบขัดข้อง หรือความไม่คุ้นเคยกับการใช้งานแพลตฟอร์มออนไลน์ไต้หวัน อาจทำให้การสื่อสารล่าช้า หรือไม่ประสบความสำเร็จ

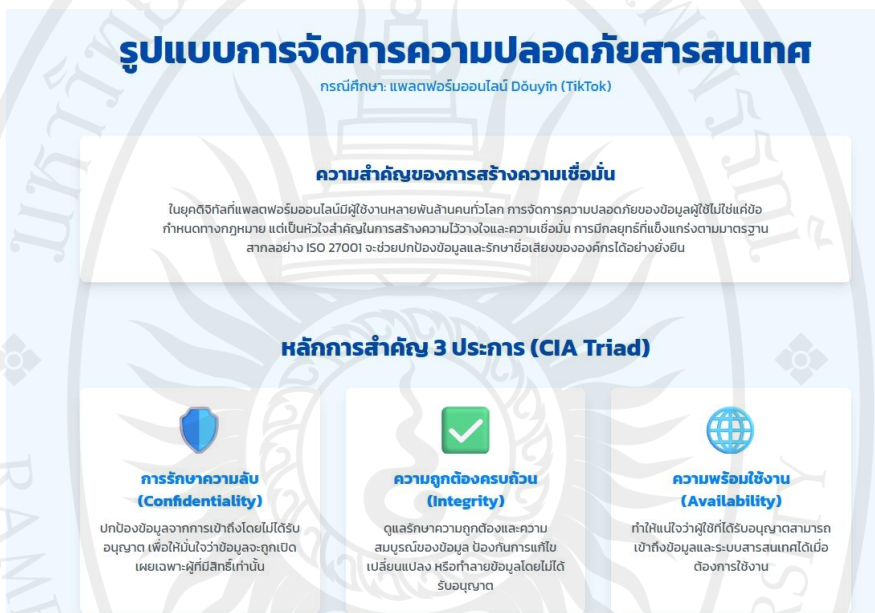
5. อุปสรรคด้านข้อมูล: ข้อมูลที่ไม่ถูกต้อง ไม่ครบถ้วน หรือไม่ชัดเจนในแหล่งข้อมูลที่แพลตฟอร์มออนไลน์ไต้หวัน หรือผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันนำมาใช้ ย่อมนำไปสู่ความเข้าใจผิดและความสับสน แพลตฟอร์มออนไลน์ไต้หวันเป็นแพลตฟอร์มที่ผู้ใช้ทุกคนสามารถเติมแต่งความคิดเห็นส่วนตัวได้ ทำให้ข้อมูลในแพลตฟอร์มออนไลน์ไต้หวันอาจบิดเบือนไปจากความเป็นจริง

2. ผลการวิเคราะห์ข้อมูลการสนทนากลุ่ม (Focus group) การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

ผลการวิเคราะห์ข้อมูลการสนทนากลุ่ม (Focus group) ตามแนวทางจากการสัมภาษณ์ผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้บริหารระดับปฏิบัติการ และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวัน มาสังเคราะห์เป็น “การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน”

การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน เป็นระบบการให้บริการข้อมูลที่มีอยู่บนเครื่องคอมพิวเตอร์และในเครือข่ายขนาดใหญ่ของแพลตฟอร์มออนไลน์ไต้หวัน ที่ถือว่าเป็นทรัพย์สินส่วนบุคคลและขององค์กรที่ใช้แพลตฟอร์มออนไลน์ไต้หวันที่สำคัญ ความสมบูรณ์ของสินทรัพย์ที่เป็นระบบสารสนเทศนี้อาจมีผลกระทบทางการสื่อสาร ทางธุรกิจ และทางการเงินหรือกระทบอื่น ๆ แพลตฟอร์มออนไลน์ไต้หวันในฐานะผู้ดูแลระบบต้องคำนึงถึงความมั่นคงปลอดภัยระบบเครือข่ายสารสนเทศ โดยต้องสามารถรักษาความลับ (Confidentiality) ความสมบูรณ์

(Integrity) และความพร้อมใช้งาน (Availability) หรือเรียกว่า CIA ของระบบความปลอดภัยสารสนเทศ ประกอบด้วยความปลอดภัยของข้อมูล ความปลอดภัยของระบบ ความปลอดภัยของซอฟต์แวร์ และความปลอดภัยของฮาร์ดแวร์ ที่มีการใช้งานในการสื่อสารบนแพลตฟอร์มออนไลน์ไต่ยืน เพื่อสร้างความมั่นใจให้กับลูกค้าผู้ใช้บริการแพลตฟอร์มออนไลน์ไต่ยืน ในลักษณะของการบูรณาการรูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน แสดงดังภาพที่ 4.2



ภาพที่ 4.2 รูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน

แพลตฟอร์มออนไลน์ไต่ยืนและบุคลากรผู้รับผิดชอบจำเป็นต้องให้ความสำคัญกับการจัดการด้านความมั่นคงปลอดภัยระบบสารสนเทศซึ่งเป็นข้อมูลเพื่อปกป้องความมั่นคงปลอดภัยของข้อมูล ป้องกันภัยคุกคามและความเสียหายที่อาจเกิดขึ้น การจัดการความปลอดภัยระบบสารสนเทศยังช่วยลดความเสี่ยงจากการละเมิดด้านข้อมูล การดูแลป้องกันระบบสารสนเทศหรือข้อมูลของแพลตฟอร์มออนไลน์ไต่ยืนไว้ก่อนย่อมดีกว่าการแก้ไขซึ่งจะส่งผลกระทบอย่างรุนแรงในภายหลัง นอกจากนี้เมื่อมีการจัดการความปลอดภัยระบบสารสนเทศอย่างถูกต้องแล้วจะทำให้ธุรกิจของแพลตฟอร์มออนไลน์ไต่ยืนได้รับความเชื่อถือ และลูกค้าที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนมีความมั่นใจเป็นอย่างมาก มาตรฐานระบบการจัดการความปลอดภัยสารสนเทศเป็นประโยชน์สำหรับธุรกิจทุกประเภท และแพลตฟอร์มออนไลน์ไต่ยืนได้รับการออกแบบมาเพื่อส่งเสริมการสื่อสารออนไลน์ รวมถึงการส่งเสริมธุรกิจและองค์กรทุกประเภท ทุกขนาด การจัดการความปลอดภัยระบบสารสนเทศที่ได้มาตรฐาน ISO 27001 จึงเป็นแนวทางเชิงระบบที่แพลตฟอร์มออนไลน์ไต่ยืนนำมาใช้ในการจัดการความปลอดภัยระบบสารสนเทศ ประกอบด้วยกระบวนการ เทคโนโลยี และบุคคลที่ช่วยปกป้องและจัดการกับข้อมูลสารสนเทศขององค์กรและผู้ใช้

แพลตฟอร์มออนไลน์ไต้ยีน ด้วยการจัดการความเสี่ยงที่มีประสิทธิภาพอย่างถูกต้องและครอบคลุม โดยมีหลักการที่สำคัญ 3 ประการ ได้แก่ การปกป้องข้อมูลให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น การปกป้องความถูกต้องครบถ้วนของข้อมูลสารสนเทศ และความพร้อมใช้งานของระบบสารสนเทศที่มีความปลอดภัยของข้อมูล

การพัฒนาารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน มีประโยชน์ต่อการจัดการความปลอดภัยสารสนเทศ สามารถอธิบาย ได้ดังนี้

1. ช่วยให้แพลตฟอร์มออนไลน์ไต้ยีนมีการปรับปรุงระบบสารสนเทศอย่างต่อเนื่อง
2. ช่วยปกป้องชื่อเสียงขององค์กรไต้ยีนจากภัยคุกคามด้านความมั่นคงปลอดภัยของสารสนเทศ
3. ช่วยให้องค์กรไต้ยีนสามารถปฏิบัติตามข้อกำหนดด้านการปกป้องข้อมูลสารสนเทศอย่างสอดคล้อง
4. ช่วยให้แพลตฟอร์มออนไลน์ไต้ยีนมั่นใจในการจัดการความปลอดภัยระบบสารสนเทศ
5. สามารถสร้างความน่าเชื่อถือและไว้วางใจสำหรับองค์กรและลูกค้าผู้ใช้แพลตฟอร์มออนไลน์
6. สามารถสร้างความได้เปรียบทางการแข่งขันระหว่างแพลตฟอร์มออนไลน์ไต้ยีนและแพลตฟอร์มออนไลน์อื่น ๆ

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

บทที่ 5

สรุป อภิปรายผล และข้อเสนอแนะ

การศึกษาเรื่องนี้ มีวัตถุประสงค์ดังนี้ 1) เพื่อศึกษากลยุทธ์การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน 2) การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

ในการวิจัยเชิงปริมาณ ประชากรในการวิจัย คือ ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันในประเทศจีน โดยการเก็บรวบรวมข้อมูลจากผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ใน 4 ภูมิภาคของประเทศจีน 1) ภาคตะวันออกมณฑลชานตง 2) ภาคเหนือมณฑลเหอหนาน 3) ภาคตะวันตกมณฑลเสฉวน 4) ภาคใต้มณฑลกว่างตง จำนวน 400 คน

ในการวิจัยเชิงคุณภาพ ผู้วิจัยได้กำหนดแนวทางสำคัญในการเก็บรวบรวมข้อมูล โดยการขอความร่วมมือจากองค์กรภาครัฐผู้กำกับดูแลนโยบายความปลอดภัยระบบสารสนเทศ ผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวัน และบุคคลากรที่มีหน้าที่ส่งเสริมสนับสนุนความปลอดภัยระบบสารสนเทศหรือแพลตฟอร์มออนไลน์ในกรุงปักกิ่ง ที่เป็นตัวแทนของกลุ่มผู้ให้ข้อมูลสำคัญ เพื่อขอสัมภาษณ์อย่างเป็นทางการจากบุคคลที่เป็นเจ้าหน้าที่ภาครัฐภาคเอกชนที่เป็นผู้บริหารและผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวันที่รับผิดชอบการส่งเสริมสนับสนุนหรือการพัฒนาความปลอดภัยระบบสารสนเทศ จำนวน 20 คน ผู้วิจัยดำเนินการบันทึกข้อมูลโดยวิธีการจดบันทึกข้อมูลและการบันทึกเสียงของผู้ให้สัมภาษณ์เพื่อนำมาใช้ในการตรวจสอบและตรวจทานความถูกต้องย้อนกลับในภายหลังได้ และการนำผลการวิเคราะห์ข้อมูลจากการวิจัยเชิงปริมาณด้านความคาดหวังและความต้องการการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และข้อมูลผลการวิเคราะห์ข้อมูลเชิงคุณภาพด้านกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน มาเป็นข้อมูลพื้นฐานในการพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

การวิจัยครั้งนี้ผู้วิจัยได้นำเสนอเอกสาร และงานวิจัยที่เกี่ยวข้องมาใช้ในการอ้างอิง เพื่อเป็นแนวทางในการกำหนดตัวแปร ซึ่งประกอบด้วย แนวคิดทฤษฎีเกี่ยวกับการสื่อสารผ่านสื่อออนไลน์ แนวคิดเกี่ยวกับการพัฒนารูปแบบ แนวคิดเกี่ยวกับกลยุทธ์ แนวคิดเกี่ยวกับความคาดหวังและความต้องการ และงานวิจัยที่เกี่ยวข้อง โดยนำมาสร้างเครื่องมือแบบสอบถาม แบบสัมภาษณ์ ระบุตัวแปรในกรอบแนวคิด เพื่อให้มีความสอดคล้องกับวัตถุประสงค์ของการวิจัย โดยผู้วิจัยได้ศึกษาและตอบวัตถุประสงค์ โดยได้ข้อสรุปผลการศึกษา อภิปรายผล และข้อเสนอแนะ ซึ่งจะนำเสนอรายละเอียดดังนี้

5.1 สรุปผลการวิจัย

การวิจัยเรื่อง การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ผู้ศึกษาสรุปผลการวิจัยตามวัตถุประสงค์ของการวิจัย ดังนี้

5.1.1 ผลการศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน 5 กลยุทธ์ ดังนี้

1. กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน พบว่า ถูกกำหนดให้เป็นกลยุทธ์ด้านความปลอดภัยในยุคดิจิทัล เป็นไปตามกฎหมายความปลอดภัยทางไซเบอร์ของรัฐบาล นโยบายด้านความปลอดภัยระบบสารสนเทศที่ต้องปฏิบัติตามอย่างเคร่งครัด และพบว่า แพลตฟอร์มออนไลน์ไต้หวันมีการจัดตั้งแผนกนวัตกรรมการใช้แพลตฟอร์มออนไลน์ไต้หวัน เพื่อรับผิดชอบงานด้านความปลอดภัยระบบสารสนเทศขึ้นมีหน้าที่การรักษาความปลอดภัยของข้อมูลให้อยู่ในมาตรฐานที่เหมาะสม มีการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต และมีมาตรการในการแก้ไขหรือเปลี่ยนแปลงข้อมูล โดยต้องกระทำจากผู้มีสิทธิ์ในการเข้าถึงเท่านั้น และพบว่า พนักงานทั่วไปของแพลตฟอร์มออนไลน์ไต้หวันไม่สามารถดูข้อมูลลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันได้เนื่องจากไม่ได้ทำกิจกรรมใด ๆ ที่เกี่ยวข้องกับลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน นอกจากพนักงานที่อยู่ฝ่ายด้านความปลอดภัยระบบสารสนเทศเท่านั้นเพื่อป้องกันผู้ไม่เกี่ยวข้องนำข้อมูลสารสนเทศไปใช้ในทางที่ผิด โดยการรักษาความปลอดภัยของข้อมูลของแพลตฟอร์มออนไลน์ไต้หวันมีระบบจัดการอย่างรัดกุมและมีการทบทวนการปฏิบัติให้เป็นไปตามข้อกำหนดอยู่เสมอในการรักษาความปลอดภัยข้อมูล แอปพลิเคชันและผู้ใช้

2. กลยุทธ์การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน พบว่า แพลตฟอร์มออนไลน์ไต้หวันให้ความสำคัญต่อการจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศทางไซเบอร์ให้ถือว่าเป็นภารกิจสำคัญสำหรับแพลตฟอร์มออนไลน์ไต้หวันในการปกป้องข้อมูลที่ละเอียดอ่อนของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน โดยการตั้งหน่วยงานตรวจสอบภายในที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านความปลอดภัยระบบสารสนเทศเป็นประจำทุกปี และดำเนินการร่วมกับแผนกนวัตกรรมการใช้แพลตฟอร์มออนไลน์ไต้หวัน เพื่อตรวจสอบระบบความปลอดภัยสารสนเทศที่มีความซับซ้อนและความถี่ของภัยคุกคามทางไซเบอร์ที่ปัจจุบันมีแนวโน้มเพิ่มสูงมากขึ้น และพบว่า ผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน ใช้แนวทางเชิงรุกด้วยมาตรการความปลอดภัยระบบสารสนเทศโดยการกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศเพื่อที่จะสามารถระบุความไม่ปลอดภัย ประเมินความไม่ปลอดภัย และลดความเสี่ยงที่จะเกิดความไม่ปลอดภัยจากการใช้สารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างมีประสิทธิภาพ ด้วยการนำกรอบงานด้านความปลอดภัยทางไซเบอร์ที่เป็นมาตรฐานสากลที่ได้รับการยอมรับทั่วโลกมาใช้เพื่อรักษาความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างจริงจัง

3. กลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัยของแพลตฟอร์มออนไลน์ไต้หวัน

พบว่า แพลตฟอร์มออนไลน์ไต้หวัน ตระหนักถึงการใช้สื่อสังคมออนไลน์ซึ่งปัจจุบันประชาชนจีนนิยมใช้กันอย่างแพร่หลาย ซึ่งเกิดผลกระทบที่อาจเกิดขึ้นทั้งด้านที่เกิดเป็นประโยชน์และด้านที่เป็นเชิงลบหรือเป็นโทษต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน โดยเฉพาะหากมีการเผยแพร่ข้อมูลที่ไม่เหมาะสมออกสู่สาธารณะ ซึ่งอาจก่อให้เกิดความเสียหายต่อตนเอง ผู้อื่น และองค์กร และพบว่า ผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน มีการกำหนดนโยบายการกำกับดูแลความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ซึ่งจัดทำขึ้นเพื่อให้การใช้แพลตฟอร์มออนไลน์ไต้หวันของประชาชน มีความเหมาะสม เป็นประโยชน์ และหลีกเลี่ยงผลกระทบต่อสังคม และการดำเนินงานของแพลตฟอร์มออนไลน์ไต้หวันในอนาคต และพบว่า แพลตฟอร์มออนไลน์ไต้หวัน มีการกำหนดนโยบายและแนวปฏิบัติด้านความปลอดภัยระบบสารสนเทศอย่างเหมาะสมเพื่อให้การดำเนินงานเป็นไปตามตามวัตถุประสงค์ ปณิธาน พันธกิจด้านการให้บริการที่มีประสิทธิภาพและการใช้แพลตฟอร์มออนไลน์ไต้หวันมีความปลอดภัยต่อการใช้ระบบสารสนเทศของแพลตฟอร์ม โดยคำนึงถึงสิทธิและเสรีภาพอย่างมีขอบเขตในการแสดงความคิดเห็นของประชาชนผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

และยังพบว่า แพลตฟอร์มออนไลน์ไต้หวัน มีการส่งเสริมให้ใช้สื่อสังคมออนไลน์ไต้หวันเพื่อการเรียนรู้ การแลกเปลี่ยนความรู้ การเสริมสร้างปฏิสัมพันธ์ทางสังคม วัฒนธรรม การท่องเที่ยว วิชาการ ฯลฯ และการเผยแพร่ข้อมูลหรือข้อคิดเห็นทางความคิดเชิงสร้างสรรค์ ที่ไม่ขัดต่อศีลธรรมอันดีของประชาชนจีน ธรรมเนียมปฏิบัติของสังคม และยังพบอีกว่า แพลตฟอร์มออนไลน์ไต้หวัน ไม่จำกัดสิทธิและเสรีภาพในการใช้สื่อแพลตฟอร์มออนไลน์ไต้หวัน แต่มีข้อกำหนดการใช้แพลตฟอร์มออนไลน์ไต้หวันที่ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันต้องตระหนักถึงสถานภาพความเป็นประชาชนจีนที่มีหน้าที่ในการรักษาวินัย จรรยาบรรณ รวมถึงการรักษาเกียรติและความน่าเชื่อถือทั้งของตนเอง ของสถาบันทางสังคม และประเทศของประชาชนจีน การให้สิทธิเสรีภาพภายใต้ข้อกำหนดในการใช้แพลตฟอร์มออนไลน์ไต้หวันนี้เป็นการสร้างความตระหนักจึงเป็นส่วนหนึ่งของกลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

4. กลยุทธ์การพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

การพัฒนาเศรษฐกิจจีนในปัจจุบันอาศัยศักยภาพจากการสื่อสารที่สะดวกรวดเร็ว ในธุรกิจและกิจการต่าง ๆ เศรษฐกิจในภาพรวมของประเทศจีนที่เติบโตได้อย่างยั่งยืนและมีเสถียรภาพในระยะยาวนั้น พบว่า รัฐบาลจีนให้ความสำคัญกับสถานการณ์ด้านต่าง ๆ และสาระสำคัญในประเด็นการพัฒนาทักษะ (Skills Development) การเตรียมแรงงานให้มีทักษะที่จำเป็นสำหรับทุกอุตสาหกรรม เพื่อให้บุคลากรที่เกี่ยวข้องกับอุตสาหกรรมสื่อสารทั้งภาครัฐ ภาคเอกชน ให้มีความรู้ความเข้าใจเกี่ยวกับสินค้าและบริการต่าง ๆ ในปัจจุบันที่ต้องอาศัยการสื่อสารผ่านแพลตฟอร์มออนไลน์ที่ต้องมีระบบการจัดการด้านความปลอดภัยระบบสารสนเทศที่ดีและมีประสิทธิภาพเพื่อให้กิจการทางธุรกิจต่างๆ ประสบความสำเร็จ และพบว่า แพลตฟอร์มออนไลน์ไต้หวันให้ความสำคัญกับการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศในทุกระดับ ในมิติของการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศ ทำให้บุคลากรด้านระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

ยีน มีความรู้ความเข้าใจและตระหนักถึงคุณค่าและความสำคัญของปัจจัยที่เกี่ยวข้องกับการพัฒนาบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศทั้งระบบ และพบว่า การประสบความสำเร็จของแพลตฟอร์มออนไลน์ไต้หวันมาจากการส่งเสริมและการพัฒนาบุคลากรด้านการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และพบว่า แพลตฟอร์มออนไลน์ไต้หวันให้ความสำคัญกับการพัฒนาบุคลากรด้านการจัดการระบบสารสนเทศในทุกระดับ ซึ่งการพัฒนาบุคลากรด้านการจัดการระบบสารสนเทศเพื่อความปลอดภัย เป็นกลไกสำคัญที่ส่งผลให้แพลตฟอร์มออนไลน์ของไต้หวันไปสู่ความสำเร็จในการพัฒนาแพลตฟอร์มออนไลน์ไต้หวันที่สามารถตอบสนองต่อกิจกรรมการสื่อสาร ที่หลากหลายของประชาชนจีน และพบอีกว่า แพลตฟอร์มออนไลน์ไต้หวัน มีบุคลากรด้านการจัดการระบบสารสนเทศทั้งระบบที่มีศักยภาพ คุณภาพ และคุณธรรมจริยธรรมที่สูงเกิดผลดีและสามารถพัฒนาแพลตฟอร์มออนไลน์ไต้หวัน ให้เข้าไปสู่ความสามารถในการแข่งขันด้านการให้บริการของแพลตฟอร์มออนไลน์ที่สูง เพื่อดึงดูดลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ ทั้งภายในประเทศ และต่างประเทศที่ให้เลือกใช้บริการของแพลตฟอร์มออนไลน์ไต้หวัน

5. กลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

แพลตฟอร์มออนไลน์ไต้หวันมีการสื่อสารข้อกำหนด และนโยบายด้านความปลอดภัยระบบสารสนเทศในการใช้แพลตฟอร์มออนไลน์ไต้หวันเพื่ออธิบายถึงความปลอดภัยระบบสารสนเทศในสิ่งที่แพลตฟอร์มออนไลน์ไต้หวันปฏิบัติอยู่อย่างสม่ำเสมอ พบว่า กลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันส่งผลทำให้ลูกค้าที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันเข้าใจและเกิดความเชื่อมั่นต่อความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ความเชื่อมั่นและความมั่นใจของลูกค้าแพลตฟอร์มออนไลน์ไต้หวันเกิดจากเชื่อใจในแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน และพบว่า แพลตฟอร์มออนไลน์ไต้หวันมีกลยุทธ์สร้างความเชื่อมั่นให้กับผู้ใช้แพลตฟอร์มโดยการนำเสนอข้อมูลข่าวสาร ด้วยข้อมูลที่เป็นจริงมีการตรวจสอบข้อมูลด้วยคนและระบบเทคโนโลยี AI ส่งผลทำให้ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันเกิดความเชื่อมั่นต่อระบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และพบว่า แพลตฟอร์มออนไลน์ไต้หวันใช้ข้อมูลข่าวสารที่เป็นจริงและมีความปลอดภัยสูงส่งผลให้การสื่อสารของแพลตฟอร์มออนไลน์ไต้หวันช่วยสร้างเสริมสร้างภาพลักษณ์ (Brand Image) ที่ดีให้กับแพลตฟอร์มออนไลน์ไต้หวัน ดังนั้นการสร้างการเชื่อใจให้กับแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน (Brand Trust) ต้องสื่อสารอย่างตรงไปตรงมา และพร้อมให้ทุกๆ คนตรวจสอบได้อยู่เสมอ ซึ่งเป็นวิธีการบริหารจัดการที่เหมาะสมกับยุคเทคโนโลยีดิจิทัลที่ทำให้เกิดความโปร่งใสทั้งภายในองค์กรและภายนอกองค์กร และยังอีกพบว่า แพลตฟอร์มออนไลน์ไต้หวัน เป็นแบรนด์ที่สามารถสร้างความเชื่อมั่นและความไว้วางใจให้กับลูกค้าผู้ใช้แพลตฟอร์ม ด้วยการยืนยันด้วยบนความถูกต้องของข้อมูล และความรับผิดชอบหากเกิดความไม่ปลอดภัยของระบบสารสนเทศที่ต้องรับผิดชอบและชดเชยต่อผู้เสียหายอย่างยุติธรรม ซึ่งการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันที่แสดงจุดยืนที่ชัดเจนในเรื่องของความรับผิดชอบที่เป็นธรรมในการทำธุรกิจของแพลตฟอร์มออนไลน์ไต้หวันได้กลายเป็นกลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันแพลตฟอร์มออนไลน์ไต้หวันที่สามารถสร้างความเชื่อใจให้เกิดความรู้สึกดีทั้งกับตัวแบรนด์แพลตฟอร์มออนไลน์ไต้หวันรวมถึงสินค้าและบริการ จนกลุ่มคนผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

เหล่านี้นักกลายเป็น Social Proof ที่ทรงพลัง ที่นำไปบอกต่อทั้งแบบปากต่อปาก (Word-of-Mouth) หรืออาจนำไปบอกต่อผ่านสื่อโซเชียลมีเดีย นอกจากนั้น Social Proof เกิดจากสิ่งที่แพลตฟอร์มออนไลน์ได้ดำเนินธุรกิจแพลตฟอร์มออนไลน์มาอย่างยาวนานและได้รับการันตีรางวัลแพลตฟอร์มออนไลน์ดีเด่นระดับโลก มีจำนวนลูกค้าที่ใช้บริการแพลตฟอร์มออนไลน์ได้ยีนทั่วโลก รางวัลด้านคุณภาพดีเด่น และรางวัลด้านการบริการที่ดี เป็นต้น

5.1.2 การพัฒนารูปแบบการจัดการจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน

โดยนำผลจากการวิเคราะห์ข้อมูลเชิงคุณภาพ และข้อมูลปริมาณ แล้วนำมาสังเคราะห์ตามวัตถุประสงค์ คือ การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน ที่ได้มีการกำหนด การจัดการเชิงกลยุทธ์ความปลอดภัยระบบสารสนเทศ การพัฒนาทักษะความปลอดภัยสารสนเทศของบุคลากร การกำหนดเป้าหมายความปลอดภัยสารสนเทศ การกำหนดนโยบายกำกับดูแลความปลอดภัยระบบสารสนเทศ การสร้างความเชื่อมั่นต่อระบบความปลอดภัยสารสนเทศ ระบบการจัดการความปลอดภัยสารสนเทศ เพื่อเป็นกรอบแนวทางการพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน สามารถสรุปการพัฒนาพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน ดังนี้

1. การจัดการเชิงกลยุทธ์ความปลอดภัยระบบสารสนเทศ

การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน ให้ประสบความสำเร็จแพลตฟอร์มออนไลน์ไต่ยีน จึงมีความจำเป็นต้องดำเนินการดังต่อไปนี้

1.1 จัดหาบุคลากรด้านเทคโนโลยีและความปลอดภัยระบบสารสนเทศและการสื่อสารที่ผ่านการวางแผนบุคลากร การกำหนดตำแหน่งงาน การสรรหาและการเลือกสรรที่มีความสามารถเข้ามาปฏิบัติงานด้านความปลอดภัยสารสนเทศมาประจำในหน่วยงานด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีน

1.2 จัดตั้งหน่วยงานหรือแผนกงานด้านความปลอดภัยของสารสนเทศและเทคโนโลยีที่เหมาะสมกับขนาดและลักษณะงานด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีนที่มีการเติบโตทั้งในประเทศ และขยายตัวในต่างประเทศ

1.3 จัดตั้งบริษัทที่ปรึกษา หรือบุคคลซึ่งมีความรู้ความสามารถด้านการจัดการระบบสารสนเทศ และความปลอดภัยระบบสารสนเทศ ทั้งนี้เนื่องมาจากการขยายตัวและเติบโตอย่างรวดเร็วในประเทศ และต่างประเทศของแพลตฟอร์มออนไลน์ไต่ยีน

1.4 เร่งรีบดำเนินการวางแผนความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีนให้สอดคล้องกับนโยบาย และกฎหมายที่เกี่ยวข้องกับความปลอดภัยระบบสารสนเทศ เพื่อใช้เป็นแนวทางหลักในการพัฒนาระบบความปลอดภัยระบบสารสนเทศที่เกิดจากการสื่อสารผ่านของแพลตฟอร์มออนไลน์ไต่ยีน

1.5 ให้ความสนใจและสนับสนุนงบประมาณ บุคลากร อุปกรณ์ ความรู้ เพื่อให้เกิดการแก้ไขปัญหาความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยีนอย่างจริงจัง

2. การพัฒนาทักษะความปลอดภัยสารสนเทศของบุคลากรของแพลตฟอร์มออนไลน์ไต่ ยิน ต้องดำเนินการ ดังนี้

2.1 ผู้บริหารของแพลตฟอร์มออนไลน์ไต่ยินจำเป็นต้องมีความรู้ในการจัดการ บุคลากรด้านความปลอดภัยระบบสารสนเทศ จะต้องทราบธรรมชาตินิสัยของบุคลากรกลุ่มดังกล่าว ตามที่ได้อธิบายไปแล้วข้างต้น เพื่อให้ผู้บริหารของแพลตฟอร์มออนไลน์ไต่ยิน จะสามารถจัดการ บุคลากรกลุ่มนี้ได้อย่างถูกต้องและเหมาะสม

2.1 ผู้บริหารของแพลตฟอร์มออนไลน์ไต่ยินต้องสร้างระบบผู้เชี่ยวชาญ (Expert System) สืบเนื่องมาจากสาเหตุของการสูญเสียบุคลากรที่มีความรู้และประสบการณ์ด้านความ ปลอดภัยระบบสารสนเทศอยู่เสมอ ซึ่งเป็นเรื่องที่ไม่สามารถหลีกเลี่ยงได้เพราะบุคลากรด้านความ ปลอดภัยสารสนเทศเหล่านั้นปฏิบัติงานมาครบกำหนดเวลา ที่ต้องเกษียณอายุการทำงาน แต่บางครั้ง การสูญเสียก็เป็นเรื่องที่เกิดขึ้นเพราะอุบัติเหตุทำให้แพลตฟอร์มออนไลน์ไต่ยินต้องสูญเสียบุคลากร ด้านความปลอดภัยระบบสารสนเทศไป การสร้างระบบที่สามารถจัดเก็บความรู้และความชำนาญของ ผู้เชี่ยวชาญด้านความปลอดภัยระบบสารสนเทศ เพื่อให้ผู้ที่มีความเชี่ยวชาญน้อยกว่าสามารถ ปฏิบัติงานด้านความปลอดภัยระบบสารสนเทศได้เช่นเดียวกับผู้ที่มีความชำนาญมากกว่า

3. การกำหนดเป้าหมายความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยิน ต้อง ดำเนินการ ดังนี้

3.1 ผู้บริหารของแพลตฟอร์มออนไลน์ไต่ยินต้องให้ความสำคัญกับการกำหนดเป้าหมาย ความปลอดภัยระบบสารสนเทศ และดำเนินการกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศไว้ เป็นแผนกลยุทธ์ด้านความปลอดภัยระบบสารสนเทศซึ่งจะกำหนดเป็นแผนระยะ 5 ปี แต่ต้องมีการ ทบทวนแผนกลยุทธ์ความปลอดภัยสารสนเทศทุกปี ทำให้ผู้บริหารแพลตฟอร์มออนไลน์ไต่ยินสามารถ จัดการกับการเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์ที่วิวัฒนาการตามการพัฒนาของเทคโนโลยี ส่งผลให้แพลตฟอร์มออนไลน์ไต่ยินสามารถช่วยแก้ไขปัญหาความปลอดภัยระบบสารสนเทศของผู้ใช้ แพลตฟอร์มออนไลน์ไต่ยิน ทำให้ผู้ใช้แพลตฟอร์มออนไลน์ไต่ยินเกิดความมั่นใจว่าข้อมูลส่วนบุคคล ของตนเองจะได้รับการปกป้อง และกลยุทธ์ด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์ม ออนไลน์ไต่ยิน กลายเป็นเครื่องมือที่ช่วยเสริมสร้างความสามารถในการแข่งขัน การตัดสินใจ และเป็น เครื่องมือในการสร้างประสิทธิภาพในการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์ม ออนไลน์ไต่ยิน การที่แพลตฟอร์มออนไลน์ไต่ยินจะทำเช่นนี้ได้ ผู้บริหารต้องสนใจเรียนรู้ให้ตนเองมี ทักษะในการจัดการความปลอดภัยระบบสารสนเทศ โดยแบ่งระดับความต้องการข้อมูลความ ปลอดภัยสารสนเทศระดับใด เพราะความปลอดภัยระบบสารสนเทศที่เข้มงวดเกินไปหรือมี รายละเอียดมาก ระบบความปลอดภัยสารสนเทศก็จะมีมากเกินไปจนทำให้สิ้นเปลืองเงินลงทุน ในการจัดหาสารสนเทศเพื่อป้องกันความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยินที่ เกินความจำเป็น

3.2 รัฐบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ค.ศ. 2020 ของจีนได้กำหนดให้มีการ จัดทำ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็น ข้อกำหนดขั้นต่ำในการดำเนินการด้านเป้าหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับ

หน่วยงานที่ดำเนินกิจการสื่อสารออนไลน์ ในส่วนของแพลตฟอร์มออนไลน์ไต้หวันมีการกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศพื้นฐาน รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงของการจัดการความปลอดภัยระบบสารสนเทศ เพื่อให้การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบต่อแพลตฟอร์มออนไลน์ไต้หวัน หรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ในฐานะหน่วยงานของเอกชนที่ให้บริการข้อมูล องค์กรความรู้และงานวิจัยในการพัฒนาด้านความปลอดภัยระบบสารสนเทศ ผ่านสื่อสารออนไลน์แพลตฟอร์มไต้หวัน และโมบายแอปพลิเคชัน (Mobile Application) จึงต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถือปฏิบัติ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของแพลตฟอร์มออนไลน์ไต้หวันปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับ มาตรฐานสากล เพื่อสนับสนุนเป้าหมายการดำเนินงานการจัดการความปลอดภัยระบบสารสนเทศ

4. การกำหนดนโยบายกำกับดูแลความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน มีรูปแบบการดำเนินการดังนี้

4.1 การให้บริการและข้อมูลของแพลตฟอร์มออนไลน์ไต้หวันที่มีและปรากฏอยู่บนเครื่องคอมพิวเตอร์ โทรศัพท์มือถือเป็นสินทรัพย์ส่วนบุคคล และของธุรกิจแพลตฟอร์มออนไลน์ไต้หวันที่สำคัญ การสร้างความมั่นคงปลอดภัยระบบสารสนเทศในแพลตฟอร์มออนไลน์ไต้หวันอย่างจริงจัง ผู้ดูแลระบบสารสนเทศต้องคำนึงถึงความมั่นคงปลอดภัยเครือข่าย (Network Security) ด้วย โดยการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้ (Availability) หรือที่เรียกว่า CIA ของข้อมูล ระบบ ซอฟต์แวร์ และฮาร์ดแวร์ ที่มีการใช้งานบนแพลตฟอร์มออนไลน์ไต้หวันเพื่อสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียของแพลตฟอร์มออนไลน์ไต้หวัน โดยเฉพาะกับผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

4.2 การกำกับดูแลการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ ปัจจุบันแพลตฟอร์มออนไลน์ไต้หวัน ให้ความสำคัญกับความเสี่ยงทางด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ โดยมีนโยบายในการกำกับดูแลความปลอดภัยระบบสารสนเทศ ไม่ว่าจะเป็นปัญหาอุปสรรคที่เกิดจากการโจมตีทางระบบเทคโนโลยีสารสนเทศจากภายนอก หรือการรั่วไหลของข้อมูลส่วนบุคคล ความไม่ปลอดภัยระบบสารสนเทศดังกล่าวเป็นความเสี่ยงที่สามารถส่งผลกระทบต่อการดำเนินงานและความปลอดภัยทางข้อมูลส่วนบุคคลของผู้ที่มีส่วนเกี่ยวข้องทั้งภายในและภายนอกของแพลตฟอร์มออนไลน์ไต้หวัน ดังนั้น แพลตฟอร์มออนไลน์ไต้หวันจึงมุ่งพัฒนาระบบเพื่อสร้างเกราะกำบังทางระบบสารสนเทศผ่านโครงสร้างการกำกับดูแลที่มั่นคงที่ช่วยลดระยะเวลาในการตรวจจับการโจมตีให้ได้เร็วที่สุด การปฏิบัติตามรัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ.2020 โดยการจัดอบรมการรักษาความปลอดภัยระบบสารสนเทศ และการถูกโจมตีทางไซเบอร์เพื่อสร้างความมั่นใจ และความรู้ความเข้าใจในการแก้ไขปัญหาที่เกิดจากภัยคุกคามที่ส่งผลกระทบต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันทุกคน

5. การสร้างความเชื่อมั่นต่อระบบความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่
ยิน มีรูปแบบการดำเนินการดังนี้

เพื่อให้ระบบเทคโนโลยีสารสนเทศของแพลตฟอร์มออนไลน์ไต่ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศใน ลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ แพลตฟอร์มออนไลน์ไต่ ยิน จึงกำหนดนโยบายการรักษา ความมั่นคงปลอดภัยของระบบสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและป้องกันภัยคุกคามต่าง ๆ

โดยการสร้างความเชื่อมั่นต่อระบบความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ ยิน ดังต่อไปนี้

5.1 จัดทำนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และทำการสื่อสารเพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศและการสื่อสารบนแพลตฟอร์มออนไลน์ไต่ ยิน ทำให้การดำเนินงานด้านความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต่ ยิน ได้อย่างมีประสิทธิภาพและประสิทธิผล

5.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ และการสื่อสารบนแพลตฟอร์มออนไลน์ไต่ ยิน โดยอ้างอิงตามมาตรฐานการจัดการความปลอดภัย ISO/IEC 27001 ที่มีมาตรฐานเป็นที่ยอมรับในระดับโลก และมีการปรับปรุงการกำหนดขอบเขตการบริหารจัดการความปลอดภัยระบบสารสนเทศอย่างต่อเนื่อง

5.3 การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ ยิน เป็นนโยบายที่ต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับของแพลตฟอร์มออนไลน์ไต่ ยิน ได้รับทราบและเจ้าหน้าที่ทุกคน จะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

5.4 กำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบสารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับแพลตฟอร์มออนไลน์ไต่ ยิน ให้ตระหนักถึงความสำคัญของการรักษาความมั่นคง ปลอดภัยในการใช้งานระบบสารสนเทศและการสื่อสารของบนแพลตฟอร์มออนไลน์ไต่ ยิน ในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด

5.5 นโยบายการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ ยิน ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย 1 ครั้งต่อปี หรือตามที่ระบุไว้ในแผนการจัดการความปลอดภัยระบบสารสนเทศ เพื่อตรวจสอบประเมินนโยบายสร้างความเชื่อต่อการจัดการความปลอดภัยระบบสารสนเทศ

ดังนั้น การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ ยิน เป็นระบบการให้บริการข้อมูลที่มีอยู่บนเครื่องคอมพิวเตอร์และในเครือข่ายขนาดใหญ่ของแพลตฟอร์มออนไลน์ไต่ ยิน ที่ถือว่าเป็นทรัพย์สินส่วนบุคคลและขององค์กรที่ใช้แพลตฟอร์มออนไลน์ไต่ ยิน ที่สำคัญ ความสมบูรณ์ของสินทรัพย์ที่เป็นระบบสารสนเทศนี้อาจมีผลกระทบทางการสื่อสาร ทางธุรกิจ และทางการเงินหรือกระทบอื่น ๆ แพลตฟอร์มออนไลน์ไต่ ยิน ในฐานะผู้ดูแลระบบ ต้องคำนึงถึงความมั่นคงปลอดภัยระบบเครือข่ายสารสนเทศ โดยต้องสามารถรักษาความลับ

(Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) หรือเรียกว่า CIA ของระบบความปลอดภัยสารสนเทศ ประกอบด้วยความปลอดภัยของข้อมูล ความปลอดภัยของระบบ ความปลอดภัยของซอฟต์แวร์ และความปลอดภัยของฮาร์ดแวร์ ที่มีการใช้งานในการสื่อสารบนแพลตฟอร์มออนไลน์ไต่ยืน เพื่อสร้างความมั่นใจให้กับลูกค้าผู้ใช้บริการแพลตฟอร์มออนไลน์ไต่ยืน ในลักษณะของการบูรณาการรูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน ดังภาพต่อไปนี้



ภาพที่ 5.1 รูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน

การจัดการความปลอดภัยระบบสารสนเทศอย่างถูกต้องแล้วจะทำให้ธุรกิจของแพลตฟอร์มออนไลน์ไต่ยืนได้รับความเชื่อถือ และลูกค้าที่เป็นผู้ใช้แพลตฟอร์มออนไลน์มีความมั่นใจเป็นอย่างมาก มาตรฐานระบบการจัดการความปลอดภัยสารสนเทศเป็นประโยชน์สำหรับธุรกิจทุกประเภท และแพลตฟอร์มออนไลน์ไต่ยืนได้รับการออกแบบมาเพื่อส่งเสริมการสื่อสารออนไลน์ รวมถึงการส่งเสริมธุรกิจและองค์กรทุกประเภท ทุกขนาด การจัดการความปลอดภัยระบบสารสนเทศที่ได้มาตรฐาน ISO 27001 จึงเป็นแนวทางเชิงระบบที่แพลตฟอร์มออนไลน์ไต่ยืนนำมาใช้ในการจัดการความปลอดภัยระบบสารสนเทศ ประกอบด้วยกระบวนการ เทคโนโลยี และบุคคลที่ช่วยปกป้องและจัดการกับข้อมูลสารสนเทศขององค์กรและผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน ด้วยการจัดการความเสี่ยงที่มีประสิทธิภาพอย่างถูกต้องและครอบคลุม โดยมีหลักการที่สำคัญ 3 ประการ ได้แก่ การปกป้องข้อมูลให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น การปกป้องความถูกต้องครบถ้วนของข้อมูลสารสนเทศ และความพร้อมใช้งานของระบบสารสนเทศที่มีความปลอดภัยของข้อมูล

5.2 อภิปรายผล

การวิจัยเรื่อง การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ทั้งเชิงคุณภาพ และเชิงปริมาณ เมื่อพิจารณาผลการวิจัยแล้ว สามารถนำผลการศึกษายืนยันมาอภิปรายผลการวิจัย ตามวัตถุประสงค์ดังนี้

5.2.1 กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน จำนวน 5 กลยุทธ์ ดังนี้

1. กลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

การจัดการความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน พบว่า ถูกกำหนดให้เป็นกลยุทธ์ด้านความปลอดภัยในยุคดิจิทัล เป็นไปตามกฎหมายความปลอดภัยทางไซเบอร์ของรัฐบาล และนโยบายด้านความปลอดภัยระบบสารสนเทศที่ต้องปฏิบัติตามอย่างเคร่งครัด และพบว่า แพลตฟอร์มออนไลน์ไต้หวันมีการจัดตั้งแผนกวิศวกรรมการใช้แพลตฟอร์มออนไลน์ไต้หวัน เพื่อรับผิดชอบงานด้านความปลอดภัยระบบสารสนเทศขึ้นมีหน้าที่การรักษาความปลอดภัยของข้อมูลให้อยู่ในมาตรฐานที่เหมาะสม มีการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต และมีมาตรการในการแก้ไขหรือเปลี่ยนแปลงข้อมูล โดยต้องกระทำจากผู้มีสิทธิ์ในการเข้าถึงเท่านั้น และพบว่า พนักงานทั่วไปของแพลตฟอร์มออนไลน์ไต้หวันไม่สามารถดูข้อมูลลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันได้เนื่องจากไม่ได้ทำกิจกรรมใด ๆ ที่เกี่ยวข้องกับลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน นอกจากพนักงานที่อยู่ฝ่ายด้านความปลอดภัยระบบสารสนเทศเท่านั้นเพื่อป้องกันผู้ไม่เกี่ยวข้องนำข้อมูลสารสนเทศไปใช้ในทางที่ผิด โดยการรักษาความปลอดภัยของข้อมูลของแพลตฟอร์มออนไลน์ไต้หวันมีระบบจัดการอย่างรัดกุมและมีการทบทวนการปฏิบัติให้เป็นไปตามข้อกำหนดอยู่เสมอในการรักษาความปลอดภัยข้อมูล แอปพลิเคชัน และผู้ใช้สอดคล้องกับแนวคิดของ Stallings & Brown, (2020) ที่อธิบายถึงแนวทางปฏิบัติและการประยุกต์ใช้ความปลอดภัยของข้อมูลว่าการปฏิบัติและการประยุกต์ใช้ความปลอดภัยของข้อมูลถือเป็นสิ่งสำคัญในสังคมยุคใหม่ โดยเฉพาะอย่างยิ่งในระดับองค์กรและส่วนบุคคล องค์กรปกป้องข้อมูลที่ละเอียดอ่อนโดยการใช้มาตรการรักษาความปลอดภัยของข้อมูลและการควบคุมการเข้าถึง ในขณะที่บุคคลจำเป็นต้องใช้มาตรการป้องกันที่เหมาะสมเพื่อรักษาข้อมูลของตนเองให้ปลอดภัย ยังสอดคล้องกับแนวคิดของ Kim & Solomon, (2019) ความปลอดภัยของข้อมูลองค์กรและการควบคุมการเข้าถึงเป็นหัวใจสำคัญของการรักษาความปลอดภัยของข้อมูลองค์กรคือ การปกป้องข้อมูลทางธุรกิจที่ละเอียดอ่อน ข้อมูลลูกค้า และทรัพย์สินทางปัญญาจากการเข้าถึงโดยไม่ได้รับอนุญาตและการโจมตีที่อาจเกิดขึ้นด้วยเหตุนี้ องค์กรต่าง ๆ มักจะใช้กลยุทธ์การปกป้องข้อมูลแบบหลายชั้น เช่น การเข้ารหัส การสำรองข้อมูล และการแบ่งส่วนข้อมูล ทั้งยังสอดคล้องกับผลการวิจัยของ Kim & Kim (2021) ศึกษาเรื่อง ผลกระทบของปัจจัยด้านเทคนิค องค์กรและสิ่งแวดล้อมต่อความตั้งใจการจัดการความปลอดภัยข้อมูลขององค์กร ผลการศึกษาพบว่า การตรวจสอบการเพิ่มประสิทธิภาพและความความปลอดภัยของข้อมูล เป็นบทบาทสำคัญของผู้บริหารในการปรับปรุงการจัดการความปลอดภัยของข้อมูล และเป็นปัจจัยที่สำคัญที่สุดที่ส่งผลต่อการจัดการความปลอดภัยของข้อมูลขององค์กร

2. กลยุทธ์การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน พบว่า แพลตฟอร์มออนไลน์ไต้หวันให้ความสำคัญต่อการจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศทางไซเบอร์โดยถือว่าเป็นภาระกิจสำคัญสำหรับแพลตฟอร์มออนไลน์ไต้หวันในการปกป้องข้อมูลที่ละเอียดอ่อนของผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน โดยการตั้งหน่วยงานตรวจสอบภายในที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านความปลอดภัยระบบสารสนเทศเป็นประจำทุกปี และดำเนินการร่วมกับแผนกนวัตกรรมการใช้แพลตฟอร์มออนไลน์ไต้หวัน เพื่อตรวจสอบระบบความปลอดภัยของสารสนเทศที่มีความซับซ้อนและความถี่ของภัยคุกคามทางไซเบอร์ที่ปัจจุบันมีแนวโน้มเพิ่มสูงมากขึ้น และพบว่า ผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน ใช้กลยุทธ์เชิงรุกด้วยมาตรการความปลอดภัยระบบสารสนเทศโดยการกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศเพื่อที่จะสามารถระบุความไม่ปลอดภัย ประเมินความไม่ปลอดภัย และลดความเสี่ยงที่จะเกิดความไม่ปลอดภัยจากการใช้สารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างมีประสิทธิภาพ ด้วยการนำกรอบงานด้านความปลอดภัยทางไซเบอร์ที่เป็นมาตรฐานสากลที่ได้รับการยอมรับทั่วโลกมาใช้เพื่อรักษาความปลอดภัยสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างจริงจัง สอดคล้องกับแนวคิดของ Jing Jiwu, (2022) ความปลอดภัยของข้อมูลเครือข่าย ที่เรียกว่าความปลอดภัยของข้อมูลเครือข่ายคอมพิวเตอร์ ที่ครอบคลุมซึ่งมุ่งเน้นไม่เพียงแต่การปกป้องข้อมูลที่เก็บไว้ในฮาร์ดแวร์คอมพิวเตอร์แต่ยังครอบคลุมความปลอดภัยของข้อมูลในขั้นตอนการส่งเพื่อให้ถูกต้องและปลอดภัยยิ่งขึ้นเป้าหมายนี้ถูกสร้างขึ้นร่วมกันโดยองค์ประกอบหลักสองประการคือความปลอดภัยของโหนดเครือข่าย และระดับการป้องกันของการเชื่อมโยงการสื่อสารส่งผลให้เกิดสภาพแวดล้อมเครือข่ายที่ครอบคลุมการป้องกันความปลอดภัยสารสนเทศ และสอดคล้องกับแนวคิดของ LiHui, (2021) เป้าหมายสูงสุดของการรักษาความปลอดภัยข้อมูลไซเบอร์โดยทั่วไปคือการรับประกันความลับความสมบูรณ์และความพร้อมของข้อมูล และยังสอดคล้องกับผลการวิจัยของ Stewart & Jurjens, (2017) ที่ศึกษาเรื่องบทบาทสำคัญในการจัดการความปลอดภัยของข้อมูลในองค์กรที่ข้อมูลเป็นทรัพย์สินที่มีค่า ผลการศึกษาพบว่า ฝ่ายบริหารและพนักงานมีบทบาทสำคัญในการจัดการความปลอดภัยของข้อมูล และพบว่า การกำหนดเป้าหมายความปลอดภัยของข้อมูลส่งผลให้การจัดการความปลอดภัยที่ถูกคุกคามได้รับการแก้ไขอย่างมีประสิทธิภาพ การกำหนดเป้าหมายความปลอดภัยระบบสารสนเทศเป็นปัจจัยที่ส่งผลโดยตรงต่อการพัฒนาและการดำเนินการด้านการจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

3. กลยุทธ์การกำหนดนโยบายการกำกับดูแลความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

พบว่า แพลตฟอร์มออนไลน์ไต้หวัน ตระหนักถึงการใช้สื่อสังคมออนไลน์ซึ่งปัจจุบันประชาชนจีนนิยมใช้กันอย่างแพร่หลาย ซึ่งเกิดผลกระทบที่อาจเกิดขึ้นทั้งด้านที่เกิดเป็นประโยชน์และด้านที่เป็นเชิงลบหรือเป็นโทษต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน โดยเฉพาะหากมีการเผยแพร่ข้อมูลที่ไม่เหมาะสมออกสู่สาธารณะ ซึ่งอาจก่อให้เกิดความเสียหายต่อตนเอง ผู้อื่น และองค์กร และพบว่า ผู้บริหารแพลตฟอร์มออนไลน์ไต้หวัน มีการกำหนดนโยบายการกำกับดูแลความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ซึ่งจัดทำขึ้นเพื่อให้การใช้แพลตฟอร์มออนไลน์ไต้หวันของประชาชน มีความเหมาะสม เป็นประโยชน์ และหลีกเลี่ยงผลกระทบต่อสังคม และการดำเนินงานของแพลตฟอร์มออนไลน์ไต้หวันในอนาคต และพบว่า แพลตฟอร์มออนไลน์ไต้หวัน มีการ

กำหนดนโยบายและแนวปฏิบัติด้านความปลอดภัยระบบสารสนเทศอย่างเหมาะสมเพื่อให้การดำเนินงานเป็นไปตามตามวัตถุประสงค์ ปณิธาน พันธกิจด้านการให้บริการที่มีประสิทธิภาพและการใช้แพลตฟอร์มออนไลน์มีความปลอดภัยต่อการใช้ระบบสารสนเทศของแพลตฟอร์ม โดยคำนึงถึงสิทธิและเสรีภาพอย่างมีขอบเขตในการแสดงความคิดเห็นของประชาชนผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

และยังพบว่า แพลตฟอร์มออนไลน์ไต้หวัน มีการส่งเสริมให้ใช้สื่อสังคมออนไลน์ไต้หวันเพื่อการเรียนรู้ การแลกเปลี่ยนความรู้ การเสริมสร้างปฏิสัมพันธ์ทางสังคม วัฒนธรรม การท่องเที่ยว วิชาการ ฯลฯ และการเผยแพร่ข้อมูลหรือข้อคิดเห็นทางความคิดเชิงสร้างสรรค์ ที่ไม่ขัดต่อศีลธรรมอันดีของประชาชนจีน ธรรมเนียมปฏิบัติของสังคม และยังพบอีกว่า แพลตฟอร์มออนไลน์ไต้หวัน ไม่จำกัดสิทธิและเสรีภาพในการใช้สื่อแพลตฟอร์มออนไลน์ไต้หวัน แต่มีข้อกำหนดการใช้แพลตฟอร์มออนไลน์ไต้หวันที่ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันต้องตระหนักถึงสถานภาพความเป็นประชาชนจีนที่มีหน้าที่ในการรักษาวินัย จรรยาบรรณ รวมถึงการรักษาเกียรติและความน่าเชื่อถือทั้งของตนเอง ของสถาบันทางสังคม และประเทศของประชาชนจีน การให้สิทธิเสรีภาพภายใต้ข้อกำหนดในการใช้แพลตฟอร์มออนไลน์ไต้หวันนี้เป็นการสร้างความตระหนักจึงเป็นส่วนหนึ่งของกลยุทธ์การกำหนดนโยบายกำกับดูแลความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน สอดคล้องกับผลการศึกษาของชินทรีทิพย์ ปันสุวรรณ และสุนทิตพย์ จิตสว่าง ที่ศึกษาเรื่อง แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล ผลการศึกษาพบว่า การขับเคลื่อนการบังคับใช้นโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ องค์กรในประเทศไทย มีการนำ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ไปใช้เพื่อประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่ช่วยให้ธุรกิจและองค์กรเข้าใจ ควบคุม และลดความเสี่ยง ทางไซเบอร์ทุกรูปแบบ โดยแนวทางการบริหารจัดการความเสี่ยงและมาตรการควบคุมด้านการรักษาความปลอดภัยที่พึงมี (Maturity Level) เป็นการประเมินการบริหารจัดการและการควบคุมความเสี่ยงภัยทางไซเบอร์ว่าอยู่ในระดับที่สอดคล้อง กับความเสี่ยงที่มี โดยประเมินใน 6 ด้านหลัก ได้แก่ (1) กรอบกำกับดูแล (Governance) เพื่อให้มีการกำกับดูแลและสนับสนุนให้องค์กรมีการบริหารความเสี่ยงด้านไซเบอร์อย่างเพียงพอเหมาะสม (2) การระบุความเสี่ยง (Risk Identification) เพื่อให้องค์กรมีการบริหารจัดการทรัพยากรสินทางด้านเทคโนโลยีที่สามารถเชื่อมโยง นำไปใช้ ในการบริหารจัดการ และสามารถระบุความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

4. กลยุทธ์การพัฒนาศักยภาพบุคลากรด้านความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน

การพัฒนาเศรษฐกิจจีนในปัจจุบันอาศัยศักยภาพจากการสื่อสารที่สะดวกรวดเร็ว ในธุรกิจและกิจการต่าง ๆ เศรษฐกิจในภาพรวมของประเทศจีนที่เติบโตได้อย่างยั่งยืนและมีเสถียรภาพในระยะยาวนั้นพบว่า รัฐบาลจีนให้ความสำคัญกับสถานการณ์ด้านต่าง ๆ และสาระสำคัญในประเด็นการพัฒนาทักษะ (Skills Development) การเตรียมแรงงานให้มีทักษะที่จำเป็นสำหรับทุกอุตสาหกรรม เพื่อให้บุคลากรที่เกี่ยวข้องกับอุตสาหกรรมสื่อสารทั้งภาครัฐ ภาคเอกชน ให้มีความรู้ ความเข้าใจเกี่ยวกับสินค้าและบริการต่าง ๆ ในปัจจุบันที่ต้องอาศัยการสื่อสารผ่านแพลตฟอร์มออนไลน์ที่ต้องมีระบบการจัดการด้านความปลอดภัยระบบสารสนเทศที่ดีและมีประสิทธิภาพเพื่อให้กิจการทางธุรกิจต่างๆ ประสบความสำเร็จ และพบว่า แพลตฟอร์มออนไลน์ไต้หวันให้ความสำคัญกับการพัฒนาศักยภาพด้าน

ความปลอดภัยระบบสารสนเทศในทุกๆระดับ ในมิติของการพัฒนาบุคลากรด้านความปลอดภัยระบบสารสนเทศ ทำให้บุคลากรด้านระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน มีความรู้ความเข้าใจ และตระหนักถึงคุณค่าและความสำคัญของปัจจัยที่เกี่ยวข้องกับการพัฒนาบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศทั้งระบบ และพบว่า การประสบความสำเร็จของแพลตฟอร์มออนไลน์ไต้หวันมาจากการส่งเสริมและการพัฒนาบุคลากรด้านการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน และพบว่า แพลตฟอร์มออนไลน์ไต้หวันให้ความสำคัญกับการพัฒนาบุคลากรด้านการจัดการระบบสารสนเทศในทุกๆระดับ ซึ่งการพัฒนาบุคลากรด้านการจัดการระบบสารสนเทศเพื่อความปลอดภัย เป็นกลไกสำคัญที่ส่งผลให้แพลตฟอร์มออนไลน์ไต้หวันประสบความสำเร็จในการพัฒนาแพลตฟอร์มออนไลน์ไต้หวันที่สามารถตอบสนองต่อกิจกรรมการสื่อสาร ที่หลากหลายของประชาชนจีน และพบอีกว่า แพลตฟอร์มออนไลน์ไต้หวัน มีบุคลากรด้านการจัดการระบบสารสนเทศทั้งระบบที่มีศักยภาพ คุณภาพ และคุณธรรมจริยธรรมที่สูงเกิดผลดีและสามารถพัฒนาแพลตฟอร์มออนไลน์ไต้หวัน ให้เข้าไปสู่ความสามารถในการแข่งขันด้านการให้บริการการของแพลตฟอร์มออนไลน์ไต้หวัน เพื่อดึงดูดลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน ทั้งภายในประเทศ และต่างประเทศให้เลือกใช้บริการของแพลตฟอร์มออนไลน์ไต้หวัน สอดคล้องกับแนวคิดของ Kim & Solomon, (2019) วิธีการพัฒนาคนขององค์กรนี้ สามารถป้องกันปัญหาการบุกรุกบัญชีที่เกิดจากการรั่วไหลของรหัสผ่านได้อย่างมีประสิทธิภาพ สำหรับบัญชีที่เกี่ยวข้องกับข้อมูลที่ละเอียดอ่อน เช่น ธนาคาร และโซเชียลมีเดีย การเปิดใช้งาน MFA เป็นหนึ่งในแนวทางปฏิบัติที่ดีที่สุดในการรับรองความปลอดภัยของข้อมูล การพัฒนาบุคลากรด้านที่ จึงจะสามารถทำให้การดูแลปกป้องข้อมูลส่วนตัวของผู้ใช้บริการได้ โดยเฉพาะอย่างยิ่งเมื่อใช้โซเชียลมีเดียและบริการออนไลน์ บริการออนไลน์จำนวนมากรวบรวมข้อมูลส่วนบุคคลของผู้ใช้ ดังนั้น บุคลากรจึงต้องเข้าใจนโยบายความเป็นส่วนตัวส่วนตัวของข้อมูลของแพลตฟอร์มเหล่านี้ เพื่อลดการเปิดเผยข้อมูลที่ละเอียดอ่อนให้เหลือน้อยที่สุด นอกจากนี้ เมื่อเข้าถึงข้อมูลที่ละเอียดอ่อนบนเครือข่าย Wi-Fi สาธารณะ การใช้เครือข่ายส่วนตัวเสมือน (VPN) สามารถเข้ารหัสการส่งข้อมูลและป้องกันไม่ให้ผู้โจมตีดักจับและขโมยได้ สอดคล้องกับผลการศึกษาของ ภูมิวุฒิ วิทวัสสารัญกุล, (2563) ศึกษาเรื่อง แนวทางการพัฒนาระบบการรักษาความปลอดภัยข้อมูลสารสนเทศโดยใช้กรอบแนวคิดระบบจัดการความปลอดภัยข้อมูลสารสนเทศ พบว่า การใช้กรอบแนวคิดการจัดการความปลอดภัยข้อมูลสารสนเทศเพื่อพัฒนาแนวทางความปลอดภัยในศูนย์ปฏิบัติการเครือข่ายสามารถกำหนดขั้นตอนปฏิบัติสำหรับองค์กรและระบบที่มีคุณสมบัติและการทำงานที่คล้ายคลึงกันได้อย่างมีประสิทธิภาพได้ ระดับหนึ่งเท่านั้นหากพิจารณาถึงรายละเอียดการรักษาความปลอดภัยสารสนเทศนั้นปัจจัยสำคัญของระบบความปลอดภัยสารสนเทศต้องตั้งบุคคลเข้ามารับผิดชอบซึ่งบุคคลนั้นต้องได้รับการพัฒนาจึงจะสามารถแก้ไขปัญหาและจัดการระบบความปลอดภัยสารสนเทศได้อย่างมีประสิทธิภาพ

5. กลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวัน

แพลตฟอร์มออนไลน์ไต้หวันมีการสื่อสารข้อกำหนด และนโยบายด้านความปลอดภัยระบบสารสนเทศ ในการใช้แพลตฟอร์มออนไลน์ไต้หวันเพื่ออธิบายถึงความปลอดภัยระบบสารสนเทศในสิ่งที่แพลตฟอร์มออนไลน์ไต้หวันปฏิบัติอยู่อย่างสม่ำเสมอ พบว่า กลยุทธ์การสร้างเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันส่งผลทำให้ลูกค้าที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันเข้าใจและเกิดความเชื่อมั่นต่อ

ความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ความเชื่อมั่นและความมั่นใจของลูกค้าแพลตฟอร์มออนไลน์ไต้หวันเกิดจากเชื่อใจในแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน และพบว่าแพลตฟอร์มออนไลน์ไต้หวันมีกลยุทธ์สร้างความเชื่อมั่นให้กับผู้ใช้แพลตฟอร์มโดยการนำเสนอข้อมูลข่าวสาร ด้วยข้อมูลที่เป็นจริงมีการตรวจสอบข้อมูลด้วยคนและระบบเทคโนโลยี AI ส่งผลทำให้ผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันเกิดความเชื่อมั่นต่อระบบการจัดการความปลอดภัยระบบสารสนเทศ ของแพลตฟอร์มออนไลน์ไต้หวัน และพบว่า แพลตฟอร์มออนไลน์ไต้หวันใช้ข้อมูลข่าวสารที่เป็นจริงและมีความปลอดภัยสูงส่งผลให้การสื่อสารของแพลตฟอร์มออนไลน์ไต้หวันช่วยสร้างเสริมสร้างภาพลักษณ์ (Brand Image) ที่ดีให้กับแพลตฟอร์มออนไลน์ไต้หวัน ดังนั้นการสร้างการเชื่อใจให้กับแบรนด์แพลตฟอร์มออนไลน์ไต้หวัน (Brand Trust) ต้องสื่อสารอย่างตรงไปตรงมา และพร้อมให้ทุกๆ คนตรวจสอบได้อยู่เสมอ ซึ่งเป็นวิธีการบริหารจัดการที่เหมาะสมกับยุคเทคโนโลยีดิจิทัลที่ทำให้เกิดความรู้สึกรังสรรค์ทั้งภายในองค์กรและภายนอกองค์กร และยังอีกพบว่า แพลตฟอร์มออนไลน์ไต้หวัน เป็นแบรนด์ที่สามารถสร้างความเชื่อมั่นและความไว้วางใจให้กับลูกค้าผู้ใช้แพลตฟอร์ม ด้วยการยืนยันด้วยข้อมูล ความถูกต้องของข้อมูล และความรับผิดชอบหากเกิดความไม่ปลอดภัยของระบบสารสนเทศที่ต้องรับผิดชอบและชดเชยต่อผู้เสียหายอย่างยุติธรรม ซึ่งการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันที่แสดงจุดยืนที่ชัดเจนในเรื่องของความรับผิดชอบที่เป็นธรรมในการทำธุรกิจของแพลตฟอร์มออนไลน์ไต้หวันได้กลายเป็นกลยุทธ์การสร้างการเชื่อมั่นต่อผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันแพลตฟอร์มออนไลน์ไต้หวันที่สามารถสร้างความเชื่อใจให้เกิดความรู้สึกดีทั้งกับตัวแบรนด์แพลตฟอร์มออนไลน์ไต้หวันรวมถึงสินค้าและบริการ จนกลุ่มคนผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันเหล่านั้นกลายเป็น Social Proof ที่ทรงพลัง ที่นำไปบอกต่อทั้งแบบปากต่อปาก (Word-of-Mouth) หรืออาจนำไปบอกต่อผ่านสื่อโซเชียลมีเดีย นอกจากนั้น Social Proof เกิดจากสิ่งที่แพลตฟอร์มออนไลน์ไต้หวันได้ดำเนินธุรกิจแพลตฟอร์มออนไลน์ไต้หวันมาอย่างยาวนานและได้รับการันตีรางวัลแพลตฟอร์มออนไลน์ไต้หวันดีเด่นระดับโลก มีจำนวนลูกค้าที่ใช้แพลตฟอร์มออนไลน์ไต้หวันทั่วโลก รางวัลด้านคุณภาพดีเด่น และรางวัลด้านการบริการที่ดี เป็นต้น สอดคล้องกับแนวคิดของ Ho Daiju, (2021) ในขณะที่ความปลอดภัยของเนื้อหาข้อมูลมุ่งเน้นไปที่ความเสียหายการรั่วไหลและการสูญเสียข้อมูลที่ได้รับในระหว่างการจัดเก็บ การประมวลผลและการส่งผ่านซึ่งเกี่ยวข้องโดยตรงกับการรักษาความลับความสมบูรณ์และความพร้อมใช้งานของข้อมูล และสอดคล้องกับแนวคิดของ LiHui, (2021) เป้าหมายสูงสุดของการรักษาความปลอดภัยข้อมูลไซเบอร์โดยทั่วไปคือการรับประกันความลับความสมบูรณ์และความพร้อมของข้อมูล ปัจจัยอื่น ๆ เช่น ความน่าเชื่อถือ ความถูกต้อง การไม่สามารถปฏิเสธได้ และการตรวจสอบได้ การรักษาความลับช่วยให้มั่นใจได้ว่าข้อมูลจะไม่ถูกเข้าถึงโดยผู้ใช้หรือบุคคลที่ไม่ได้รับอนุญาตและการรับประกันความสมบูรณ์ของข้อมูลจะไม่ถูกแก้ไขหรือถูกทำลายโดยไม่ได้รับอนุญาตในระหว่างการส่งหรือจัดเก็บ ขณะที่ความพร้อมในการใช้งานช่วยให้ผู้ใช้บริการมั่นใจได้ว่าข้อมูลจะถูกเข้าถึงและใช้โดยผู้ใช้หรือระบบที่ได้รับอนุญาตอย่างถูกต้องตามกฎหมาย

5.2.2 การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน

ผู้บริหารแพลตฟอร์มออนไลน์ไต่ยืนและบุคลากรผู้รับผิดชอบระบบสารสนเทศจำเป็นต้องให้ความสำคัญกับการจัดการความปลอดภัยระบบสารสนเทศ เพื่อปกป้องความมั่นคงปลอดภัยของข้อมูลและสารสนเทศ ป้องกันภัยคุกคามและความเสียหายที่อาจเกิดขึ้น การจัดการความปลอดภัยระบบสารสนเทศยังสามารถช่วยลดความเสี่ยงจากการละเมิดด้านข้อมูล

การดูแลป้องกันระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนไว้ก่อนย่อมเป็นการกระทำที่ดีกว่าการแก้ไขเมื่อเกิดความไม่ปลอดภัยของระบบสารสนเทศ ซึ่งจะส่งผลกระทบต่ออย่างรุนแรงในภายหลัง นอกจากนี้เมื่อมีการจัดการความปลอดภัยระบบสารสนเทศอย่างถูกต้องแล้วจะทำให้ธุรกิจของแพลตฟอร์มออนไลน์ไต่ยืนได้รับความไว้วางใจเชื่อถือ และลูกค้าที่เป็นผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืนจะเกิดความมั่นใจเป็นอย่างมากต่อการจัดการความปลอดภัยระบบสารสนเทศ มาตรฐานระบบการจัดการความปลอดภัยสารสนเทศจะเป็นประโยชน์สำหรับองค์กรทุกประเภท แพลตฟอร์มออนไลน์ไต่ยืนได้รับการออกแบบมาเพื่อส่งเสริมการสื่อสารออนไลน์ รวมถึงการส่งเสริมธุรกิจและองค์กรทุกประเภท ทุกขนาด การจัดการความปลอดภัยระบบสารสนเทศที่ได้มาตรฐาน ISO 27001 ของแพลตฟอร์มออนไลน์ไต่ยืนนำมาใช้ในการจัดการความปลอดภัยระบบสารสนเทศ ประกอบด้วย กระบวนการ เทคโนโลยี และบุคคลที่ช่วยปกป้องและจัดการกับข้อมูลสารสนเทศขององค์กรและผู้ใช้แพลตฟอร์มออนไลน์ไต่ยืน ด้วยการจัดการความเสี่ยงที่มีประสิทธิภาพอย่างถูกต้องและครอบคลุม โดยมีหลักการที่สำคัญ 3 ประการ ได้แก่ การปกป้องข้อมูลให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น การปกป้องความถูกต้องครบถ้วนของสารสนเทศ และความพร้อมใช้งานของระบบสารสนเทศที่มีความปลอดภัยของสารสนเทศ สอดคล้องกับแนวคิดประเภทของรูปแบบ Semantic Model ของ Joyce and Weil, (1985 : 41) ที่กล่าวอธิบายว่าเป็นรูปแบบที่ใช้วัจนภาษาและอวัจนภาษาเป็นสื่อในการบรรยายหรืออธิบายปรากฏการณ์ที่ศึกษาด้วยภาษา แผนภูมิ หรือรูปภาพ เพื่อให้เห็นโครงสร้างทางความคิด องค์ประกอบ และความสัมพันธ์ขององค์ประกอบของปรากฏการณ์นั้น ๆ ในภาพรวมที่สามารถเข้าใจได้ง่าย และสอดคล้องกับแนวคิดการตรวจสอบรูปแบบของ อุทุมพร จามรมาน, (2541 : 23) ที่กล่าวว่าจุดมุ่งหมายที่สำคัญของการสร้างรูปแบบก็เพื่อทดสอบหรือตรวจสอบรูปแบบนั้นด้วยข้อมูลเชิงประจักษ์ การตรวจสอบรูปแบบมีหลายวิธี ซึ่งอาจใช้การวิเคราะห์จากหลักฐานเชิงคุณลักษณะ (Qualitative) และเชิงปริมาณ (Quantitative) โดยที่การตรวจสอบรูปแบบจากหลักฐานเชิงคุณลักษณะอาจใช้ผู้เชี่ยวชาญเป็นผู้ตรวจสอบในโมเดลจากหลักฐานเชิงปริมาณใช้เทคนิคทางสถิติ

5.3 ข้อเสนอแนะ

การศึกษาเรื่อง การพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืน จากผลการวิเคราะห์อย่างละเอียด การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต่ยืนนั้น เป็นกระบวนการที่ซับซ้อนและต้องอาศัยแนวทางเชิงกลยุทธ์ที่รอบด้าน เพื่อให้โมเดลมีความยืดหยุ่นและตอบสนองต่อภูมิทัศน์ที่เปลี่ยนแปลงอยู่เสมอ จึงมีข้อเสนอแนะเพิ่มเติมดังนี้

1. การลงทุนในเทคโนโลยีการจัดการความปลอดภัยระบบสารสนเทศอัตโนมัติ เพื่อลดจุดอ่อนด้านกระบวนการทำงานแบบแมนนวลที่ทำให้เกิดความล่าช้าในการตรวจจับและตอบสนองต่อภัยคุกคาม ผู้บริหารแพลตฟอร์มออนไลน์ควรพิจารณาการลงทุนในระบบอัตโนมัติ (automation) และเทคโนโลยีการเรียนรู้ของเครื่องจักร (Machine Learning) เพื่อช่วยยกระดับประสิทธิภาพการป้องกันภัยคุกคามเชิงรุกให้มีความรวดเร็วยิ่งขึ้น

2. การเพิ่มงบประมาณสำหรับการพัฒนาบุคลากร แม้ว่าแพลตฟอร์มออนไลน์โตขึ้นจะให้ความสำคัญกับการพัฒนาบุคลากรอยู่แล้ว แต่จากผลการศึกษาที่ชี้ว่ายังขาดแคลนบุคลากรที่มีทักษะเฉพาะทาง ควรมีการจัดสรรงบประมาณเพิ่มเติมเพื่อการศึกษา, การฝึกอบรม, และการพัฒนาทักษะอย่างต่อเนื่องและลึกซึ้งยิ่งขึ้น เพื่อให้บุคลากรสามารถเป็นแกนหลักในการขับเคลื่อนระบบความปลอดภัยได้อย่างแท้จริง

3. การเสริมสร้างการสื่อสารแบบสองทาง เพื่อตอบสนองความคาดหวังของผู้ใช้ที่ต้องการการป้องกันความปลอดภัยของข้อมูลส่วนบุคคลที่สูงขึ้น ควรมีการสร้างช่องทางการสื่อสารแบบสองทางที่เปิดกว้างและโปร่งใส เพื่อให้ผู้ใช้สามารถแสดงความกังวลและให้ข้อเสนอแนะได้อย่างง่าย ซึ่งนอกจากจะเป็นการสร้างเชื่อมั่นแล้ว ยังเป็นแหล่งข้อมูลที่มีค่าสำหรับการปรับปรุงระบบในอนาคต

กล่าวโดยสรุป รูปแบบการจัดการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์โตขึ้นเป็นตัวอย่างที่น่าสนใจของการผสมผสานระหว่างหลักการความปลอดภัยสากล กลยุทธ์เชิงรุก และการปรับตัวให้เข้ากับบริบททางสังคมและวัฒนธรรม การนำโมเดลนี้ไปใช้ไม่ได้เป็นเพียงภาระหน้าที่ แต่เป็นโอกาสในการสร้างคุณค่าที่ยั่งยืนให้กับองค์กรและผู้ใช้ในระยะยาว โดยโมเดลนี้เป็นแนวทางที่ครอบคลุมและยืดหยุ่นสำหรับแพลตฟอร์มดิจิทัลทุกประเภทในการรับมือกับความท้าทายด้านความปลอดภัยในปัจจุบันและอนาคต

5.3.1 ข้อเสนอแนะในการนำไปใช้ประโยชน์

การนำโมเดลการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์โตขึ้นไปใช้อย่างเต็มรูปแบบจะนำมาซึ่งประโยชน์และผลลัพธ์ที่สำคัญหลายประการ ดังนี้

1. การปกป้องข้อมูลอย่างมีประสิทธิภาพ โมเดลนี้ช่วยให้แพลตฟอร์มออนไลน์โตขึ้นสามารถปกป้องข้อมูลที่ละเอียดอ่อนของลูกค้าและองค์กรได้อย่างเป็นระบบและครอบคลุม โดยลดความเสี่ยงจากการรั่วไหล การสูญหาย หรือความเสียหายของข้อมูล ทั้งในระหว่างการจัดเก็บ การประมวลผล และการส่งผ่านข้อมูล

2. ความต่อเนื่องในการดำเนินธุรกิจของแพลตฟอร์มออนไลน์โตขึ้น การใช้แนวทางเชิงรุกในการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ช่วยให้องค์กรสามารถระบุ ประเมิน และลดความเสี่ยงที่อาจเกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ ซึ่งส่งผลให้การดำเนินงานของแพลตฟอร์มออนไลน์โตขึ้นมีความต่อเนื่องและยืดหยุ่นต่อภัยคุกคามที่อาจเกิดขึ้นได้ตลอดเวลา

3. การปฏิบัติตามข้อกำหนดและกฎหมาย การนำมาตรฐานสากลอย่าง ISO 27001 มาใช้ และการปฏิบัติตามกฎหมายท้องถิ่นของรัฐบาลจีนอย่างเคร่งครัด จะช่วยให้การบริหารแพลตฟอร์มออนไลน์โตขึ้นสามารถปฏิบัติตามข้อกำหนดด้านการปกป้องข้อมูลได้อย่างสอดคล้องและหลีกเลี่ยงข้อผิดพลาดทางกฎหมายที่อาจเกิดขึ้นได้

4. การสร้างความได้เปรียบในการแข่งขัน การแสดงให้เห็นถึงความมุ่งมั่นในการรักษาความปลอดภัยของข้อมูลอย่างจริงจังของแพลตฟอร์มออนไลน์ไต้หวัน และการได้รับการรับรองมาตรฐานสากลช่วยสร้างความน่าเชื่อถือและความเชื่อมั่นให้กับลูกค้า ซึ่งเป็นปัจจัยสำคัญที่ทำให้แพลตฟอร์มออนไลน์ไต้หวันโดดเด่นและได้เปรียบในตลาดที่มีการแข่งขันสูง

5. การปรับปรุงระบบอย่างต่อเนื่อง โมเดลการจัดการความปลอดภัยนี้ถูกออกแบบมาในลักษณะที่ส่งเสริมให้มีการประเมินและปรับปรุงระบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันอย่างต่อเนื่อง โดยเฉพาะในส่วนของการแก้ไขจุดอ่อนด้านกระบวนการแมนนวลและการขาดแคลนบุคลากร เพื่อให้ระบบสามารถรับมือกับความซับซ้อนและความถี่ของภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นได้อย่างมีประสิทธิภาพ

5.3.2 ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

1. งานวิจัยนี้เป็นงานวิจัยผสมผสานระหว่างเชิงปริมาณและเชิงคุณภาพ โดยมุ่งศึกษากลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวัน ซึ่งในงานวิจัยนี้เป็นการศึกษากลุ่มตัวอย่างเจาะจงเฉพาะประเด็นการรักษาความปลอดภัยระบบสารสนเทศ ดังนั้นผู้สนใจควรที่จะศึกษาปัจจัยที่ส่งผลกระทบต่อการพัฒนาศักยภาพของการรักษาความปลอดภัยระบบสารสนเทศ เป็นต้น เพื่อจะได้มองเห็นภาพรวมทั้งหมดของการพัฒนาระบบความปลอดภัยสารสนเทศได้ชัดเจนยิ่งขึ้น

2. งานวิจัยครั้งนี้ใช้การเก็บข้อมูลจากกลุ่มตัวอย่าง จากผู้ให้ข้อมูลสำคัญเฉพาะใน 4 มณฑลเท่านั้น ดังนั้น ในการวิจัยครั้งต่อไป ผู้สนใจควรที่จะใช้การวิจัยโดยเก็บข้อมูลกลุ่มตัวอย่างและผู้ให้ข้อมูลสำคัญในภูมิภาคอื่นๆ ทั่วประเทศจีน หรือในประเทศอื่นๆ ที่มีการใช้แพลตฟอร์มออนไลน์ไต้หวัน เพื่อที่จะได้เห็นลักษณะของแนวทางการพัฒนารูปแบบการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้หวันในประเทศอื่น ๆ

3. ควรทำการศึกษา เพิ่มเติมเกี่ยวกับตัวแปรอื่นๆ ในการวิจัย เช่น ประสิทธิภาพของการจัดการความปลอดภัยระบบสารสนเทศ ผ่านแผนงาน กิจกรรม โครงการ เพื่อตอบสนองความต้องการของลูกค้าผู้ใช้แพลตฟอร์มออนไลน์ไต้หวันที่อาจส่งผลกระทบต่อวิจัยที่ชัดเจนขึ้น เพื่อให้ได้ข้อมูลที่ชัดเจนขึ้น และสามารถนำมาพัฒนาปรับปรุง แก้ไข ให้มีประสิทธิภาพมากยิ่งขึ้น

4. ควรทำการศึกษา เพิ่มเติมเกี่ยวกับปัจจัยที่มีบทบาทและมีผลกระทบต่อความสำเร็จของการจัดการความปลอดภัยระบบสารสนเทศ เช่น ความสำคัญของบุคลากรด้านการจัดการความปลอดภัยระบบสารสนเทศ การพัฒนาความรู้เพื่อสร้างความเข้าใจที่หลากหลายด้านการจัดการความปลอดภัยระบบสารสนเทศ การสร้างการมีส่วนร่วมระหว่างหน่วยงานภาครัฐ ภาคเอกชนเพื่อกำกับดูแลความปลอดภัยข้อมูลส่วนบุคคล และระบบสารสนเทศขององค์กร และการสนับสนุนด้านต่าง ๆ เพื่อพัฒนาระบบความปลอดภัยของสารสนเทศ เป็นต้น



บรรณานุกรม

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

บรรณานุกรม

- Allwood, J., & Schroeder, R. (2000). Intercultural communication in a virtual environment. *Intercultural Communication*, 4, 1-15.
- Bagdasaryn, N. G. (2011). Intercultural communication in the context of new media. Retrieved November, 20, 2011.
- Bai, C. (2020). The practical logic of management innovation. *Nankai Business Review*, 23(5), 1.
- Belay, G. (2018). The (re) construction and negotiation of cultural identities in the age of globalization. In *Interaction and identity* (pp. 319-346). Routledge.
- Berlo, D. (1961). *The process of communication*. New York: Holt, Rinehart and Winston, Inc.
- Bower, J. L., & Christensen, C. M. (1995). *Disruptive technologies: catching the wave*.
- Cai, W. (2015). Research on the integrated development of traditional broadcasting and new media in the new media era. *New Media Research*, 1(11), 56-57.
- Castells, M. (2000). Materials for an exploratory theory of the network society¹. *The British journal of sociology*, 51(1), 5-24.
- Chang, C. (2021). Analysis of computer network information security and its protection strategies. *China Informatization*, (8), 83-84.
- Chang, Y. (2021). Computer network information security risks and solutions under the background of big data. *Information Recording Materials*, 22(4), 198-199.
- Chen, G. (2008a). Creative communication management (CCM): The new communication environment and the marketing communication revolution. *Grand View of Advertising (Comprehensive Edition)*, (5), 23-28.
- Chen, G. (2008b). Post-advertising era: The creative communication management revolution. *Grand View of Advertising: Comprehensive Edition*, (7), 22-25.
- Chen, G. (2009). Emotional marketing and entertainment marketing: Netizens' psychology and creative communication management (CCM). *China Advertising*, (4), 158-158.
- Chen, G. (2013). Trends and changes in creative communication management (CCM). *Grand View of Advertising: Comprehensive Edition*, (8), 24-25.
- Chen, G. M. (2005). A model of global communication competence.
- Chen, G. M. (2012). The impact of new media on intercultural communication in global context.
- Chen, G. M., & Starosta, W. J. (1998). *Foundations of intercultural communication*. (No Title).

- Chen, L. (2021). The construction of short videos in domestic news media and the challenges they face: Taking the video development strategy of The Paper as an example. *China Newspaper Industry*, (5), 18-21.
- Chen, Q., & Peng, Y. (2022). Research on the influencing factors of information dissemination effects of government TikTok accounts in major public health emergencies: An empirical analysis based on 25 provincial health commission official TikTok accounts. *Journal of Guangxi Normal University (Philosophy and Social Sciences Edition)*, 58(4), 72-85.
- Chen, X., Yang, W., Han, W., & Sun, X. (2021). Research on network information security issues based on the "Internet+" era. *Computer Knowledge and Technology*.
- Chen, Y., Qiu, J., Zou, J., & Ni, C. (2008). Thoughts on the regulations of information dissemination management in online communities in China. *Shandong Social Sciences*, (5), 32-37.
- Cheng, Y. (2015). Research on corporate network communication marketing based on creative communication management theory: Taking Jumei as an example. *Communication and Copyright*, (8), 82-83.
- Cheng, Z. (2020). Construction of a full-process corporate management innovation system. *Science and Technology Innovation Herald*.
- Chu, A. M., & So, M. K. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability*, 12(8), 3163.
- COTEC, F. (1999). A guide to technology management an innovation for Companies–Temaguide. URL: <http://www.cotec.es/ca/publicaciones>.
- Crosbie, V. (2002). What is new media. Retrieved November 5, 2011.
- Dai, S. (2012). Development strategies of television media in the new media era. *Press Circles*, (4), 9-11.
- Day, G. S., & Shea, G. (2020). Changing the work of innovation: A systems approach. *California Management Review*, 63(1), 41-60.
- Deacon, D., Pickering, M., Golding, P., & Murdock, G. (2021). *Researching communications: A practical guide to methods in media and cultural analysis*. Bloomsbury Publishing USA.
- Dong, Y., & Wang, A. (2021). Protection measures for computer network information security in the big data environment. *Information Recording Materials*, 22(6), 22-23.

- Du, B., Zhong, H., & Ge, Y. (2020). Analysis of the effective application of firewall technology in computer network information security. *China New Telecommunications*, (1), 154-155.
- Duan, P. (2022). Information flow in China's international communication: History, problems, and countermeasures. *Journal of Xi'an Jiaotong University (Social Sciences)*, 42(4).
- Fan, H. (2015). The development path of traditional media in the new media era. *Radio & Television Journal*, (1), 8-9.
- Fang, Y. (2020). The three major significances of the introduction of new regulations on network ecology governance. *Network Communication*.
- Feng, R., & Jin, J. (2007). On the ubiquitous communication characteristics of the new media era. *Press Circles*, (4), 27-28.
- Fischer, M. M. (2001). Innovation, knowledge creation and systems of innovation. *The annals of regional science*, 35, 199-216.
- Flew, T. (2005). *New media*. New York: Oxford University Press.
- Gao, B., & Zhang, Z. (2007). Analysis of consumer behavior in brand communication management. *Journal of Mudanjiang Normal University (Philosophy and Social Sciences Edition)*, (3), 142-143.
- Gao, J. (2022). Analysis of the impact of the new media environment on the development of digital media technology. *Cultural Industry*.
- Gong, J. (2022). Construction of network information security protection system based on computer network technology. *Journal of Hunan Institute of Engineering (Natural Science Edition)*.
- Govindarajan, V., & Gupta, A. K (1997). The changing global landscape. Retrieved August 10, 2007, from <http://www.bmgt.umd.edu/cib/wplist.htm/>
- Gray, L. M., Wong-Wylie, G., Rempel, G. R., & Cook, K. (2020). Expanding qualitative research interviewing strategies: Zoom video communications. *The qualitative report*, 25(5), 1292-1301.
- Guo, K. (2020). Analysis of the scientific communication mechanism of short video platforms from the perspective of value co-creation: Taking the TikTok short video platform as an example. *Southeast Communication*, (2), 31-33.
- Hampton, K. N., & Wellman, B. (1999). Netville online and offline: Observing and surveying a wired suburb. *American behavioral scientist*, 43(3), 475-492.
- He, D. (2021). Analysis of computer network information security issues under the background of big data. *South China Agriculture*, (23), 126-128.

- He, W., & Xin, J. (2019). Problems in network information security and research on data encryption technology. *Cyberspace Security*, (1).
- Herman, E. S., & McChesney, R. W. (1997). *The global media: The new missionaries of corporate capitalism*. Bloomsbury Academic.
- Huang, B. (2021). The reasons for Douyin's success from the perspective of business model, algorithm and functions. In *6th International Conference on Financial Innovation and Economic Development (ICFIED 2021)* (pp. 320-325). Atlantis Press.
- Huang, W., Qin, L., Liu, X., Xu, N., & Li, Y. (2020). Research progress on network information security governance: Based on the current situation of rule of law at home and abroad. *Journal of Intelligence*, 39(4), 132-139.
- Huang, Y., & Ye, W. (2024). 'Traffic rewards', 'algorithmic visibility', and 'advertiser satisfaction': How Chinese short-video platforms cultivate creators in stages. *Convergence*, 30(1), 659-682.
- Jensen, K. B. (Ed.). (2020). *A handbook of media and communication research: Qualitative and quantitative methodologies*. routledge.
- Jia, Z. (2012). The development and opportunities of traditional media in the new media era. *Value Engineering*, 31(8), 221-222.
- Jiang, Y. (2011). Response strategies and development trends of traditional media in the new media era. *Press Circles*, (9), 100-104.
- Jin, C. (2021). Analysis of computer network information security threats and data encryption technology. *Network Security Technology & Application*, (10), 31-32.
- Jin, X., Chen, S., & Shao, J. (2019). Multidimensional effects of ambidextrous innovation strategy and organizational dynamic capabilities on firm performance. *Forecasting*, 38(1), 30-36.
- Jing, J. (2022). Discussion on the development of China's network information security. *Bulletin of Chinese Academy of Sciences*, 37(11), 1543-1545.
- Jones, G. (1995). *Computer-Mediated communication and community*. Cybersociety.
- Kim, Y., & Kim, B. (2021). The effective factors on continuity of corporate information security management: Based on TOE framework. *Information*, 12(11), 446.
- Kogabayev, T., & Maziliauskas, A. (2017). The definition and classification of innovation. *HOLISTICA–Journal of Business and Public Administration*, 8 (1), 59–72.
- Kong, C. (2007). Market communication management and evaluation. *News Window*, (2), 126-127.

- Kör, B., & Metin, B. (2021). Understanding human aspects for an effective information security management implementation. *International Journal of Applied Decision Sciences*, 14(2), 105-122.
- Li, H. (2021). Research on countermeasures for computer network information security in the big data environment. *Information Recording Materials*, (5), 44-46.
- Li, L., & Li, H. (2022). Research on the impact of digital media technology development on news communication. *Cultural Industry*, (4), 16-18.
- Li, N. (2021). Research on cloud computing network information security protection ideas. *Modern Industrial Economy and Informationization*, 11(9), 117-119.
- Li, S., & Lu, Z. (2020). Solving China's innovation crisis and cultivating innovation culture. *Journal of Southwest Minzu University (Humanities and Social Science)*, (9).
- Li, X. (2020). TikTok's algorithm recommendation mode and development strategy. *Collection*, (5).
- Lister, M., Dovey, J., Giddings, S., Grant, I., & Kelly, K. (2008). *New media: A critical introduction*. Routledge.
- Lister, M., Dovey, J., Giddings, S., Grant, I., & Kelly, K. (2009). *New Media: a critical introduction* 2nd Edition.
- Liu, G., Ruan, B., & Liu, Q. (2021). Strengthening data security protection and improving data governance capabilities: Interpretation of the Data Security Law of the People's Republic of China (Draft). *Journal of Library and Information Sciences in Agriculture*, 33(4), 4-13.
- Liu, H., Shen, Y., Li, S., & Wang, X. (2020). Revenue allocation of cross-boundary collaborative innovation. *Journal of Systems & Management*, 29(2), 318.
- Liu, J. (2019). Inclusive leadership and employee innovative behavior: Research on the influence mechanism of labor relations atmosphere and power distance [Master's thesis, Shanghai International Studies University].
- Liu, R. (2022). Research on the dissemination mechanism of news short videos on the TikTok platform. *West China Broadcasting TV*.
- Liu, W. (2022). Research on TikTok native advertising and its communication mechanism and communication strategy [Master's thesis, Beijing Foreign Studies University].
- Liu, Y., Dong, J., & Wei, J. (2020). Digital innovation management: Theoretical framework and future research. *Management World*, 36(7), 198-217.

- Lv, Y. (2023). Essays on Political Economy (Doctoral dissertation, University of Pittsburgh).
- Manovich, L. (2003). New media from Borges to HTML. *The new media reader*, 1(2), 13-25.
- McDermott, C. M., & O'connor, G. C. (2002). Managing radical innovation: an overview of emergent strategy issues. *Journal of Product Innovation Management: an international publication of the product development & management association*, 19(6), 424-438.
- Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *computers & security*, 109, 102383.
- Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. *IEEE Transactions on Engineering Management*, 68(1), 87-100.
- NARAYANA, M. S. A. (2021). THE NEW MEDIA IN TOURISM PROMOTION IN INDIA: AN OVERVIEW.
- Ongkiko, Ila Virginia, and Flor, Alexander (2006). *Introduction to Development Communication*. University of the Philippines-Open University.
- Paat, Y. F., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, 19(1), 18-40.
- Pedersen, C. Ø., & Dalum, B. (2004). Incremental versus radical change-the case of the digital north Denmark Program.
- Peng, S. (2023). Research on the current situation and protection of network information security of "Internet+". *Electronic Communications and Computer Science*, 5(4), 180-182.
- Pfister, D. S., & Soliz, J. (2011). (Re)conceptualizing intercultural communication in a networked society. *Journal of International and Intercultural Communication*, 4(4), 246-251.
- Roberts, J. A., & David, M. E. (2023). Instagram and TikTok flow states and their association with psychological well-being. *Cyberpsychology, Behavior, and Social Networking*, 26(2), 80-89.
- Rogers, E. M., Singhal, A., & Quinlan, M. M. (2014). Diffusion of innovations. In *An integrated approach to communication theory and research* (pp. 432-448). Routledge.

- Rowe, L. A., & Boise, W. B. (1974). Organizational innovation: Current research and evolving concepts. *Public Administration Review*, 34(3), 284-293.
- Russell, N. W. (1991). The future of the mass audience.
- Ryu, S. (2024). *Media and Entertainment Industry Management: How to Integrate Business and Management with Creativity and Imagination*. Taylor & Francis.
- Satell, G. (2017). *Mapping innovation: A playbook for navigating a disruptive age* (Vol. 21). New York, NY: McGraw-Hill Education.
- Satell, G. (2017). The 4 types of innovation and the problems they solve. *Harvard Business Review*, 11, 2-9.
- SCHUMPETER, J. A. T. D. D. (1982). *ECONÔMICO*. São Paulo: abril cultural.
- Senapati, K. K., Kumar, A., & Sinha, K. (2023). Impact of information leakage and conserving digital privacy. In *Malware analysis and intrusion detection in cyber-physical systems* (pp. 166-188). IGI Global.
- Sengelmann, M. (2020). An Overview of Reverse Engineering and A Security Analysis of TikTok.
- Seo, H., Blomberg, M., Altschwager, D., & Vu, H. T. (2021). Vulnerable populations and misinformation: A mixed-methods approach to underserved older adults' online information assessment. *New Media & Society*, 23(7), 2012-2033.
- Servaes, J. (2022). Communication for development and social change. In *The Routledge Handbook of Nonprofit Communication* (pp. 23-31). Routledge.
- Shen, G., & Qu, F. (2004). The new subject of corporate communication: Marketing communication managers. *China Soft Science*, (4), 98-104.
- Shuter, R. (2011). Introduction: New media across cultures—prospect and promise. *Journal of International and Intercultural Communication*, 4(4), 241-245.
- Singh, C. L. (2010). New media and cultural identity. *China Media Research*, 6(1).
- Sirirak, S., Islam, N., & Ba Khang, D. (2011). Does ICT adoption enhance hotel performance?. *Journal of Hospitality and Tourism Technology*, 2(1), 34-49.
- Song, W., Ming, X., Han, Y., Xu, Z., & Wu, Z. (2015). An integrative framework for innovation management of product-service system. *International Journal of Production Research*, 53(8), 2252-2268.
- Stalder, F. (1999). The control revolution: how the internet is putting individuals in charge and changing the world. *Acm Sigcas Computers and Society*, 29(4), 38-39.
- Steger, M. B. (2023). *Globalization: A very short introduction*. Oxford University Press.
- Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security*, 25(5), 494-534.

- Sun, J., & Zhang, Q. (2020). Analysis of the impact of network communication on college student management. Knowledge Library.
- Sun, Y., & Huang, W. (2022). Construction of behavioral spectrum and behavioral hierarchy model of user participation in social media platforms. *Library and Information Service*, 66(9), 40-45.
- Sun, Z., & Wang, D. (2020). Practice innovation of nature reserve management under the condition of hydropower development: Taking the National Nature Reserve for Rare and Endemic Fishes in the Upper Reaches of the Yangtze River as an example. *Journal of Yangtze River Scientific Research Institute*, 37(11), 1.
- Tidd, J. (2001). Innovation management in context: environment, organization and performance. *International journal of management reviews*, 3(3), 169-183.
- Tidd, J., & Bessant, J. R. (2020). *Managing innovation: integrating technological, market and organizational change*. John Wiley & Sons.
- Tong, Y., Yao, H., & Liang, J. (2021). Exploration of computer network information security threats and data encryption technology. *Network Security Technology & Application*, (4), 20-21.
- Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. *Information & Computer Security*, 27(3), 326-342.
- Twiss, B. C. (1989). *Technological Innovation: Strategies for a New Partnership*.
- Urabe, K., Child, J., & Kagono, T. (Eds.). (1988). *Innovation and management: International comparisons* (Vol. 13). Walter de Gruyter.
- Utterback, J. M. (1994). Radical innovation and corporate regeneration. *Research Technology Management*, 37(4), 10.
- Van Dijk, J. (1998). The reality of virtual communities. *Trends in Communication*, 1(1), 39-63.
- Wang, F. (2021). Research on the communication and interaction behavior of TikTok short video users from the perspective of meme theory [Master's thesis, Inner Mongolia University].
- Wang, H., Wang, Y., & Hu, Z. (2010). Research on network information communication management. *Science and Technology Management Research*, (7), 140-143.
- Wang, J. (2021a). A review of audience research on TikTok short videos. *Today's Massmedia*, 1(3), 30-34.
- Wang, J. (2021b). Research on computer network information security issues in the big data era. *Electronic Test*, (4), 123-124.

- Wang, L., & Ding, X. (2021). On the highlights, characteristics, and application of the Personal Information Protection Law. *The Jurist*, (6), 1-16.
- Wang, X. (2020). Analysis of the application of data encryption technology in computer network information security. *Computer Knowledge and Technology*, 16(33), 53-54.
- Wang, Z., Walther, J. B., & Hancock, J. T. (2009). Social identification and interpersonal communication in computer-mediated communication: What you do versus who you are in virtual groups. *Human Communication Research*, 35(1), 59-85.
- Waters, M. (2013). *Globalization*. routledge.
- Weber, S., & Mitchell, C. (2008). Imaging, keyboarding, and posting identities: Young people and new media technologies. *Youth, identity, and digital media*, 7, 25-47.
- Wei, J., Liu, J., & Liu, Y. (2021). New trends and issues of innovation strategy theory under the new organizational context. *Management World*, 37(7), 182-197.
- Wei, L., & Ding, F. (2013). On the transformation of communication research in the new media era. *Journal of Zhejiang University (Humanities and Social Sciences)*, (4), 93-103.
- Wen, J., & Jin, K. (2022). Network information security and preventive measures in the big data era. *Network Security Technology & Application*, 7(2).
- Williams, D., Martins, N., Consalvo, M., & Ivory, J. D. (2009). The virtual census: Representations of gender, race and age in video games. *New media & society*, 11(5), 815-834.
- Xie, F., Li, B., & Xie, P. (2016, September). An integrated innovation management model from the viewpoint fitting customer value: Based on Chinese cases. In 2016 Portland International Conference on Management of Engineering and Technology (PICMET) (pp. 1086-1097). IEEE.
- Xie, L. (2021). Research on computer application based on network information security technology management. *Digital Technology and Application*, 39(6), 177-179.
- Xiong, T. (2020). Discussion on computer network information security issues in the big data era. *Computer Programming Skills & Maintenance*, (10), 160-161.
- Xu, G. (2021). Research on the relationship among inter-organizational learning, knowledge management process, and innovation performance of tech-based SMEs [Doctoral dissertation, Jilin University].
- Xu, K. (2019). Innovating brand communication management on all-media platforms to enhance corporate brand value. *Jiangxi Electric Power*, (3).

- Xu, T., & Li, T. (2021). Effect analysis of short video social reading promotion: Taking TikTok short video as an example. *Library*, 2(3), 74-81.
- Yu, S. (2019). Research on the design of management process and system for MM innovative enterprise [Master's thesis, Jilin University].
- Yuan, C., & Zhang, S. (2019). Industry-university-research collaborative innovation with enterprises as the main body: Construction of a management framework. *Science Research Management*, 40(10), 184.
- Yuan, J. (2015). Innovative models of news communication in the new media era. *Journal of News Research*, (5).
- Zhan, C., & Xu, M. (2023). The asymmetric amplification effect of digital empowerment in risk communication: Based on the epidemic information dissemination map analysis of the "WeChat, Weibo, and TikTok" platforms. *Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)*, 36(1), 71-80.
- Zhang, J., Wang, D., & Peng, H. (2022). The impact of organizational culture on innovation performance in high-tech enterprises: Based on the mediating effect of job involvement. *Journal of Changchun University*.
- Zhang, M. (2023). Compliance investigation of App personal privacy protection in China: Textual analysis based on the privacy policies of four typical social Apps. *Open Journal of Legal Science*, 11, 6396.
- Zhang, X., Li, Y., Cheng, Y., & Zhu, H. (2021). A review of theoretical and applied research on digital knowledge management. *Frontiers of Data & Computing*, 3(2), 23-28.
- Zhang, X., Peng, J., & Tu, H. (2021). The impact of corporate innovation resource allocation structure on innovation performance: Based on the perspective of different property rights. *Science & Technology Progress and Policy*, 38(8), 126-135.
- Zhang, Y. (2021). Analysis of the application of data encryption technology in computer network information security. *Electronics World*, (8), 15-16.
- Zhao, J. (2024). Research on personal information protection mechanism under the background of e-commerce. *E-Commerce Letters*, 13, 2044.
- Zhao, Y. (2022). Research on the communication mechanism and effect improvement of government TikTok from the perspective of interaction ritual chains [Master's thesis, Lanzhou University of Finance and Economics].
- Zheng, C. (2023). Research on the flow experience and social influences of users of short online videos. A case study of DouYin. *Scientific Reports*, 13(1), 3312.

- Zheng, Y. (2007). Media convergence: The development concept in the new media era. *Contemporary Communications*, (3), 1-1.
- Zhu, H., & Li, Z. (2009). Integrated marketing communication and the essence of its management. *Hebei Academic Journal*, 29(2), 208-211.
- Zhu, Z. (2022). Exploring the practical path of creative communication of popular science new media: Taking Guokr as an example. *Voice & Screen World*.



ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี



ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี



ภาคผนวก ก
เครื่องมือที่ใช้ในการวิจัย

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

แบบสัมภาษณ์เชิงลึก

1. กลุ่มเป้าหมายสำหรับการสัมภาษณ์ ได้แก่ เจ้าหน้าที่ภาครัฐ ผู้บริหารระดับสูง ผู้บริหารระดับกลาง ผู้บริหารระดับปฏิบัติการ และบล็อกเกอร์ผู้พัฒนาแพลตฟอร์มออนไลน์ไต้หวัน

ส่วนที่ 1.1 ข้อมูลทั่วไปของผู้ให้สัมภาษณ์

1. ตำแหน่งและบทบาทหน้าที่ความรับผิดชอบในปัจจุบันที่เกี่ยวข้องกับแพลตฟอร์มออนไลน์ไต้หวัน

.....

.....

.....

2. ประสบการณ์การทำงานที่เกี่ยวข้องกับการจัดการความปลอดภัยระบบสารสนเทศ

.....

.....

.....

ส่วนที่ 1.2 คำถามเกี่ยวกับกลยุทธ์การจัดการความปลอดภัยระบบสารสนเทศทั้ง 5 ด้าน

1. ด้านระบบการจัดการความปลอดภัย: แพลตฟอร์มออนไลน์ไต้หวันมีการกำหนดโครงสร้างคณะกรรมการความปลอดภัย ระดับการเข้าถึงข้อมูล และมีการใช้เทคโนโลยีใดในการรักษาความปลอดภัยทางไซเบอร์เพื่อปกป้องข้อมูลจากการโจมตี

.....

.....

.....

2. ด้านการกำหนดเป้าหมาย: องค์กรมีการนำกรอบงานมาตรฐานสากล เช่น ISO 27001 หรือ NIST มาใช้ในการประเมินความเสี่ยงและกำหนดเป้าหมายความปลอดภัยของระบบสารสนเทศอย่างไร

.....

.....

.....

3. ด้านนโยบายการกำกับดูแล: แพลตฟอร์มมีแนวทางและกฎระเบียบในการจัดการเนื้อหาที่ผิดกฎหมาย การสร้างความโปร่งใส และปกป้องสิทธิข้อมูลส่วนบุคคลของผู้ใช้งานอย่างไรให้สอดคล้องกับกฎหมายของรัฐบาลจีน

.....

.....

.....

4. ด้านการพัฒนาบุคลากร: องค์กรมีรูปแบบการส่งเสริมบุคลากรด้านความปลอดภัยสารสนเทศ ผ่านกระบวนการฝึกอบรม (Training) การศึกษา (Education) และการพัฒนา (Development) อย่างไรเพื่อให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลง

5. ด้านการสร้างเชื่อมั่น: แพลตฟอร์มมีวิธีการสื่อสารและสร้างความมั่นใจให้แก่ผู้ใช้งาน อย่างไรในเรื่องการปกป้องข้อมูลส่วนบุคคล โดยเฉพาะเมื่อมีการประยุกต์ใช้ AI ร่วมกับบุคลากรที่เป็นมนุษย์ในการให้บริการ

ส่วนที่ 1.3 คำถามเกี่ยวกับการพัฒนารูปแบบการจัดการความปลอดภัยในอนาคต

1. ในมุมมองของท่าน จุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT) ในการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มไต่ขึ้นในปัจจุบันมีอะไรบ้าง

2. แพลตฟอร์มออนไลน์ไต่ขึ้นควรบูรณาการหลักการสำคัญ 3 ประการ (CIA Triad) ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) เข้ากับระบบการทำงานอย่างเป็นรูปธรรมได้อย่างไร

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

แบบสอบถามเพื่อการวิจัย

ส่วนที่ 2.1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. ภูมิภาคที่ท่านอาศัยอยู่ในปัจจุบัน

- () ภาคตะวันออก (มณฑลชานตง)
- () ภาคเหนือ (มณฑลเหอหนาน)
- () ภาคตะวันตก (มณฑลเสฉวน)
- () ภาคใต้ (มณฑลกวางตุ้ง)

2. ความถี่ในการใช้งานแพลตฟอร์มออนไลน์ต่อวัน

- () น้อยกว่า 1 ชั่วโมง
- () 1 - 3 ชั่วโมง
- () 4 - 6 ชั่วโมง
- () มากกว่า 6 ชั่วโมงขึ้นไป

3. วัตถุประสงค์หลักในการใช้งาน

- () เพื่อความบันเทิงและพักผ่อนหย่อนใจ
- () เพื่อซื้อสินค้าและบริการ
- () เพื่อติดตามข่าวสารและข้อมูลความรู้
- () เพื่อการทำธุรกิจหรือสร้างรายได้
- () อื่น ๆ (โปรดระบุ).....

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

ส่วนที่ 2.2 ความคาดหวังและความต้องการต่อการจัดการความปลอดภัยระบบสารสนเทศของ

แพลตฟอร์มออนไลน์ไต้ยีน

คำชี้แจง: โปรดทำเครื่องหมายในช่องที่ตรงกับระดับความเห็นของท่าน (5 = มากที่สุด, 4 = มาก, 3 = ปานกลาง, 2 = น้อย, 1 = น้อยที่สุด)

ความคาดหวังและความต้องการต่อการจัดการความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน	ระดับความเห็น				
	5	4	3	2	1
1. ท่านคาดหวังให้แพลตฟอร์มมีระบบป้องกันผู้ไม่มีสิทธิเข้าถึงหรือแก้ไขข้อมูลส่วนบุคคลของท่านเพื่อป้องกันข้อมูลรั่วไหล					
2. ท่านมีความต้องการให้ระบบการจัดการความปลอดภัยเปลี่ยนจากระบบแมนนวลไปสู่การตรวจจับภัยคุกคามทางไซเบอร์เชิงรุกเพื่อความเร็ว					
3. ท่านคาดหวังให้แพลตฟอร์มปฏิบัติตามกฎหมายและมาตรฐานสากล เช่น ISO 27001 อย่างเคร่งครัดเพื่อปกป้องข้อมูลของท่าน					
4. ท่านมีความต้องการให้แพลตฟอร์มเปิดเผยนโยบายการกลั่นกรองเนื้อหาและมีช่องทางให้ร้องเรียนเนื้อหาที่เป็นอันตรายได้อย่างชัดเจน					
5. ท่านต้องการความช่วยเหลือจากพนักงานที่เป็นมนุษย์ในการตอบคำถามด้านความปลอดภัยที่มีความซับซ้อนนอกเหนือจากการใช้เทคโนโลยี AI					

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี

ส่วนที่ 2.3 ความเชื่อมั่นต่อความปลอดภัยระบบสารสนเทศของแพลตฟอร์มออนไลน์ไต้ยีน

คำชี้แจง: โปรดทำเครื่องหมายในช่องที่ตรงกับระดับความเห็นของท่าน (5 = มากที่สุด, 4 = มาก, 3 = ปานกลาง, 2 = น้อย, 1 = น้อยที่สุด)

ความเชื่อมั่นต่อความปลอดภัยระบบสารสนเทศ ของแพลตฟอร์มออนไลน์ไต้ยีน	ระดับความเห็น				
	5	4	3	2	1
1. ท่านมีความเชื่อมั่นว่าแพลตฟอร์มสามารถรักษาความลับ (Confidentiality) ของข้อมูลไม่ให้ถูกเปิดเผยต่อผู้ไม่มีสิทธิ์					
2. ท่านมีความเชื่อมั่นในความถูกต้องครบถ้วน (Integrity) ของข้อมูลในระบบว่าจะไม่ถูกทำลายหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต					
3. ท่านมีความเชื่อมั่นในความพร้อมใช้งาน (Availability) ของระบบสารสนเทศที่สามารถเข้าถึงได้ตลอดเวลาเมื่อต้องการใช้งาน					
4. ท่านรู้สึกมั่นใจในความน่าเชื่อถือของแพลตฟอร์มและยินดีที่จะตัดสินใจซื้อสินค้าหรือจ่ายเงินเพิ่มขึ้นเพื่อซื้อสินค้าผ่านแพลตฟอร์มออนไลน์ไต้ยีน					
5. แม้จะมีความกังวลด้านไซเบอร์ลมีเดีย แต่ท่านยินดีให้แพลตฟอร์มนำข้อมูลของท่านไปใช้เพื่อนำเสนอบริการหรือโปรโมชั่นเฉพาะบุคคล เนื่องจากมีความเชื่อมั่นในระบบความปลอดภัย					

ประวัติผู้วิจัย

ชื่อ-นามสกุล	Liu Yin
วัน เดือน ปีเกิด	18 พฤศจิกายน ค.ศ. 1983
สถานที่เกิด	เขตอู่เจียง เมืองซูโจว มณฑลเจียงซู ประเทศจีน
ที่อยู่ปัจจุบัน	ห้อง 1501 อาคาร 1 คอร์ทยาร์ด 3 อินเตอร์ เนชันแนล การ์เดน ตำบลฉางหยาง เขตฝาง ซาน กรุงปักกิ่ง ประเทศจีน
อาชีพปัจจุบัน	ทนายความ
สถานที่ทำงานปัจจุบัน	สำนักงานกฎหมายปักกิ่ง ไท่หยวน (Beijing Taiyuan Law Firm)
ประวัติการศึกษา	พ.ศ. 2548 ปริญญานิติศาสตรบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยปักกิ่ง (Peking University) พ.ศ. 2563 ปริญญานิติศาสตรมหาบัณฑิต บัณฑิตวิทยาลัย สถาบันสังคมศาสตร์แห่ง สาธารณรัฐประชาชนจีน

ลิขสิทธิ์ของมหาวิทยาลัยราชภัฏรำไพพรรณี