การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

Government Agencies' Cyber Threat Risk Management : Lessons Learned from Judicial Agencies under the Jurisdiction of the Chief Justice Region 9

ธนพงศ์ ฉันทวิเชียร

Thanaphong Chanthawichian

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญารัฐประศาสนศาสตรมหาบัณฑิต
สาขาวิชารัฐประศาสนศาสตร์
มหาวิทยาลัยสงขลานครินทร์

A Minor Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Public Administration
Prince of Songkla University

2566

การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

Government Agencies' Cyber Threat Risk Management : Lessons Learned from Judicial Agencies under the Jurisdiction of the Chief Justice Region 9

ธนพงศ์ ฉันทวิเชียร

Thanaphong Chanthawichian

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญารัฐประศาสนศาสตรมหาบัณฑิต
สาขาวิชารัฐประศาสนศาสตร์
มหาวิทยาลัยสงขลานครินทร์

A Minor Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Public Administration
Prince of Songkla University
2566

ชื่อสารนิพนธ์ การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ผู้เขียน นายธนพงศ์ ฉันทวิเชียร

สาขาวิชา รัฐประศาสนศาสตร์

อาจารย์ที่ปรึกษาสารนิพนธ์

.....

(รองศาสตราจารย์ ดร.สมพร คุณวิชิต)

คณะกรรมการสอบ

.....ประธานกรรมการ

(รองศาสตราจารย์ ดร.สมพร คุณวิชิต)

.....กรรมการ

(รองศาสตราจารย์ ดร.บุษบง ชัยเจริญวัฒนะ)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.จุฑามณี ตระกูลมุทุตา)

.....

(ผู้ช่วยศาสตราจารย์ ดร.จุฑามณี ตระกูลมุทุตา)

ผู้อำนวยการหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต

สาขาวิชารัฐประศาสนศาสตร์

ชื่อสารนิพนธ์ การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
ผู้เขียน นายธนพงศ์ ฉันทวิเชียร
สาขาวิชา รัฐประศาสนศาสตร์
ปีการศึกษา 2565

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ (1) วิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง และแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 (2) ศึกษาความสำเร็จและอุปสรรคในการดำเนินงานด้านการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ และ (3) เพื่อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคต สำหรับหน่วยงานดังกล่าว ใช้ระเบียบการวิจัยเชิงคุณภาพ โดยการศึกษาค้นคว้าเอกสารและการสัมภาษณ์เชิงลึก เก็บข้อมูลจากผู้ให้ข้อมูลหลักทั้งสิ้น 36 คน ได้แก่ เจ้าหน้าที่ผู้ดูแลระบบและเจ้าหน้าที่ผู้ปฏิบัติงานศาล จากนั้นนำข้อมูลมาวิเคราะห์โดยใช้เทคนิคการสร้างข้อสรุปแบบอุปนัย

ผลการศึกษา พบว่า ปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์ มีอยู่ 5 ประเภท ได้แก่ การใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด การใช้เครือข่ายไร้สาย สภาพแวดล้อมที่ล่อแหลม การโจมตีแบบไม่ตั้งใจ และการโจมตีแบบตั้งใจ ความสำเร็จของการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานดังกล่าว ได้แก่ มีการกำหนดระดับการเข้าถึงข้อมูลและการป้องกันการเข้าระบบโดยไม่พึงประสงค์ ข้อมูลมีความถูกต้อง ครบถ้วนแม่นยำ และฮาร์ดแวร์และซอฟต์แวร์อยู่ในสภาพพร้อมใช้งานและพร้อมป้องกันจากภัยคุกคามไซเบอร์ ส่วนอุปสรรคของการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ งบประมาณในการจัดหาฮาร์ดแวร์และซอฟต์แวร์ยังไม่เพียงพอ บุคลากรยังขัดความรู้และทักษะการจัดการความเสี่ยงไซเบอร์ จำนวนบุคลากรทางไซเบอร์ที่มีไม่เพียงพอ ที่ตั้งของศาลที่อยู่ใกล้ทะเลทำให้มีความเสี่ยงได้รับผลกระทบต่อฮาร์ดแวร์ทำให้เกิดความเสียหาย และระบบที่เกิดขึ้นใหม่เป็นระบบงานซ้ำซ้อนที่มีอยู่เดิม ข้อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคต ได้แก่ เพิ่มการจัดสรรงบประมาณสำรวจประเมินความเสี่ยงของฮาร์ดแวร์และซอฟต์แวร์รวมทั้งการต่อประกันอุปกรณ์เครือข่าย จัดอบรมพัฒนาทักษะเจ้าหน้าที่ผู้ดูแลระบบและเจ้าหน้าที่ ขออัตรากำลังเพิ่มเติมหรือใช้บุคลากรทางไซเบอร์ร่วมกันในการแก้ไขปัญหา ควรปรับเปลี่ยนนโยบายที่ตั้งศาลที่อยู่ใกล้ทะเลหรือควรออกแบบอาคารและวัสดุในการปกป้องอุปกรณ์ ครุภัณฑ์ต่าง ๆ ไม่ให้เกิดความเสียหายหากศาลตั้งอยู่ใกล้ทะเล และสุดท้ายควรพัฒนาระบบงานใหม่ไม่ให้เกิดความซ้ำซ้อน

Title Government Agencies' Cyber Threat Risk Management
: Lessons Learned from Judicial Agencies under the Jurisdiction of the Chief Justice Region 9
Author Mr. Thanaphong Chanthawichian
Major Public Administration
Academie Year 2022

ABSTRACT

The purposes of this research are to (1) analyze threats, risk factors, and current practices of cyber threat risk management among judicial agencies under the jurisdiction of the Chief Justice Region 9; (2) examine the success and obstacles of cyber threat risk management; and (3) provide suggestions for better management of cyber threat risk in the future. Qualitative research methods were employed. Data were gathered through documentary research and in-depth interviews. The 36 participants who served as key informants in this study consisted of representatives from the judicial agencies under the jurisdiction of the Chief Justice Region 9. Data were verified using the data triangulation method, and after that, data were analyzed inductively.

Results reveal that cyber threat risk factors faced by these agencies include the free-downloaded program software, wireless internet connection, exposed environment, unintentional attack and intentional attack. The successes of cyber threat risk management among these agencies include the establishment of accessibility levels, correctness of data, accuracy of data, and the readiness for preventing cyber threat for both software and hardware. Results also show that they are 5 obstacles that hampered the management of cyber threat risk among these agencies, which include inadequate budget for software and hardware procurement, the lack of knowledge and skill regarding cyber threat risk management among personnel, the insufficiency of IT or cyber personnel, the locations of judicial agencies that are near the coasts, and the new systems that are often redundant with the existing systems. It is recommended in this research that judicial agencies allocate more budget to assess risk in both software and hardware and to purchase insurance for connection equipment, train personnel about cyber treat risk management, request for more IT or cyber personnel, change location from coastal areas and reduce redundancy of systems.

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้ สำเร็จลุล่วงไปได้ด้วยความกรุณาจากหลายฝ่าย โดยเฉพาะอย่างยิ่ง รองศาสตราจารย์ ดร.สมพร คุณวิชิต อาจารย์ที่ปรึกษาสารนิพนธ์ ที่กรุณาสละเวลาในการให้ความรู้ คำปรึกษา ตลอดจนตรวจสอบแก้ไขความถูกต้องจนสารนิพนธ์เสร็จสมบูรณ์

ขอขอบคุณ รองศาสตราจารย์ ดร.บุษบง ชัยเจริญวัฒนะ และผู้ช่วยศาสตราจารย์ ดร.จุฑามณี ตระกูลมุทุตา คณะกรรมการสอบทั้ง 2 ท่านที่ได้กรุณาให้แนวคิด และข้อเสนอแนะต่าง ๆ จนทำให้สารนิพนธ์สำเร็จลงได้ด้วยดี

ขอขอบคุณ อธิบดีผู้พิพากษาภาค 9 ข้าราชการฝ่ายตุลาการศาลยุติธรรมทุกท่านที่กรุณาเสียสละเวลาในการตอบแบบสอบถามที่เป็นประโยชน์ต่องานวิจัย รวมถึงเจ้าหน้าที่ประจำหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต ที่คอยช่วยเหลือและอำนวยความสะดวกแก่ผู้วิจัย ในการช่วยเหลือประสานงานให้งานวิจัยสำเร็จลุล่วงไปด้วยดี

ขอขอบคุณ บิดา มารดา บุคคลในครอบครัว ที่ห่วงใย เป็นกำลังใจ และสนับสนุนการศึกษาแก่ผู้วิจัยเสมอมา

คุณประโยชน์ใดอันพึงมีจากสารนิพนธ์ฉบับนี้ ผู้วิจัยขอมอบเป็นกตัญญูกตเวทีแด่บิดา มารดา บูรพาจารย์ และสถาบันการศึกษาที่ได้ประสิทธิ์ประสาทวิชา รวมทั้งผู้มีพระคุณทุกท่าน

ธนพงศ์ ฉันทวิเชียร

สารบัญ

	หน้า
บทคัดย่อ	(3)
ABSTRACT	(4)
กิตติกรรมประกาศ	(5)
สารบัญ	(6)
รายการตาราง	(8)
รายการภาพประกอบ	(9)
บทที่ 1 บทนำ	1
1.1 ความเป็นมาของปัญหาและปัญหา	1
1.2 วัตถุประสงค์	3
1.3 ความสำคัญและประโยชน์ของการวิจัย	3
1.4 ขอบเขตของการวิจัย	3
1.5 นิยามศัพท์เฉพาะ	4
บทที่ 2 เอกสารงานวิจัยที่เกี่ยวข้อง	6
2.1 แนวคิดเกี่ยวกับภัยคุกคามไซเบอร์	6
2.2 แนวคิดการจัดการความเสี่ยง	9
2.3 แนวคิดความมั่นคงปลอดภัยไซเบอร์	19
2.4 แนวคิดการบริการสาธารณะและการให้บริการสาธารณะหน่วยงานศาลยุติธรรม	21
2.5 เอกสารงานวิจัยที่เกี่ยวข้อง	27
2.6 กรอบแนวคิดการวิจัย	51
บทที่ 3 วิธีดำเนินการวิจัย	52
3.1 ประชากรกลุ่มตัวอย่างและหน่วยงานในพื้นที่ที่ทำการศึกษา	52
3.2 กลุ่มผู้ให้ข้อมูลสำคัญ	54
3.3 แบบแผนการวิจัย	56
3.4 วิธีการเก็บข้อมูลและเครื่องมือที่ใช้ในการวิจัย	56
3.5 การสร้างเครื่องมือและการตรวจสอบคุณภาพเครื่องมือในการวิจัย	57
3.6 การวิเคราะห์ข้อมูล	57
3.7 การพิทักษ์สิทธิของกลุ่มผู้ให้ข้อมูลหลัก	59
บทที่ 4 ผลการวิจัย	60
4.1 ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9	60
4.2 เครื่องมือ มาตรการ และแนวปฏิบัติในการจัดการภัยคุกคามไซเบอร์ของศาลหน่วยงานยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9	67

สารบัญ (ต่อ)

หน้า

4.3 ความสำเร็จและอุปสรรคในการจัดการภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 75
4.4 เสนอแนะและแนวทางการจัดการภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 80
บทที่ 5 สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ 83
5.1 สรุปผลการวิจัย 83
5.2 การอภิปราย 88
5.3 ข้อเสนอแนะ 95
บรรณานุกรม 98
ภาคผนวก 103
ภาคผนวก ก แบบสัมภาษณ์ 104
ภาคผนวก ข หนังสือขอความอนุเคราะห์ในการเข้าสัมภาษณ์ 109
ประวัติผู้เขียน 128

รายการตาราง

ตาราง		หน้า
1	ระดับความเสี่ยง	17
2	งานวิจัยงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์	42
3	งานวิจัยเกี่ยวกับการบริการสาธารณะ	49
4	กลุ่มผู้ให้ข้อมูลหลัก เจ้าหน้าที่ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ปฏิบัติงานศาล	55
5	ตรวจสอบความสอดคล้องข้อคำถามกับวัตถุประสงค์การวิจัย	58

รายการภาพประกอบ

ภาพประกอบ		หน้า
1	กรอบแนวคิด	51
2	การโจมตีแบบไม่ตั้งใจ	65
3	ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรม ในเขตอำนาจอธิบดีผู้พิพากษาภาค 9	66
4	สรุปปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรม ในเขตอำนาจอธิบดีผู้พิพากษาภาค 9	67
5	เครื่องมือการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์	70
6	มาตรการการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์	71
7	แนวปฏิบัติการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์	75
8	ความสำเร็จในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์	77
9	ปัญหาและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์	80

บทที่ 1
บทนำ

1.1 ความเป็นมาของปัญหาและปัญหา

ในปัจจุบันเทคโนโลยีได้เข้ามามีบทบาทและความสำคัญต่อการดำเนินชีวิตของมนุษย์อย่างมากโดยอยู่ในรูปแบบของสื่อต่าง ๆ เสียง ภาพ และตัวอักษร บทบาทที่สำคัญของเทคโนโลยีที่เกี่ยวข้องกับการพัฒนาด้านต่าง ๆ ได้แก่ ด้านเศรษฐกิจ ด้านสังคม ด้านการศึกษา ด้านสาธารณสุข ด้านการเกษตร ด้านสิ่งแวดล้อม ด้านอุตสาหกรรมและบริการ ด้านการบริการของรัฐ ด้านการท่องเที่ยว ฯลฯ ในหลายประเทศได้มีการพัฒนาและสร้างสรรค์เทคโนโลยีและนวัตกรรมใหม่ ๆ มาโดยตลอด ซึ่งเทคโนโลยีทำให้สภาพของสังคมเปลี่ยนไปจากยุคโลกาภิวัตน์เป็นยุคดิจิทัล ความก้าวหน้าของเทคโนโลยีทำให้การติดต่อสื่อสารสะดวกรวดเร็วมากขึ้น รวมถึงข้อมูลข่าวสารและความรู้ซึ่งประกอบกันเป็นสารสนเทศ สามารถประยุกต์ใช้ได้ตั้งแต่ระดับบุคคล ระดับองค์การ ระดับประเทศ จนถึงไร้พรหมแดนอันเนื่องมากจากอิทธิพลของเทคโนโลยีทั้งสิ้น

จากการพัฒนาเทคโนโลยีก้าวหน้าอย่างรวดเร็ว ทำให้ประเทศไทยต้องปรับเปลี่ยนให้ทันกับเทคโนโลยีที่มีความเปลี่ยนแปลง โดยการกำหนดกรอบและแนวทางพัฒนาให้หน่วยงานของรัฐทุกภาคส่วนต้องปฏิบัติตาม เพื่อให้บรรลุวิสัยทัศน์ประเทศไทย ภายใต้แผนยุทธศาสตร์ชาติ 20 ปี ซึ่งมีโมเดลไทยแลนด์ 4.0 โดยระบบราชการเป็นกำลังสำคัญในการขับเคลื่อนนโยบายให้บรรลุตามวัตถุประสงค์ จึงต้องมีการปรับเปลี่ยนและปฏิรูประบบราชการให้สอดคล้องกับยุทธศาสตร์ชาติ 20 ปี และรองรับโมเดลการพัฒนาประเทศไทย 4.0 ให้เป็นระบบราชการ 4.0 ดังนั้นเพื่อให้การดำเนินงานของศาลยุติธรรมสอดคล้องกับนโยบายของรัฐที่ต้องการขับเคลื่อนประเทศไทยให้มีความก้าวหน้าทางเทคโนโลยี

ศาลยุติธรรมได้มีการพัฒนาระบบโดยรวมทั้งในส่วนฮาร์ดแวร์และซอฟต์แวร์ โดยติดตั้งอุปกรณ์ป้องกันเครือข่าย และอุปกรณ์ตรวจสอบการบุกรุก เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น อย่างไรก็ตามในปี 2559 เว็บไซต์ศาลยุติธรรมถูกเจาะระบบเนื่องจากมีกลุ่มแฮกเกอร์ที่ไม่พึงพอใจในการตัดสินคดีเกาะเต่าของศาลจังหวัดสมุย ซึ่งส่งผลทำให้เว็บไซต์ศาลยุติธรรมทั่วประเทศใช้งานไม่ได้ รวมถึงต้องปิดระบบต่าง ๆ ภายในของศาลยุติธรรมด้วย ซึ่งสำนักเทคโนโลยีสารสนเทศ (2559) ได้ตรวจพบการทำงานของเครื่องคอมพิวเตอร์ข่ายที่ให้บริการเว็บไซต์หน่วยงานศาลยุติธรรมทั่วประเทศมีการทำงานที่ผิดปกติ จึงได้ดำเนินการตรวจสอบและวิเคราะห์ปัญหาของระบบดังกล่าว พบว่ามีผู้ไม่หวังดีพยายามชัดขวางการทำงานหรือเจาะระบบ (โจมตีในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเว็บไซต์หน่วยงานศาลทั่วประเทศโดยใช้วิธี Denial Of Service (Dos) ซึ่งส่งผลกระทบทำให้การเข้าดูหรือค้นหาข้อมูลบนเว็บไซต์ของสำนักงานศาลยุติธรรมช้า ทั้งนี้ สำนักเทคโนโลยีสารสนเทศจึงได้ดำเนินการตรวจสอบแก้ไข

ปัญหาดังกล่าวโดยเร่งด่วน จากการตรวจสอบสาเหตุที่ถูกเจาะระบบผ่านช่องโหว่ของเว็บไซต์ศาลยุติธรรมที่ไม่ได้ให้ความสำคัญการเขียนโค๊ดอย่างไรให้มีความปลอดภัย หลังจากนั้นศาลยุติธรรมได้เพิ่มเติมในส่วนของเว็บแอพลิเคชั่นไฟล์วอล และให้ความสำคัญในการเขียนโค๊ดให้มีความปลอดภัยมากขึ้น รวมถึงการปรับปรุงระบบเครือข่ายให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นโดยระบบที่จะออกสู่ภายนอกได้จะต้องผ่านอุปกรณ์ป้องกันเครือข่าย (Firewall) ถึงสองชั้น ได้แก่ ที่หน่วยงานศาลยุติธรรมทั่วประเทศและที่สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรมที่ส่วนกลาง

การจัดการความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่าง ๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่าง ๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร เทคโนโลยีสารสนเทศมีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์ คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

ที่ผ่านมีเพียงการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เช่น การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของวิสาหกิจขนาดกลางและขนาดย่อมในอำเภอหนองแค จังหวัดสระบุรี หรือ การจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เช่น แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร แต่ยังไม่มีงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ทั้งนี้คณะกรรมการบริหารจัดการความเสี่ยงของสำนักงานศาลยุติธรรม (2564) มีเพียงแต่การจัดการความเสี่ยงทางด้านเทคโนโลยี และยังไม่เคยมีการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์สำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ด้วยเหตุนี้ผู้วิจัยจึงสนใจที่จะศึกษาถึงการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของภาครัฐ หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 โดยหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ปัจจุบันมีภารกิจการดำเนินงานซึ่งครอบคลุมหน่วยงานจำนวน 18 ศาล (ศาลที่ตั้งอยู่ในพื้นที่ 7 จังหวัด ได้แก่ จังหวัดตรัง จังหวัดพัทลุง จังหวัดสตูล จังหวัดสงขลา จังหวัดปัตตานี จังหวัดยะลา จังหวัดนราธิวาส) เพื่อได้แนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ และเป็นข้อมูลประกอบการสนับสนุนฮาร์ดแวร์และซอฟต์แวร์

เพื่อลดความเสี่ยงจากภัยคุกคามด้านไซเบอร์ได้อย่างเหมาะสม และมีความมั่นคงปลอดภัยทันต่อการเปลี่ยนแปลงของโลกไซเบอร์ในปัจจุบัน

1.2 วัตถุประสงค์

1. เพื่อศึกษาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
2. เพื่อศึกษาความสำเร็จและอุปสรรคในการดำเนินงานด้านการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
3. เพื่อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

1.3 ความสำคัญและประโยชน์ของการวิจัย

1. เพื่อให้ได้ข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์และความเสี่ยงจากภัยคุกคามไซเบอร์
2. เพื่อนำผลการศึกษาไปใช้ในพัฒนาแนวทางในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
3. เพื่อได้แนวปฏิบัติในการปรับปรุงการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
4. ทำให้หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีความมั่นคงความปลอดภัยจากความเสี่ยงภัยคุกคามไซเบอร์มากขึ้น
5. เพื่อเป็นข้อมูลประกอบการสนับสนุนฮาร์ดแวร์และซอฟต์แวร์เพื่อลดความเสี่ยงจากภัยคุกคามด้านไซเบอร์ ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

1.4 ขอบเขตของการวิจัย

การวิจัยนี้เป็นการจัดการเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 โดยการวิเคราะห์ภัยคุกคามทางไซเบอร์และความเสี่ยงด้านไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

1. ขอบเขตด้านประชากร

เจ้าหน้าที่ผู้ดูแลระบบหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ทั้งสิ้น 18 ศาล โดยเป็นเจ้าหน้าที่ผู้ดูแลระบบ จำนวน 18 ท่าน และในส่วนเจ้าหน้าที่ผู้ปฏิบัติงานมีทั้งหมด 715 ท่าน ใช้ตัวแทนอย่างน้อยจำนวน 18 ท่าน รวมทั้งสิ้น 36 ท่าน

2. ขอบเขตด้านเนื้อหา

ศึกษาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จและอุปสรรค การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์เพื่อแก้ไขปัญหาและปรับปรุงการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

3. ขอบเขตด้านพื้นที่

พื้นที่ภาคใต้ตอนล่างของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 จำนวน 18 ศาล (ศาลที่ตั้งอยู่ในพื้นที่ 7 จังหวัด ได้แก่ จังหวัดตรัง จังหวัดพัทลุง จังหวัดสตูล จังหวัดสงขลา จังหวัดปัตตานี จังหวัดยะลา จังหวัดนราธิวาส)

1.5 นิยามศัพท์เฉพาะ

ภัยคุกคามไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และกระทบหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ หมายถึง การดำเนินการในการป้องกันภัยคุกคามไซเบอร์โดยใช้มาตรการ และกระบวนการบริหารความเสี่ยง เพื่อวิเคราะห์ภัยคุกคามไซเบอร์ ประเมินความเสี่ยงที่อาจจะเกิดขึ้น โดยการจัดหา จัดทำมาตรการ จัดหาวัสดุอุปกรณ์ เพื่อป้องกันและลดผลกระทบจากภัยคุกคามไซเบอร์หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ความมั่นคงปลอดภัยไซเบอร์ หมายถึง วิธีการ มาตรการ หรือการดำเนินการใด ๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ การรักษาความครบถ้วน และสภาพพร้อมใช้งาน ของอุปกรณ์และข้อมูลภายในระบบสารสนเทศของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ความสำเร็จในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีหลายมิติดังนี้

1. การรักษาความลับ ข้อมูลควรจะต้องมีการกำหนดระดับการเข้าถึงข้อมูลและการป้องกันการเข้าระบบโดยไม่พึงประสงค์

2. การรักษาความครบถ้วน ข้อมูลควรจะมีความถูกต้อง ครบถ้วนแม่นยำ โดยถ้ามีความคลาดเคลื่อน (error) อยู่ในเกณฑ์ที่ยอมรับได้

3. สภาพพร้อมใช้งาน ทั้งฮาร์ดแวร์และซอฟต์แวร์อยู่ในสภาพพร้อมใช้งานและมีพร้อมป้องกันจากภัยคุกคามไซเบอร์

หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 หมายถึง ศาลยุติธรรมชั้นต้นที่ตั้งอยู่ในพื้นที่ 7 จังหวัดภาคใต้ ได้แก่ จังหวัดตรัง (ศาลจังหวัดตรัง ศาลแขวงตรัง ศาลเยาวชนและครอบครัวจังหวัดตรัง) จังหวัดพัทลุง (ศาลจังหวัดพัทลุง ศาลเยาวชนและครอบครัวจังหวัดพัทลุง) จังหวัดสตูล (ศาลจังหวัดสตูล ศาลเยาวชนและครอบครัวจังหวัดสตูล) จังหวัดสงขลา (ศาลจังหวัดสงขลา ศาลจังหวัดนาทวี ศาลแขวงสงขลา ศาลเยาวชนและครอบครัวจังหวัดสงขลา) จังหวัดปัตตานี (ศาลจังหวัดปัตตานี ศาลเยาวชนและครอบครัวจังหวัดปัตตานี) จังหวัดยะลา (ศาลจังหวัดยะลา ศาลจังหวัดเบตง ศาลเยาวชนและครอบครัวจังหวัดยะลา) จังหวัดนราธิวาส (ศาลจังหวัดนราธิวาส ศาลเยาวชนและครอบครัวจังหวัดนราธิวาส)

บทที่ 2
เอกสารงานวิจัยที่เกี่ยวข้อง

การศึกษาเรื่องการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ผู้วิจัยได้ทำการทบทวนแนวคิดทฤษฎี และงานวิจัยที่เกี่ยวข้องเพื่อนำมาใช้ในการดำเนินการวิจัยและสร้างกรอบแนวคิดสำหรับการวิจัยดังนี้

2.1 แนวคิดเกี่ยวกับภัยคุกคามไซเบอร์

2.2 แนวคิดการจัดการความเสี่ยง

2.3 แนวคิดความมั่นคงปลอดภัยทางไซเบอร์

2.4 แนวคิดการบริการสาธารณะและการให้บริการสาธารณะหน่วยงานศาลยุติธรรม

2.5 เอกสารงานวิจัยที่เกี่ยวข้อง

2.6 กรอบแนวคิดงานวิจัย

2.1 แนวคิดเกี่ยวกับภัยคุกคามไซเบอร์

2.1.1 ความหมายของภัยคุกคามไซเบอร์

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562; ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่องหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ. 2563, 2563; ยุทธศักดิ์ รักเสรีพิทักษ์ และ ศิริลักษม์ ตันตยกุล, 2565)

ส่วน ปรัชญา เฉลิมวัฒน์ (2560) ได้ให้ความหมาย ภัยคุกคามไซเบอร์ หมายถึงรูปแบบของภัยคุกคามที่มากับระบบอินเทอร์เน็ต และคอมพิวเตอร์ที่เชื่อมต่อ โดยมีเป้าหมายในหลาย ๆ ระดับ ตั้งแต่ระดับผู้ใช้งานอินเทอร์เน็ตทั่วไป องค์กร หรือ ระดับประเทศ

วิลาส วิถีไพร (2561) ได้ให้ความหมาย ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า ภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจ ตลอดจนความมั่นคงของประเทศ การโจมตีทางไซเบอร์มีหลายรูปแบบ เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ การดักรับข้อมูลคอมพิวเตอร์ (Sniffing)

การโจมตีโดยชุดคำสั่งไม่พึงประสงค์ (Malicious Software: Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack: DOS)

โดยสรุป ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และกระทบต่อทางเศรษฐกิจ สังคม ตลอดจนความมั่นคงของประเทศ

2.1.2 ประเภทภัยคุกคามไซเบอร์

อนาวิล แก้วสอาด และ ณัฐวี อุตกฤษฎ์ (2564) ได้แบ่งประเภทภัยคุกคามไซเบอร์ดังนี้

1. ธรรมชาติ ได้แก่ น้ำท่วม แผ่นดินไหว พายุฟ้าคะนอง การพังทลายของอาคารพื้นที่

2. สภาพแวดล้อม ได้แก่ ระบบไฟฟ้าขัดข้อง อุณหภูมิไม่เหมาะสม ความชื้นจากเครื่องปรับอากาศ พื้นที่ก่อสร้างโครงสร้างพื้นฐาน

3. ภัยคุกคามที่มาจากมนุษย์

3.1 การโจมตีแบบตั้งใจ อาชญากรรมคอมพิวเตอร์ ผู้ก่อการร้ายทางไซเบอร์ การจารกรรมทางไซเบอร์

3.2 การโจมตีแบบไม่ตั้งใจ เจ้าหน้าที่ภายในหน่วยงานที่ขาดความรู้ในการปฏิบัติงาน เจ้าหน้าที่ภายในหน่วยงานขาดความตระหนักรู้

ส่วน วิศณุ สร้างวงศ์ใหม่ (2561) ณรงค์เวตย์ เรืองจวง (2561) แบ่งภัยคุกคามทางไซเบอร์ออกเป็นกลุ่มต่าง ๆ ได้ 4 กลุ่ม ได้แก่

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ และแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคามที่เรียกว่ามัลแวร์ ซึ่งถูกออกแบบมาเพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ที่ทำให้เกิดการขัดข้อง เสียหายกับระบบปฏิบัติการ นอกจากนี้สามารถส่งข้อความไม่พึงประสงค์ออกไปยังที่อื่น ขโมยข้อมูลสำคัญออกไป ตัวอย่างของโปรแกรมเหล่านี้ได้แก่ Virus, Worm, Trojan, Botnets

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์หลอกที่ถูกออกแบบมาให้เหมือนของจริง หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล์ เฟซบุ๊ก หรือเว็บไซต์ทางการเงิน แล้วดักจับรหัสของผู้ใช้งาน ทำให้ข้อมูลหรือบัญชีนั้น ๆ มีความเสี่ยงไม่ปลอดภัย

3. ภัยคุกคามจากการใช้เครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้น ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรงรวมถึงยังสามารถเป็นต้นตอของผลกระทบไปยังอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ของผู้อื่นด้วยเช่นกันโดยผู้ใช้เครือข่ายไร้สายอาจถูกโจมตีด้วยมัลแวร์ผ่านข้อบกพร่องของระบบปฏิบัติการ และถูกเปลี่ยนสถานะมาเป็นผู้โจมตีโดยการส่งต่อหรือแพร่กระจายมัลแวร์เหล่านี้ไปยังอุปกรณ์อื่นผ่านเครือข่ายไร้สายหรือบลูทูธ นอกจากนี้การใช้เครือข่ายไร้สายยังเปิดโอกาสให้ผู้ไม่ประสงค์ดีดักจับข้อมูลสำคัญหรือรหัสผ่านบนเครือข่ายไร้สายได้อีกด้วย

4. ภัยคุกคามที่เกิดจากการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตีหรือแฮกเกอร์ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐาน วิกฤตสถาบันการเงิน และองค์กรอื่น ๆ ของภาครัฐและภาคเอกชนในหลายประเทศอาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

สรุปการแบ่งประเภทภัยคุกคามทางไซเบอร์ได้ 4 ประเภท

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลดหรือได้มาจากสื่ออุปกรณ์อื่นเพื่อติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ และแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคามที่เรียกว่ามัลแวร์ เพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ ทำให้ขัดข้อง เสียหายต่อระบบปฏิบัติการ และสามารถส่งข้อความไม่พึงประสงค์ออกไปยังที่อื่น ขโมยข้อมูลสำคัญออกไป ตัวอย่างของโปรแกรมเหล่านี้ ได้แก่ Virus, Worm, Trojan, Botnets เป็นต้น

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์หลอกที่ออกแบบมาให้เหมือนของจริง หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล์ เฟซบุ๊ก หรือเว็บไซต์ทางการเงิน แล้วดักจับรหัสของผู้ใช้งานนั้นไป ทำให้ข้อมูลหรือบัญชีนั้น ๆ มีความเสี่ยงไม่ปลอดภัย

3. ภัยคุกคามจากการใช้เครือข่ายไร้สาย ซึ่งปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและไม่น่าเชื่อถือ ดังนั้น ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรงรวมถึงยังสามารถเป็นต้นตอของผลกระทบไปยังอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ของผู้อื่นด้วย โดยผู้ใช้เครือข่ายไร้สายอาจถูกโจมตีด้วยมัลแวร์ผ่านข้อบกพร่องของระบบปฏิบัติการ และถูกเปลี่ยนสถานะมาเป็นผู้โจมตีโดยการส่งต่อหรือแพร่กระจายมัลแวร์เหล่านี้ไปยังอุปกรณ์อื่นผ่านเครือข่ายไร้สายหรือบลูทูธ และการใช้เครือข่ายไร้สายยังทำให้เกิดความเสี่ยงจากผู้ไม่ประสงค์ดีดักจับข้อมูลสำคัญหรือรหัสผ่านบนเครือข่ายไร้สายได้อีกด้วย

4. ภัยคุกคามที่เกิดจากการโจมตีแบบเจาะจงเป้าหมาย ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตีหรือแฮกเกอร์ในประเทศต่าง ๆ จะโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐาน ของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้ จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามนี้เป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

2.2 แนวคิดการจัดการความเสี่ยง

2.2.1 ความหมายการจัดการความเสี่ยง

จากการศึกษาพบว่า อนาวิล แก้วสอาด และ ณัฐวี อุตกฤษฎ์ (2564) ได้ให้ความหมายของความเสี่ยง (Risk) คือความไม่แน่นอนที่มีโอกาสเกิดขึ้น เนื่องจากการมีข้อมูลไม่เพียงพอต่อการยืนยันผลลัพธ์ตามแผนการดำเนินงาน หรือวัตถุประสงค์ที่ตั้งไว้ รวมถึงปัจจัย หรือสิ่งที่อยู่นอกเหนือกจากการควบคุม (Project Management Institute [PMI], 2017) และนุกูล แดงภูมี (2563) ได้ให้ความหมายของความเสี่ยง (Risk) หมายถึง ความไม่แน่นอนที่เกิดขึ้นและส่งผลด้านลบต่อองค์กร อาทิ ความเสี่ยงจากความเปลี่ยนแปลงของสื่อใหม่ (New Media) ที่ส่งผลต่อยอดการจัดจำหน่ายสินค้าผ่านช่องทางและรูปแบบเดิม

ในขณะที่ สุฏิกา รักประสูติ และนงนิภา ตุลยานนท์ (2563) ได้ให้ความหมายของความเสี่ยง (Risk) หมายถึง ความเป็นไปได้ที่จะเกิดเหตุการณ์ ที่เป็นอุปสรรคต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงวัดได้จากผลกระทบที่ได้รับจากเหตุการณ์และโอกาสที่จะเกิดเหตุการณ์นั้น ส่วนคณะกรรมการบริหารความเสี่ยง สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (2561 อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) ได้ให้ความหมายของความเสี่ยง คือ ความไม่แน่นอนของเหตุการณ์ที่ไม่สามารถคาดการณ์ล่วงหน้าได้ จึงทำให้เสี่ยงเป็นโอกาสของเหตุการณ์ที่อาจเกิดขึ้นได้เสมอในอนาคตที่จะเกิดความผิดพลาดขึ้นทำให้เกิดความสูญเสีย ล้มเหลวหรือภยันตรายในหมู่สมาชิกหรือองค์ประกอบของหน่วยงานส่งผลกระทบต่ออนาคตทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายขององค์กรทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงินและการบริหาร

ส่วนสำนักงานคณะกรรมการการอุดมศึกษา (2554 อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) ได้กำหนดนิยามความเสี่ยงไว้ว่า ความเสี่ยงหมายถึง เหตุการณ์/การกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลัก ซึ่งเป็นนิยามความเสี่ยงที่ใกล้เคียงกับนิยามความเสี่ยงของกรอบการบริหารความเสี่ยงขององค์กร (Committee of Sponsoring Organisations of The Treadway Commission : COSO) โดยสำนักงานคณะกรรมการพัฒนาระบบราชการ

(2551 อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) ได้ให้นิยามความเสี่ยงไว้ว่า ความเสี่ยงเป็นเหตุการณ์ที่มีโอกาสเกิดขึ้นได้ในอนาคตและอาจส่งผลในด้านลบที่ไม่ต้องการและมีผลกระทบให้เกิดความเสียหาย หรือทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กร ดังนั้นการตัดสินใจกระทำการใด ๆ โดยไม่มีข้อมูลหรือไม่มีการวางแผนใด ๆ จึงกล่าวได้ว่าเป็นการเสี่ยงตัดสินใจในสภาวะของความเสี่ยง

เจนเนตร มณีนาค และ คณะ (2548 อ้างถึงใน วิจิตรา สีแดงก่ำ, 2562) กล่าวว่าความเสี่ยง หมายถึง นิยามได้เป็น 4 ความหมาย ดังนี้ (1) ความไม่แน่นอนว่าผลลัพธ์จะเกิดขึ้นตามที่ตั้งเป้าหมายไว้หรือไม่ (2) การกระทำหรือเหตุการณ์ที่อาจจะมีผลบั่นทอนความสามารถขององค์กรที่จะบรรลุเป้าประสงค์ที่ตั้งไว้ (3) การกระทำหรือเหตุการณ์ที่อาจเป็นไปได้ทั้งโอกาสหรือสิ่งคุกคาม และ (4) แนวโน้มหรือโอกาสที่จะเกิดความเสี่ยงและผลกระทบหากเหตุการณ์อุบัติขึ้นจริง

ในส่วนของสำนักงานศาลยุติธรรม (2565) ได้ให้ความหมายของความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นในอนาคต หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร

โดยสรุป ความเสี่ยงคือ ความไม่แน่นอนหรือโอกาสที่จะเหตุการณ์ที่ส่งผลทางลบ อาจจะนำมาสู่ความสูญเสีย ล้มเหลวหรือเกิดอันตรายแก่องค์กรหรือหน่วยงานทั้งในรูปแบบที่เป็นตัวเงินหรือไม่ใช่ตัวเงิน ความเสี่ยงเป็นสาเหตุอันนำไปสู่การดำเนินงานที่ไม่ประสบความสำเร็จ การบรรลุวัตถุประสงค์ การปฏิบัติงาน ด้านการเงินและการบริหาร

ในการศึกษานี้จะใช้คำว่า การจัดการความเสี่ยง (Risk Management)

จากการศึกษาพบว่า Olson และ Dolgui (2015 อ้างถึงใน ญาณิศา เผื่อนเพาะ, 2562) กล่าวว่า การจัดการความเสี่ยงขององค์กร (Enterprise Risk Management : ERM) เป็นแนวทางแบบบูรณาการเพื่อจัดการความเสี่ยงที่องค์กรเผชิญหน้าและแสวงหาผลประโยชน์สูงสุด ด้วยวิธีการรับมือกับความเสี่ยงการจัดการความเสี่ยงขององค์กร เป็นกระบวนการที่ส่งผลกระทบต่อการจัดการในองค์กร โดยใช้ในการกำหนดกลยุทธ์ทั่วทั้งองค์กร มีการออกแบบมาเพื่อระบุเหตุการณ์ที่อาจเกิดขึ้นแล้วส่งผลกระทบต่อกิจการ ต้องมีการบริหารความเสี่ยงให้อยู่ในความเสี่ยงที่ยอมรับได้เพื่อให้เกิดความเชื่อมั่น และส่งผลต่อการบรรลุวัตถุประสงค์ของกิจการ COSO (2004 อ้างถึงใน ญาณิศา เผื่อนเพาะ, 2562) การจัดการความเสี่ยงขององค์กรเป็นการพยายามเชื่อมโยงการบริหารความเสี่ยงกับ กลยุทธ์ธุรกิจ และการกำหนดเป้าหมายการเข้าสู่ความรับผิดชอบและการทำการตัดสินใจ

COSO ให้ความหมาย การจัดการความเสี่ยงองค์กร (Enterprise Risk Management: ERM) ไว้ว่าเป็นกระบวนการ ซึ่งเกิดจากคณะกรรมการ ผู้บริหารและพนักงานของ

องค์กรร่วมกันนำมาใช้ในการกำหนดกลยุทธ์ทั่วทั้งองค์กร และออกแบบไว้เพื่อระบุเหตุการณ์ที่เป็นไปได้ซึ่งอาจมีผลกระทบต่อองค์กร และจัดการความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้ เพื่อให้มีความมั่นใจอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ขององค์กร IIA (2004 อ้างถึงใน สุฏิกา รักประสูติ, 2558)

ในขณะ สุฏิกา รักประสูติ และนงนิภา ตุลยานนท์ (2563) ได้ให้ความหมาย การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ ประเมิน บริหาร และควบคุมเหตุการณ์หรือสถานการณ์ไม่พึงประสงค์ที่อาจจะเกิดขึ้น เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลว่าองค์กรสามารถบรรลุวัตถุประสงค์

ส่วน สุวันต์นา เสมอเนตร (2561) การจัดการความเสี่ยง (risk management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิด เหตุการณ์ความเสี่ยงลดลงหรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้

คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ (2556 กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) (2556 อ้างถึงใน วิจิตรา สีแดงก่ำ, 2562) ได้กล่าวว่า การจัดการความเสี่ยง คือ กระบวนการดำเนินงานขององค์กรที่เป็นระบบและต่อเนื่อง เพื่อช่วยให้องค์กรลดมูลเหตุของแต่ละโอกาสที่จะเกิด ความเสียหาย ให้ระดับของความเสียหายและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์ หรือเป้าหมายขององค์กรเป็นสำคัญ

กองทุนเพื่อการส่งเสริมและอนุรักษ์พลังงาน (2557 อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) (2556 อ้างถึงใน วิจิตรา สีแดงก่ำ, 2562) กล่าวว่า การจัดการความเสี่ยง (Risk Management) หมายถึง การกำหนดนโยบาย โครงสร้าง และกระบวนการเพื่อให้คณะกรรมการผู้บริหาร และบุคลากรนำไปปฏิบัติในการกำหนดกลยุทธ์และปฏิบัติงานทั่วทั้งองค์กรโดยกระบวนการจัดการความเสี่ยงจะสัมฤทธิ์ผลได้องค์กรจะต้องสามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้น ประเมินผลกระทบต่อองค์กร และกำหนดวิธีการจัดการที่เหมาะสมให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ ทั้งนี้เพื่อให้เกิดความเชื่อมั่นในระดับหนึ่งว่าผลการดำเนินงานตามภารกิจต่าง ๆ จะสามารถบรรลุวัตถุประสงค์ที่ได้กำหนดไว้

สำนักงานพัฒนาการวิจัยการเกษตร (องค์การมหาชน) (2556 อ้างถึงใน วิจิตรา สีแดงก่ำ, 2562) กล่าวว่า การจัดการความเสี่ยง หมายถึง กระบวนการในการระบุประเด็นความเสี่ยงการตอบสนอง/การจัดการความเสี่ยง เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่เหมาะสมยอมรับได้

องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (2562 อ้างถึงใน วิจิตรา สีแดงก่ำ, 2562) กล่าวว่า การจัดการความเสี่ยง คือ กระบวนการดำเนินงานขององค์กรที่เป็นระบบและ

ต่อเนื่อง เพื่อช่วยให้องค์กรลดมูลเหตุของแต่ละโอกาสที่จะเกิดความเสียหาย ให้ระดับของความเสียหายและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคต อยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุวัตถุประสงค์ หรือเป้าหมายขององค์กรเป็นสำคัญ

กรธัช อยู่สุข (2555 อ้างถึงใน วิจิตรา สีแดงก่ำ, 2562) กล่าวว่า การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ (Risk Identification) วิเคราะห์ (Risk Analysis) ประเมิน (Risk Assessment) ดูแลตรวจสอบและควบคุมความเสี่ยง (Risk Control) ที่สัมพันธ์กับกิจกรรม หน้าที่และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง

กลุ่มตรวจสอบภายใน, กระทรวงศึกษาธิการ (2561 อ้างถึงใน วิจิตรา สีแดงก่ำ, 2562) กล่าวว่า การจัดการความเสี่ยง หมายถึง กระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหารและบุคลากรในองค์กรเพื่อช่วยให้การกำหนดกลยุทธ์และดำเนินงาน ซึ่งกระบวนการบริหารความเสี่ยงได้รับการออกแบบไว้ให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กรและสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้

สำนักงานศาลยุติธรรม (2565) ได้ให้ความหมายของ การจัดการความเสี่ยง (Risk Management) คือ กระบวนการที่ใช้ในการบริหารจัดการปัจจัยเสี่ยงต่าง ๆ เพื่อให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite) การจัดการความเสี่ยงต้องมองปัญหาความเสี่ยงแบบองค์รวม ดังนั้น การจัดการความเสี่ยงที่เหมาะสมจะต้องอาศัยการมีส่วนร่วมจากผู้บริหารและผู้ปฏิบัติการในทุกระดับร่วมกัน พิจารณาทั้งประเด็นความเสี่ยงที่ยอมรับได้และระดับความเสี่ยงที่ยอมรับได้ เพื่อให้เกิดความเข้าใจและเห็นพ้องร่วมกันทั่วทั้งองค์กร จึงจะสามารถควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

สรุปได้ว่าการจัดการความเสี่ยง (Risk Management) คือ กระบวนการดำเนินงานหรือการกำหนดวิธีการจัดการที่เหมาะสมขององค์กร ขั้นตอนที่เป็นระบบและมีความต่อเนื่องอย่างเหมาะสม เพื่อลดเหตุของความเสี่ยงที่เกิดขึ้นหรือโอกาสของเหตุการณ์ที่เกิดในอนาคตให้อยู่ในระดับที่องค์กรยอมรับได้ มีการประเมิน ควบคุม และตรวจสอบอย่างเป็นระบบ เพื่อให้เกิดความเชื่อมั่นต่อองค์กร เป็นภาพลักษณ์ที่ดีขององค์กร

2.2.2 ประเภทของความเสี่ยง

จิรพร สุเมธีประสิทธิ์ และคณะ (2556 อ้างถึงใน ญาณิศา เผื่อนเพาะ, 2562) ได้กล่าวว่า เป้าหมายของความเสี่ยงมี 4 ประเภท คือ

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) เป็นความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนการดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสมกับปัจจัยภายในองค์กร และสภาพแวดล้อมภายนอก

2. ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) เป็นความเสี่ยงที่เกิดจากการดำเนินงานที่อาจเกิดข้อผิดพลาดขึ้นจากการบริหารงาน และระบบงานขององค์กร

3. ความเสี่ยงด้านการเงิน (Financial Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับด้านการเงินทั้งหมด เช่น สภาพคล่องทางการเงิน ความน่าเชื่อถือทางบัญชี อัตราแลกเปลี่ยนเงินตรา การรายงานทางการเงินที่ผิดปกติ เป็นต้น

4. ความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ (Compliance Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบและกฎหมาย โดยจากความเสี่ยงทั้ง 4 ประเภทนั้น องค์กรจะมุ่งเน้นให้ความสำคัญกับประสิทธิผลของการบริหารความเสี่ยงด้านการเงิน ความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ (Compliance Risk) มากกว่า ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) และความเสี่ยงด้านการปฏิบัติการ (Operational Risk) โดยศิระประภา ศรีวิโรจน์ และลักขณา ลุสวัสดิ์ (2559) ได้ระบุว่าความเสี่ยงด้านการเงินโดยเฉพาะในเรื่องของต้นทุน ที่ส่งผลกระทบต่อกำไร เป็นความเสี่ยงที่สัมพันธ์กับความอยู่รอดของธุรกิจ SMEs ผู้ประกอบการควรต้องตระหนักถึงความสำคัญพร้อมการพัฒนาองค์กรอย่างต่อเนื่องเพื่อความสามารถในการแข่งขันอย่างยั่งยืนในยุคการค้าเสรีอาเซียน ทั้งนี้ ผู้ประกอบการ SMEs ควรให้ความสำคัญกับความเสี่ยงด้านอื่น ๆ ด้วยเช่นกัน เพราะเมื่อความเสี่ยงประเภทใดประเภทหนึ่งเกิดขึ้นแล้ว ย่อมสามารถส่งผลกระทบไปสู่ทุกประเภทของความเสี่ยง และนำไปสู่ความล้มเหลวของกิจการได้ ทั้งนี้ในธุรกิจ SMEs เรามักจะพบความเสี่ยงอีกประเภทที่มีผลกระทบอย่างมาก คือ ความเสี่ยงด้านเทคโนโลยี เพราะในปัจจุบัน ธุรกิจ SMEs ขับเคลื่อนด้วยเทคโนโลยีและการใช้เทคโนโลยีท่ามกลางการเปลี่ยนแปลงในปัจจุบันเสมือนดาบ 2 คม หากรู้เท่าทันการใช้งานก็ส่งผลดี สร้างความเจริญเติบโตให้กิจการได้อย่างรวดเร็ว หากแต่ใช้อย่างขาดประสิทธิภาพย่อมเกิดผลเสียหายต่อธุรกิจได้

ส่วน สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (2563 อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) แบ่งประเภทของความเสี่ยงออกเป็น 4 ด้าน ดังนี้

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) คือ เหตุการณ์ทางลบที่เกี่ยวข้องกับกลยุทธ์ขององค์กร เช่น เป็นความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์/แผน

ดำเนินงานที่ไม่เหมาะสมไม่สอดคล้องกับ สภาพแวดล้อมที่เกี่ยวข้อง และการนำไปปฏิบัติไม่เหมาะสม หรือการวางแผนกลยุทธ์แล้วไม่สามารถนำไปปฏิบัติจริงได้

2. ความเสี่ยงด้านการดำเนินงาน (Operational Risk) คือ เหตุการณ์ทางลบที่เกิดจากความผิดพลาด ของบุคลากร กระบวนการปฏิบัติงาน หรือระบบงานต่าง ๆ ซึ่งส่งผลกระทบต่อการดำเนินงานขององค์กร รวมไปถึงเหตุการณ์ทางลบที่เกิดจากปัจจัยภายนอกองค์กรด้วย เช่น ภัยธรรมชาติ หรือเหตุจลาจลทางการเมือง

3. ความเสี่ยงด้านการรายงาน (Reporting Risk) คือ ความผิดพลาดของรายงานประเภทต่าง ๆ ที่ใช้ในองค์กร เช่น งบการเงิน รายงานยอดขาย รายงานต้นทุนการผลิต เป็นต้น ความเสี่ยงด้านการรายงานอาจจะอยู่ในรูปของข้อมูลไม่ถูกต้อง ไม่น่าเชื่อถือ ไม่สอดคล้องกับความต้องการของผู้ใช้ข้อมูล รวมไปถึงการรายงาน ไม่ทันเวลาด้วย

4. ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ หรือข้อกำหนดที่เกี่ยวข้อง (Compliance Risk) ความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบ หรือข้อกำหนดที่เกี่ยวข้อง คือ การดำเนินงานของธุรกิจไม่เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับต่าง ๆ ที่เกี่ยวข้องซึ่งอาจจะเป็นทั้งข้อกำหนดจากภายนอกองค์กร เช่น กฎหมายต่าง ๆ หรือข้อกำหนดภายในองค์กร เช่น นโยบาย แนวทางการปฏิบัติงาน หรือคู่มือการปฏิบัติงาน เป็นต้น

โดยสำนักงานศาลยุติธรรม แบ่งประเภทของความเสี่ยงประกอบด้วย 4 ประเภท ดังนี้

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงที่ส่งผลโดยตรงต่อการบรรลุเป้าหมายและพันธกิจขององค์กรในภาพรวม

2. ความเสี่ยงด้านการดำเนินงาน (Operation Risk) หมายถึง ความเสี่ยงที่เกี่ยวข้องกับประสิทธิภาพ หรือประสิทธิผลของการปฏิบัติงาน เป็นความเสี่ยงที่มักเกิดจากระบบงานภายในองค์กรกระบวนการ เทคโนโลยี นวัตกรรม บุคลากร ข้อมูล ซึ่งส่งผลต่อประสิทธิภาพ หรือประสิทธิผลในการดำเนินงาน

3. ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงเกี่ยวกับการบริหารงบประมาณและการเงิน อันเนื่องมาจากขาดการจัดการข้อมูล การวิเคราะห์ การวางแผนการควบคุม และการจัดทำรายงาน เพื่อนำมาใช้ในการบริหารงบประมาณและการเงิน

4. ความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบ (Compliance Risk) หมายถึง ความเสี่ยงเกี่ยวกับการปฏิบัติงานที่อาจขัดต่อกฎหมาย กฎ ระเบียบ อันเนื่องมาจากความไม่ชัดเจนไม่ทันสมัย หรือความไม่ครอบคลุมของกฎหมาย กฎ ระเบียบ เหล่านั้น

ในการศึกษาได้แบ่งประเภทของความเสี่ยงประกอบด้วย 4 ประเภทดังนี้

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) เป็นความเสี่ยงที่ส่งผลต่อการบรรลุเป้าหมายและพันธกิจที่องค์กรได้กำหนดไว้

2. ความเสี่ยงด้านการดำเนินงาน (Operation Risk) เป็นความเสี่ยงที่เกิดจากกระบวนการ เทคโนโลยี บุคลากร ข้อมูล ซึ่งส่งผลกระทบต่อประสิทธิภาพและประสิทธิผลการดำเนินงานขององค์กร

3. ความเสี่ยงด้านการเงิน (Financial Risk) เป็นความเสี่ยงที่เกิดจากขาดการจัดการข้อมูล การวิเคราะห์ การวางแผน การควบคุม และจัดทำรายงาน ในการบริหารงบประมาณและการเงินให้ถูกต้อง

4. ความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบ (Compliance Risk) เป็นความเสี่ยงที่เกิดจากการปฏิบัติงานที่ขัดต่อกฎหมาย กฎ ระเบียบ ซึ่งอาจจะเป็นทั้งกฎระเบียบทั้งภายนอกองค์กรหรือภายในองค์กร

2.2.3 องค์ประกอบของการจัดการความเสี่ยง

จากการศึกษาพบว่า องค์ประกอบของการจัดการความเสี่ยง ERM (Enterprise Risk Management) ประกอบด้วยองค์ประกอบ 8 ประการ ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน และ การจัดการความเสี่ยงมาบูรณาการของทั้ง 3 มิติเข้าด้วยกัน ดังนี้ (The Committee of Sponsoring Organizations' (COSO) (2017 อ้างถึงในกมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564)

1. สภาพแวดล้อมภายในองค์กร (Internal Environment) สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญในการกำหนดกรอบการจัดการความเสี่ยง ประกอบด้วยปัจจัยหลายประการ เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงานบุคลากร กระบวนการทำงาน ระบบสารสนเทศ ระเบียบ เป็นต้น สภาพแวดล้อมภายในองค์กรประกอบเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการจัดการความเสี่ยงขององค์กร

2. การกำหนดวัตถุประสงค์ (Objective Setting) องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการจัดการความเสี่ยงให้มีความสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการจัดการความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม โดยทั่วไปวัตถุประสงค์และกลยุทธ์ควรได้รับการบันทึกเป็นลายลักษณ์อักษรและสามารถพิจารณาได้ในด้านต่างๆ ดังนี้ (กลุ่มตรวจสอบภายในระดับกระทรวง , กระทรวงศึกษาธิการ)

- ด้านกลยุทธ์ เกี่ยวข้องกับเป้าหมายและพันธกิจในภาพรวมขององค์กร
- ด้านการปฏิบัติงาน เกี่ยวข้องกับประสิทธิภาพ ผลการปฏิบัติงาน และความสามารถในการทำกำไร
- ด้านการรายงาน เกี่ยวข้องกับการรายงานทั้งภายในและภายนอกองค์กร

- ด้านการปฏิบัติตามกฎ ระเบียบเกี่ยวข้องกับการปฏิบัติตามกฎหมายและกฎระเบียบต่าง ๆ

การกำหนดวัตถุประสงค์ที่ชัดเจนจะช่วยระบุและวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นได้อย่างครบถ้วน โดยอาจใช้หลักแบบ SMART ประกอบด้วย

Specific มีการกำหนดเป้าหมายที่ชัดเจน

Measurable สามารถวัดผลหรือประเมินผลได้

Attainable สามารถปฏิบัติให้บรรลุผลได้

Relevant มีความสอดคล้องกับวัตถุประสงค์และเป้าหมายขององค์กร

Timely มีกรอบระยะเวลาที่แน่นอน

3. การบ่งชี้เหตุการณ์ (Event Identification) เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งในส่วนของปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร เช่น นโยบายบริหารงานบุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบ กฎหมาย ระบบบัญชี ภาษีอากร ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้น เพื่อให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นได้เป็นอย่างดี

การบ่งชี้เหตุการณ์หรือระบุความเสี่ยงควร ประกอบด้วยความเสี่ยงที่ครอบคลุมในด้านต่าง ๆ ดังนี้

- ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)
- ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)
- ความเสี่ยงด้านนโยบาย/กฎหมาย/ระเบียบ/ข้อบังคับ (Policy and Compliance Risk)
- ความเสี่ยงด้านการเงิน (Financial Risk)
- ความเสี่ยงด้านสุขภาพ (Healthy Risk)
- ความเสี่ยงด้านสิ่งแวดล้อม (Environment Risk)
- ความเสี่ยงด้านชุมชน (Community Risk)
- ความเสี่ยงด้านภาพลักษณ์และชื่อเสียง (Image and Reputation Risk)

4. การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงเป็นการจำแนกและพิจารณาจัดลำดับความสำคัญความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยสามารถประเมินความเสี่ยงได้ทั้งจากปัจจัยความเสี่ยงภายนอกและปัจจัยความเสี่ยงภายในองค์กรการประเมินความเสี่ยงจำแนกเป็น 2 มิติ มหาวิทยาลัยราชภัฏวไลอลงกร ในพระบรมราชูปถัมภ์(2557 อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) คือ

4.1. โอกาส/ความถี่ที่จะเกิด หมายถึง ความน่าจะเป็นที่จะเกิดเหตุการณ์ที่นำมาพิจารณาเกิดขึ้นมากน้อยเพียงใด ซึ่งจะมีการพิจารณาหาระดับของโอกาสที่จะเกิด

4.2 ผลกระทบ (ความรุนแรง) ที่เกิดจากเหตุการณ์ที่เกิดขึ้น หรือคาดคะเนว่าจะเกิดเหตุการณ์ โดยมีเกณฑ์มาตรฐานระดับความเสี่ยงจากการคำนวณ คือ ระดับความเสี่ยง = โอกาสที่จะเกิดเหตุการณ์ x ผลกระทบต่อเหตุการณ์ ซึ่งแบ่งระดับความเสี่ยงได้เป็น 4 ระดับ ศรีวรรณ์ ทาปัญญา (ม.ป.ป. อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) ดังนี้

ตาราง 1 ระดับความเสี่ยง

ลำดับคะแนน	ระดับความเสี่ยง	แทนด้วยแทบสี	ความหมาย
22-25	สูงมาก		ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
16-21	สูง		ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
5-15	ปานกลาง		ระดับที่พอยอมรับได้แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
1-4	ต่ำ		ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยงไม่ต้องมีการจัดการเพิ่มเติม

5. การจัดการความเสี่ยง หรือ การตอบสนองความเสี่ยง (Risk Response) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (2561 อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) ได้กล่าวว่า เป็นการดำเนินการหลังจากที่องค์กรสามารถบ่งชี้ความเสี่ยงขององค์กร และประเมินความสำคัญของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงมาดำเนินการตอบสนองด้วยวิธีการที่เหมาะสม เพื่อลดความสูญเสียหรือโอกาสที่จะเกิดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้ หลักการตอบสนองความเสี่ยง องค์การพิพิธภัณฑ์วิทยาศาสตร์แห่งชาติ (2564 อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564) คือ

5.1 Take การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับให้มีความเสี่ยงเนื่องจากค่าใช้จ่ายในการจัดการหรือสร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้ แต่ควรมีมาตรการติดตามและดูแล เช่น การกำหนดระดับของผลกระทบที่ยอมรับได้ เตรียมแผนการตั้งรับจัดการความเสี่ยง

5.2 Treat การลด/การควบคุมความเสี่ยง (Risk Reduction/Control) การออกแบบระบบควบคุม การแก้ไขปรับปรุงการทำงานเพื่อป้องกันหรือจำกัดผลกระทบและโอกาสเกิดความเสียหาย เช่น ติดตั้งอุปกรณ์ความปลอดภัย ฝึกอบรมเพื่อพัฒนาทักษะ วางมาตรการเชิงรุก เป็นต้น

5.3 Terminate การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การหยุดหรือเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น งดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบการทำงาน ลดขอบเขตการดำเนินการ เป็นต้น

5.4 Transfer การกระจาย/โอนความเสี่ยง (Risk sharing/spreading) การกระจายทรัพย์สินหรือกระบวนการต่าง ๆ เพื่อลดความเสี่ยงจากการสูญเสีย เช่น การประกันทรัพย์สินเพื่อโอนความเสี่ยงไปยังบริษัทประกัน การจ้างบริษัทภายนอกให้ทำงานบางส่วนแทน การทำสำเนาเอกสารหลาย ๆ ชุด การกระจายที่เก็บทรัพย์สินมีค่า เป็นต้น

6. กิจกรรมการควบคุม (Control Activities) การกำหนดกิจกรรมและการปฏิบัติต่าง ๆ ที่กระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุตามวัตถุประสงค์และเป้าหมายขององค์กร เช่น การกำหนดกระบวนการปฏิบัติงานที่เกี่ยวข้องกับ การจัดการความเสี่ยงให้กับบุคลากรภายในองค์กรเพื่อเป็นการสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้องและเป็นไปตามเป้าหมายที่กำหนด

7. สารสนเทศและการสื่อสาร (Information and Communication) องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงให้เป็นไปตามกรอบ และขั้นตอนการปฏิบัติที่องค์กรกำหนด และเพื่อช่วยให้บุคลากรที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ การสื่อสารอย่างมีประสิทธิผลรวมถึงการแลกเปลี่ยนข้อมูลกับบุคคลภายนอกองค์กร เช่น เจ้าหน้าที่ของหน่วยงานอื่น ๆ ผู้จัดหาสินค้า ผู้ให้บริการ ผู้กำกับดูแลและประชาชน

8. การติดตามประเมินผล (Monitoring) องค์กรจะต้องมีการติดตามผลเพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่ โดยมีประเด็นสำคัญของการติดตามผล ได้แก่

- การติดตามผลเพื่อให้มั่นใจได้ว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม และการบริหารความเสี่ยงได้นำไปประยุกต์ใช้ในทุกระดับขององค์กร

- ความเสี่ยงทั้งหมดที่มีผลกระทบสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กรได้รับการรายงานต่อผู้บริหารที่รับผิดชอบ การติดตามการบริหารความเสี่ยงสามารถทำได้ 2 ลักษณะคือ การติดตามอย่างต่อเนื่องและการติดตามเป็นรายครั้ง การติดตามอย่างต่อเนื่องเป็นการดำเนินการอย่างสม่ำเสมอ เพื่อให้สามารถตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงทีและถือเป็นส่วนหนึ่งของการปฏิบัติงาน ส่วนการติดตามรายครั้งเป็นการดำเนินการภายหลังจากเกิดเหตุการณ์ ดังนั้นปัญหาที่เกิดขึ้นจะได้รับการแก้ไขอย่างรวดเร็วหากองค์กรมีการติดตามอย่าง

ต่อเนื่อง นอกจากนี้องค์กรควรมีการจัดทำรายงานความเสี่ยงเพื่อให้การติดตามการบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล สำนักงานส่งเสริมการจัดประชุมและนิทรรศการ (ม.ป.ป. อ้างถึงใน กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ์, 2564)

สรุปได้ว่า การจัดการความเสี่ยงขององค์กร ประกอบด้วย 8 องค์ประกอบ การจัดการความเสี่ยงที่มีความเกี่ยวข้องสัมพันธ์ซึ่งกันและกัน โดยองค์ประกอบเหล่านี้ได้มาจากการบริหารดำเนินการองค์กรและนำมาผสมผสานเข้ากับกระบวนการบริหารจัดการ

2.3 แนวคิดความมั่นคงปลอดภัยทางไซเบอร์

2.3.1 ความหมายความมั่นคงปลอดภัยทางไซเบอร์

จากการศึกษาพบว่า พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (2562) ความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ขณะที่ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ สถาบันเทคโนโลยีป้องกันประเทศ (2559) กล่าวว่า ความมั่นคงปลอดภัยไซเบอร์ คือ การสร้างความมั่นคงปลอดภัยในระบบเครือข่าย (Network) และข้อมูล (Data) การที่จะบรรลุวัตถุประสงค์ดังกล่าว จะต้องใช้ทั้งมาตรการทางเทคโนโลยี มาตรการทางกฎหมาย (Statutory Regulation) รวมถึงการกากับดูแลตนเอง (Self-Regulation) และการกากับดูแลร่วมกัน (Co-Regulation) ของทั้ง 3 ฝ่าย ผู้ที่ได้รับผลกระทบจากการโจมตีทางไซเบอร์ ได้แก่ รัฐ หน่วยงานภาคเอกชน และประชาชน

ส่วนสำนักงานราชบัณฑิตยสภา คณะกรรมการจัดทำพจนานุกรมศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ (2562 อ้างถึงใน สุภาพร พรมโส, ปราลี มณีรัตน์ และประสงค์ ประณีตพลกรัง, 2564) ให้นิยามของ ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ว่า คือ ภาวะที่เครือข่าย ระบบคอมพิวเตอร์ โปรแกรม และข้อมูล พ้นจากภัยคุกคาม มีลักษณะสำคัญ 3 ประการ คือ คงความลับ คงความถูกต้องครบถ้วน และคงความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ต้องอาศัยบุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม โดย Bodeau and Graubart (2017 อ้างถึงใน อนาวิล แก้วสะอาด และณัฐวี อุตกฤษฎ์, 2564) ให้ความหมายของความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) การลดความเสี่ยงให้กับโครงสร้างพื้นฐานทั้งทางกายภาพและทางไซเบอร์ มุ่งเน้นไปที่การบริหารจัดการ การบุกรุก การโจมตี รวมทั้งภัยธรรมชาติและภัยที่มนุษย์ได้ก่อขึ้น ทั้งตั้งใจและไม่ได้ตั้งใจ เช่น การก่อการร้าย หรือการโจมตีทางไซเบอร์

ขณะที่ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ความมั่นคงปลอดภัยทางไซเบอร์หมายถึง วิธีการ มาตรการ หรือการดำเนินการใด ๆ เพื่อป้องกัน รับมือ บรรเทา และ

ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของอุปกรณ์และข้อมูลภายในระบบสารสนเทศ ซึ่งหากการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีความอ่อนแออาจทำให้ผู้ประสงค์ร้ายสามารถสร้างความเสียหายต่อตัวผู้ใช้งานและข้อมูลส่วนบุคคลของผู้ใช้งานได้ สพธอ. (2564 อ้างถึงใน เมธาพร ธรรมศิริ และศิรภัสสค์ วงศ์ทองดี, 2565)

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) สรุปได้ว่า ความมั่นคงปลอดภัยทางไซเบอร์หมายถึง วิธีการ มาตรการ หรือการดำเนินการใด ๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ การรักษาความครบถ้วน และสภาพพร้อมใช้งาน ของอุปกรณ์และข้อมูลภายในระบบสารสนเทศ

2.3.2 โครงสร้างหลักของกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ โดยมี Framework Core ดังนี้

1. กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ อาทิ การจัดการทรัพย์สิน การควบคุมการเข้าถึง

2. กลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค และหรือกิจกรรมในการบริหารจัดการ

3. ข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทาง และแนวปฏิบัติที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม

องค์ประกอบ Framework Core Functions แบ่งย่อยออกเป็นกรอบงานหลัก 5 functions ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ได้แก่

1. Identify พัฒนาความเข้าใจขององค์กรเกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ในด้าน คน สินทรัพย์ ข้อมูล และความสามารถ กิจกรรมในฟังก์ชัน Identify เป็นพื้นฐานในการใช้กรอบอย่างมีประสิทธิภาพ ให้เข้าใจถึงบริบทของการดำเนินธุรกิจ ทรัพยากรที่สนับสนุนฟังก์ชันที่สำคัญ และความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง เพื่อให้องค์กรสามารถมุ่งเน้นและจัดลำดับความสำคัญ ให้สอดคล้องกับกลยุทธ์การบริหารความเสี่ยงและความต้องการทางธุรกิจ ได้แก่ การบริหารสินทรัพย์ สิ่งแวดล้อมทางธุรกิจ ธรรมาภิบาล การประเมินความเสี่ยง และกลยุทธ์การบริหารความเสี่ยง

2. Protect พัฒนาและจัดทำการป้องกันที่เหมาะสมเพื่อให้แน่ใจว่าหน่วยงานที่สำคัญได้รับการปกป้อง ฟังก์ชัน Protect ช่วยเพิ่มความสามารถในการจำกัดหรือยับยั้งผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ได้แก่ การระบุตัวตนและการควบคุมการเข้าถึง การสร้างความตระหนักและการฝึกอบรม การรักษาความปลอดภัยของ

ข้อมูล กระบวนการและขั้นตอนการปกป้องสารสนเทศ การบำรุงรักษา และเทคโนโลยีด้านการป้องกัน

3. Detect พัฒนาและจัดทำกิจกรรมที่เหมาะสมในการระบุเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นฟังก์ชัน Detect ช่วยให้สามารถตรวจพบเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ได้ทันท่วงที ได้แก่ เหตุการณ์ความผิดปกติ การเฝ้าระวังอย่างต่อเนื่อง และกระบวนการตรวจจับ

4. Respond พัฒนาและจัดทำกิจกรรมที่เหมาะสม เพื่อดำเนินการเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ฟังก์ชัน Respond ช่วยให้สามารถยับยั้งผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ได้แก่ การวางแผนรับมือ การสื่อสาร การวิเคราะห์ การบรรเทาความเสียหาย และการปรับปรุง

5. Recover พัฒนาและจัดทำกิจกรรมที่เหมาะสมเพื่อวางแผน เตรียมรับมือและกู้คืนการดำเนินงานหรือการให้บริการที่เสียหายจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ฟังก์ชัน Recover ช่วยให้สามารถกู้คืนการปฏิบัติงานให้กลับเป็นปกติได้ทันท่วงที เพื่อลดผลกระทบที่เกิดจากเหตุการณ์ภัยคุกคามไซเบอร์ ได้แก่ การวางแผนการกู้คืน การปรับปรุง การสื่อสาร NIST (2014 อ้างถึงใน ปริญญา หอมอเนก และACIS Research LAB, 2557; 2014 อ้างถึงใน วิลาส วิถีไพร, 2561)

2.4 แนวคิดการบริการสาธารณะและการให้บริการสาธารณะหน่วยงานศาลยุติธรรม

2.4.1 ความหมายของการบริการสาธารณะ

การบริการสาธารณะ มีขึ้นตั้งแต่มนุษย์เริ่มมาอยู่รวมกันเป็นชุมชนต่อมาพัฒนาเป็นเมืองหรือประเทศ โดยมีการบริการสาธารณะที่แตกต่างกัน ตามความเหมาะสมของบริบทประเทศนั้น ซึ่งการบริการสาธารณะที่มีอยู่ส่วนใหญ่มาจากฝ่ายปกครองหรือรัฐบาล และถือได้ว่าเป็นหน้าที่ที่สำคัญยิ่งในการบริหารงานของภาครัฐที่จะต้องส่งต่อบริการสาธารณะให้กับประชาชน โดย ทิพรัตน์ วัชระ (2554 อ้างถึงใน ชวนพิศ เงินฉลาด, 2561) ได้ให้ความหมาย การบริการสาธารณะ หมายถึง การที่บุคคล กลุ่มบุคคล หรือหน่วยงานที่มีหน้าที่เกี่ยวกับการบริการสาธารณะ ซึ่งอาจจะเป็นภาครัฐหรือเอกชน ทำหน้าที่ให้การบริการสาธารณะแก่ประชาชน เพื่อตอบสนองความต้องการของประชาชนส่วนใหญ่ โดยระบบของการบริการสาธารณะจะประกอบไปด้วย 1. ที่ทำการและผู้ให้บริการ 2. ทรัพยากร 3. กระบวนการ 4. บริการ 5. ช่องทางการบริการ 6. ผลลัพธ์ที่มีต่อผู้รับบริการ ซึ่งสอดคล้องกับแนวคิดของ พิทยา บวรวัฒนา (2549 อ้างถึงใน ชวนพิศ เงินฉลาด, 2561) ที่เห็นว่าการบริการสาธารณะเป็นกิจกรรมที่อยู่ในความอำนวยการหรือความควบคุมของฝ่ายปกครอง มีวัตถุประสงค์เพื่อสนองความต้องการ ส่วนร่วมของประชาชน ตลอดจนต้องมีความเท่าเทียมในการบริการ โดยการบริการสาธารณะสามารถปรับปรุงหรือ

เปลี่ยนแปลงวิธีการดำเนินการให้เหมาะสมกับบริบทที่เปลี่ยนไป ซึ่งการบริการสาธารณะจะต้องดำเนินอย่างต่อเนื่อง ไม่หยุดชะงักเพื่อไม่ให้เกิดผลกระทบกับประชาชน

ขณะที่ เนตรชนก สูนาสวน, อำนวย บุญรัตนไมตรี, ชัยยงค์ พรหมวงค์ และอนันต์ เตียวต๋อย 2565 การบริการสาธารณะ (Public Service) หมายถึง กิจกรรมที่รัฐจัดทำขึ้นเพื่อตอบสนองความต้องการของประชาชนโดยส่วนรวม ในสิ่งที่จำเป็นในการดำรงชีวิตหรือเพื่อส่งเสริมชีวิตความเป็นอยู่ให้ได้รับความสะดวกสบาย โดยถือว่าเป็นภารกิจที่รัฐจะต้องจัดทำ (สุเชาวน์ มีหนองหว้า และคณะ, 2563) ได้กล่าวว่า ในการให้บริการสาธารณะนั้น ต้องมีเป้าหมายเพื่อผลประโยชน์และเพื่อตอบสนองความต้องการของประชาชน หน่วยงานหรือองค์กรต้องเปิดโอกาสให้ประชาชนเข้ามามีส่วนร่วมบริหารจัดการโครงการด้วย (กุลธน ธนาพงศธร, 2537) ได้กล่าวไว้ว่า บริการสาธารณะเป็นสิ่งที่เกิดขึ้นได้เฉพาะ เมื่อมีความต้องการของส่วนรวมหรือมีผลประโยชน์สาธารณะที่จะต้องดำเนินการและ การบริการสาธารณะเป็นการตอบสนองความต้องการของชุมชนและประชาชนที่จะได้รับบริการในเรื่องที่เอกชนหรือวิสาหกิจเอกชนไม่อาจตอบสนองได้ ไม่ว่าจะเป็นการจัดให้มีบริการสาธารณะ ในด้านให้ความคุ้มครองความปลอดภัยในชีวิตและทรัพย์สิน

ส่วน นราธิป ศรีราม (2557, อ้างถึงใน เขมิกา ทองเรือง และพัณณกร สอนไว, 2565) ได้กล่าวว่าการบริการสาธารณะ หมายถึง การบริการหรือกิจกรรมที่รัฐจัดทำขึ้นเพื่อประโยชน์สาธารณะหรือเพื่อตอบสนองความต้องการของส่วนรวม โดยเป็นกิจการที่อยู่ในความอำนวยการหรืออยู่ในความควบคุมของฝ่ายปกครองที่จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อสนองความต้องการส่วนรวมของประชาชน อันเป็นการพัฒนาคุณภาพชีวิตที่ดีให้แก่ประชาชนและสร้างการพัฒนาทั้งด้านเศรษฐกิจและสังคมให้กับท้องถิ่น รวมถึงการพัฒนาประเทศชาติในภาพรวม โดยมีหลักการที่เป็นประเด็นสำคัญในการจัดบริการสาธารณะคือ การจัดบริการสาธารณะต้องดำเนินการเพื่อก่อให้เกิดประโยชน์แก่ส่วนรวม สามารถตอบสนองความต้องการของท้องถิ่นมีความเสมอภาค ความต่อเนื่อง และความโปร่งใสในการให้บริการ

ประยูรณ์ กาญจนดุล (2547, อ้างถึงใน สถาพร วิชัยรัมย์ ธัญญรัตน์ พุฑฒิพงษ์ชัยชาญ ภัทรนันท์ เกิดในหล้า และจุฑารัตน์ จัตุกูล, 2562) ได้ให้ความหมายว่า การบริการสาธารณะหมายถึง กิจกรรมที่ฝ่ายปกครองจัดทำขึ้น เพื่อสนองต่อความต้องการส่วนรวมของประชาชนและเพื่อให้ประชาชนได้รับประโยชน์ตอบแทนมากที่สุด รวมถึงประชาชนทุกคนต้องได้รับโอกาสในการรับบริการอย่างเสมอภาคเท่าเทียมกัน

นนทวัฒน์ บรมนันท์ (2552, อ้างถึงใน สถาพร วิชัยรัมย์ ธัญญรัตน์ พุฑฒิพงษ์ชัยชาญ ภัทรนันท์ เกิดในหล้า และจุฑารัตน์ จัตุกูล, 2562) ได้อธิบายว่า การบริการสาธารณะเป็นกิจกรรม (Activity) ของฝ่ายปกครองที่จัดทำขึ้นเพื่อประโยชน์สาธารณะ ประกอบด้วยการดำเนินกิจกรรม

ที่เกี่ยวข้องกับนิติบุคคลมหาชนเป็นผู้ประกอบกิจกรรมด้วยตนเอง และกิจกรรมดังกล่าวมีวัตถุประสงค์เพื่อประโยชน์สาธารณะและตอบสนองความต้องการของประชาชน

Gaston Jeze (1928, อ้างถึงใน ศิริพงษ์ ปานจันทร์, 2554) กล่าวว่า การบริการสาธารณะหมายถึง กิจกรรมที่เกิดขึ้นได้เฉพาะเมื่อมีความต้องการของส่วนรวมหรือมีผลประโยชน์สาธารณะที่ต้องดำเนินการและผู้ปกครองของประเทศนั้นได้ตัดสินใจดำเนินการในขณะนั้นโดยวิธีการของการบริการสาธารณะจากความหมายดังกล่าวอธิบายได้ว่า การให้บริการสาธารณะเป็นหน้าที่ของรัฐซึ่งกระทำโดยฝ่ายปกครองคือเป็นองค์กรหรือเจ้าหน้าที่รัฐที่มีอำนาจหน้าที่ในการตระเตรียมการและปฏิบัติให้เป็นไปตามนโยบายที่ฝ่ายบริหารกำหนดไว้เพื่อตอบสนองความต้องการของประชาชน

สรุปได้ว่า การบริการสาธารณะ เป็นกิจกรรมที่หน่วยงานที่มีอำนาจหน้าที่ที่เกี่ยวข้องที่อาจเป็นหน่วยงานของรัฐหรือเอกชนเป็นผู้ดำเนินการให้แก่ประชาชนผู้มารับบริการ ทั้งนี้โดยมีเป้าเหมาย ที่สำคัญคือ การให้บริการที่ตอบสนองความต้องการของประชาชนอย่างทั่วถึงและเสมอภาค โดยหน่วยงานที่ให้บริการจะต้องส่งมอบบริการแก่ประชาชนด้วยจิตสำนึกที่ดีในการให้บริการ และมีการนำผลสะท้อนกลับจากประชาชนในฐานะผู้มาใช้บริการ เพื่อนำมาปรับปรุงพัฒนาการให้บริการให้มีประสิทธิภาพ ไม่ว่าจะเกี่ยวข้องกับข้อร้องเรียน ข้อเสนอแนะต่าง ๆ ทั้งนี้อาจกล่าวได้ว่า การบริการสาธารณะจำเป็นต้องคำนึงถึงคุณภาพ และประสิทธิภาพของการให้บริการ โดยอาศัยเทคนิควิธีการที่หมาะสมต่อกลุ่มเป้าหมายที่ให้บริการ ช่วงเวลาและสถานที่การให้บริการ

2.4.2 การบริการสาธารณะของศาลยุติธรรม

การให้บริการของศาลถือเป็นภารกิจด้านการยุติธรรมที่รัฐต้องจัดทำเพื่ออำนวยความยุติธรรมให้กับประชาชนทุกคนอย่างเสมอภาค และบริหารจัดการบริการของศาลให้มีประสิทธิภาพ และปรับปรุงเปลี่ยนแปลงบริการให้เหมาะสมกับสถานการณ์ และทันกับความต้องการของประชาชน ซึ่งเป็นภารกิจที่สอดคล้องกับหลักการจัดทำบริการสาธารณะ ทั้ง 3 ประการ ศาลยุติธรรมได้ให้ความสำคัญกับการบริหารจัดการบริการของศาล เพื่อให้ประชาชนผู้มาใช้บริการสามารถเข้าถึงศาลได้อย่างทั่วถึง และส่งเสริมความรู้ความเข้าใจเกี่ยวกับบทบาทและหน้าที่ของศาลยุติธรรม โดยในปัจจุบันศาลยุติธรรมได้มีการจัดทำโครงการเผยแพร่ให้ความรู้เกี่ยวกับบทบาท หน้าที่และการดำเนินงานของศาลหลายโครงการ เช่น โครงการศาลยุติธรรมเผยแพร่ความรู้ทางกฎหมายแก่ประชาชน โครงการเสริมสร้างทักษะการต้อนรับประชาชนและการประชาสัมพันธ์โครงการพัฒนาระบบการสื่อสารประชาสัมพันธ์ของศาลยุติธรรมเพื่อบริการประชาชนและสังคม และโครงการอนุรักษ์พิพิธภัณฑ์ศาลไทยและการจัดทำจดหมายเหตุ เป็นต้น นอกจากนี้แล้ว ศาลยุติธรรมยังได้ให้ความสำคัญกับการพัฒนาการบริหารจัดการบริการของศาล

ซึ่งเป็นการเพิ่มโอกาส การเข้าถึงบริการให้กับประชาชนและผู้มาใช้บริการ ส่งเสริมความรู้ความเข้าใจการดำเนินงานของศาล และความสัมพันธ์ระหว่างศาลและประชาชน

2.4.3 นโยบายประธานศาลฎีกา

สำนักงานศาลยุติธรรมเป็นองค์กรอิสระ ปัจจุบันสำนักงานศาลยุติธรรม มี นายโชติวัฒน์ เหลืองประเสริฐ ดำรงตำแหน่งประธานศาลฎีกาคนที่ 48 โดยมีนโยบายในการบริหารสำนักงานศาลยุติธรรม ดังนี้ รักศาล ร่วมใจ รับใช้ประชาชน

1. รักศาล เสริมสร้างจิตสำนึกให้บุคลากรในองค์กรศาลยุติธรรม ทั้งข้าราชการตุลาการ ข้าราชการศาลยุติธรรม พนักงานราชการ เจ้าหน้าที่ ผู้พิพากษาสมทบ ผู้ประนีประนอม ตลอดจนบุคคลภายนอกที่เข้าร่วมงานกับศาลยุติธรรม มีความรักความผูกพันในองค์กร โดยมุ่งเน้นการสร้างความสามัคคี การทำงานเป็นทีม การสร้างทัศนคติและสภาวะแวดล้อมที่ดีในการทำงาน รวมทั้งมุ่งพัฒนาคุณภาพชีวิตของบุคลากรทุกฝ่ายเพื่อเพิ่มประสิทธิภาพการทำงานของศาลยุติธรรมในการให้บริการประชาชน

2. ร่วมใจ มุ่งเน้นให้บุคลากรในองค์กรศาลยุติธรรมร่วมมือร่วมใจปฏิบัติหน้าที่อย่างมุ่งมั่นตั้งใจ โปร่งใส มีความรับผิดชอบ มีจิตใจบริการ พร้อมอำนวยความยุติธรรมให้แก่ประชาชนด้วยความรวดเร็ว เป็นธรรม อย่างทั่วถึงและมีมาตรฐานเดียวกันบนระบบการทำงานที่เน้นผลสัมฤทธิ์และประโยชน์ส่วนรวม

3. รับใช้ประชาชน ยกระดับการอำนวยความยุติธรรมและการคุ้มครองสิทธิและเสรีภาพของประชาชนมุ่งให้บุคลากรมีจิตสำนึกในการปฏิบัติหน้าที่ ร่วมกันให้บริการประชาชนอย่างมีประสิทธิภาพและเต็มกำลังความสามารถ โดยถือความต้องการของประชาชนผู้รับบริการเป็นศูนย์กลางเน้นการนำเทคโนโลยีสารสนเทศและนวัตกรรมใหม่มาใช้สนับสนุนการปฏิบัติงาน เพื่อให้ประชาชนเข้าถึงบริการของศาลยุติธรรมโดยง่าย สะดวก ประหยัด รวดเร็ว เสมอภาคและเท่าเทียม เพื่อธำรงความเชื่อมั่นและศรัทธาของประชาชนต่อองค์กรศาลยุติธรรม

2.4.4 อำนาจหน้าที่และโครงสร้าง

ตามประกาศคณะกรรมการบริหารศาลยุติธรรมโดยความเห็นชอบของประธานศาลฎีกามีผู้อำนวยการสำนักอำนวยการประจำศาลเป็นผู้บังคับบัญชาและรับผิดชอบในการปฏิบัติราชการในฐานะหัวหน้าส่วนราชการที่สูงกว่ากอง โดยอยู่ภายใต้การกำกับดูแล และคำสั่งให้ปฏิบัติราชการตามกฎหมายของผู้พิพากษาหัวหน้าศาลสำนักอำนวยการประจำศาลจังหวัด สำนักงานประจำศาลแขวง และสำนักงานประจำศาลเยาวชนและครอบครัว และมีอำนาจหน้าที่ดังต่อไปนี้

(ก) บริหารจัดการงานธุรการคดีและกิจการของศาลยุติธรรม

(ข) ดำเนินการเกี่ยวกับงานด้านนิติการ เพื่อสนับสนุนการพิจารณาพิพากษาคดี ของศาลยุติธรรม

(ค) ดำเนินการนำระบบการระงับข้อพิพาททางเลือกมาใช้นอกเหนือจากการพิจารณา พิพากษาคดี

(ง) ดำเนินการพัฒนาระบบเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการงานธุรการคดี ในสำนักอำนวยการประจำศาล

(จ) ให้คำปรึกษา แนะนำ และบริการประชาชนเกี่ยวกับกระบวนการพิจารณาคดีของศาลยุติธรรม

(ฉ) ดำเนินการเกี่ยวกับงบประมาณ การเงิน การบัญชี การพัสดุ อาคารสถานที่ และยานพาหนะของสำนักอำนวยการประจำศาล

(ช) บริหารงานทั่วไปของสำนักอำนวยการประจำศาล

(ซ) รายงานเกี่ยวด้วยคดีหรือรายงานกิจการอื่นตามคำสั่งของประธานศาลฎีกา ประธานศาลอุทธรณ์ ประธานศาลอุทธรณ์ภาค อธิบดีผู้พิพากษาศาลชั้นต้น อธิบดีผู้พิพากษาภาค และผู้พิพากษาหัวหน้าศาล

(ฌ) ปฏิบัติงานอื่นใดตามที่กฎหมายกำหนด

(ญ) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

ตามประกาศคณะกรรมการบริหารศาลยุติธรรมโดยความเห็นชอบของประธานศาลฎีกา ศาลจังหวัดแบ่งงานภายใน ออกเป็น 9 ส่วนงาน มีหน้าที่ความรับผิดชอบ ดังนี้

1) ส่วนช่วยอำนวยการ

2) ส่วนคลัง

3) ส่วนบริการประชาชนและประชาสัมพันธ์

4) ส่วนบริหารจัดการคดี

5) ส่วนช่วยพิจารณาคดี

6) ส่วนไกล่เกลี่ยและประนอมข้อพิพาท

7) ส่วนเทคโนโลยีสารสนเทศ

8) ส่วนเจ้าพนักงานตำรวจศาล

9) ส่วนเจ้าพนักงานคดี

ตามประกาศคณะกรรมการบริหารศาลยุติธรรมโดยความเห็นชอบของประธานศาลฎีกา ศาลแขวงแบ่งงานภายใน ออกเป็น 8 กลุ่มงาน มีหน้าที่ความรับผิดชอบ ดังนี้

1) กลุ่มงานช่วยอำนวยการ

2) กลุ่มงานคลัง

3) กลุ่มงานบริการประชาชนและประชาสัมพันธ์

4) กลุ่มงานบริหารจัดการคดี

5) กลุ่มงานช่วยพิจารณาคดี

6) กลุ่มงานไกล่เกลี่ยและประนอมข้อพิพาท

7) กลุ่มงานเจ้าพนักงานตำรวจศาล

8) กลุ่มเจ้าพนักงานคดี

ตามประกาศคณะกรรมการบริหารศาลยุติธรรมโดยความเห็นชอบของประธานศาลฎีกา ศาลเยาวชนและครอบครัวแบ่งงานภายใน ออกเป็น 6 ส่วนงาน มีหน้าที่ความรับผิดชอบ ดังนี้

1) กลุ่มงานช่วยอำนวยการ

2) กลุ่มงานคลัง

3) กลุ่มงานบริการประชาชนและประชาสัมพันธ์

4) กลุ่มงานคดี

5) กลุ่มงานช่วยพิจารณา

6) กลุ่มงานไกล่เกลี่ยและประนอมข้อพิพาท

2.4.5 ภัยคุกคามที่มีความเสี่ยงของหน่วยงานศาลในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ภัยคุกคามไซเบอร์ที่มีความเสี่ยงของหน่วยงานในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีดังนี้

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลดหรือได้มาจากสื่ออุปกรณ์อื่นเพื่อติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ ได้แก่ โปรแกรมที่ผู้ใช้งานดาวน์โหลดหรือนำมาจากสื่ออุปกรณ์อื่นติดตั้งเพื่อใช้งานเอง

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์หลอกที่ออกแบบมาให้เหมือนของจริง หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล์ เฟซบุ๊ก เช่น โปรแกรมรับ-ส่งจดหมายอิเล็กทรอนิกส์ระหว่างหน่วยงานศาลกับสำนักงานคุมประพฤติ เป็นต้น

3. ภัยคุกคามจากการใช้เครือข่ายไร้สาย ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่างๆ เนื่องจากหน่วยงานศาลยุติธรรมในสังกัดเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีการใช้งานระบบเครือข่ายไร้สาย ซึ่งสามารถใช้ระบบงานต่างๆ ผ่านระบบเครือข่ายไร้สายด้วย โดยเฉพาะระบบงานที่เชื่อมโยงไปจากกับระบบจากภายนอก เช่น ระบบยื่นคำฟ้องอิเล็กทรอนิกส์สำหรับประชาชน (e-Filing) ระบบบริการออนไลน์ศาลยุติธรรม Court Integral Online Service (CIOS) โปรแกรมระบบงานฐานข้อมูลหมายจับ (Arrest Warrant Information System : AWIS) เป็นต้น

4. ภัยคุกคามที่เกิดจากการโจมตีแบบเจาะจงเป้าหมาย โดยการโจมตีดังกล่าวจะมาในรูปแบบผู้โจมตีหรือแฮกเกอร์ ที่อาศัยช่องโหว่ไม่ว่าจะเป็นจากระบบงานหรือ ไม่มีอุปกรณ์ป้องกันได้อย่างปลอดภัย

2.5 เอกสารงานวิจัยที่เกี่ยวข้อง

สำหรับงานวิจัยที่เกี่ยวข้องกับการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 จากที่ผู้วิจัยได้ศึกษาทบทวนวรรณกรรมมานั้นผู้วิจัยพบว่าจากการศึกษามีนักวิชาการที่ได้ศึกษาวิจัยเกี่ยวกับการจัดการความเสี่ยง ความมั่นคงปลอดภัย และภัยคุกคามไซเบอร์ ในหลาย ๆ ด้านด้วยกันซึ่งมีรายละเอียดผลการวิจัยที่คล้ายคลึงกันและแตกต่างกันออกไปในหลาย ๆ งานวิจัย ดังนี้

2.5.1 งานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์ด้านการบริหารความเสี่ยง

การบริหารความเสี่ยงเป็นกระบวนการดำเนินงานหรือการกำหนดวิธีการจัดการที่เหมาะสมขององค์กร ขั้นตอนที่เป็นระบบและมีความต่อเนื่องอย่างเหมาะสม เพื่อลดเหตุของความเสี่ยงที่เกิดขึ้นหรือโอกาสของเหตุการณ์ที่เกิดในอนาคตให้อยู่ในระดับที่องค์กรยอมรับได้ มีการประเมิน ควบคุม และตรวจสอบอย่างเป็นระบบ เพื่อให้เกิดความเชื่อมั่นต่อองค์กรเป็นภาพลักษณ์ที่ดีขององค์กร

ธีระศักดิ์ เปี่ยมสุภัคพงศ์, ธีระรัตน์ เปี่ยมสุภัคพงศ์, พรพรรณ สุวรรณประทีป, สุกานดา โรจนประภายนต์ และ วัฒนา เสรีคุณากุล (2561) ศึกษาการเรียนรู้เพื่อรับมือกับการบริหารความเสี่ยงของธุรกิจในบริบทใหม่ ยุคอุตสาหกรรม 4.0 พบว่า ความสำคัญของการบริหารความเสี่ยง ภายใต้การเปลี่ยนแปลงอย่างรวดเร็ว ความเสี่ยงที่สำคัญที่สุด คือ การไม่ปรับตัว หรือไม่พร้อมที่จะปรับตัวได้อย่างเท่าทัน อย่างเช่นในธุรกิจระดับโลกที่เคยเป็นผู้นำต้องเสียส่วนแบ่งตลาด บางบริษัทต้องปิดกิจการ หลาย ๆ แบรนด์สินค้าหายไปจากความนิยม หรือถูกทดแทนด้วยแบรนด์ใหม่ ๆ ดังนั้นการมีระบบกำกับดูแลกิจการและการบริหารความเสี่ยงที่ดีที่ครอบคลุมในทุกด้าน จะช่วยให้องค์กรมีความพร้อมในการรับมือกับการเปลี่ยนแปลงและการปรับตัวที่เกิดขึ้นในอนาคตได้อย่างถูกต้อง ทันท่วงที

ขณะที่ วิจิตรา สีแดงก่ำ (2562) ศึกษาการบริหารความเสี่ยงขององค์กรในศตวรรษที่ 21 พบว่าการบริหารองค์กรในปัจจุบันการบริหารความเสี่ยง (Risk Management) จะประสบความสำเร็จได้นั้น ทุกคนในองค์กรควรมีส่วนร่วมในการวิเคราะห์ ภาระงานในเชิงลึกเชิงบูรณาการ เพื่อเชื่อมโยงกับการกำหนดวิสัยทัศน์ พันธกิจ นโยบาย มาตรการ เป้าประสงค์ และ

แผนปฏิบัติการขององค์กร ซึ่งจะได้แนวทางการปฏิบัติงานที่ดี (Best Practice) ดังนั้น ความเสี่ยงของทุกองค์กรจึงจำเป็นต้องกำจัดโอกาสหรือเหตุการณ์ที่ไม่พึงประสงค์ ที่จะทำให้องค์กรไม่บรรลุเป้าประสงค์ โดยองค์กรจะสร้างแนวทางในการจัดการกับความเสี่ยงที่จะเกิดขึ้นกับองค์กร ดังนั้น ผู้บริหาร บุคลากรในสถานศึกษาต้องมีส่วนร่วมในประเมินความเสี่ยงและผลกระทบต่อองค์กรและร่วมกันกำหนดกลยุทธ์องค์กร หรือกำหนดระดับความเสี่ยงที่เหมาะสมที่องค์กรสามารถยอมรับได้ ซึ่งสอดคล้องกับ กมลพร บุญนนทารมย์ และ ศันสนีย์ จะสุวรรณ์ (2564) ศึกษาการบริหารความเสี่ยงอย่างมืออาชีพ Professional Risk Management พบว่าการบริหารองค์กรในปัจจุบันการบริหารความเสี่ยงให้ประสบความสำเร็จได้นั้น ถือเป็นเรื่องของทุกคนในองค์กรควรมีส่วนร่วมในการวิเคราะห์บริหารงานทั้งเชิงลึก และเชิงบูรณาการ เพื่อเชื่อมโยงเข้ากับการกำหนดวิสัยทัศน์ พันธกิจ นโยบาย เป้าหมายและแผนปฏิบัติงานขององค์กร การกำจัดโอกาสหรือเหตุการณ์ไม่พึงประสงค์ที่จะทำให้องค์กรไม่บรรลุเป้าหมายจึงถือเป็นเรื่องสำคัญ ผู้บริหาร บุคลากรในสถานศึกษา รวมถึงบุคคลที่มีส่วนเกี่ยวข้องต้องมีส่วนร่วมในการประเมินความเสี่ยงและผลกระทบต่อองค์กรและร่วมกันกำหนดระดับความเสี่ยงที่เหมาะสมที่องค์กรสามารถยอมรับได้

ขณะที่ พิชญาพร พีรพันธุ์ และ วิโรจน์ เจษฎาลักษณ์ (2564) ศึกษากรอบแนวคิดปัจจัยเชิงสาเหตุและผลลัพธ์ของความสามารถในการจัดการความเสี่ยงขององค์กร พบว่าการจัดการความเสี่ยงขององค์กรเป็นกระบวนการเพื่อป้องกันและลดความเสี่ยง รวมทั้งจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ และช่วยในการบรรลุวัตถุประสงค์ขององค์กร ดังนั้นการเสนอแนวคิดปัจจัยเชิงสาเหตุและผลลัพธ์ของความสามารถในการจัดการความเสี่ยงขององค์กร รวมทั้งอิทธิพลของปัจจัยแทรกที่มีผลกระทบในความสัมพันธ์ โดยศึกษาและทบทวนวรรณกรรมจากแหล่งต่าง ๆ เช่น ตำรา บทความวิชาการ บทความวิจัย และเอกสารเผยแพร่ เพื่อเป็นประโยชน์ในการนำไปประยุกต์ใช้ในองค์กร และเป็นแนวทางในการศึกษาเชิงประจักษ์ต่อไป สอดคล้องกับ สุฏิกา รักประสูติ (2558) ศึกษาบทบาทของผู้ตรวจสอบภายในต่อการจัดการความเสี่ยงองค์กร: ปัจจัยสาเหตุและผลลัพธ์ พบว่า ผู้ตรวจสอบภายในมีส่วนร่วมในการจัดการความเสี่ยงองค์กร และการจัดการความเสี่ยงองค์กรสร้างมูลค่าเพิ่มให้แก่องค์กร เช่น มูลค่าของกิจการเพิ่มขึ้น กิจการมีกำไรสูงขึ้น ลดความผันผวนของกำไร ค่าสอบบัญชีลดลง ตลอดจนลดการทุจริตในองค์กร ปัจจัยที่ส่งผลกระทบต่อการปฏิบัติงานตรวจสอบภายใน ปัจจัยที่ส่งผลต่อความเป็นอิสระและความเที่ยงธรรมของผู้ตรวจสอบภายใน และความสัมพันธ์ระหว่างคุณภาพการตรวจสอบภายใน การจัดการความเสี่ยง และผลการดำเนินงานของบริษัท ซึ่งคาดว่าการพัฒนาคุณภาพของการตรวจสอบภายใน จะเป็นประโยชน์ต่อองค์กรอย่างแท้จริง

ในขณะที่ นริส อุไรพันธ์ และ ธรนี มณีศรี (2563) โมเดลสมการเชิงโครงสร้าง เพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนสำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย พบว่าโมเดลปัจจัยตัวแปรเชิงสาเหตุที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน พบว่าความร่วมมือกัน การจัดการ

ภัยคุกคามทางไซเบอร์ และการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน เป็นปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนและเป็นปัจจัยที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจด้วย โดยความร่วมมือกันและการจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชน เป็นปัจจัยที่มีผลต่อการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน

ในส่วนงานวิจัยของ ปริญญา หอมอเนก และ ACIS Research LAB (2557) ศึกษาบทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก พบว่าหน่วยงานของรัฐและทุกองค์กร โดยเฉพาะองค์กรในกลุ่มโครงสร้างพื้นฐานสำคัญซึ่งความมั่นคงปลอดภัยของระบบควบคุมอุตสาหกรรม (ICS) สำหรับระบบโครงสร้างพื้นฐานสำคัญขององค์กร มีผลกระทบทางกายภาพโดยตรงต่อสังคมและโลก รวมทั้งความเสี่ยงที่อาจเกิดขึ้นต่อสุขภาพและความปลอดภัยของประชาชน และผลกระทบต่อสิ่งแวดล้อม ผู้บริหารหน่วยงานของรัฐและทุกองค์กรต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นสำคัญ ซึ่งต้องมาจากวิสัยทัศน์และภาวะผู้นำของผู้บริหารระดับสูงขององค์กร ที่ต้องเตรียมพร้อมรับมือ ด้วยการมองหาแนวทางและโอกาสในการปรับปรุง การป้องกันที่ดี ย่อมทำให้พร้อมที่จะรับมือและแก้ไขได้อย่างเหมาะสมทันท่วงที แต่หากไม่มีการป้องกันที่ดี ภัยคุกคามก็อาจจะเป็นความเสี่ยงที่ยากต่อการบริหารจัดการ กระทบต่อความอยู่รอดขององค์กรในระยะยาวและยากที่ดำเนินธุรกิจแบบยั่งยืนได้ในที่สุด

ซึ่งสอดคล้องกับ อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) ศึกษาเรื่องการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร และเสนอวิธีการบริหารความเสี่ยงอย่างเหมาะสมเป็นไปตามมาตรฐานสากล สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเกิดขึ้นกับระบบสารสนเทศขององค์กรได้ในอนาคตโดยอธิบายถึงกระบวนการบริหารความเสี่ยง ตั้งแต่กระบวนการเตรียมการ กระบวนการประเมินความเสี่ยง การรายงานผลการประเมินความเสี่ยงและการติดตามผลการประเมินความเสี่ยงตามวงรอบ และการกำหนดมาตรการควบคุม เพื่อตอบสนองต่อความเสี่ยงที่เกิดขึ้นจากการสังเคราะห์กรอบแนวคิด NIST Framework กฎหมาย ระเบียบข้อบังคับ ข้อมูลจากเอกสารทางวิชาการต่าง ๆ เพื่อให้ได้แนวทางปฏิบัติ และลำดับกระบวนการบริหารความเสี่ยงอย่างเป็นระบบที่สามารถนำไปปฏิบัติหรือประยุกต์ใช้ได้จริงในองค์กร

ในขณะที่ นุกูล แดงภูมี (2564) ศึกษาเทคนิควิธีการบริหารจัดการความเสี่ยงในชื่อ การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM) โดยนำเสนอเนื้อหาเกี่ยวกับความเป็นมาและความหมาย กรอบแนวคิด ประโยชน์ของการบริหารความเสี่ยงทั่วทั้งองค์กร ซึ่งวิเคราะห์ความแตกต่างเชิงทฤษฎีระหว่างการควบคุมภายในและการบริหารความเสี่ยงทั่วทั้งองค์กร บทบาทหน้าที่ของบุคลากรทุกระดับในองค์กรและขั้นตอนการพัฒนาระบบและปัจจัยแห่งความสำเร็จ ในการพัฒนาระบบบริหารความเสี่ยงทั่วทั้งองค์กร รวมถึงประเด็นที่มักมีความเข้าใจคลาดเคลื่อนเพื่อสร้างความเข้าใจที่ถูกต้องเกี่ยวกับการบริหาร

ความเสี่ยงทั่วทั้งองค์กร ให้สามารถนำไปประยุกต์ใช้เพื่อเป็นหนึ่งปัจจัยสร้างความสำเร็จให้แก่องค์กรต่อไป

ในขณะที่วิศณุ สร้างวงศ์ใหม่ (2561) ศึกษาการเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์ พบว่าองค์กรสมัยใหม่ทั้งภาครัฐและเอกชนต่างพึ่งพาเทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงานให้ประสบความสำเร็จ ระบบสารสนเทศมีความซับซ้อนตั้งแต่ระบบบัญชี การเงิน บุคลากรหรือระบบควบคุมอุตสาหกรรม ระบบอาวุธ ระบบดังกล่าวมีความเสี่ยงที่จะเสียหาย ผู้บริหารทุกระดับจำเป็นต้องตระหนักถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล ดังนั้นการวางแผนเพื่อเตรียมรับมือกับเหตุการณ์และการบริหารความเสี่ยงจะทำให้ค่าความเสียหายลดลง หรืออาจไม่เกิดเหตุการณ์

กล่าวโดยสรุปจากการทบทวนวรรณกรรมพบว่าในประเด็นการบริหารความเสี่ยงได้ว่าการบริหารความเสี่ยงขององค์กรมีความสำคัญและเป็นประโยชน์ต่อองค์กร ช่วยให้ฝ่ายบริหารสามารถจัดการกับความไม่แน่นอนและความเสี่ยงของโอกาสได้อย่างมีประสิทธิผล ทำให้การดำเนินงานขององค์กรอยู่ในระดับความเสี่ยงที่ยอมรับได้ การบริหารความเสี่ยงที่ดีจะช่วยให้องค์กรกำหนดทิศทาง หรือการกำหนดกลยุทธ์ที่สอดคล้องกับระดับความเสี่ยงอันเป็นที่ยอมรับได้ เป็นเครื่องมือในการตัดสินใจเพื่อตอบสนองต่อความเสี่ยง และสุดท้ายทำให้องค์กรลดเหตุการณ์สิ่งที่ไม่คาดคิดว่าจะเผชิญได้ เนื่องจากองค์กรได้มีการบริหารความเสี่ยง และคิดไว้ล่วงหน้าแล้ว ดังนั้นเมื่อสถานการณ์นั้นเกิดขึ้นจริง ๆ ก็จะสามารถตอบสนองได้ในทิศทางที่ดีที่องค์กรสามารถยอมรับได้ เกิดการพัฒนาแนวทางการจัดการกับความเสี่ยงและนำไปปฏิบัติอย่างเป็นระบบต่อไป

ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง

พิชญาพร พีรพันธุ์ และ วิโรจน์ เจษฎาลักษณ์ (2564) ศึกษากรอบแนวคิดปัจจัยเชิงสาเหตุและผลลัพธ์ของความสามารถในการจัดการความเสี่ยงขององค์กร พบว่าการจัดการความเสี่ยงขององค์กรมีความสำคัญในการจัดการการดำเนินกิจกรรมต่าง ๆ ขององค์กรเพื่อป้องกันและลดความเสี่ยง รวมทั้งจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ และช่วยในการบรรลุวัตถุประสงค์ขององค์กร แนวคิดปัจจัยเชิงสาเหตุและผลลัพธ์ของความสามารถในการจัดการความเสี่ยงขององค์กร และปัจจัยแทรกที่มีผลกระทบในความสัมพันธ์ โดยศึกษาและทบทวนวรรณกรรมจากแหล่งต่าง ๆ อาทิ ตำรา บทความวิชาการ บทความวิจัย และเอกสารเผยแพร่เพื่อเป็นประโยชน์ในการนำไปประยุกต์ใช้ในองค์กร และเป็นแนวทางในการศึกษาเชิงประจักษ์ต่อไปในอนาคต สอดคล้องกับ สุฏิกา รักประสูติ (2558) ศึกษาบทบาทของผู้ตรวจสอบภายในต่อการจัดการความเสี่ยงองค์กร: ปัจจัยสาเหตุและผลลัพธ์ พบว่า ผู้ตรวจสอบภายในมีส่วนร่วมในการจัดการความเสี่ยงองค์กร และการจัดการความเสี่ยงองค์กรสร้างมูลค่าเพิ่มให้แก่องค์กร เช่น มูลค่าของกิจการเพิ่มขึ้น กิจการมีกำไรสูงขึ้น ลดความผันผวนของกำไร ค่าสอบบัญชีลดลง ตลอดจนลดการทุจริตในองค์กร ปัจจัยที่ส่งผลกระทบต่อการปฏิบัติงานตรวจสอบ

ภายใน ปัจจัยที่ส่งผลต่อความเป็นอิสระและความเที่ยงธรรมของผู้ตรวจสอบภายใน และความสัมพันธ์ระหว่างคุณภาพการตรวจสอบภายใน การจัดการความเสี่ยง และผลการดำเนินงานของบริษัท ซึ่งคาดว่าการพัฒนาคุณภาพของการตรวจสอบภายใน จะเป็นประโยชน์ต่อองค์กรอย่างแท้จริง

กล่าวโดยสรุปจากการทบทวนวรรณกรรมพบว่าในประเด็นปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง องค์กรสามารถคิดปัจจัยสาเหตุและผลลัพธ์จะสามารถนำไปสู่กระบวนการจัดการความเสี่ยงซึ่งส่งผลต่อผลลัพธ์ในการบริหารจัดการความเสี่ยงได้อย่างดี เป็นสิ่งที่อยู่ในเกณฑ์ขององค์กรยอมรับได้ ป้องกันหรือลดความเสียหายที่จะเกิดขึ้น ทำงานให้งานมีความสำเร็จเป็นไปด้วยความเรียบร้อย

ด้านความมั่นคงปลอดภัยไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์ เป็นวิธีการ มาตรการ หรือการดำเนินการใด ๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษาความลับ การรักษาความครบถ้วน และสภาพพร้อมใช้งาน ของอุปกรณ์และข้อมูลภายในระบบสารสนเทศ

อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) ศึกษาเรื่องการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร และเสนอวิธีการบริหารความเสี่ยงอย่างเหมาะสมเป็นไปตามมาตรฐานสากล สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเกิดขึ้นกับระบบสารสนเทศขององค์กรได้ในอนาคตโดยอธิบายถึงกระบวนการบริหารความเสี่ยงตั้งแต่กระบวนการเตรียมการ กระบวนการประเมินความเสี่ยง การรายงานผล การประเมินความเสี่ยงและการติดตามผลการประเมินความเสี่ยงตามวงรอบ และการกำหนดมาตรการควบคุมเพื่อตอบสนองต่อความเสี่ยงที่เกิดขึ้นจากการสังเคราะห์กรอบแนวคิด NIST Framework กฎหมาย ระเบียบข้อบังคับ ข้อมูลจากเอกสารทางวิชาการต่าง ๆ เพื่อให้ได้แนวทางปฏิบัติ และลำดับกระบวนการบริหารความเสี่ยงอย่างเป็นระบบที่สามารถนำไปปฏิบัติหรือประยุกต์ใช้ได้จริงในองค์กร

ทั้งนี้ กริน ธัญญวิกร และ ธีระ กุลสวัสดิ์ (2564) ศึกษาเรื่องการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศกรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย พบว่า 1) ปัญหาภัยคุกคามทางไซเบอร์ คือ ปัญหาด้านความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์และความพร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ โดยมีกฎหมาย 2 ฉบับ ในปี พ.ศ. 2562 คือ พ.ร.บ.ไซเบอร์ฯ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และธนาคารแห่งประเทศไทยได้ออกกฎระเบียบต่าง ๆ ในการกำกับดูแลธนาคารพาณิชย์ไทย 2) การดำเนินงานของธนาคารพาณิชย์ไทยได้จัดทำนโยบายและแนวทางการดำเนินการด้านการรักษาความปลอดภัยของข้อมูลและความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013) และ 3)

จากการศึกษาข้อเสนอแนะเพื่อให้แนวทางในการดำเนินงานตาม พ.ร.บ.ไซเบอร์ฯ สอดคล้องกับ NIST Cybersecurity Framework และนำมาตรฐาน ISO/IEC 27701:2019 มาใช้เป็นมาตรการเพิ่มเติมสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และสอดคล้องกับ สุวันต์นา เสมอเนตร (2561) ศึกษาการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC) พบว่า จากการประเมินผลความพึงพอใจของผู้รับบริการระบบบริหารความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO/IEC 27001:2013 พบว่า กลุ่มที่ 1 ผู้ใช้บริการ VM (Virtual Machine) และ Web Hosting มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก กลุ่มที่ 2 ผู้ให้บริการ (Vendor) มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก และกลุ่มที่ 3 ผู้รับบริการทั่วไป มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก โดยการนำมาตรฐาน ISO/IEC 27001:2013 เข้ามาใช้เพื่อเพิ่มความมั่นคงปลอดภัยขององค์กรให้เป็นไปตามมาตรฐานสากล ผลการดำเนินงานประสบผลสำเร็จเป็นอย่างดี

ในขณะชฎาภรณ์ สิงห์แก้ว (2564) ศึกษาบทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม ปัญหาและอุปสรรคของภาครัฐในการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทางเศรษฐกิจและสังคม และข้อเสนอแนะและแนวทางแก้ไขการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทางเศรษฐกิจและสังคม พบว่าประเทศไทยมีการพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์ อาชญากรรมไซเบอร์จึงเป็นภัยที่ไทยต้องเผชิญอย่างหลีกเลี่ยงไม่ได้ การโจมตีระบบ การขโมยข้อมูล การปลอมบัญชีโซเชียลมีเดีย และภัยคุกคามไซเบอร์อื่น ๆ มีปรากฏอย่างต่อเนื่อง ซึ่งภาครัฐเล็งเห็นความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงได้ผลักดันร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และร่างพระราชบัญญัติข้อมูลส่วนบุคคล เพื่อรองรับการเติบโตทางเศรษฐกิจดิจิทัลอย่างมั่นคงและปลอดภัย ซึ่งกำหนดให้มีสำนักงานคณะกรรมการรักษา-ความมั่นคงปลอดภัยไซเบอร์แห่งชาติทำหน้าที่เป็นหน่วยงานกลางในการประสานและขับเคลื่อนนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

อรรคเดช ประทีปอุษานนท์ และ ธาราทิพย์ กัลยาณมิตร (2560) ศึกษาแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พบว่าความมั่นคงของชาติได้รับผลกระทบจากไซเบอร์ในหลายระดับตั้งแต่รูปแบบที่มีผลกระทบต่อการใช้ชีวิตประจำวันของประชาชน ความน่าเชื่อถือทางเศรษฐกิจ สังคม การเมืองรวมไปถึงสภาวะแวดล้อมรอบตัว คุณลักษณะสำคัญประการหนึ่งของไซเบอร์ คือ สามารถแพร่กระจายอย่างรวดเร็วและไร้ซึ่งพรมแดน จึงนับเป็นภัยที่สามารถเกิดขึ้นได้ในทุกภูมิภาคทั่วโลก ประเทศไทยจึงต้องเตรียมการและใช้ศักยภาพด้านไซเบอร์ให้เป็นไปอย่างสอดคล้องกับสถานการณ์ระดับประเทศ ระดับภูมิภาค และในระดับโลกอย่างเกิดประโยชน์สูงสุด ปัจจุบันประเทศไทยมี

กรอบนโยบายและกฎหมายไซเบอร์ที่เกี่ยวข้องทั้งสิ้น สอดคล้องกับ เกียรติศักดิ์ ลุยทอง (2561) ศึกษาการพัฒนาระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก พบว่าการพัฒนาแอปพลิเคชัน และโปรแกรม MySQL สำหรับจัดการฐานข้อมูล กลุ่มตัวอย่างที่ใช้ มีจำนวน 2 กลุ่ม คือ กลุ่มผู้เชี่ยวชาญทางด้านซอฟต์แวร์ จำนวน 6 คน และกลุ่มผู้ใช้งานระบบ ซึ่งเป็นบุคลากรภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน สรุปได้ว่าระบบที่พัฒนาขึ้นมานั้นมีความเหมาะสม และสามารถตอบสนองการทำงานผู้ใช้งานได้ในทุกระดับการตรวจสอบและการรายงานผลสถิติภัยคุกคามทางไซเบอร์เป็นไปอย่างรวดเร็ว ลดขั้นตอนการตรวจสอบภัยคุกคามของเจ้าหน้าที่และลดปริมาณการใช้กระดาษ รวมถึงเป็นการรักษาความลับของทางราชการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้อย่างมีประสิทธิภาพ

วิลาส วิถีไพร (2561) ศึกษาการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง พบว่าอินเทอร์เน็ตประสานสรรพสิ่งมีความเสี่ยงมาก เนื่องจากยังไม่มีมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ดี และแบบสอบถามปลายปิดสำหรับบุคลากรของกองวิศวกรรมและแผนงาน การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน ผลการวิจัยพบว่า ความคิดเห็นเกี่ยวกับความเสี่ยงของภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่งอยู่ในระดับปานกลาง จากการวิเคราะห์ข้อมูลที่ได้ประกอบกับการอ้างอิงกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา จึงทำการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง พร้อมทั้งพัฒนาแอปพลิเคชันสำหรับประเมินองค์กรถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ซึ่งจะทำให้องค์กรสามารถเตรียมความพร้อมและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการใช้อินเทอร์เน็ตประสานสรรพสิ่งในองค์กรได้

ในขณะที่ปริญญา หอมอเนก และ ACIS Research LAB (2557) ศึกษาบทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก พบว่าหน่วยงานของรัฐและทุกองค์กร โดยเฉพาะองค์กรในกลุ่มโครงสร้างพื้นฐานสำคัญซึ่งความมั่นคงปลอดภัยของระบบควบคุมอุตสาหกรรม (ICS) สำหรับระบบโครงสร้างพื้นฐานสำคัญขององค์กร มีผลกระทบทางกายภาพโดยตรงต่อสังคมและโลก รวมทั้งความเสี่ยงที่อาจเกิดขึ้นต่อสุขภาพและความปลอดภัยของประชาชน และผลกระทบต่อสิ่งแวดล้อม ผู้บริหารหน่วยงานของรัฐและทุกองค์กรต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นสำคัญ ซึ่งต้องมาจากวิสัยทัศน์และภาวะผู้นำของผู้บริหารระดับสูงขององค์กรที่ต้องเตรียมพร้อมรับมือด้วยการมองหาแนวทางและโอกาสในการปรับปรุง การป้องกันที่ดีย่อมทำให้พร้อมที่จะรับมือและแก้ไขได้อย่างเหมาะสมทันท่วงที แต่หากไม่มีการป้องกันที่ดี ภัยคุกคามก็อาจจะเป็นความเสี่ยงที่ยากต่อการบริหารจัดการ กระทบต่อความอยู่รอดขององค์กรในระยะยาวและยากที่ดำเนินธุรกิจแบบยั่งยืนได้ในที่สุด

วิศณุ สร้างวงศ์ใหม่ (2561) ศึกษาการเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์ พบว่าองค์กรสมัยใหม่ทั้งภาครัฐและเอกชนต่างพึ่งพาเทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงานให้ประสบความสำเร็จ ระบบสารสนเทศมีความซับซ้อนตั้งแต่ระบบบัญชี การเงิน บุคลากรหรือระบบควบคุมอุตสาหกรรม ระบบอาวุธ ระบบดังกล่าวมีความเสี่ยงที่จะเสียหาย ผู้บริหารทุกระดับจำเป็นต้องตระหนักถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล ดังนั้นการวางแผนเพื่อเตรียมรับมือกับเหตุการณ์และการบริหารความเสี่ยงจะทำให้ค่าความเสียหายลดลง หรืออาจไม่เกิดเหตุการณ์

กล่าวโดยสรุปจากการทบทวนวรรณกรรมพบว่าในประเด็นความมั่นคงปลอดภัยนั้น องค์กรควรจะมีมาตรการในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ โดยมีการสร้างความมั่นคงปลอดภัยทางไซเบอร์ ไม่ว่าจะเป็นการจัดการความเสี่ยงต่าง ๆ ซึ่งตั้งแต่เตรียมความพร้อมทั้ง ฮาร์ดแวร์และซอฟต์แวร์ ในการปกป้องภัยคุกคาม การพัฒนาทั้งบุคลากร แอพพลิเคชั่น รวมถึงมาตรฐานในการออกกฎหมายพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และร่างพระราชบัญญัติข้อมูลส่วนบุคคล และมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013) แนวทางในการดำเนินงานตาม พ.ร.บ.ไซเบอร์ฯ ควรสอดคล้องกับ NIST Cybersecurity Framework และนำมาตรฐาน ISO/IEC 27701:2019 มาใช้เป็นมาตรการเพิ่มเติม

ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์

เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี (2565) ศึกษาความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร พบว่า บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก โดยเมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่าบุคลากรในบริษัทเอกชนแห่งนี้ที่มีเพศ อายุ และประสบการณ์การทำงานที่ต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในส่วนบุคลากรที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ

ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ สถาบันเทคโนโลยีป้องกันประเทศ (2559) ศึกษาภัยคุกคามทางไซเบอร์ พบว่าการเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ ในการปกป้อง ป้องกัน ภัยคุกคาม ด้านไซเบอร์ นับว่าเป็นสิ่งที่สำคัญ ภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรง และมีความสลับซับซ้อนในการแก้ไขปัญหามากยิ่งขึ้น ส่งผลเสียหายให้กับองค์กรภาครัฐ และเอกชน ไม่ว่าจะเป็นผลเสียในด้านความมั่นคง ธุรกิจการเงิน การธนาคาร และข้อมูลส่วนบุคคล จึงมีความจำเป็นอย่างยิ่งในการกำหนดมาตรการในการป้องกันทั้งเชิงรุก/รับ ต่อภัยคุกคามทาง ไซเบอร์ โดยเฉพาะอย่างยิ่ง หน่วยงานด้านความมั่นคงจำเป็นต้องมีการวางแผน/แนวทาง สำหรับการป้องกันภัยคุกคามทางไซเบอร์ โดยมี

การปรับเปลี่ยนมาตรการให้สอดคล้องกับการเปลี่ยนแปลงทางยุทธศาสตร์ เพื่อให้สอดคล้องและทันต่อความทันสมัยของเทคโนโลยีที่มีความล้าหน้าอย่างรวดเร็วได้อย่างมีประสิทธิภาพ สอดคล้องกับภาณุพล บรรณกิจโสภณ (2560) ศึกษาแนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศของกองทัพไทย พบว่าภัยคุกคามนั้นเกิดได้จาก 2 แหล่ง แหล่งแรก คือ การโจมตีจากภายนอก จะโจมตีผ่านเครือข่ายภายนอกที่เชื่อมต่อ ต้องผ่านระบบป้องกันหากระบบป้องกันมีประสิทธิภาพเพียงพอจะสามารถป้องกันการโจมตีนั้นได้ แต่หากการป้องกันไม่มีประสิทธิภาพเพียงพอจะทำให้สามารถโจมตีได้ถึงระบบงาน และมีผลกระทบต่อการทำงานในที่สุด แหล่งที่สอง คือ การโจมตีจากภายในจะเห็นได้ว่าการโจมตีจากภายในอาจโจมตีจากภายในระบบป้องกันหรือภายในระบบงานที่อยู่หลังระบบป้องกัน ทำให้สามารถโจมตีได้ง่าย การโจมตีชนิดนี้เป็นอันตรายมากและป้องกันได้ยาก เนื่องจากเป็นการโจมตีที่มาจากบุคคลภายในหน่วยงาน

ขณะที่วิจัยนริส อุไรพันธ์ และ ธรนี มณีศรี (2563) โมเดลสมการเชิงโครงสร้าง เพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนสำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย พบว่าโมเดลปัจจัยตัวแปรเชิงสาเหตุที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน พบว่าความร่วมมือกัน การจัดการภัยคุกคามทางไซเบอร์ และการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน เป็นปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนและเป็นปัจจัยที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจด้วย โดยความร่วมมือกันและการจัดการภัยคุกคามทางไซเบอร์ของดิจิทัลซัพพลายเชน เป็นปัจจัยที่มีผลต่อการจัดการความเสี่ยงทางไซเบอร์ของดิจิทัลซัพพลายเชน

งานวิจัยของกริน ธัญญวิกร และ ธีระ กุลสวัสดิ์ (2564) ศึกษาเรื่องการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศกรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย พบว่า 1) ปัญหาภัยคุกคามทางไซเบอร์ คือ ปัญหาด้านความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์และความพร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ โดยมีกฎหมาย 2 ฉบับ ในปี พ.ศ. 2562 คือ พ.ร.บ.ไซเบอร์ฯ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และธนาคารแห่งประเทศไทยได้ออกกฎระเบียบต่าง ๆ ในการกำกับดูแลธนาคารพาณิชย์ไทย 2) การดำเนินงานของธนาคารพาณิชย์ไทยได้จัดทำนโยบายและแนวทางการดำเนินการด้านการรักษาความปลอดภัยของข้อมูลและความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013) และ 3) จากการศึกษาข้อเสนอแนะเพื่อให้แนวทางในการดำเนินงานตาม พ.ร.บ. ไซเบอร์ฯ ควรสอดคล้องกับ NIST Cybersecurity Framework และนำมาตรฐาน ISO/IEC 27701:2019 มาใช้เป็นมาตรการเพิ่มเติมสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

นอกจากนี้งานวิจัยของ ยุทธศักดิ์ รักเสรีพิทักษ์ และ ศิริลักษม์ ตันตยกุล (2565) ศึกษาบทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน

ภัยคุกคามรูปแบบใหม่ พบว่าสภาพปัญหาภัยคุกคามทางไซเบอร์ของประเทศไทยแบ่งออกเป็น 2 ปัญหาใหญ่ ได้แก่ 1) ความไม่พร้อมในการป้องกันและแก้ไขภัยคุกคามทางไซเบอร์ และความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ และ 2) ความไม่พร้อมในการรับมือปรากฏการณ์อำนาจแฝงจากโซเชียลมีเดีย และการสูญเสียอธิปไตยไซเบอร์ของชาติ ในส่วนของความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ จากผลการวิเคราะห์ขีดความสามารถด้านไซเบอร์ พบว่า ประเทศไทยมีขีดความสามารถด้านไซเบอร์โดยรวม อยู่ที่ระดับ 1.95 หมายความว่า ไทยจำเป็นต้องพัฒนาขีดความสามารถด้านไซเบอร์ในทุกมิติ

กล่าวโดยสรุปจากการทบทวนวรรณกรรมพบว่าในประเด็นความตระหนักรู้และภัยคุกคามไซเบอร์ องค์กรควรต้องมีบุคลากรที่มีความรู้และความเข้าใจจากภัยคุกคามไซเบอร์ เพื่อที่จะได้ปฏิบัติงานได้อย่างปลอดภัย ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ด้านการพัฒนาบุคลากร พัฒนาแอพพลิเคชั่นและการปรับปรุงอุปกรณ์

ปรัชญา เฉลิมวัฒน์ (2560) ศึกษาแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ พบว่าแนวทางในการพัฒนากำลังพลด้านไซเบอร์ที่ได้นำเสนอนี้จะเป็นประโยชน์ต่อการกำหนดกรอบเวลา การวางแผน การดำเนินการเสริมสร้างความแข็งแกร่งของบุคลากรด้านไซเบอร์ให้กับประเทศชาติ ซึ่งหากนำไปใช้ปฏิบัติได้อย่างจริงจังจะทำให้สามารถลดปัญหาการขาดแคลนกำลังพลไซเบอร์ และทำให้เกิดความยั่งยืน ในการเสริมสร้างกำลังพลไซเบอร์ในระยะยาวได้เป็นอย่างดี นอกจากนั้นกำลังพลสำรองไซเบอร์ยังเป็นส่วนสำคัญในการพัฒนาอุตสาหกรรมซอฟต์แวร์เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศในอนาคต สอดคล้องกับธนภัทร กิตติวณิชพันธุ์ และ อานนท์ ทับเที่ยง (2561) ศึกษาสมรรถนะ ของ บุคลากรในหน่วยงานราชการด้านความมั่นคงปลอดภัยไซเบอร์ ตามข้อกำหนด NIST และ มาตรฐาน ISO27001/2013 เพื่อหาสมรรถนะในด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) สำหรับบุคลากรในหน่วยงานรัฐบาล เพื่อเป็นแนวทางในการบริหารจัดการและพัฒนาสมรรถนะของบุคลากรในหน่วยงานราชการทั้ง 5 ระดับชั้น โดยเกณฑ์ที่ใช้กำหนดความสามารถของบุคลากรแบ่งเป็นทั้งหมด 6 ระดับ ผลการวิจัยพบว่า สมรรถนะหลักในด้านความมั่นคงปลอดภัย มีทั้งหมด 15 สมรรถนะหลัก 107 สมรรถนะย่อย โดยมีสมรรถนะย่อยในหัวข้อที่แตกต่างกัน โดยแนวคิดการจัดระดับสมรรถนะของผู้เชี่ยวชาญจะแบ่งออกเป็น 4 ด้าน ประกอบด้วย 1.ด้านเทคนิค 2.ด้านความเสี่ยง 3.ด้านแผนและทิศทางการบริหารองค์กร 4.ด้านบุคลากรและการติดต่อกับผู้มีส่วนได้เสียภายในและภายนอก

ณรงค์เวตย์ เรืองจวง (2561) ศึกษาแนวทางการพัฒนาขีดความสามารถบุคลากร ด้านไซเบอร์ของกองทัพอากาศ พบว่าขีดความสามารถการปฏิบัติการด้านไซเบอร์ของกองทัพอากาศ การปฏิบัติเชิงรับอยู่ในระดับดีและการปฏิบัติเชิงรุกอยู่ในระดับปานกลาง มีนโยบาย กระบวนการแผนแม่บท และแผนงานที่เกี่ยวข้องรองรับการปฏิบัติเกือบทุกด้าน แต่ยัง

ขาดแนวความคิดการปฏิบัติการด้านไซเบอร์ รวมถึงมีระบบและอุปกรณ์ที่ทันสมัยมีประสิทธิภาพ ปัจจัยที่มีผลกระทบต่อขีดความสามารถในการปฏิบัติด้านไซเบอร์คือ บุคลากร ซึ่งมีไม่เพียงพอ ขาดความรู้และทักษะในการปฏิบัติงานด้านไซเบอร์ ระบบการจัดการความรู้มีข้อมูลไม่ครบถ้วน และโครงสร้างการจัดหน่วยสามารถรองรับบุคลากรที่ปฏิบัติงานได้ในปัจจุบันเท่านั้น ดังนั้นต้องพัฒนาบุคลากรด้วยการให้การศึกษา การฝึกปฏิบัติ การอบรมทบทวนให้มีความรู้ความสามารถ มีทักษะ พร้อมที่จะปฏิบัติภารกิจด้านไซเบอร์ได้อย่างมีประสิทธิภาพ เร่งดำเนินการจัดทำแนวความคิดการปฏิบัติการด้านไซเบอร์เพื่อให้บุคลากรนำไปเป็นแนวทางการปฏิบัติภารกิจ ทบทวนแผนงานให้ทันสมัยและครอบคลุมการปฏิบัติ และควรจัดทำระบบการจัดการความรู้ให้มีข้อมูลถูกต้องครบถ้วน หากมีภารกิจด้านไซเบอร์มากขึ้นควรพิจารณาทบทวนโครงสร้างการจัดหน่วยให้สอดคล้องกับการปฏิบัติภารกิจด้วย

เกียรติศักดิ์ ลุยทอง (2561) ศึกษาการพัฒนาระบบตรวจสอบ เฝ้าระวังและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก พบว่าการพัฒนาแอปพลิเคชัน และโปรแกรม MySQL สำหรับจัดการฐานข้อมูล กลุ่มตัวอย่างที่ใช้ มีจำนวน 2 กลุ่ม คือ กลุ่มผู้เชี่ยวชาญทางด้านซอฟต์แวร์ จำนวน 6 คน และกลุ่มผู้ใช้งานระบบ ซึ่งเป็นบุคลากรภายในศูนย์ไซเบอร์กองทัพบก จำนวน 35 คน สรุปได้ว่าระบบที่พัฒนาขึ้นมานั้นมีความเหมาะสม และสามารถตอบสนองการทำงานผู้ใช้งานได้ในทุกระดับ การตรวจสอบและการรายงานผลสถิติภัยคุกคามทางไซเบอร์เป็นไปอย่างรวดเร็ว ลดขั้นตอนการตรวจสอบภัยคุกคามของเจ้าหน้าที่และลดปริมาณการใช้กระดาษ รวมถึงเป็นการรักษาความลับของทางราชการทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ สอดคล้องกับวิลาส วิถีไพร (2561) ศึกษาการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง พบว่าอินเทอร์เน็ตประสานสรรพสิ่งมีความเสี่ยงมาก เนื่องจากยังไม่มีมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ดี และแบบสอบถามปลายปิดสำหรับบุคลากรของกองวิศวกรรมและแผนงานการไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน ผลการวิจัยพบว่า ความคิดเห็นเกี่ยวกับความเสี่ยงของภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่งอยู่ในระดับปานกลาง จากการวิเคราะห์ข้อมูลที่ได้ประกอบกับการอ้างอิงกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา จึงทำการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง พร้อมทั้งพัฒนาแอปพลิเคชันสำหรับประเมินองค์กรถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ซึ่งจะทำให้องค์กรสามารถเตรียมความพร้อมและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการใช้อินเทอร์เน็ตประสานสรรพสิ่งในองค์กรได้

ในขณะที่งานวิจัยของสุวันต์นา เสมอเนตร (2561) ศึกษาการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC) พบว่า จากการ

ประเมินผลความพึงพอใจของผู้รับบริการระบบบริหารความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO/IEC 27001:2013 พบว่า กลุ่มที่ 1 ผู้ใช้บริการ VM (Virtual Machine) และ Web Hosting มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก กลุ่มที่ 2 ผู้ให้บริการ (Vendor) มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก และกลุ่มที่ 3 ผู้รับบริการทั่วไป มีความพึงพอใจในภาพรวมทุกด้านอยู่ในระดับมาก โดยการนำมาตรฐาน ISO/IEC 27001:2013 เข้ามาใช้เพื่อเพิ่มความมั่นคงปลอดภัยขององค์กรให้เป็นไปตามมาตรฐานสากล ผลการดำเนินงานประสบผลสำเร็จเป็นอย่างดี

ในขณะที่กริน ธัญญวิกร และ ธีระ กุลสวัสดิ์ (2564) ศึกษาเรื่อง การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศกรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย พบว่า 1) ปัญหาภัยคุกคามทางไซเบอร์ คือ ปัญหาด้านความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์และความพร้อมในการรับมือต่อการสูญเสียอธิปไตยไซเบอร์ของชาติ โดยมีกฎหมาย 2 ฉบับ ในปี พ.ศ. 2562 คือ พ.ร.บ. ไซเบอร์ฯ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และธนาคารแห่งประเทศไทยได้ออกกฎระเบียบต่าง ๆ ในการกำกับดูแลธนาคารพาณิชย์ไทย 2) การดำเนินงานของธนาคารพาณิชย์ไทยได้จัดทำนโยบายและแนวทางการดำเนินการด้านการรักษาความปลอดภัยของข้อมูลและความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013) และ 3) จากการศึกษาข้อเสนอแนะเพื่อให้แนวทางในการดำเนินงานตาม พ.ร.บ.ไซเบอร์ฯ สอดคล้องกับ NIST Cybersecurity Framework และนำมาตรฐาน ISO/IEC 27701:2019 มาใช้เป็นมาตรการเพิ่มเติมสำหรับการคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ส่วนงานวิจัยของยุทธศักดิ์ รักเสรีพิทักษ์ และ ศิริลักษม์ ตันตยกุล (2565) ศึกษาบทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามรูปแบบใหม่ พบว่าสภาพปัญหาภัยคุกคามทางไซเบอร์ของประเทศไทยแบ่งออกเป็น 2 ปัญหาใหญ่ ได้แก่ 1) ความไม่พร้อมในการป้องกันและแก้ไขภัยคุกคามทางไซเบอร์ และความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ และ 2) ความไม่พร้อมในการรับมือปรากฏการณ์อำนาจแฝงจากโซเชียลมีเดีย และการสูญเสียอธิปไตยไซเบอร์ของชาติ ในส่วนของความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ จากผลการวิเคราะห์ขีดความสามารถด้านไซเบอร์ พบว่า ประเทศไทยมีขีดความสามารถด้านไซเบอร์โดยรวม อยู่ที่ระดับ 1.95 หมายความว่า ไทยจำเป็นต้องพัฒนาขีดความสามารถด้านไซเบอร์ในทุกมิติ

กล่าวโดยสรุปจากการทบทวนวรรณกรรมพบว่าในประเด็นด้านการพัฒนาบุคลากร พัฒนาแอพพลิเคชั่นและการปรับปรุงอุปกรณ์ องค์กรควรต้องมีการพัฒนาทั้งทางด้านสมรรถนะบุคลากร แอพพลิเคชั่น และการปรับปรุงอุปกรณ์ให้มีความทันสมัยและ

สามารถรักษาความปลอดภัยให้กับระบบได้ เป็นการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กรได้

ด้านสถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์

สุภาพร พรมโส, ปราลี มณีรัตน์ และ ประสงค์ ประณีตพลกรัง (2564) ศึกษา สถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ผลการวิจัยพบว่า ปัญหาความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ได้แก่ ปัญหาเกี่ยวกับมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ การกำหนดนโยบายองค์กร ปัญหาด้านบุคลากร และปัญหาการถูกโจมตี อุปสรรคที่ส่งผลต่อการพัฒนาสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร พบว่ามหาวิทยาลัยราชภัฏ มีอุปสรรค ด้านนโยบายผู้บริหาร ด้านทักษะความรู้ ด้านวัฒนธรรมองค์กร ด้านความไม่เสถียรของระบบ ด้านสภาพความพร้อม และดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ โดยได้นำเสนอตัวแบบสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย มาตรฐานของระบบ การปรับด้านโครงสร้างพื้นฐาน การใช้ประโยชน์ทางเทคโนโลยีดิจิทัล การพัฒนาศักยภาพบุคลากร สมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์และการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์ สอดคล้องกับยุทธศักดิ์ รักเสรีพิทักษ์ และ ศิริลักษม์ ตันตยกุล (2565) ศึกษาบทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามรูปแบบใหม่ พบว่าสภาพปัญหาภัยคุกคามทางไซเบอร์ของประเทศไทยแบ่งออกเป็น 2 ปัญหาใหญ่ ได้แก่ 1) ความไม่พร้อมในการป้องกันและแก้ไขภัยคุกคามทางไซเบอร์ และความไม่พร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ และ 2) ความไม่พร้อมในการรับมือปรากฏการณ์อำนาจแฝงจากโซเชียลมีเดีย และการสูญเสียอธิปไตยไซเบอร์ของชาติ ในส่วนของความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ จากผลการวิเคราะห์ขีดความสามารถด้านไซเบอร์ พบว่า ประเทศไทยมีขีดความสามารถด้านไซเบอร์โดยรวม อยู่ที่ระดับ 1.95 หมายความว่า ไทยจำเป็นต้องพัฒนาขีดความสามารถด้านไซเบอร์ในทุกมิติ

กล่าวโดยสรุปจากการทบทวนวรรณกรรมพบว่าในประเด็นด้านสถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ องค์กรควรต้องมีความพร้อมในการป้องกันและแก้ไขภัยคุกคามทางไซเบอร์ และความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจะได้จัดการกับความเสี่ยงต่าง ๆ จากภัยคุกคามไซเบอร์ได้อย่างดีและเป็นที่ยอมรับได้ขององค์กร รวมถึงการคืนสภาพกลับมาทำงานได้อีกโดยเร็ว

2.5.2 งานวิจัยเกี่ยวกับการบริการสาธารณะ

ด้านการมีส่วนร่วม

เนตรชนก สูนาสวน,อำนวย บุญรัตนไมตรี, ชัยยงค์ พรหมวงค์ และอนันต์ เตียวต๋อย (2565) ศึกษาการบริการสาธารณะและการมีส่วนร่วมเพื่อการพัฒนาอย่างยั่งยืนของผู้ประกอบการ พบว่าการศึกษาการบริการสาธารณะเพื่อการพัฒนาที่ยั่งยืนของผู้ประกอบการ คือ กิจกรรมที่จัดขึ้นนั้นจะต้องมีความสอดคล้องกับความต้องการของผู้ประกอบการ การจัดกิจกรรมการให้บริการสาธารณะจะต้องมีขึ้นอย่างสม่ำเสมอ โดยคำนึงถึงผู้มาใช้บริการทุกคนอย่างเสมอภาคและเท่าเทียมกัน กิจกรรมดังกล่าวจะต้องมีความสะดวกต่อผู้รับบริการ จึงจะส่งผลให้เกิดการพัฒนาที่ยั่งยืนต่อผู้ประกอบการใน 3 ด้าน ได้แก่ 1. ด้านสังคม 2. ด้านเศรษฐกิจ และ 3. ด้านสิ่งแวดล้อม สามารถทำให้เศรษฐกิจเจริญเติบโตอย่างมีคุณภาพพัฒนาคนให้มีความรู้ มีสมรรถนะและมีคุณภาพชีวิตดีขึ้น เป็นสังคมแห่งการเรียนรู้ และใช้ทรัพยากรธรรมชาติในปริมาณที่ระบบนิเวศสามารถฟื้นตัวกลับสู่สภาพเดิมได้

ด้านการป้องกันยาเสพติด

เขมิกา ทองเรือง และ พัณณกร สอนไว (2565) ศึกษาการบริการสาธารณะของกำนันและผู้ใหญ่บ้าน ด้านการป้องกันยาเสพติดในชุมชน พบว่าหลักการบริการสาธารณะ ด้านการให้ความรู้เกี่ยวกับพิษภัยของยาเสพติดโดยสอดแซกหลักคำสอนทางศาสนาพร้อมหลักกฎหมาย ซึ่งวิธีการนี้อาจช่วยให้ผู้ค้าและผู้ติดยาเสพติดสามารถแก้ไขปัญหาชีวิตของตนเองอีกทั้งทำให้ผู้ที่ค้าและติดยาเสพติดได้ทำให้จิตใจเข้มแข็งต่อสู้กับพิษร้ายของยาเสพติด ควรมีกิจกรรมต่าง ๆ เช่น การจัดให้มีแข่งขันกีฬา การจัดให้ผู้ค้าและผู้ติดยาเสพติดเข้าเข้าร่วมกิจกรรมภายในหมู่บ้าน ทั้งนี้เพื่อเป็นแนวทางในการแก้ไขปัญหายาเสพติด สอดคล้องกับบทบาทของกำนันและผู้ใหญ่บ้านผู้นำชุมชนในการแก้ไขปัญหายาเสพติดในพื้นที่ ซึ่งอาจทำให้ทุกฝ่ายให้ความร่วมมือเป็นอย่างดี ซึ่งอาจทำให้ชุมชนมีความเข้มแข็งในการแก้ไขปัญหายาเสพติดได้อย่างเป็นรูปธรรม นอกจากนี้ผู้นำยังสามารถนำมาประยุกต์เป็นภูมิปัญญาเพื่อนำไปสู่การจัดกิจกรรมที่สอดคล้องกับวิถีชีวิตการเป็นอยู่ ประเพณี และวัฒนธรรมของประชาชนในพื้นที่หรือเขตท้องถิ่นที่มีความเข้มแข็งในการแก้ไขปัญหายาเสพติดให้เกิดประสิทธิภาพประสิทธิผลต่อไป

ด้านโครงสร้างเชิงเส้นผลการปฏิบัติงานองค์การภาครัฐแรงจูงใจบริการสาธารณะและภาวะผู้นำการเปลี่ยนแปลง

ธีรศานต์ สิกขะโต (2560) ศึกษาความสัมพันธ์โครงสร้างเชิงเส้นผลการปฏิบัติงานองค์การภาครัฐแรงจูงใจบริการสาธารณะและภาวะผู้นำการเปลี่ยนแปลงขององค์การการไฟฟ้าส่วนภูมิภาค พบว่าผลการปฏิบัติงานองค์การภาครัฐ แรงจูงใจบริการสาธารณะของพนักงานมีความคิดเห็นอยู่ในระดับมากที่สุด ส่วนภาวะผู้นำการเปลี่ยนแปลงอยู่ในระดับมาก จากการเปรียบเทียบระดับความคิดเห็นของพนักงานต่อผลการปฏิบัติงานองค์กรภาครัฐจำแนกตามปัจจัยส่วนบุคคลพบว่า การมีบุตร และระดับตำแหน่งของพนักงานที่แตกต่างกันมีระดับ

ความคิดเห็นต่อผลการปฏิบัติงานองค์กรภาครัฐที่แตกต่างกัน ส่วนแรงจูงใจบริการสาธารณะเมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่า พนักงานที่มีตำแหน่งงานแตกต่างกัน มีระดับแรงจูงใจบริการสาธารณะที่แตกต่างกัน และเมื่อเปรียบเทียบระดับความคิดเห็นของพนักงานต่อภาวะผู้นำการเปลี่ยนแปลงเมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่า การมีบุตร สถานภาพ และระดับตำแหน่งของพนักงานที่แตกต่างกัน มีระดับความคิดเห็นต่อภาวะผู้นำการเปลี่ยนแปลงที่แตกต่างกัน และความสัมพันธ์ระหว่างผลการปฏิบัติงานองค์การภาครัฐ แรงจูงใจบริการสาธารณะ และภาวะผู้นำการเปลี่ยนแปลงมีความสัมพันธ์กัน ส่วนในการวิเคราะห์อิทธิพลของแรงจูงใจบริการสาธารณะและภาวะผู้นำการเปลี่ยนแปลงที่มีต่อผลการปฏิบัติงานองค์การภาครัฐ พบว่าได้รับอิทธิพลทางตรงจากแรงจูงใจบริการสาธารณะ และภาวะผู้นำการเปลี่ยนแปลง

ด้านจริยธรรมในการให้บริการสาธารณะ

สถาพร วิชัยรัมย์ ธัญญรัตน์ พุฑฒิพงษ์ชัยชาญ ภัทรนันท์ เกิดในหล้า และ จุฑารัตน์ จัตุกูล (2562) ศึกษาจริยธรรมในการให้บริการสาธารณะของไทย พบว่า การบริการสาธารณะ เป็นภารกิจที่รัฐได้ดำเนินการแก่ประชาชน ด้วยหลักการพื้นฐานได้แก่ หลักความต่อเนื่อง หลักความเสมอภาคและหลักความก้าวหน้า ซึ่งเป็นมาตรฐานทั่วไปที่รัฐจะต้องให้บริการแก่ประชาชน นอกจากนี้การจะเสริมสร้างหลักการดังกล่าวให้มีประสิทธิภาพจำเป็นต้องพัฒนาผู้ให้บริการโดยใช้หลักจริยธรรมที่เหมาะสมและมีความเกี่ยวข้องสัมพันธ์กัน จะได้พัฒนาในลักษณะของการนำไปใช้ได้จริงซึ่งจะทำให้การบริการสาธารณะมีคุณภาพและส่งผลให้เกิดความน่าเชื่อถือ ความไว้เนื้อเชื่อใจและความพึงพอใจแก่ประชาชนในภาพรวม

แรงจูงใจในการบริการสาธารณะ

ชวนพิศ เงินฉลาด (2562) ศึกษาแรงจูงใจในการบริการสาธารณะ กรณีศึกษาศูนย์อุตุนิยมวิทยาภาคใต้ พบว่าข้าราชการศูนย์อุตุนิยมวิทยาภาคใต้มีแรงจูงใจในการบริการสาธารณะในระดับมากที่สุด โดยมิติแรงจูงใจในการบริการสาธารณะ ระดับมากที่สุด คือเรื่องความเห็นอกเห็นใจผู้อื่นมี รองลงมา ความมุ่งมั่นในการรับผิดชอบต่อผลประโยชน์ส่วนรวม ตามด้วย การเข้าไปมีส่วนร่วมในการกำหนดนโยบายสาธารณะ และน้อยที่สุด ความเสียสละ

จากการทบทวนงานวิจัยที่ศึกษามาในข้างต้นและแยกเป็นประเด็นการศึกษาได้ตารางดังนี้

ตาราง 2 งานวิจัยงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์

ประเด็นงานวิจัย/นักวิจัย	ด้านการบริหารความเสี่ยง	ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง	ด้านความมั่นคงปลอดภัยไซเบอร์	ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์	ด้านการพัฒนาบุคลากร พัฒนาเอกสารและการปรับปรุงอุปกรณ์	ด้านสถาปัตยกรรมองค์กรและเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์
อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) ศึกษาเรื่องการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร	✓		✓			
นุกูล แดงภูมี (2564) ศึกษาเทคนิควิธีการบริหารจัดการความเสี่ยงในชื่อ การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM)	✓					
ธนภัทร กิตติวณิชพันธุ์ และ อานนท์ ทับเที่ยง (2561) ศึกษาสมรรถนะ ของ บุคลากร ใน หน่วยงาน ราชการ ด้าน ความ มั่นคงปลอดภัย ไซเบอร์ ตาม ข้อกำหนด NIST และ มาตรฐาน ISO27001/2013					✓	

ตาราง 2 งานวิจัยงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์ (ต่อ)

ประเด็นงานวิจัย/นักวิจัย	ด้านการบริหารความเสี่ยง	ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง	ด้านความมั่นคงปลอดภัยไซเบอร์	ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์	ด้านการพัฒนาบุคลากร พัฒนาเอกสารและการปรับปรุงอุปกรณ์	ด้านสถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์
ชฎาภรณ์ สิงห์แก้ว (2564) ศึกษาบทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม			✓			
กมลพร บุญนนทารมย์ และ ศันสนีย์ จะสุวรรณ์ (2564) ศึกษาการบริหารความเสี่ยงอย่างมืออาชีพ	✓					
เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี (2565) ศึกษาความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร				✓		
สุภาพร พรมโส, ปราลี มณีรัตน์ และ ประสงค์ ประณีตพลกรัง (2564) ศึกษา สถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ						✓

ตาราง 2 งานวิจัยงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์ (ต่อ)

ประเด็นงานวิจัย/นักวิจัย	**ด้านการบริหารความเสี่ยง**	**ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง**	**ด้านความมั่นคงปลอดภัยไซเบอร์**	**ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์**	**ด้านการพัฒนาบุคลากร พัฒนาแอพพลิเคชั่นและการปรับปรุงอุปกรณ์**	**ด้านสถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์**
วิจิตรา สีแดงก่ำ (2562) ศึกษาการบริหารความเสี่ยงขององค์กรในศตวรรษที่ 21	✓					
พิชญาพร พีรพันธุ์ และ วิโรจน์ เจษฎาลักษณ์ (2564) ศึกษากรอบแนวคิดปัจจัยเชิงสาเหตุและผลลัพธ์ของความสามารถในการจัดการความเสี่ยงขององค์กร	✓	✓				
สุฎิกา รักประสูติ (2558) ศึกษาบทบาทของผู้ตรวจสอบภายในต่อการจัดการความเสี่ยงองค์กร: ปัจจัยสาเหตุและผลลัพธ์	✓	✓				
ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ สถาบันเทคโนโลยีป้องกันประเทศ (2559) ศึกษาภัยคุกคามทางไซเบอร์				✓		

ตาราง 2 งานวิจัยงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์ (ต่อ)

ประเด็นงานวิจัย/นักวิจัย	ด้านการบริหารความเสี่ยง	ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง	ด้านความมั่นคงปลอดภัยไซเบอร์	ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์	ด้านการพัฒนาบุคลากร พัฒนาเทคนิคเชิงลึกและการปรับปรุงอุปกรณ์	ด้านสถาบันที่มีความพร้อมและมีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์
เกียรติศักดิ์ ลุยทอง (2561) ศึกษาการพัฒนาระบบตรวจสอบ เฝ้าระวังและแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก			✓		✓	
ปริญญา หอมอเนก and ACIS Research LAB (2557) ศึกษาบทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก	✓		✓			
วิลาส วิถีไพร (2561) ศึกษาการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง			✓		✓	
วิศณุ สร้างวงศ์ใหม่ (2561) ศึกษาการเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์	✓		✓			

ตาราง 2 งานวิจัยงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์ (ต่อ)

ประเด็นงานวิจัย/นักวิจัย	ด้านการบริหารความเสี่ยง	ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง	ด้านความมั่นคงปลอดภัยไซเบอร์	ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์	ด้านการพัฒนาบุคลากร พัฒนาเอกสารและการปรับปรุงอุปกรณ์	ด้านสถาบันที่เกี่ยวข้องและนโยบายความมั่นคงปลอดภัยไซเบอร์
ณรงค์เวตย์ เรืองจวง (2561) ศึกษาแนวทางการพัฒนาขีดความสามารถบุคลากร ด้านไซเบอร์ของกองทัพอากาศ					✓	
ภาณุพล บรรณกิจโสภณ (2560) ศึกษาแนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศของกองทัพไทย				✓		
กริน ธัญญวิกร และ ธีระ กุลสวัสดิ์ (2564) ศึกษาการจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย			✓	✓	✓	
ยุทธศักดิ์ รักเสรีพิทักษ์ และ ศิริลักษม์ ตันตยกุล (2565) ศึกษาบทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามรูปแบบใหม่				✓	✓	✓

ตาราง 2 งานวิจัยงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์ (ต่อ)

ประเด็นงานวิจัย/นักวิจัย	ด้านการบริหารความเสี่ยง	ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง	ด้านความมั่นคงปลอดภัยไซเบอร์	ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์	ด้านการพัฒนาบุคลากร พัฒนาเทคโนโลยีดิจิทัลและการปรับปรุงอุปกรณ์	ด้านสถาบันการศึกษาและหน่วยงานที่มีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์
นริส อุไรพันธ์ และ ธรนี มณีศรี (2563) โมเดลสมการเชิงโครงสร้างเพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนสำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย	✓			✓		
อรรคเดช ประทีปอุษานนท์ และ ธาราทิพย์ กัลยาณมิตร (2560) แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์			✓			
ธีระศักดิ์ เปี่ยมสุภัคพงศ์, ธีระรัตน์ เปี่ยมสุภัคพงศ์, พรพรรณ สุวรรณประทีป, สุกานดา โรจนประภายนต์ และ วัฒนา เสรีคุณากุล (2561) ศึกษาการเรียนรู้เพื่อรับมือกับการบริหารความเสี่ยงของธุรกิจในบริบทใหม่ ยุคอุตสาหกรรม 4.0	✓					

ตาราง 2 งานวิจัยงานวิจัยที่เกี่ยวกับการจัดการความเสี่ยงและภัยคุกคามไซเบอร์ (ต่อ)

ประเด็นงานวิจัย/นักวิจัย	ด้านการบริหารความเสี่ยง	ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง	ด้านความมั่นคงปลอดภัยไซเบอร์	ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์	ด้านการพัฒนาบุคลากร พัฒนาเอกสารเชิงเทคนิค และการปรับปรุงอุปกรณ์	ด้านความตระหนักรู้และการฝึกอบรมเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
สุวันต์นา เสมอเนตร (2561) ศึกษา การพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC)			✓		✓	
ปรัชญา เฉลิมวัฒน์ (2560) ศึกษาแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ					✓	

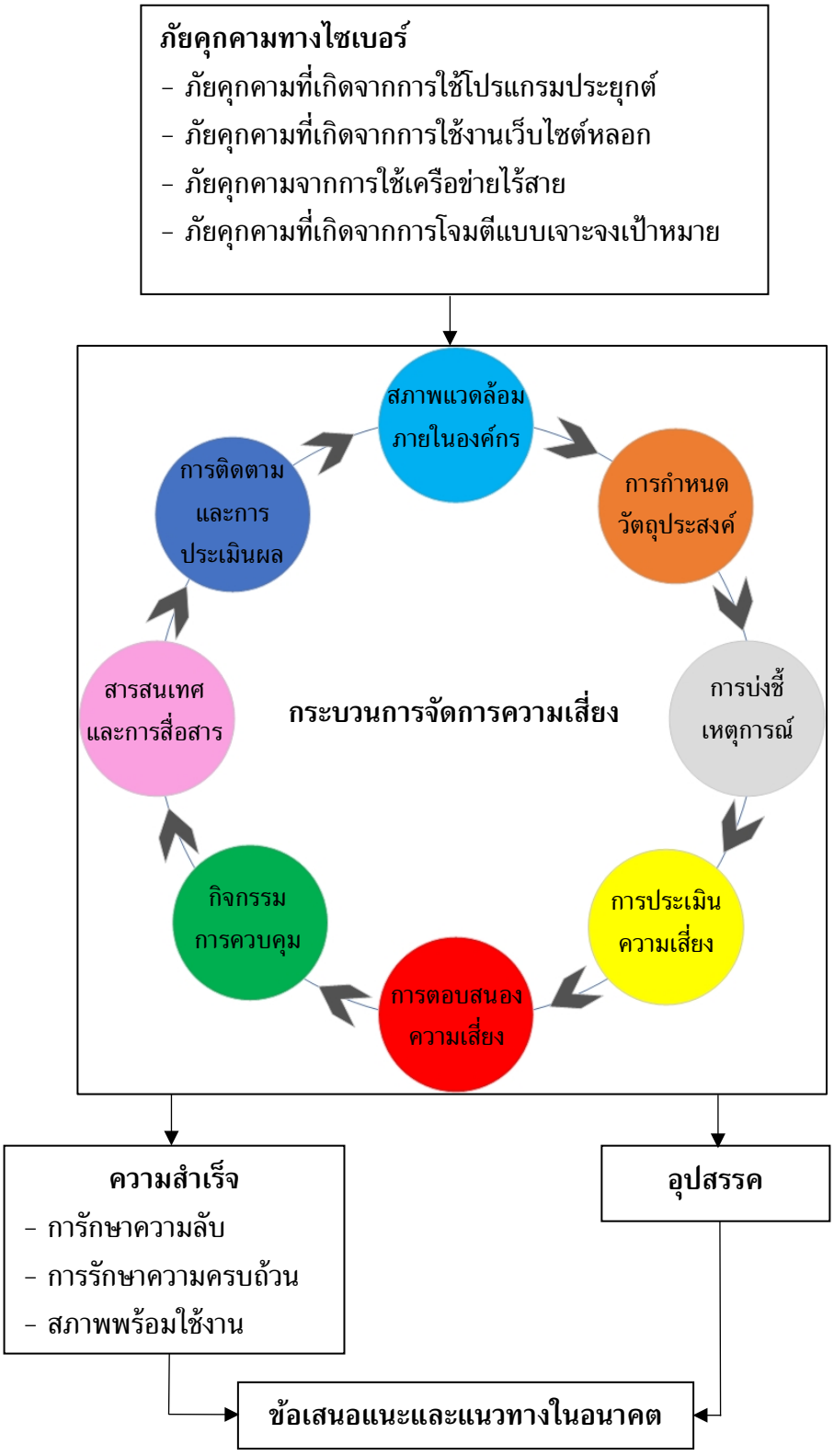
ตาราง 3 งานวิจัยเกี่ยวกับการบริการสาธารณะ

ประเด็นงานวิจัย/นักวิจัย	ด้านการมีส่วนร่วม	ด้านการป้องกันยาเสพติด	ด้านโครงสร้างเชิงเส้นผลการปฏิบัติงานองค์การภาครัฐแรงจูงใจบริการสาธารณะและภาวะผู้นำการ	ด้านจริยธรรมในการให้บริการสาธารณะ	แรงจูงใจในการบริการสาธารณะ
เนตรชนก สูนาสวน,อำนวย บุญรัตนไมตรี, ชัยยงค์ พรหมวงค์ และอนันต์ เตียวต๋อย (2565) ศึกษาการบริการสาธารณะและการมีส่วนร่วมเพื่อการพัฒนาอย่างยั่งยืนของผู้ประกอบการ	✓				
เขมิกา ทองเรือง และ พัณณกร สอนไว (2565) ศึกษาการบริการสาธารณะของกำนันและ ผู้ใหญ่บ้าน ด้านการป้องกันยาเสพติดในชุมชน		✓			
ธีรศานต์ สิกขะโต (2560) ศึกษาความสัมพันธ์โครงสร้างเชิงเส้นผลการปฏิบัติงานองค์การภาครัฐแรงจูงใจบริการสาธารณะและภาวะผู้นำการเปลี่ยนแปลงขององค์การการไฟฟ้าส่วนภูมิภาค			✓		
สถาพร วิชัยรัมย์ ธัญญรัตน์ พุฑฒิพงษ์ ชัยชาญ ภัทรนันท์ เกิดในหล้า และ จุฑารัตน์ จัตุกูล (2562) ศึกษาจริยธรรมในการให้บริการสาธารณะของไทย				✓	

ตาราง 3 งานวิจัยเกี่ยวกับการบริการสาธารณะ (ต่อ)

ประเด็นงานวิจัย/นักวิจัย	ด้านการมีส่วนร่วม	ด้านความโปร่งใสและคอรัปชั่น	ด้านความมั่นคงปลอดภัยไซเบอร์	ด้านความตระหนักรู้และความเข้าใจทางไซเบอร์	ด้านการพัฒนาเทคโนโลยีและนวัตกรรมเพื่อเพิ่มขีดความสามารถในการแข่งขัน
ชวนพิศ เงินฉลาด (2562) ศึกษาแรงจูงใจในการบริการสาธารณะ กรณีศึกษาศูนย์อุตุนิยมวิทยาภาคใต้					✓

2.6 กรอบแนวคิดงานวิจัย



ภาพที่ 1 กรอบแนวคิด

บทที่ 3
วิธีดำเนินการวิจัย

การศึกษาเรื่องการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ในการศึกษาครั้งนี้ ได้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) ประกอบด้วย การวิจัยเอกสาร (Documentary Research) ดังนี้

3.1 ประชากรกลุ่มตัวอย่างและหน่วยงานในพื้นที่ที่ทำการศึกษา

3.2 กลุ่มผู้ให้ข้อมูลสำคัญ

3.3 แบบแผนการวิจัย

3.4 วิธีการเก็บข้อมูลและเครื่องมือที่ใช้ในการวิจัย

3.5 การสร้างเครื่องมือและการตรวจสอบคุณภาพเครื่องมือในการวิจัย

3.6 การวิเคราะห์ข้อมูล

3.7 การพิทักษ์สิทธิของกลุ่มผู้ให้ข้อมูลหลัก

3.1 ประชากรกลุ่มตัวอย่างและหน่วยงานในพื้นที่ที่ทำการศึกษา

หน่วยที่ใช้ในการวิเคราะห์คือ หน่วยงานศาลยุติธรรมในเขตอำนาจผู้พิพากษาภาค 9 โดยแบ่งการวิเคราะห์ข้อมูลออกเป็น 2 กลุ่ม ได้แก่ 1. ศาลจังหวัด ได้แก่ ศาลจังหวัดสงขลา ศาลจังหวัดตรัง ศาลจังหวัดพัทลุง ศาลจังหวัดสตูล ศาลจังหวัดนาทวี ศาลจังหวัดปัตตานี ศาลจังหวัดยะลา ศาลจังหวัดนราธิวาส และศาลจังหวัดเบตง ศาลแขวง ได้แก่ ศาลแขวงสงขลา และศาลแขวงตรัง 2. ศาลเยาวชนและครอบครัว ได้แก่ ศาลเยาวชนครอบครัวจังหวัดสงขลา ศาลเยาวชนและครอบครัวจังหวัดตรัง ศาลเยาวชนและครอบครัวจังหวัดพัทลุง ศาลเยาวชนและครอบครัวจังหวัดสตูล ศาลเยาวชนและครอบครัวจังหวัดปัตตานี ศาลเยาวชนและครอบครัวจังหวัดยะลา และศาลเยาวชนและครอบครัวจังหวัดนราธิวาส ซึ่งมีรายละเอียดข้อมูลเบื้องต้นของพื้นที่หน่วยงานศาลยุติธรรมในเขตอำนาจผู้พิพากษาภาค 9 ในการวิจัยดังต่อไปนี้

ศาลจังหวัดสงขลา ศาลแขวงสงขลา และศาลเยาวชนครอบครัวจังหวัดสงขลา เป็นศาลที่ตั้งอยู่ในตำบ่อยาง อำเภอเมืองสงขลา จังหวัดสงขลา จังหวัดสงขลามีพื้นที่ทางตอนเหนือเป็นคาบสมุทรแคบและยาวยื่นลงมาทางใต้ เรียกว่า คาบสมุทรสทิงพระ กับส่วนที่เป็นแผ่นดินรูปสี่เหลี่ยมผืนผ้าทางตอนใต้ แผ่นดินทั้งสองส่วนเชื่อมต่อกันโดยสะพานติณสูลานนท์ พื้นที่ทางทิศเหนือส่วนใหญ่เป็นราบลุ่ม ทิศตะวันออกเป็นที่ราบริมทะเล ทิศใต้และทิศตะวันตกเป็นภูเขาและที่ราบสูง ซึ่งเป็นแหล่งกำเนิดต้นน้ำลำธารที่สำคัญ จังหวัดสงขลาตั้งอยู่ในเขตอิทธิพลของลมมรสุมเมืองร้อน มีลมมรสุมพัดผ่านประจำทุกปี เริ่มตั้งแต่เดือนตุลาคมถึง

กลางเดือนมกราคม เป็นช่วงลมมรสุมตะวันออกเฉียงเหนือ และเริ่มตั้งแต่กลางเดือนพฤษภาคม ถึงกลางเดือนตุลาคม จะเป็นลมมรสุมตะวันตกเฉียงใต้

ศาลจังหวัดตรัง ศาลแขวงตรัง และศาลเยาวชนและครอบครัวจังหวัดตรัง เป็นศาลที่ตั้งอยู่ในตำบลทับเที่ยง อำเภอเมืองตรัง จังหวัดตรัง จังหวัดตรังมีพื้นที่ส่วนใหญ่โดยทั่วไปจะเป็นเนินสูง ๆ ต่ำ ๆ สลับด้วยภูเขาใหญ่เล็กกระจัดกระจายอยู่ทั่วไป พื้นที่ราบเรียบมีจำนวนน้อย ทางทิศตะวันออกมีเทือกเขาบรรทัดยาวจากเหนือจรดใต้ และเป็นเส้นแบ่งเขตแดนระหว่างจังหวัดตรังกับจังหวัดพัทลุง มีพื้นที่เป็นเกาะจำนวน 46 เกาะอยู่ในพื้นที่อำเภอกันตัง 12 เกาะ อำเภอปะเหลียน 13 เกาะ และอำเภอสิเกา 21 เกาะ มีลักษณะภูมิอากาศอบอุ่น มีฤดูกาลที่สำคัญ 2 ฤดู คือ ฤดูร้อน เริ่มตั้งแต่เดือนกุมภาพันธ์ถึงเดือนกรกฎาคม และฤดูฝน เริ่มตั้งแต่เดือนสิงหาคมถึงเดือนมกราคม

ศาลจังหวัดนราธิวาส เป็นศาลที่ตั้งอยู่ในศูนย์ราชการ และศาลศาลเยาวชนและครอบครัวจังหวัดนราธิวาส ตำบลโคกเคียน อำเภอเมืองนราธิวาส จังหวัดนราธิวาส จังหวัดนราธิวาสมีพื้นที่เป็นป่าและภูเขาประมาณ 2 ใน 3 ของพื้นที่ทั้งหมด มีภูเขาหนาแน่น แถบทิศตะวันตกเฉียงใต้จดเทือกเขาสันกาลาคีรีซึ่งถือเป็นแนวกั้นพรหมแดนไทยมาเลเซีย ลักษณะของพื้นที่มีความลาดเอียงจากทางทิศตะวันตกไปสู่ทิศตะวันออก พื้นที่ราบส่วนใหญ่อยู่บริเวณติดกับอ่าวไทยและที่ราบลุ่มบริเวณแม่น้ำ 3 สาย คือ แม่น้ำสายบุรี แม่น้ำบางนราและแม่น้ำโก-ลก มีฤดูกาล 2 คือ ฤดูร้อน และฤดูฝน

ศาลจังหวัดเบตง เป็นศาลที่ตั้งอยู่ใน อำเภอเบตง จังหวัดยะลา อำเภอเบตงตั้งอยู่ในแนวทิวเขาสันกาลาคีรี มีลักษณะคล้ายหัวหอกพุ่งไปอยู่ในดินแดนประเทศมาเลเซีย มีพื้นที่เป็นที่ราบสูงเนินเขา ลุ่มน้ำ สภาพของเมืองเบตงตั้งอยู่ในหุบเขา มีลักษณะเหมือนแอ่งกระทะที่โอบล้อมด้วยหุบเขาน้อยใหญ่ พื้นที่ทั่วไปสูงกว่าระดับน้ำทะเลประมาณ 1,900 ฟุต ตัวเมืองเบตงอยู่ห่างจากด่านชายแดนเบตงเป็นระยะทาง 7 กิโลเมตร มี 2 ฤดู คือ ฤดูร้อน และฤดูฝน โดยฤดูร้อนอยู่ในช่วงเดือนมกราคมถึงเดือนเมษายน ส่วนฤดูฝนอยู่ในช่วงเดือนพฤษภาคมถึงเดือนธันวาคม

ศาลจังหวัดยะลา และศาลเยาวชนและครอบครัวจังหวัดยะลา เป็นศาลที่ตั้งอยู่ในตำบลตำสะเตง อำเภอเมืองยะลา จังหวัดยะลา จังหวัดยะลามีพื้นที่เป็นป่าเขาเนินสูงและภูเขาเตี้ยสลับซับซ้อนจะมีพื้นที่ราบเพียงเล็กน้อยบริเวณตอนเหนือของจังหวัดส่วนใหญ่เป็นที่ราบลุ่ม มี 2 ฤดู คือ ฤดูร้อน เริ่มตั้งแต่เดือนกุมภาพันธ์ถึงกลางเดือนกรกฎาคม และฤดูฝนเริ่มตั้งแต่กลางเดือนกรกฎาคม ถึงกลางเดือนกุมภาพันธ์

ศาลจังหวัดพัทลุง และศาลเยาวชนและครอบครัวจังหวัดพัทลุง เป็นศาลที่ตั้งอยู่ในตำบลคูหาสวรรค์ อำเภอเมือง จังหวัดพัทลุง จังหวัดพัทลุงมีสภาพพื้นที่เป็นภูเขาและที่ราบสูง ทางด้านตะวันตกอันประกอบด้วย เทือกเขาบรรทัด ทางด้านตะวันออกเป็นที่ราบสลับที่ดอนทิศตะวันตกมาสู่ทิศตะวันออกของจังหวัด ลักษณะภูมิประเทศโดยภาพรวมลาดเทจาก

ที่สูง ด้านทิศตะวันตกไปทางทิศตะวันออกจนถึงทะเลสาบสงขลา มีเพียง 2 ฤดูกาล คือ ฤดูร้อน เริ่มตั้งแต่ปลายเดือนมีนาคม – กลางเดือนกันยายน ฤดูฝน เริ่มตั้งแต่กลางเดือนกันยายน – กลางเดือนมีนาคม

ศาลจังหวัดสตูล และศาลเยาวชนและครอบครัวจังหวัดสตูล เป็นศาลที่ตั้งอยู่ในตำบลพิมาน อำเภอเมืองสตูล จังหวัดสตูล จังหวัดสตูลมีลักษณะเป็นพื้นที่ราบสลับกับภูเขา พื้นที่ทางทิศเหนือและทิศตะวันออกเป็นเนินเขาและภูเขาสูง โดยมีเทือกเขาสำคัญ ๆ คือ ภูเขาสันกาลาคีรี พื้นที่ค่อย ๆ ลาดเอียงลงสู่ทะเลด้านตะวันตก และทิศใต้มีที่ราบแคบ ๆ ขนานไปกับชายฝั่งทะเล ถัดจากที่ราบลงไปเป็นป่าชายเลน น้ำเค็มขึ้นถึงมีป่าแสม หรือป่าโกงกางอยู่เป็นจำนวนมาก นอกจากนั้นจังหวัดสตูลเป็นจังหวัดที่มีลำน้ำสายสั้น ๆ ไหลผ่านซึ่งเกิดจากภูเขาโดยรอบ พื้นที่ทางตอนเหนือและทิศตะวันออกของจังหวัด ประกอบด้วยภูเขามากมายสลับซับซ้อนโดยมีทิวเขานครศรีธรรมราชแบ่งเขตจังหวัดสตูลกับจังหวัดสงขลา และทิวเขาสันกาลาคีรีแบ่งเขตประเทศไทยและประเทศมาเลเซีย นอกจากนั้นยังมีภูเขาน้อยใหญ่อยู่กระจัดกระจายในตอนล่างและชายฝั่งตะวันตก ภูเขาที่สำคัญได้แก่ เขาจีน เขาบารัง เขาหัวกาหมิง เขาใหญ่ เขาทะนาน เขาควนกาหลง และเขาโต๊ะพญาวัง

3.2 กลุ่มผู้ให้ข้อมูลสำคัญ

การวิจัยมีการคัดเลือกผู้ให้ข้อมูลหลัก (Key Informants) โดยใช้วิธีการเลือกแบบเฉพาะเจาะจง (Purposive Sampling) เพื่อได้ตัวอย่างที่เหมาะมากที่สุดสำหรับตอบโจทย์แนวคิดจุดมุ่งหมาย และวัตถุประสงค์ของการศึกษา โดยกลุ่มตัวอย่างที่เลือกมีลักษณะเป็น Information–Rich Case คือมีข้อมูลให้ศึกษาในระดับลึกได้ผู้ให้ข้อมูลหลักที่สำคัญเหมาะสมกับจุดมุ่งหมาย และวัตถุประสงค์ของการศึกษามากที่สุดจนครบถ้วนอิ่มตัว โดยกำหนดคุณสมบัติของผู้ให้ข้อมูลซึ่งผู้ให้ข้อมูลหลักนี้ ต้องมีคุณสมบัติสอดคล้อง โดยแบ่งออกเป็น 2 กลุ่ม ดังนี้

1. เป็นเจ้าหน้าที่ผู้ดูแลระบบ ได้แก่ นักวิชาการคอมพิวเตอร์ หรือพนักงานคอมพิวเตอร์ ประจำหน่วยงานศาลในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
2. เป็นเจ้าหน้าที่ผู้ปฏิบัติงาน ได้แก่ ข้าราชการ พนักงานราชการ และลูกจ้างชั่วคราว ประจำหน่วยงานศาลในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
3. เป็นผู้ปฏิบัติงานไม่น้อยกว่า 1 ปี
4. เป็นผู้มีอายุไม่น้อยกว่า 25 ปี

ทั้งนี้ กลุ่มผู้ให้ข้อมูลหลักแบ่งออกเป็น 2 กลุ่ม โดยมีจำนวนรวมทั้งสิ้น 36 ท่าน ดังตารางต่อไปนี้

ตาราง 4 กลุ่มผู้ให้ข้อมูลหลัก เจ้าหน้าที่ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ปฏิบัติงานศาล แบ่งเป็น 2 กลุ่ม

1.ศาลจังหวัดและศาลแขวง	
กลุ่มผู้ดูแลระบบ ศาลในสังกัดอำนาจอธิบดีผู้พิพากษาภาค 9 จำนวน 11 ท่าน ศาลจังหวัดสงขลา ศาลจังหวัดตรัง ศาลจังหวัดพัทลุง ศาลจังหวัดสตูล ศาลจังหวัดนาทวี ศาลจังหวัดปัตตานี ศาลจังหวัดยะลา ศาลจังหวัดนราธิวาส ศาลแขวงสงขลา ศาลแขวงตรัง	กลุ่มเจ้าหน้าที่ผู้ปฏิบัติงาน ศาลในสังกัดอำนาจอธิบดีผู้พิพากษาภาค 9 จำนวน 11 ท่าน ศาลจังหวัดสงขลา ศาลจังหวัดตรัง ศาลจังหวัดพัทลุง ศาลจังหวัดสตูล ศาลจังหวัดนาทวี ศาลจังหวัดปัตตานี ศาลจังหวัดยะลา ศาลจังหวัดนราธิวาส ศาลแขวงสงขลา ศาลแขวงตรัง
2.ศาลเยาวชนและครอบครัว	
กลุ่มผู้ดูแลระบบ ศาลในสังกัดอำนาจอธิบดีผู้พิพากษาภาค 9 จำนวน 7 ท่าน ศาลเยาวชนและครอบครัวจังหวัดสงขลา ศาลเยาวชนและครอบครัวจังหวัดตรัง ศาลเยาวชนและครอบครัวจังหวัดพัทลุง ศาลเยาวชนและครอบครัวจังหวัดสตูล ศาลเยาวชนและครอบครัวจังหวัดปัตตานี ศาลเยาวชนและครอบครัวจังหวัดยะลา ศาลเยาวชนและครอบครัวจังหวัดนราธิวาส	กลุ่มเจ้าหน้าที่ผู้ปฏิบัติงาน ศาลในสังกัดอำนาจอธิบดีผู้พิพากษาภาค 9 จำนวน 7 ท่าน ศาลเยาวชนและครอบครัวจังหวัดสงขลา ศาลเยาวชนและครอบครัวจังหวัดตรัง ศาลเยาวชนและครอบครัวจังหวัดพัทลุง ศาลเยาวชนและครอบครัวจังหวัดสตูล ศาลเยาวชนและครอบครัวจังหวัดปัตตานี ศาลเยาวชนและครอบครัวจังหวัดยะลา ศาลเยาวชนและครอบครัวจังหวัดนราธิวาส

โดยไม่สามารถเก็บข้อมูลจากผู้ให้ข้อมูลหลักผู้ดูแลระบบศาลแขวงสงขลา เนื่องจากไม่สามารถเข้าถึงผู้ให้สัมภาษณ์ เนื่องจากมีผู้ที่ให้ข้อมูลหลักไม่ประสงค์ที่จะให้ข้อมูล จึงขอปรับผู้ให้ข้อมูลหลักเป็นเจ้าหน้าที่ที่ถูกแต่งตั้งเป็นเจ้าหน้าที่ด้านดิจิทัลประจำหน่วยงาน

3.3 แบบแผนการวิจัย

ในการศึกษานี้ใช้แบบแผนการวิจัยโดยอาศัยแหล่งข้อมูล 2 ประเภทคือ ข้อมูลปฐมภูมิ (Primary Data) และข้อมูลทุติยภูมิ (Secondary Data) ดังนี้

3.3.1 ข้อมูลปฐมภูมิ (Primary Data) เป็นการเลือกผู้ให้ข้อมูลสำคัญของการวิจัยครั้งนี้ โดยใช้เกณฑ์ที่ครอบคลุมของหน่วยงานศาลในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 เพื่อบอกข้อมูลที่เกิดขึ้นและให้มีความถูกต้องของข้อมูลมากที่สุด ด้วยการสัมภาษณ์เชิงลึก โดยผู้ให้ข้อมูลสำคัญในการวิจัยครั้งนี้ประกอบด้วยบุคคลต่าง ๆ ดังนี้ เจ้าหน้าที่ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ปฏิบัติงานที่ท้างานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 เพื่อให้ทราบถึงการแนวปฏิบัติการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ

3.3.2 ข้อมูลทุติยภูมิ (Secondary Data) เป็นข้อมูลที่ได้จากการศึกษาการทบทวนหนังสือบทความวิชาการ เอกสารงานวิจัยทางวิชาการที่เกี่ยวข้อง เช่น แผนบริหารจัดการความเสี่ยงสำนักงานศาลยุติธรรม ประจำปีงบประมาณ พ.ศ.2565 แนวคิดเกี่ยวกับภัยคุกคามไซเบอร์ แนวคิดการจัดการความเสี่ยง แนวคิดความมั่นคงปลอดภัยทางไซเบอร์ แนวคิดการบริการสาธารณะของหน่วยงานศาลยุติธรรมเอกสารงานวิจัยที่เกี่ยวข้อง เพื่อนำมากำหนดกรอบแนวคิดและวิธีการวิจัยที่เกี่ยวข้องดังที่ได้ทบทวนเรียบเรียงไว้ในบทที่สอง

3.4 วิธีการเก็บข้อมูลและเครื่องมือที่ใช้ในการวิจัย

การศึกษาวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยวิธีการเก็บรวบรวมข้อมูลจากการวิจัยเอกสาร (Documentary Research) ด้วยเครื่องมือ การเก็บรวบรวมข้อมูลจากเอกสาร (Documentary Research) การสัมภาษณ์เชิงลึก (In-Depth Interview) เพื่อศึกษาการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานรัฐ ใช้วิธีการเก็บข้อมูลและเครื่องมือวิจัยดังต่อไปนี้

วิธีที่ 1 เก็บรวบรวมข้อมูลจากเอกสาร (Documentary Research) ผู้วิจัยได้ทำการศึกษาและรวบรวมข้อมูลจากหนังสือ ภาพถ่าย เอกสารราชการ บทความ วิทยานิพนธ์ และเอกสารงานวิจัยที่เกี่ยวข้อง เกี่ยวกับ แนวคิดเกี่ยวกับภัยคุกคามไซเบอร์ แนวคิดการจัดการความเสี่ยง แนวคิดความมั่นคงปลอดภัยทางไซเบอร์ แนวคิดการบริการสาธารณะของหน่วยงานศาลยุติธรรม แผนบริหารจัดการความเสี่ยงสำนักงานศาลยุติธรรม ประจำปี พ.ศ. 2565 และงานเอกสารวิจัยที่เกี่ยวข้อง

วิธีที่ 2 การสัมภาษณ์เชิงลึก (In-Depth Interview) ใช้แนวคำถามแบบกึ่งโครงสร้างปลายเปิดที่ผู้วิจัยสร้างขึ้นจากการทบทวนวรรณกรรมต่าง ๆ ที่เกี่ยวข้อง โดยรวบรวมข้อมูลจากผู้ให้ข้อมูลหลัก (Key Informants) มาจากการเลือกแบบเฉพาะเจาะจง (Purposive

Sampling) ประกอบด้วยเจ้าหน้าที่ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ปฏิบัติงานศาล ในสังกัดอำนาจอธิบดีผู้พิพากษาภาค 9 โดยพื้นที่ในการเก็บข้อมูลคือ หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

3.5 การสร้างเครื่องมือและการตรวจสอบคุณภาพเครื่องมือในการวิจัย

ผู้วิจัยได้ทำการสร้างและตรวจสอบคุณภาพเครื่องมือการวิจัยเชิงคุณภาพดังนี้

1) ศึกษาแนวคิดเกี่ยวกับการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ โดยนำกรอบแนวคิดมาใช้เป็นตัวแบบในการศึกษาการและปรับ

2) นำข้อมูลที่รวบรวมได้มาสร้างเป็นข้อคำถามเพื่อใช้ในการสัมภาษณ์เจ้าหน้าที่ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ปฏิบัติงานศาล ในสังกัดอำนาจอธิบดีผู้พิพากษาภาค 9

3) นำเครื่องมือที่สร้างเสร็จเสนอต่ออาจารย์ที่ปรึกษา เพื่อตรวจสอบ เสนอแนะและปรับปรุงแก้ไข

4) คุณภาพของเครื่องมือในเรื่องของความเชื่อใจ (Dependability) ให้ผู้เชี่ยวชาญเป็นผู้ตรวจสอบ ซึ่งผู้เชี่ยวชาญในงานวิจัยนี้ได้ให้ผู้ทรงคุณวุฒิเป็นผู้ตรวจสอบ ส่วนประเด็นการถ่ายโอน (Transferability) ได้แสดงรายละเอียดในเรื่องของสถานที่บริบท และสภาพแวดล้อม

3.6 การวิเคราะห์ข้อมูล

การวิจัยนี้ได้ทำการวิเคราะห์ข้อมูลแบบเชิงคุณภาพดังนี้

1) ทำการวิเคราะห์ข้อมูลโดยใช้กระบวนการวิเคราะห์ข้อมูลและการตีความข้อมูลแบบอุปนัย (Analytic Induction) คือการตีความการสร้างข้อสรุปจากข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก (In-Depth Interview) เพื่อทำการศึกษากลุ่มเจ้าหน้าที่ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ปฏิบัติงานศาล ในสังกัดอำนาจอธิบดีผู้พิพากษาภาค 9 เพื่อศึกษาการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์สู่รูปแบบแนวปฏิบัติในการปรับปรุงการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

2) ทำการวิเคราะห์ข้อมูลที่เป็นบทสัมภาษณ์เชิงลึก กลุ่มเจ้าหน้าที่ผู้ดูแลระบบและเจ้าหน้าที่ผู้ปฏิบัติงานศาล ในสังกัดอำนาจอธิบดีผู้พิพากษาภาค 9 โดยการหารูปแบบของข้อความเพื่อจัดกลุ่มข้อความที่เนื้อหาหรือนัยยะ ความหมายที่คล้ายคลึงกัน (Thematic Analysis)

ทั้งนี้ ได้มีการตรวจสอบข้อคำถามกับวัตถุประสงค์การวิจัยดังตาราง 5 ดังนี้

ตาราง 5 ตรวจสอบความสอดคล้องข้อคำถามกับวัตถุประสงค์การวิจัย

วัตถุประสงค์การวิจัย	คำถามที่ใช้ในการสัมภาษณ์	ผู้ให้ข้อมูลหลัก	
		เจ้าหน้าที่ผู้ดูแลระบบ	เจ้าหน้าที่ศาล ผู้ปฏิบัติงาน
1. เพื่อศึกษาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9	1. ศาลของท่านมีปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์อย่างไรบ้าง	✓	✓
	2. ศาลของท่านมีขั้นตอนหรือเครื่องมือในการจัดการภัยคุกคามไซเบอร์อย่างไรบ้าง	✓	
	3. ศาลของท่านมีแนวทางหรือมาตรการจัดการภัยคุกคามไซเบอร์อย่างไรบ้าง	✓	✓
2. เพื่อศึกษาความสำเร็จและอุปสรรคในการดำเนินงานด้านการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9	4. ศาลของท่านมีความสำเร็จการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ใน1. ความถูกต้องแม่นยำ 2. ความทันเวลา 3. ความปลอดภัย	✓	✓
	5. ศาลของท่านมีปัญหาอุปสรรคในการดำเนินงานเพื่อจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ ด้านงบประมาณ ด้านทักษะบุคลากรและจำนวนบุคลากรทางด้านไซเบอร์ ด้านนโยบายของหน่วยงาน และด้านระเบียบหรือกฎหมายที่เกี่ยวข้อง อย่างไรบ้าง	✓	✓
3. เพื่อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9	6. ข้อคิดเห็นและเสนอแนะอื่น ๆ	✓	✓

3.7 การพิทักษ์สิทธิของกลุ่มผู้ให้ข้อมูลหลัก

1. เคารพและไม่ล่วงละเมิดสิทธิมนุษยชนของผู้ให้ข้อมูลโดยผู้วิจัยขอความยินยอมจากผู้ให้ข้อมูลผู้วิจัยและได้อธิบายถึงวัตถุประสงค์ของการวิจัย ขั้นตอนต่าง ๆ ในการดำเนินการวิจัย ในการจดบันทึกเปิดโอกาสให้ซักถามผู้วิจัยได้ตลอดจนถึงการตัดสินใจอย่างอิสระที่จะยินยอมหรือปฏิเสธการให้ข้อมูล โดยที่ไม่ส่งผลกระทบใด ๆ ต่อผู้ให้ข้อมูลทั้งสิ้น

2. คำนึงการให้เกียรติและความรู้สึกของผู้ให้ข้อมูลรวมถึงการแสดงออกในความจริงใจต่อผู้ให้ข้อมูล

บทที่ 4
ผลการวิจัย

การศึกษาเรื่องการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 เป็นการวิจัยเชิงคุณภาพ ใช้การสัมภาษณ์เชิงลึก สัมภาษณ์เจ้าหน้าที่ผู้ดูแลระบบ และผู้ปฏิบัติงานศาล ในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 โดยผลการศึกษาแบ่งออกเป็น 4 ประเด็น ดังนี้

1. ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
2. เครื่องมือ มาตรการ และแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
3. ความสำเร็จและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
4. เสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ผลการวิเคราะห์ข้อมูล

4.1 ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

จากการลงพื้นที่สัมภาษณ์เชิงลึก พบว่าปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 สามารถสรุป ได้ดังนี้

4.1.1 การใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด

จากการสัมภาษณ์หนึ่งในปัจจัยเสี่ยงจากการดาวน์โหลดโปรแกรมประยุกต์หรือไดร์เวอร์เพื่อมาใช้งานเป็นช่องทางที่ทำให้เกิดความเสี่ยงจากภัยคุกคามไซเบอร์ได้ ดังคำสัมภาษณ์ตัวแทนผู้ให้ข้อมูลหลักดังต่อไปนี้

“...มีการดาวน์โหลดไดร์เวอร์อุปกรณ์ที่ต้องติดตั้งโปรแกรมที่อาจจะมีโฆษณาหรือลิงค์เด้งขึ้นมาซึ่งอาจแฝงภัยมาด้วย...”

(ผู้ให้ข้อมูลหลักคนที่ 8, 28 ธันวาคม 2565 : สัมภาษณ์)

“...เจ้าหน้าที่มีการติดตั้งโปรแกรมแปลก ๆ เข้ามาในเครื่องคอมพิวเตอร์...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...การดาวน์โหลดโปรแกรมมาติดตั้งอาจทำให้ผู้ไม่หวังดีแฝงมัลแวร์หรือไวรัสมาด้วย...”

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

4.1.2 การใช้เครือข่ายไร้สาย

ความเสี่ยงนึง จากกรณีเจ้าหน้าที่นำอุปกรณ์ส่วนตัว ได้แก่ คอมพิวเตอร์หรือมือถือมาเชื่อมต่อกับระบบเครือข่ายไร้สายของหน่วยงานทำให้อุปกรณ์ข้างต้นเชื่อมโยงกับระบบภายในหน่วยงานเกิดความเสี่ยงจากภัยคุกคามไซเบอร์ ได้ดังคำสัมภาษณ์ของผู้ให้ข้อมูลหลักดังนี้

“...การใช้งานอุปกรณ์สื่อสารส่วนตัวที่ใช้อินเตอร์เน็ต เช่นโทรศัพท์มือถือหรือเครื่องคอมพิวเตอร์โน๊ตบุ๊คของเจ้าหน้าที่ที่นำมาใช้งานอื่นเชื่อมต่อเครือข่ายไร้สายและใช้งานในระบบเครือข่ายภายใน...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

4.1.3 สภาพแวดล้อม

ปัจจัยความเสี่ยงจากสภาพแวดล้อมอันได้แก่ ระบบไฟฟ้าขัดข้อง อุณหภูมิไม่เหมาะสม ความชื้นจากเครื่องปรับอากาศ พื้นที่ก่อสร้างโครงสร้างพื้นฐาน ซึ่งจากการสัมภาษณ์ ตัวแทนของผู้ให้ข้อมูลหลักได้กล่าวถึงเรื่องระบบไฟฟ้าขัดข้อง ดังนี้

ระบบไฟฟ้าขัดข้อง

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลเกี่ยวกับปัจจัยเสี่ยงระบบไฟฟ้าขัดข้องส่งผลต่ออุปกรณ์ดังนี้

“...ด้านอุปกรณ์ ระบบไฟฟ้าขัดข้อง ไฟกระชาก ทำให้ข้อมูลไม่ถูกต้อง...”

(ผู้ให้ข้อมูลหลักคนที่ 13, 3 มกราคม 2566 : สัมภาษณ์)

“...ระบบไฟฟ้าขัดข้อง ไฟกระชาก ส่งผลทำให้อุปกรณ์ชำรุด ทำให้เกิดช่องโหว่และทำให้ข้อมูลไม่ถูกต้อง...”

(ผู้ให้ข้อมูลหลักคนที่ 23, 14 มกราคม 2566 : สัมภาษณ์)

“...ระบบไฟฟ้าขัดข้อง ไฟกระชาก ส่งผลทำให้อุปกรณ์ไฟล์วอลชำรุด ทำให้เกิดช่องโหว่...”

(ผู้ให้ข้อมูลหลักคนที่ 33, 4 กุมภาพันธ์ 2566 : สัมภาษณ์)

4.1.4 การโจมตีแบบไม่ตั้งใจ

ประเด็นปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์จากการโจมตีแบบไม่ตั้งใจของหน่วยงานศาลยุติธรรมในดเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีดังต่อไปนี้

การเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานและบุคคลอื่น

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลเกี่ยวกับปัจจัยเสี่ยงที่จากภัยคุกคามไซเบอร์จากการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานและบุคคลอื่น โดยใช้งานระบบขาดความระมัดระวังในการเข้าระบบ ออกจากระบบหรือส่งต่อข้อมูล ก็เป็นช่องโหว่ที่เป็นปัจจัยเสี่ยง โดยการให้สัมภาษณ์ตัวแทนของกลุ่มผู้ให้ข้อมูลของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 หลักดังนี้

“...การที่ผู้ใช้งานระบบเข้าสู่ระบบและไม่ได้ออกจากระบบอาจมีบุคคลอื่นเข้ามาใช้งานต่อและสามารถที่จะรู้ข้อมูลส่วนบุคคลของผู้ใช้งาน...”

(ผู้ให้ข้อมูลหลักคนที่ 2, 20 ธันวาคม 2565 : สัมภาษณ์)

“...การรั่วไหลของข้อมูล เช่น ตำรวจ ขอข้อมูล ส่งข้อมูลเป็นไฟล์ทางอีเมลหรือส่งทางไลน์ส่วนตัวหรือกลุ่ม โซเชียล...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

“...ผู้ใช้ล็อคอินแล้วไม่ได้ล็อคเอาท์ ทำให้เข้าถึงข้อมูลของบุคคลอื่นได้ ทำให้คนอื่นได้รับความเสียหายได้ ล่วงรู้ข้อมูลในคดี หรือการที่มาเปิดข้อมูลแล้วไม่ปิด...”

(ผู้ให้ข้อมูลหลักคนที่ 18, 10 มกราคม 2566 : สัมภาษณ์)

ขาดแคลนบุคลากรผู้ปฏิบัติงานด้านไซเบอร์

ปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์ที่เกิดจากการขาดแคลนบุคลากรผู้ปฏิบัติงานด้านไซเบอร์ ถ้าผู้ใช้งานไม่ระวังหรือกระทำการใด ๆ โดยไม่ทราบผลกระทบหรือเกิดเหตุการณ์แล้วจะปรึกษาหรือให้บุคลากรดังกล่าวแก้ปัญหาให้ ก็จะมีผลให้การแก้ไขปัญหาล่าช้าหรือการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์มีความเสี่ยงเพิ่มมากขึ้น โดยผู้ให้ข้อมูลหลักทั้งหมดให้ความเห็นว่าการขาดแคลนบุคลากรผู้ปฏิบัติงานด้านไซเบอร์เป็นปัจจัยความเสี่ยงตามคำให้สัมภาษณ์ของตัวแทนผู้ให้ข้อมูลหลักดังต่อไปนี้

“...การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก...”

(ผู้ให้ข้อมูลหลักคนที่ 1, 20 ธันวาคม 2565 : สัมภาษณ์)

“...ขาดแคลนบุคลากรด้านไซเบอร์ มีคนเดียว ทำให้ไม่ทันกับการแก้ไขปัญหาต่าง ๆ...”

(ผู้ให้ข้อมูลหลักคนที่ 23, 14 มกราคม 2566 : สัมภาษณ์)

“...มีจำนวนนักวิชาการคอมพิวเตอร์ไม่เพียงพอต่อการดูและระบบ...”

(ผู้ให้ข้อมูลหลักคนที่ 28, 23 มกราคม 2566 : สัมภาษณ์)

การนำเอาอุปกรณ์อื่นมาเชื่อมต่อระบบคอมพิวเตอร์

หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 เป็นหน่วยงานอำนวยความยุติธรรม ดังนั้นการให้บริการคู่ความหรือเจ้าหน้าที่ผู้ปฏิบัติงานศาล มีการนำอุปกรณ์ แฟลชไดร์ฟมาเชื่อมต่อกับระบบคอมพิวเตอร์ ซึ่งจะทำให้มีความเสี่ยงจากไวรัสเข้ามา

ในระบบได้ จากการสัมภาษณ์ผู้ให้ข้อมูลหลัก จากตัวแทนให้ข้อมูลเกี่ยวกับปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์จากการนำเอาอุปกรณ์อื่นมาเชื่อมต่อระบบคอมพิวเตอร์

"...คู่ความ และเจ้าหน้าที่หน่วยงานในกระบวนการยุติธรรมใช้แฟลชไดร์ฟ..."

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

"...เจ้าหน้าที่ศาล เอาแฟลชไดร์ฟจากที่บ้านเข้ามาใช้ที่ทำงาน..."

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

"...คู่ความ นำไฟล์ใส่ใน แฟลชไดร์ฟ มาให้เจ้าหน้าที่เปิดที่เครื่องคอมพิวเตอร์ของศาลในห้องพิจารณาคดี..."

(ผู้ให้ข้อมูลหลักคนที่ 29, 28 มกราคม 2566 : สัมภาษณ์)

การตั้งรหัสผ่านและการเก็บรักษารหัสผ่านระบบ

ปัจจัยเสี่ยงที่มากจากผู้ใช้งานระบบเองก็คือ การตั้งรหัสผ่านควรจะเป็นรหัสที่คาดเดาได้ยากและในส่วนของการเก็บรักษารหัสผ่านระบบก็ควรให้เป็นความลับซึ่งในหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค **9** ยังมีการแปะรหัสผ่านไว้หน้าจอคอมพิวเตอร์ซึ่งทำให้เกิดความเสี่ยงได้ ดังการให้คำสัมภาษณ์ดังนี้

"...ผู้ใช้แปะรหัสผ่านไว้หน้าจอ หรือให้จำรหัสระบบไว้ที่หน้าจอคอมพิวเตอร์..."

(ผู้ให้ข้อมูลหลักคนที่ 20, 12 มกราคม 2566 : สัมภาษณ์)

"...มีเจ้าหน้าที่ที่มีอายุแปะรหัสผ่านการใช้งานระบบไว้หน้าจอคอมพิวเตอร์..."

(ผู้ให้ข้อมูลหลักคนที่ 30, 28 มกราคม 2566 : สัมภาษณ์)

"...มีเจ้าหน้าที่มีบางคนแปะรหัสผ่านการใช้งานระบบไว้หน้าจอคอมพิวเตอร์เพื่อความสะดวก หรือเพื่อให้ผู้ที่ทำงานแทน..."

(ผู้ให้ข้อมูลหลักคนที่ 34, 4 กุมภาพันธ์ 2566 : สัมภาษณ์)

การเข้าลิงค์จากอีเมล และการเข้าเว็บไซต์

การเข้าลิงค์จากอีเมล และการเข้าเว็บไซต์ก็เป็นช่องทางนึงที่เป็นปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์ มีการโจมตีผ่านช่องทางเหล่านี้ได้ ซึ่งจากการสัมภาษณ์ผู้ให้ข้อมูลหลักเกี่ยวกับปัจจัยเสี่ยงจากการเข้าลิงค์จากอีเมล และการเข้าเว็บไซต์ มีดังนี้

"...เจ้าหน้าที่เข้าเมลศาลแล้วมีลิงค์ให้กดเข้าไปทำให้เกิดความเสี่ยง..."

(ผู้ให้ข้อมูลหลักคนที่ 5, 27 ธันวาคม 2565 : สัมภาษณ์)

"...เป็นการหลอกเป้าหมายเข้าถึงข้อมูลส่วนบุคคล พวกเว็บไซต์หลอก..."

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

"...เจ้าหน้าที่เข้าใช้เว็บไซต์ไม่พึงประสงค์ ดูหนังออนไลน์ มีเว็บโฆษณา ผู้ไม่หวังดีวางตัวมัลแวร์ไวรัสแฝงมาด้วย..."

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

“...เจ้าหน้าที่เข้าเว็บไซต์แล้วมีหน้าจอ Popup ขึ้นมาแสดง หรือเข้าเว็บอื่น ๆ แล้วมีโฆษณาต่าง ๆ ขึ้นมา...”

(ผู้ให้ข้อมูลหลักคนที่ 35, 14 กุมภาพันธ์ 2566 : สัมภาษณ์)

คอมพิวเตอร์สำหรับใช้ปฏิบัติงานไม่เพียงพอ

ในส่วนคอมพิวเตอร์ที่ไม่เพียงพอต่อการใช้งานทำให้หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ต้องนำเครื่องคอมพิวเตอร์ที่ถูกทดแทนแล้วมาใช้งาน ซึ่งจะทำให้เครื่องไม่สามารถปรับปรุงระบบปฏิบัติการได้ทำให้เกิดช่องโหว่ หรือการใช้งานร่วมกันของเจ้าหน้าที่ก็อาจทำให้หลงลืมในการใช้รหัสผู้ใช้ของตนเองไปใช้รหัสผู้ใช้ของผู้อื่น ดังการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลเกี่ยวกับคอมพิวเตอร์สำหรับใช้ปฏิบัติงานไม่เพียงพอดังนี้

“...คอมพิวเตอร์ไม่เพียงพอ นำคอมเก่ามาใช้วินโดว์ไม่อัพเดต...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...คอมพิวเตอร์ไม่เพียงพอ ทำให้มีการใช้งานหลายคนทำให้มีการบันทึกผู้ปฏิบัติงานทำหน้าที่ในนาม User และ Password ของอีกคน...”

(ผู้ให้ข้อมูลหลักคนที่ 12, 3 มกราคม 2566 : สัมภาษณ์)

คอมพิวเตอร์บริการคู่ความเชื่อมไปยังเครื่องคอมพิวเตอร์แม่ข่าย

สำหรับคอมพิวเตอร์ที่ให้บริการคู่ความ มีการเชื่อมต่อฐานข้อมูลไปยังเครื่องคอมพิวเตอร์แม่ข่ายซึ่งทำให้บุคคลผู้มีความรู้ด้านระบบคอมพิวเตอร์อาจเข้าไปแก้ไขหรือเจาะเข้าระบบเครื่องคอมพิวเตอร์แม่ข่ายได้ จากการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลเกี่ยวกับปัจจัยเสี่ยงที่จากภัยคุกคามไซเบอร์จากคอมพิวเตอร์บริการคู่ความเชื่อมไปยังเครื่องคอมพิวเตอร์แม่ข่ายดังนี้

“...อุปกรณ์คอมพิวเตอร์ของหน่วยงานบริการประชาชน เชื่อมต่อผ่านระบบเครือข่ายภายใน สามารถเข้าถึง Server ถ้าผู้มีความรู้ทางคอมพิวเตอร์ก็จะสามารถเข้าถึงฐานข้อมูลหรือจัดการกับข้อมูลได้...”

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

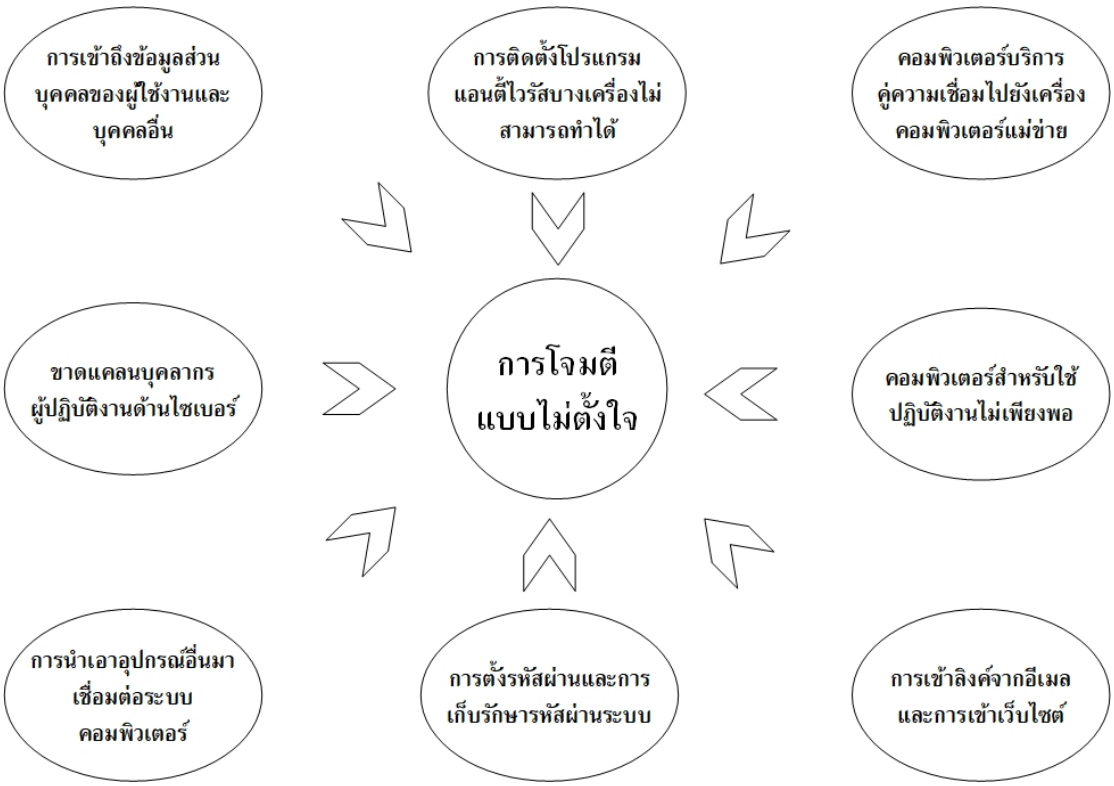
การติดตั้งโปรแกรมแอนตี้ไวรัสบางเครื่องไม่สามารถทำได้

ในส่วนคอมพิวเตอร์ที่ถูกทดแทนแล้วจะไม่สามารถติดตั้งแอนตี้ไวรัสที่มีลิขสิทธิ์ได้ จึงทำให้เครื่องคอมพิวเตอร์ดังกล่าวมีความเสี่ยงจากภัยคุกคามไซเบอร์ดังการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลเกี่ยวกับปัจจัยเสี่ยงที่จากภัยคุกคามไซเบอร์จากการติดตั้งโปรแกรมแอนตี้ไวรัสบางเครื่องไม่สามารถทำได้ดังนี้

“...การติดตั้งโปรแกรมสแกนไวรัสบนเครื่องคอมพิวเตอร์บางเครื่องไม่สามารถทำได้...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

กล่าวโดยสรุปปัจจัยเสี่ยงจากภัยคุกคามทางไซเบอร์ในส่วนการโจมตีแบบไม่ตั้งใจเกิดจากเจ้าหน้าที่ศาลที่ขาดความรู้ในการปฏิบัติงาน และขาดความตระหนักรู้ ได้แก่ การเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานและบุคคลอื่น เช่น การลืมล็อกเอาท์ออกจากระบบ การส่งต่อข้อมูลทางออนไลน์ที่ไม่มีความปลอดภัย เป็นต้น ในส่วนการขาดแคลนบุคลากรผู้ปฏิบัติงานด้านไซเบอร์ ถ้าเกิดปัญหาแล้วไม่สามารถแก้ไขได้ทันก็ทำให้เกิดปัญหาหรือความเสี่ยงมากขึ้นได้ การนำเอาอุปกรณ์อื่นมาเชื่อมต่อระบบคอมพิวเตอร์ เช่น แฟลชไดร์ฟ เป็นสื่อในการนำเอาไวรัสแฝงเข้ามาในระบบได้ ส่วนการตั้งรหัสผ่านและการเก็บรักษารหัสผ่านระบบ ถ้าตั้งรหัสที่คาดเดาได้ง่ายหรือแปะรหัสไว้ที่หน้าจอเพื่อความสะดวก ก็จะทำให้เกิดช่องโหว่ได้เช่นกัน การเข้าลิงค์จากอีเมล และการเข้าเว็บไซต์ถ้าเจ้าหน้าที่ขาดความรู้คลิกไปโดยไม่ระวังจะทำให้ระบบเกิดความเสี่ยงจากเข้าลิงค์อีเมลหรือเว็บไซต์นั้น ๆ ได้เช่นกัน คอมพิวเตอร์สำหรับใช้ปฏิบัติงานไม่เพียงพอที่ต้องไปนำเครื่องคอมพิวเตอร์ทดแทนแล้วมาใช้ทำให้เกิดช่องโหว่ของระบบคอมที่ไม่สามารถปรับปรุงเป็นรุ่นล่าสุดได้ คอมพิวเตอร์บริการคู่ความเชื่อมไปยังเครื่องคอมพิวเตอร์แม่ข่ายจะทำให้เครื่องคอมพิวเตอร์แม่ข่ายมีความเสี่ยงได้เช่นกัน ถ้าผู้ใช้งานมีทักษะด้านระบบคอมพิวเตอร์ และการติดตั้งโปรแกรมแอนตี้ไวรัสบางเครื่องไม่สามารถทำได้เนื่องด้วยเป็นคอมพิวเตอร์ที่ถูกทดแทนแล้ว จึงต้องไปใช้โปรแกรมฟรีซึ่งไม่สามารถป้องกันได้ดี ซึ่งปัจจัยดังกล่าวเป็นช่องโหว่ที่ทำให้เกิดภัยคุกคามทางไซเบอร์ได้ ดังภาพประกอบ 2



ภาพประกอบ 2 การโจมตีแบบไม่ตั้งใจ

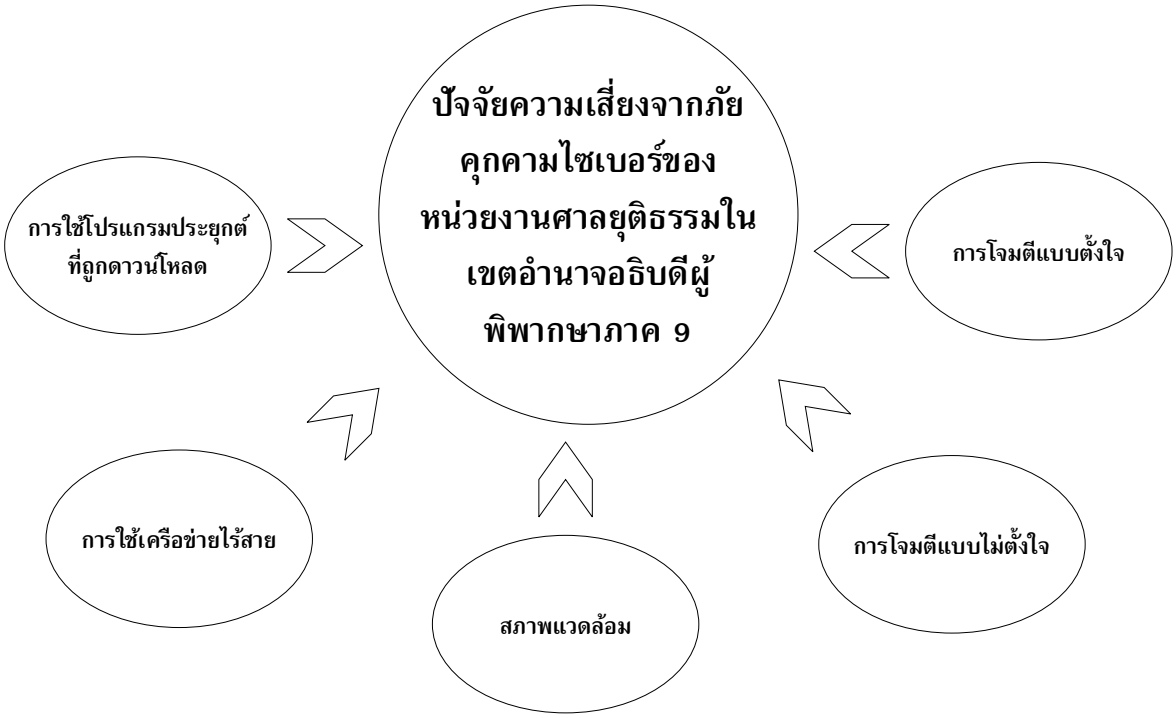
4.1.5 การโจมตีแบบตั้งใจ

ในยุคปัจจุบันการรูปแบบภัยคุกคามทางไซเบอร์มาในแบบการโจมตีแบบตั้งใจซึ่งจะเห็นได้หลาย ๆ เหตุการณ์ที่เกิดขึ้นสำหรับศาลยุติธรรมนั้นเคยถูกเจาะระบบมาแล้วเมื่อปี 2559 ซึ่งจะเข้ากับบทสัมภาษณ์ของผู้ให้สัมภาษณ์หลักดังนี้

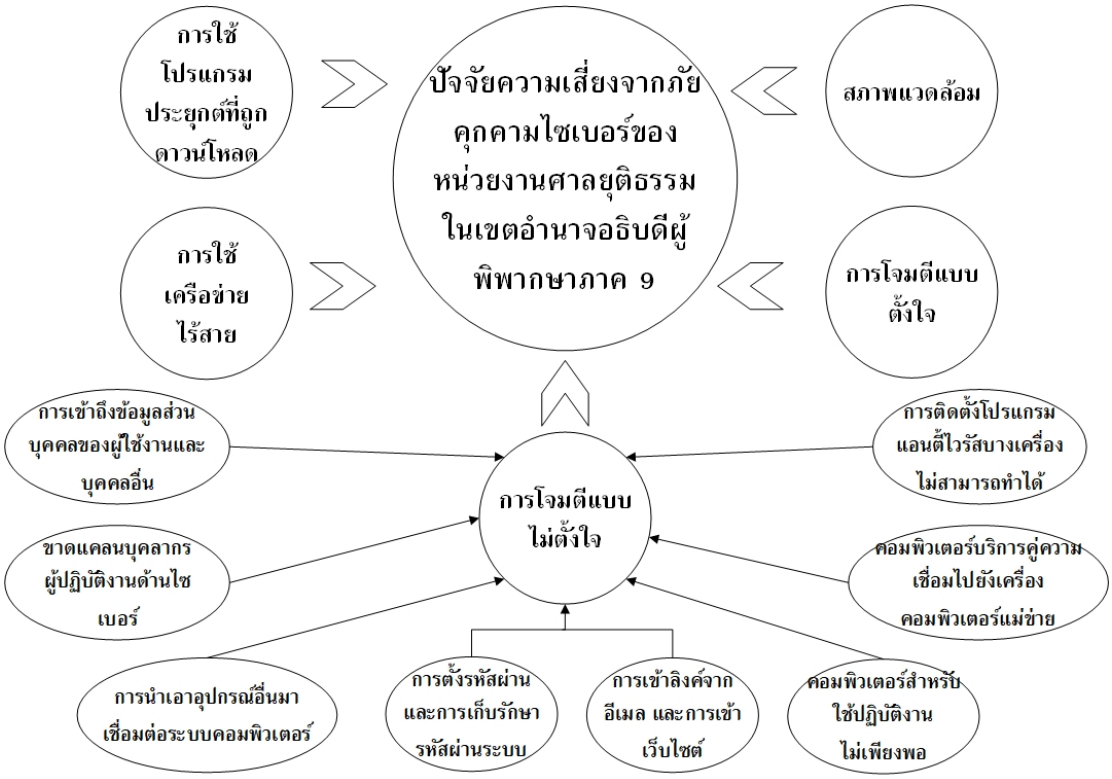
“...ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี...”

(ผู้ให้ข้อมูลหลักคนที่ 2, 20 ธันวาคม 2565 : สัมภาษณ์)

กล่าวโดยสรุปปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีอยู่ 5 ประเภท ได้แก่ การใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด การใช้เครือข่ายไร้สาย สภาพแวดล้อม การโจมตีแบบไม่ตั้งใจ โดยปัจจัยที่เกิดการโจมตีแบบไม่ตั้งใจมักจะเกิดจากเจ้าหน้าที่ศาลที่ขาดความรู้ในการปฏิบัติงาน หรือขาดความตระหนักรู้ในเรื่องความเสี่ยงจากภัยคุกคามไซเบอร์ ซึ่งมีได้หลายปัจจัย ดังนั้นการที่เจ้าหน้าที่ได้รับความรู้และมีความตระหนักในเรื่องความเสี่ยงจากภัยคุกคามไซเบอร์จึงเป็นสิ่งสำคัญ และสุดท้ายเป็นการโจมตีแบบตั้งใจ ดังภาพประกอบ 3



ภาพประกอบ 3 ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9



ภาพประกอบ 4 สรุปปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

4.2 เครื่องมือ มาตรการ และแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

จากการลงพื้นที่สัมภาษณ์เชิงลึก พบว่าเครื่องมือ มาตรการ และแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 สามารถสรุปได้ดังนี้

4.2.1 เครื่องมือการจัดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

เครื่องมือที่มีส่วนสำคัญในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ การติดตั้งฮาร์ดแวร์และซอฟต์แวร์ คือ อุปกรณ์ป้องกันเครือข่าย (Firewall) ซอฟต์แวร์แอนตี้ไวรัสติดตั้งกับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย การแนะนำและอบรมเป็นการให้ความรู้และสร้างความตระหนักให้กับเจ้าหน้าที่ผู้ปฏิบัติงาน และการบริหารความเสี่ยงทางด้านเทคโนโลยีมาใช้จะช่วยในการประเมินระดับความเสี่ยงตลอดจนแนวทางการแก้ไขปัญหาต่าง ๆ ในการฟื้นฟูระบบให้กลับมาได้ ดังนี้

ติดตั้งฮาร์ดแวร์และซอฟต์แวร์

จากการสัมภาษณ์ผู้ให้ข้อมูลหมด 18 หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ตอบตรงกันทั้งหมด ดังคำสัมภาษณ์ของตัวแทนผู้ให้ข้อมูลหลัก ดังนี้

“...ติดตั้งอุปกรณ์ Firewall โดยสำนักงานศาลยุติธรรม และติดตั้งโปรแกรมแอนตี้ไวรัส...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...ติดตั้งอุปกรณ์ Firewall โดยสำนักงานศาลยุติธรรม และติดตั้งโปรแกรมแอนตี้ไวรัสเครื่องคอมพิวเตอร์หน่วยงาน...”

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

“...ติดตั้งอุปกรณ์ Firewall โดยสำนักงานศาลยุติธรรม และติดตั้งโปรแกรมแอนตี้ไวรัสหรือโปรแกรมที่สร้างความปลอดภัยด้านข้อมูลทุกเครื่อง...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

แนะนำและอบรม

จากการสัมภาษณ์ผู้ให้ข้อมูลหมด 18 หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 จากการตอบส่วนใหญ่ในการได้รับการแนะนำและอบรม ดังคำสัมภาษณ์ของตัวแทนผู้ให้ข้อมูลหลัก 10 ท่าน ดังนี้

“...อบรมให้ความรู้ ป้องกันแฟลชไดร์ฟ เว็บโฆษณา เพจแปลกห้ามคลิก...”

(ผู้ให้ข้อมูลหลักคนที่ 3, 27 ธันวาคม 2565 : สัมภาษณ์)

“...แนะนำหน้างานในการปฏิบัติงานให้ถูกต้องและมีความปลอดภัย กับอบรมของสำนักงานศาล...”

(ผู้ให้ข้อมูลหลักคนที่ 5, 27 ธันวาคม 2565 : สัมภาษณ์)

“...จัดอบรมการตั้งรหัสผ่าน การตรวจสอบเครื่องสำรองไฟฟ้า และสแกนแฟลชไดร์ฟ หรือส่งไฟล์ทางไลน์ ทางเมล...”

(ผู้ให้ข้อมูลหลักคนที่ 7, 28 ธันวาคม 2565 : สัมภาษณ์)

“...จัดอบรมให้ความรู้ ตามเทรน และนโยบายผู้บริหารของสำนักงานศาล ช่วงนี้เน้น ความมั่นคงปลอดภัยด้านไซเบอร์ พรบ.ส่วนบุคคล การตั้งรหัสผ่าน...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

“...จัดอบรมปีละครั้ง การใช้งานให้มีความปลอดภัย การส่งข้อมูล การเปลี่ยนรหัสผ่านทุก ๆ 4 เดือน เวลาใช้งานมีความเสี่ยงอะไรบ้าง...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...มีการอบรมภัยคุกคามทางไซเบอร์ แจ้งเตือนเว็บไซต์ Popup และFake News (ข่าวปลอม)...”

(ผู้ให้ข้อมูลหลักคนที่ 12, 3 มกราคม 2566 : สัมภาษณ์)

“...จัดอบรม KM ในหัวข้อแต่ละระบบงาน และย้ำเตือนสอดแทรกการใช้การจัดการความเสี่ยงทางไซเบอร์...”

(ผู้ให้ข้อมูลหลักคนที่ 13, 3 มกราคม 2566 : สัมภาษณ์)

“...มีการจัดอบรม มีการใช้งานให้กับ จนท. KM ปีละครั้งระบบติดตามสำนวนคดี การใช้งานระบบต่าง ๆ ทางด้านไอที การตั้งรหัสผ่าน การสแกนไวรัส การตรวจสอบเครื่องสำรองไฟฟ้า...”

(ผู้ให้ข้อมูลหลักคนที่ 15, 9 มกราคม 2566 : สัมภาษณ์)

“...การอบรมมีทั้งอบรมโดยนักวิชาการคอมพิวเตอร์และสำนักงานศาล ปีละ 2 ครั้ง ทบทวนการสอนงานระบบงาน ให้ความรู้จากภัยคุกคามจากไซเบอร์ ใช้งานอย่างไรให้ปลอดภัยจากไซเบอร์ การตั้งรหัสผ่าน การส่งข้อมูล...”

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

“...ส่วนกลางจัดอบรมทางไซเบอร์ก็จะเชิญชวนให้เจ้าหน้าที่ และทำคำสั่งออกมาเข้าไปฟังที่ห้องประชุมใหญ่ หรืออบรมให้ตัวแทนกลุ่มงาน นอกจากระบบงานทั่วไปที่เจ้าหน้าที่ทุกคนต้องสามารถทำได้ก็จัดอบรมทั้งศาล...”

(ผู้ให้ข้อมูลหลักคนที่ 25, 20 มกราคม 2566 : สัมภาษณ์)

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศไว้ดังนี้

“...ใช้เครื่องมือการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยง...”

(ผู้ให้ข้อมูลหลักคนที่ 1, 20 ธันวาคม 2565 : สัมภาษณ์)

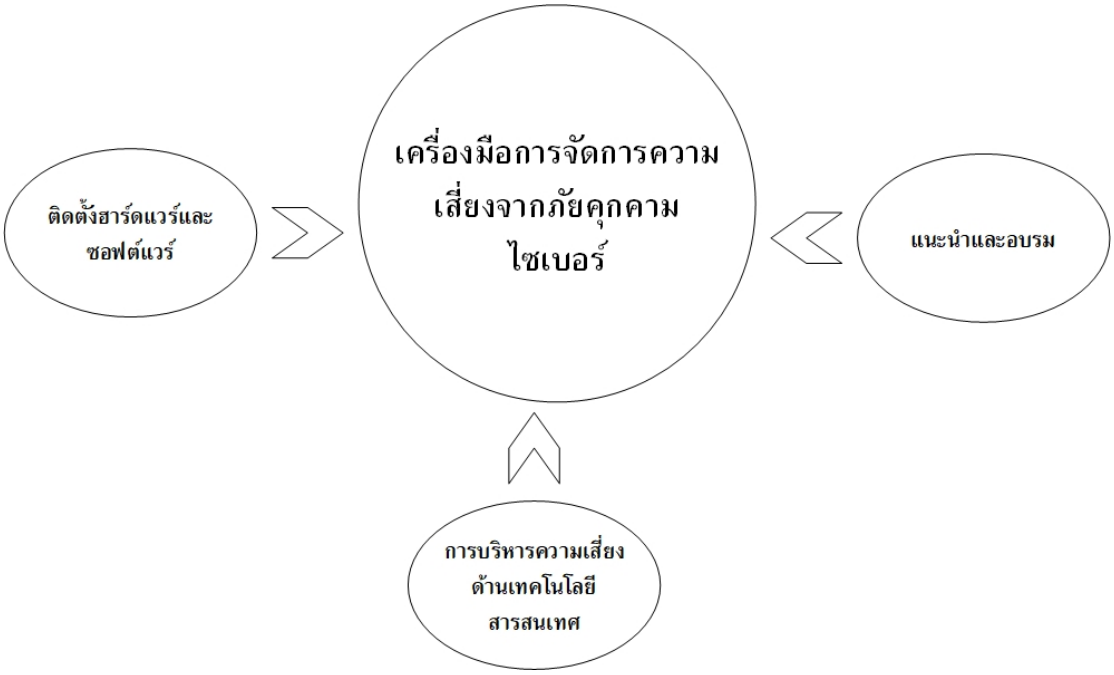
“...ได้นำ Risk Management System การบริหารจัดการความเสี่ยง เพื่อให้หน่วยงานจัดการทั้งหมด 5 ด้าน รวมถึงระบบเทคโนโลยีสารสนเทศ...”

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

“...ใช้เครื่องมือการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ...”

(ผู้ให้ข้อมูลหลักคนที่ 19, 12 มกราคม 2565 : สัมภาษณ์)

กล่าวโดยสรุปการจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์เครื่องมือเป็นส่วนหนึ่งที่จะช่วยปกป้องระบบให้ปลอดภัย ได้แก่ การติดตั้งฮาร์ดแวร์และซอฟต์แวร์ การแนะนำหรืออบรมการผู้ปฏิบัติงาน และการนำเอาการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศมาใช้ดังภาพประกอบ 5



ภาพประกอบ 5 เครื่องมือการจัดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

4.2.2 มาตรการการจัดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

สำหรับมาตรการในการจัดการความเสี่ยงได้แก่ คำสั่งแต่งตั้งและมอบหมาย ควบคุมจำกัดสิทธิในการใช้งาน ของแต่ละตำแหน่งละกลุ่มงาน และจำกัดการใช้อุปกรณ์ส่วนตัว

คำสั่งแต่งตั้งและมอบหมายงาน

สำหรับมาตรการโดยการแต่งตั้งและมอบหมายงาน มีการให้ข้อมูลจากการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลดังนี้

“...มีคำสั่งแต่งตั้งและมอบหมายให้เจ้าหน้าที่แต่ละส่วนงานให้สามารถเข้าถึงระบบได้ตามหน้าที่และมาตรการในการใช้งานระบบงานหรือ Application...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

ควบคุมจำกัดสิทธิในการใช้งาน ของแต่ละตำแหน่งกลุ่มงาน

ส่วนมาตรการโดยการควบคุมจำกัดสิทธิในการใช้งาน ของแต่ละตำแหน่งกลุ่มงาน มีผู้ให้ข้อมูลหลักจากการสัมภาษณ์ดังนี้

` “...ควบคุมจำกัดสิทธิในการใช้งาน ของแต่ละตำแหน่งกลุ่มงาน...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

“...มีบางโปรแกรมที่อาจจะต้องใช้ร่วมกันซึ่งผู้มีสิทธิคนเดียวแต่ต้องใช้งานเนื่องด้วยเป็นเฉพาะตำแหน่งหรือหน้าที่ และผู้อื่นมาปฏิบัติหน้าที่ในวันนั้น...”

(ผู้ให้ข้อมูลหลักคนที่ 15, 9 มกราคม 2566 : สัมภาษณ์)

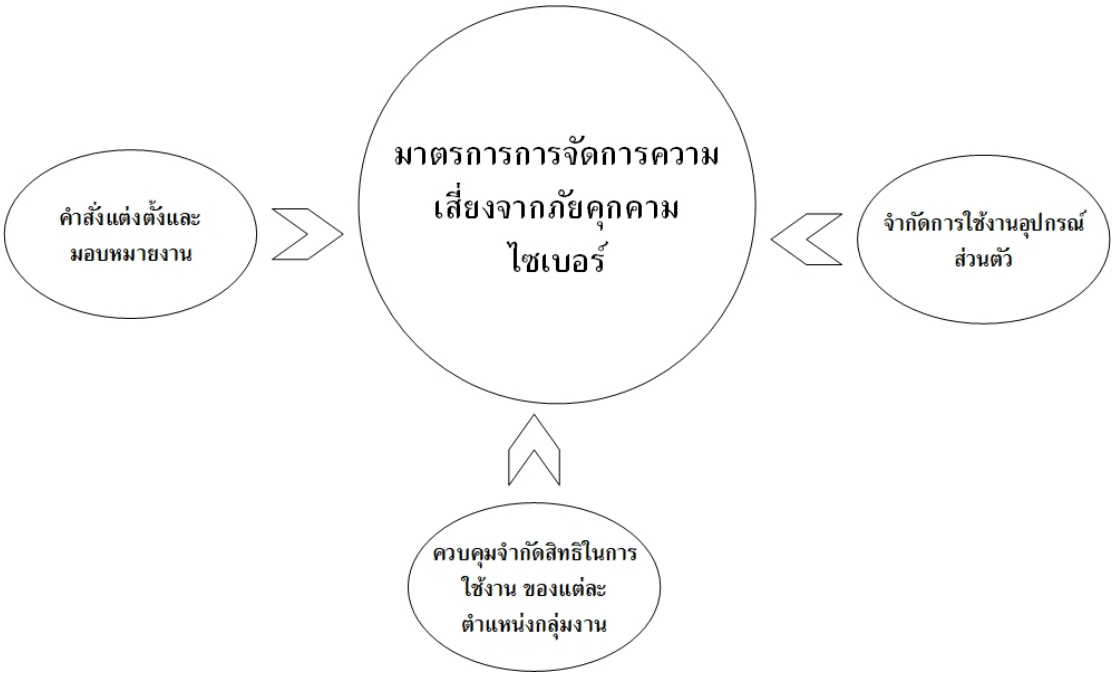
จำกัดการใช้งานอุปกรณ์ส่วนตัว

มาตรการโดยการจำกัดการใช้งานอุปกรณ์ส่วนตัวมีผู้ให้ข้อมูลหลักให้สัมภาษณ์ดังนี้

“...จำกัดการใช้งานอุปกรณ์สื่อสารส่วนตัวที่ใช้อินเตอร์เน็ต เช่น โทรศัพท์มือถือหรือเครื่องคอมพิวเตอร์โน๊ตบุ๊คของเจ้าหน้าที่ที่นำมาใช้งานอื่น...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

กล่าวโดยสรุปมาตรการการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ที่มีการดำเนินการได้แก่ มีคำสั่งแต่งตั้งและมอบหมายงานให้กับเจ้าหน้าที่ผู้ปฏิบัติงานในแต่ละตำแหน่งหรือแต่ละส่วนที่รับผิดชอบอย่างชัดเจน ซึ่งจะเชื่อมโยงกับสิทธิในการใช้งานโปรแกรมแต่ละระบบ และการจำกัดการใช้อุปกรณ์ส่วนตัวจะช่วยให้ระบบปลอดภัยมากขึ้น ดังภาพประกอบ 6



ภาพประกอบ 6 มาตรการการจัดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

4.2.3 แนวปฏิบัติการจัดการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

แนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ การสำรองข้อมูล เก็บประวัติการใช้งาน อัพเดตระบบปฏิบัติการ การตั้งรหัสผ่านและบันทึกรหัสผ่าน การสแกนไวรัส และไม่ให้ใช้แฟลชไดร์ฟ

สำรองข้อมูล

การสำรองข้อมูลเป็นประจำจะทำให้เป็นการรับประกันได้ว่าข้อมูลในระบบถ้ามีปัญหาจะสามารถนำมาใช้งานต่อได้ จากการสัมภาษณ์ผู้ให้ข้อมูลหลัก 18 หน่วยงานให้คำตอบตรงกัน ดังตัวแทนการให้สัมภาษณ์ 5 ท่านดังนี้

“...สำรองข้อมูลที่เครื่องคอมพิวเตอร์แม่ข่าย ผู้ดูแลระบบ และคลาวด์ไดร์ แต่ละช่วงเวลาที่ต่างกัน...”

(ผู้ให้ข้อมูลหลักคนที่ 5, 27 ธันวาคม 2565 : สัมภาษณ์)

“...มีการสำรองข้อมูล 3 เวลา 12.30 16.30 และเที่ยงคืนที่เครื่องผู้ดูแลระบบ External ต่อผ่าน Usb และ Nas...”

(ผู้ให้ข้อมูลหลักคนที่ 7, 28 ธันวาคม 2565 : สัมภาษณ์)

“...สำรองข้อมูล เวลา 9.00, 12.00, 13.00 และ 18.00 สำรองที่ Nas และ PC ของผู้ดูแลระบบ...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

“...Backup ข้อมูลเป็นประจำทุกวัน 2 ครั้ง 12 นาฬิกา หลังเลิกงาน 16:30 ที่คอมผู้ดูและระบบ และ Nas...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...Backup ข้อมูลเป็นประจำทุกวัน หลังเลิกงาน 16:30 ที่คอมผู้ดูและระบบ และ Nas...”

(ผู้ให้ข้อมูลหลักคนที่ 13, 3 มกราคม 2566 : สัมภาษณ์)

เก็บประวัติการใช้งานระบบ

การเก็บประวัติการใช้งานระบบจะช่วยให้ทราบว่าผู้ใดกระทำอะไรกับระบบในข้อมูลระบบ ซึ่งในระบบจะมีการจัดเก็บประวัติการใช้งานระบบไว้ จากการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลการเก็บประวัติการใช้งานดังนี้

“...การโดนโจมตีทางไซเบอร์ยังมีอยู่ในLog ของไฟล์วอลและแอนตี้ไวรัส...”

(ผู้ให้ข้อมูลหลักคนที่ 5, 27 ธันวาคม 2565 : สัมภาษณ์)

“...มีการเก็บ Log การใช้งานระบบช่วยให้ทราบว่าใครทำอะไรกับข้อมูลหรือขั้นตอนไหน...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

อัพเดตระบบปฏิบัติการ

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลสำหรับแนวปฏิบัติการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ด้วยการปรับปรุงระบบปฏิบัติการให้เป็นรุ่นล่าสุดเพื่อป้องกันช่องโหว่ของระบบปฏิบัติการดังนี้

"...คอมพิวเตอร์ไม่เพียงพอ นำคอมเก่ามาใช้วินโดว์ไม่อัพเดต..."

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

"...อัพเดตระบบปฏิบัติการของเครื่องคอมพิวเตอร์อยู่เสมอ..."

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

"...ผู้ดูแลระบบตรวจสอบโปรแกรมหรืออัพเดตโปรแกรม..."

(ผู้ให้ข้อมูลหลักคนที่ 8, 28 ธันวาคม 2565 : สัมภาษณ์)

สรุปได้ว่าการปรับปรุงระบบปฏิบัติการจะทำให้ระบบคอมพิวเตอร์มีความปลอดภัยมากขึ้น เนื่องจากบริษัทผู้พัฒนาจะเพิ่มเติมฟังก์ชั่นการทำงานของระบบและอุดช่องโหว่ของระบบปฏิบัติการทำให้ระบบมีความปลอดภัยจากภัยคุกคามไซเบอร์

การตั้งรหัสผ่านและการบันทึกรหัสผ่าน

แนวปฏิบัติที่สำคัญในการตั้งรหัสผ่านและการบันทึกรหัสผ่านสำหรับการปฏิบัติงาน จะทำให้การเข้าใช้ปฏิบัติงาน ข้อมูลส่วนตัวหรือข้อมูลทางคดีมีความปลอดภัยมากขึ้น จากการสัมภาษณ์ผู้ให้ข้อมูลหลัก 18 หน่วย ให้ข้อมูลตรงกัน ดังคำสัมภาษณ์ของตัวแทนผู้ให้ข้อมูล 5 ท่าน ให้ข้อมูลดังนี้

"...เปลี่ยนรหัสผ่านบ่อยครั้ง กรณีเปลี่ยนรหัสดำเนินการจดบันทึกในสมุด ป้องกันการหลงลืมรหัสผ่าน..."

(ผู้ให้ข้อมูลหลักคนที่ 2, 20 ธันวาคม 2565 : สัมภาษณ์)

"...User Name Password เปลี่ยนทุก ๆ 4 เดือน และอย่าตั้งให้เหมือนกัน ตั้งให้ยาก..."

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

"...ชื่อผู้ใช้งาน และรหัสผ่าน ในส่วนอาจใช้ชื่อผู้ใช้งาน ชื่อเดิม แต่ละโปรแกรมอาจเปลี่ยนแค่รหัสผ่าน ให้ไม่เหมือนกัน..."

(ผู้ให้ข้อมูลหลักคนที่ 12, 3 มกราคม 2566 : สัมภาษณ์)

"...ให้เจ้าหน้าที่ จดรหัสผ่านส่วนตัว จะใช้รหัสผ่านทุกระบบ คาดเดาได้ยาก หมั่นเปลี่ยนสม่ำเสมอ ประกอบด้วยตัวอักษร ตัวเล็ก ใหญ่ อักขระพิเศษ ยกเลิกการจำรหัสผ่านของ Google Chrome..."

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

"...ให้เจ้าหน้าที่ตั้งรหัสผ่านให้คาดเดายาก จดไว้ในสมุดตัวเอง..."

(ผู้ให้ข้อมูลหลักคนที่ 31, 1 กุมภาพันธ์ 2566 : สัมภาษณ์)

การสแกนไวรัส

การสแกนไวรัสใช้ในกรณีมีการดาวน์โหลดไฟล์หรือการเชื่อมต่อแฟลชไดร์ฟเพื่อความปลอดภัยจะต้องมีการดำเนินการสแกนไวรัส จากการสัมภาษณ์ผู้ให้ข้อมูลหลัก 18 หน่วยงาน ให้ข้อมูลส่วนใหญ่ตรงกัน จากการให้สัมภาษณ์ตัวแทน 5 ท่านดังนี้

"...ให้ เจ้าหน้าที่ สแกนแฟลชไดร์ฟ หรือส่งทางไลน์ ทางเมล..."

(ผู้ให้ข้อมูลหลักคนที่ 7, 28 ธันวาคม 2565 : สัมภาษณ์)

"...นำแฟลชไดร์ฟ ของคู่ความหรือเจ้าหน้าที่ สแกนไวรัสก่อนนำไปใช้งาน..."

(ผู้ให้ข้อมูลหลักคนที่ 8, 28 ธันวาคม 2565 : สัมภาษณ์)

"...ใช้เครื่องผู้ดูแลระบบสแกนแฟลชไดร์ฟ ดึงสายแลนออก..."

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

"...สแกนหาไวรัส หรือแจ้งพนักงานคอมพิวเตอร์เพื่อดำเนินการก่อนใช้แฟลชไดร์ฟเชื่อมต่อเข้าระบบ..."

(ผู้ให้ข้อมูลหลักคนที่ 10, 29 ธันวาคม 2565 : สัมภาษณ์)

"...สแกนไวรัสแฟลชไดร์ฟก่อนเสมอ กรณีที่มีการขอข้อมูลที่ไม่สามารถดาวน์โหลดจากระบบได้..."

(ผู้ให้ข้อมูลหลักคนที่ 15, 9 มกราคม 2566 : สัมภาษณ์)

ไม่ให้ใช้แฟลชไดร์ฟ

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักให้ข้อมูลสำหรับแนวปฏิบัติการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ด้วยการไม่ให้ใช้แฟลชไดร์ฟหรือใช้เท่าที่จำเป็นดังนี้

"...บุคลากร คู่ความ ไม่นำอุปกรณ์อื่น ที่ไม่น่าเชื่อถือมาเชื่อมต่อในระบบเครือข่าย..."

(ผู้ให้ข้อมูลหลักคนที่ 2, 20 ธันวาคม 2565 : สัมภาษณ์)

`"...ไม่ให้ใช้แฟลชไดร์ฟ ไม่ให้ส่งข้อมูลผ่านระบบไลน์..."

(ผู้ให้ข้อมูลหลักคนที่ 5, 27 ธันวาคม 2565 : สัมภาษณ์)

"...เปลี่ยนจากการใช้แฟลชไดร์ฟเป็นรับส่งผ่านอีเมล ฝากในไดร์ฟ Nas แทน..."

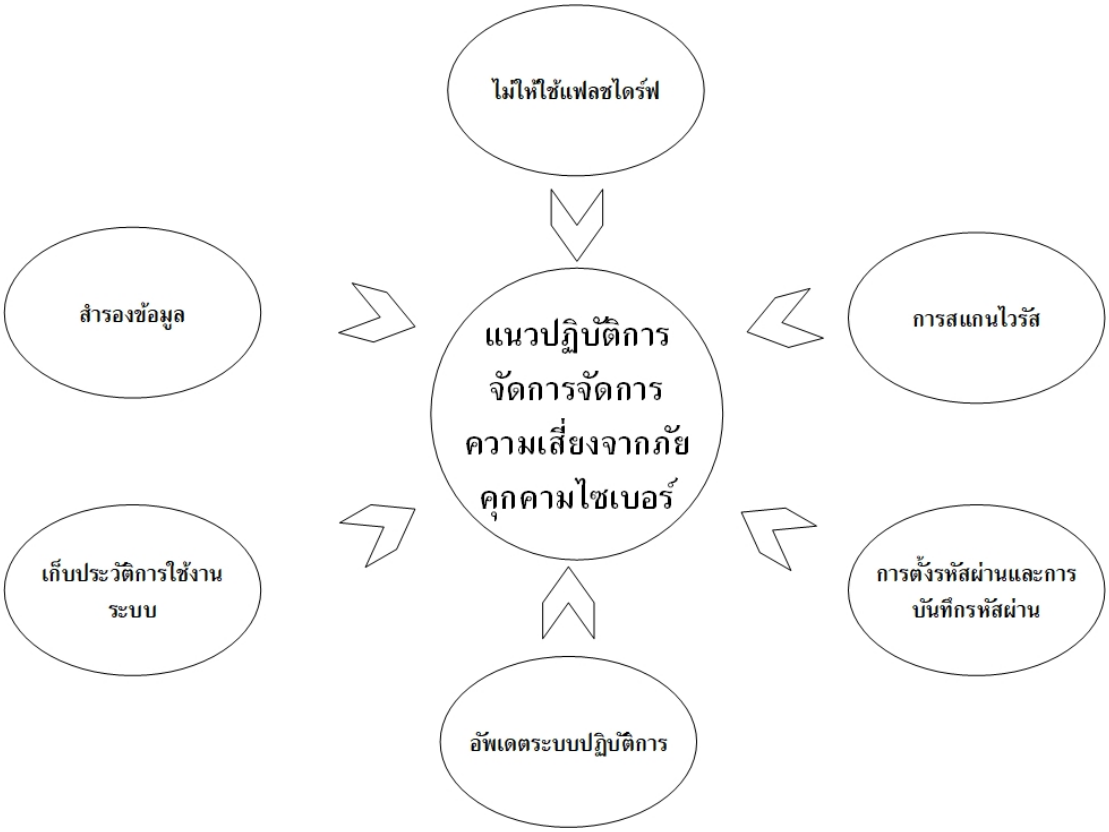
(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

"...หลีกเลี่ยงการใช้ แฟลชไดร์ฟ ใช้วิธีการส่งทางเมล หรือCloud Storage..."

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

กล่าวโดยสรุปสำหรับแนวปฏิบัติการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ที่นำมาใช้ได้แก่การสำรองข้อมูลเป็นประจำเป็นการรับประกันข้อมูลจะมีความเป็นปัจจุบันมากที่สุด การเก็บประวัติการใช้งานระบบจะช่วยให้ทราบสถานการณ์การใช้งานระบบของแต่ละบุคคล การปรับปรุงระบบปฏิบัติการจะช่วยในการปิดช่องโหว่ของตัวระบบปฏิบัติการให้มีความปลอดภัย การตั้งรหัสผ่านและการบันทึกรหัสผ่านที่ปลอดภัยจะทำให้การเข้าถึงระบบรวมทั้งการใช้งานระบบ

มีความปลอดภัยมากยิ่งขึ้น ไม่ควรใช้แฟลชไดร์ฟอีกต่อไปแต่ถ้าหลีกเลี่ยงไม่ได้ก็ให้ทำการสแกนไวรัสก่อนใช้งานดังภาพประกอบ 7



ภาพประกอบ 7 แนวปฏิบัติการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

4.3 ความสำเร็จและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

4.3.1 ความสำเร็จในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

ความสำเร็จในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ได้แก่ การรักษาความลับ การรักษาความถูกต้อง และสภาพพร้อมใช้งาน

การรักษาความลับ

ในการรักษาความลับ มีการกำหนดระดับการเข้าถึงข้อมูลและการป้องกันการเข้าระบบโดยไม่พึงประสงค์ จากการสัมภาษณ์หน่วยงานทั้ง 18 หน่วยมีคำตอบตรงกันทั้งหมด ดังคำสัมภาษณ์ของตัวแทนผู้ให้ข้อมูล 5 ท่าน หลักดังนี้

“...การรักษาความปลอดภัยของข้อมูล ปรับปรุงการสูญเสียข้อมูล การล่มของระบบข้อมูลน้อยลง...”

(ผู้ให้ข้อมูลหลักคนที่ 5, 27 ธันวาคม 2565 : สัมภาษณ์)

“...ระบบอยู่เฉพาะเครือข่ายภายใน จึงมีความปลอดภัย...”

(ผู้ให้ข้อมูลหลักคนที่ 7, 28 ธันวาคม 2565 : สัมภาษณ์)

“...มีจำกัดในการเรียกดูตามสิทธิ์การใช้งาน หัวหน้าส่วนกำหนดสิทธิ์ของเค้าขึ้นมาเองได้...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...มีการติดตั้งเทคโนโลยี Firewall การกำหนดผู้รับผิดชอบทางเทคโนโลยีสารสนเทศระบบต่าง ๆ...”

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

“...การรักษาความลับ บุคลากรตระหนักการเข้าถึงข้อมูลต่าง ๆ อยู่ ไม่มอบรหัสให้ใคร มีพรบ.ข้อมูลส่วนบุคคล การรักษาสิทธิ์ รักษาข้อมูลส่วนบุคคล ส่วนรหัสจดบันทึกไว้ป้องกันไม่ให้ใครรู้...”

(ผู้ให้ข้อมูลหลักคนที่ 18, 10 มกราคม 2566 : สัมภาษณ์)

การรักษาความถูกต้อง

ในส่วนของการรักษาความถูกต้อง คือข้อมูลมีความถูกต้อง ครบถ้วน แม่นยำ จากการสัมภาษณ์หน่วยงานทั้ง 18 หน่วยมีคำตอบตรงกันทั้งหมดดังคำสัมภาษณ์ของตัวแทนผู้ให้ข้อมูลหลักดังนี้

“...สิทธิในการจัดการข้อมูล มีการตรวจสอบความถูกต้องของข้อมูล...”

(ผู้ให้ข้อมูลหลักคนที่ 1, 20 ธันวาคม 2565 : สัมภาษณ์)

“...ในการปฏิบัติงาน สามารถเรียกใช้ข้อมูลมาใช้งานได้ทันทีและครบถ้วน...”

(ผู้ให้ข้อมูลหลักคนที่ 2, 20 ธันวาคม 2565 : สัมภาษณ์)

“...หัวหน้าส่วนเป็นผู้ตรวจสอบความถูกต้องของข้อมูล คนแก้ไขได้หัวหน้าส่วน การยกเลิกใบเสร็จ สิทธิ์ของหัวหน้าส่วน...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

สภาพพร้อมใช้งาน

ด้านสภาพพร้อมใช้งานทั้งฮาร์ดแวร์และซอฟต์แวร์อยู่ในสภาพพร้อมใช้งานและพร้อมป้องกันจากภัยคุกคามไซเบอร์ จากการสัมภาษณ์หน่วยงานทั้ง 18 หน่วยมีคำตอบตรงกันทั้งหมดดังคำสัมภาษณ์ของตัวแทนผู้ให้ข้อมูล 5 ท่าน หลักดังนี้

“...ในส่วนฮาร์ดแวร์และซอฟต์แวร์พร้อมใช้งานไม่ค่อยมีปัญหา...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

“...สภาพพร้อมใช้งาน ก็ยังมีปัญหาอยู่บ้าง สัปดาห์ละครั้ง บางทีก็ 4 ครั้งต่อสัปดาห์ ทั้งเก่าและใหม่...”

(ผู้ให้ข้อมูลหลักคนที่ 12, 3 มกราคม 2566 : สัมภาษณ์)

“...ระบบไม่ค่อยมีปัญหา แต่แก้ไขได้ มีความพร้อมใช้งาน ทั้งฮาร์ดแวร์และซอฟต์แวร์ไม่ค่อยมีปัญหา...”

(ผู้ให้ข้อมูลหลักคนที่ 15, 9 มกราคม 2566 : สัมภาษณ์)

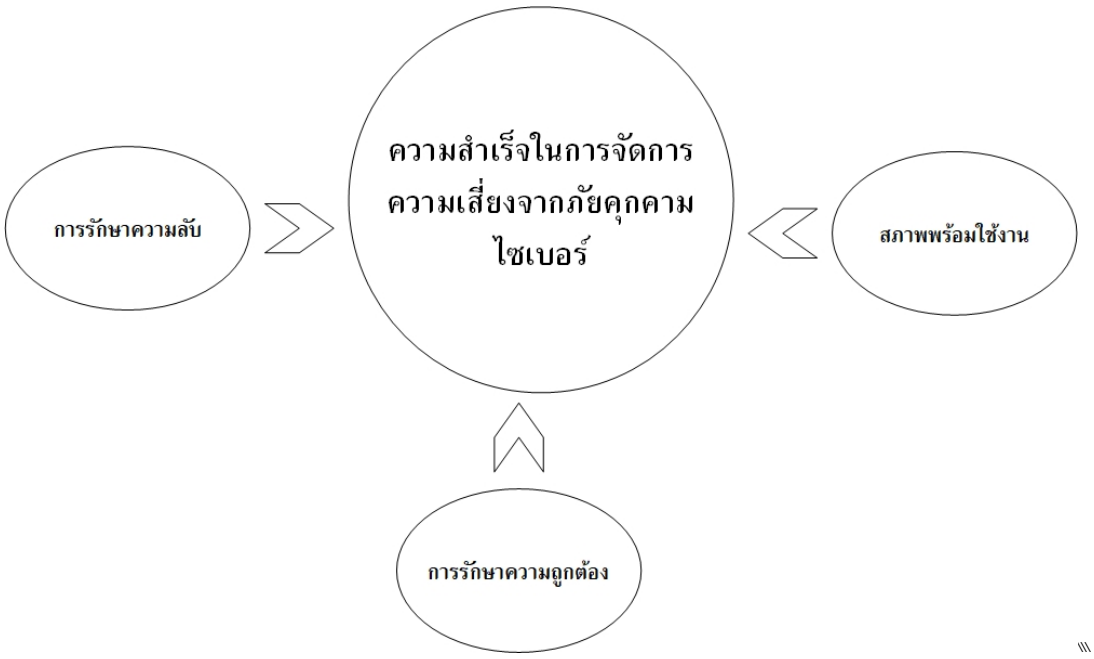
“...นักวิชาการคอมพิวเตอร์ดูแลเบื้องต้น และมีบริษัทมาบำรุงรักษาให้สม่ำเสมอสำหรับอุปกรณ์พวกเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ป้องกันเครือข่าย และอุปกรณ์กระจายสัญญาณ...”

(ผู้ให้ข้อมูลหลักคนที่ 17, 10 มกราคม 2566 : สัมภาษณ์)

“...ส่วนใหญ่พร้อม ที่ศาลมีการปรับปรุงสำนักงานอยู่ พวกอุปกรณ์บางอย่างถูกถอด ไวไฟ ให้เจ้าหน้าที่ใช้อย่างเดียว...”

(ผู้ให้ข้อมูลหลักคนที่ 27, 23 มกราคม 2566 : สัมภาษณ์)

กล่าวโดยสรุปความสำเร็จในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ประกอบด้วยการรักษาความลับข้อมูลควรจะต้องมีการกำหนดระดับการเข้าถึงข้อมูลและการป้องกันการเข้าระบบโดยไม่พึงประสงค์ การรักษาความถูกต้องข้อมูลควรจะมีความถูกต้อง ครบถ้วนแม่นยำ โดยถ้ามีความคลาดเคลื่อน (error) อยู่ในเกณฑ์ที่ยอมรับได้ และสภาพพร้อมใช้งานทั้งฮาร์ดแวร์และซอฟต์แวร์โดยรวมอยู่ในสภาพพร้อมใช้งานและมีพร้อมป้องกันจากภัยคุกคามไซเบอร์ ดังภาพประกอบ 8



ภาพประกอบ 8 ความสำเร็จในการจัดการความเสียงจากภัยคุกคามไซเบอร์

4.3.2 ปัญหาและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

ปัญหาและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ได้แก่ ด้านงบประมาณ ด้านทักษะบุคลากรและจำนวนบุคลากรทางด้านไซเบอร์ ด้านนโยบายของหน่วยงาน และด้านระเบียบหรือกฎหมายที่เกี่ยวข้อง

ด้านงบประมาณ

ปัจจัยด้านงบประมาณมีส่วนสำคัญในการจัดซื้อทั้งฮาร์ดแวร์และซอฟต์แวร์ในการสนับสนุนการปฏิบัติงาน ดังคำสัมภาษณ์ของผู้ให้ข้อมูลหลักดังนี้

"...ด้านงบประมาณ ของโครงการของบประมาณต่าง ๆ จัดสรรเอามาให้ศาลจัดซื้อเอง ทำให้ศาลไม่สามารถจัดซื้อเองได้ในงบประมาณที่จัดสรรมาให้เพราะงบดังกล่าวอยู่ในราคาที่จัดซื้อได้ในจำนวนที่ซื้อหลายเครื่อง..."

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

"...ด้านอุปกรณ์มีไม่เพียงพอ คอมพิวเตอร์ต้องใช้ User Pass รหัสตรงนั้น..."

(ผู้ให้ข้อมูลหลักคนที่ 15, 9 มกราคม 2566 : สัมภาษณ์)

"...อุปกรณ์เครื่องคอมพิวเตอร์ไม่เพียงพอต่อการใช้งานเพราะปัจจุบันรูปแบบการทำงานในศาลหลากหลายกว่าก่อนมากขึ้น เจ้าหน้าที่หนึ่งคนอาจต้องทำงานหลายหน้าที่และหลายห้องทำให้ต้องมีการใช้งานคอมพิวเตอร์มากกว่าหนึ่งเครื่อง บางครั้งต้องเอาคอมพิวเตอร์เก่าที่ทดแทนแล้วมาใช้งานทำให้อาจมีความเสี่ยงจากภัยคุกคามไซเบอร์ และการจัดหาซอฟต์แวร์ลิขสิทธิ์มาใช้งาน ลดการดาวน์โหลดซอฟต์แวร์และฟรีแวร์หรือแบบแชร์แวร์..."

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

"...ด้านซอฟต์แวร์ ไม่มีโปรแกรม Photoshop และ Adobe Acrobat..."

(ผู้ให้ข้อมูลหลักคนที่ 27, 23 มกราคม 2566 : สัมภาษณ์)

ด้านทักษะบุคลากร

ในด้านทักษะบุคลากรเป็นส่วนสำคัญที่จะต้องมีการแนะนำและอบรมบุคลากรในการปฏิบัติงานและความระมัดระวังในการเข้าใช้งานระบบต่าง ๆ ให้มีความปลอดภัย ซึ่งตรงกับคำให้สัมภาษณ์ผู้ให้ข้อมูลหลักดังนี้

"...มีปัญหาขาดทักษะการใช้งานคอมพิวเตอร์ ต้องเน้นย้ำ การใช้มาตรการเพื่อลดความเสี่ยงบ่อยครั้ง ยกตัวอย่างเบื้องต้น เช่น กรณีเครื่องคอมพิวเตอร์เปิดไม่ได้ เครื่องพิมพ์ไม่สามารถพิมพ์งานได้ หรือเครื่องไม่อยู่ในระบบเครือข่าย.."

(ผู้ให้ข้อมูลหลักคนที่ 2, 20 ธันวาคม 2565 : สัมภาษณ์)

"...มีปัญหาขาดทักษะการใช้งานคอมพิวเตอร์ ฟื้นฟูทักษะให้..."

(ผู้ให้ข้อมูลหลักคนที่ 4, 27 ธันวาคม 2565 : สัมภาษณ์)

“...ด้านทักษะบุคลากร เจ้าหน้าที่สูงวัยเรียนรู้ได้ช้า และไม่ค่อยอยากที่จะปรับเปลี่ยนการทำงาน...”

(ผู้ให้ข้อมูลหลักคนที่ 8, 28 ธันวาคม 2565 : สัมภาษณ์)

“...ด้านทักษะบุคลากร มีปัญหาเล็กน้อย ขาดทักษะการใช้งานคอมพิวเตอร์ ต้องเน้นย้ำการใช้งานและทบทวน...”

(ผู้ให้ข้อมูลหลักคนที่ 10, 29 ธันวาคม 2565 : สัมภาษณ์)

จำนวนบุคลากรทางด้านไซเบอร์

อุปสรรคด้านจำนวนบุคลากรทางด้านไซเบอร์มีความสำคัญเป็นอย่างมาก เนื่องด้วยมีเพียง 1 ท่านต่อหน่วยงาน ซึ่งหน่วยงานส่วนใหญ่มีความต้องการเพิ่มบุคลากรทางด้านไซเบอร์ ดังคำให้สัมภาษณ์ของผู้ให้ข้อมูลหลักดังนี้

“...ด้านจำนวนบุคลากรทางด้านไซเบอร์ มีปัญหา ควรจัดสรรเพิ่มเป็น 2 คน ผู้ช่วยก็มีหน้าที่ประจำอยู่ไม่สามารถปฏิบัติงานได้อย่างเต็มที่ และมีการประเมินว่าควรแก้ปัญหาอันไหนเร่งด่วนมากกว่ากัน...”

(ผู้ให้ข้อมูลหลักคนที่ 8, 28 ธันวาคม 2565 : สัมภาษณ์)

“...ด้านบุคลากรมีไม่เพียงพอ ทุกอย่างผ่านระบบหมดเลย ทั้งอุปกรณ์คอม แก้โปรแกรม แทนที่จะจัดอบรมให้ไอทีอย่างเดียวการจัดอบรมผ่านระบบ Streaming ไม่ค่อยได้ผล เป็นการสื่อสารทางเดียว การฟังเฉยๆ ไม่ได้ลึกซึ้ง...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...ให้มีเจ้าหน้าที่ด้านคอมพิวเตอร์เพิ่มขึ้นในศาลที่ปริมาณคอมพิวเตอร์จำนวนมากหรือศาลที่มีงานคดีหรือผู้ใช้บริการจำนวนมาก เพื่อส่งเสริมงานและลดความเสี่ยงจากความเสี่ยงจากภัยคุกคามไซเบอร์...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

ด้านนโยบายของหน่วยงาน

สำหรับปัญหาและอุปสรรคด้านนโยบายของหน่วยงานในเรื่องของการจัดตั้งที่ทำการศาลหรือการพัฒนาระบบใหม่ๆ มาเพื่อการปฏิบัติงานดังคำให้สัมภาษณ์ของผู้ให้ข้อมูลหลักดังนี้

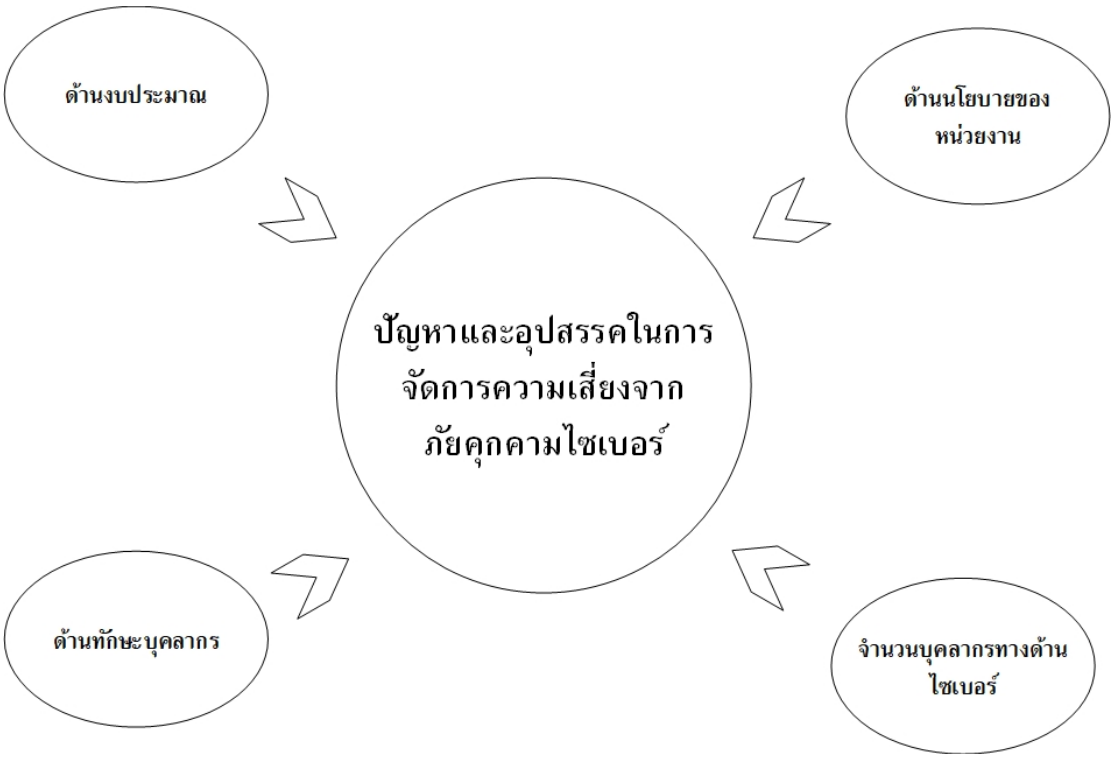
“...ศาลอยู่ใกล้ทะเล เกลือ ทำให้ Core Switch พัดลมพัง ใช้งานเน็ตไม่ได้ Server พังไอน้ำ ขี้เกลือ สนิม...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

“...ด้านนโยบาย ทำให้ผู้ใช้งานระบบ จะต้องเรียนรู้ระบบใหม่อยู่ตลอดเวลา ผู้ใช้งานมีรหัสจำรหัส มีระบบเพิ่มมาใหม่ มีงานที่ซ้ำซ้อนอยู่...”

(ผู้ให้ข้อมูลหลักคนที่ 13, 3 มกราคม 2566 : สัมภาษณ์)

กล่าวสรุปได้ว่าปัญหาและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ด้านงบประมาณในส่วนของการจัดหาทั้งฮาร์ดแวร์และซอฟต์แวร์ที่ให้ศาลจัดซื้อเองเรื่องราคา เครื่องคอมพิวเตอร์มียังไม่เพียงพอและโปรแกรมที่ใช้งานไม่มีลิขสิทธิ์ ด้านทักษะบุคลากรและในเรื่องของอายุในการเรียนรู้ทักษะที่ต้องเน้นย้ำใช้ในการปฏิบัติงานเป็นส่วนหนึ่งของการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ จำนวนบุคลากรทางไซเบอร์โดยศาลที่เป็นศาลที่มีขนาดใหญ่ หรือปริมาณเครื่องคอมพิวเตอร์มาก หรือปริมาณคดีมาก หรือผู้รับบริการมากควรจัดสรรตำแหน่งเพิ่มเติมเพื่อให้สามารถรองรับการปฏิบัติงานในการแก้ไขปัญหาได้ทันท่วงที ด้านนโยบายเรื่องเกี่ยวกับที่ตั้งศาลถ้าตั้งอยู่ใกล้น้ำทะเลส่งผลต่ออุปกรณ์ชำรุด หรือระบบที่เกิดขึ้นใหม่นั้นมีความซ้ำซ้อนกับระบบเดิม มีรหัสผู้ใช้และรหัสผ่านมากจากการที่เพิ่มขึ้นของหลายระบบ ดังภาพประกอบ 9



ภาพประกอบ 9 ปัญหาและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

4.4 เสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

จากการลงพื้นที่สัมภาษณ์ ผู้ให้ข้อมูลสัมภาษณ์เชิงลึกได้ให้ข้อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ดังคำสัมภาษณ์ต่อไปนี้

ด้านงบประมาณ

การจัดซื้อครุภัณฑ์คอมพิวเตอร์ตามโครงการต่าง ๆ ความต้องการครุภัณฑ์คอมพิวเตอร์ที่ยังไม่เพียงพอ และการใช้โปรแกรมที่มีความจำเป็นต้องใช้งาน ดังคำให้สัมภาษณ์ของผู้ให้ข้อมูลหลักดังนี้

“...เห็นการจัดซื้อครุภัณฑ์คอมพิวเตอร์ตามโครงการต่าง ๆ ไม่สามารถจัดซื้อได้เพราะราคาที่ส่วนกลางประมาณการมาเป็นการซื้อจำนวนมาก ควรให้ส่วนกลางเป็นผู้จัดซื้อและจัดส่งมาให้ตามศาลต่าง ๆ...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...ด้านงบประมาณอยากให้จัดสรรเครื่องคอมพิวเตอร์มาให้เพียงพอจะได้ไม่ต้องใช้เครื่องคอมพิวเตอร์ที่ถูกทดแทนแล้ว...”

(ผู้ให้ข้อมูลหลักคนที่ 12, 3 มกราคม 2566 : สัมภาษณ์)

“...ในด้านงบประมาณเห็นว่าควรจัดสรรเครื่องคอมพิวเตอร์มาให้เพียงพอ และในส่วนของซอฟต์แวร์ต่าง ๆ ควรจัดสรรมาด้วยเพื่อลดความเสี่ยงจากภัยคุกคามไซเบอร์...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 3 มกราคม 2566 : สัมภาษณ์)

สรุปได้ว่า การจัดซื้อครุภัณฑ์คอมพิวเตอร์ตามโครงการต่าง ๆ ความต้องการครุภัณฑ์คอมพิวเตอร์ที่ยังไม่เพียงพอ และการใช้โปรแกรมที่มีความจำเป็นต้องใช้งาน ควรให้ส่วนกลางสนับสนุนงบประมาณและดำเนินการจัดซื้อให้กับหน่วยงานศาลยุติธรรม

ด้านทักษะบุคลากร

ทักษะบุคลากรมีความจำเป็นสำหรับการปฏิบัติงานจะทำให้การทำงานประสบผลสำเร็จ และการรู้เท่าทันภัยคุกคามไซเบอร์จะทำให้ระบบภายในหน่วยงานศาลยุติธรรมมีความปลอดภัยมากขึ้น ดังคำให้สัมภาษณ์ของผู้ให้ข้อมูลหลักดังนี้

“...การที่สำนักงานศาลยุติธรรม มีการออกนโยบายหรือโปรแกรมให้ดำเนินการก็ควรให้มีการจัดอบรมให้สามารถปฏิบัติงานได้ทันที และมีการอบรมเกี่ยวกับภัยคุกคามทางไซเบอร์ด้วย...”

(ผู้ให้ข้อมูลหลักคนที่ 18, 10 มกราคม 2566 : สัมภาษณ์)

ด้านจำนวนบุคลากรทางด้านไซเบอร์

หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีจำนวนบุคลากรด้านไซเบอร์หน่วยละ 1 ท่านทำให้การแก้ไขปัญหาได้ล่าช้าและส่งผลต่อความเสี่ยงจากภัยคุกคามไซเบอร์ได้ ควรเพิ่มจำนวนเจ้าหน้าที่ผู้ดูและระบบ ดังคำให้สัมภาษณ์ของผู้ให้ข้อมูลหลักดังนี้

“...ควรเพิ่มอัตรากำลังบุคลากรทางด้านไซเบอร์เพิ่มเติม ตามขนาดศาลหรือปริมาณคดี หรือคอมพิวเตอร์ หรือผู้รับบริการ...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 3 มกราคม 2566 : สัมภาษณ์)

ด้านนโยบายของหน่วยงาน

ในด้านนโยบายของหน่วยงานศาลยุติธรรมในเรื่องของการจัดตั้งที่ทำการควรอยู่ห่างจากทะเล และในการพัฒนาระบบงานที่มีความซ้ำซ้อนของระบบ ดังคำให้สัมภาษณ์ของผู้ให้ข้อมูลหลักดังนี้

“...ในด้านนโยบายการจัดตั้งอาคารที่ทำการอยู่ใกล้ทะเลอยากให้พิจารณาไม่ให้สถานที่ตั้งอยู่ใกล้ทะเล เพราะทำให้อุปกรณ์พวกเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ป้องกันเครือข่าย และอุปกรณ์กระจายสัญญาณชำรุด เกิดคราบเกลือ สนิม...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

“...การที่สำนักงานศาลยุติธรรม มีการออกนโยบายหรือโปรแกรมให้ดำเนินการก็ไม่ควรซ้ำซ้อนกับโปรแกรมเดิมที่มีอยู่ โดยให้มีการจัดอบรมให้สามารถปฏิบัติงานได้ทันที และมีการอบรมเกี่ยวกับภัยคุกคามทางไซเบอร์ด้วย...”

(ผู้ให้ข้อมูลหลักคนที่ 18, 10 มกราคม 2566 : สัมภาษณ์)

สรุปได้ว่า นโยบายของหน่วยงานในการจัดตั้งอาคารที่ทำการควรพิจารณาที่ตั้งให้อยู่ห่างจากทะเล หรือออกแบบอาคารวัสดุอุปกรณ์เพื่อเป็นการป้องกันความเสียหายของอุปกรณ์ต่าง ๆ และในส่วนนโยบายระบบงานใหม่ ๆ ควรเป็นระบบที่ไม่ซ้ำซ้อนกับระบบเดิมที่มีอยู่เดิม

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

การศึกษาเรื่องการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีวัตถุประสงค์ 1) เพื่อศึกษาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 2) เพื่อศึกษาความสำเร็จและอุปสรรคในการดำเนินงานด้านการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 3) เพื่อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

การวิจัยนี้ใช้วิธีแบบเชิงคุณภาพ เป็นรูปแบบการวิจัยเชิงพรรณนา กลุ่มผู้ให้ข้อมูลหลักที่ใช้ในการวิจัยมี 2 กลุ่ม ได้แก่ เจ้าหน้าที่ผู้ดูแลระบบ และเจ้าหน้าที่ผู้ปฏิบัติงานศาลในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ด้านการวิเคราะห์ข้อมูลได้นำข้อมูลที่มีการเก็บรวบรวมจากการสัมภาษณ์เชิงลึก (In-Depth Interview) และนำข้อมูลมาวิเคราะห์โดยใช้เทคนิคการวิเคราะห์ข้อมูลเชิงคุณภาพแล้วนำมาเขียนเป็นข้อความเพื่อวิเคราะห์สร้างข้อสรุปตามกรอบแนวคิดในการวิจัย เพื่อตอบคำถามของการวิจัย

5.1 สรุปผลการวิจัย

การสรุปผลการศึกษาการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 แบ่งการนำเสนอออกเป็น 4 ส่วน ดังนี้

1. ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
2. เครื่องมือ มาตรการ และแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
3. ความสำเร็จและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9
4. แนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

1. ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

จากผลการศึกษาสามารถสรุปปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ได้แก่

การใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด เป็นการดาวน์โหลดไดร์เวอร์ของอุปกรณ์ต่อพ่วงหรือการที่ดาวน์โหลดโปรแกรมอื่นที่ไม่ได้เกี่ยวกับการใช้งานของศาลซึ่งอาจก่อให้เกิดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่แฝงมากับตัวโปรแกรมที่ดาวน์โหลดมาติดตั้งที่เครื่องคอมพิวเตอร์ได้

การใช้เครือข่ายไร้สาย คือการที่นำเอาอุปกรณ์ส่วนตัวมาเชื่อมต่อกับระบบภายในศาล ได้แก่ โทรศัพท์เคลื่อนที่ หรือคอมพิวเตอร์ส่วนบุคคลของเจ้าหน้าที่ ซึ่งการเชื่อมต่อระบบดังกล่าวอาจส่งผลกระทบต่อระบบเครือข่ายภายในศาลเพราะไม่ว่าจะเป็นโทรศัพท์เคลื่อนที่ หรือคอมพิวเตอร์ส่วนบุคคลของเจ้าหน้าที่ก็อาจมีไวรัสแฝงอยู่ด้วย

สภาพแวดล้อมจากระบบไฟฟ้าขัดข้อง ได้แก่ ไฟตก ไฟกระชาก ซึ่งจะส่งผลต่อฮาร์ดแวร์และซอฟต์แวร์ เช่น ในส่วนของฮาร์ดแวร์ ทำให้คอมพิวเตอร์แม่ข่ายเสียหาย ทั้งในส่วนอุปกรณ์หรือฐานข้อมูลภายในเครื่อง หรืออุปกรณ์ป้องกันเครือข่าย (Firewall) ถ้าอุปกรณ์ชำรุดเสียหายก็เป็นการเปิดช่องโหว่ให้เกิดความเสี่ยงจากภัยคุกคามไซเบอร์ได้ และในส่วนของซอฟต์แวร์ ระหว่างที่บันทึกข้อมูลทำให้ข้อมูลไม่ถูกบันทึกเข้าฐานข้อมูลหรือโปรแกรมค้าง ช้า ชำรุดเสียหายเพราะอุปกรณ์ชำรุดแล้ว

การโจมตีแบบไม่ตั้งใจ สามารถแยกออกเป็นหลายประเด็น ได้แก่ การเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานและบุคคลอื่นซึ่งเกิดจากการที่ผู้ใช้งานไม่ได้ล็อกเอาท์ออกจากระบบ การขาดแคลนบุคลากรด้านไซเบอร์ก็ส่งผลในเรื่องของการแก้ไขปัญหาทำให้ล่าช้าและอาจส่งผลกระทบมากขึ้นด้วย การนำเอาอุปกรณ์อื่นมาเชื่อมต่อระบบคอมพิวเตอร์ เช่น การนำเอาแฟลชไดร์ฟมาต่อเข้าระบบคอมพิวเตอร์ก็จัดว่ามีความเสี่ยงจากไวรัสและสามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในศาลด้วย ในส่วนการตั้งรหัสผ่านและการเก็บรักษารหัสผ่านระบบการตั้งรหัสผ่านที่คาดเดาได้ง่ายอาจทำให้ผู้ไม่ประสงค์ดีเข้าใช้งานแทนเจ้าของรหัสผู้ใช้นั้นได้ และการบันทึกรหัสผ่านก็เป็นปัจจัยที่สำคัญต้องบันทึกจัดเก็บไว้ในที่ลับเฉพาะ เช่นสมุดจดบันทึกส่วนตัวหรือที่เก็บในรูปแบบอื่นที่ผู้อื่นไม่สามารถล่วงรู้ได้ ในส่วนการเข้าลิงค์จากอีเมล และการเข้าเว็บไซต์ถือว่าเป็นภัยที่มีความเสี่ยงมากเพราะการเข้าไปตามลิงค์หรือเว็บดังกล่าวผู้ไม่ประสงค์ดีก็มีการปล่อยไวรัสเพื่อมาเจาะระบบหรือดักจับข้อมูลออกไป ในส่วนเรื่องคอมพิวเตอร์สำหรับใช้ปฏิบัติงานไม่เพียงพอระบบราชการยังมีความไม่พร้อมในเรื่องงบประมาณซึ่งจำเป็นที่จะต้องนำเครื่องคอมพิวเตอร์ที่ถูกทดแทนแล้วมาใช้งานซึ่งไม่สามารถปรับปรุงรุ่นระบบปฏิบัติการให้มีความปลอดภัยได้ทำให้เกิดช่องโหว่ ส่วนคอมพิวเตอร์บริการคู่ความเชื่อมไปยังเครื่องคอมพิวเตอร์แม่ข่ายเป็นความเสี่ยงที่ระบบส่งสำนวนคดีศาลชั้นต้นถ้าบุคคลผู้มีความรู้ด้านคอมพิวเตอร์ก็

สามารถเข้าไปจัดการกับข้อมูลนี้ได้ ซึ่งหน่วยงานศาลควรจะใช้การเชื่อมยังฐานสำรองแทนในเครื่องที่ให้บริการ และในส่วนการติดตั้งโปรแกรมแอนตี้ไวรัสบางเครื่องไม่สามารถทำได้เนื่องจากคอมพิวเตอร์ดังกล่าวเป็นคอมพิวเตอร์ที่ถูกจัดสรรทดแทนจึงไม่สามารถซื้อลิขสิทธิ์แอนตี้ไวรัสได้

การโจมตีแบบตั้งใจสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีโอกาสที่จะถูกโจมตีแบบตั้งใจจากผู้ไม่ประสงค์ดีได้โดยตลอด เพราะผู้ไม่ประสงค์ดีก็จะหาช่องโหว่ของระบบเข้ามาเจาะระบบได้หลายช่องทาง หลายวิธีการ

2. เครื่องมือ มาตรการ และแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

สำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีเครื่องมือ มาตรการ และแนวปฏิบัติจะช่วยป้องกันและลดความเสี่ยงจากภัยคุกคามไซเบอร์ได้ดังนี้

2.1 เครื่องมือในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

การติดตั้งฮาร์ดแวร์และซอฟต์แวร์เป็นเครื่องมือในการป้องกันภัยคุกคามไซเบอร์ โดยหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีเครื่องมือโดยเฉพาะ คืออุปกรณ์ป้องกันเครือข่าย (Firewall) และซอฟต์แวร์แอนตี้ไวรัสซึ่งทางสำนักงานศาลยุติธรรมได้จัดสรรให้กับทุกหน่วยงานศาล ทำให้ระบบมีความมั่นคงปลอดภัยมากยิ่งขึ้น

การแนะนำและอบรมเป็นเครื่องมือที่ดี คือการจัดการกับบุคลากรให้มีความตระหนักมีความรู้ความเข้าใจจากภัยคุกคามไซเบอร์ซึ่งทางสำนักงานศาลยุติธรรมหรือหน่วยงานศาลยุติธรรมในสังกัดเขตอำนาจอธิบดีผู้พิพากษาภาค 9 จะมีจัดอบรมการใช้งานระบบการทบทวน การใช้งานระบบคอมพิวเตอร์ที่ควรระมัดระวัง เป็นสิ่งสำคัญทำให้เจ้าหน้าที่ผู้ปฏิบัติงานสามารถปฏิบัติงานได้อย่างถูกต้อง ครบถ้วน ปลอดภัยทั่วทั้งหน่วยงาน

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นเครื่องมือที่สำนักงานศาลยุติธรรมได้มีการกำหนดให้จัดทำแผนการบริหารความเสี่ยงประจำปี พ.ศ.2566 ซึ่งมีด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หัวข้อที่เกี่ยวข้องคือ ระบบรักษาความมั่นคงปลอดภัยของข้อมูลจากการบุกรุกและภัยคุกคามที่อาจจะเกิดขึ้นจากผู้ที่ไม่ประสงค์ดี

2.2 มาตรการในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

สำหรับมาตรการในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ได้แก่

คำสั่งแต่งตั้งและมอบหมายงาน ในการปฏิบัติงานตามอำนาจหน้าที่ของเจ้าหน้าที่จะต้องมีการแต่งตั้งและมอบหมาย ให้กับเจ้าหน้าที่ผู้ปฏิบัติงานในแต่ละตำแหน่งหรือแต่ละส่วนงานที่รับผิดชอบอย่างชัดเจน

การควบคุมจำกัดสิทธิในการใช้งาน ของแต่ละตำแหน่งและกลุ่มงาน สิทธิในอำนาจหน้าที่ที่รับผิดชอบจะเป็นไปกับสิทธิในการใช้งานโปรแกรมแต่ละระบบ

การจำกัดการใช้งานอุปกรณ์ส่วนตัวจะช่วยให้ระบบปลอดภัยมากขึ้น เพราะการที่มีอุปกรณ์เชื่อมต่อในเครือข่ายจำนวนมากเท่าไร ความเสี่ยงที่จะเกิดภัยคุกคามทางไซเบอร์ก็จะเพิ่มขึ้นไปด้วย

2.3 แนวปฏิบัติการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์

แนวปฏิบัติเป็นการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ซึ่งหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีแนวปฏิบัติดังนี้

สำรองข้อมูล เป็นการรับประกันได้ว่าถ้าเกิดเหตุการณ์ฐานข้อมูลล่ม หรือจากการถูกโจมตีจากภัยคุกคามไซเบอร์หรือรูปแบบอื่น ก็ยังมีฐานสำรองล่าสุดซึ่งสามารถนำมาใช้งานได้

เก็บประวัติการใช้งานระบบต่าง ๆ จะช่วยให้ทราบว่าผู้ใช้งานระบบดำเนินการอะไรบ้างเกี่ยวกับระบบ เช่น เพิ่มข้อมูล แก้ไขข้อมูล ลบข้อมูล เป็นต้น

อัพเดตระบบปฏิบัติการ การปรับปรุงระบบปฏิบัติการเป็นเรื่องที่สำคัญ นอกจากจะมีฟังก์ชันเพิ่มขึ้นมาแล้วยังมีการปรับปรุงที่จะทำให้ระบบปฏิบัติการนั้นมีความปลอดภัยมากขึ้น

การตั้งรหัสผ่านและการบันทึกรหัสผ่าน การตั้งรหัสผ่านที่คาดเดาได้ยาก และจดบันทึกรหัสผ่านในสมุดบันทึกส่วนตัว หรือจะใช้ความจำในการจำรหัส ซึ่งจะมีความปลอดภัยมากยิ่งขึ้น

การสแกนไวรัส ในการใช้อุปกรณ์แฟลชไดร์ฟต่อเข้ากับระบบคอมพิวเตอร์ควรจะสแกนไวรัสก่อนการเปิดไฟล์หรือคัดลอกไฟล์ต่าง ๆ กับคอมพิวเตอร์เครื่องนั้น ๆ

ไม่ให้ใช้แฟลชไดร์ฟ การไม่ใช้แฟลชไดร์ฟจะช่วยลดความเสี่ยงจากการติดไวรัส จากระบบที่จะแพร่กระจายไปต่อเครื่องอื่น ๆ ได้

3. ความสำเร็จและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

3.1 ความสำเร็จในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่

การรักษาความลับ ระบบต่าง ๆ ของสำนักงานศาลยุติธรรมมีการกำหนดสิทธิในการเข้าถึงข้อมูลในการปฏิบัติหน้าที่ตามอำนาจหน้าที่ ซึ่งบางระบบจำเป็นต้องมีคำสั่งแต่งตั้ง ทำให้บุคคลอื่นซึ่งไม่มีสิทธิในระบบก็จะไม่สามารถเข้าถึงข้อมูลได้

การรักษาความถูกต้อง ข้อมูลในระบบของฐานข้อมูลของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ความถูกต้อง ครบถ้วนแม่นยำจะเกิดขึ้นได้ เริ่มต้น

จากการบันทึกข้อมูลเข้าระบบ แก้ไขข้อมูล และบันทึกข้อมูล โดยส่วนที่จะกระทบกับความครบถ้วนของข้อมูล ได้แก่ ผู้บันทึกข้อมูล หรือระบบไฟฟ้าขัดข้อง เป็นต้น

สภาพพร้อมใช้งาน ความพร้อมใช้งานของฮาร์ดแวร์ขึ้นอยู่กับระบบไฟฟ้า ซึ่งถ้าอุปกรณ์ต่าง ๆ มีเครื่องสำรองไฟฟ้าในการป้องกันแรงดันไฟฟ้าไม่เสถียรจะทำให้ฮาร์ดแวร์หรืออุปกรณ์มีความพร้อมมากขึ้น แต่ถ้าเป็นคอมพิวเตอร์ที่ถูกทดแทนเสื่อมตามอายุการใช้งาน และในส่วนซอฟต์แวร์นั้นขึ้นกับลิขสิทธิ์ของซอฟต์แวร์นั้น ๆ สำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีความพร้อมใช้งาน

3.2 ปัญหาและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่

ด้านงบประมาณ ในการจัดซื้อครุภัณฑ์คอมพิวเตอร์ตามโครงการต่าง ๆ ซึ่งไม่สามารถดำเนินการได้เพราะราคาในท้องถิ่นจะสูงกว่าที่ส่วนกลางประมาณการแบบเหมารวม การจัดสรรครุภัณฑ์คอมพิวเตอร์ยังไม่เพียงพอต่อความต้องการการใช้งาน และโปรแกรมที่มีความจำเป็นต้องใช้งานแต่ไม่มีลิขสิทธิ์

ด้านทักษะบุคลากร การที่สำนักงานศาลยุติธรรมมีการนำระบบต่าง ๆ มาใช้ในการสนับสนุนการปฏิบัติงาน มีความจำเป็นที่จะต้องอบรมหรือพัฒนาทักษะให้กับบุคลากร และต้องทบทวนให้สม่ำเสมอ

ด้านจำนวนบุคลากรทางด้านไซเบอร์ หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีจำนวนบุคลากรทางไซเบอร์ขาดแคลนไม่สามารถรองรับการปฏิบัติงานในการแก้ไขปัญหาได้ทันท่วงที

ด้านนโยบายของหน่วยงาน เรื่องเกี่ยวกับที่ตั้งศาลถ้าตั้งอยู่ใกล้น้ำทะเลจะดำเนินการอย่างไร ในการป้องกันไม่ให้เกิดคราบเกลือ สนิม ทำให้อุปกรณ์เสื่อมสภาพเร็วขึ้น หรือระบบที่เกิดขึ้นใหม่ทำอย่างไรให้ระบบไม่เกิดการทำงานที่ซ้ำซ้อนมีรหัสผู้ใช้และรหัสผ่านมากจากการที่เพิ่มขึ้นของหลายระบบ

4. แนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

4.1 ด้านงบประมาณ

ในการจัดซื้อครุภัณฑ์คอมพิวเตอร์ตามโครงการต่าง ๆ ให้ส่วนกลางเป็นผู้จัดซื้อและจัดส่งครุภัณฑ์คอมพิวเตอร์มาให้ตามศาลต่าง ๆ

สำรวจความต้องการเพิ่มเติมครุภัณฑ์คอมพิวเตอร์ ความต้องการใช้โปรแกรมที่มีความจำเป็นต้องใช้งานแต่ไม่มีลิขสิทธิ์ และอุปกรณ์เครือข่ายที่หมดอายุการรับประกันเพื่อต่อประกันและบำรุงรักษาอุปกรณ์เครือข่ายอยู่เสมอเสนอของบประมาณ

4.2 ด้านทักษะบุคลากร

การนำระบบต่าง ๆ มาใช้ในการสนับสนุนการปฏิบัติงานกรณีมีความคล้ายคลึงเหมือนกันควรปรับเป็นโปรแกรมเดียวกันผู้ใช้งานระบบจะได้สะดวกและความพร้อมในการปฏิบัติงาน ซึ่งการอบรมหรือพัฒนาทักษะให้กับเจ้าหน้าที่ผู้ปฏิบัติงานและเจ้าหน้าที่ผู้ดูแลระบบของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 และต้องทบทวนให้สม่ำเสมอ

4.3 ด้านจำนวนบุคลากรทางด้านไซเบอร์

การขออัตรากำลังบุคลากรทางด้านไซเบอร์เพิ่มเติม ควรพิจารณาตามขนาดศาลหรือปริมาณคดี หรือจำนวนคอมพิวเตอร์ หรือผู้รับบริการ จัดทำข้อมูลประกอบให้กับสำนักงานศาลยุติธรรม หรือใช้บุคลากรทางด้านไซเบอร์ร่วมกันภายในจังหวัดกรณี ระบบมีปัญหาต้องรีบแก้ไข ในระหว่างการรออัตรากำลัง

4.4 ด้านนโยบายของหน่วยงาน

การตั้งอาคารที่ทำการอยู่ใกล้ทะเลควรออกแบบอาคารและวัสดุในการปกป้องอุปกรณ์ ครุภัณฑ์ต่าง ๆ ไม่ให้เกิดความเสียหาย ไม่ให้เกิดคราบเกลือ สนิม ระบบใหม่ควรเป็นระบบที่ไม่ซ้ำซ้อนกับระบบเดิมที่มีอยู่เดิม การตั้งรหัสผู้ใช้และรหัสผ่านเป็นแบบเดียวกันในทุกระบบ การยืนยันตัวตนที่อนุญาตให้ผู้ใช้ลงชื่อเข้าใช้หลายแอปพลิเคชันและเว็บไซต์

5.2 การอภิปราย

จากการศึกษาเรื่องการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 อภิปรายผลได้ดังนี้ ได้แก่

5.2.1 ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ปัจจัยความเสี่ยงจากการใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด สาเหตุมาจากหลากหลายความต้องการ เช่น ติดตั้งไดร์เวอร์เพื่อติดตั้งอุปกรณ์ หรือการดาวน์โหลดโปรแกรมสำหรับการใช้งานโปรแกรมต่าง ๆ ที่เจ้าหน้าที่ต้องการจะติดตั้งเพื่อใช้งานโดยโปรแกรมต่าง ๆ ซึ่งอาจอยู่ในรูปแบบฟรีแวร์ แชร์แวร์ โปรแกรมดังกล่าวมีความเสี่ยงที่จะนำพาไวรัสหรือสิ่งไม่พึงประสงค์เข้ามาในระบบคอมพิวเตอร์ได้

การใช้เครือข่ายไร้สายที่เกิดความเสี่ยงจากการที่นำเอาอุปกรณ์ส่วนตัว ได้แก่ โทรศัพท์มือถือ เครื่องคอมพิวเตอร์แบบพกพา ซึ่งอาจมีไวรัสหรือสิ่งไม่พึงประสงค์แปลกปลอมเข้ามาด้วยผ่านการเชื่อมต่อเครือข่ายไร้สายภายในศาลได้

โดยปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ข้างต้น สอดคล้องกับ วิศณุ สร้างวงศ์ใหม่ (2561) ศึกษาการเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์ พบว่าองค์กรสมัยใหม่ทั้งภาครัฐและเอกชนต่างพึ่งพาเทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงานให้ประสบความสำเร็จ ระบบสารสนเทศมีความซับซ้อนตั้งแต่ระบบบัญชี การเงิน บุคลากรหรือระบบควบคุมอุตสาหกรรม ระบบอาวุธ ระบบดังกล่าวมีความเสี่ยงที่จะเสียหาย ผู้บริหารทุกระดับจำเป็นต้องตระหนักถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล ดังนั้น การวางแผนเพื่อเตรียมรับมือกับเหตุการณ์และการบริหารความเสี่ยงจะทำให้ค่าความเสียหายลดลง หรืออาจไม่เกิดเหตุการณ์

ส่วนณรงค์เวตย์ เรืองจวง (2561) ศึกษาแนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ พบว่าขีดความสามารถการปฏิบัติการด้านไซเบอร์ของกองทัพอากาศ การปฏิบัติเชิงรับอยู่ในระดับดีและการปฏิบัติเชิงรุกอยู่ในระดับปานกลาง มีนโยบาย กระบวนการแผนแม่บท และแผนงานที่เกี่ยวข้องรองรับการปฏิบัติเกือบทุกด้าน แต่ยังขาดแนวความคิดการปฏิบัติการด้านไซเบอร์ รวมถึงมีระบบและอุปกรณ์ที่ทันสมัยมีประสิทธิภาพ ปัจจัยที่มีผลกระทบต่อขีดความสามารถในการปฏิบัติด้านไซเบอร์คือ บุคลากร ซึ่งมีไม่เพียงพอ ขาดความรู้และทักษะในการปฏิบัติงานด้านไซเบอร์ ระบบการจัดการความรู้มีข้อมูลไม่ครบถ้วนและโครงสร้างการจัดหน่วยสามารถรองรับบุคลากรที่ปฏิบัติงานได้ในปัจจุบันเท่านั้น ดังนั้นต้องพัฒนาบุคลากรด้วยการให้การศึกษา การฝึกปฏิบัติ การอบรมทบทวนให้มีความรู้ความสามารถ มีทักษะ พร้อมที่จะปฏิบัติภารกิจด้านไซเบอร์ได้อย่างมีประสิทธิภาพเร่งดำเนินการจัดทำแนวความคิดการปฏิบัติการด้านไซเบอร์เพื่อให้บุคลากรนำไปเป็นแนวทางการปฏิบัติภารกิจทบทวนแผนงานให้ทันสมัยและครอบคลุมการปฏิบัติ และควรจัดทำระบบการจัดการความรู้ให้มีข้อมูลถูกต้องครบถ้วน หากมีภารกิจด้านไซเบอร์มากขึ้นควรพิจารณาทบทวนโครงสร้างการจัดหน่วยให้สอดคล้องกับการปฏิบัติภารกิจด้วย

ปัจจัยการโจมตีแบบตั้งใจเป็นกรณีที่ระบบอาจมีโอกาสที่จะถูกโจมตีแบบตั้งใจจากผู้ไม่ประสงค์ดีได้หลากหลายช่องทาง หรือจากการขาดความรู้ความตระหนักของเจ้าหน้าที่ผู้ปฏิบัติงานหรือผู้ดูแลระบบก็เป็นช่องโหว่ที่ทำให้ผู้ไม่ประสงค์ดีเข้ามาในระบบได้โดยง่าย

ปัจจัยการโจมตีแบบไม่ตั้งใจสามารถแยกออกเป็นหลายประเด็น ได้แก่ การเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานและบุคคลอื่น การขาดแคลนบุคลากรด้านไซเบอร์ การนำเอาอุปกรณ์อื่นมาเชื่อมต่อระบบคอมพิวเตอร์ การตั้งรหัสผ่านและการเก็บรักษารหัสผ่าน การเข้าลิงค์จากอีเมล และการเข้าเว็บไซต์ คอมพิวเตอร์สำหรับใช้ปฏิบัติงานไม่เพียงพอ คอมพิวเตอร์บริการคู่ความเชื่อมไปยังเครื่องคอมพิวเตอร์แม่ข่าย การติดตั้งโปรแกรมแอนตี้ไวรัสบางเครื่องไม่สามารถทำได้ จากผลการศึกษาในประเด็นนี้เป็นปัจจัยการโจมตีที่มีความสำคัญมาก

ที่สุด เนื่องจากเกี่ยวกับความรู้ทักษะความตระหนักรู้ของผู้ปฏิบัติงานและผู้ดูแลระบบ เป็นช่องโหว่ที่ทำให้เกิดความเสี่ยงจากภัยคุกคามไซเบอร์ในด้านนี้มาก

ด้านปัจจัยความเสี่ยงจากการภัยคุกคามไซเบอร์จากสภาพแวดล้อมที่เกิดจากระบบไฟฟ้าขัดข้อง ได้แก่ ไฟตก ไฟกระชาก ซึ่งจะส่งผลต่อฮาร์ดแวร์และซอฟต์แวร์ ซึ่งสอดคล้องกับ อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) ศึกษาเรื่องการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร และเสนอวิธีการบริหารความเสี่ยงอย่างเหมาะสมเป็นไปตามมาตรฐานสากล สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเกิดขึ้นกับระบบสารสนเทศขององค์กรได้ในอนาคตโดยอธิบายถึงกระบวนการบริหารความเสี่ยง ตั้งแต่กระบวนการเตรียมการ กระบวนการประเมินความเสี่ยง การรายงานผล การประเมินความเสี่ยงและการติดตามผลการประเมินความเสี่ยงตามวงรอบ และการกำหนดมาตรการควบคุม เพื่อตอบสนองต่อความเสี่ยงที่เกิดขึ้นจากการสังเคราะห์กรอบแนวคิด NIST Framework กฎหมาย ระเบียบข้อบังคับ ข้อมูลจากเอกสารทางวิชาการต่าง ๆ เพื่อให้ได้แนวทางปฏิบัติ และลำดับกระบวนการบริหารความเสี่ยงอย่างเป็นระบบที่สามารถนำไปปฏิบัติหรือประยุกต์ใช้ได้จริงในองค์กร

ดังนั้น ประเภทภัยคุกคามจากไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มี 5 ประเภท ได้แก่ การใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด การใช้เครือข่ายไร้สาย การโจมตีแบบไม่ตั้งใจ การโจมตีแบบตั้งใจ และสภาพแวดล้อมจากระบบไฟฟ้าขัดข้อง

5.2.2 เครื่องมือ มาตรการ และแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีเครื่องมือในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ดังนี้

เครื่องมือที่สำคัญคือการติดตั้งฮาร์ดแวร์และซอฟต์แวร์ โดยหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 จะมีอุปกรณ์ป้องกันเครือข่าย (Firewall) และซอฟต์แวร์แอนตี้ไวรัส ที่ส่วนกลางจะมีอุปกรณ์ป้องกันเครือข่ายซ้อนอีกชั้นเช่นกัน ก่อนที่ทุกหน่วยงานจะออกไปยังระบบเครือข่ายภายนอกหรืออินเตอร์เน็ต ซึ่งอุปกรณ์ดังกล่าวได้แก่ อุปกรณ์การตรวจจับและป้องกันภัยคุกคามที่เกิดจากภายในระบบเครือข่าย (Intrusion Detection and Prevention System) การป้องกันการแพร่กระจายไวรัสผ่านเครือข่ายอินเทอร์เน็ตเข้าสู่เครือข่าย (Anti-Virus Gateway) ทำให้ระบบโดยรวมมีความมั่นคงปลอดภัยทางไซเบอร์มากขึ้น และในการแนะนำและอบรมการจัดการบุคลากรให้มีความตระหนักมีความรู้ความเข้าใจจากภัยคุกคามไซเบอร์ เจ้าหน้าที่ผู้ดูแลระบบให้มีทักษะการจัดการภัยคุกคามไซเบอร์ และมีการ

บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งสำนักงานศาลยุติธรรมได้มีการกำหนดให้จัดทำแผนการบริหารความเสี่ยงประจำปี พ.ศ.2566 มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งมีหัวข้อที่เกี่ยวข้องคือ ระบบรักษาความมั่นคงปลอดภัยของข้อมูลจากการบุกรุกและภัยคุกคามที่อาจจะเกิดขึ้นจากผู้ที่ไม่ประสงค์ดีเพิ่มเข้ามาทำให้เห็นได้ว่าสำนักงานศาลยุติธรรมได้ให้ความสำคัญกับความเสี่ยงจากภัยคุกคามไซเบอร์

ส่วนมาตรการในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีดังนี้

มีคำสั่งแต่งตั้งและมอบหมายงาน ในการปฏิบัติงานตามอำนาจหน้าที่ของเจ้าหน้าที่จะต้องมีการคำสั่งแต่งตั้งและมอบหมายในการปฏิบัติงาน เพื่อขออนุญาตสิทธิในการเข้าใช้งานระบบต่าง ๆ ตามที่ได้รับมอบหมาย และจะมีการควบคุมจำกัดสิทธิในการใช้งาน ของแต่ละตำแหน่งและกลุ่มงาน ระดับการเข้าถึงข้อมูลได้แก่ การเพิ่ม การแก้ไข การลบ การตรวจสอบข้อมูลในระบบต่าง ๆ และการจำกัดการใช้งานอุปกรณ์ส่วนตัวจะเป็นการจำกัดการใช้อุปกรณ์ส่วนตัวของเจ้าหน้าที่ผู้ปฏิบัติงานที่จะนำมาเชื่อมต่อเข้ากับระบบเครือข่ายภายในของศาลซึ่งจะต้องขออนุญาตจากผู้ดูแลระบบ จะช่วยให้ระบบปลอดภัยมากขึ้น

สำหรับแนวปฏิบัติการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีดังนี้

การสำรองข้อมูลเป็นประจำจะช่วยให้ระบบมีข้อมูลที่มีการปรับปรุงเป็นปัจจุบันมากที่สุด รองรับเหตุการณ์ต่าง ๆ เช่น ฐานข้อมูลล่ม ข้อมูลเสียหาย หรือจากการถูกโจมตีจากภัยคุกคามไซเบอร์หรือรูปแบบอื่น ๆ มีฐานสำรองที่เป็นปัจจุบันล่าสุดซึ่งสามารถนำมาใช้งานได้

การเก็บประวัติการใช้งาน (Log) ระบบต่าง ๆ จะทำให้ทราบว่าผู้ใช้งานระบบดำเนินการเกี่ยวกับระบบตั้งแต่ต้นทางไปยังปลายทาง ในขั้นตอนกระบวนการต่าง ๆ อย่างไรบ้าง เป็นความรับผิดชอบของเจ้าหน้าที่ผู้ปฏิบัติงานตามอำนาจหน้าที่ที่มีคำสั่งแต่งตั้งและมอบหมายงานนั้น ๆ

ส่วนการอัพเดตระบบปฏิบัติการ การปรับปรุงระบบปฏิบัติการมีฟังก์ชันเพิ่มขึ้นมาและมีการปรับปรุงที่จะทำให้ระบบปฏิบัติการนั้นมีความปลอดภัยมากขึ้น ดังนั้นจึงควรปรับปรุงระบบปฏิบัติการสม่ำเสมอ และการปรับปรุงระบบปฏิบัติการดังกล่าวจะไม่สามารถทำได้กับเครื่องที่ไม่รองรับระบบปฏิบัติการปัจจุบัน ได้แก่ เครื่องคอมพิวเตอร์ที่ถูกทดแทนแล้ว เครื่องดังกล่าวจะมีช่องโหว่ความเสี่ยงจากภัยคุกคามไซเบอร์ได้มากถ้าเชื่อมต่อกับระบบเครือข่ายภายในของหน่วยงาน เครื่องคอมพิวเตอร์ที่ถูกทดแทนไม่ควรนำมาเชื่อมต่อกับระบบเครือข่ายภายในของหน่วยงานเพื่อความปลอดภัยจากภัยคุกคามทางไซเบอร์

การตั้งรหัสผ่านและการบันทึกรหัสผ่าน โดยการตั้งรหัสผ่านที่คาดเดาได้ยาก ควรจะตั้งรหัสที่ประกอบไปด้วยตัวอักษร ตัวใหญ่ ตัวเล็ก ตัวเลข และอักขระพิเศษ หรือ

ตามที่ระบบแนะนำและควรเปลี่ยนรหัสผ่านบ่อย ๆ หรือมีการแจ้งเตือนให้เปลี่ยนรหัสผ่านอยู่เสมอ และจดบันทึกรหัสผ่านในสมุดบันทึกส่วนตัว จะช่วยป้องกันการเข้าใช้งานระบบจากผู้ไม่ประสงค์ดีหรือโดยไม่ตั้งใจ มีความปลอดภัยจากการจัดการข้อมูลมากยิ่งขึ้น

ในส่วนการไม่ให้แฟลชไดร์ฟ จะช่วยลดความเสี่ยงจากการติดไวรัส จากระบบที่จะแพร่กระจายไปต่อเครื่องอื่น ๆ ได้เนื่องจากเป็นการบริการประชาชนหรือคู่ความถ้าหลีกเลี่ยงไม่ได้มีความจำเป็นต้องใช้แฟลชไดร์ฟจำเป็นต้องทำการสแกนไวรัส ในการใช้อุปกรณ์แฟลชไดร์ฟต่อเข้ากับระบบคอมพิวเตอร์ควรจะสแกนไวรัสก่อนการเปิดไฟล์หรือคัดลอกไฟล์ต่าง ๆ เพื่อป้องกันไม่ให้ไวรัสหรือสิ่งไม่พึงประสงค์เข้าสู่ระบบได้ ซึ่งสอดคล้องกับ ปริญญา หอมอเนก และ ACIS Research LAB (2557) ศึกษาบทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก พบว่าหน่วยงานของรัฐและทุกองค์กร โดยเฉพาะองค์กรในกลุ่มโครงสร้างพื้นฐานสำคัญซึ่งความมั่นคงปลอดภัยของระบบควบคุมอุตสาหกรรม (ICS) สำหรับระบบโครงสร้างพื้นฐานสำคัญขององค์กร มีผลกระทบทางกายภาพโดยตรงต่อสังคมและโลก รวมทั้งความเสี่ยงที่อาจเกิดขึ้นต่อสุขภาพและความปลอดภัยของประชาชน และผลกระทบต่อสิ่งแวดล้อม ผู้บริหารหน่วยงานของรัฐและ ทุกองค์กรต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นสำคัญ ซึ่งต้องมาจากวิสัยทัศน์และภาวะผู้นำของผู้บริหารระดับสูงขององค์กร ที่ต้องเตรียมพร้อมรับมือ ด้วยการมองหาแนวทางและโอกาสในการปรับปรุง การป้องกันที่ดีย่อมทำให้พร้อมที่จะรับมือและแก้ไขได้อย่างเหมาะสมทันท่วงที แต่หากไม่มีการป้องกันที่ดี ภัยคุกคามก็อาจจะเป็นความเสี่ยงที่ยากต่อการบริหารจัดการ กระทบต่อความอยู่รอดขององค์กรในระยะยาวและยากที่ดำเนินธุรกิจแบบยั่งยืนได้ในที่สุด

ดังนั้นในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ได้แก่ 1. Identify เป็นการพัฒนาความเข้าใจของหน่วยงานศาลยุติธรรมเกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ในด้าน คน สินทรัพย์ ข้อมูล และความสามารถ เป็นการใช้กรอบอย่างมีประสิทธิภาพ ให้เข้าใจถึงการดำเนินงานของศาลยุติธรรม เพื่อให้หน่วยงานศาลยุติธรรมสามารถมุ่งเน้นและจัดลำดับความสำคัญ ให้สอดคล้องกับกลยุทธ์การบริหารความเสี่ยงและความต้องการของศาลยุติธรรม 2. Protect การพัฒนาและจัดทำการป้องกันที่เหมาะสมเพื่อให้แน่ใจว่าหน่วยงานศาลยุติธรรมได้รับการปกป้อง เพิ่มความสามารถในการจำกัดหรือยับยั้งผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ซึ่งศาลยุติธรรมมีการพัฒนาและจัดทำการป้องกันได้แก่ การระบุตัวตนและการควบคุมการเข้าถึง การสร้างความตระหนักและการฝึกอบรม การรักษาความปลอดภัยของข้อมูล กระบวนการและขั้นตอนการปกป้องสารสนเทศ การบำรุงรักษาและเทคโนโลยีด้านการป้องกัน ได้แก่ ฮาร์ดแวร์และซอฟต์แวร์ 3. Detect หน่วยงานศาลยุติธรรมมีการพัฒนาและจัดทำกิจกรรมในการระบุเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น ทำให้สามารถตรวจพบเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ได้ทันท่วงที ได้แก่ เหตุการณ์ความผิดปกติ การเฝ้าระวังอย่างต่อเนื่อง และกระบวนการตรวจจับ 4. Respond ในส่วนการพัฒนาและ

จัดทำกิจกรรมเพื่อดำเนินการเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ทำให้สามารถยับยั้งผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ได้แก่ การวางแผนรับมือ การสื่อสาร การวิเคราะห์ การบรรเทาความเสียหาย และการปรับปรุง และ 5. Recover ในการพัฒนาและจัดทำกิจกรรมเพื่อวางแผน เตรียมรับมือและกู้คืนการระบบต่าง ๆ เพื่อให้ระบบบริการที่เสียหายจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ทำให้สามารถกู้คืนการปฏิบัติงานให้กลับเป็นปกติได้ทันท่วงที เพื่อลดผลกระทบที่เกิดจากเหตุการณ์ภัยคุกคามไซเบอร์ ได้แก่ การวางแผนการกู้คืน การปรับปรุง การสื่อสาร เป็นต้น

5.2.3 ความสำเร็จและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ความสำเร็จในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มี 3 ด้าน ดังนี้

1. ด้านการรักษาความลับของหน่วยงานศาลยุติธรรม ระบบต่าง ๆ ของสำนักงานศาลยุติธรรมจะมีการกำหนดสิทธิในการเข้าถึงข้อมูลในการปฏิบัติหน้าที่ตามอำนาจหน้าที่ โดยมีฮาร์ดแวร์และซอฟต์แวร์เป็นเครื่องมือในการป้องกันความปลอดภัยจากภัยคุกคามไซเบอร์ ได้แก่ อุปกรณ์ป้องกันเครือข่าย (Firewall) อุปกรณ์ตรวจสอบการบุกรุก (Intrusion Prevention System) และซอฟต์แวร์แอนตี้ไวรัสติดตั้งกับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย

2. ด้านการรักษาความถูกต้อง ข้อมูลในระบบของฐานข้อมูลของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ภาพรวมของข้อมูลมีความถูกต้องครบถ้วนแม่นยำ เนื่องจากมีการตรวจข้อมูลก่อนส่งข้อมูลรายงานไปที่สำนักศาลยุติธรรม ประจำภาค 9 สำนักแผนงานและงบประมาณ และสำนักส่งเสริมงานตุลาการ

3. สภาพพร้อมใช้งาน ความพร้อมใช้งานของฮาร์ดแวร์ขึ้นอยู่กับระบบไฟฟ้าถ้าอุปกรณ์มีเครื่องสำรองไฟฟ้าจะทำให้อุปกรณ์ดังกล่าว ลดการเสื่อมสภาพของอุปกรณ์ มีความพร้อมใช้งาน ส่วนซอฟต์แวร์นั้นขึ้นกับลิขสิทธิ์ของซอฟต์แวร์นั้น ๆ สำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ในภาพรวมมีความพร้อมใช้งาน ซึ่งสอดคล้องกับ เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี (2565) ศึกษาความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร พบว่า บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก โดยเมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่าบุคลากรในบริษัทเอกชนแห่งนี้ที่มีเพศ อายุ และประสบการณ์การทำงานที่ต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในส่วนบุคลากรที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์

เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ

ปัญหาและอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีดังนี้

ด้านงบประมาณในการจัดซื้อทั้งฮาร์ดแวร์และซอฟต์แวร์ สำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ต้องรองบประมาณสนับสนุนในส่วนการจัดหาครุภัณฑ์ตามโครงการทางส่วนกลางให้งบประมาณมาจัดซื้อเองแต่ไม่สามารถจัดซื้อได้เนื่องด้วยราคาที่สูง ครุภัณฑ์คอมพิวเตอร์ที่มีไม่เพียงพอเนื่องจากระบบงานต่าง ๆ เพิ่มขึ้นอย่างมากและไม่มีเครื่องที่ไว้สำหรับบริการประชาชนหรือคู่ความที่มาติดต่อราชการทำให้ต้องนำเครื่องคอมพิวเตอร์ที่ถูกทดแทนแล้วมาใช้งาน ซึ่งเครื่องดังกล่าวไม่สามารถที่จะปรับปรุงระบบปฏิบัติการได้จะเกิดช่องโหว่ของระบบปฏิบัติการ และไม่สามารถจัดหาโปรแกรมแอนตี้ไวรัสหรือโปรแกรมที่จำเป็นในการใช้งานได้ ถ้าใช้โปรแกรมฟรีแวร์ หรือแชร์แวร์ก็เป็นไม่สามารถใช้ได้เต็มประสิทธิภาพหรือโปรแกรมเหล่านี้อาจมีช่องโหว่ให้ไวรัสหรือโปรแกรมที่ไม่พึ่งประสงค์โจมตี

ด้านทักษะบุคลากร การนำระบบต่าง ๆ มาใช้ในการสนับสนุนการปฏิบัติงานของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีความจำเป็นที่จะต้องอบรมหรือพัฒนาทักษะให้กับบุคลากร ปัจจุบันภัยคุกคามไซเบอร์มีหลากหลายช่องทางหลากหลายรูปแบบทำให้การอบรมหรือพัฒนาทักษะให้ผู้ดูแลระบบจึงมีความสำคัญ และต้องทบทวนให้สม่ำเสมอ

ด้านจำนวนบุคลากรทางด้านไซเบอร์ หน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีจำนวนบุคลากรทางไซเบอร์ขาดแคลนไม่สามารถรองรับการปฏิบัติงานในการแก้ไขปัญหาได้ทันท่วงที จากระบบที่จำนวนเครื่องคอมพิวเตอร์เพิ่มขึ้น ปริมาณคดี คู่ความ ที่เข้ามาติดต่อเมื่อเกิดปัญหาหลาย ๆ จุดพร้อมกัน หรือปัญหาบางทีใช้เวลาในการแก้ไข แล้วเกิดปัญหาจุดอื่นตามมา ทำให้การแก้ไขปัญหาล่าช้า ปัจจุบันศาลยุติธรรมมีแนวทางในการแต่งตั้งเจ้าหน้าที่ผู้ปฏิบัติงานศาลมาเป็นผู้ปฏิบัติงานด้านดิจิตอล เพื่อช่วยแก้ปัญหาต่าง ๆ ในศาลช่วยได้ไม่เต็มศักยภาพ เพราะด้วยผู้ที่ได้รับการแต่งตั้งเองก็มีหน้าที่ประจำอยู่ด้วยแล้วจึงไม่สามารถมาช่วยแก้ไขได้ตลอดที่มีปัญหาเกิดขึ้น และก็มีปัญหาหลาย ๆ อย่างที่จะแก้ไขได้ก็ต้องเป็นสิทธิผู้ดูแลระบบเท่านั้น การแก้ปัญหาพวกอุปกรณ์ก็ทำได้ในระดับนึงเท่านั้น แต่กรณีเป็นปัญหาที่เกิดจากภัยคุกคามไซเบอร์ก็จะไม่ทันท่วงทีในการแก้ไขปัญหา

ด้านนโยบายของหน่วยงาน เกี่ยวกับที่ตั้งศาลกรณีตั้งอยู่ใกล้น้ำทะเลจะดำเนินการความเหมาะสมของสถานที่ตั้ง หรือการออกแบบวัสดุอุปกรณ์ต่าง ๆ ในการป้องกันไม่ให้เกิดคราบเกลือ สนิม ทำส่งผลต่ออุปกรณ์เสื่อมสภาพเร็วขึ้น หรือระบบใหม่ให้เป็นระบบที่ไม่เกิดการทำงานที่ซ้ำซ้อนมีรหัสผู้ใช้และรหัสผ่านมากจากการเพิ่มขึ้นของหลาย ๆ ระบบ

5.2.4 แนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ด้านงบประมาณ

การจัดซื้อครุภัณฑ์คอมพิวเตอร์ตามโครงการต่าง ๆ ให้ส่วนกลางเป็นผู้จัดซื้อและจัดส่งครุภัณฑ์คอมพิวเตอร์มาให้ตามศาลต่าง ๆ เสนอสำนักเทคโนโลยีสารสนเทศ

สำรวจความต้องการเพิ่มเติมครุภัณฑ์คอมพิวเตอร์ที่ยังไม่เพียงพอ และตามจุดต่าง ๆ ตามความจำเป็น ความต้องการใช้โปรแกรมที่มีความจำเป็นต้องใช้งานแต่ไม่มีลิขสิทธิ์ และอุปกรณ์เครือข่ายที่หมดอายุการรับประกันเพื่อต่อประกันและบำรุงรักษาอุปกรณ์เครือข่ายอยู่เสมอ เสนอของบประมาณไปที่สำนักศาลยุติธรรมประจำภาค 9 เพื่อของบต่อที่สำนักแผนงานและงบประมาณ

ด้านทักษะบุคลากร

การนำระบบต่าง ๆ มาใช้ในการสนับสนุนการปฏิบัติงานกรณีมีความคล้ายคลึงเหมือนกันควรปรับเป็นโปรแกรมเดียวกันผู้ใช้งานระบบจะได้สะดวกในการปฏิบัติงาน

อบรมหรือพัฒนาทักษะให้กับเจ้าหน้าที่ผู้ปฏิบัติงานและเจ้าหน้าที่ผู้ดูแลระบบศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 และต้องทบทวนให้สม่ำเสมอ

ด้านจำนวนบุคลากรทางด้านไซเบอร์

ในการขออัตรากำลังบุคลากรทางด้านไซเบอร์เพิ่มเติม ตามขนาดศาลหรือปริมาณคดี หรือคอมพิวเตอร์ หรือผู้รับบริการ จัดทำข้อมูลประกอบให้กับสำนักงานศาลยุติธรรม หรือใช้บุคลากรทางด้านไซเบอร์ร่วมกันภายในจังหวัดกรณี ระบบมีปัญหาต้องรีบแก้ไข ในระหว่างการรออัตรากำลัง

ด้านนโยบายของหน่วยงาน

การตั้งอาคารที่ทำการอยู่ใกล้ทะเลควรออกแบบอาคารและวัสดุในการปกป้องอุปกรณ์ ครุภัณฑ์ต่าง ๆ ไม่ให้เกิดความเสียหาย ไม่ให้เกิดคราบเกลือ สนิม

ระบบใหม่ควรเป็นระบบที่ไม่ซ้ำซ้อนกับระบบเดิมที่มีอยู่เดิม

ควรตั้งรหัสผู้ใช้และรหัสผ่านเป็นแบบเดียวกันในทุกระบบ การยืนยันตัวตนที่อนุญาตให้ผู้ใช้ลงชื่อเข้าใช้หลายแอปพลิเคชันและเว็บไซต์

5.3 ข้อเสนอแนะ

5.3.1 ข้อเสนอแนะที่ได้จากการทำวิจัยในครั้งนี้

ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 และให้มีการนำข้อเสนอแนะแนวทาง**การ**จัดการความเสี่ยงจาก

ภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ดังนี้

1. ด้านงบประมาณ การขาดแคลนฮาร์ดแวร์อย่างครุภัณฑ์คอมพิวเตอร์ ทำให้ต้องนำเครื่องที่ถูกทดแทนแล้วมาใช้งานต่อโดยเครื่องดังกล่าวไม่สามารถปรับปรุงระบบปฏิบัติการได้ ไม่มีลิขสิทธิ์โปรแกรมแอนตี้ไวรัสการนำไปต่อกับระบบเครือข่ายภายในจะเกิดช่องโหว่ที่ทำให้มีปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ได้ ควรทำการสำรวจเพื่อของบประมาณหรือสามารถนำคอมพิวเตอร์ที่ถูกทดแทนแล้วมาใช้งานได้เพียงแต่ไม่นำเครื่องดังกล่าวเชื่อมต่อกับระบบเครือข่ายภายในและห้ามนำแฟลชไดร์ฟต่อเข้าเครื่องคอมพิวเตอร์ ส่วนการจัดหาครุภัณฑ์โครงการต่าง ๆ หน่วยงานศาลไม่สามารถจัดซื้อได้เนื่องจากงบประมาณที่จัดสรรมาให้ไม่เพียงพอ เห็นว่าควรให้ส่วนกลางเป็นผู้จัดซื้อเนื่องจากการจัดซื้อจำนวนมากจะทำให้ลดงบประมาณลงได้ และในส่วนอุปกรณ์เครือข่ายต้องต่อประกันอุปกรณ์ที่สำคัญได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ป้องกันเครือข่าย อุปกรณ์กระจายสัญญาณ จะช่วยในการปรับปรุงเฟิร์มแวร์ (Firmware) การดูแลและบำรุงรักษาอุปกรณ์ (Maintenance Service Agreement) ทำให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น

2. ด้านทักษะบุคลากร จากปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 การป้องกันจากภัยคุกคามทางไซเบอร์ที่สำคัญที่สุดคือ เจ้าหน้าที่ผู้ปฏิบัติงานควรได้รับการอบรมและพัฒนาทักษะความรู้เกี่ยวกับภัยคุกคามไซเบอร์เป็นประจำ เพื่อความตระหนักรู้ รู้ทันภัยคุกคามทางไซเบอร์ รวมถึงขั้นตอนการปฏิบัติงานเกี่ยวกับระบบงานต่าง ๆ การแก้ไขปัญหาที่สามารถทำเองได้โดยไม่ต้องรอผู้ดูแลระบบ จะช่วยป้องกันความเสียหายที่อาจลุกลามมากขึ้นได้ หรือสามารถปฏิบัติงานต่อได้โดยที่งานไม่หยุดชะงัก ควรมีการทบทวนอยู่เสมอ และในส่วนผู้ดูแลระบบควรได้รับการอบรมและพัฒนาทักษะความรู้เกี่ยวกับภัยคุกคามไซเบอร์ และการจัดการภัยคุกคามไซเบอร์ในรูปแบบต่าง ๆ มีการฝึกปฏิบัติร่วมด้วยจะช่วยให้เกิดความชำนาญ เกิดความปลอดภัยของระบบโดยรวม

3. ด้านจำนวนบุคลากรทางด้านไซเบอร์ สำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มีจำนวนผู้ดูแลระบบไม่เพียงพอ ส่งผลต่อการแก้ไขระบบได้ล่าช้า ควรขออัตรากำลังเพิ่มเติม ตามขนาดศาลหรือปริมาณคดี หรือคอมพิวเตอร์ หรือผู้รับบริการ โดยจัดทำข้อมูลประกอบให้กับสำนักงานศาลยุติธรรม หรือการใช้บุคลากรทางด้านไซเบอร์ร่วมกันภายในจังหวัดและอาจขอเจ้าหน้าที่ผู้ดูแลระบบของสำนักศาลยุติธรรมประจำภาค 9 ไปช่วยดูแลระบบซึ่งเกิดปัญหาต้องรีบแก้ไข หรืออาจแต่งตั้งเจ้าหน้าที่ผู้ปฏิบัติงานด้านดิจิตอลเพิ่มเติม เช่น อาจแต่งตั้งเจ้าหน้าที่ผู้ปฏิบัติงานด้านดิจิตอลแต่ละห้องแต่ละฝ่าย และฝึกทักษะและมอบสิทธิการแก้ไขปัญหาที่สามารถเข้าถึงได้ของระบบต่าง ๆ ในระดับที่เหมาะสมเพื่อแก้ปัญหาให้กับหน่วยงานได้รวดเร็วและมีความปลอดภัยมากขึ้น

5.3.2 ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

1. ควรมีเก็บข้อมูลจากผู้ดูแลระบบ สำนักเทคโนโลยีสารสนเทศ สำนักงานศาลยุติธรรม

2. ควรมีการเก็บข้อมูลด้วยวิธีการสังเกตเพิ่มเติมเพื่อที่จะได้ทราบพฤติกรรมการปฏิบัติงานจริง

3. ควรมีการเก็บข้อมูลในพื้นที่จัดตั้งอาคารศาลที่อยู่ต่างภูมิประเทศ เพื่อได้ปัจจัยเสียงจากภัยคุกคามเพิ่มเติม

5.3.3 ปัญหาและอุปสรรคในการทำวิจัย

1. เจ้าหน้าที่ผู้ดูแลระบบและเจ้าหน้าที่ผู้ปฏิบัติงานศาลบางท่านมีความวิตกกังวลในการให้ข้อมูลเชิงลึก การเปิดเผยข้อมูลส่วนบุคคล และการบันทึกเทปการให้สัมภาษณ์

2. เจ้าหน้าที่ผู้ดูแลระบบและเจ้าหน้าที่ผู้ปฏิบัติงานศาลบางท่านไม่สะดวกในการให้สัมภาษณ์

บรรณานุกรม

กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ. (2564). การบริหารความเสี่ยงอย่างมืออาชีพ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://www.journalgrad.ssru.ac.th/index.php/8thconference/article/view/2523.

กริน ธัญญวิกร และธีระ กุลสวัสดิ์. (2564). การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so04.tci-thaijo.org/index.php/JSBA/article/view/247389/169638.

เกียรติศักดิ์ ลุยทอง. (2561) การพัฒนาระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://dspace.spu.ac.th/bitstream/123456789/5747/2/OK_%e0%b8%a3%e0%b8%a7%e0%b8%a1%e0%b9%80%e0%b8%a5%e0%b9%88%e0%b8%a1%e0%b8%aa%e0%b8%a1%e0%b8%9a%e0%b8%b9%e0%b8%a3%e0%b8%93%e0%b9%8c.pdf.

เขมิกา ทองเรือง และพัณณกร สอนไว. (2565). การบริการสาธารณะของกำนันและผู้ใหญ่บ้านด้านการป้องกันยาเสพติดในชุมชน. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so04.tci-thaijo.org/index.php/jsa-journal/article/view/258692/176313

คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย. (2563). ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่องหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ. 2563. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://www.tgia.org/upload/file_group/16/download_1883.pdf.

ชฎาภรณ์ สิงห์แก้ว. (2564). บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so06.tci-thaijo.org/index.php/umt-poly/article/view/249037/168688.

ญาณิศา เผื่อนเพาะ. (2562). การจัดการความเสี่ยงในธุรกิจขนาดกลางและขนาดย่อม. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://msjournals.aru.ac.th/index.php/msjournals/article/view/90/21.

ชวนพิศ เงินฉลาด. (2562). แรงจูงใจในการบริการสาธารณะ กรณีศึกษาศูนย์อุตุนิยมวิทยาภาคใต้. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://kb.psu.ac.th/psukb/bitstream/2016/12329/2/%e0%b8%8a%e0%b8%a7%e0%b8%99%e0%b8%9e%e0%b8%b4%e0%b8%a8%20%e0%b9%80%e0%b8%87%e0%b8%b4%e0%b8%99%e0%b8%89%e0%b8%a5%e0%b8%b2%e0%b8%94.pdf.

ณรงค์เวตย์ เรืองจวง. (2561). แนวทางการพัฒนาขีดความสามารถบุคลากร ด้านไซเบอร์ของกองทัพอากาศ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/ratthapirak/article/view/189480/132695.

ธนภัทร กิตติวณิชพันธุ์ และอานนท์ ทับเที่ยง. (2561). สมรรถนะของบุคลากรในหน่วยงานราชการด้านความมั่นคงปลอดภัยไซเบอร์ตามข้อกำหนด NIST และมาตรฐาน ISO27001/2013. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://ph02.tci-thaijo.org/index.php/ET/article/view/243980/165443.

ธีระศักดิ์ เปี่ยมสุภัคพงศ์, ธีระรัตน์ เปี่ยมสุภัคพงศ์, พรพรรณ สุวรรณประทีป, สุกานดา โรจนประภายนต์ และวัฒนา เสรีคุณากุล. (2561-2562). การเรียนรู้เพื่อรับมือกับการบริหารความเสี่ยงของธุรกิจในบริบทใหม่ ยุคอุตสาหกรรม 4.0. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so03.tci-thaijo.org/index.php/trujournal/article/view/193524/148978.

นริส อุไรพันธ์ และธรนี มณีศรี. (2563). โมเดลสมการเชิงโครงสร้าง เพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://dspace.spu.ac.th/bitstream/123456789/6701/1/%e0%b8%9a%e0%b8%97%e0%b8%84%e0%b8%a7%e0%b8%b2%e0%b8%a1%e0%b8%a7%e0%b8%b4 %e0%b8%88%e0%b8%b1%e0%b8%a2%201.pdf.

นุกูล แดงภูมี. (2564). การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management : ERM) เครื่องมือบริหารเชิงรุกปัจจัยความสำเร็จขององค์กร. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so02.tci-thaijo.org/index.php/DRURDI/article/view/251526/169421.

เนตรชนก สูนาสวน, อำนวย บุญรัตนไมตรี, ชัยยงค์ พรหมวงค์ และอนันต์ เตียวต๋อย (2565). การบริการสาธารณะและการมีส่วนร่วมเพื่อการพัฒนาอย่างยั่งยืนของผู้ประกอบการ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so03.tci-thaijo.org/index.php/jeir/article/view/257777/173806.

ปรัชญา เฉลิมวัฒน์. (2560). แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2560-2561/PDF/8451sc/%E0%B8%A3%E0%B8%A7%E0%B8%A1.pdf.

ปริญญา หอมอเนก และACIS Research LAB. (2557). บทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so04.tci-thaijo.org/index.php/ndsijournal/article/view/38171/31657

พลากร ลาภอลงกรณ์. (2564). การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://ict.dmh.go.th/events/events/files/CyberSecurity-Awareness.pdf

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (24 พฤษภาคม 2562). ราชกิจจานุเ*บกษา.* เล่ม 136 ตอนที่ 69 ก หน้า 20-51. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF.

พิชญาพร พีรพันธุ์ และวิโรจน์ เจษฎาลักษณ์. (2564). กรอบแนวคิดปัจจัยเชิงสาเหตุและผลลัพธ์ของความสามารถในการจัดการความเสี่ยงขององค์กร. สืบค้นเมื่อ 1 มิถุนายน 2565,จาก https://so03.tci-thaijo.org/index.php/trujournal/article/view/249409/170470.

พร้อมศักดิ์ จิตจำ. (2560). การปรับตัวต่อการเปลี่ยนแปลงสภาพภูมิอากาศ: ศึกษาการเตรียมความพร้อมรับมืออุทกภัยขององค์กรปกครองส่วนท้องถิ่นในพื้นที่ลุ่มน้ำคลองอู่ตะเภา. มหาวิทยาลัยสงขลานครินทร์

ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ. (2559). ภัยคุกคามทางไซเบอร์ (Cyber Security). สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://dtd.dti.or.th/jspui/bitstream/123456789/1880/1/%e0%b8%a0%e0%b8%b1%e0%b8%a2%e0%b8%84%e0%b8%b8%e0%b8%81%e0%b8%84%e0%b8%b2%e0%b8%a1%e0%b8%97%e0%b8%b2%e0%b8%87%e0%b9%84%e0%b8%8b%e0%b9%80%e0%b8%9a%e0%b8%ad%e0%b8%a3%e0%b9%8c%20%28Cyber%20Security%29.pdf.

ภาณุพล บรรณกิจโสภณ. (2560). แนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศของกองทัพไทย. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/ratthapirak/article/view/189415/132674.

เมธาพร ธรรมศิริ และศิรภัสสศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/TRDMJOPOlSU/article/view/259170/174347.

ยุทธศักดิ์ รักเสรีพิทักษ์ และศิริลักษม์ ตันตยกุล. (2565). บทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามรูปแบบใหม่. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://202.41.160.104/index.php/MPA/article/view/316/258.

วิลาส วิถีไพร. (2561). การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://www.dspace.spu.ac.th/bitstream/123456789/5769/1/IS_All_Wilas_Sep%2017%2c%202018.pdf.

วิจิตรา สีแดงก่ำ. (2562). การบริหารความเสี่ยงขององค์กรในศตวรรษที่ 21. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://journalgrad.ssru.ac.th/index.php/miniconference/article/view/2050.

วิศณุ สร้างวงศ์ใหม่. (2561). การเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/ratthapirak/article/view/188754/132306.

ศิริพงษ์ ปานจันทร์. (2554). ประสิทธิผลในการบริหารงานของเทศบาลในจังหวัดนครปฐม. วิทยานิพนธ์ ดุษฎีบัณฑิต (สาขารัฐประศาสนศาสตร์). วิทยาลัยบัณฑิตศึกษาด้านการจัดการ. มหาวิทยาลัยศรีปทุม.

สถาพร วิชัยรัมย์, ธัญญรัตน์ พุฑฒิพงษ์ชัยชาญ, ภัทรนันท์ เกิดในหล้า และจุฑารัตน์ จัตุกูล (2562). จริยธรรมในการให้บริการสาธารณะของไทย. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so02.tci-thaijo.org/index.php/bruj/article/view/220195/160749.

สุฎิกา รักประสูติ. (2558). บทบาทของผู้ตรวจสอบภายในต่อการจัดการความเสี่ยงองค์กร: ปัจจัยสาเหตุและผลลัพธ์. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/DPUSuthiparithatJournal/article/view/244357/166034.

สุฎิกา รักประสูติ และนงนิภา ตุลยานนท์. (2563). การจัดการความเสี่ยงของการพัฒนาผลิตภัณฑ์ใหม่ : ความสำเร็จของธุรกิจเกิดใหม่ในยุคเศรษฐกิจดิจิทัล. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so02.tci-thaijo.org/index.php/isshmu/article/view/243837/165429.

สุภาพร พรมโส, ปราลี มณีรัตน์ และประสงค์ ปราณีตพลกรัง. (2564). สถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://ph02.tci-thaijo.org/index.php/nkrafa-sct/article/view/244698/166774.

สุวันต์นา เสมอเนตร. (2561). การพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC). สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://thaidj.org/index.php/JHS/article/view/5914/5747.

สนธิญา สุวรรณราช, จตุรภัทร วงศ์ศิริสถาพร, ฐิฎิกานต์ สุริยะสาร, สรัชนุช บุญวุฒิ, ทิพยาภรณ์ ปัตถา, สุพรรณี คาวาส และแดน กุลรูป. (2563). ความสัมพันธ์ระหว่างการบริหารความเสี่ยงองค์กรกับการวัดผลองค์กรแบบสมดุลของบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so03.tci-thaijo.org/index.php/JMMS/article/view/242377/167976.

สำนักเทคโนโลยีสารสนเทศ. (2559). รายงานการตรวจจับและป้องกันการบุกรุกเครื่องคอมพิวเตอร์แม่ข่ายเว็บไซต์หน่วยงานศาลยุติธรรม

สำนักแผนและงบประมาณศาลยุติธรรม. (มปป). การส่งเสริมความรู้ความเข้าใจเกี่ยวกับศาลยุติธรรม. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://oppb.coj.go.th/th/file/get/file/20190131e9c725c5a1fa8010d2985f6484416299104532.pdf

สำนักแผนและงบประมาณศาลยุติธรรม. (2565). แผนบริหารจัดการความเสี่ยงสำนักงานศาลยุติธรรม ประจำปีงบประมาณ พ.ศ.2565. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://oppb.coj.go.th/th/content/page/index/id/270986

อนาวิล แก้วสะอาด และณัฐวี อุตกฤษฎ์. (2564). แนวทางบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so04.tci-thaijo.org/index.php/ndsijournal/article/view/245941/170493.

อรรคเดช ประทีปอุษานนท์ และธาราทิพย์ กัลยาณมิตร. (2560). แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ วารสารสถาบันวิชาการป้องกันประเทศ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so04.tci-thaijo.org/index.php/ndsijournal/article/view/107618/85175.

เอกชัย ประเสริฐวงษ์. (2561). การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของวิสาหกิจขนาดกลาง และขนาดย่อมในอำเภอหนองแค จังหวัดสระบุรี. สืบค้นเมื่อ 1 มิถุนายน 2565,จาก https://rsuirlibrary.rsu.ac.th/bitstream/123456789/894/1/Akachai%20Prasertwong.pdf

ภาคผนวก

ภาคผนวก ก แบบสัมภาษณ์

ชุดที่ ....

แบบสัมภาษณ์เพื่อการวิจัยสำหรับ

(เจ้าหน้าที่ผู้ดูแลระบบ หน่วยงานศาลในสังกัดอำนาจอธิบดีผู้พิพากษา 9)

เรื่องการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

<u>คำชี้แจง</u>

แบบสัมภาษณ์เพื่อการวิจัยนี้มีจุดมุ่งหมาย เพื่อศึกษาแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ทั้งนี้ผู้วิจัย ความอนุเคราะห์ท่านตอบคำถามทุกข้อตามความเป็นจริงด้วยตัวท่านเอง โดยข้อมูลเหล่านี้จะใช้เพื่อประโยชน์ทางการศึกษาเท่านั้น และจะไม่มีการเปิดเผยข้อมูลส่วนบุคคลของท่านแต่อย่างใด หากมีข้อสงสัยในงานวิจัยในครั้งนี้ประการใด ท่านสามารถติดต่อผู้วิจัย นายธนพงศ์ ฉันทวิเชียร อีเมล tanapong.tc@gmail.com ผู้วิจัยขอขอบพระคุณท่านเป็นอย่างสูง ในการให้ความอนุเคราะห์ตอบแบบสอบถามในครั้งนี้

ขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้

นายธนพงศ์ ฉันทวิเชียร
นักศึกษาหลักสูตร รัฐประศาสนศาสตรมหาบัณฑิต
มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

<u>ตอนที่ 1</u> ข้อมูลทั่วไป

ผู้ให้ข้อมูล.....ตำแหน่ง.....

สังกัด.....เบอร์โทรศัพท์.....

<u>ตอนที่ 2</u> ข้อคำถามที่ใช้สัมภาษณ์เจ้าหน้าที่ผู้ดูแลระบบ

1. ศาลของท่านมีปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์อย่างไรบ้าง
2. ศาลของท่านมีขั้นตอนหรือเครื่องมือในการจัดการภัยคุกคามไซเบอร์อย่างไรบ้าง
3. ศาลของท่านมีแนวทางหรือมาตรการจัดการภัยคุกคามไซเบอร์อย่างไรบ้าง
4. ศาลของท่านมีความสำเร็จหรือไม่เพียงใด ในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ การรักษาความลับ การรักษาความครบถ้วน สภาพพร้อมใช้งาน
5. ศาลของท่านมีปัญหาอุปสรรคในการดำเนินงานเพื่อจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ ด้านงบประมาณ ด้านทักษะบุคลากรและจำนวนบุคลากรทางด้านไซเบอร์ ด้านนโยบายของหน่วยงาน และด้านระเบียบหรือกฎหมายที่เกี่ยวข้อง อย่างไรบ้าง

<u>ตอนที่ 3</u> ข้อคิดเห็นและเสนอแนะอื่น ๆ

.....

.....

.....

.....

.....

.....

ชุดที่ ....

แบบสัมภาษณ์เพื่อการวิจัยสำหรับ
(ผู้ปฏิบัติงานศาลในเขตอำนาจอธิบดีผู้พิพากษาภาค 9)
เรื่องการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

<u>คำชี้แจง</u>

แบบสัมภาษณ์เพื่อการวิจัยนี้มีจุดมุ่งหมาย เพื่อศึกษาแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ทั้งนี้ผู้วิจัย ความอนุเคราะห์ท่านตอบคำถามทุกข้อตามความเป็นจริงด้วยตัวท่านเอง โดยข้อมูลเหล่านี้จะใช้เพื่อประโยชน์ทางการศึกษาเท่านั้น และจะไม่มีการเปิดเผยข้อมูลส่วนบุคคลของท่านแต่อย่างใด หากมีข้อสงสัยในงานวิจัยในครั้งนี้ประการใด ท่านสามารถติดต่อผู้วิจัย นายธนพงศ์ ฉันทวิเชียร อีเมล tanapong.tc@gmail.com ผู้วิจัยขอขอบพระคุณท่านเป็นอย่างสูง ในการให้ความอนุเคราะห์ตอบแบบสอบถามในครั้งนี้

ขอขอบคุณในความอนุเคราะห์ของท่านมา ณ โอกาสนี้

นายธนพงศ์ ฉันทวิเชียร
นักศึกษาหลักสูตร รัฐประศาสนศาสตรมหาบัณฑิต
มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

<u>ตอนที่ 1</u> ข้อมูลทั่วไป

ผู้ให้ข้อมูล.....ตำแหน่ง.....

สังกัด.....เบอร์โทรศัพท์.....

<u>ตอนที่ 2</u> ข้อคำถามที่ใช้สัมภาษณ์เจ้าหน้าที่ผู้ปฏิบัติงานศาล

1. ศาลของท่านมีปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์อย่างไรบ้าง
2. ศาลของท่านมีแนวทางหรือมาตรการจัดการภัยคุกคามไซเบอร์อย่างไรบ้าง
3. ศาลของท่านมีความสำเร็จหรือไม่เพียงใด ในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ การรักษาความลับ การรักษาความครบถ้วน สภาพพร้อมใช้งาน
4. ศาลของท่านมีปัญหาอุปสรรคในการดำเนินงานเพื่อจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ ด้านงบประมาณ ด้านทักษะบุคลากรและจำนวนบุคลากรทางด้านไซเบอร์ ด้านนโยบายของหน่วยงาน และด้านระเบียบหรือกฎหมายที่เกี่ยวข้อง อย่างไรบ้าง

<u>ตอนที่ 3</u> ข้อคิดเห็นและเสนอแนะอื่น ๆ

.....

.....

.....

.....

.....

.....

ภาคผนวก ข หนังสือขอความอนุเคราะห์ในการเข้าสัมภาษณ์

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักอำนวยการประจำศาลจังหวัดตรัง

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักอำนวยการประจำศาลจังหวัดนราธิวาส

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลจังหวัดนาทวี

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลจังหวัดเบตง

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักอำนวยการประจำศาลจังหวัดปัตตานี

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักอำนวยการประจำศาลจังหวัดพัทลุง

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักอำนวยการประจำศาลจังหวัดยะลา

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลแขวงตรัง

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลแขวงสงขลา

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลเยาวชนและครอบครัวจังหวัดตรัง

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลเยาวชนและครอบครัวจังหวัดนราธิวาส

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลเยาวชนและครอบครัวจังหวัดปัตตานี

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลเยาวชนและครอบครัวจังหวัดพัทลุง

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลเยาวชนและครอบครัวจังหวัดยะลา

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลเยาวชนและครอบครัวจังหวัดสงขลา

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักงานประจำศาลเยาวชนและครอบครัวจังหวัดสตูล

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักอำนวยการประจำศาลจังหวัดสงขลา

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ที่ ๖๘๑๐๖/๖๕๖๕

คณะวิทยาการจัดการ
มหาวิทยาลัยสงขลานครินทร์
๑๕ ถนนกาญจนวนิชย์
ตำบลคอหงส์ อำเภอหาดใหญ่
จังหวัดสงขลา ๙๐๑๑๐

๑๙ ธันวาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์ในการขอเข้าสัมภาษณ์

เรียน ผู้อำนวยการสำนักอำนวยการประจำศาลจังหวัดสตูล

ด้วยนักศึกษาหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์ นายธนพงศ์ ฉันทวิเชียร รหัสนักศึกษา ๖๔๑๐๕๒๑๕๑๗ กำลังศึกษารายวิชาวิทยานิพนธ์ในหัวข้อ “การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ: บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙” โดยมี รองศาสตราจารย์ ดร.สมพร คุณวิชิต เป็นอาจารย์ที่ปรึกษาสารนิพนธ์ มีความประสงค์ขอเข้าสัมภาษณ์เพื่อศึกษาปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙

ในการนี้ หลักสูตรฯ จึงขอความอนุเคราะห์ท่านในการให้นักศึกษา นายธนพงศ์ ฉันทวิเชียร เข้าสัมภาษณ์นักวิชาการคอมพิวเตอร์หรือพนักงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ปฏิบัติงาน เพื่อนำข้อมูลที่ได้รับมาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง แนวปฏิบัติ ความสำเร็จ อุปสรรค ในการดำเนินงานการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค ๙ ทั้งนี้ผลจากการสัมภาษณ์จะนำไปประมวลผลวิเคราะห์ในภาพรวม และใช้ในแง่ของการศึกษาเท่านั้น ซึ่งจะเป็นประโยชน์ทางวิชาการต่อไป โดยจะไม่มีผลกระทบใดๆ ต่อผู้ให้การสัมภาษณ์ที่ให้ความร่วมมือในการเข้าสัมภาษณ์ หากท่านต้องการข้อมูลเพิ่มเติมประการใดสามารถติดต่อประสานงานได้โดยตรงกับ นายธนพงศ์ ฉันทวิเชียร หมายเลขโทรศัพท์ ๐๘๑-๙๙๗๙๘๐๖ หรืออีเมล์ tanapong.tc@gmail.com

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย และขอขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอแสดงความนับถือ

(ดร.สิริวิท อิสโร)
รองคณบดีฝ่ายยุทธศาสตร์และบัณฑิตศึกษา

งานบัณฑิตศึกษาวิทยาการจัดการ คณะวิทยาการจัดการ
โทร ๐ ๗๔๒๘ ๗๘๕๘-๙

ประวัติผู้เขียน

ชื่อ-สกุล นายธนพงศ์ ฉันทวิเชียร

รหัสนักศึกษา 6410521517

วุฒิการศึกษา

วุฒิ	**ชื่อสถาบัน**	**ปีที่สำเร็จการศึกษา**
วิทยาศาสตรบัณฑิต	มหาวิทยาลัยราชภัฏนครราชสีมา	2552

ตำแหน่งและสถานที่ทำงาน

ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

สถานที่ทำงาน สำนักศาลยุติธรรมประจำภาค 9 อาคารสำนักงานอธิบดีผู้พิพากษาภาค 9