NCSA
สกมช
สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

รายงานประจำปี 2564

คำนำ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. ได้จัดทำรายงานผลการดำเนินงานประจำปี 2564 ซึ่งเป็นไปตามมาตรา 39 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่ได้บัญญัติให้ สกมช. จัดทำรายงานผลการดำเนินงานประจำปีเสนอคณะกรรมการและรัฐมนตรีภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน

เพื่อให้เป็นไปตามที่กฎหมายกำหนด สกมช. ได้จัดทำรายงานผลการดำเนินงานประจำปี 2564 โดยมีสาระสำคัญประกอบด้วย ข้อมูลทั่วไป สรุปสถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทยปี 2564 ผลการดำเนินงานและการบริหารงบประมาณ ประจำปี 2564 รวมทั้งผลการประเมินการดำเนินงานของสำนักงานตลอดปี 2564 ดังรายละเอียดที่ปรากฏอยู่ในรายงานฉบับนี้ ซึ่งนอกจากมีวัตถุประสงค์เพื่อเสนอต่อคณะกรรมการและรัฐมนตรีที่เกี่ยวข้องแล้ว ยังได้เผยแพร่ให้ประชาชน บริษัท ห้างร้าน หน่วยงานภาคเอกชนและส่วนราชการ รวมทั้งสาธารณชนทั่วไปได้รับทราบผลการดำเนินงานในปีที่ผ่านมาของ สกมช. ตามที่กฎหมายกำหนดด้วย หวังเป็นอย่างยิ่งว่าจะเป็นแหล่งรวบรวมข้อมูลที่สำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในโลกยุคดิจิทัล ให้แก่ผู้สนใจ เช่น นักวิชาการ นักศึกษา สื่อมวลชน และประชาชนทั่วไปได้นำไปใช้ประโยชน์ตามที่เห็นสมควรต่อไป

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
มีนาคม 2565

สารบัญ

สารนายกรัฐมนตรี

การพัฒนาอย่างก้าวกระโดดของเทคโนโลยีและการเปลี่ยนแปลงของวิถีชีวิตในสังคมยุคใหม่ ส่งผลให้ความเสี่ยงต่อภัยคุกคามทางไซเบอร์มีปริมาณมากและทวีความรุนแรงยิ่งขึ้นตามไปด้วย รัฐบาลเห็นถึงความสำคัญของการพัฒนาเทคโนโลยีและการสร้างระบบรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ จึงได้มีนโยบายและมาตรการต่าง ๆ ตามมาตรฐานสากล เพื่อรองรับเทคโนโลยีและวิถีชีวิตที่เปลี่ยนแปลงไป รวมทั้งได้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้น เพื่อทำหน้าที่เป็นศูนย์กลางในการรวบรวม วิเคราะห์ข้อมูล และเผยแพร่ข้อมูลที่เกี่ยวข้อง พร้อมทั้งประสานความร่วมมือด้านการรักษาความมั่นคงทางไซเบอร์ กับหน่วยงานของรัฐและเอกชนทั้งในและต่างประเทศ ผมหวังว่าผู้บริหารและเจ้าหน้าที่ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทุกท่านจะปฏิบัติหน้าที่ด้วยความมุ่งมั่นตั้งใจ และพัฒนาความรู้ความสามารถของตนให้เท่าทันเทคโนโลยีอย่างสม่ำเสมอ เพื่อสร้างความมั่นคงเข้มแข็งให้แก่ประเทศต่อไป

ในโอกาสนี้ ผมขออาราธนาคุณพระศรีรัตนตรัยและสิ่งศักดิ์สิทธิ์ทั้งหลาย อีกทั้งพระบารมีของพระบาทสมเด็จพระเจ้าอยู่หัว และสมเด็จพระนางเจ้าฯ พระบรมราชินี โปรดดลบันดาลประทานพรให้ผู้บริหาร และเจ้าหน้าที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติพร้อมทั้งครอบครัว จงประสบแต่ความสุขความเจริญ มีสุขภาพกาย และสุขภาพใจที่สมบูรณ์แข็งแรงโดยทั่วกัน

พลเอก

(ประยุทธ์ จันทร์โอชา)
นายกรัฐมนตรี

สารรองนายกรัฐมนตรี

ประธานกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ปัจจุบันสังคมโลกเผชิญกับภัยคุกคามรูปแบบต่าง ๆ ที่ก่อให้เกิดความเสียหายต่อชีวิต ทรัพย์สินของประชาชน และความมั่นคงของประเทศ อีกทั้งเทคโนโลยีเข้ามามีบทบาทในวิถีชีวิตของมนุษย์มากขึ้น ทำให้เกิดภัยคุกคามทางไซเบอร์หรือการโจมตีทางคอมพิวเตอร์ที่ส่งผลต่อการดำเนินชีวิตของประชาชนและความมั่นคงของประเทศ รัฐบาลมีนโยบายในการรักษาความมั่นคงปลอดภัยของประเทศ โดยเฉพาะการเพิ่มขีดความสามารถในการบริหารจัดการภัยคุกคามทางไซเบอร์ โดยบูรณาการความร่วมมือจากทุกภาคส่วน ทั้งในประเทศและต่างประเทศ เพื่อให้เป็นเครือข่ายในการป้องกันการคุกคามทางไซเบอร์และรักษาความมั่นคงปลอดภัยทางไซเบอร์ ผมขอชื่นชมสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีบทบาทสำคัญในการยกระดับการรักษาความมั่นคงปลอดภัยของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ให้มีประสิทธิภาพ รวมทั้งผลักดันให้ทุกหน่วยงานมีมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อทำให้ประเทศมีภูมิคุ้มกันที่เข้มแข็ง และมีความพร้อมรับมือกับความเสี่ยงที่จะส่งผลกระทบต่อความมั่นคงทางไซเบอร์ของชาติ

ในนามคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ผมหวังเป็นอย่างยิ่งว่า การจัดทำรายงานผลการดำเนินงานประจำปี 2564 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเป็นรายงานฉบับแรกที่ได้ดำเนินงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จะเป็นประโยชน์ต่อทุกภาคส่วนที่เกี่ยวข้องที่จะนำไปประกอบการพิจารณากำหนด วางแผน นโยบาย มาตรการ แนวทางในการป้องกัน เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งทำให้หน่วยงานภาครัฐ ภาคเอกชน และภาคประชาชนมีความรู้ ความเข้าใจ และมีความพร้อมในการบริหารจัดการกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพและประสิทธิผลต่อไป

พลเอก
(ประวิตร วงษ์สุวรรณ)
รองนายกรัฐมนตรี

สารรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และประธานกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ในปัจจุบันประเทศไทยมีแนวโน้มการโจมตีทางไซเบอร์ที่เพิ่มขึ้นเรื่อย ๆ ทั้งเชิงปริมาณและความรุนแรง และด้วยสถานการณ์การแพร่ระบาดของโรค Covid-19 ทำให้องค์กรต่าง ๆ ทั้งภาครัฐและเอกชน มีการปรับเปลี่ยนรูปแบบการทำงานผ่านระบบออนไลน์แอพพลิเคชันมากขึ้น จึงทำให้อาชญากรไซเบอร์ ใช้ช่องโหว่ของระบบเข้าถึงข้อมูลสำคัญขององค์กรได้ จะเห็นได้ว่าภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์มีรูปแบบการโจมตีที่รุนแรงมากขึ้น และมีแนวโน้มที่พัฒนาตามการเปลี่ยนแปลงของเทคโนโลยี ซึ่งภัยคุกคามดังกล่าวอาจส่งผลต่อความมั่นคงของรัฐ ความสงบเรียบร้อยของสังคมและเศรษฐกิจของประเทศได้ รัฐบาลตระหนักดีว่าต้องเตรียมพร้อมรับมือกับภัยคุกคาม ดังนั้น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงถูกบัญญัติขึ้น เพื่อรับมือ ป้องกัน และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบต่อหน่วยงานต่าง ๆ โดยเฉพาะกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศอันจะส่งผลกระทบต่อการให้บริการประชาชนในวงกว้างได้

(นายชัยวุฒิ ธนาคมานุสรณ์)
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สารเลขาธิการ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พันธกิจหลักของ สกมช. คือ เป็นหน่วยงานกลางผู้สร้างกลไกขับเคลื่อนการทำงานด้านการดูแลและรับมือภัยคุกคามไซเบอร์ รวมทั้งให้ความช่วยเหลือสนับสนุนหน่วยงานภาครัฐ และหน่วยงานที่เป็นพื้นฐานสำคัญทางสารสนเทศเพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามที่อาจเกิดขึ้น การดำเนินงานดังกล่าวต้องอาศัยผู้เชี่ยวชาญเฉพาะด้าน และมีกลไกการทำงานที่มีความคล่องตัวพร้อมสำหรับการปฏิบัติงาน ทั้งด้านนโยบาย เทคโนโลยี การวิจัยพัฒนาและกฎหมาย สำหรับปี 2564-2565 สกมช. มีโครงการต่าง ๆ ที่มีการดำเนินการอย่างต่อเนื่อง อาทิ

• **การจัดทำแผนและนโยบายระดับประเทศและจัดทำเฟรมเวิร์กต่าง ๆ** เพื่อดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ทั้ง 7 ภาคส่วน ได้แก่ ด้านความมั่นคงภาครัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงิน-การธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค และด้านสาธารณสุข

• **เร่งรัดพัฒนาบุคลากรด้านไซเบอร์** โดยมีเป้าหมายกว่า 2,000 คน สำหรับปี 2564 ถึงปี 2565 ได้พัฒนาระดับผู้บริหาร 70 คน ระดับผู้เชี่ยวชาญ 300 คน จัดโปรแกรมสัมมนาเพื่อพัฒนาบุคลากรอย่างต่อเนื่อง มีโครงการพัฒนาความรู้ในบุคคลทั่วไป ตลอดจนนักเรียน นักศึกษา มีโครงการจัดแข่งขันทักษะทางไซเบอร์ในระดับมัธยม มหาวิทยาลัย ตลอดจนบุคคลทั่วไป ซึ่งได้รับความสนใจเป็นอันมาก เนื่องจากเป็นเส้นทางสายอาชีพกระแสใหม่ มีรายได้ดี เป็นที่ต้องการสูง จึงเกิดการผลักดันให้เกิดความต้องการศึกษาด้านไซเบอร์ซิเคียวริตี้ที่ประเทศยังขาดแคลน

• **การสร้างความตระหนักให้องค์กรที่เป็น CII ทั้ง 7 ภาคส่วน** ตามแนวทางปฏิบัติของ พ.ร.บ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ซึ่งเป็นแผนพัฒนาและปฏิบัติระยะยาวภายใต้การดูแลเชิงปฏิบัติการของ สกมช. เพื่อให้เกิดผลสัมฤทธิ์ในการป้องกันตัวเองตลอดจนแก้ไขภัยทางไซเบอร์รูปแบบต่าง ๆ

• **การแสวงหาความร่วมมือกับองค์กรทั้งในประเทศและต่างประเทศ ตลอดจนกระทรวงต่าง ๆ** ซึ่งขณะนี้มีการร่าง MOU กับประเทศอิสราเอล จีน อังกฤษ และอีกหลายประเทศ

สำหรับประเทศไทย พ.ร.บ.ไซเบอร์ ได้แบ่งภัยคุกคามไซเบอร์เป็น 3 ระดับคือ **ระดับไม่ร้ายแรง** ส่งผลให้เกิดความด้อยประสิทธิภาพในการให้บริการอิเล็กทรอนิกส์ **ภัยไซเบอร์ระดับร้ายแรง** มีการโจมตีระบบจนเกิดความเสียหายไม่สามารถทำงานต่อได้ และ**ระดับวิกฤต** ระบบล้มเหลวจนรัฐทำงานจากส่วนกลางไม่ได้ ส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศทั้งระบบ ซึ่ง พ.ร.บ.ไซเบอร์ ให้อำนาจ สกมช. ในการเข้าตรวจสอบหรือจัดการแก้ปัญหาการโจมตีไซเบอร์เฉพาะที่มีการ**ถูกโจมตีระดับร้ายแรง**และ**ระดับวิกฤต** ตั้งแต่ต้นปี 2564 ถึงปัจจุบัน สกมช. ได้เข้าร่วมแก้ปัญหาในหน่วยงานหรือองค์กรต่าง ๆ จนผ่านพ้นวิกฤตหลายหน่วยงาน

พลเอก
(ดร.ปรัชญา เฉลิมวัฒน์)
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Agency constructs 40 new rules to bolster law

The National Cyber Security Agency (NCSA) aims to roll out 40 subordinate regulations of the Cybersecurity Act to strengthen the country's infrastructures this year.

To guard against cyberthreats, roughly 100 organisations linked with Critical Information Infrastructure (CII) stipulated by the act must be complied the standard framework of security requirements this year, said the agency.

The act stipulates that NCSA is responsible for providing assistance to prevent and mitigate risks from cyberthreats to 7 sectors of CII: national security, public service, banking and finance, information technology and telecoms, transportation and logistics, energy and public utilities, as well as public health.

NCSA established in January 2021, will develop cybersecurity skills for organisations of CII to meet international standards through intensive capacity-building programmes targeting 2,250 attendees, including 400 specialists and executives in 2022. This move will enhance the country's capacity to defend against escalating cyberthreats.

Additionally, regarding to Section 44 of the Cybersecurity Act, the agency will formulate a code of practice and standard framework of cybersecurity as a guideline for organisations of CII.

NCSA will enforce security standard including software and operating systems for state and private agencies linked CII by the end of this year. The requirements include daily monitoring of threats to ensure the security of their databases.

NCSA plans to work with regulators in various sectors on this tasks, such as the Thailand Banking Sector Computer Emergency Response Team, the Securities and Exchange Commission, the National Broadcasting and Telecommunications Commission and the Telecommunications Association of Thailand.

In August 2021, NCSA established a national computer emergency response team (National CERT), which was transformed from ThaiCert (Thailand Computer Emergency Response Team) under the Electronic Transactions Development Agency.

The agency received a budget of 40 million baht in its first year of operation, which was raised to 140 million in fiscal 2022. Also, it secured another 200 million baht from the Digital Economy and Society Ministry's Digital Fund for its operations and management in fiscal 2022.

NCSA aims to have 480 staff for its full-scale operations, but it may take 10 years to reach that level.

Gen.Prachya Chalermwat, Phd.

ที่มาจากหนังสือพิมพ์ Bangkok Post 2 FEB 2022

WIN TOGETHER

สารผู้ตรวจประเมิน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ “สกมช.” ได้ก่อตั้งขึ้นด้วยวัตถุประสงค์เพื่อให้รัฐมีหน่วยงานที่ส่งเสริมให้เกิดการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อย่างเป็นระบบและมีประสิทธิภาพ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ ความสงบเรียบร้อยภายในประเทศ หรือผลกระทบต่อด้านอื่น ๆ รวมทั้งทำหน้าที่เป็นศูนย์กลางดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง

จากการประเมินผลการดำเนินการของ สกมช. ประจำปี 2564 ซึ่งเป็นปีแรกของการก่อตั้งสำนักงาน ผ่านการพิจารณาใน 4 มิติ คือ 1. มิติด้านประสิทธิผล (Effectiveness) 2. มิติด้านประสิทธิภาพ (Efficiency) 3. มิติด้านการตอบสนองต่อประชาชน (Service) และ 4. มิติด้านความยั่งยืน (Sustainability) นั้นได้คะแนนเฉลี่ยรวมอยู่ที่ **92.831 คะแนน หรือระดับ “ดีมาก”** เนื่องจากมีผลการดำเนินการในหลากหลายภารกิจ ทั้งความสำเร็จในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) การจัดทำระเบียบหรือกฎหมายลำดับรองภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 การส่งเสริมความร่วมมือกับหน่วยงานทั้งในและต่างประเทศ การพัฒนาบุคลากรด้านการรักษาความปลอดภัยไซเบอร์ การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และการประสาน เฝ้าระวัง แจ้งเหตุ และแก้ไขภัยคุกคามทางไซเบอร์

อย่างไรก็ดี สกมช. อาจต้องพิจารณาปรับปรุงด้านการบริหารงานด้านทรัพยากรบุคคล การบริหารความเสี่ยง การบริหารงบประมาณ และการกำกับดูแลที่ดีตั้งแต่เริ่มต้น เพื่อให้เกิดความยั่งยืนในระยะยาว รวมถึงควรเพิ่มกำลังคนและกลไกการส่งเสริม สนับสนุนงานวิจัยและพัฒนาเทคโนโลยีองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมกับการพัฒนาความสัมพันธ์กับภาคีเครือข่ายการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในและต่างประเทศผ่านการสื่อสาร การประสานงาน การพัฒนาศักยภาพ และการสร้างความร่วมมือที่เข้มแข็ง เพื่อให้พร้อมตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพตามนโยบาย แผนงาน หลักเกณฑ์ แนวปฏิบัติและกฎระเบียบที่ได้กำหนดไว้

โดยรวม คะแนนผลการประเมินองค์กรในปีแรกที่ระดับ “ดีมาก” ด้วยกำลังคนและงบประมาณที่จำกัด **คงเป็นสัญญาณที่ดีว่า สกมช. จะสามารถเป็นผู้นำในการขับเคลื่อนการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ**อย่างมีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ในทุกมิติตามวิสัยทัศน์ที่องค์กรได้กำหนดไว้อย่างยั่งยืน

(นายอดิศัย กุญชร ณ อยุธยา)
กรรมการผู้จัดการ บริษัท วินทูเกเตอร์ จำกัด

คณะกรรมการ สกมช.

พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี
ปฏิบัติหน้าที่ประธานกรรมการ

กรรมการโดยตำแหน่ง

พลเอก ชัยชาญ ช้างมงคล
รัฐมนตรีช่วยว่าการ
กระทรวงกลาโหม

ศาสตราจารย์พิเศษ วิศิษฏ์ วิศิษฏ์สรอรรถ
ปลัดกระทรวงยุติธรรม

นายชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

พลตำรวจเอก สุวัฒน์ แจ้งยอดสุข
ผู้บัญชาการตำรวจแห่งชาติ

นายกฤษฎา จีนะวิจารณะ
ปลัดกระทรวงการคลัง

พลเอก ณัฐพล นาคพาณิชย์
เลขาธิการ
สภาความมั่นคงแห่งชาติ

พลเอก ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ

คณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

กรรมการผู้ทรงคุณวุฒิ

ดร.ปริญญา หอมเอนก
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

พลเอก มโน นุชเกษม
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

พันตำรวจเอก ญาณพล ยั่งยืน
ด้านวิศวกรรมศาสตร์

นายไพบูลย์ อมรภิญโญเกียรติ
ด้านกฎหมาย

นายวิเชฐ ตันติวานิช
ด้านการเงิน

นายแพทย์บดินทร์ ทรัพย์สมบูรณ์
ด้านสาธารณสุข

รองศาสตราจารย์ ดร.ปณิธาน วัฒนายากร
ด้านความสัมพันธ์ระหว่างประเทศ

นายชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
ประธานกรรมการ

กรรมการโดยตำแหน่ง

นายธานี ทองภักดี
ปลัดกระทรวง
การต่างประเทศ

นายชยธรรม์ พรหมศร
ปลัดกระทรวงคมนาคม

นางสาวอัจฉรินทร์ พัฒนพันธิชัย
ปลัดกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

นายกุลิศ สมบัติศิริ
ปลัดกระทรวงพลังงาน

นายสุทธิพงษ์ จุลเจริญ
ปลัดกระทรวงมหาดไทย

นายแพทย์เกียรติภูมิ วงศ์รจิต
ปลัดกระทรวงสาธารณสุข

พลตำรวจเอก สุวัฒน์ แจ้งยอดสุข
ผู้บัญชาการตำรวจแห่งชาติ

พลเอก เฉลิมพล ศรีสวัสดิ์
ผู้บัญชาการทหารสูงสุด

พลเอก ณัฐพล นาคพาณิชย์
เลขาธิการสภาความมั่นคงแห่งชาติ

นายธนากร บัวรัษฎ์
ผู้อำนวยการสำนักข่าวกรองแห่งชาติ

พลเอก ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ

คณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

กรรมการผู้ทรงคุณวุฒิ

นายเศรษฐพุฒิ สุทธิวาทนฤพุฒิ
ผู้ว่าการธนาคารแห่งประเทศไทย

นางสาวรื่นวดี สุวรรณมงคล
เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์ และตลาดหลักทรัพย์

นายไตรรัตน์ วิริยะศิริกุล
รองเลขาธิการ กสทช.
รักษาการแทน
เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

พลตรี ปนิวัธน์ ทรัพย์รุ่งเรือง
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ดร.พันธ์ศักดิ์ ศิริรัชตพงษ์
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ดร.รอม หิรัญพฤกษ์
ด้านวิทยาศาสตร์หรือด้านวิศวกรรมศาสตร์

พลตำรวจตรี พิสิษฐ์ เปาอินทร์
ด้านกฎหมาย

นายชัยวุฒิ ธนาคมานุสรณ์
รัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
ประธานกรรมการ

กรรมการโดยตำแหน่ง

นางสาวอัจฉรินทร์ พัฒนพันธิชัย
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

นางสาวกุลยา ตันติเตมิท
อธิบดีกรมบัญชีกลาง

นายกิติพงษ์ มหารัตนวงศ์
ผู้ช่วยเลขาธิการ ก.พ.

นางสาวสุนทรี สุภาสงวน
รองเลขาธิการ ก.พ.ร.

พลเอก ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กรรมการและเลขานุการ

คณะกรรมการบริหาร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

กรรมการผู้ทรงคุณวุฒิ

ดร.ชัยชนะ มิตรพันธ์
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

พลเอก ภุชพงศ์ พงษ์ศิริ
ด้านสังคมศาสตร์

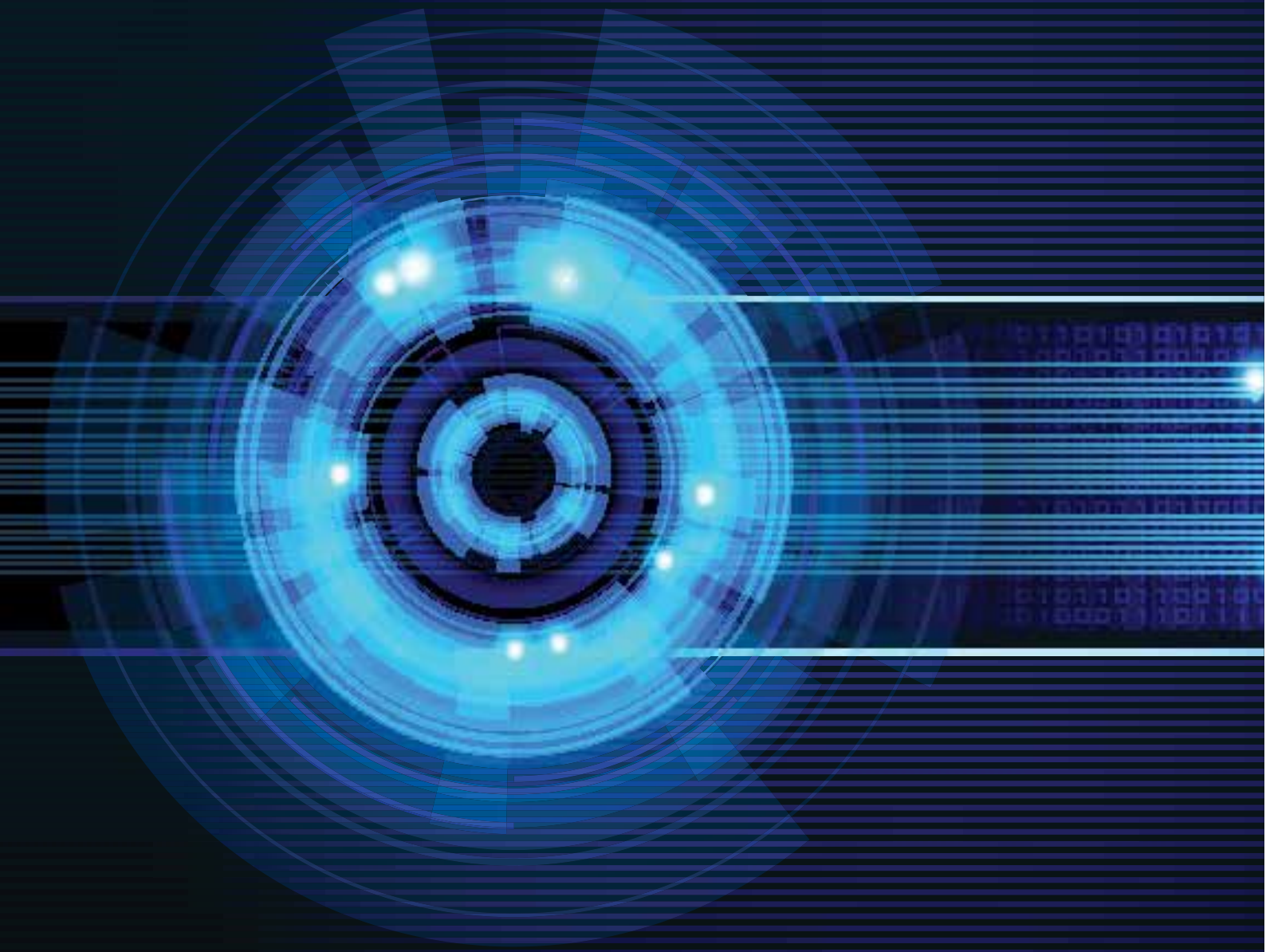
รองศาสตราจารย์ สุรศักดิ์ สงวนพงษ์
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

นายสราวุธ เบญจกุล
ด้านกฎหมาย

รองศาสตราจารย์ ดร.เสาวณีย์ ไทยรุ่งโรจน์
ด้านเศรษฐศาสตร์

นางแก้วใจ นาคสกุล
ด้านบริหารจัดการองค์กร

บทสรุปผู้บริหาร



ทุกวันนี้เราปฏิเสธไม่ได้ว่าภัยคุกคามทางไซเบอร์มีผลต่อการดำเนินชีวิตประจำวันของเราไม่ว่าจะทางตรงหรือทางอ้อมและนับวันจะทวีความรุนแรงขึ้นและก่อให้เกิดผลเสียหายเป็นวงกว้าง ดังนั้น รัฐบาลได้เล็งเห็นความจำเป็นอย่างยิ่งในการที่จะต้องมีหน่วยงานเฉพาะที่จะทำหน้าที่ป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ให้เป็นไปอย่างมีประสิทธิภาพ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงได้รับการจัดตั้งขึ้นตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 โดยเมื่อวันที่ 7 ตุลาคม 2563 ในการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ 3/2563 ซึ่งมี พลเอก ประวิตร วงษ์สุวรรณ รองนายกรัฐมนตรี ปฏิบัติหน้าที่ ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นประธานการประชุมได้มีมติเห็นชอบการแต่งตั้ง พลโท ดร.ปรัชญา เฉลิมวัฒน์ (ยศในขณะนั้น) เป็นเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และได้เริ่มปฏิบัติหน้าที่อย่างเป็นทางการโดยมีผลการดำเนินงานตามภารกิจสำคัญที่ได้รับมอบหมายดังต่อไปนี้

• การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นแนวทางสำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ เสริมสร้างศักยภาพในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนตอบสนองต่อเหตุภัยคุกคามและฟื้นฟูระบบให้กลับคืนสู่สภาวะปกติอย่างทันท่วงที ซึ่งสอดคล้องกับนโยบายยุทธศาสตร์และแผนระดับชาติและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

• การจัดทำกฎหมายลำดับรอง ประกาศระเบียบที่เกี่ยวข้อง

การจัดทำกฎหมายลำดับรองสำหรับบังคับใช้กับหน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศเป็นหลัก จำนวนทั้งสิ้น 5 ฉบับ และกฎหมายลำดับรองที่เกี่ยวกับหน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National Computer Emergency Response Team : National-CERT) รวมทั้งกฎหมายลำดับรองที่เกี่ยวกับการบริหารงานภายในของสำนักงาน

• ส่งเสริมความร่วมมือ กับหน่วยงานองค์กรทั้งภายในประเทศ และระหว่างประเทศ

ความร่วมมือกับหน่วยงานในประเทศ ได้มีการจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Thailand's National Cyber Exercise 2022) โดยมีผู้เข้าร่วมการฝึกจากหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง จำนวน 66 หน่วยงาน รวมเป็นจำนวนทั้งสิ้น 458 คน โดยดำเนินการฝึกแบบผสมผสาน (Hybrid Event) รวมทั้งการส่งเสริมความร่วมมือกับหน่วยงานต่างประเทศ ภายใต้กรอบความร่วมมือทวิภาคีและพหุภาคี ASEAN APEC EU OSCE โดยดำเนินการภายใต้ข้อจำกัดจากการแพร่ระบาดโรคติดเชื้อไวรัสโคโรนา 2019 เพื่อให้เกิดผลเป็นรูปธรรมในการสร้างเครือข่ายที่เข้มแข็งต่อไปในอนาคต

• เฝ้าระวัง ตอบโต้ ภัยคุกคามทางไซเบอร์

จากสถานการณ์ภัยคุกคามทางไซเบอร์ในปีที่ผ่านมา สกมช. จึงได้จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ National CERT ขึ้นเมื่อวันที่ 11 สิงหาคม 2564 เพื่อเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ติดตาม วิเคราะห์และประมวลผลข้อมูลและการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยกำหนดมาตรการเชิงรุก มาตรการเชิงรับ และการบริหารจัดการคุณภาพเพื่อให้ตอบสนองภัยคุกคามได้อย่างทันท่วงที โดยได้มีส่วนในการแก้ปัญหาให้แก่หลายหน่วยงาน ที่เห็นได้อย่างชัดเจนที่สุดคือการแก้ปัญหาในสถานการณ์การแพร่ระบาดโรคติดเชื้อไวรัสโคโรนา 2019 ในระบบการบริหารจัดการวัคซีนของภาครัฐ โดยการตรวจสอบช่องโหว่ เฝ้าระวังและป้องกันภัยที่อาจมีต่อระบบ ทำให้ประชาชนและประเทศไทยข้ามพ้นวิกฤติมาได้อย่างปลอดภัย ซึ่งภัยคุกคามทางไซเบอร์ในอนาคต ได้แก่ การสร้างเว็บไซต์ปลอมหรือเลียนแบบเพื่อหลอกลวง (Website Phishing) และ การโจมตีโดย Ransomware จะมีแนวโน้มสูงขึ้นเป็นทวีคูณ จึงจำเป็นที่จะต้องสร้างความตระหนักรู้ให้แก่ผู้ใช้งานทุกคนอย่างต่อเนื่องต่อไป

• การพัฒนาบุคลากร หลักสูตรด้านความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนสร้างการตระหนักรู้

สกมช. ได้จัดโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 1 เป็นโครงการที่จัดทำขึ้นเพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สูงขึ้น และเพื่อเร่งพัฒนาผู้เชี่ยวชาญและบุคลากรด้าน Cybersecurity ทั้งในภาครัฐและภาคเอกชน ให้เพียงพอรองรับกับภัยคุกคามไซเบอร์ที่มาพร้อมกับยุคดิจิทัล มีการจัดการบรรยาย/เสวนาให้ความรู้ Cybersecurity Knowledge Sharing การจัดงานสัมมนา Thailand National Cyber Week 2021 การประชุมเชิงปฏิบัติการสำหรับหน่วยงานควบคุมหรือกำกับดูแล หน่วยงานภาครัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประจำปี พ.ศ. 2564 – 2565 (NCSA Cyber Clinic 2021 - 2022) การจัดโครงการความร่วมมือทางวิชาการเพื่อพัฒนาบุคลากรด้านไซเบอร์ โครงการ APT Expert Mission in 2021 และโครงการ Microsoft Women@Cybersecurity เป็นต้น

• การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ

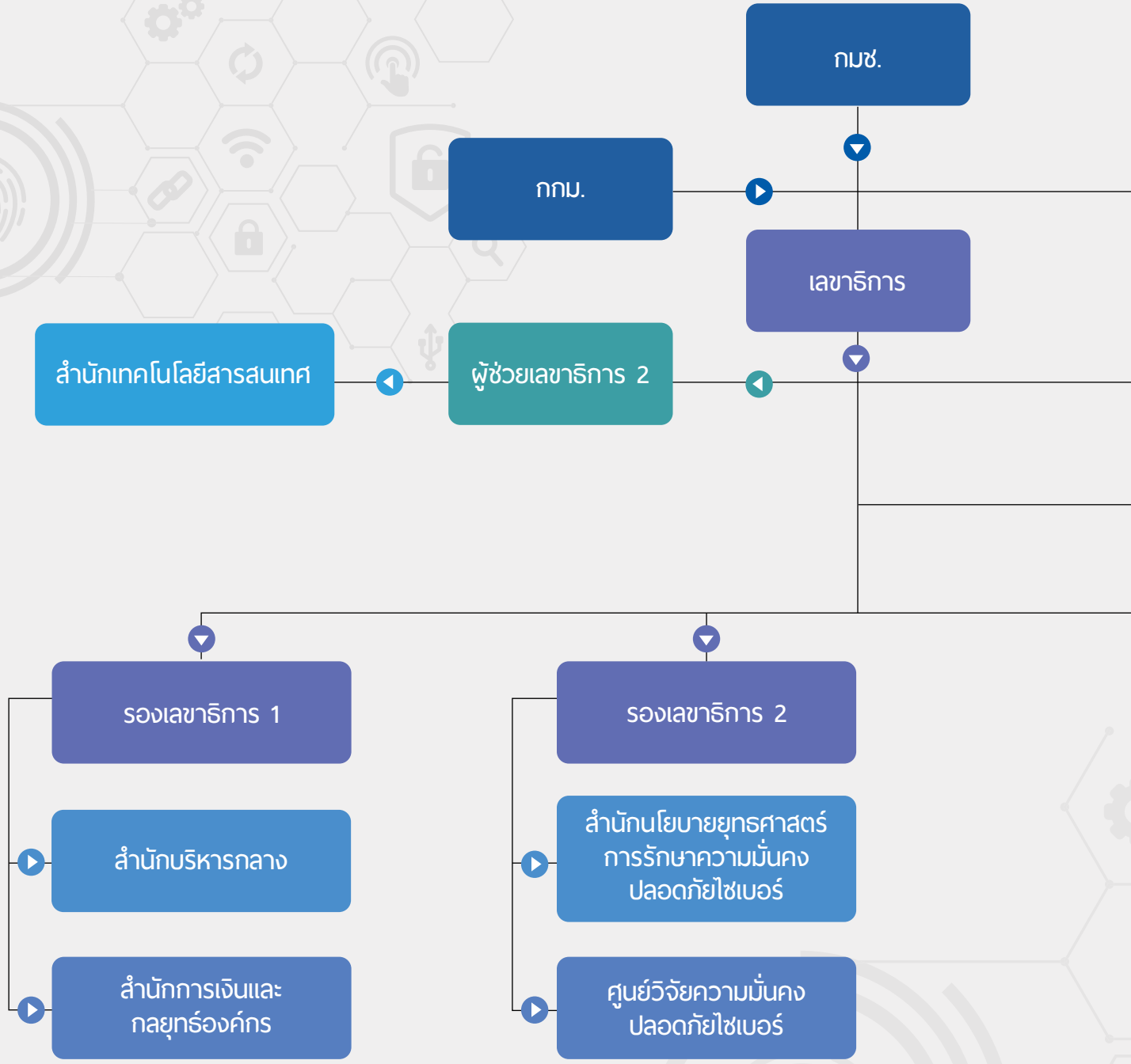
สกมช. ได้จัดกิจกรรมเพื่อยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้มาตรการควบคุมเข้มงวดตามที่รัฐบาลกำหนดเรื่องการลดการแพร่ระบาดโรคติดเชื้อไวรัสโคโรนา 2019 จึงได้จัดการอบรมเชิงปฏิบัติการในการใช้อีเมลสื่อสารด้วย Pretty Good Privacy (PGP) จัดการแข่งขัน Thailand Cyber Top

Talent 2021 เข้าร่วมแข่งขัน Cyber SEA Games 2021 ตลอดจนจัดการอบรม World Class Cyber Security Practices โดย MITRE/CISA/SEI ทั้งหมดในรูปแบบออนไลน์

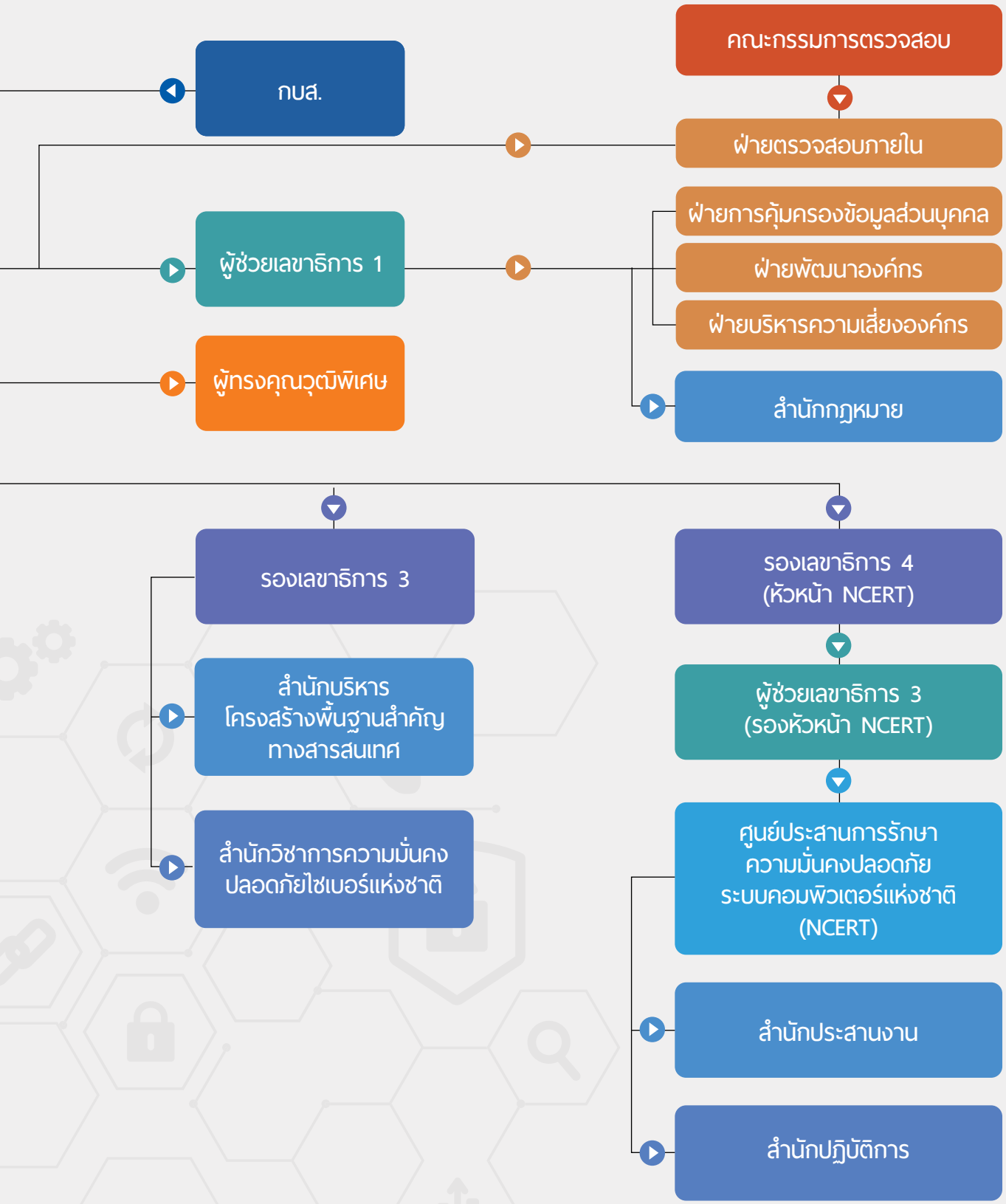
ผลการประเมินการดำเนินงาน ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประจำปี 2564

ผลการประเมินการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตามมาตรา 39 แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีการประเมินผลการดำเนินงานองค์กรในปีแรกผ่านแนวคิดการประเมินในมุมมอง 4 มิติ ตาม “2E2S” คือ 1) มิติด้านประสิทธิผล (Effectiveness) ได้ระดับคะแนน 95.330 คะแนน 2) มิติด้านประสิทธิภาพ (Efficiency) ได้ระดับคะแนน 99.995 คะแนน 3) มิติด้านการตอบสนองต่อประชาชน (Service) ได้ระดับคะแนน 100.000 คะแนน 4) มิติด้านความยั่งยืน (Sustainability) ได้ระดับคะแนน 76.000 คะแนน รวมแล้วได้คะแนนผลการประเมินการดำเนินงาน ประจำปี 2564 คือ **92.831 คะแนน หรือ “ดีมาก”** โดยอาจต้องพิจารณาปรับปรุงการบริหารงานภายใน เพื่อให้เกิดความยั่งยืนในระยะยาว

“วันนี้ด้วยความร่วมแรงร่วมใจของพี่น้อง สกมช. จึงทำให้เราได้รับการยอมรับและเป็นที่รู้จักอย่างกว้างขวางและเราจะมุ่งมั่นพัฒนาต่อไปอย่างไม่หยุดยั้งเพื่อให้องค์กรที่เป็นฟันเฟืองเล็กๆ อย่างพวกเราสามารถช่วยงานที่ยิ่งใหญ่ของรัฐบาลในการขับเคลื่อนเศรษฐกิจและความมั่นคงของประเทศไทยในยุคดิจิทัลและทำให้พี่น้องประชาชนทุกคนปลอดภัยจากภัยคุกคามทางไซเบอร์ตลอดไป”


กมช.
กกม.
เลขาธิการ
สำนักเทคโนโลยีสารสนเทศ
ผู้ช่วยเลขาธิการ 2
รองเลขาธิการ 1
รองเลขาธิการ 2
สำนักบริหารกลาง
สำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์
สำนักการเงินและกลยุทธ์องค์กร
ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์

โครงสร้างองค์กร



พลเอก ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการ

พลโท กฤษณ์ ลัยวิรัตน์
รองเลขาธิการ 1

นาวาอากาศเอก อมร ชมเชย
รองเลขาธิการ 4

พลโท ปริญญา ฉายดิลก
ผู้เชี่ยวชาญ

พลโท สุชาติ วงษ์มาก
ผู้ทรงคุณวุฒิพิเศษ 1

พันเอก คทาวุธ ขจรกิตติยุทธ
ผู้ทรงคุณวุฒิพิเศษ 2

พันเอก ธีรวุฒิ วิทยากรณ์
ผู้ช่วยเลขาธิการ 3

ผู้บริหาร
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

นาวาเอก ดร.ณัฐพนธ์ ชาติปรีชากุล
ปฏิบัติหน้าที่ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ผศ. ดร.วราภรณ์ พรหมวิกร
ผู้อำนวยการสำนักบริหารกลาง

นางมัตติกา จงพิริยะอนันต์
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

นางกิ่งนภา บางชวด
ผู้อำนวยการสำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์

พันเอก สุวัจชัย บุญสม
ปฏิบัติหน้าที่ ผู้อำนวยการศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์

นาวาอากาศเอก จเด็ด คูหะก้องกิจ
ผู้อำนวยการสำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

นาวาเอกหญิง ศิริเนตร รักษ์วงศ์
ผู้อำนวยการสำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นางสาวสายชล แซ่ลี้
รักษาการ ผู้อำนวยการสำนักประสานงาน

พันตำรวจเอก ณัทกฤช พรหมจันทร์
ผู้อำนวยการสำนักปฏิบัติการ

นางสาวดรุณี พิกุลทอง
ผู้อำนวยการสำนักกฎหมาย

นาวาตรี ศักติพงษ์ สิบหมื่นเปี่ยม
ผู้อำนวยการฝ่ายตรวจสอบภายใน

Our Profile

เกี่ยวกับ สกมช.

เหตุการณ์สำคัญ สกมช.

01 28 พฤษภาคม 2562 “สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “สกมช.” หรือเรียกเป็นภาษาอังกฤษว่า “National Cyber Security Agency” (NCSA) ได้จัดตั้งขึ้นตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ภายใต้การกำกับดูแลของนายกรัฐมนตรี

02 11 ธันวาคม 2562 ตามมาตรา 5 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มี “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กมช.” หรือเรียกเป็นภาษาอังกฤษว่า “National Cyber Security Committee” (NCSC) โดยมี พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรีเป็นประธานกรรมการ

03 10 พฤษภาคม 2563 ตามมาตรา 12 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.” โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

04 13 สิงหาคม 2563 คำสั่งสำนักนายกรัฐมนตรี ที่ 239/2563 มอบหมายและมอบอำนาจให้ พลเอก ประวิตร วงษ์สุวรรณ รองนายกรัฐมนตรี ปฏิบัติหน้าที่ประธานกรรมการ

05 20 สิงหาคม 2563 ตามมาตรา 25 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กบส.” โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ

06 1 มกราคม 2564 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ได้แต่งตั้ง พลโท ดร.ปรัชญา เฉลิมวัฒน์ (ยศในขณะนั้น) เป็นเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

07 18 พฤษภาคม 2564 คณะรัฐมนตรีมีมติให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ จำนวนทั้งสิ้น 42 ราย มาปฏิบัติงานที่สำนักงานเป็นการชั่วคราวภายในระยะเวลาหนึ่งร้อยแปดสิบวัน

08 18 สิงหาคม 2564 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้เปิดตัวสำนักงานอย่างเป็นทางการ เพื่อรับมือกับภัยคุกคามด้านไซเบอร์ที่ทวีความรุนแรงมากขึ้นและอาจส่งผลกระทบต่อเศรษฐกิจ สังคม และความมั่นคงของประเทศ

วิสัยทัศน์ VISION

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

พันธกิจ MISSIONS

เสนอแนะนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดแนวทาง มาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

กำกับ ดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

เป็นศูนย์กลางในการประสานความร่วมมือ รวมทั้งส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศและต่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

เผยแพร่ความรู้ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เป้าหมาย GOALS

1. มีระบบบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ที่พร้อมรับมือต่อภัยคุกคามในทุกรูปแบบ

2. หน่วยงานภาครัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีการปกป้องและพร้อมตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

3. มีเครือข่ายความร่วมมือที่เข้มแข็งทั้งในประเทศและต่างประเทศ

4. มีบุคลากรไซเบอร์อย่างเพียงพอสอดรับกับความต้องการของประเทศ

5. หน่วยงานที่เกี่ยวข้องมีความตระหนัก รับรู้ และเข้าใจถึงความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์องค์กร STRATEGIES

กลยุทธ์ที่ 1 พัฒนาขีดความสามารถของสำนักงานในการป้องกัน รับมือ เฝ้าระวัง และแก้ไขภัยคุกคามไซเบอร์

กลยุทธ์ที่ 2 ศึกษาแนวโน้ม ทิศทาง และการจัดทำนโยบาย/แผน/กฎหมาย/กฎระเบียบ/ประกาศ/มาตรการ/มาตรฐาน ที่สนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

กลยุทธ์ที่ 3 ส่งเสริม สนับสนุนงานวิจัยและพัฒนาเทคโนโลยีองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 4 สนับสนุนการดำเนินงานตามยุทธศาสตร์ นโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระดับหน่วยงาน

กลยุทธ์ที่ 5 กำกับ ดูแล ให้หน่วยงานที่เกี่ยวข้องสามารถป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์

กลยุทธ์ที่ 6 สร้างเครือข่ายความร่วมมือเพื่อบูรณาการทำงานร่วมกัน รวมถึงส่งเสริมสนับสนุนการแลกเปลี่ยนข้อมูล

กลยุทธ์ที่ 7 พัฒนาศักยภาพและเพิ่มทักษะบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 8 สร้างบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 9 สร้างความตระหนักและการรับรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางขับเคลื่อนระยะ 3 ปี PROGRESSION

ผลที่ได้รับ SUCCESS

ประเทศไทยมีความมั่นคงและมีขีดความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์ในทุกมิติ

ค่านิยมองค์กร Core Value

S	E	C	U	R	E
Sustainable (ความยั่งยืน)	Enthusiastic (มีศรัทธาแรงกล้า)	Collaboration (พร้อมให้ความร่วมมือ)	Unity (ความเป็นน้ำหนึ่งใจเดียว)	Responsiveness (ตอบสนองอย่างรวดเร็ว)	Excellency (ความเป็นเลิศ)

"

สกมช. จะมุ่งมั่นสร้างเสถียรภาพด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ประชาชนมีความมั่นใจและรู้สึกปลอดภัยในการใช้เทคโนโลยีดิจิทัล เราพร้อมให้ความร่วมมือกับทุกภาคส่วน เพื่อรวมพลังกันในการตอบสนองต่อภัยคุกคามทางไซเบอร์ในทุกรูปแบบอย่างรวดเร็วด้วยการเป็นศูนย์แห่งความเป็นเลิศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศเพื่อให้เกิดประโยชน์และความปลอดภัยสูงสุดแก่ประเทศชาติและประชาชนอย่างยั่งยืนตลอดไป

"

พลเอก ดร.ปรัชญา เฉลิมวัฒน์

เป้าหมายการดำเนินงาน



NCSA
สกมช

NCSA



NCSA
สกมช

NCX
2022
NCSA
สกมช
DGA
กสท
true
PEA
ptt
SET

รายงานผลการดำเนินงาน 2564

1 ขับเคลื่อน

การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์

2 จัดทำ

การจัดทำกฎหมายลำดับรอง ประกาศ ระเบียบที่เกี่ยวข้อง

3 ส่งเสริม

ส่งเสริมความร่วมมือกับหน่วยงานองค์กรทั้งภายในประเทศและระหว่างประเทศ

4 ตอบสนอง

เฝ้าระวังตอบโต้ภัยคุกคามทางไซเบอร์

5 พัฒนา

การพัฒนาบุคลากรหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ตลอดจนสร้างการตระหนักรู้

6 ยกระดับ

การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ

1 ขับเคลื่อน

การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์

2 จัดทำ

การจัดทำกฎหมายลำดับรอง ประกาศ ระเบียบที่เกี่ยวข้อง

3 ส่งเสริม

ส่งเสริมความร่วมมือกับหน่วยงานองค์กรทั้งภายในประเทศและระหว่างประเทศ

4 ตอบสนอง

เฝ้าระวังตอบโต้ภัยคุกคามทางไซเบอร์

5 พัฒนา

การพัฒนาบุคลากรหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ตลอดจนสร้างการตระหนักรู้

6 ยกระดับ

การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ

การขับเคลื่อนนโยบายและแผน ด้านความมั่นคงปลอดภัยไซเบอร์

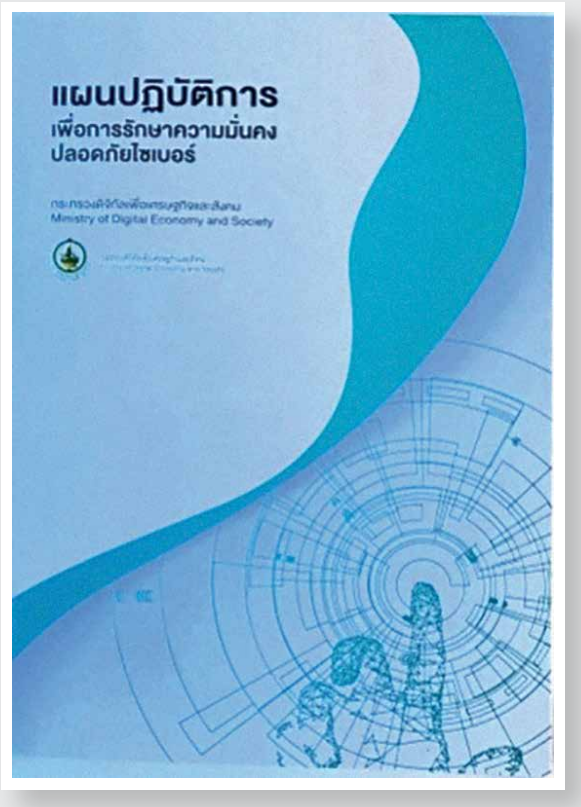
นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)

นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ในการเสริมสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ สามารถตอบสนองต่อเหตุภัยคุกคามตลอดจนฟื้นฟูบริการที่สำคัญให้กลับคืนสู่สภาวะปกติอย่างทันท่วงที และพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

วิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ คือ **“บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์ เพื่อความยั่งยืนทางเศรษฐกิจและสังคม”** และมีประเด็นยุทธศาสตร์หลักทั้งหมด 4 ประเด็นและกลยุทธ์ที่สนับสนุน ดังนี้

แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 – 2570

แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ เสริมสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนตอบสนองต่อเหตุภัยคุกคามและฟื้นฟูระบบให้กลับคืนสู่สภาวะปกติอย่างทันท่วงที ซึ่งสอดคล้องกับนโยบายยุทธศาสตร์และแผนระดับชาติ กรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ



นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (พ.ศ. 2565 - 2570)

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นแนวทางสำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน โดยใช้หลักการตามแนวทางการปฏิบัติที่ดีที่ใช้กันแพร่หลายทั่วโลก รวมถึงประเทศไทย ซึ่งคือ หลักการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) ประกอบด้วย 3 หลักการ ดังนี้

1. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)
2. การบริหารความเสี่ยง (Risk Management)
3. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

1 ขับเคลื่อน

การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์

2 จัดทำ

การจัดทำกฎหมายลำดับรอง ประกาศ ระเบียบที่เกี่ยวข้อง

3 ส่งเสริม

ส่งเสริมความร่วมมือกับหน่วยงานองค์กรทั้งภายในประเทศและระหว่างประเทศ

4 ตอบสนอง

เฝ้าระวังตอบโต้ภัยคุกคามทางไซเบอร์

5 พัฒนา

การพัฒนาบุคลากรหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ตลอดจนสร้างการตระหนักรู้

6 ยกระดับ

การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ

การจัดทำกฎหมายลำดับรองภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

Critical Information Infrastructure

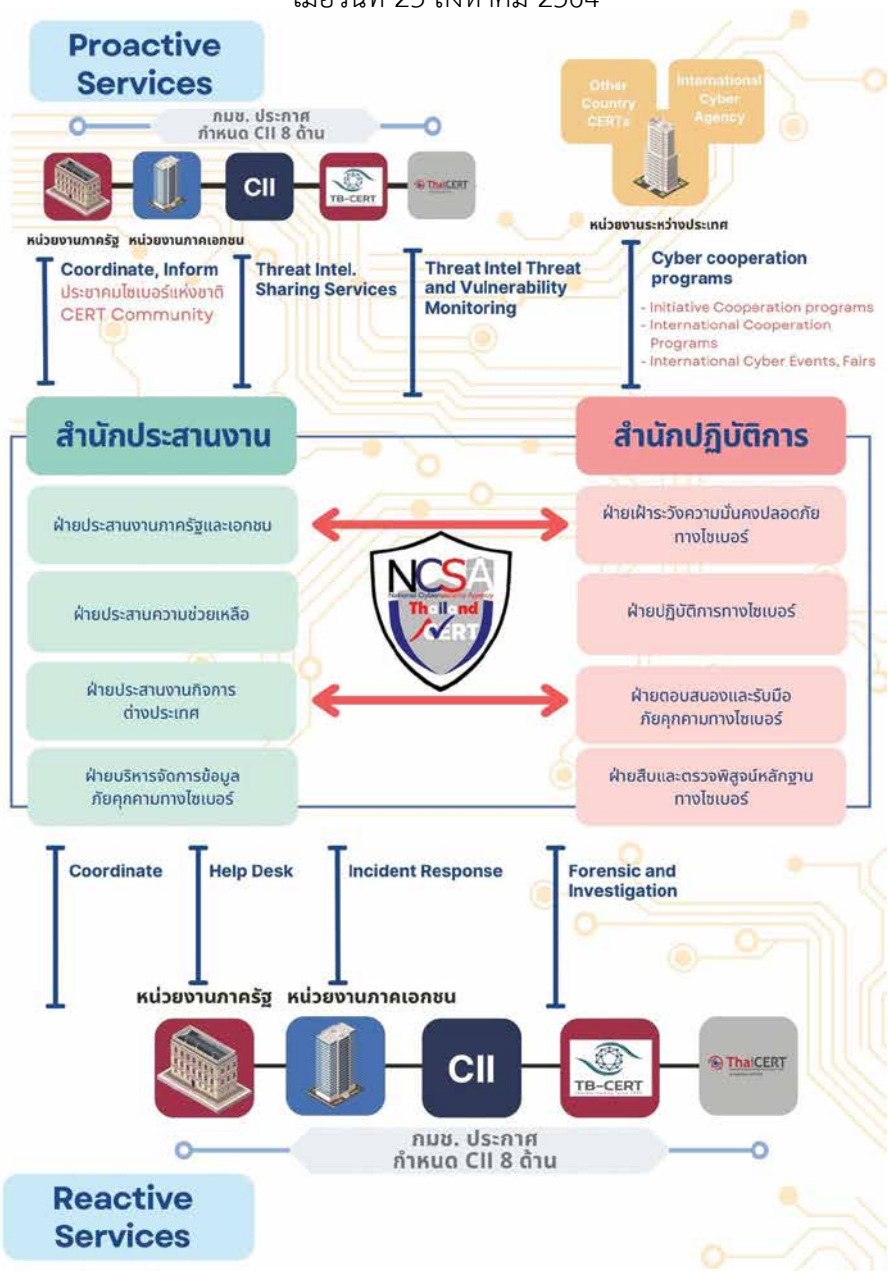
กฎหมายลำดับรอง สำหรับบังคับใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศเป็นหลัก ในการนี้สำนักงานได้ดำเนินการจัดทำและประกาศในราชกิจจานุเบกษาแล้ว ทั้งสิ้น 5 ฉบับ

1. ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศฯ
2. ประกาศ กมช. เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ฯ
3. ประกาศ กมช. เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ฯ
4. ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตราการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับฯ
5. ประกาศ กกม. เรื่องประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ

CYBER SECURITY

การจัดทำกฎหมายลำดับรองที่เกี่ยวกับหน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National Computer Emergency Response Team : National CERT)

สกมช. ได้ดำเนินการจัดทำกฎหมายลำดับรองที่เกี่ยวกับหน้าที่และอำนาจของ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ National CERT ได้แก่ ประกาศคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. 2564 และได้ประกาศลงในราชกิจจานุเบกษา เล่ม 138 ตอนพิเศษ 194 ง เมื่อวันที่ 23 สิงหาคม 2564



ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National Computer Emergency Response Team : National CERT)

การจัดทำระเบียบ ข้อบังคับ และประกาศที่สำคัญของสำนักงาน

การจัดองค์กร

การเงิน

การบริหารงานบุคคล

การบริหารงานทั่วไป

งานตรวจสอบภายใน

สวัสดิการ

1 ขับเคลื่อน

การขับเคลื่อน
นโยบายและแผน
ด้านความมั่นคง
ปลอดภัยไซเบอร์

2 จัดทำ

การจัดทำ
กฎหมายลำดับรอง
ประกาศ ระเบียบ
ที่เกี่ยวข้อง

3 ส่งเสริม

ส่งเสริม
ความร่วมมือ
กับหน่วยงาน
องค์กร
ทั้งภายในประเทศ
และระหว่างประเทศ

4 ตอบสนอง

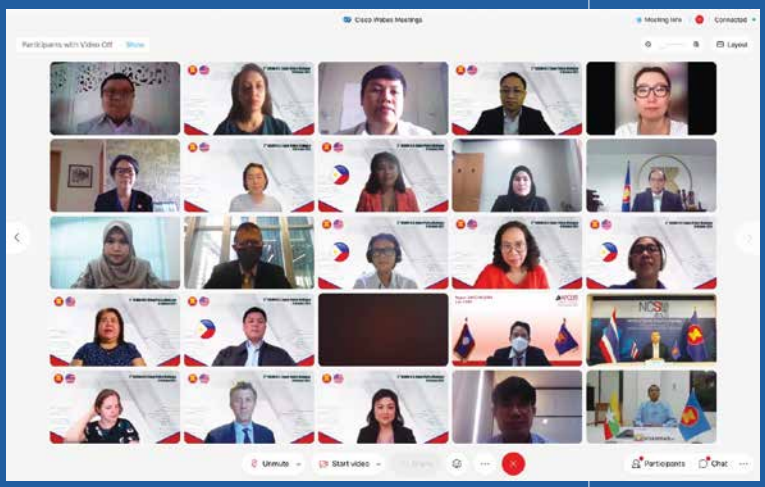
เฝ้าระวัง
ตอบโต้
ภัยคุกคาม
ทางไซเบอร์

5 พัฒนา

การพัฒนา
บุคลากร
หลักสูตร
ด้านความมั่นคง
ปลอดภัย
ไซเบอร์
ตลอดจน
สร้างการตระหนักรู้

6 ยกระดับ

การยกระดับ
หน่วยงาน
โครงสร้าง
พื้นฐานสำคัญ
ทางสารสนเทศ
และหน่วยงาน
ของรัฐ


Cisco Webex Meetings
Meeting Info
Connected
Layout
Unmute
Start video
Participants
Chat


NCSA
สกมช
National Cyber Security Agency
THAILAND


NCSA
สกมช

ความร่วมมือกับหน่วยงาน องค์กรระหว่างประเทศ

Association of South East Asian Nations (ASEAN)

- การเข้าร่วมประชุมต่าง ๆ เช่น การประชุมเตรียมการ ASEAN Network Security Action Council (ANSAC), การประชุม ASEAN - US Cyber Policy Dialogue, การประชุม ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC), การประชุมคณะทำงานร่วมอาเซียนด้านดิจิทัล ภายใต้ ADGSOM และ ATRC ประจำปี 2564 เป็นต้น
- การพิจารณาและความร่วมมืออื่น ๆ เช่น ความเห็นต่อการจัดทำร่างเอกสารแนวคิดการดำเนินงานของศูนย์ ASEAN - CERT, กลุ่มหารือระหว่างอาเซียนกับรัสเซียในประเด็นที่เกี่ยวข้องกับความมั่นคงในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร (ASEAN - Russia), ร่างแผนปฏิบัติการว่าด้วยการดำเนินงานหุ้นส่วนความร่วมมือระหว่างอาเซียน - จีน ด้านเศรษฐกิจดิจิทัล ค.ศ. 2021 - 2025 เป็นต้น

Asia-Pacific Economic Cooperation (APEC)

การเข้าร่วมการประชุมต่าง ๆ เช่น การเป็นเจ้าภาพจัดการประชุมเอเปคของไทยในปี 2565, การประชุมคณะทำงานเอเปคด้านโทรคมนาคมและสารสนเทศ ครั้งที่ 63, ร่างแผนปฏิบัติการวิสัยทัศน์ปุตราจายาของเอเปค ค.ศ. 2040 เป็นต้น

European Union (EU)
การพิจารณาร่างกรอบความตกลงว่าด้วยความเป็นหุ้นส่วนและความร่วมมือรอบด้านระหว่างไทยกับสหภาพยุโรปและรัฐสมาชิก

United Nations (UN)
ความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภายใต้กรอบสหประชาชาติ เช่น OEWG on developments in the field of information and telecommunications, Open-ended Working Group (OEWG) on security of and in the use of ICTs 2021, Global Cybersecurity Index (GCI), การประชุมสหประชาชาติว่าด้วยการค้าและการพัฒนา (United Nations Conference on Trade and Development: UNCTAD) เป็นต้น

Eurasia
การประชุมคณะทำงานร่วมระหว่างไทยกับคณะกรรมาธิการเศรษฐกิจยูเรเซีย ครั้งที่ 2

Organization for Security and Co-operation in Europe (OSCE)
เข้าร่วมการสัมมนาในหลายหัวข้อ เช่น หัวข้อ The Individual and Cyber Security Inter-Regional Conference on Cyber/ICT Security และ Emerging Challenges in Advancing Comprehensive Security เป็นต้น

Organization for Economic Co-operation and Development (OECD)
การจัดทำบันทึกความเข้าใจระหว่างสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้กับองค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา

Conference on Interaction and Confidence-Building Measures in Asia (CICA)
ร่างเอกสาร CICA Catalogue of Confidence Building Measures ว่าด้วยการส่งเสริมปฏิสัมพันธ์และมาตรฐานการสร้างความไว้เนื้อเชื่อใจระหว่างประเทศในภูมิภาคเอเชีย

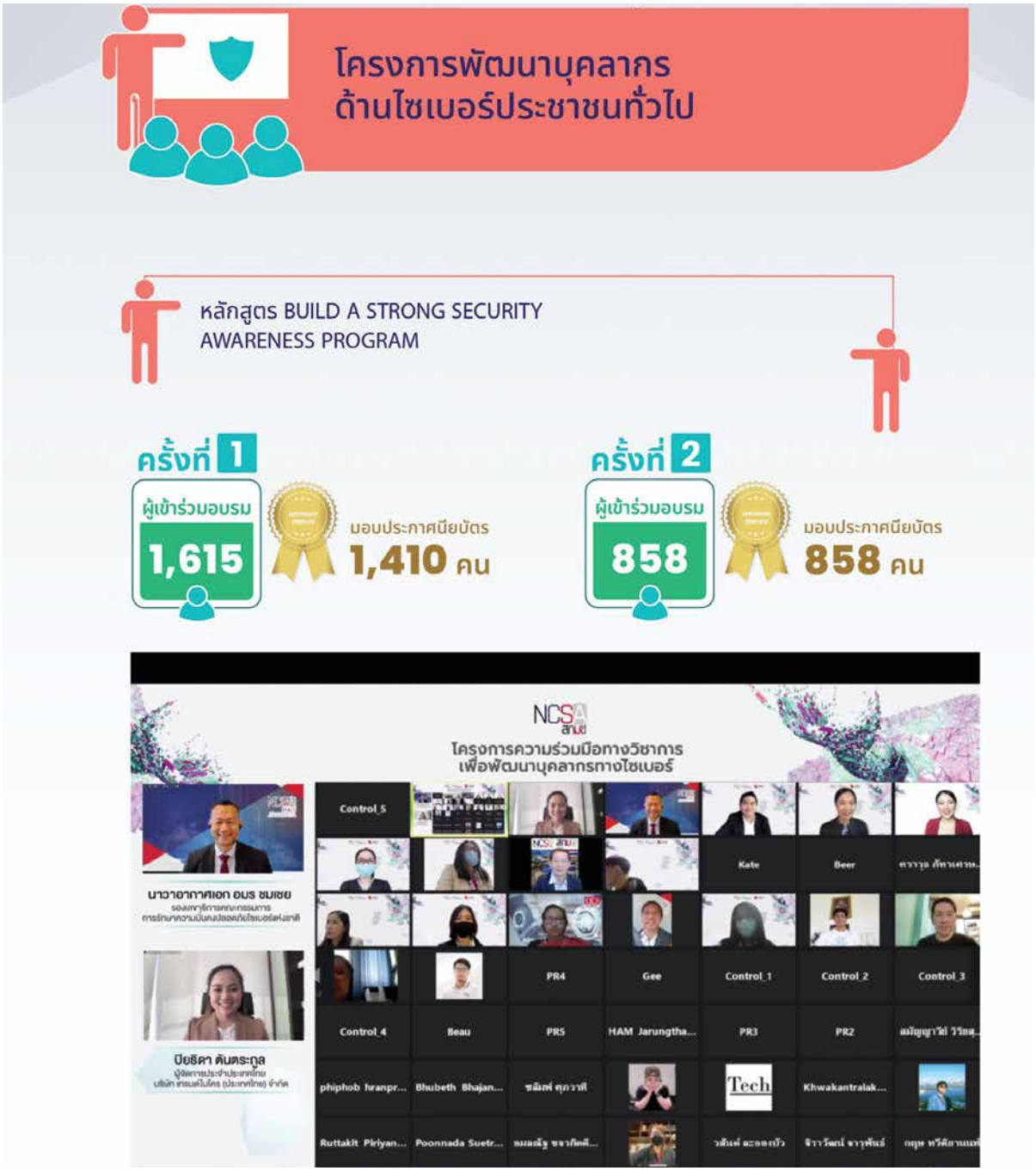
Asian African Legal Consultative Organization (AALCO)
การพิจารณาร่างเอกสาร Consensual Basic Principles of International Law Applicable in Cyberspace

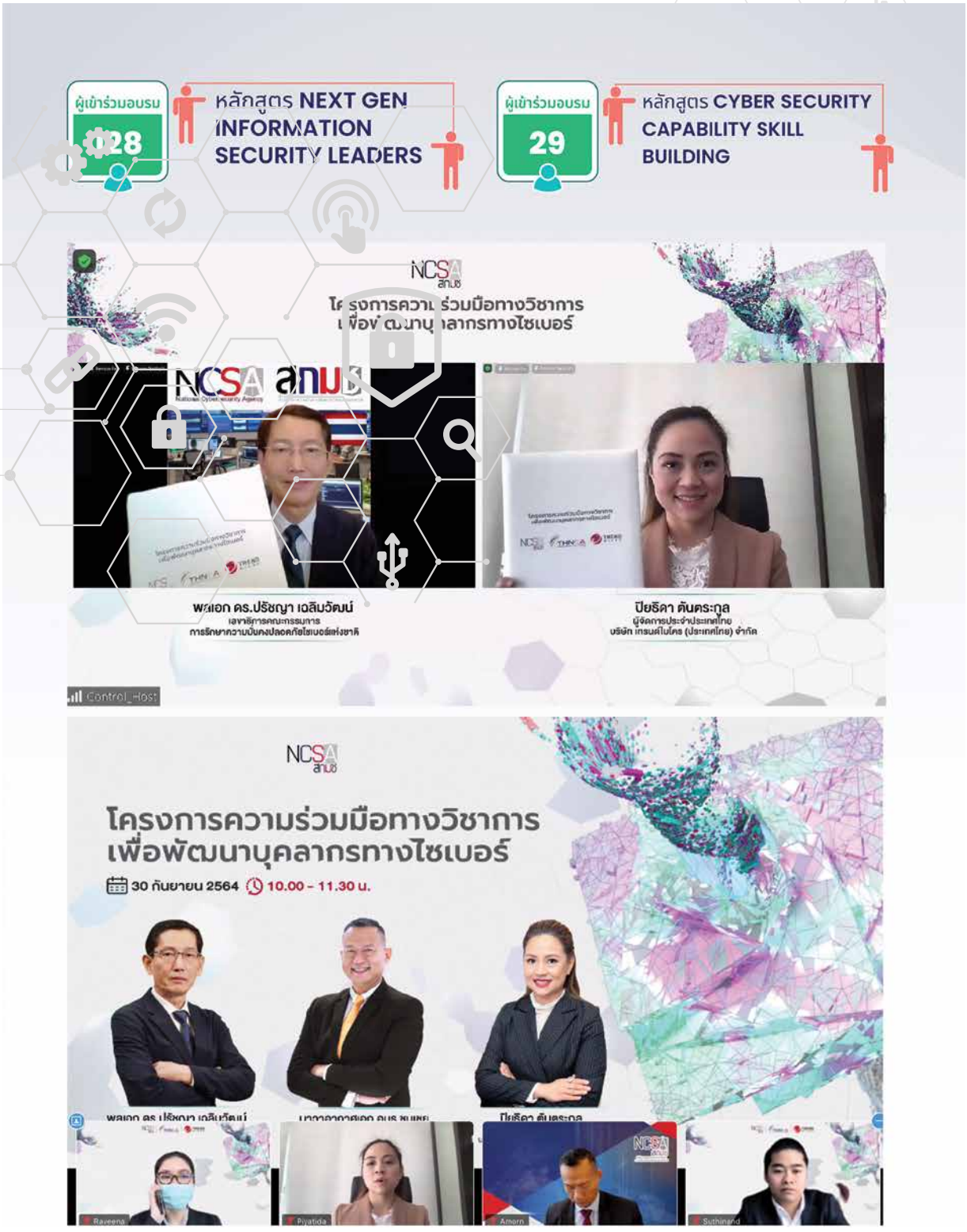
กรอบทวิภาคี (Bilateral)
ออสเตรเลีย : อยู่ระหว่างจัดทำหนังสือแสดงเจตจำนงความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างไทยและออสเตรเลีย (Statement of Intent - Thailand - Australia Cyber Security Cooperation) ภายใต้โครงการ Defensive Readiness and Cyber Security Exercises Program
อินเดีย : อยู่ระหว่างจัดทำบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ระหว่างไทยกับอินเดีย

กรอบความร่วมมืออื่นๆ
ความร่วมมือระหว่างประเทศกับประเทศอื่น ๆ เช่น จีน อินเดีย อิสราเอล สหราชอาณาจักร ออสเตรเลีย ฝรั่งเศส นิวซีแลนด์ สหรัฐอเมริกา เยอรมณี มองโกเลีย และสาธารณรัฐเกาหลี

ความร่วมมือกับหน่วยงานองค์กรในประเทศ

โครงการความร่วมมือทางวิชาการเพื่อพัฒนาบุคลากรด้านไซเบอร์ สกมช. ได้มีแผนฝึกอบรมความรู้ทางด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติที่มุ่งยกระดับความรู้และขีดความสามารถของบุคลากรทางด้านความมั่นคงปลอดภัยไซเบอร์ โดยได้ร่วมมือทางวิชาการกับ บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด ในการพัฒนาบุคลากรด้านไซเบอร์ระหว่างกันในรูปแบบการอบรมออนไลน์ โดยแบ่งเนื้อหาออกเป็น 3 หลักสูตร




ผู้เข้าร่วมอบรม
28
หลักสูตร NEXT GEN INFORMATION SECURITY LEADERS
ผู้เข้าร่วมอบรม
29
หลักสูตร CYBER SECURITY CAPABILITY SKILL BUILDING
NCSA สกมช
พลเอก ดร.ปรัชญา เฉลิมวัฒน์
ปิยธิดา ตันตระกูล
Control_Host
NCSA สกมช
โครงการความร่วมมือทางวิชาการ
เพื่อพัฒนาบุคลากรทางไซเบอร์
30 กันยายน 2564 10.00 - 11.30 น.

4
ตอบสนอง

1
ขับเคลื่อน

2
จัดทำ

3
ส่งเสริม

5
พัฒนา

6
ยกระดับ

เฝ้าระวัง
ตอบโต้
ภัยคุกคาม
ทางไซเบอร์

การขับเคลื่อน
นโยบายและแผน
ด้านความมั่นคง
ปลอดภัยไซเบอร์

การจัดทำ
กฎหมายลำดับรอง
ประกาศ ระเบียบ
ที่เกี่ยวข้อง

ส่งเสริม
ความร่วมมือ
กับหน่วยงาน
องค์กร
ทั้งภายในประเทศ
และระหว่างประเทศ

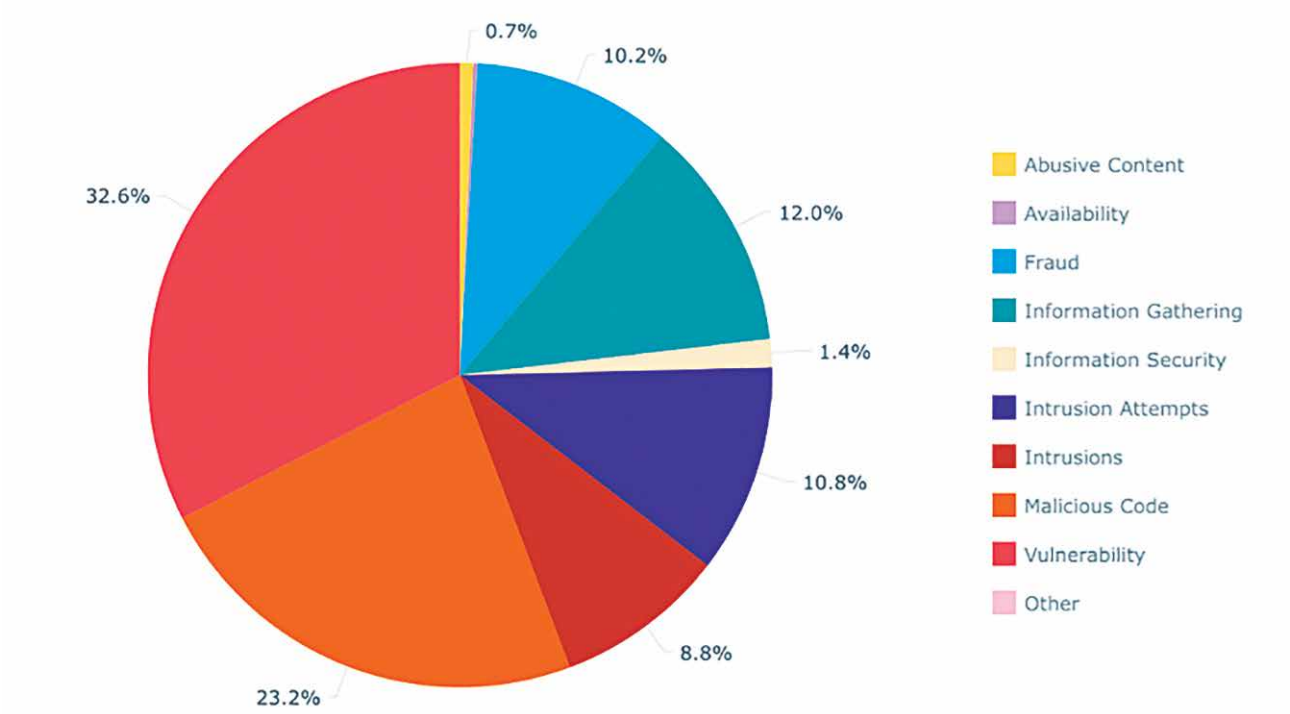
การพัฒนา
บุคลากร
หลักสูตร
ด้านความมั่นคง
ปลอดภัย
ไซเบอร์
ตลอดจน
สร้างการตระหนักรู้

การยกระดับ
หน่วยงาน
โครงสร้าง
พื้นฐานสำคัญ
ทางสารสนเทศ
และหน่วยงาน
ของรัฐ

สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย ปี 2564

ประเภทภัยคุกคาม/เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive Content	0	1	0	0	0	1	0	0	0	5	2	5	14
Availabililty	0	0	1	0	1	0	1	0	0	2	0	0	5
Fraud	46	20	26	16	27	16	13	10	9	13	9	7	212
Information Gathering	12	24	49	25	29	27	42	20	11	4	4	1	248
Information Security	4	5	0	0	2	2	0	2	9	3	1	2	30
Intrusion Attemps	21	15	25	20	14	5	6	4	2	4	13	95	224
Intrusions	32	27	29	8	15	15	11	14	11	14	4	3	183
Malicious Code	8	29	21	10	12	9	11	5	23	96	128	127	479
Vulnerability	31	5	121	64	81	94	77	75	35	31	25	35	674
Total	**154**	**126**	**272**	**143**	**181**	**169**	**161**	**130**	**100**	**172**	**186**	**275**	**2,069**

ตารางที่ 1: แสดงสถิติภัยคุกคาม เดือนมกราคม ถึง ธันวาคม 2564 ของไทยเซิร์ต

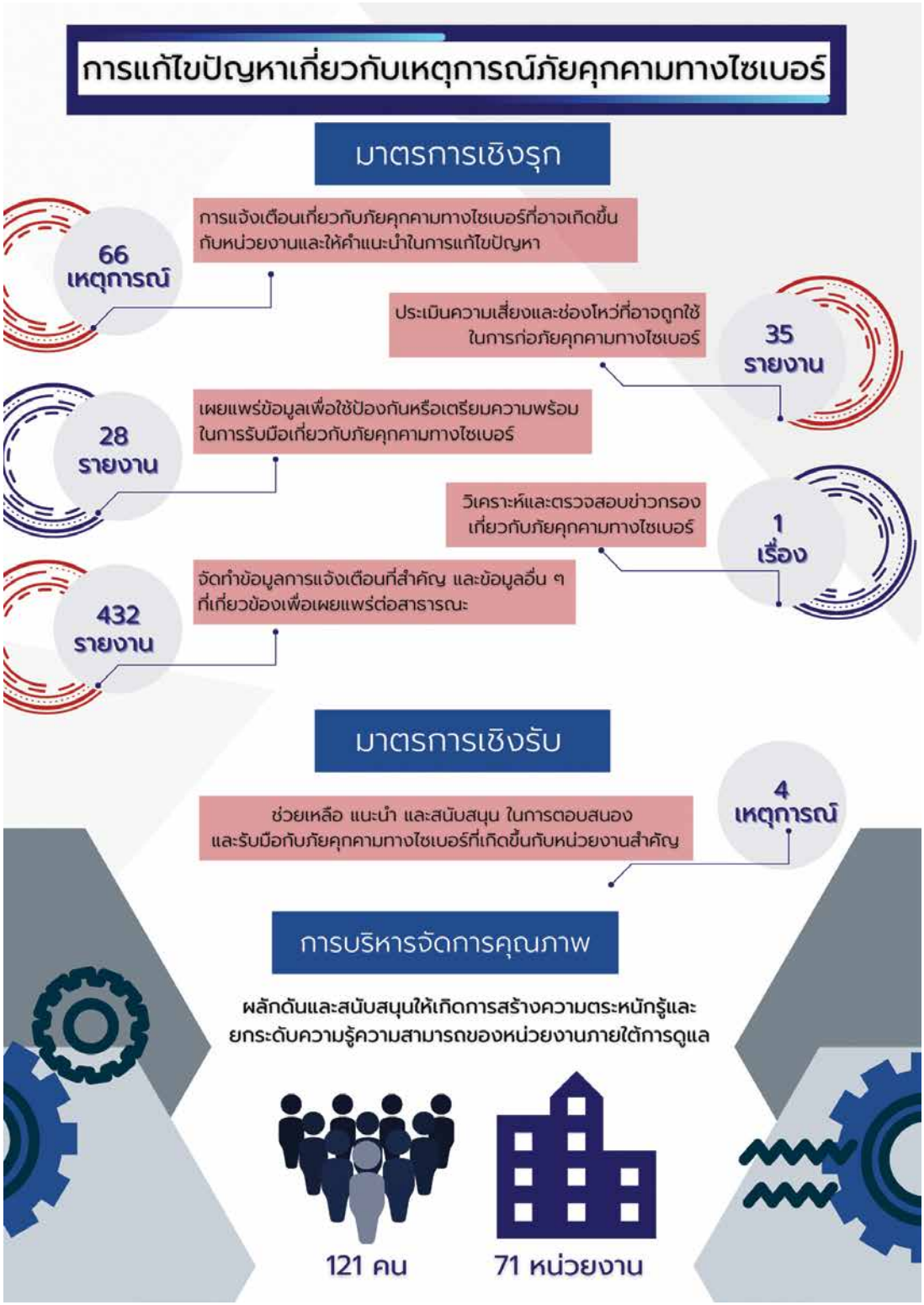


ภาพที่ 1: แสดงประเภทภัยคุกคามทางไซเบอร์

จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ ในปี 2564 โดย ThaiCERT ปรากฏพบภัยคุกคามทางไซเบอร์ประเภท Vulnerability มากที่สุด มีสัดส่วน 32.6% รองลงมาคือ ประเภท Malicious Code และ Information Gathering มีสัดส่วนอยู่ที่ 23.2% และ 12.0% ตามลำดับ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

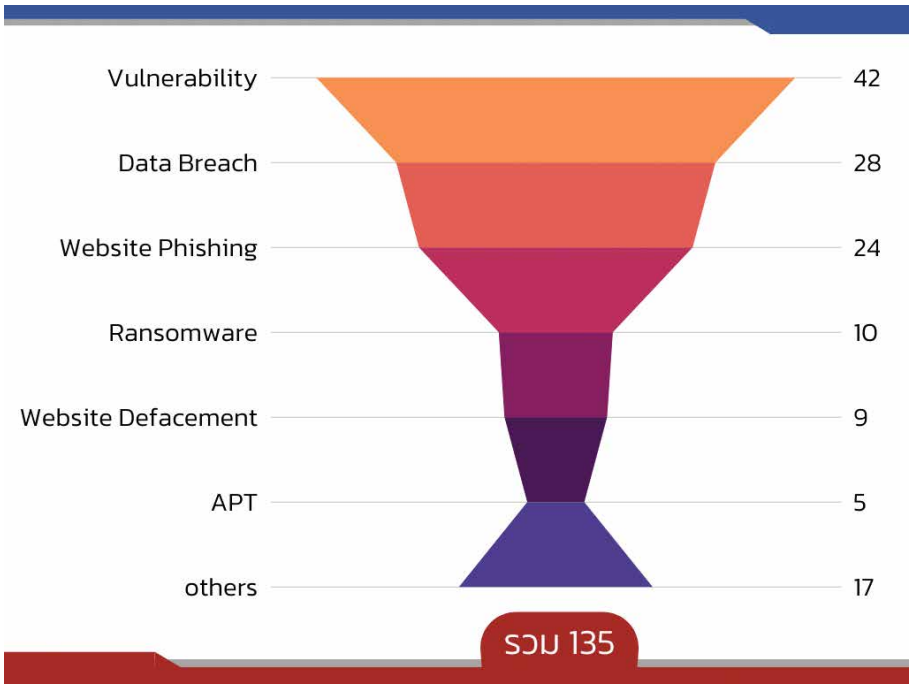
ในปี 2564 ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ National CERT ได้สนับสนุนการแก้ไขปัญหาเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น



การรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์การแพร่ระบาดของเชื้อไวรัสโคโรน่า 2019

จากสถานการณ์การแพร่ระบาดของเชื้อไวรัสโคโรน่า 2019 รัฐบาลได้นำเอาระบบเทคโนโลยีดิจิทัลเข้ามาช่วยแก้ไขปัญหาบริหารการจัดการวัคซีน และสนับสนุนระบบธุรกิจการท่องเที่ยวของประเทศ ได้แก่ แอปพลิเคชันหมอพร้อม โครงการภูเก็ตต้องชนะ เป็นต้น National CERT ซึ่งเป็นหน่วยงานสังกัด สกมช. ได้มีส่วนร่วมในการสนับสนุนกิจการเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในเรื่องดังกล่าว โดยเฉพาะการตรวจสอบช่องโหว่ เฝ้าระวัง และป้องกันภัยคุกคามที่อาจเกิดขึ้นกับระบบที่เกี่ยวข้อง เพื่อให้ประชาชนมีความเชื่อมั่นต่อการใช้งานระบบเทคโนโลยีสารสนเทศให้ประเทศไทยข้ามพ้นวิกฤตอันสืบเนื่องมาจากการแพร่ระบาดของเชื้อไวรัสโคโรน่า 2019

• ประเภทภัยคุกคามทางไซเบอร์ที่ NATIONAL CERT ดำเนินการและตรวจพบมากที่สุด ในปี 2564



บทวิเคราะห์สถานการณ์ที่สำคัญใน ปี 2564

Website Phishing

ผู้ไม่หวังดีสร้างหน้าเว็บไซต์ปลอมหรือเลียนแบบหน้า Login ของสถาบันการเงินหรือแพลตฟอร์มอีคอมเมิร์ซต่างประเทศ โดยการฝังไว้ภายในส่วนหนึ่งของเว็บไซต์หน่วยงานของรัฐและเอกชนในประเทศไทย เพื่อใช้ประกอบการหลอกลวง และได้มาซึ่งชื่อผู้ใช้งาน รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ จากนั้นจะนำข้อมูลที่ได้มาใช้ประโยชน์ในทางทุจริต

Data Breach

การติดตามปัญหาสถานการณ์การรั่วไหลของข้อมูล โดยเฉพาะข้อมูลที่ละเอียดอ่อนที่เป็นของคนไทยและชาวต่างประเทศจำนวนมาก ปัจจุบันพบว่ามีการประกาศเผยแพร่ หรือโฆษณาจำหน่ายข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาต การละเมิดข้อมูลเหล่านี้ เกิดจากผู้ไม่หวังดีโจมตีข้อมูลเว็บไซต์ของหน่วยงาน การขโมยข้อมูลที่สำคัญออกจากฐานข้อมูล ความหละหลวมของผู้ใช้งาน หรือการที่ผู้เกี่ยวข้องไม่สามารถดูแลเรื่องความปลอดภัยของข้อมูลได้ดีเพียงพอ เหล่านี้เป็นปัญหาสำคัญที่มีแนวโน้มตรวจพบมากขึ้น และจำเป็นต้องมีการเตรียมการรับมือกับปัญหาดังกล่าวมากขึ้น

Ransomware

ปัญหาเรื่องการโจมตีโดยซอฟต์แวร์เรียกค่าไถ่ พบว่ามีกลุ่มผู้ไม่หวังดีเลือกเป้าหมายที่เป็นองค์กรหรือบริษัทที่มีขนาดใหญ่มากกว่าเป้าหมายที่เป็นบุคคล เป็นไปได้ว่ากลุ่มดังกล่าวเชื่อว่าองค์กรหรือบริษัทจะมีศักยภาพทางการเงิน สามารถจ่ายเงินเพื่อแลกเปลี่ยนกับการปลดล็อกไฟล์เข้ารหัส หรือการไม่ถูกเปิดเผยข้อมูลความลับ

แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์

การสร้างหน้าเว็บไซต์ปลอมหรือเลียนแบบเพื่อหลอกลวง **(Website Phishing)** มีโอกาสพบบ่อยครั้ง และอาจมีรูปแบบที่แตกต่างไปขึ้นอยู่กับสถานการณ์และช่องทางการโจมตี เช่น ช่องทางอีเมลหรือคลาวด์ ก็อาจเกิดขึ้นได้ เหตุผลที่มีโอกาสเพิ่มสูงขึ้นเพราะเป็นการโจมตีที่ทำได้ง่ายและมีโอกาสประสบความสำเร็จสูง

การรั่วไหลของข้อมูล **(Data Breach)** อาจพบได้มากขึ้นและจะก่อให้เกิดความเสียหายแก่องค์กรสูงขึ้น เนื่องจากปีที่ผ่านมาองค์กรต่าง ๆ ถูกบีบให้ต้องปรับตัวและนำเทคโนโลยีมาใช้ หลายบริษัทต้องให้พนักงานทำงานจากบ้าน ขณะที่หน่วยงานหลายแห่งปรับงานสู่คลาวด์มากขึ้น ทำให้ขาดการดูแลเรื่องการรักษาความมั่นคงปลอดภัย และเป็นสาเหตุสำคัญให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล ทั้งนี้ มีการศึกษาว่าการโจมตีทางไซเบอร์ของอาชญากรมักใช้ประโยชน์จากข้อมูลส่วนบุคคลที่ได้รั่วไหลมาก่อนหน้านี้

กรณีการโจมตีโดยซอฟต์แวร์เรียกค่าไถ่ **(Ransomware)** ซึ่งสามารถสร้างความเสียหายอย่างรุนแรงให้กับหน่วยงานของรัฐและภาคเอกชนได้ด้วยการโจมตีเพียงครั้งเดียว ในอนาคตอาจพบการโจมตีที่รุนแรงและมีความถี่ที่สูงขึ้น ทั้งนี้เนื่องจากมีการให้บริการในลักษณะ Ransomware as a Service (RaaS) ซึ่งมีผลประโยชน์ต่างตอบแทนสูง การสืบสวนติดตามตัวผู้เกี่ยวข้องทำได้ยาก เป็นการกระทำในลักษณะกลุ่มองค์กรอาชญากรรม ผู้กระทำความผิดอาจอยู่คนละประเทศ มีลักษณะเป็นอาชญากรรมข้ามชาติ

1 ขับเคลื่อน

การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์

2 จัดทำ

การจัดทำกฎหมายลำดับรอง ประกาศ ระเบียบที่เกี่ยวข้อง

3 ส่งเสริม

ส่งเสริมความร่วมมือกับหน่วยงานองค์กรทั้งภายในประเทศและระหว่างประเทศ

4 ตอบสนอง

เฝ้าระวังตอบโต้ภัยคุกคามทางไซเบอร์

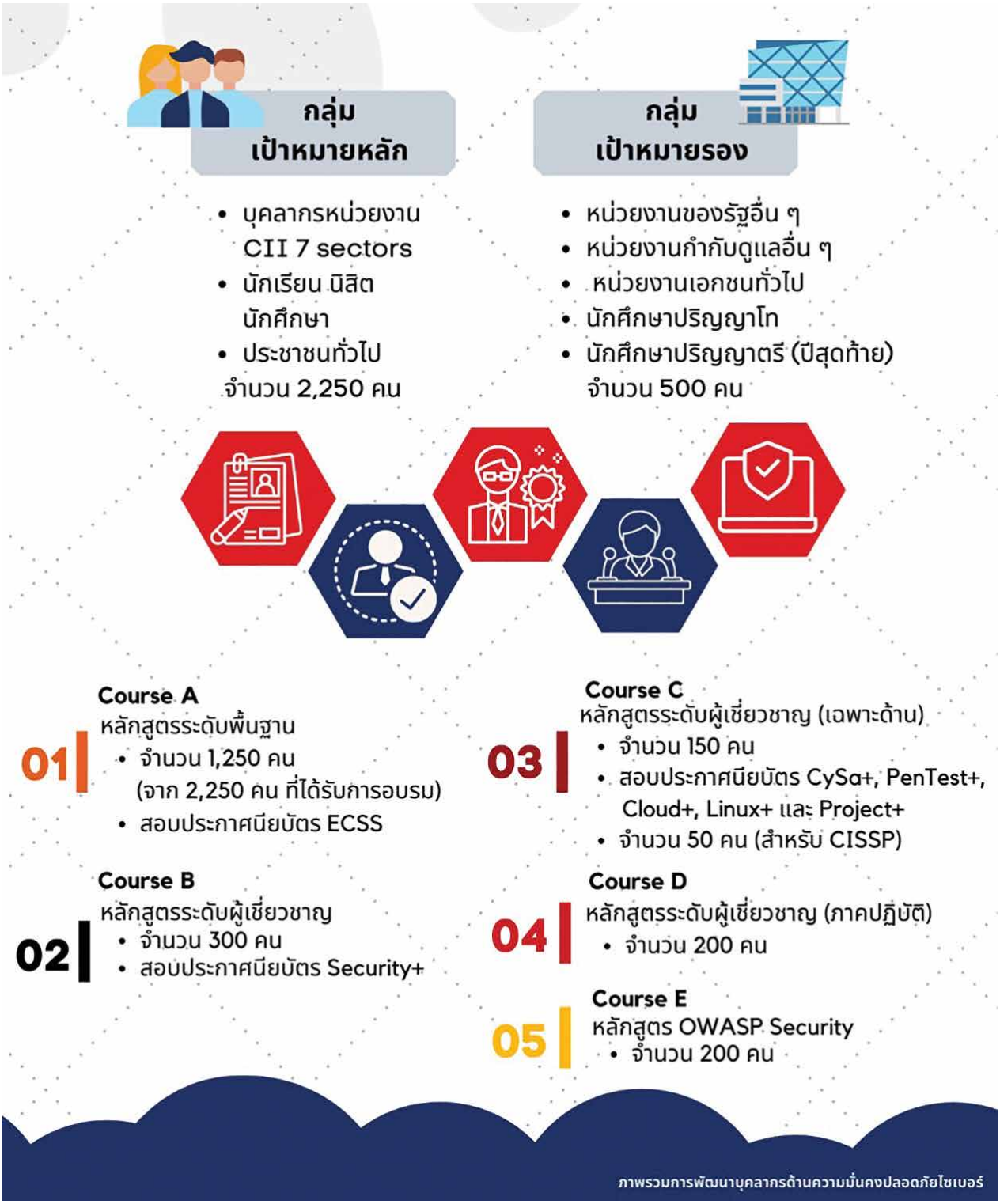
5 พัฒนา

การพัฒนาบุคลากรหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ตลอดจนสร้างการตระหนักรู้

6 ยกระดับ

การยกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ

โครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 1
การอบรมเชิงปฏิบัติการหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์



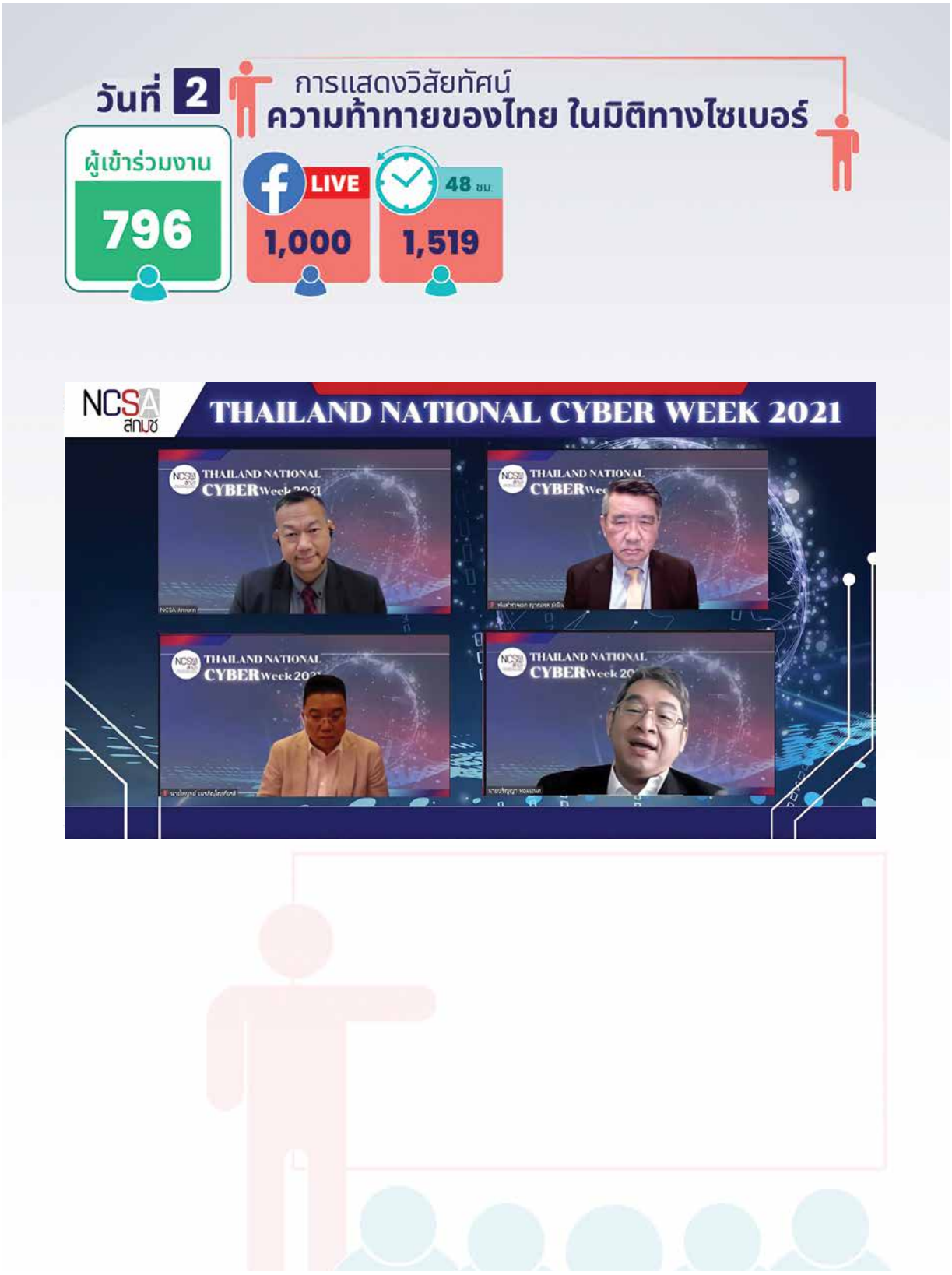
ภาพรวมการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

การอบรมเชิงปฏิบัติการหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์

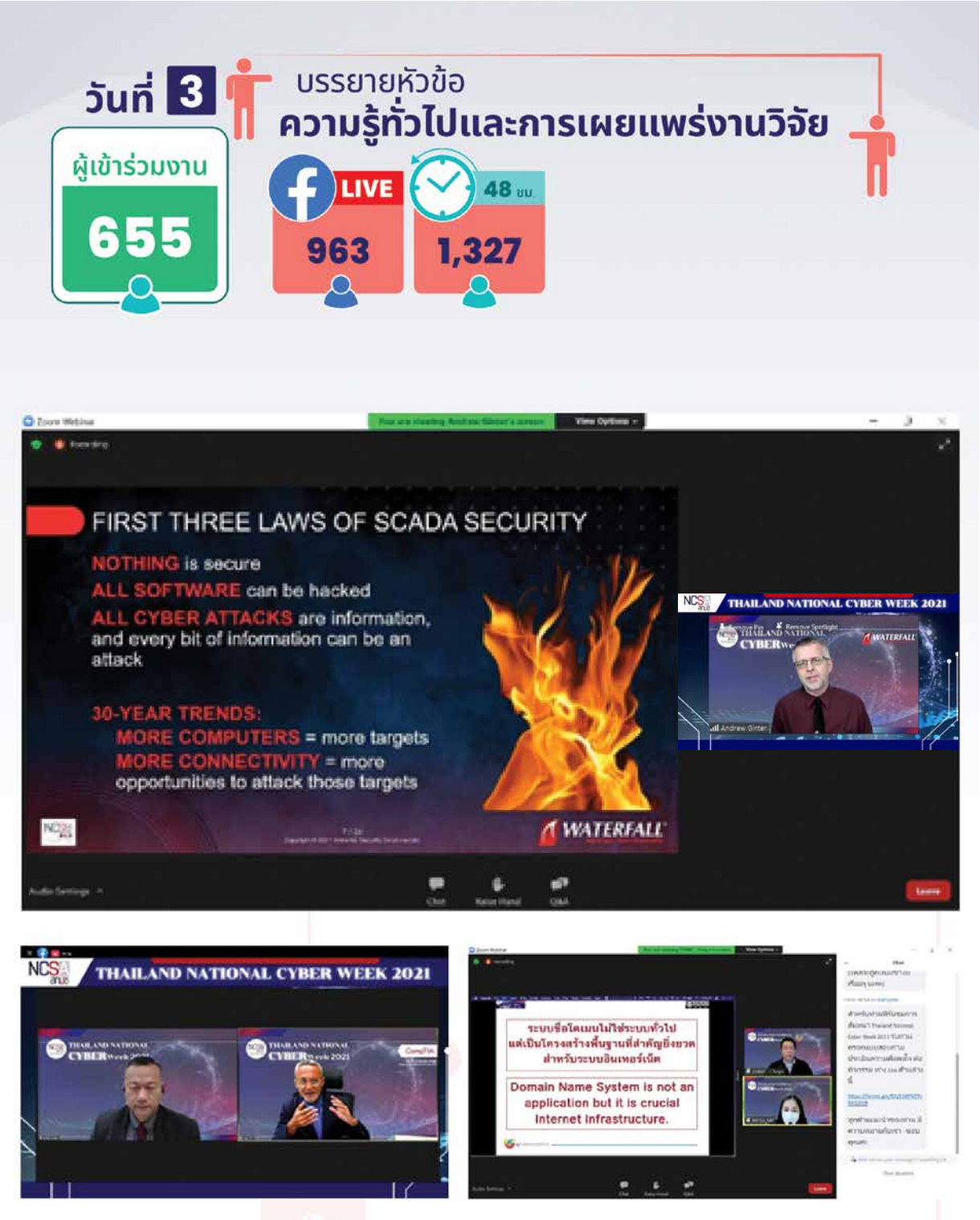
ภาพรวมการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

งานสัมมนา Thailand National Cyber Week 2021

งานสัมมนา Thailand National Cyber Week 2021



งานสัมมนา Thailand National Cyber Week 2021



NCSA Cyber Clinic 2021-2022

NCSA Cyber Clinic 2021-2022

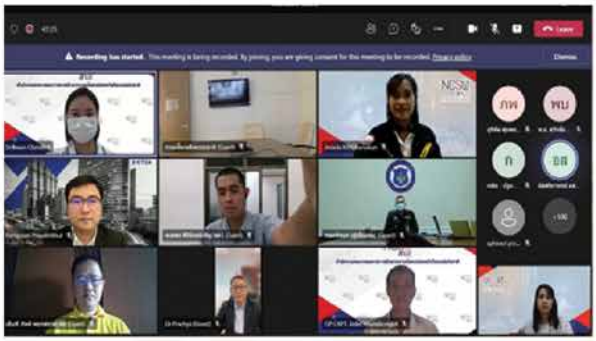
ครั้งที่ 2

แนวทางการแต่งตั้ง/ทบทวนผู้รับผิดชอบ ตามนโยบายการบริหารจัดการ (กำกับ) /ทบทวนบัญชีทรัพย์สิน ตามกรอบมาตรฐาน (การจัดการทรัพย์สิน)/การทำบัญชีทรัพย์สินสารสนเทศ

ผู้เข้าร่วมประชุม 98

ครั้งที่ 3

แนวทางการจัดทำ/ทบทวนการบริหารความเสี่ยงฯ ตามนโยบายการบริหารจัดการ แนวทางการประเมินความเสี่ยงด้านไซเบอร์ตามประมวลแนวทางปฏิบัติ (การประเมินความเสี่ยง) แนวทางการจัดทำ/ทบทวนนโยบายและแนวปฏิบัติตามนโยบายการบริหารจัดการ (นโยบายและแนวปฏิบัติ)



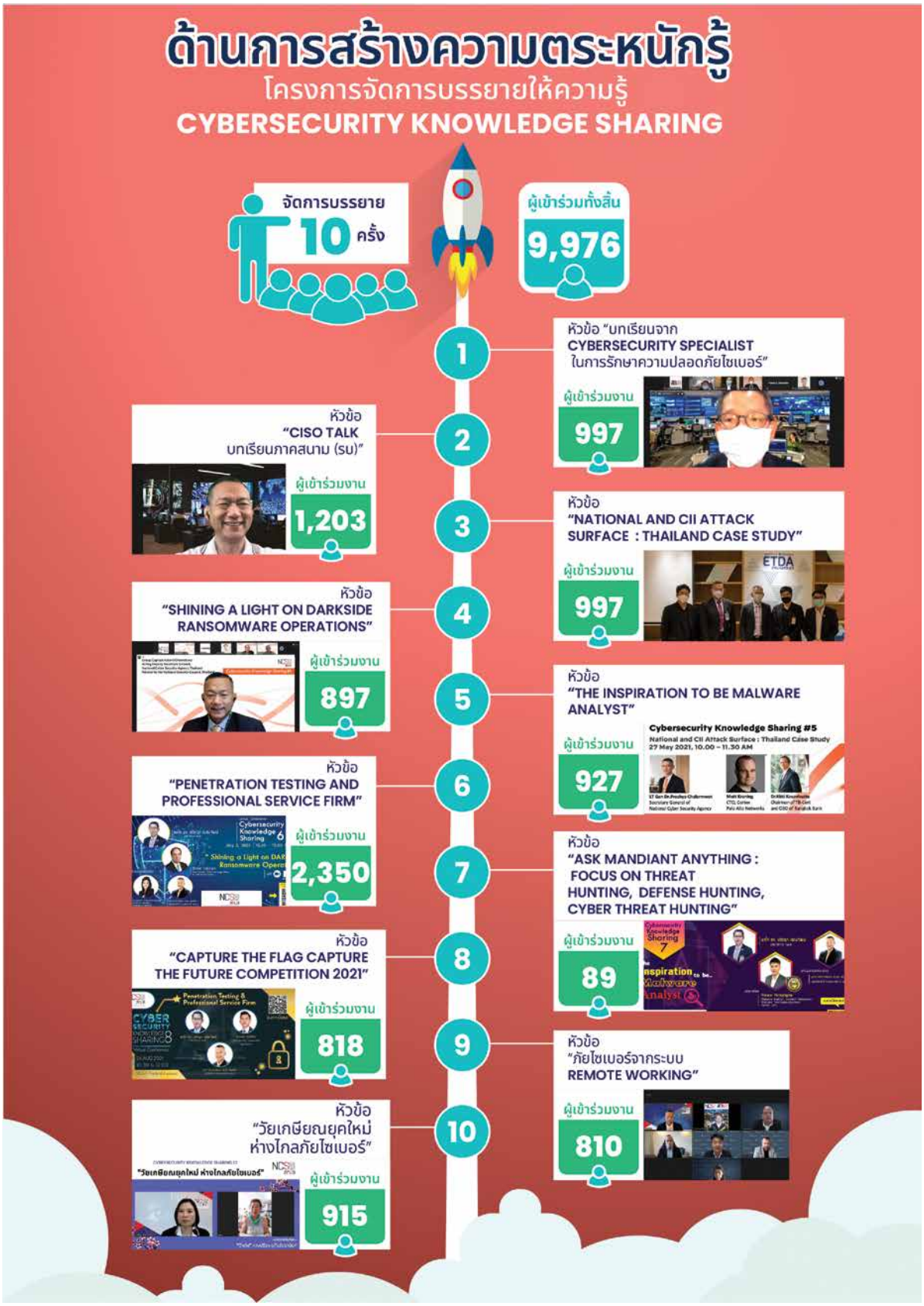
ผู้เข้าร่วมประชุม 111

APT Expert Mission in 2021

ด้านการสร้างความตระหนักรู้

การบรรยาย/เสวนาให้ความรู้

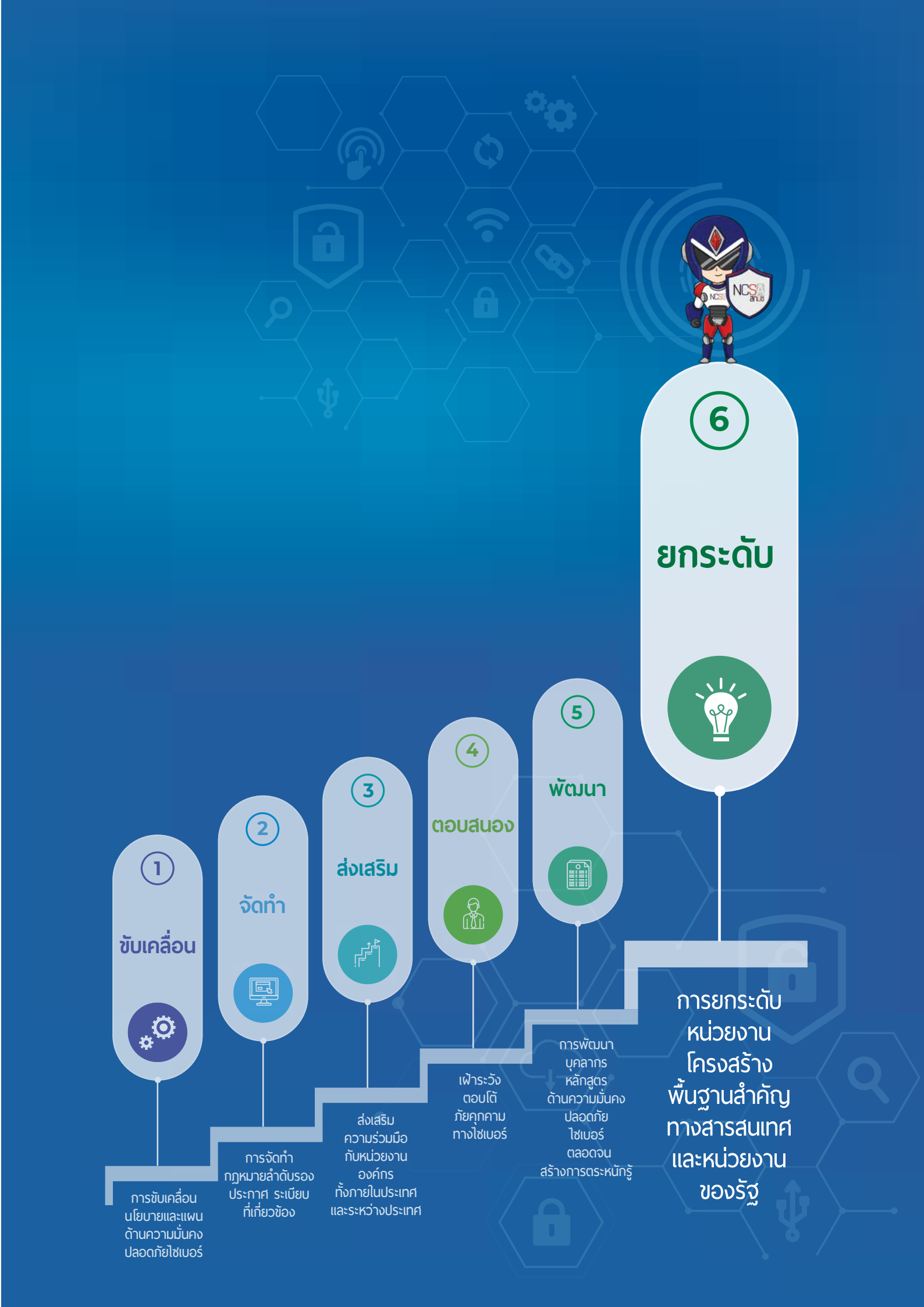
- **Cybersecurity Knowledge Sharing**



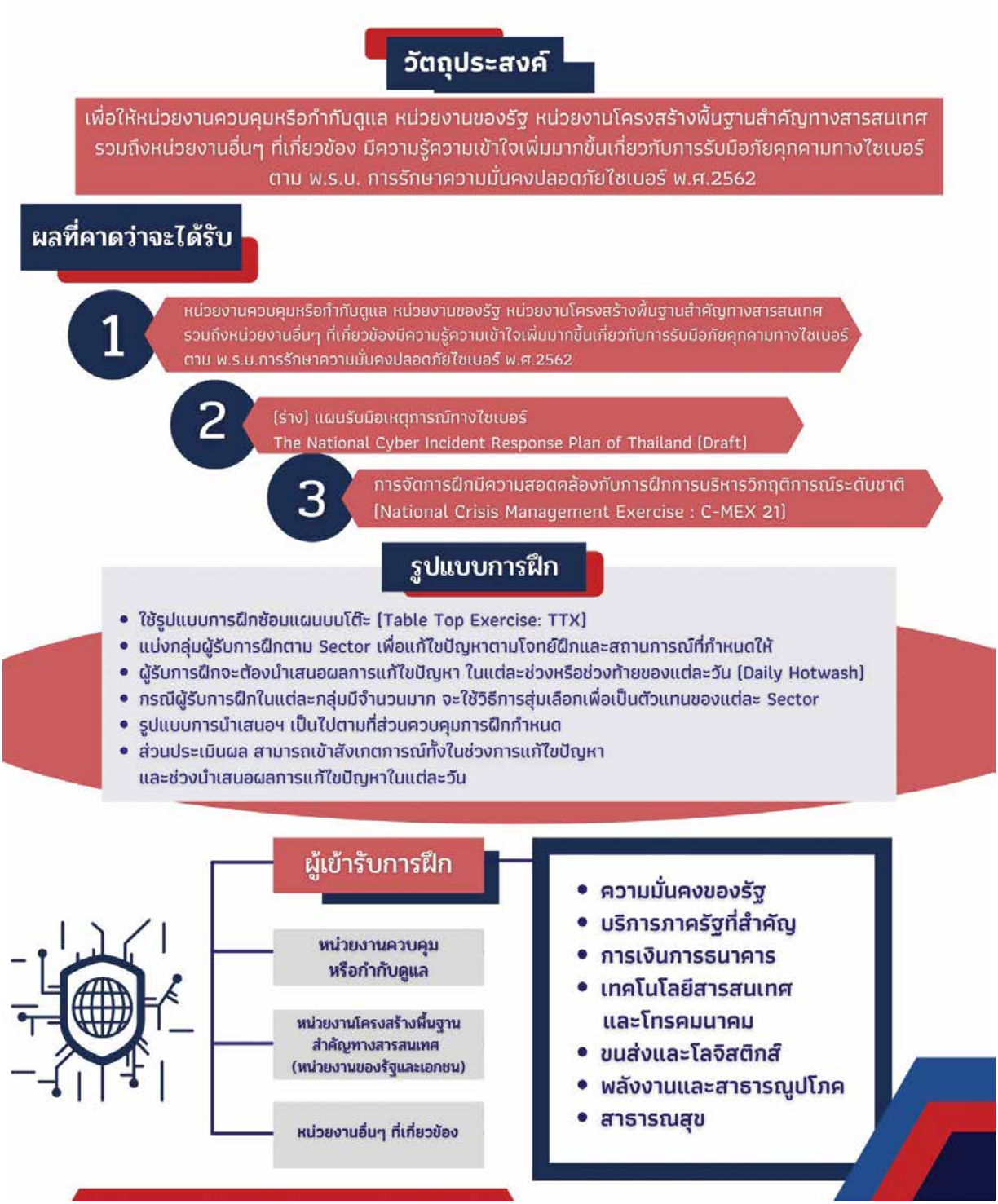
การจัดการแข่งขันทักษะทางไซเบอร์

- **Thailand Cyber Top Talent 2021**

- **Cyber SEA Game 2021**


1
ขับเคลื่อน
การขับเคลื่อน
นโยบายและแผน
ด้านความมั่นคง
ปลอดภัยไซเบอร์
2
จัดทำ
การจัดทำ
กฎหมายลำดับรอง
ประกาศ ระเบียบ
ที่เกี่ยวข้อง
3
ส่งเสริม
ส่งเสริม
ความร่วมมือ
กับหน่วยงาน
องค์กร
ทั้งภายในประเทศ
และระหว่างประเทศ
4
ตอบสนอง
เฝ้าระวัง
ตอบโต้
ภัยคุกคาม
ทางไซเบอร์
5
พัฒนา
การพัฒนา
บุคลากร
หลักสูตร
ด้านความมั่นคง
ปลอดภัย
ไซเบอร์
ตลอดจน
สร้างการตระหนักรู้
6
ยกระดับ
การยกระดับ
หน่วยงาน
โครงสร้าง
พื้นฐานสำคัญ
ทางสารสนเทศ
และหน่วยงาน
ของรัฐ

การฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



การฝึก Thailand's National Cyber Exercise

หน่วยงานที่เข้าร่วม

จำนวน 66 หน่วยงาน
คิดเป็น 23,823.5 ชั่วโมงทำงาน
ผู้เข้าร่วม 458 คน

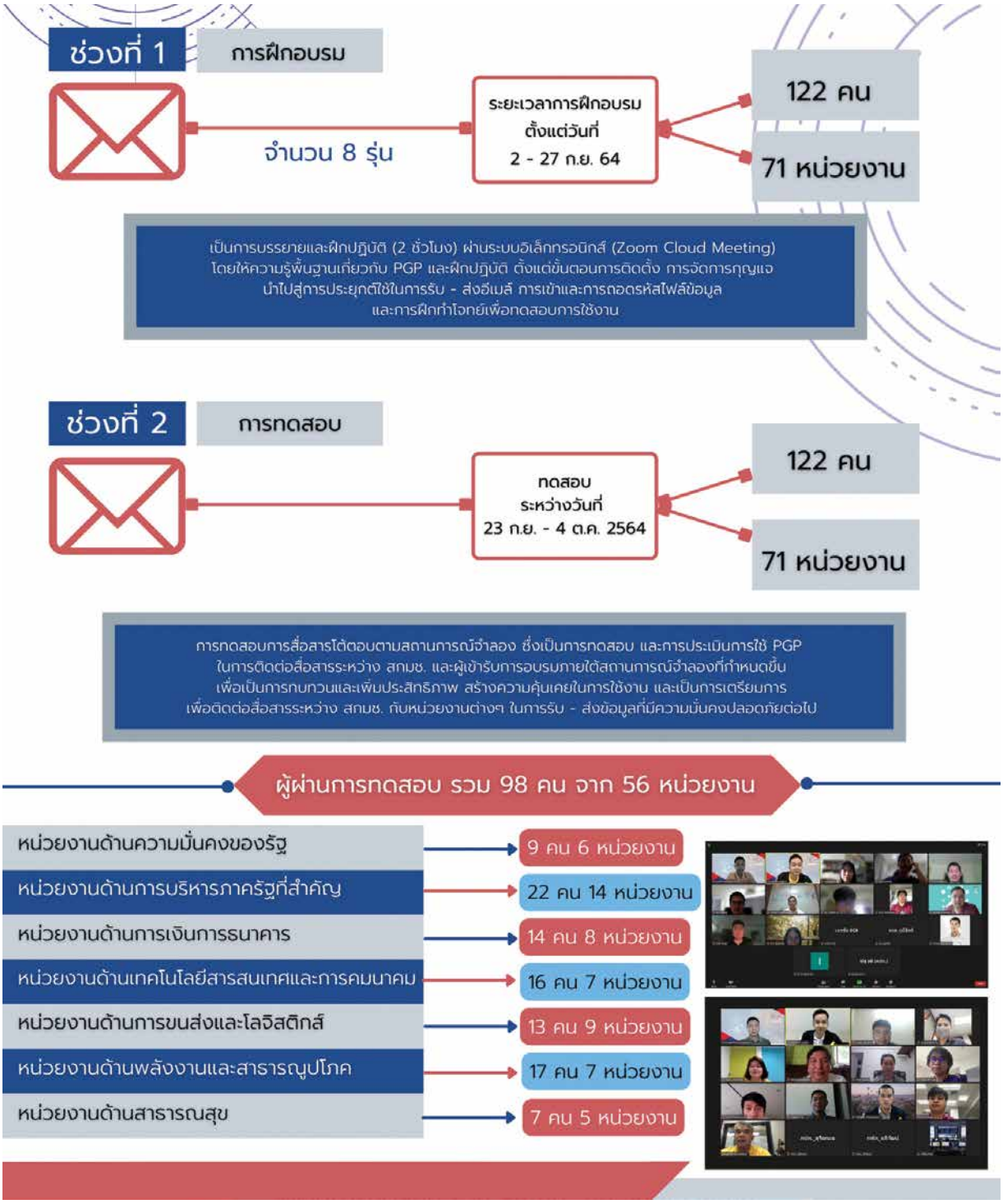
การฝึก Thailand's National Cyber Exercise







การอบรมเชิงปฏิบัติการในการใช้อีเมลสื่อสารด้วย Pretty Good Privacy (PGP)



จัดการอบรม

- **World Class Cyber Security Practices โดย MITRE/CISA/SEI**

- **การอบรม INCIDENT RESPONSE FUNDAMENTAL**

รายงานการเงิน

สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน) ถึงวันที่ 30 กันยายน 2564

รายงานของผู้สอบบัญชีรับอนุญาต

เสนอ คณะกรรมการบริหาร
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)

ความเห็น

ข้าพเจ้าได้ตรวจสอบรายงานการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน) ซึ่งประกอบด้วยงบแสดงฐานะการเงิน ณ วันที่ 30 กันยายน 2564 งบแสดงผลการดำเนินงานทางการเงิน และงบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน) ถึงวันที่ 30 กันยายน 2564 และหมายเหตุประกอบงบการเงิน รวมถึงหมายเหตุสรุปนโยบายการบัญชีที่สำคัญ

ข้าพเจ้าเห็นว่า รายงานการเงินข้างต้นนี้แสดงฐานะการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน) ณ วันที่ 30 กันยายน 2564 และผลการดำเนินงาน สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน) ถึงวันที่ 30 กันยายน 2564 โดยถูกต้องตามที่ควรในสาระสำคัญตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด

เกณฑ์ในการแสดงความเห็น

ข้าพเจ้าได้ปฏิบัติงานตรวจสอบเป็นไปตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชี ความรับผิดชอบของข้าพเจ้าได้กล่าวไว้ในวรรคความรับผิดชอบของผู้สอบบัญชีต่อการตรวจสอบรายงานการเงินในรายงานของข้าพเจ้า ข้าพเจ้ามีความเป็นอิสระจากสำนักงานตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินที่กำหนดโดยคณะกรรมการตรวจเงินแผ่นดินตามข้อกำหนดจรรยาบรรณของผู้ประกอบวิชาชีพบัญชีที่กำหนดโดยสภาวิชาชีพบัญชีในส่วนที่เกี่ยวข้องกับการตรวจสอบรายงานการเงิน และข้าพเจ้าได้ปฏิบัติตามความรับผิดชอบด้านจรรยาบรรณอื่นๆ ซึ่งเป็นไปตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและข้อกำหนดจรรยาบรรณเหล่านี้ ข้าพเจ้าเชื่อว่าหลักฐานการสอบบัญชีที่ข้าพเจ้าได้รับเพียงพอและเหมาะสม เพื่อใช้เป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า

ข้อมูลอื่น

ผู้บริหารเป็นผู้รับผิดชอบต่อข้อมูลอื่น ข้อมูลอื่นประกอบด้วยข้อมูลซึ่งรวมอยู่ในรายงานประจำปี แต่ไม่รวมถึงรายงานการเงินและรายงานของผู้สอบบัญชีที่อยู่ในรายงานประจำปีนั้น ซึ่งคาดว่ารายงานประจำปีจะถูกจัดเตรียมให้ข้าพเจ้าภายหลังวันที่ในรายงานของผู้สอบบัญชีนี้

ความเห็นของข้าพเจ้าต่อรายงานการเงินไม่ครอบคลุมถึงข้อมูลอื่นและข้าพเจ้าไม่ได้ให้ความเชื่อมั่นต่อข้อมูลอื่น

ความรับผิดชอบของข้าพเจ้าที่เกี่ยวเนื่องกับการตรวจสอบรายงานการเงินคือ การอ่านและพิจารณาว่าข้อมูลอื่นมีความขัดแย้งที่มีสาระสำคัญกับรายงานการเงินหรือกับความรู้ที่ได้รับจากการตรวจสอบของข้าพเจ้า หรือปรากฏว่า ข้อมูลอื่นมีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่

เมื่อข้าพเจ้าได้อ่านรายงานประจำปี หากข้าพเจ้าสรุปได้ว่ามีการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ ข้าพเจ้าต้องสื่อสารเรื่องดังกล่าวกับผู้มีหน้าที่ในการกำกับดูแล เพื่อให้ผู้มีหน้าที่ในการกำกับดูแลดำเนินการแก้ไขข้อมูลที่แสดงขัดต่อข้อเท็จจริง

ความรับผิดชอบของผู้บริหารและผู้มีหน้าที่ในการกำกับดูแลต่อรายงานการเงิน

ผู้บริหารมีหน้าที่รับผิดชอบในการจัดทำและนำเสนอรายงานการเงินเหล่านี้โดยถูกต้องตามที่ควรตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังกำหนด และรับผิดชอบเกี่ยวกับการควบคุมภายในที่ผู้บริหารพิจารณาว่าจำเป็นเพื่อให้สามารถจัดทำรายงานการเงินที่ปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด

ในการจัดทำรายงานการเงิน ผู้บริหารรับผิดชอบในการประเมินความสามารถของสำนักงานในการดำเนินงานต่อเนื่อง เปิดเผยเรื่องที่เกี่ยวกับการดำเนินงานต่อเนื่องตามความเหมาะสม และการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่อง เว้นแต่มีข้อกำหนดในกฎหมายหรือเป็นนโยบายรัฐบาลที่จะเลิกสถานักงานหรือหยุดดำเนินงานหรือไม่สามารถดำเนินงานต่อเนื่องต่อไปได้

ผู้มีหน้าที่ในการกำกับดูแลมีหน้าที่ในการกำกับดูแลกระบวนการในการจัดทำรายงานทางการเงินของสำนักงาน

ความรับผิดชอบของผู้สอบบัญชีต่อการตรวจสอบรายงานการเงิน

การตรวจสอบของข้าพเจ้ามีวัตถุประสงค์เพื่อให้ได้ความเชื่อมั่นอย่างสมเหตุสมผลว่ารายงานการเงินโดยรวมปราศจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญหรือไม่ ไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด และเสนอรายงานของผู้สอบบัญชีซึ่งรวมความเห็นของข้าพเจ้าอยู่ด้วย ความเชื่อมั่นอย่างสมเหตุสมผลคือความเชื่อมั่นในระดับสูงแต่ไม่ได้เป็นการรับประกันว่าการปฏิบัติงานตรวจสอบตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชีจะสามารถตรวจพบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญที่มีอยู่ได้เสมอไป ข้อมูลที่ขัดต่อข้อเท็จจริงอาจเกิดจากการทุจริตหรือข้อผิดพลาดและถือว่ามีสาระสำคัญเมื่อคาดการณ์ได้อย่างสมเหตุสมผลว่ารายการที่ขัดต่อข้อเท็จจริงแต่ละรายการหรือทุกรายการรวมกันจะมีผลต่อการตัดสินใจทางเศรษฐกิจของผู้ใช้รายงานการเงินจากการใช้รายงานการเงินเหล่านี้

ในการตรวจสอบของข้าพเจ้าตามหลักเกณฑ์มาตรฐานเกี่ยวกับการตรวจเงินแผ่นดินและมาตรฐานการสอบบัญชี ข้าพเจ้าได้ใช้ดุลยพินิจและการสังเกตและสงสัยเยี่ยงผู้ประกอบวิชาชีพตลอดการตรวจสอบ การปฏิบัติงานของข้าพเจ้ารวมถึง

- ระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญในงบการเงินไม่ว่าจะเกิดจากการทุจริตหรือข้อผิดพลาด ออกแบบและปฏิบัติงานตามวิธีการตรวจสอบเพื่อตอบสนองต่อความเสี่ยงเหล่านั้น และได้หลักฐานการสอบบัญชีที่เพียงพอและเหมาะสมเพื่อเป็นเกณฑ์ในการแสดงความเห็นของข้าพเจ้า ความเสี่ยงที่ไม่พบข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญซึ่งเป็นผลมาจากการทุจริตจะสูงกว่าความเสี่ยงที่เกิดจากข้อผิดพลาด เนื่องจากการทุจริตอาจเกี่ยวกับการสมรู้ร่วมคิด การปลอมแปลงเอกสารหลักฐาน การตั้งใจละเว้นการแสดงข้อมูล การแสดงข้อมูลที่ไม่ตรงตามข้อเท็จจริงหรือการแทรกแซงการควบคุมภายใน
- ทำความเข้าใจในระบบการควบคุมภายในที่เกี่ยวข้องกับการตรวจสอบ เพื่อออกแบบวิธีการตรวจสอบที่เหมาะสมกับสถานการณ์ แต่ไม่ใช่เพื่อวัตถุประสงค์ในการแสดงความเห็นต่อความมีประสิทธิผลของการควบคุมภายในของสำนักงาน

- ประเมินความเหมาะสมของนโยบายการบัญชีที่ผู้บริหารใช้และความสมเหตุสมผลของประมาณการทางบัญชีและการเปิดเผยข้อมูลที่เกี่ยวข้องซึ่งจัดทำขึ้นโดยผู้บริหาร

- สรุปเกี่ยวกับความเหมาะสมของการใช้เกณฑ์การบัญชีสำหรับการดำเนินงานต่อเนื่องของผู้บริหารและจากหลักฐานการสอบบัญชีที่ได้รับ สรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญที่เกี่ยวกับเหตุการณ์ หรือสถานการณ์ที่อาจเป็นเหตุให้เกิดข้อสงสัยอย่างมีนัยสำคัญต่อความสามารถของสำนักงานในการดำเนินงานต่อเนื่องหรือไม่ ถ้าข้าพเจ้าได้ข้อสรุปว่ามีความไม่แน่นอนที่มีสาระสำคัญ ข้าพเจ้าต้องกล่าวไว้ในรายงานของผู้สอบบัญชีของข้าพเจ้าโดยให้ข้อสังเกตถึงการเปิดเผยข้อมูลในรายงานการเงินที่เกี่ยวข้อง หรือถ้าการเปิดเผยข้อมูลดังกล่าวไม่เพียงพอ ความเห็นของข้าพเจ้าจะเปลี่ยนแปลงไป ข้อสรุปของข้าพเจ้าขึ้นอยู่กับหลักฐานการสอบบัญชีที่ได้รับจนถึงวันที่ในรายงานของผู้สอบบัญชีของข้าพเจ้า อย่างไรก็ตามเหตุการณ์หรือสถานการณ์ในอนาคตอาจเป็นเหตุให้หน่วยงานต้องหยุดการดำเนินงานต่อเนื่อง

- ประเมินการนำเสนอโครงสร้างและเนื้อหาของรายงานการเงินโดยรวม รวมถึงการเปิดเผยข้อมูลว่ารายงานการเงินแสดงรายการและเหตุการณ์ในรูปแบบที่ทำให้มีการนำเสนอข้อมูลโดยถูกต้องตามที่ควรหรือไม่

ข้าพเจ้าได้สื่อสารกับผู้บริหารและผู้มีหน้าที่ในการกำกับดูแลในเรื่องต่างๆ ที่สำคัญ ซึ่งรวมถึงขอบเขตและช่วงเวลาของการตรวจสอบตามที่ได้วางแผนไว้ ประเด็นที่มีนัยสำคัญที่พบจากการตรวจสอบรวมถึงข้อบกพร่องที่มีนัยสำคัญในระบบการควบคุมภายในหากข้าพเจ้าได้พบในระหว่างการตรวจสอบของข้าพเจ้า

ผู้สอบบัญชีที่รับผิดชอบงานสอบบัญชีและนำเสนอรายงานฉบับนี้คือ นายสุวัฒน์ มณีกนกสกุล

(นายสุวัฒน์ มณีกนกสกุล)
ผู้สอบบัญชีรับอนุญาต ทะเบียนเลขที่ 8134

บริษัท สอบบัญชีธรรมนิติ จำกัด
กรุงเทพมหานคร
วันที่ 11 มกราคม 2565

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
งบแสดงฐานะการเงิน
ณ วันที่ 30 กันยายน 2564

	หมายเหตุ	บาท 2564
สินทรัพย์		
สินทรัพย์หมุนเวียน		
เงินสดและรายการเทียบเท่าเงินสด	5	28,354,116.76
ลูกหนี้ระยะสั้น	6	114,871.08
วัสดุคงเหลือ		185,584.80
รวมสินทรัพย์หมุนเวียน		28,654,572.64
สินทรัพย์ไม่หมุนเวียน		
ที่ดิน อาคารและอุปกรณ์	7	1,371,436.30
รวมสินทรัพย์ไม่หมุนเวียน		1,371,436.30
รวมสินทรัพย์		30,026,008.94
หนี้สินและสินทรัพย์สุทธิ/ส่วนทุน		
หนี้สินหมุนเวียน		
เจ้าหนี้ระยะสั้น	8	189,545.66
เงินรับฝากระยะสั้น	9	401,250.00
หนี้สินหมุนเวียนอื่น	10	85,411.81
รวมหนี้สินหมุนเวียน		676,207.47
รวมหนี้สิน		676,207.47
<u>สินทรัพย์สุทธิ/ส่วนทุน</u>		
ทุน		-
รายได้สูงกว่าค่าใช้จ่ายสะสม		29,349,801.47
รวมสินทรัพย์สุทธิ/ส่วนทุน		29,349,801.47
รวมหนี้สินและสินทรัพย์สุทธิ/ส่วนทุน		30,026,008.94

พลเอก

(นางมัตติกา จงพิริยะอนันต์)
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

(ปรัชญา เฉลิมวัฒน์)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
งบแสดงผลการดำเนินงานทางการเงิน
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

	หมายเหตุ	บาท สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน) ถึงวันที่ 30 กันยายน 2564
รายได้		
รายได้จากงบประมาณ (เงินอุดหนุน)	12	41,591,500.00
รวมรายได้		41,591,500.00
ค่าใช้จ่าย		
ค่าใช้จ่ายบุคลากร	13	2,375,000.00
ค่าตอบแทน	14	5,758,875.32
ค่าใช้สอย	15	3,146,955.91
ค่าวัสดุ	16	487,896.94
ค่าสาธารณูปโภค	17	355,871.36
ค่าเสื่อมราคา	18	117,099.00
รวมค่าใช้จ่าย		12,241,698.53
รายได้สูงกว่าค่าใช้จ่ายสุทธิ		29,349,801.47

(นางมัตติกา จงพิริยะอนันต์)
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

พลเอก
(ปรัชญา เฉลิมวัฒน์)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
งบแสดงการเปลี่ยนแปลงสินทรัพย์สุทธิ/ส่วนทุน
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

	บาท		
	ทุน	รายได้สูงกว่าค่าใช้จ่ายสะสม	รวมสินทรัพย์สุทธิ/ส่วนทุน
ยอดคงเหลือ ณ วันที่ 1 มกราคม 2564	-	-	-
รายได้สูงกว่าค่าใช้จ่ายสำหรับปี	-	29,349,801.47	29,349,801.47
ยอดคงเหลือ ณ วันที่ 30 กันยายน 2564	-	29,349,801.47	29,349,801.47

(นางมัตติกา จงพิริยะอนันต์)
ผู้อำนวยการสำนักการเงินและกลยุทธ์องค์กร

พลเอก
(ปรัชญา เฉลิมวัฒน์)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
รายงานฐานะเงินงบประมาณรายจ่ายปีปัจจุบัน
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

รายงานฐานะเงินงบประมาณรายจ่ายปี 2564

(หน่วย:บาท)

รายการ	งบสุทธิ	ใบสั่งซื้อ/สัญญา	เบิกจ่าย	คงเหลือ
แผนงบประมาณ				
งบอุดหนุน				
ค่าใช้จ่ายบุคลากร	2,375,000.00	-	2,375,000.00	-
ค่าใช้จ่ายดำเนินงาน	10,412,014.42	550,191.63	9,860,926.75	896.04
ค่าครุภัณฑ์และสิ่งก่อสร้าง	19,863,243.58	18,374,708.28	1,488,535.30	-
ค่าใช้จ่ายดำเนินงานตาม				
แผนโครงการ	8,941,242.00	8,941,242.00	-	-
รวม	41,591,500.00	27,866,141.91	13,724,462.05	896.04

หมายเหตุประกอบงบการเงินเป็นส่วนหนึ่งของรายงานการเงินนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
หมายเหตุประกอบงบการเงิน
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

หมายเหตุที่ 1 ข้อมูลทั่วไป

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม 2562 แต่ทางสำนักงานได้มีการเริ่มดำเนินงานในวันที่ 1 มกราคม 2564 เมื่อทางสำนักงานได้มีการดำเนินการครบตามองค์ประกอบในการจัดตั้งสำนักงาน โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับองค์กรภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นองค์กรรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

สถานที่ตั้งหลักสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210 สกมช. “เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพพร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ” ทำหน้าที่กำหนดนโยบาย ระเบียบ มาตรการ มาตรฐานขั้นต่ำ แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับองค์กรภาครัฐและภาคเอกชนที่เป็นองค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการเฝ้าระวัง ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบและสร้างความเดือดร้อนต่อประชาชน ตลอดจนความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ โดยประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์เมื่อมีเหตุภัยคุกคามเกิดขึ้นอย่างมีนัยสำคัญให้องค์กรโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม และรายงานต่อองค์กรและองค์กรควบคุมหรือกำกับดูแลโดยเร็ว และสำหรับองค์กรที่เกี่ยวข้องหากพบการโจมตีทางไซเบอร์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

หมายเหตุที่ 2 เกณฑ์การจัดทำรายงานการเงิน

รายงานการเงินของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน) ฉบับนี้จัดทำขึ้นตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ.2561 รายการที่ปรากฏในรายงานการเงินฉบับนี้เป็นไปตามมาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่กระทรวงการคลังประกาศใช้ ซึ่งรวมถึงหลักการและนโยบายการบัญชีภาครัฐ มาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐ และหลักเกณฑ์และวิธีการจัดทำรายงานการเงินประจำปี ตามหนังสือกระทรวงการคลัง ที่ กค 0410.2/ว 479 ลงวันที่ 2 ตุลาคม 2563

หมายเหตุที่ 3 มาตรฐานและนโยบายการบัญชีภาครัฐฉบับใหม่

ในระหว่างปีปัจจุบัน กระทรวงการคลังได้ประกาศใช้มาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐฉบับใหม่ และฉบับปรับปรุงใหม่ ดังนี้

มาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐที่มีผลบังคับใช้สำหรับรอบระยะเวลาบัญชีปัจจุบันที่เริ่มในหรือหลังวันที่ 1 ตุลาคม 2563

- มาตรฐานการบัญชีภาครัฐ ฉบับที่ 9 เรื่อง รายได้จากรายการแลกเปลี่ยน

มาตรฐานการบัญชีภาครัฐและนโยบายการบัญชีภาครัฐฉบับใหม่ข้างต้นไม่มีผลกระทบอย่างเป็นสาระสำคัญต่อรายงานการเงินในงวดปัจจุบัน

หมายเหตุที่ 4 สรุปนโยบายการบัญชีที่สำคัญ

4.1 เงินสดและรายการเทียบเท่าเงินสด

เงินสด หมายถึง เงินสดในมือ เช็ค ดราฟต์และธนาณัติ หน่วยงานจะรับรู้เงินสดและเงินฝากธนาคารในราคาตามมูลค่าที่ตราไว้ และแสดงรายการดังกล่าวไว้ในเงินสดและรายการเทียบเท่าเงินสดในงบแสดงฐานะการเงิน

รายการเทียบเท่าเงินสด หมายถึง เงินลงทุนระยะสั้นที่มีสภาพคล่องสูงซึ่งพร้อมที่จะเปลี่ยนเป็นเงินสดในจำนวนเงินที่เท่ากันหรือใกล้เคียงกับมูลค่าเดิม ซึ่งความแตกต่างในมูลค่าดังกล่าวไม่มีนัยสำคัญ

4.2 ลูกหนี้ระยะสั้น

ลูกหนี้จากการให้บริการ หมายถึง จำนวนเงินที่หน่วยงานมีสิทธิได้รับชำระจากบุคคลภายนอกหรือหน่วยงานอื่น ซึ่งเกิดจากการให้บริการอันเป็นส่วนหนึ่งของการดำเนินงานปกติของหน่วยงาน หน่วยงานจะรับรู้ลูกหนี้จากการให้บริการตามมูลค่าสุทธิที่จะได้รับโดยมีการประมาณการค่าเผื่อหนี้สงสัยจะสูญสำหรับลูกหนี้ส่วนที่คาดว่าจะไม่สามารถเรียกเก็บเงินได้

ค่าเผื่อหนี้สงสัยจะสูญ ประมาณขึ้นจากการพิจารณาประสบการณ์ที่ผ่านมาเกี่ยวกับจำนวนลูกหนี้ที่เก็บเงินไม่ได้ และสถานะทางการเงินของลูกหนี้ในปัจจุบัน โดยคำนวณตามอัตราร้อยละของยอดลูกหนี้คงค้าง ณ วันสิ้นงวดแยกตามกลุ่มของอายุลูกหนี้ที่ค้างชำระ/ ของยอดลูกหนี้คงค้างทั้งหมด

ลูกหนี้เงินยืม หมายถึง ลูกหนี้ภายในหน่วยงานกรณีให้ข้าราชการ พนักงาน หรือเจ้าหน้าที่ยืมเงินไปใช้จ่ายในการปฏิบัติงานโดยไม่มีดอกเบี้ย เช่น ลูกหนี้เงินงบประมาณ ลูกหนี้เงินนอกงบประมาณแสดงตามมูลค่าที่จะได้รับโดยไม่ตั้งบัญชีค่าเผื่อหนี้สงสัยจะสูญ

4.3 วัสดุคงเหลือ

วัสดุคงเหลือ หมายถึง สินทรัพย์ที่หน่วยงานมีไว้เพื่อใช้ในการดำเนินงานตามปกติ โดยทั่วไปมีมูลค่าไม่สูง และไม่มีลักษณะคงทนถาวร หน่วยงานวัดมูลค่าวัสดคงเหลือในราคาทุนตามวิธีเข้าก่อนออกก่อน

4.4 อาคาร และอุปกรณ์

หน่วยงานแสดงรายการอาคารและอุปกรณ์ตามราคาทุนหักค่าเสื่อมราคาสะสม และค่าเผื่อการด้อยค่า (ถ้ามี)

หน่วยงานรับรู้รายการอุปกรณ์ เฉพาะรายการที่มีมูลค่าขั้นต่ำต่อหน่วยหรือต่อชุดตั้งแต่ 5,000 บาท ขึ้นไป

ราคาทุนรวมต้นทุนทางตรงที่เกี่ยวข้องกับการจัดหาสินทรัพย์ เพื่อให้สินทรัพย์นั้นอยู่ในสภาพและสถานที่ที่พร้อมจะใช้งานได้ตามความประสงค์ของฝ่ายบริหาร ราคาทุนของสินทรัพย์ที่ก่อสร้างขึ้นเองประกอบด้วยต้นทุนค่าวัสดุ ค่าแรงงานทางตรง แตะต้นทุนทางตรงอื่น ๆ ที่เกี่ยวข้องกับการจัดหาสินทรัพย์

ส่วนประกอบของรายการที่ดิน อาคาร และอุปกรณ์แต่ละรายการที่มีรูปแบบและอายุการให้ประโยชน์ที่แตกต่างกัน และมีต้นทุนที่มีนัยสำคัญจะบันทึกส่วนประกอบนั้นแยกต่างหากจากกัน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

ต้นทุนที่เกิดขึ้นในภายหลัง ต้นทุนในการเปลี่ยนแทนส่วนประกอบจะรับรู้เป็นส่วนหนึ่งของมูลค่าตามบัญชีของรายการที่ดิน อาคาร และอุปกรณ์ เมื่อมีความเป็นไปได้ค่อนข้างแน่ที่จะได้รับประโยชน์เชิงเศรษฐกิจในอนาคตหรือศักยภาพในการให้บริการเพิ่มขึ้นจากรายการนั้น และสามารถวัดมูลค่าต้นทุนของรายการนั้นได้อย่างน่าเชื่อถือ และตัดมูลค่าของชิ้นส่วนที่ถูกเปลี่ยนแทนออกมาจากบัญชีด้วยมูลค่าตามบัญชี ส่วนต้นทุนที่เกิดขึ้นในการซ่อมบำรุงที่ดิน อาคาร และอุปกรณ์ที่เกิดขึ้นเป็นประจำจะรับรู้เป็นค่าใช้จ่ายเมื่อเกิดขึ้น

ค่าเสื่อมราคาบันทึกเป็นค่าใช้จ่ายในงบแสดงผลการดำเนินงานทางการเงิน คำนวณโดยวิธีเส้นตรงตามอายุการให้ประโยชน์โดยประมาณ ตามหนังสือกรมบัญชีกลาง ที่ กค 0410.3/ว 43 ลงวันที่ 29 มกราคม 2562 เรื่อง คู่มือการบัญชีภาครัฐ เรื่อง ที่ดิน อาคาร และอุปกรณ์ ดังนี้

อายุการให้ประโยชน์โดยประมาณของสินทรัพย์มีดังนี้

ครุภัณฑ์สำนักงาน	3 ปี
ครุภัณฑ์โฆษณาและเผยแพร่	5 ปี
ครุภัณฑ์คอมพิวเตอร์	3 ปี
ครุภัณฑ์งานบ้านงานครัว	2 ปี

ไม่มีการคิดค่าเสื่อมราคาสำหรับสินทรัพย์ระหว่างก่อสร้าง

4.5 ประมาณการหนี้สิน

ประมาณการหนี้สิน หมายถึง หนี้สินที่มีความไม่แน่นอนเกี่ยวกับจังหวะเวลา หรือจำนวนที่ต้องจ่ายชำระ แต่เป็นภาระผูกพันในปัจจุบันซึ่งมีความเป็นไปได้ค่อนข้างแน่ที่หน่วยงานจะต้องจ่ายชำระภาระผูกพันนั้นในอนาคต และสามารถประมาณมูลค่าภาระผูกพันนั้นได้อย่างน่าเชื่อถือ เช่น หนี้สินค่าชดเชยความเสียหาย หน่วยงานจะรับรู้ประมาณการหนี้สินด้วยจำนวนประมาณการที่ดีที่สุดของรายจ่ายที่จะต้องจ่าย ณ วันที่ในงบแสดงฐานะการเงินเพื่อชำระภาระผูกพันนั้น

4.6 การรับรู้รายได้

รายได้จากเงินงบประมาณรับรู้ตามเกณฑ์ดังนี้

(1) กรณีที่เบิกจ่ายเงินเข้าบัญชีของหน่วยงานเพื่อนำไปจ่ายต่อให้แก่ผู้มีสิทธิรับเงินของหน่วยงานรับรู้รายได้จากเงินงบประมาณเมื่อได้ส่งคำขอเบิกเงินกับคลัง

(2) กรณีที่เบิกหักผลักส่งหรือเบิกจ่ายตรงจากรัฐบาลให้แก่ผู้มีสิทธิรับเงินของหน่วยงานโดยหน่วยงานไม่ได้รับตัวเงิน รับรู้รายได้จากเงินงบประมาณเมื่อได้รับอนุมัติคำขอเบิกเงินจากคลัง

(3) รายได้อื่นรับรู้ตามเกณฑ์คงค้าง

4.7 การรับรู้ค่าใช้จ่าย

(1) ค่าใช้จ่ายจากเงินงบประมาณรับรู้ตามเกณฑ์คงค้าง

(2) ค่าใช้จ่ายอื่นรับรู้ตามเกณฑ์คงค้าง

หมายเหตุที่ 5 เงินสดและรายการเทียบเท่าเงินสด

	บาท
	2564
เงินฝากธนาคาร - ในงบประมาณ	27,952,866.76
เงินฝากธนาคาร - นอกงบประมาณ	401,250.00
รวมเงินสดและรายการเทียบเท่าเงินสด	28,354,116.76

เงินฝากธนาคาร ณ วันที่ 30 กันยายน 2564 จำนวน 28,354,116.76 บาท ซึ่งฝากไว้ที่ธนาคารกรุงไทย ประเภทกระแสรายวัน ประกอบด้วย

	บาท
	2564
1. เลขบัญชี 955-6-00528-5 ชื่อบัญชีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (เงินงบประมาณ)	27,952,866.76
2. เลขบัญชี 955-6-00529-3 ชื่อบัญชีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (เงินนอกงบประมาณ)	401,250.00
รวม	28,354,116.76

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

หมายเหตุที่ 6 ลูกหนี้ระยะสั้น

	บาท
	2564
ลูกหนี้เงินยืม	65,600.00
ค่าใช้จ่ายจ่ายล่วงหน้า	49,271.08
รวมลูกหนี้ระยะสั้น	114,871.08

ลูกหนี้เงินยืม ณ วันสิ้นปี แยกตามอายุหนี้ ดังนี้

	บาท			
ลูกหนี้เงินยืม	ยังไม่ถึงกำหนดชำระ	เกินกำหนดชำระไม่เกิน 30 วัน	เกินกำหนดชำระเกินกว่าเกิน 30 วัน	รวม
2564	65,600.00	-	-	65,600.00

หมายเหตุที่ 7 อาคาร และอุปกรณ์

	บาท
	2564
ครุภัณฑ์สำนักงาน	513,013.20
หัก ค่าเสื่อมราคาสะสม - ครุภัณฑ์สำนักงาน	(11,313.64)
ครุภัณฑ์สำนักงาน-สุทธิ	**501,699.56**
ครุภัณฑ์โฆษณาและเผยแพร่	109,936.50
หัก ค่าเสื่อมราคาสะสม - ครุภัณฑ์โฆษณาและเผยแพร่	(1,461.38)
ครุภัณฑ์โฆษณาและเผยแพร่ - สุทธิ	**108,475.12**
ครุภัณฑ์คอมพิวเตอร์	737,230.00
หัก ค่าเสื่อมราคาสะสม - ครุภัณฑ์คอมพิวเตอร์	(103,679.94)
ครุภัณฑ์คอมพิวเตอร์-สุทธิ	**633,550.06**
ครุภัณฑ์งานบ้านงานครัว	128,355.60
หัก ค่าเสื่อมราคาสะสม - ครุภัณฑ์งานบ้านงานครัว	(644.04)
ครุภัณฑ์งานบ้านงานครัว - สุทธิ	**127,711.56**
รวมอาคาร และอุปกรณ์ - สุทธิ	**1,371,436.30**

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

หมายเหตุที่ 8 เจ้าหนี้ระยะสั้น

	บาท
	2564
ค่าสาธารณูปโภคค้างจ่าย	43,248.66
ค่าใช้จ่ายค้างจ่าย	145,880.00
รายได้ค่าปรับอื่น รอนำส่ง	417.00
รวมเจ้าหนี้ระยะสั้น	189,545.66

หมายเหตุที่ 9 เงินรับฝากระยะสั้น

	บาท
	2564
เงินประกันอื่น	401,250.00
รวมเงินรับฝากระยะสั้น	401,250.00

หมายเหตุที่ 10 หนี้สินหมุนเวียนอื่น

	บาท
	2564
เจ้าหนี้กรมสรรพากร	85,411.81
รวมหนี้สินหมุนเวียนอื่น	85,411.81

หมายเหตุที่ 11 สัญญาจ้างบริการ

11.1 หน่วยงานมีภาระผูกพันตามสัญญาจ้างเหมาบริการ เป็นจำนวนเงิน 8,941,242.00 บาท

11.2 หน่วยงานมีภาระผูกพันตามสัญญาจ้างก่อสร้าง ปรับปรุง และจัดหาสินทรัพย์ เป็นจำนวนเงิน 18,374,708.28 บาท

11.3 หน่วยงานมีภาระผูกพันตามสัญญาจ้างบริการ เป็นจำนวนเงิน 550,191.63 บาท

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

หมายเหตุที่ 12 รายได้จากงบประมาณ

	บาท
	2564
ค่าใช้จ่ายบุคลากร	2,375,000.00
ค่าใช้จ่ายในการดำเนินงาน	10,412,014.42
ค่าครุภัณฑ์ที่ดินและสิ่งก่อสร้าง	19,863,243.58
ค่าใช้จ่ายในการดำเนินงานตามแผนโครงการ	8,941,242.00
รวมรายได้จากงบประมาณ	41,591,500.00

หมายเหตุที่ 13 ค่าใช้จ่ายบุคลากร

	บาท
	2564
เงินเดือนและค่าจ้าง	2,375,000.00
รวมค่าใช้จ่ายบุคลากร	2,375,000.00

หมายเหตุที่ 14 ค่าตอบแทน

	บาท
	2564
ค่าใช้จ่ายในการประชุม	1,337,936.00
ค่าตอบแทนการปฏิบัติ	4,420,939.32
รวมค่าตอบแทน	5,758,875.32

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

หมายเหตุที่ 15 ค่าใช้สอย

	บาท
	2564
ค่าใช้จ่ายในการอบรม	206,800.00
ค่าใช้จ่ายในการเดินทาง	9,309.00
ค่าจ้างเหมาบริการ	1,341,791.90
ค่าธรรมเนียม	4,000.00
ค่าเช่า	17,120.00
ค่าประชาสัมพันธ์	480,000.00
ค่าใช้สอยอื่น	1,087,935.01
รวมค่าใช้สอย	3,146,955.91

หมายเหตที่ 16 ค่าวัสดุ

	บาท
	2564
ค่าวัสดุ	487,896.94
รวมค่าวัสดุ	487,896.94

หมายเหตุที่ 17 ค่าสาธารณูปโภค

	บาท
	2564
ค่าไฟฟ้า	291,953.16
ค่าโทรศัพท์	3,076.36
ค่าบริการสื่อสารและโทรคมนาคม	23,617.84
ค่าบริการไปรษณีย์	37,224.00
รวมค่าสาธารณูปโภค	355,871.36

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (องค์การมหาชน)
หมายเหตุประกอบงบการเงิน (ต่อ)
สำหรับรอบระยะเวลาบัญชีตั้งแต่วันที่ 1 มกราคม 2564 (วันจดทะเบียนจัดตั้งองค์การมหาชน)
ถึงวันที่ 30 กันยายน 2564

หมายเหตุที่ 18 ค่าเสื่อมราคา

	บาท
	2564
ครุภัณฑ์	117,099.00
รวมค่าเสื่อมราคา	117,099.00

รายงานสรุปผล
การประเมินการดำเนินงาน

ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ประจำปี 2564

เสนอ
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ประจำปี 2564

กุมภาพันธ์ 2565

รายงานสรุปผลการประเมินการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประจำปี 2564

"สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ" หรือ "สกมช." มีชื่อภาษาอังกฤษว่า National Cyber Security Agency หรือ "NCSA" เป็นองค์การมหาชนที่จัดตั้งตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งเป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

ตามมาตรา 39 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้ สกมช. ดำเนินการจัดทำรายงานประจำปี โดยแสดงผลงานและรายงานการประเมินผลการดำเนินงานของสำนักงานโดยบุคคลภายนอกที่ กบส. ให้ความเห็นชอบ ทั้งนี้ บริษัท วินทูเกเตอร์ จำกัด ได้รับการมอบหมายให้เป็นหน่วยงานที่ดำเนินการประเมิน โดยบริษัทฯ ได้ใช้กรอบในการประเมินผลการดำเนินงานองค์กรในปีแรกผ่านแนวคิดการประเมินในมุมมอง 4 มิติ ตาม "2E2S" ดังนี้

Figure ที่ 1 แสดงแนวทางการประเมินใน 4 ด้าน

มิติด้านประสิทธิผล (Effectiveness)	มิติด้านประสิทธิภาพ (Efficiency)	มิติด้านการตอบสนองต่อประชาชน (Service)	มิติด้านความยั่งยืน (Sustainability)
เป็นการประเมินผลโดยเปรียบเทียบผลลัพธ์ที่ได้กับวัตถุประสงค์ของการจัดตั้งองค์กร หรือภารกิจตามกลยุทธ์ที่ได้กำหนดไว้	เป็นการประเมินการบริหารงาน/หรือการดำเนินการขับเคลื่อนแผนงานเปรียบเทียบกับต้นทุนหรืองบประมาณที่ใช้	เป็นการประเมินการตอบความคาดหวังและความต้องการของผู้รับบริการและประชาชนกลุ่มเป้าหมายขององค์กร	เป็นการประเมินความยั่งยืนขององค์กรจากผลการพัฒนาองค์กร เช่น การพัฒนาบุคลากร ความโปร่งใสในการดำเนินงาน เป็นต้น

(1) มิติด้านประสิทธิผล (Effectiveness)

เนื่องจากยังไม่ได้มีการกำหนดตัวชี้วัดและค่าเป้าหมายในปีแรก ดังนั้นในการประเมินในด้านนี้จะประเมินใน 2 ส่วน คือ

1. ผลลัพธ์โดยเปรียบเทียบกับวัตถุประสงค์ของการจัดตั้งองค์กร (ตามมาตรา 22) เพื่อให้สามารถประเมินความครบถ้วน ความสอดคล้องและความสมบูรณ์ของภาระงานของ สกมช.

2. ผลลัพธ์โดยเปรียบเทียบกับภารกิจและเป้าหมายที่กำหนดไว้ตามกลยุทธ์ของ สกมช. เพื่อให้สามารถประเมินผลที่คาดหวังในกลยุทธ์เปรียบเทียบกับเป้าประสงค์เชิงยุทธศาสตร์ที่กำหนดไว้ โดยผลการประเมินทั้ง 2 ส่วนสามารถแสดงได้ใน Figure ที่ 2 และ 3 ดังต่อไปนี้

Figure ที่ 2 แสดงผลการประเมินผลลัพธ์ที่เกิดขึ้นเปรียบเทียบกับวัตถุประสงค์ของการจัดตั้งองค์กร

วัตถุประสงค์และหน้าที่ของ สกมช. ตามที่กฎหมายกำหนด	ผลที่เกิดขึ้น ในปี 2564	ผลการประเมิน ในปีแรก
(1) เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์	• มีการกำหนดนโยบายและแผนที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ (1) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) (2) แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) (3) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (พ.ศ. 2565 - 2570)	มีรูปธรรมของผลการดำเนินการ
(2) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อ กกม. เพื่อให้ความเห็นชอบ	• มีการจัดทำกฎหมายลำดับรองจำนวน 5 ฉบับโดยได้ประกาศและบังคับใช้แล้วทั้งสิ้น โดยประกาศ กกม. เรื่องประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564	มีรูปธรรมของผลการดำเนินการแต่อาจเน้นการสื่อสารและสร้างความเข้าใจมากยิ่งขึ้น
(3) ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)	• มีการดำเนินการจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Thailand's National Cyber Exercise 2022) โดยมีหน่วยงานที่เกี่ยวข้องเข้าร่วม 66 หน่วยงาน รวมเป็นจำนวนคนทั้งสิ้น 458 ราย	มีผลการดำเนินการแต่ควรทดลองหรือซักซ้อมการใช้งานระบบฝึกให้มากขึ้น รวมถึงแยกเป็นแต่ละ Sector ให้ชัดเจน

วัตถุประสงค์และหน้าที่ของ สกมช. ตามที่กฎหมายกำหนด	ผลที่เกิดขึ้น ในปี 2564	ผลการประเมิน ในปีแรก
(4) ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์	• เข้าร่วมกิจกรรมความร่วมมือระดับนานาชาติ เพื่อร่วมมือป้องกันและต่อต้านอาชญากรรมไซเบอร์ (Cyber-Crime) ทุกรูปแบบจำนวน 151 ครั้ง ครอบคลุมกรอบ ASEAN, APEC, EU, OSCE และกรอบทวิภาคีต่าง ๆ เช่น อินเดีย ออสเตรเลีย เป็นต้น	มีรูปธรรมของผลการดำเนินการ
(5) ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ (6) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์	• กมช. ได้พิจารณามอบหมายให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ทำหน้าที่ไปพลางก่อน โดยในปี 2564 ได้รับการแจ้งเหตุภัยคุกคามทางไซเบอร์ทั้งหมด 1,607 รายการ ทั้งนี้ได้มีการประสานและเตรียมความพร้อมในการรับมือจำนวน 51 เหตุการณ์ มีการดำเนินการแจ้งเตือนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์จำนวน 12 รายงาน เป็นต้น • มีการตรวจพบการโจมตีเปลี่ยนหน้าเว็บไซต์ 199 หน่วยงาน และมีการแจ้งเตือนเหตุการณ์และให้คำแนะนำในการแก้ไขปัญหาจำนวน 2,076 ครั้ง	ส่วนใหญ่จะเป็นการดำเนินการจากความร่วมมือของพันธมิตร โดยเฉพาะไทยเซิร์ตในช่วงแรก ของการก่อตั้งใหม่
(7) ปฏิบัติการ ประสานงาน สนับสนุนและให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือตามคำสั่งของคณะกรรมการ	• มีการให้คำแนะนำช่วยเหลือหน่วยงานต่าง ๆ รวมทั้งสิ้น 105 หน่วยงาน และตอบรับและให้คำแนะนำแก้ปัญหาจำนวน 137 เหตุการณ์ • มี Cybersecurity Knowledge Sharing กับหน่วยงานและผู้เข้าสัมมนาทั้งหมด 9,976 คน	มีรูปธรรมของผลการดำเนินการ

วัตถุประสงค์และหน้าที่ของ สกมช. ตามที่กฎหมายกำหนด	ผลที่เกิดขึ้น ในปี 2564	ผลการประเมิน ในปีแรก
(8) ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ	• มีการกำหนดหลักเกณฑ์และลักษณะหน่วยงาน ที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบการควบคุมและกำกับดูแล พ.ศ. 2564 จำนวน 7 หมวด ซึ่งอยู่จะมีการประสานและให้ความร่วมมือช่วยเหลือต่อไป	มีรูปธรรมของผลการดำเนินการ
(9) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน	• มีการดำเนินการโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 1 เพื่อพัฒนาผู้เชี่ยวชาญและบุคลากรด้าน Cybersecurity ของทั้งภาครัฐและเอกชน • มีโครงการพัฒนาจำนวนมาก เช่น โครงการความร่วมมือทางวิชาการเพื่อพัฒนาบุคลากรด้านไซเบอร์ โครงการ APT Expert Mission in 2021 โครงการ Microsoft Women @ Cybersecurity โครงการฝึกอบรมการใช้อีเมลสื่อสารด้วย PGP การจัดการแข่งขัน Thailand Cyber Top Talent เป็นต้น	มีรูปธรรมของผลการดำเนินการ
(10) เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน	• มีบทวิเคราะห์สถานการณ์สำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ • มีการเผยแพร่ข้อมูลข่าวสารภัยคุกคาม 432 เรื่อง	มีผลการดำเนินการแต่ยังมีบทบาทการเป็นศูนย์กลางที่ไม่ชัดเจน เนื่องจากยังพึ่งก่อตั้ง และมีบุคลากรจำกัด

วัตถุประสงค์และหน้าที่ของ สกมช. ตามที่กฎหมายกำหนด	ผลที่เกิดขึ้น ในปี 2564	ผลการประเมิน ในปีแรก
(11) เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชนทั้งในประเทศและต่างประเทศ	• มีโครงการในการเชื่อมโยงและสร้างสัมพันธ์กับประเทศในกลุ่มภูมิภาคเอเชียตะวันออกเฉียงใต้ เช่น กิจกรรม Cyber SEA GAMES 2021 • การอบรม World Class Cyber Security Practices โดย MITRE/CISA/SEI	มีรูปธรรมของผลการดำเนินการ
(12) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ	• อยู่ระหว่างการจัดทำบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างไทยกับอินเดีย • อยู่ระหว่างการจัดทำหนังสือแสดงเจตจำนงความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างไทยและออสเตรเลีย	เริ่มมีผลการดำเนินการ
(13) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ	• ยังไม่ได้ดำเนินการด้านการวิจัยอย่างชัดเจน แต่มีการดำเนินการเพื่อกำหนดมาตรการตามกฎหมายระดับรอง • มีการฝึกซ้อมการรับมือกับภัยคุกคามแล้ว (ตามที่ระบุไว้ในข้อ (3) ผ่านกิจกรรม Thailand's National Cyber Exercise 2022)	ควรเพิ่มงานวิจัยและข้อเสนอแนะเชิงนโยบาย หรือมาตรการใหม่ ๆ
(14) ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์	• มีกิจกรรมในการยกระดับบุคลากรหน่วยงานควบคุม หรือกำกับดูแลหน่วยงานภาครัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) เช่น งานสัมมนา Thailand National Cyber Week 2021 งานสัมมนา NCSA Cyber Clinic 2021-2022 จำนวน 3 ครั้ง เป็นต้น	มีรูปธรรมของผลการดำเนินการ

วัตถุประสงค์และหน้าที่ของ สกมช. ตามที่กฎหมายกำหนด	ผลที่เกิดขึ้น ในปี 2564	ผลการประเมิน ในปีแรก
(15) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้ง ปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ	• มีการวิเคราะห์ และจัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยในระยะถัดไปจะแสดงผลกระทบ และมูลค่าเพิ่มที่เกิดขึ้น รวมถึงรายงานผลเป็นรายไตรมาส/รายเดือนกรณีเกิดเหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	มีผลการดำเนินการแต่สามารถปรับปรุงให้มีประสิทธิภาพเพิ่มขึ้นได้

จาก **Figure 2** จะเห็นว่า สกมช. ได้มีการดำเนินการตามวัตถุประสงค์ของการจัดตั้งได้ครบถ้วน ในปีแรกของการจัดตั้งสำนักงานตามภารกิจหลักทั้ง 4 ด้านคือ (1) การเสนอแนะนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (2) การกำกับดูแล เฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุมคามทางไซเบอร์ (3) การประสานความร่วมมือ ส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศ และต่างประเทศ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และ (4) การเผยแพร่ความรู้ความเข้าใจ และสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างไรก็ดี สกมช. ยังสามารถปรับปรุงให้มีประสิทธิภาพเพิ่มขึ้นได้ผ่านการวิจัย และพัฒนาบุคลากรที่เกี่ยวข้อง โดยเฉพาะบุคลากรในสำนักงาน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure) เพื่อเสริมศักยภาพในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนตอบสนองต่อเหตุภัยคุกคามและฟื้นฟูระบบให้กลับสู่ภาวะปกติได้อย่างทันท่วงที

นอกจากนั้น จากผลการประเมินความสำเร็จตามแผนปฏิบัติการและแผนกลยุทธ์ของ สกมช. ได้ผลดังแสดงใน Figure ที่ 3 ผลการประเมินผลลัพธ์ที่เกิดขึ้นเปรียบเทียบกับตัวชี้วัดและค่าเป้าหมายตามกลยุทธ์ของ สกมช. ปี 2564 ดังต่อไปนี้

ตัวชี้วัด	น้ำหนัก (ร้อยละ) / หน่วยนับ	ผลการดำเนินงาน	
		คะแนนที่ได้ (เทียบจากค่าเป้าหมาย)	คะแนนถ่วงน้ำหนัก
1. มีการจัดตั้งและบริหารสำนักงานฯ ให้มีทรัพยากรบุคคล ระบบข้อมูลและองค์ความรู้เพื่อรองรับการปฏิบัติงาน รวมทั้งพัฒนาระบบการบริหารจัดการสารสนเทศและดิจิทัล และการสื่อสาร			
1. ร้อยละความสำเร็จการจัดตั้งและบริหารสำนักงานฯ	**30**	**95.40**	**28.62**
1.1 การจัดเตรียมสถานที่ทำงานชั่วคราว	คะแนน	100.00	
1.2 ร้อยละความสำเร็จด้านการบริหารทรัพยากรบุคคล	ร้อยละ	100.00	
1.3 ร้อยละความสำเร็จการบริหารงบประมาณ	ร้อยละ	67.80	
1.4 การดำเนินการให้ความรู้ Wednesday Talk	คะแนน	100.00	
1.5 การดำเนินการพัฒนาระบบการบริหารจัดการสารสนเทศเพื่อรองรับการใช้งานในองค์กร	คะแนน	100.00	
1.6 การสื่อสารประชาสัมพันธ์องค์กรเพื่อสร้างความรับรู้แก่หน่วยงานที่เกี่ยวข้องและประชาชนทั่วไป	คะแนน	100.00	
1.7 จำนวนระเบียบข้อบังคับในการบริหารสำนักงานฯ	ฉบับ	100.00	
2. การจัดทำและดำเนินการตามนโยบาย แผน และยุทธศาสตร์เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์			
2. จำนวนนโยบายและแผน เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์	**20**	**100.00**	**20.00**

ตัวชี้วัด	น้ำหนัก (ร้อยละ) / หน่วยนับ	ผลการดำเนินงาน	
		คะแนนที่ได้ (เทียบจากค่าเป้าหมาย)	คะแนนถ่วงน้ำหนัก
3. การบริหารจัดการสำนักงานฯ ให้เป็นไปตามวัตถุประสงค์ของกฎหมาย นโยบาย มติ ของ กมช. กกม. และ กบส. และกฎหมายที่เกี่ยวข้องภายในปี 2564			
3. ร้อยละความสำเร็จการบริหารจัดการสำนักงานให้เป็นไปตามวัตถุประสงค์ของกฎหมาย นโยบาย มติ ของ กมช. กกม. และ กบส. และกฎหมายที่เกี่ยวข้องภายในปี 2564	**10**	**98.0**	**9.80**
3.1 ร้อยละความสำเร็จการดำเนินการจัดประชุมของคณะกรรมการตามแผนงาน	ร้อยละ	100.00	
3.2 ร้อยละความสำเร็จการบริหารแผนงาน/โครงการ ปี 2564	ร้อยละ	96.00	
4. แนวทางในการส่งเสริมและผลักดันให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐมีความพร้อมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์			
4. ร้อยละความสำเร็จการดำเนินการส่งเสริมและผลักดันให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐมีความพร้อมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์	**10**	**100.00**	**10.00**
4.1 ระดับความสำเร็จในการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	คะแนน	100.00	
4.2 การสำรวจความพร้อมด้าน IT ดิจิทัล และความมั่นคงปลอดภัยไซเบอร์ ครั้งที่ 1	คะแนน	100.00	

ตัวชี้วัด	น้ำหนัก (ร้อยละ) / หน่วยนับ	ผลการดำเนินงาน	
		คะแนนที่ได้ (เทียบจากค่าเป้าหมาย)	คะแนนถ่วงน้ำหนัก
5. มีแนวทางและมาตรการในการพัฒนาสำนักงานฯ ให้มีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์			
5. การดำเนินการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของสำนักงานฯ	**10**	**100.00**	**10.00**
6. มีกฎหมายลำดับรองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องและเป็นไปตามมาตรฐานสากล			
6. จำนวนกฎหมายลำดับรองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องและเป็นไปตามมาตรฐานสากล	15	100.00	15.00
7 มีรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบต่อนัยสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ			
7. การดำเนินการจัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบต่อนัยสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	5	80.00	4.00
		คะแนนรวม	**97.42**
		สรุปผลการประเมิน	**ระดับดีมาก**

หมายเหตุ: ใช้เกณฑ์การประเมินขององค์การมหาชนดังนี้

ระดับดีมาก หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 90 คะแนนขึ้นไป

ระดับดี หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 75 – 89.99 คะแนน

ระดับพอใช้ หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 60 – 74.99 คะแนน

ระดับต้องปรับปรุง หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ต่ำกว่า 60 คะแนน

จาก **Figure ที่ 3** จะเห็นว่าผลคะแนนการดำเนินการของ สกมช. ตามเกณฑ์การประเมินในปีแรกนั้นได้คะแนนอยู่ที่ 97.42 หรือ**ระดับดีมาก** โดยจะสังเกตว่าหัวข้อที่ต้องปรับปรุงอย่างเร่งด่วนคือการบริหารทรัพยากรบุคคล และการบริหารงบประมาณ ซึ่งอาจจะเป็นความเสี่ยงในระยะยาวขององค์กรได้ จึงมีข้อเสนอให้พิจารณาดังนี้

(1) ควรเร่งการสรรหาและบรรจุกำลังคนตามกรอบอัตรากำลังที่กำหนดไว้ เพื่อให้สามารถขับเคลื่อนภารกิจของ สกมช. ได้อย่างมีประสิทธิภาพ อันจะส่งผลต่อการเบิกจ่ายงบประมาณ และความสำเร็จของแผนงานที่กำหนดไว้

(2) ควรทบทวนระบบบริหารงานบุคคล เช่น ระบบประเมินผลการปฏิบัติงานประจำปี ระบบการจ่ายค่าตอบแทน ระบบการพัฒนาศักยภาพทรัพยากรบุคคล เป็นต้น เพื่อรองรับภาระงานที่มีความยากและซับซ้อนในอนาคต

(3) ควรมีระบบติดตามและบริหารการใช้เงินงบประมาณให้เป็นไปตามแผนการใช้จ่ายเงินในแต่ละปี เพื่อไม่ให้มีการกันเงินเหลื่อมปี หรือเงินคงเหลือจากการดำเนินงานจำนวนมาก ซึ่งอาจส่งผลต่อการของบประมาณในปีถัดไป ทั้งนี้ ระบบติดตามและบริหารการใช้เงินงบประมาณ อาจรายงานในที่ประชุมผู้บริหารเป็นรายเดือน เพื่อร่วมกันแก้ไขอุปสรรคที่เกิดขึ้นในการขับเคลื่อนงาน อันจะส่งผลให้เกิดการทำงานเป็นทีมอย่างมีประสิทธิภาพ

นอกจากนั้น ยังมีข้อเสนอในการกำหนดตัวชี้วัดตามภารกิจงานหลัก ซึ่งแม้จะได้คะแนนในระดับดีมาก ก็สามารถปรับปรุงให้มีประสิทธิผลแก่ภาครัฐมากขึ้นได้ ดังต่อไปนี้

(1) การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ อาจเพิ่มการมองภาพอนาคต (Scenario Planning) เพื่อกำหนดแนวทางการประเมินความพร้อมรับมือ และทักษะที่จำเป็น อันจะทำให้การพัฒนาบุคลากรมีประสิทธิผลมากกว่าการทดสอบ Pre-Post Test เท่านั้น

(2) การกำหนดแนวทางการจัดทำกฎหมายและระเบียบลำดับรองที่เกี่ยวข้อง อาจมีการสรุปภาพรวมที่จำเป็นต้องดำเนินการให้แล้วเสร็จในระยะเร่งด่วน ระยะสั้น ระยะกลาง และระยะยาวก่อน เพื่อให้วางแผนการดำเนินการได้อย่างครบถ้วนและสมบูรณ์ มากกว่าการกำหนดจำนวนกฎหมายหรือระเบียบลูกที่ดำเนินการแล้วเสร็จในแต่ละปีเท่านั้น

(3) อาจพิจารณาเพิ่มตัวชี้วัดเชิงผลกระทบ เช่น SROI หรือมูลค่าเชิงเศรษฐศาสตร์จากการป้องกันและรักษาความมั่งคงปลอดภัยไซเบอร์ของหน่วยงานรัฐ เป็นต้น เพื่อให้สามารถประเมินผลความคุ้มค่าของการดำเนินงานได้เหมาะสมยิ่งขึ้นในระยะยาว

(2) มิติด้านประสิทธิภาพ (Effectiveness)

เนื่องจากยังไม่ได้มีการกำหนดตัวชี้วัดและค่าเป้าหมายในปีแรก ดังนั้นในการประเมินจึงจะอ้างอิงจากตัวชี้วัดของ กพร. ที่ใช้ประเมินองค์การมหาชน ดังนี้

2.1 ประเมินประสิทธิภาพในการควบคุมค่าใช้จ่ายด้านบุคลากรขององค์การมหาชน ซึ่งจะกำหนดการประเมินตามมติคณะรัฐมนตรีในการประชุมเมื่อวันที่ 28 พฤษภาคม 2561 เรื่อง กรอบวงเงินรวมสำหรับค่าใช้จ่ายด้านบุคลากรสำหรับองค์การมหาชน ซึ่งได้ (1) เห็นชอบการกำหนดกรอบวงเงินรวมค่าใช้จ่ายด้านบุคลากรฯ ให้ไม่เกินร้อยละ 30 ของแผนการใช้จ่ายเงินประจำปี ให้กับองค์การมหาชนที่จัดตั้งตามพระราชบัญญัติองค์การมหาชน พ.ศ. 2542 และที่แก้ไขเพิ่มเติม และองค์การมหาชนที่จัดตั้งตามพระราชบัญญัติเฉพาะ รวมถึงองค์การมหาชนทั้งสองประเภทที่จะได้รับการจัดตั้งในภายหลังด้วย ยกเว้นองค์การมหาชน จำนวน 5 แห่ง ทั้งนี้ เพื่อมิให้เป็นภาระงบประมาณในระยะยาว

2.2 ประเมินประสิทธิภาพในการบริหารงาน หรือวัตกรรมการให้บริการ โดยในปีแรกที่ก่อตั้งจึงเสนอให้ได้ระดับความสำเร็จของการบริหารงบประมาณ ทั้งนี้ มีการรับงบประมาณในการดำเนินงานในปีงบประมาณ พ.ศ. 2564 เป็นเงิน 161.2827 ล้านบาท

โดยมีผลการดำเนินการตาม **Figure** 4 ผลการประเมินด้านประสิทธิภาพ ดังนี้

ตัวชี้วัด	ผลการดำเนินการ	ผลการประเมิน
2.1 ประเมินประสิทธิภาพในการควบคุมค่าใช้จ่ายด้านบุคลากรขององค์การมหาชน	ค่าใช้จ่ายบุคลากร/ค่าใช้จ่ายทั้งหมด = 19.36% < 30% (มี 42 ราย)	100
2.2 ประเมินประสิทธิภาพในการบริหารงาน	99.99 ของงบประมาณ	99.99
	รวม	**99.995**

3) มิติด้านการตอบสนองต่อประชาชน (Service)

เนื่องจากยังไม่ได้มีการกำหนดตัวชี้วัดและค่าเป้าหมายในปีแรก ดังนั้น ในการประเมินจึงจะอ้างอิงจากตัวชี้วัดของ กพร. ที่ใช้ประเมินองค์การมหาชน โดยจะประเมินการตอบสนองความคาดหวังและความต้องการของผู้รับบริการและประชาชน ซึ่งในปีนี้ได้ดำเนินการสำรวจความพร้อมด้านบุคลากร ระบบอุปกรณ์เทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์ในหน่วยงานรัฐที่เป็นผู้กำกับดูแล (Regulators) และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) เพื่อให้ได้ซึ่งข้อมูลเบื้องต้น โดยสามารถสรุปประเด็นที่น่าสนใจดังนี้

(3.1) ด้านบุคลากร หน่วยงาน Regulators และ CII มีเจ้าหน้าที่ทั้ง 2 ด้าน คือ ด้านเทคโนโลยีสารสนเทศและด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ คิดเป็นร้อยละ 58.7 และมีเฉพาะเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ คิดเป็นร้อยละ 39.7 ซึ่งแสดงให้เห็นว่าหน่วยงาน Regulators และ CII จำนวนประมาณร้อยละ 40 ยังไม่มีเจ้าหน้าที่เฉพาะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนั้นเพื่อให้เจ้าหน้าที่สามารถปฏิบัติงานในแต่ละด้านได้อย่างมีประสิทธิภาพ จึงมีข้อเสนอแนะให้เพิ่มจำนวนเจ้าหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยสามารถพัฒนาจากบุคลากรด้านเทคโนโลยีสารสนเทศเพื่อเพิ่มความพร้อมของหน่วยงานต่อการรับมือจากภัยคุกคามทางไซเบอร์และเนื่องจากจำนวนเจ้าหน้าที่ที่มีใบรับรองมีเพียง ร้อยละ 10.4 ดังนั้นควรมีการสนับสนุนให้เจ้าหน้าที่ได้รับใบรับรองมีจำนวนเพิ่มขึ้นเพื่อเพิ่มศักยภาพและความน่าเชื่อถือของหน่วยงาน

(3.2) ด้านระบบอุปกรณ์เทคโนโลยีสารสนเทศ หน่วยงานที่มีการจัดสรรงบประมาณสำหรับการต่ออายุของลิขสิทธิ์ซอฟต์แวร์ คิดเป็นร้อยละ 67.2 มีงบประมาณต่ออายุเพียงบางส่วนและไม่มีงบประมาณต่ออายุลิขสิทธิ์ซอฟต์แวร์ คิดเป็นร้อยละ 19.7 และ 13.1 ตามลำดับ และยังพบว่าลิขสิทธิ์ซอฟต์แวร์ที่ใช้ในหน่วยงานไม่ครอบคลุมเครื่องลูกข่ายและเครื่องให้บริการคิดเป็น ร้อยละ 27.3 ซึ่งจากผลสำรวจดังกล่าวแสดงว่าหน่วยงานมีความเสี่ยงในการถูกโจมตีทางไซเบอร์ได้ง่ายขึ้น ดังนั้น เพื่อลดความเสี่ยงจากการถูกโจมตีจากภัยคุกคามทางไซเบอร์ของหน่วยงาน จึงควรมีการสนับสนุนให้หน่วยงาน Regulators และ CII มีงบประมาณในการต่ออายุของลิขสิทธิ์ซอฟต์แวร์มีความครอบคลุมทั้งเครื่องลูกข่ายและเครื่องให้บริการ

นอกจากนี้หน่วยงาน Regulators และ CII ไม่มีการจัดตั้งศูนย์ SOC คิดเป็นร้อยละ 36.4 มีศูนย์ SOC เป็นของหน่วยงานเอง คิดเป็นร้อยละ 34.7 และเป็นของหน่วยงานภายนอก คิดเป็นร้อยละ 28.1 โดยผลสำรวจดังกล่าวแสดงให้เห็นว่าหน่วยงานของ Regulators และ CII มีความเสี่ยงในการถูกโจมตีจากภัยคุกคามทางไซเบอร์ โดยเฉพาะหน่วยงานที่ไม่มีศูนย์ SOC ดังนั้นจึงควรสนับสนุนให้หน่วยงานมีการจัดตั้งศูนย์ SOC เป็นของหน่วยงานเอง เพื่อให้หน่วยงานมีความปลอดภัยจากการถูกโจมตีได้มากขึ้น เพราะเจ้าหน้าที่สามารถทำการตรวจสอบการเข้าถึงเครือข่ายและระบบสารสนเทศต่าง ๆ ของหน่วยงานได้ตลอดเวลา และสามารถตรวจสอบความผิดปกติ พร้อมกับตอบสนองต่อการโจมตีและสามารถหยุดการโจมตีได้ทันท่วงที อีกทั้งสามารถเก็บข้อมูลเพื่อตรวจหาช่องทางที่ผู้บุกรุกเข้ามาได้อย่างแม่นยำ

(3.3) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ผลการสำรวจพบว่าหน่วยงานมีการประเมินความเสี่ยงภัยคุกคามทางไซเบอร์ การประเมินช่องโหว่และภัยคุกคามทางไซเบอร์ การประเมินภัยคุกคามทางไซเบอร์ อยู่ในช่วงร้อยละ 33.1 ถึง 67.8 การจัดทำแผนการรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์และการจัดทำแผนเพื่อให้หน่วยงานสามารถดำเนินการให้บริการได้ในกรณีที่เกิดภัยคุกคามทางไซเบอร์หรือเกิดเหตุภัยพิบัติคิดเป็นร้อยละ 72.7 และ 86.0 ตามลำดับ ซึ่งจากผลสำรวจดังกล่าวชี้ให้เห็นว่าหน่วยงานร้อยละ 32.2-66.9 อาจมีความเสี่ยงในการถูกโจมตีจากภัยคุกคามทางไซเบอร์และมีหน่วยงานร้อยละ 27.3 และ 14.0 ไม่มีการจัดทำแผนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์และไม่มีการจัดทำแผนเพื่อให้หน่วยงานสามารถดำเนินการให้บริการได้ในกรณีที่เกิดภัยคุกคามทางไซเบอร์หรือเกิดเหตุภัยพิบัติตามลำดับ จึงเสนอแนะให้หน่วยงานมีการดำเนินการประเมินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มมากขึ้นเพื่อทำให้หน่วยงานมีความปลอดภัยจากภัยคุกคามทางไซเบอร์ รวมทั้งให้หน่วยงานมีการจัดทำแผนการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์และจัดทำแผนเพื่อให้หน่วยงานสามารถดำเนินการให้บริการได้ในกรณีที่เกิดภัยคุกคามทางไซเบอร์หรือเกิดเหตุภัยพิบัติ

นอกจากนี้ Regulators และ CII ต้องการการสนับสนุนเพิ่มเติม กล่าวคือ ต้องการให้ผู้บริหารเข้าใจความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องการให้มีทีมเจ้าหน้าที่จากส่วนกลางให้ความช่วยเหลืออย่างทันท่วงทีเมื่อถูกโจมตีจากภัยคุกคามทางไซเบอร์ ให้ความช่วยเหลือด้านการให้คำแนะนำ ปรึกษา ให้ข้อมูลเพิ่มเติมเมื่อหน่วยงานมีปัญหาและอุปสรรคด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การจัดอบรมหลักสูตรมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงาน Regulators และ CII อย่างต่อเนื่อง และให้ National CERT จัดทำระบบการแบ่งปันข้อมูลที่เป็นทางการมากกว่า Line Open Chat ที่มีการใช้งานในปัจจุบัน เป็นต้น

ทั้งนี้ สกมช. จะนำผลการสำรวจนี้ไปใช้ในการจัดทำแผนงบประมาณและกำหนดนโยบายและยุทธศาสตร์ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศต่อไปจึงได้คะแนน 100.00 คะแนน

(4) มิติด้านความยั่งยืน (Sustainability)

เนื่องจากยังไม่ได้มีการกำหนดตัวชี้วัดและค่าเป้าหมายในปีแรก ดังนั้นในการประเมินจึงจะอ้างอิงจากตัวชี้วัดของ กพร. ที่ใช้ประเมินองค์การมหาชน คือ ความสำเร็จของการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน ตาม **Figure 5** ผลการประเมินด้านความยั่งยืน ดังนี้

ที่	ประเด็นการประเมิน	น้ำหนัก (ร้อยละ)	ผลการดำเนินการ		สรุปคะแนน
			ผ่าน (1)	ไม่ผ่าน (0)	
1	1) คณะกรรมการทบทวนผลการดำเนินงานขององค์การมหาชนเพื่อกำหนดทิศทางและนโยบายการปฏิบัติงานขององค์การมหาชน อย่างน้อย ปีละ 1 ครั้ง 2) คณะกรรมการพิจารณาแผนปฏิบัติการ 3 ปี และแผนปฏิบัติการประจำปีงบประมาณ พ.ศ. 2563 ภายในเวลาที่คณะรัฐมนตรีกำหนด	8 7	√ √		8 7
2	คณะกรรมการพิจารณาแผนและรายงานผล (1) การควบคุมภายใน (2) การตรวจสอบภายใน (3) การบริหารความเสี่ยง (4) การบริหารงานบุคคล (5) การนำเทคโนโลยีดิจิทัล มาใช้ปฏิบัติงานทุกไตรมาส (อย่างน้อยสามไตรมาส) (กรณีการบริหารงานบุคคลจะพิจารณาด้วยว่าองค์การมหาชนมีระบบประเมินผลการปฏิบัติงานเจ้าหน้าที่และผู้บริหาร และมีการนำผลประเมินเชื่อมโยงกับการเลื่อนขั้นเลื่อนตำแหน่ง และการต่อสัญญาจ้างงาน)	15 (ประเด็นละ 3 คะแนน)	√ ได้แค่ 2 ประเด็น		6
3	คณะกรรมการพิจารณารายงานผลการปฏิบัติงานด้านการเงินและรายงานด้านภารกิจหลักทุกไตรมาส (อย่างน้อยสามไตรมาส) โดยรายงานได้ระบุปัญหาอุปสรรคที่ผลงานไม่เป็นไปตามเป้าหมายและข้อเสนอแนะเพื่อแก้ไข	15	√		15
4	คณะกรรมการควบคุมให้องค์การมหาชนมีการเบิกจ่ายงบประมาณตามแผนการใช้จ่ายเงินที่ได้รับอนุมัติจากคณะกรรมการ ณ ต้นปีงบประมาณได้ไม่น้อยกว่าร้อยละ 96	15	√		15
5	คณะกรรมการกำกับให้มีการรายงานผลการดำเนินงานแก่รัฐมนตรีที่กำกับดูแลองค์การมหาชน อย่างน้อยปีละ 2 ครั้ง	10	√		10
6	ในการเข้าร่วมประชุมของคณะกรรมการร้อยละ 90 ของจำนวนการประชุมมีกรรมการ เข้าประชุมร้อยละ 80 ขึ้นไป	10	√		10

ที่	ประเด็นการประเมิน	น้ำหนัก (ร้อยละ)	ผลการดำเนินการ		สรุปคะแนน
			ผ่าน (1)	ไม่ผ่าน (0)	
7	เว็บไซต์ขององค์การมหาชนมีข้อมูลสำคัญครบถ้วนและเป็นปัจจุบัน ดังนี้ (1) ประวัติความเป็นมา คำอธิบายภาพรวมการปฏิบัติงานตามภารกิจหลักในปัจจุบัน การเปลี่ยนแปลงและพัฒนาการที่สำคัญ ความเสี่ยงสำคัญขององค์กร และผลการปฏิบัติงาน ทั้งด้านการเงินและภารกิจหลัก แผนยุทธศาสตร์และเป้าหมายการปฏิบัติงานขององค์กร (2) ประวัติของคณะกรรมการรายบุคคล ประกอบด้วย (1) อายุ (2) วุฒิการศึกษา (3) ประวัติการทำงาน (4) วัน เดือน ปีที่ได้รับการแต่งตั้งเป็นกรรมการ และ (5) ตำแหน่งหน้าที่ปัจจุบัน (นอกจากการเป็นคณะกรรมการ) (3) โครงสร้างของคณะกรรมการ คณะกรรมการตรวจสอบ และคณะอนุกรรมการทุกคณะ พร้อมทั้งอำนาจหน้าที่และอัตราการจ่ายเบี้ยประชุม (4) ข้อมูลการเข้าประชุมของคณะกรรมการ (5) รายงานงบการเงิน พร้อมหมายเหตุประกอบงบการเงิน (6) โครงการลงทุนที่สำคัญ (ถ้ามี) (7) การจัดซื้อจัดจ้าง (8) นโยบายการกำกับดูแลกิจการที่ดี (9) ข้อบังคับและ/หรือระเบียบขององค์การมหาชน (10) รายงานประจำปีที่ผ่านมา	10	√ c แต่ไม่ครบ 5 ข้อ		5
8	คณะกรรมการมีการประเมินตนเอง ทั้งแบบรายบุคคลและแบบทั้งคณะ และมีการเปิดเผยผลการประเมินตนเองของคณะกรรมการในที่ประชุม และกำหนดแนวปฏิบัติเพื่อเพิ่มประสิทธิภาพในการปฏิบัติหน้าที่	10	√		0
	รวม	**100**			**76**

โดยผลการประเมินใน 8 ประเด็นทั้งหมดได้ 76 คะแนน หรือในระดับ “ดี” แต่ควรเพิ่มการติดตามแผนการบริหารความเสี่ยง แผนการบริหารงานบุคคล และแผนการนำเทคโนโลยีดิจิทัล รวมถึงกับการปรับปรุงเว็บไซต์ และการประเมินผลตนเองของคณะกรรมการทั้งแบบรายบุคคลและแบบทั้งคณะ และมีการเปิดเผย

จากผลการประเมินทั้งหมดในทั้ง 4 ด้าน สามารถสรุปผลได้ Figure 6 สรุปผลการดำเนินการรวม ดังนี้

ข้อ	มิติการประเมิน	คะแนนรวม
1	มิติด้านประสิทธิผล (Effectiveness)	95.330
2	มิติด้านประสิทธิภาพ (Efficiency)	99.995
3	มิติด้านการตอบสนองต่อประชาชน (Service)	100.000
4	มิติด้านความยั่งยืน (Sustainability)	76.000
	รวมคะแนนทั้งหมด	92.831
	ผลการประเมิน	**ดีมาก**

หมายเหตุ: ใช้เกณฑ์การประเมินขององค์การมหาชนดังนี้

ระดับดีมาก หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 90 คะแนนขึ้นไป

ระดับดี หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 75 – 89.99 คะแนน

ระดับพอใช้ หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 60 – 74.99 คะแนน

ระดับต้องปรับปรุง หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ต่ำกว่า 60 คะแนน

จาก **Figure 6** จะเห็นได้ว่าผลการประเมินทั้งหมดประจำปี 2564 ได้ **92.831 คะแนน หรือ “ดีมาก”** ในปีแรกของการก่อตั้งสำนักงานฯ อย่างไรก็ดี สกมช. อาจมีความจำเป็นต้องพิจารณาปรับปรุงการบริหารงานด้านทรัพยากรบุคคล การบริหารความเสี่ยง การบริหารงบประมาณ และการกำกับดูแลที่ดี เพื่อให้เกิดความยั่งยืนในระยะยาว รวมถึงควรเพิ่มกำลังคนและกลไกการส่งเสริม สนับสนุนงานวิจัยและพัฒนาเทคโนโลยีองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน เพื่อให้องค์กรมีบทบาทนำในการกำหนดมาตรการและแผนในระดับประเทศได้มากขึ้นตามภารกิจที่ได้รับมอบหมาย

นอกจากนั้น สกมช. ควรให้ความสำคัญกับการเป็นศูนย์กลางประสานงานในด้านที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ผ่านการพัฒนาความสัมพันธ์กับภาคีเครือข่ายการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในและต่างประเทศ โดยเฉพาะ Regulators และ CII ในประเทศผ่านการสื่อสาร การประสานงาน การพัฒนาศักยภาพ และการสร้างความร่วมมือที่เข้มแข็ง เพื่อให้พร้อมตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพตามนโยบาย แผนงาน หลักเกณฑ์ แนวปฏิบัติ และกฎระเบียบที่ได้กำหนดไว้

โดยรวม คะแนนผลการประเมินในปีแรกที่ได้คะแนนระดับ “ดีมาก” ด้วยกำลังคนและงบประมาณที่จำกัดนั้น ควรได้รับการชื่นชม และส่งเสริมขวัญกำลังใจเพื่อให้พนักงานมีความมุ่งมั่นทุ่มเท เพื่อให้ สกมช. เป็นฟันเฟืองเล็ก ๆ ที่สามารถช่วยประเทศในการขับเคลื่อนเศรษฐกิจและความมั่นคงของประเทศไทยในยุคดิจิทัล และทำให้ประชาชนทุกคนปลอดภัยจากภัยคุกคามทางไซเบอร์ตลอดไป

คำจำกัดความ

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
APT	เอพีที	APT ย่อมาจาก Advanced Persistent Threat คือ การที่ผู้โจมตีฝังตัวอยู่ในระบบของเหยื่อเป็นเวลานานเพื่อเฝ้าดูพฤติกรรมและดักรับข้อมูล	ETDA Thailand Facebook page
Data Breach	ดาต้าบรีช	การเจาะระบบและขโมยข้อมูลสำคัญออกไปขายหรือเผยแพร่ เช่น การนำข้อมูลส่วนบุคคลของลูกค้าไปขาย หรือการล้วงข้อมูลงานวิจัยเพื่อแข่งขันทางการค้า	ETDA Thailand Facebook page
Fake Website	เฟค เว็บไซต์	เป็นองค์ประกอบที่ฟิชชิง สร้างขึ้นเพื่อล่อลวงข้อมูลโดยการสร้างเว็บไซต์ที่มีความเหมือนเว็บไซต์จริงมากที่สุดเพื่อให้ผู้ใช้งานหลงกลเข้ามาในระบบ รอให้ผู้ใช้ใส่ข้อมูลส่วนตัวต่าง ๆ ทำให้ข้อมูลส่วนตัวที่ควรรักษาเป็นความลับถูกโจรกรรมไปได้ ซึ่งทำให้ผู้ใช้ได้รับผลกระทบเป็นอย่างมาก เพราะข้อมูลอาจถูกนำไปใช้ในทางที่เสียหาย โดยที่เราไม่สามารถหยุดได้เลยเพราะข้อมูลเป็นข้อมูลจริงของผู้ใช้เอง ส่งผลเสียให้กับเหยื่อที่หลงกลเป็นอย่างมาก	www.mindphp.com หมายเหตุ : เนื่องจากคำว่า Fake website มีข้อมูลจำกัดและไม่เพียงพอต่อการให้ความหมาย และมีคำที่คล้ายคลึงกันคือ Fake webpage ที่มีข้อมูลอธิบาย จึงทำการนำข้อมูลความหมายของ Fake webpage มาใช้เพื่ออธิบายความหมาย
Fraud	ฟรอด	ภัยคุกคามประเภทฟรอด หรือการฉ้อโกงหลอกลวง สามารถแบ่งออกได้เป็น 2 ประเภท คือ Phishing (ฟิชชิง) คือการล่อหลอกเหยื่อเข้าหน้าเว็บไซต์ปลอม ซึ่งทำให้ดูคล้ายกับหน้าล็อกอินของเว็บไซต์จริง จุดประสงค์เพื่อขโมยพาสเวิร์ด และนำไปสู่การขโมยข้อมูลอื่น ๆ โดยเฉพาะในเรื่อง	ETDA Thailand Facebook page หมายเหตุ : เนื่องจาก Fraud มีความหมายโดยทั่วไปด้วย จึงทำการค้นหาด้วยการใส่แหล่งอ้างอิงตามหลังเพื่อให้ได้ความหมายที่เกี่ยวข้องกับงานด้านไซเบอร์ยิ่งขึ้น

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
		ธุรกรรมทางการเงิน Scam (สแคม) คือการแอบอ้างเพื่ออาศัยผลจากความเข้าใจผิด เช่น การสร้างหน้าเว็บไซต์ปลอมแอบอ้างว่าเป็นเว็บไซต์ของบริการที่มีชื่อเสียง หลอกให้ร่วมเล่นเกมเพื่อชิงรางวัล เพื่อขโมยข้อมูลส่วนบุคคล ซึ่งจะนำไปสู่การปลอมแปลงอื่น ๆ เพื่อผลประโยชน์ของผู้ไม่หวังดีต่อไป	
Misconfiguration	มิสคอนฟิกกูเรชั่น	การกำหนดค่าที่ไม่ถูกต้อง หรือไม่เหมาะสมของระบบข้อมูล หรือส่วนประกอบของระบบ ที่อาจนำไปสู่ช่องโหว่หรือจุดอ่อนของระบบ	https://csrc.nist.gov หมายเหตุ : ภายใน www.digitalskill.org มีการให้ความหมายของคำว่า Security Misconfiguration คือช่องโหว่เกี่ยวกับการตั้งค่าความมั่นคงปลอดภัย โดยสามารถเกิดได้ทุกที่ในระบบที่มีการตั้งค่า สาเหตุหลักเกิดจากการตั้งค่าอย่างไม่มั่นคงปลอดภัย หรือใช้ค่าตั้งต้นที่ไม่มั่นคงปลอดภัยมาตั้งแต่ต้นอยู่แล้ว เกือบทุกระบบสามารถเกิดการตั้งค่าที่ไม่มั่นคงปลอดภัยขึ้นได้ แต่จากคำศัพท์หลักคือ Misconfiguration จึงยึดคำศัพท์หลักโดยการหาข้อมูลจากเว็บไซต์ https://csrc.nist.gov และทำการแปลความหมายจากเว็บไซต์ดังกล่าว
Penetration Test	เพนิเทรชัน เทส	Penetration Test หรือ PenTest เป็นวิธีการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ โดยใช้ผู้เชี่ยวชาญ ช่วยให้สามารถประเมินความเสี่ยงของ	www.uih.co.th

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
		ระบบเครือข่ายลูกค้าว่ามีความเสี่ยงตรงจุดใด ซึ่งจะเป็นการทดสอบเจาะระบบในเชิงลึก พร้อมแจ้งผลการทดสอบ และประเมินความเสี่ยงเพื่อเตรียมการป้องกันไว้ก่อน ซึ่งการตรวจหาช่องโหว่นี้เป็นหนึ่งในมาตรการป้องกันภัยคุกคามทางไซเบอร์ที่เหมาะสำหรับองค์กรที่ต้องการรักษาความปลอดภัยเป็นพิเศษ และจำเป็นต้องตรวจสอบระบบอย่างสม่ำเสมอ	
Ransomware	แรนซัมแวร์	มัลแวร์เรียกค่าไถ่ เป็นมัลแวร์ที่เข้ารหัสลับข้อมูลในเครื่องเหยื่อ ทำให้ไม่สามารถเข้าถึงข้อมูลได้ และเรียกค่าไถ่จากเหยื่อเพื่อแลกกับการถอดรหัสลับ	ETDA Thailand Facebook page
Social Engineering	โซเชียล อินเจอเนริ่ง	วิศวกรรมสังคม เป็นเทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูล ซึ่งบางครั้งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้องเลย ผู้ที่ตกเป็นเหยื่อของ Social Engineering อาจจะตกเป็นเหยื่อโดยความตั้งใจหรือไม่ตั้งใจของผู้ไม่หวังดีก็ได้ กล่าวคือ ถ้าผู้ไม่หวังดีมีเป้าหมายเฉพาะเจาะจง เช่น ต้องการข้อมูลความลับขององค์กรใดองค์กรหนึ่ง เหยื่อในที่นี้ก็มักจะเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลความลับขององค์กรนั้น แต่หากเป้าหมายของผู้ไม่หวังดีเป็นแบบที่ไม่ได้เจาะจงเหยื่อ เช่น ต้องการรหัสบัตรเครดิต หรือบัญชีผู้ใช้และรหัสผ่านของบริการต่าง ๆ ของใครก็ได้ เหยื่อของผู้ไม่หวังดีนี้จะเป็นใครก็ตามซึ่งหลงเชื่อการหลอกลวงนั้น	www.etda.or.th

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
Supply Chain Attack	ซัพพลายเชน แอทแทค	การจู่โจมไปที่ผู้พัฒนาซอฟต์แวร์ โดยมีจุดประสงค์เพื่อสอดแทรกมัลแวร์ลงในแอปพลิเคชัน ซึ่งจะทำให้ลูกค้าผู้ใช้งานแอปพลิเคชันนั้นตกเป็นเหยื่อได้โดยไม่รู้ตัว เนื่องจากมัลแวร์จะแฝงตัวมาในรูปของแอปพลิเคชันที่องค์กรซื้อใช้งานอยู่แล้ว หรืออาจกระจายตัวออกมาในรูปของอัปเดตสำหรับแอปพลิเคชันนั้น จึงมีโอกาสที่จะหลุดรอดจากการตรวจจับได้สูงกว่าปกติ และสามารถทำงานในเครือข่ายของเป้าหมายได้เสมือนเป็นแอปพลิเคชันดั้งเดิมที่องค์กรไว้วางใจ	https://news.microsoft.com/
Website Defacement	เว็บไซต์ ดีเฟซเมนต์	การลอบเจาะระบบเข้าไปเปลี่ยนหน้าเว็บไซต์ แสดงสัญลักษณ์ โอ้อวดความสามารถ หรือความเห็นทางการเมือง	ETDA Thailand Facebook page
Website Phishing	เว็บไซต์ฟิชชิง	การหลอกให้เข้าเว็บไซต์ปลอม เพื่อลวงเอาข้อมูลที่สำคัญ เช่น การปลอมเว็บไซต์ธนาคารและส่งอีเมลแจ้งลูกค้าธนาคารให้เข้ามากรอกข้อมูล username และ password ที่เว็บปลอม และข้อมูลที่กรอกจะส่งไปยังมิจฉาชีพ	ETDA Thailand Facebook page

NCSA
สกมช

Protection is better than cure

จัดทำโดย สำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พิมพ์ครั้งที่ 1 จำนวน 1,000 เล่ม
มีนาคม 2565
พิมพ์ที่ บริษัท สุขุมวิทการพิมพ์ จำกัด
ปีที่พิมพ์ 2565
ISBN.....

E-Book

QR Code

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ
80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02 142 6888 โทรสาร 02 143 7593
Email: saraban@ncsa.or.th

แจ้งเหตุภัยคุกคามไซเบอร์: ncert@ncsa.or.th