TB-CERT
Thailand Banking Sector CERT

ANNUAL REPORT 2021

Collaboration

Building strong partnerships will foster a rapid response to cyber threats and an overall effective defense against it.

Incident Response

Response correctly helps organization handle cyber incident faster.

Building Trust is difficult,
Maintainning Trust is more challenge

02-5587500 The Thai Bankers' Association Contact@tb-cert.or.th

รายงานประจำปี

ANNUAL REPORT 2021

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร

Thailand Banking Sector CERT: TB-CERT

จัดทำโดย

ชัชวัฒน์ อัศวรักวงศ์

ธาวินี วงศ์วิศว์

ปรมินทร์ ช่วงมณี

ปิลันญา เชิญถนอมวงศ์

ชญานิน แก้วหาญ

ที่ปรึกษา

กิตติ โฆษะวิสุทธิ์

บรรณาธิการ

ธาวินี วงศ์วิศว์

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร

สมาคมธนาคารไทย

5/13 หมู่ 3 ถนนแจ้งวัฒนะ ตำบลคลองเกลือ

อำเภอปากเกร็ด จังหวัดนนทบุรี 11120

โทร. 0 2558 7500

Email: contact@tb-cert.or.th

เผยแพร่เมื่อ

มีนาคม 2022

TLP: WHITE

สารบัญ

เกี่ยวกับ TB-CERT

ความเป็นมา

Thailand Banking Sector Computer Emergency Response Team หรือ TB-CERT จัดตั้งขึ้นโดยความเห็นชอบของผู้บริหารระดับสูงของธนาคารพาณิชย์ในประเทศไทย เพื่อสนับสนุนให้สมาชิกกลุ่มซึ่งเป็นพนักงานของธนาคารได้มีการแลกเปลี่ยนข้อมูลและประสบการณ์เพื่อประโยชน์โดยรวมของสถาบันการเงินในประเทศไทย โดยเฉพาะเพื่อการนำไปใช้ในการป้องกันเหตุภัยคุกคามทางไซเบอร์ที่อาจจะมีผลกระทบกับการบริการ ทรัพยากร หรือบุคลากรขององค์กร โดยจะไม่เสนอความเห็นต่อผลิตภัณฑ์ทางการเงิน (Product) หรือให้ข้อมูลเชิงลบต่อหน่วยงานหรือบุคคลที่สาม อันจะทำให้เกิดความเสื่อมเสียและเป็นอุปสรรคต่อกิจกรรมการแลกเปลี่ยนความคิดเห็นหรือความสัมพันธ์อันดีของสมาชิกในกลุ่ม

ค่านิยมหลัก

TB-CERT เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลในด้านความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์รวมของบุคลากรที่มีความชำนาญด้านไซเบอร์ และเป็นแหล่งให้ความรู้และสร้างความตระหนักในการระวังภัยที่อาจเกิดขึ้นได้ทุกเมื่อ ไม่ว่าจะเกิดกับบุคลากร ลูกค้า หรือธุรกิจของธนาคาร รวมถึงเป็นศูนย์กลางในการติดต่อสื่อสารกับองค์กรที่เกี่ยวข้องทั้งในและต่างประเทศ เพื่อให้สามารถรับรู้ข่าวสารและช่วยเหลือในการแก้ปัญหาภัยไซเบอร์ที่เกิดขึ้นกับสมาชิก ทั้งนี้เพื่อให้ทุกภาคส่วนมีความรู้และเข้าใจเรื่องภัยไซเบอร์และพร้อมรับมือกับภัยเหล่านี้ได้อย่างมีประสิทธิภาพ

การดำเนินงาน

การดำเนินงานของ TB-CERT จะครอบคลุม 4 ด้านที่สำคัญคือ

1. **เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูล** ทั้งภัยคุกคามด้านไซเบอร์และแนวทางการแก้ไข
2. **สร้างมาตรฐานกลางด้านความมั่นคงปลอดภัย** ของการใช้เทคโนโลยีใหม่
3. **กำหนดกระบวนการในการรับมือภัยไซเบอร์ภาคการธนาคาร** และจัดให้มีการซ้อมรับมือร่วมกันอย่างสม่ำเสมอ
4. **ส่งเสริมการพัฒนาบุคลากรด้าน Cybersecurity** โดยครอบคลุมทั้งการสร้างบุคลากรใหม่เข้าสู่ภาคการเงิน และพัฒนาบุคลากรของสถาบันการเงินให้มีความรู้ความเข้าใจ และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์

คำนิยม

พลเอก ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ปัจจุบันสถาบันการเงินทุกแห่งล้วนมีอัตราการทำธุรกรรมการเงินผ่านระบบอิเล็กทรอนิกส์เพิ่มขึ้นอย่างมีนัยสำคัญ เหตุผลหลักมาจากการเติบโตอย่างก้าวกระโดดของระบบการซื้อขายสินค้าออนไลน์ ประกอบกับการแพร่ระบาดของโรคติดต่อในระบบทางเดินหายใจที่ทุกวันนี้ยังคงเป็นภัยคุกคามที่สำคัญต่อระบบสาธารณสุขและเศรษฐกิจของประเทศไทยและทั่วโลกและเมื่อรัฐบาลได้มีโครงการให้ความช่วยเหลือประชาชนในรูปแบบต่าง ๆ ผ่านระบบกระเป๋าเงินอิเล็กทรอนิกส์ ทำให้ประชาชนเกิดความตื่นตัวในการที่จะเข้าถึงเทคโนโลยีที่ช่วยทำธุรกรรมการเงินผ่านระบบอิเล็กทรอนิกส์มากยิ่งขึ้น เนื่องจากมีความ

สะดวก รวดเร็ว และที่สำคัญคือ ช่วยลดการสัมผัส และลดความเสี่ยงต่อการติดเชื้อในการที่จะต้องออกจากที่พักอาศัยเพื่อไปทำธุรกรรมทางการเงิน ณ ที่ตั้งสำนักงาน หรือสาขาของสถาบันการเงิน อย่างไรก็ตามความสะดวกสบายเหล่านี้ ย่อมมีความล่อแหลมและเสี่ยงต่อระบบรักษาความปลอดภัยทางไซเบอร์ในการที่จะเกิดการรั่วไหล หรือการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต รวมทั้ง การถูกขโมยชุดข้อมูลของลูกค้าจากสถาบันการเงินเพื่อนำไปแลกกับผลประโยชน์ในรูปแบบต่าง ๆ ซึ่งถือเป็นภัยคุกคามต่อระบบการเงินการธนาคารที่สำคัญ และอาจส่งผลกระทบต่อความเชื่อมั่นของประชาชนอย่างหลีกเลี่ยงมิได้

TB-CERT ถือเป็นต้นแบบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านการเงินการธนาคาร ตามที่ได้กำหนดไว้ในมาตรา ๕๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒ เป็นกลไกที่สำคัญยิ่งในการประสานงาน เฝ้าระวัง รับมือ และตอบสนองและแก้ไข ภัยคุกคามทางไซเบอร์ ที่นับวันจะมีแนวโน้มเพิ่มสูงขึ้น และทวีความรุนแรงเพิ่มมากขึ้น จนอาจส่งผลกระทบเป็นวงกว้างต่อภาคธุรกิจในยุคดิจิทัลนี้

ถึงแม้ TB-CERT ซึ่งถือว่าเป็นหนึ่งใน Sectorial-CERT ที่สำคัญ ได้จัดตั้งมาเพียงระยะเวลาไม่นานนัก แต่ด้วยศักยภาพขององค์กรและบุคลากรภายใน TB-CERT จึงสามารถนับได้ว่า TB-CERT เป็นหน่วยงานที่มีความสำคัญต่อระบบเศรษฐกิจของประเทศไทยเป็นอย่างมาก โดยเฉพาะด้านการเงินการธนาคาร ซึ่งถือว่าเป็นเส้นเลือดใหญ่ที่หล่อเลี้ยงการขับเคลื่อนเศรษฐกิจของประเทศไทยในทุกภาคส่วน ผมหวังเป็นอย่างยิ่งว่าท่านผู้บริหารตลอดจนพนักงานเจ้าหน้าที่ TB-CERT ทุกท่านจะช่วยกันขับเคลื่อนองค์กรให้มีความเข้มแข็งและประสานความร่วมมือกับภาคส่วนต่าง ๆ ในการที่จะรักษาไว้ซึ่งความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะในด้านการเงินการธนาคาร เพื่อสร้างความเชื่อมั่นให้กับหน่วยงานทั้งภาครัฐและเอกชน ตลอดจนพี่น้องประชาชนคนไทยทุกคน ในการที่จะดำเนินธุรกรรมผ่านระบบอิเล็กทรอนิกส์ได้อย่างมั่นคงสืบไป

คำนิยม

คุณสิริธิดา พนมวัน ณ อยุธยา
ผู้ช่วยผู้ว่าการ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน
ธนาคารแห่งประเทศไทย (ธปท.)

ปัจจุบันการทำธุรกรรมทางการเงินออนไลน์เข้ามาเป็นส่วนสำคัญในชีวิตประจำวันของประชาชนอย่างปฏิเสธไม่ได้โดยจะเห็นได้จากการทำธุรกรรมโอนเงินและชำระเงินออนไลน์ของคนไทยผ่าน Mobile banking/Internet banking เพิ่มขึ้นกว่า 64% ในปีที่ผ่านมา และในอนาคตเราจะเห็นนวัตกรรมทางการเงินใหม่ๆ ถูกนำมาประยุกต์ใช้ซึ่งจะมีความเชื่อมโยงกับระบบงานผู้ให้บริการต่าง ๆ ที่หลากหลายมากขึ้น เช่น บริการชำระเงินและส่งข้อมูลการค้าสำหรับภาคธุรกิจ (Smart Financial and Payment Infrastructure for Business) การชำระเงินระหว่างประเทศแบบมีผลทันที (Real-time Cross-border payment) เป็นต้น

การนำเทคโนโลยีมาใช้แม้จะช่วยอำนวยความสะดวกได้ดีขึ้น แต่มักจะมาพร้อมกับความเสี่ยงจากภัยคุกคามทางไซเบอร์อย่างหลีกเลี่ยงไม่ได้ ขณะที่พัฒนาการของเทคโนโลยีมีความก้าวหน้าอย่างต่อเนื่อง ภัยไซเบอร์ก็มีการพัฒนาด้วยเช่นกัน ทั้งความซับซ้อนและการถูกนำไปใช้เป็นเครื่องมือในการทำทุจริตทางการเงิน ดังจะเห็นได้จากกรณีการทุจริตบัตรเดบิต/เครดิต แอปพลิเคชันหลอกกู้เงิน หรือ SMS หลอกลวง เป็นต้น ซึ่งภัยเหล่านี้ไม่สามารถจะแก้ไขได้เพียงหน่วยงานใดหน่วยงานหนึ่ง ต้องอาศัยความร่วมมือหลายภาคส่วน ไม่ว่าจะเป็นหน่วยงานกำกับดูแล หน่วยงานด้านธุรกิจ หน่วยงานภาครัฐ รวมทั้งหน่วยงานด้านที่ดูแลความมั่นคงปลอดภัย

ตลอดระยะเวลาที่ผ่านมา TB-CERT ได้แสดงให้เห็นว่าเป็นส่วนสำคัญในการพัฒนาองค์ความรู้ แลกเปลี่ยนประสบการณ์ ร่วมมือแก้ไขปัญหา รวมทั้งให้ความร่วมมือกับ ธปท. และหน่วยงานที่เกี่ยวข้องในการวางรากฐานการพัฒนาการบริหารจัดการความเสี่ยงและการรับมือภัยคุกคามไซเบอร์อย่างต่อเนื่อง ทั้งในด้านพัฒนามาตรฐานหรือกระบวนการในการรับมือภัยไซเบอร์ การสร้างความร่วมมือ และการพัฒนาศักยภาพบุคลากรเชิงลึกผ่านโครงการต่าง ๆ เช่น Cybersecurity Boot Camp และ Tech Career เพื่อสร้างความเข้มแข็งด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ สถาบันการเงิน ระบบการชำระเงิน และเศรษฐกิจไทยอย่างยั่งยืนต่อไป

ดิฉันขอชื่นชมและขอบคุณคณะทำงาน TB-CERT ทุกท่านที่ทุ่มเทและมุ่งมั่นในการสร้างความมั่นคงปลอดภัยให้กับระบบการเงินของไทยอย่างดียิ่งเสมอมา และขออวยพรให้ประสบความสำเร็จในภารกิจของ TB-CERT ในการดูแลความมั่นคงปลอดภัยให้กับระบบการเงินไทยต่อไป

คำนิยม

คุณผยง ศรีวณิช
กรรมการผู้จัดการใหญ่ ธนาคารกรุงไทย
และประธานสมาคมธนาคารไทย

ในยุคที่โลกถูกขับเคลื่อนด้วยเทคโนโลยี และข้อมูลข่าวสาร อินเทอร์เน็ตได้เข้ามาเป็นส่วนหนึ่งของวิถีชีวิตประจำวันมากขึ้น เพราะเทคโนโลยีและนวัตกรรมได้ถูกออกแบบมาเพื่อตอบโจทย์ไลฟ์สไตล์คนยุคดิจิทัลในทุกด้าน รวมถึงด้านบริการทางการเงิน ที่เทคโนโลยีช่วยทำให้ประชาชนทุกกลุ่มเข้าถึงบริการทางการเงินได้สะดวก รวดเร็ว ทุกที่ ทุกเวลา ผ่านบริการ Mobile Banking หรือ Internet Banking ซึ่งมีอัตราการใช้งานเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยเฉพาะในช่วงสถานการณ์การแพร่ระบาดของโควิด-19 บริการดิจิทัลได้เข้ามาตอบโจทย์เรื่องการเว้นระยะห่างทางสังคม การลดใช้เงินสด เพื่อลดความเสี่ยงจากการติดเชื้อ ประกอบกับภาครัฐยังใช้ดิจิทัลแพลตฟอร์ม เป็นกลไกหลักในการขับเคลื่อนมาตรการเยียวยา และกระตุ้นเศรษฐกิจ ทำให้ประชาชนทุกกลุ่มได้เรียนรู้และคุ้นเคยกับการใช้เทคโนโลยีดิจิทัลในการใช้จ่ายในชีวิตประจำวัน อย่างไรก็ตาม ก็มีความเสี่ยงจากจากผู้ไม่หวังดีที่ใช้เทคโนโลยีเป็นเครื่องมือในการแสวงหาผลประโยชน์อันมิชอบ หรือที่เรียกว่าอาชญากรรมทางไซเบอร์ที่มาในทุกรูปแบบและปรับเปลี่ยนวิธีการไปตามยุคสมัย

แม้ว่าทุกหน่วยงานที่เกี่ยวข้องจะพยายามป้องกันอย่างเต็มที่ ไม่ว่าจะด้วยการพัฒนาเทคโนโลยี เครื่องมือ บุคลากร รวมถึงการสร้างความตระหนักรู้เกี่ยวกับภัยไซเบอร์ให้กับประชาชน แต่ภัยไซเบอร์ก็ยังมีให้เห็นอย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งในปีนี้ ภาคธนาคารต้องเผชิญภัยคุกคามทางไซเบอร์ที่รุนแรงซับซ้อนมากขึ้น เพราะจากวิกฤตโควิด-19 ทำให้ผู้คนต้องอาศัยเทคโนโลยีในการใช้ชีวิตมากขึ้น ไม่ว่าจะเป็นการ Work From Home หรือการเข้าถึงบริการต่าง ๆ และด้วยจำนวนอุปกรณ์เชื่อมต่อกับอินเตอร์เน็ตที่มากขึ้น ทำให้บรรดาอาชญากรไซเบอร์มีโอกาสเข้าถึงข้อมูลผ่านอุปกรณ์ต่าง ๆ ได้มากขึ้น จึงเป็นความท้าทายของภาคการเงิน ในการช่วยกันป้องกัน จัดการกับความเสี่ยงด้าน IT และ Cyber Security ให้อยู่ในระดับมาตรฐาน และตอบโจทย์การพัฒนาผลิตภัณฑ์บริการและนวัตกรรมทางการเงินใหม่ ๆ ซึ่งจะเป็นหัวใจสำคัญอย่างยิ่งในการสร้างความเชื่อมั่นต่อระบบการเงินของผู้ใช้บริการ

สำหรับการป้องกันภัยไซเบอร์ภาคการเงินการธนาคารในประเทศไทย ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (Thailand Banking Sector Computer Emergency Response Team) หรือ TB-CERT ซึ่งเป็นศูนย์รวมของบุคคลที่มีความเชี่ยวชาญด้านไซเบอร์ เป็นศูนย์กลางแหล่งให้ความรู้และการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ รวมไปถึงการสร้างความตระหนักในการระวังภัยคุกคามทางไซเบอร์ ได้มีบทบาทสำคัญในการทำงานเชิงรุกร่วมกับธนาคารสมาชิก เพื่อเตรียมความพร้อมทุกด้านในการรับมือกับภัยทางไซเบอร์ โดยเฉพาะการให้ความรู้กับประชาชน และผู้ใช้บริการทางการเงิน ให้รู้เท่าทันกลโกงของมิจฉาชีพ ซึ่งเปรียบเสมือนการฉีดวัคซีนเพื่อสร้างภูมิคุ้มกันสำหรับภัยไซเบอร์ในรูปแบบใหม่ ๆ ให้กับประชาชน และองค์กรต่าง ๆ อยู่เสมอ เพราะการฉีดวัคซีนหรือสร้างภูมิคุ้มกันทางด้านไซเบอร์ที่ดีให้กับองค์กร จะเป็นมาตรการที่ช่วยลดความเสี่ยงและบรรเทาผลกระทบจากการถูกโจมตีในรูปแบบต่าง ๆ ได้ ดังนั้น ภารกิจของ TB-CERT ในการสร้างภูมิคุ้มกันอย่างรอบด้าน ทั้ง Technology, Process และ People ที่ได้ทำอย่างต่อเนื่องกว่า 5 ปีที่ผ่านมา รวมทั้งการให้ความร่วมมือ สร้างมาตรฐาน มีส่วนในการพัฒนาบุคลากรภาคการธนาคาร และสร้างความตระหนักรู้ให้กับภาคประชาชน อย่างไรก็ดี การได้รับความสนับสนุนจากภาคส่วนต่างๆ ที่เป็นจุดเชื่อมโยงในการเข้าถึงบริการต่างๆของภาคธนาคาร ถือเป็นอีกส่วนหนึ่งที่สำคัญยิ่ง ที่จะช่วยสนับสนุน ส่งเสริม ตลอดจนร่วมมือป้องกันภัยทางไซเบอร์ต่างๆ และทั้งหมดทั้งมวลที่ได้กล่าวมานั้น นับได้ว่าเป็นกลไกที่สำคัญที่จะช่วยสร้างความเชื่อมั่นต่อการใช้บริการทางการเงินการธนาคาร และมีส่วนร่วมในการสร้างสังคมยุคดิจิทัลที่เข้มแข็งในระดับประเทศต่อไป

สารจากคณะกรรมการ TB-CERT

คุณชัชวัฒน์ อัศวรักวงศ์
Managing Director and Chief Information Security Officer
ธนาคารกสิกรไทย

"ในยุคดิจิทัลที่เต็มไปด้วย VUCA (Volatility,Uncertainty,Complexity and Ambiguity) นี้ การปรับตัวให้ทันต่อสถานการณ์ และการมี "สติ" เป็นสิ่งจำเป็นอย่างยิ่งยวดที่จะทำให้องค์กรและตัวเรารอดพ้นจากภัยต่างๆ ไม่ว่าจะจากภัย COVID-19 หรือภัยไซเบอร์ ก็ตาม"

…. Stay Safe, Stay Secure …

คุณสมภพ สุรัตนกวีกุล
Director, IT Security Office, Information Technology Department
ธนาคารแห่งประเทศไทย

"ช่วง 2 ปีที่ผ่านมา COVID-19 ทำให้ประชาชนและหน่วยงานต่างต้องปรับวิถีการใช้ชีวิตและการทำงานที่จำเป็นต้องพึ่งพาไอที และ Internet เพิ่มขึ้นอย่างมาก สิ่งหนึ่งที่ตามมาอย่างหลีกเลี่ยงไม่ได้ คือ การเผชิญกับภัยไซเบอร์ที่น่ากลัวและจัดการได้ยากขึ้น TB-CERT ในฐานะที่เป็นตัวกลางความร่วมมือเพื่อป้องกันภัยไซเบอร์และแลกเปลี่ยนข้อมูลของภาคการธนาคารไทย หวังว่าจะสามารถขยายความร่วมมือนี้ไปยังภาคอื่น ๆ ทั้งในและต่างประเทศ และร่วมกันปกป้องผู้ใช้บริการและประชาชนจากภัยไซเบอร์ให้ดียิ่งขึ้นไป"

ดร. กิตติ โฆษะวิสุทธิ์

Senior Vice President and Chief Information Security Officer

ธนาคารกรุงเทพ

Code for Secured Organization

รหัสลับองค์กรปลอดภัย

Collaboration

Openness

Vigilance

Information

Development

คุณนิโรจน์ ผิวพรรณ
First Vice President, IT Security, Technology Group
ธนาคารกรุงไทย

"รู้ทันกันพลาด"...ในยุคปัจจุบันที่ภัยคุกคามทางไซเบอร์มีแนวโน้มทวีความรุนแรงและสามารถสร้างผลกระทบในวงกว้างมากขึ้น นอกเหนือจากประสิทธิภาพของเทคโนโลยีต่าง ๆ ที่นำมาใช้ป้องกันภัยทางไซเบอร์แล้ว สิ่งสำคัญไม่แพ้กันคือความตระหนักรู้และเท่าทันต่อการรับมือภัยคุกคามดังกล่าว ซึ่งสิ่งนี้ไม่ได้เป็นหน้าที่ของหน่วยงานใดหน่วยงานหนึ่ง แต่ถือเป็นสิ่งที่ทุกภาคส่วนต้องให้ความสำคัญและให้ความร่วมมือช่วยกันเพื่อยกระดับความรู้ให้เท่าทันต่อเหตุการณ์และภัยทางไซเบอร์ หากทุกคนมีความรู้เท่าทันต่อภัยทางไซเบอร์แล้วนั้น ก็เปรียบเสมือนได้รับวัคซีนที่ช่วยสร้างภูมิคุ้มกันต่อภัยคุกคามดังกล่าว ซึ่งจะช่วยลดโอกาสในการตกเป็นเป้าการโจมตีจากผู้ไม่ประสงค์ดี หรืออย่างน้อยหากถูกโจมตีก็สามารถลดผลกระทบหรือบรรเทาความเสียหายที่เกิดขึ้นได้ไม่มากก็น้อย

คุณพาวิต ศักดิ์สูง
Head of Digital Technology Security
ธนาคารไทยพาณิชย์

ปีที่ผ่านมาการดำเนินธุรกิจภาคการเงินต่าง ๆ ได้ปรับกลยุทธ์ให้มีความเป็นดิจิทัลและมีบทบาทรองรับการ Work from Anywhere เพิ่มขึ้น ทำให้การกำหนดมาตรการควบคุมความปลอดภัยไซเบอร์ที่สอดคล้องกับความเสี่ยงที่เกี่ยวข้องมีความสำคัญและท้าทายเพิ่มขึ้น โดยเฉพาะการควบคุมการเข้าถึงข้อมูลสำคัญทั้งจากพนักงานและบุคคลภายนอก (Third party) ซึ่งทางภาคการเงินจำต้องมีการติดตามประเมินความเสี่ยงและมาตรการควบคุมทั้งของตัวองค์กรเองและบุคคลภายนอกขององค์กรที่สนับสนุนบริการสำคัญในด้านต่าง ๆ เพื่อให้องค์กรมั่นใจว่าความเสี่ยงด้านไซเบอร์ ด้านความมั่นคงปลอดภัยและการรักษาความลับของข้อมูล ตลอดจนการหยุดชะงักของบริการสำคัญ ได้รับการควบคุมอย่างเหมาะสม

คุณประกลกฤษ แสงชูวงศ์
Team Head of Information Security Detection and Response
ธนาคารทหารไทยธนชาต

ปัจจุบันโลกเรา เป็นโลกยุคดิจิทัล ธุรกิจการค้า การสื่อสาร สามารถดำเนินการได้รวดเร็ว ส่งผลให้ภัยคุกคามยุคดิจิทัลมีความซับซ้อนขึ้น รูปแบบการโจมตีก็ซับซ้อน ดังที่ปรากฏในปีที่ผ่านมา ไม่ใช่แต่อุตสาหกรรมการเงิน การแพทย์ หรือแม้แต่ซัพพลายเชนในอุตสาหกรรมไอที ก็เป็นเป้าหมายในปัจจุบันแล้ว ส่งผลให้เราต้องมีความพร้อมที่จะต่อต้านภัยคุกคามไซเบอร์ได้ตลอดเวลา ความร่วมมือในภาคการธนาคาร ก็มีความสำคัญมาก เพื่อที่จะให้เราก้าวไปข้างหน้าพร้อมกัน และเท่าทันต่อเหตุการณ์ภัยคุกคามได้เท่ากัน ส่งผลให้เกิดความปลอดภัยในระดับชาติอีกด้วย

คุณภคพงศ์ จุลวงศาศิลป์
Head of Cyber Security Department
ธนาคารกรุงศรีอยุธยา

"ในปี 2021 มี 3 Cyber Threat Trends หลัก

"Ransomware Attack" มีบริษัททั่วโลกจำนวนมากได้รับผลกระทบจาก Double-extortion Ransomware ซึ่งมีผลทั้งทำให้ระบบไม่สามารถทำงานได้ และข้อมูลถูกขโมยเพื่อเรียกค่าไถ่ เพื่อลดความเสี่ยงต่อองค์กร องค์กรต้องเตรียมความพร้อมทั้งด้านเครื่องมือป้องกัน, ตรวจจับ, กระบวนการ Incident Response, และการซ้อมรับมือภัยไซเบอร์แบบ Tabletop exercise

"3rd Party Attack" ในบางกรณี การมุ่งเป้าโจมตีไปที่ 3rd party ของธนาคารอาจง่ายกว่าการโจมตีธนาคารโดยตรง และด้วยแนวโน้มปริมาณ 3rd Party ที่ธนาคารมีการใช้บริการมากขึ้น เมื่อ 3rd Party ถูกโจมตีทางไซเบอร์ จึงมีโอกาสส่งผลกระทบมายังธนาคารในหลายด้านขึ้นกับบริการธนาคาร การจัดทำ 3rd Party Inventory ที่มีรายละเอียดเพียงพอ จะเป็นส่วนสำคัญในการเตรียมความพร้อมที่สำคัญ

"Critical Vulnerabilities" ภัยไซเบอร์ที่เกิดจากช่องโหว่ซอฟต์แวร์ที่ส่งผลระดับร้ายแรง มีความจำเป็นเร่งด่วนในการแก้ไข ซึ่งอาจจำเป็นต้องมีกระบวนการจัดการเป็นพิเศษ ทั้งการเฝ้าระวังจาก Threat Intelligence, Software Inventory, และการบริหารจัดการปิดช่องโหว่ (Patch Management) รวมถึง Virtual Patch เพื่อลดความเสี่ยงที่เกิดจากภัยประเภทนี้ที่มีความถี่สูงขึ้น

TB-CERT มีบทบาทสำคัญในการทำงานร่วมกับธนาคารสมาชิกเพื่อเตรียมความพร้อมรับความท้าทาย และรักษาความเชื่อมั่นของประชาชนต่อบริการของธนาคารในภาพรวม"

คุณวชิราวัชร์ มหาทัพกฤษ

Inspector general, Chief Information Security Officer

ธนาคารออมสิน

ความมั่นคงปลอดภัยทางไซเบอร์ มิใช่ธุรกิจที่ต้องแข่งขันทุกวิถีทาง เพื่อความเป็นที่หนึ่ง แต่เป็นสิ่งที่ทุกองค์กร ทุกภาคส่วน ควรให้ความเอื้อเฟื้อ ช่วยเหลือ และให้ความร่วมมือต่อกัน เพื่อความมั่นคงปลอดภัย ต่อการให้บริการประชาชนในภาคอุตสาหกรรมเดียวกัน และต่อประเทศ

Information security SHARING IS THE BEST for all.

คุณยศ กิมสวัสดิ์
Head of Payment System Office
สมาคมธนาคารไทย

ในช่วง 1-2 ปีที่ผ่านมา จะเห็นได้ว่าอัตราการใช้งาน Digital Payment ได้เติบโตขึ้นอย่างอย่างก้าวกระโดด พร้อมกับความตื่นตัวและตระหนักรู้ถึงเทคโนโลยีทั้งในแง่ของประโยชน์และความเสี่ยงจากผู้ไม่หวังดีที่จะหาผลประโยชน์จากช่องโหว่ที่เกิดขึ้น ในแง่ของผู้ให้บริการก็เช่นกัน นอกจากจะมุ่งพัฒนาผลิตภัณฑ์และบริการเพื่ออำนวยความสะดวกสบายให้กับผู้บริโภคแล้ว ยังพัฒนาความร่วมมือให้เกิดขึ้นอย่างเข้มแข็ง สำหรับภาคการธนาคารเองช่วงที่ผ่านมานอกจากจะสร้างความร่วมมือภายในกลุ่ม TB-CERT แล้ว ยังได้มุ่งเน้นถึงความร่วมมือในกลุ่มภาคการเงินร่วมกับภาคการลงทุนและประกันภัยในการเสริมสร้างเกราะป้องกันจากความเสี่ยงด้านภัยคุกคามไซเบอร์รูปแบบต่าง ๆ ไม่ว่าจะเป็นการแลกเปลี่ยนข้อมูลภัยคุกคาม การพัฒนาความรู้และทักษะให้กับบุคลากรทั้งด้าน IT และ Non-IT รวมทั้งความพยายามในการสรรหาบุคลากรด้าน Cybersecurity รุ่นใหม่เข้าสู่อุตสาหกรรม เพื่อให้ภาคการเงินซึ่งมีโครงสร้างพื้นฐานด้านสารสนเทศที่สำคัญ เกิดภูมิคุ้มกันหมู่ในการพร้อมรับมือภัยไซเบอร์ให้มากที่สุด

บทความประจำปี

It's a Journey, Resiliency, and Collaboration

ปี 2021 ที่ผ่านมายังเป็นปีที่ท้าทายมากสำหรับการบริหารจัดการและรับมือกับการระบาดของ COVID-19 ประชาชน และหลายองค์กรทั่วโลกจำเป็นต้องปรับตัวกันอย่างจริงจังเพื่อให้การใช้ชีวิต และการดำเนินธุรกิจเดินหน้าต่อไปได้ในท่ามกลางความไม่แน่นอนในหลาย ๆ ปัจจัย องค์กรส่วนใหญ่ให้พนักงานทำงานจากที่บ้าน (Work From Home) ในช่วงสถานการณ์การแพร่ระบาดรุนแรงของ COVID-19 ด้วยความที่สถานการณ์การระบาดของ COVID-19 ยืดเยื้อ และยังไม่มีใครทราบได้ว่าจะจบลงเมื่อไร การทำงานแบบ Work From Home กลายเป็นวิถีการทำงานแบบใหม่ที่องค์กรต่าง ๆ กำหนดให้เป็นรูปแบบการทำงานปกติไปแล้ว นอกจากนี้ องค์กรต่าง ๆ ยังนำเทคโนโลยีดิจิทัลมาประยุกต์ใช้ให้บริการออนไลน์กันอย่างแพร่หลาย เพื่อคงไว้ซึ่งความสามารถในการแข่งขันในยุคดิจิทัล

การนำเทคโนโลยีดิจิทัล โดยเฉพาะการให้บริการต่าง ๆ ผ่านอินเทอร์เน็ต เป็นการสร้างความได้เปรียบ และเปิดโอกาสในการเข้าถึงลูกค้าเป็นวงกว้าง อีกทั้งยังทำให้พนักงานในองค์กรมีความยืดหยุ่นในการทำงานจากนอกสถานที่ ผ่านอุปกรณ์ต่าง ๆ ที่เชื่อมต่ออินเทอร์เน็ต และทำงานเมื่อไรก็ได้ (Anywhere, Anytime, Any Devices) จึงเป็นประโยชน์ที่องค์กรมองว่าคุ้มค่าต่อการลงทุน และหันมามุ่งเน้นการใช้เทคโนโลยีดิจิทัลกันมากขึ้นแบบก้าวกระโดด

เทคโนโลยีดิจิทัลมีประโยชน์มหาศาล แต่ก็อาจจะก่อให้เกิดความเสียหายได้มากมายเช่นกัน หากองค์กรนำเทคโนโลยีดิจิทัลมาใช้โดยขาดความตระหนักรู้ถึงการดูแลด้านความมั่นคงปลอดภัยไซเบอร์ที่รัดกุม ขาดการป้องกันข้อมูลสำคัญขององค์กร และข้อมูลส่วนบุคคลของลูกค้าที่ดีพอ และจะกลายเป็นการเพิ่มความเสี่ยงต่อองค์กรในการถูกคุกคามหรือโจมตีทางด้านไซเบอร์อย่างคาดไม่ถึง ดังจะเห็นได้จากข่าวเหตุการณ์การโจมตีทางด้านไซเบอร์หลายเหตุการณ์ที่เกิดขึ้นทั่วโลกในปี 2021 เช่น กรณี Colonial Pipeline, Fujifilm, AXA Group และอีกหลาย ๆ องค์กรชั้นนำถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) และถูกขโมยข้อมูลสำคัญไปประกาศขาย ข่าวการค้นพบและประกาศเรื่องช่องโหว่รุนแรงแบบ Zero Day อย่างต่อเนื่อง ทำให้ทีมงานที่ดูแลเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรต่างต้องจัดการช่องโหว่เหล่านั้นแข่งกับเวลากันอย่างไม่หยุดหย่อน ภัยคุกคามทางด้านไซเบอร์ไม่ได้เกิดขึ้นที่ประเทศใดประเทศหนึ่ง

แต่เกิดขึ้นทั่วโลก รวมถึงประเทศไทยด้วยเช่นกัน ภัยไซเบอร์จึงไม่ใช่เรื่องไกลตัวอย่างที่หลาย ๆ คนเข้าใจอีกต่อไป และไม่ได้สร้างผลกระทบแค่เรื่องธุรกรรมทางการเงิน แต่กระทบถึงชื่อเสียงขององค์กร และอาจจะกระทบต่อความปลอดภัยของชีวิตประชาชนได้

ในปีที่ผ่านมา นอกเหนือจากภัยไซเบอร์ที่เกิดขึ้นอย่างต่อเนื่อง ในประเทศไทยยังมีเหตุการณ์ที่เป็นที่จับตามอง และสร้างความกังวลต่อภาคประชาชนอยู่พอสมควร คือเรื่องการทุจริตทางดิจิทัล (Digital Fraud) เช่น ประชาชนบางรายถูกนำข้อมูลบัตรเดบิตไปใช้ทำธุรกรรมออนไลน์ต่าง ๆ จนเป็นข่าวคึกโครมในช่วงปลายปี การถูกหลอกให้กดลิงก์ที่ส่งมาทาง SMS หรืออีเมล เพื่อขอข้อมูลส่วนบุคคล หรือหลอกให้สินเชื่อแบบผิดกฎหมาย หรือแม้กระทั่งการถูกหลอกจากแก๊ง Call Center ที่ยังมีอย่างต่อเนื่อง และหลายรูปแบบ ภัยไซเบอร์และภัยจากการทุจริตทางดิจิทัล (Digital Fraud) ล้วนก่อให้เกิดความเสียหายต่อภาคธุรกิจ ภาคประชาชน อีกทั้งยังส่งผลต่อความเชื่อมั่นในภาครัฐ หน่วยงานกำกับ และการดำรงชีวิตของประชาชน การลงทุน การเติบโตทางเศรษฐกิจของประเทศ ดังนั้น การจัดการ การป้องกัน การตรวจจับเหตุการณ์ และการตอบสนองต่อเหตุการณ์ที่ทันท่วงที รวมถึงการทำงานและความร่วมมือกันของหน่วยงานที่รับผิดชอบในทุกภาคส่วน ทั้งในองค์กร และระหว่างองค์กร จึงเป็นกลไกสำคัญ ที่จะช่วยลดความเสี่ยงจากภัยไซเบอร์และภัยจากการทุจริตทางดิจิทัล ที่จะเกิดขึ้นกับองค์กรและประชาชนได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ในองค์กรให้มีประสิทธิภาพในยุคดิจิทัลนี้ นอกจากต้องยึดหลัก C I A (Confidentiality : การรักษาความลับของข้อมูล Integrity : คงไว้ซึ่งความถูกต้องของข้อมูล และ Availability : ข้อมูลและระบบต้องมีความพร้อมใช้อยู่ตลอดเวลา) แล้ว เรายังต้องคำนึงถึง F S R (Flexibility : ความยืดหยุ่นในการใช้งาน Simplicity : ใช้งานง่าย และ Resiliency : ทนทานต่อการถูกโจมตี) เพื่อตอบโจทย์ผู้ใช้งานในยุคดิจิทัลที่ต้องการความเร็ว ความยืดหยุ่น และยังต้องปลอดภัยด้วย เมื่อเรารวมทั้ง 6 เรื่องมาผสมผสานกัน การจะรักษาไว้ซึ่งความสมดุลเป็นเรื่องที่ค่อนข้างท้าทายเลยทีเดียว แต่โลกหมุนไปทางนี้แล้ว องค์กรต่าง ๆ ต้องหาวิธีที่จะจัดการทั้ง 6 เรื่องนี้ให้ผสมผสาน เหมาะสมกับบริบท และสอดคล้องกับความเสี่ยงที่ยอมรับได้ขององค์กรนั้น ๆ

การป้องกันและรับมือกับภัยไซเบอร์ ไม่ใช่หน้าที่ของคนใดคนหนึ่ง หรือหน่วยงานใดหน่วยงานหนึ่ง แต่เป็นหน้าที่ของทุกภาคส่วน ที่ต้องร่วมมือกัน ทำงานร่วมกันแบบบูรณาการ สำหรับภาคธนาคารนั้น ในปี 2021 Thailand Banking Sector Computer Emergency Response Team (TB-CERT) ได้ผลักดันงานต่าง ๆ ไม่ว่าจะเป็นเรื่องการสร้างความรู้ ความสามารถ ทักษะให้กับบุคลากรของธนาคารสมาชิก และบุคคลทั่วไป ผ่านการจัดงานสัมมนา การจัดงานประชุมเชิงปฏิบัติการต่าง ๆ เป็นศูนย์กลางในการแลกเปลี่ยนด้านข้อมูลเหตุการณ์ผิดปกติด้านภัยไซเบอร์ระหว่างสมาชิก เพื่อให้ธนาคารสมาชิกนำไป

ป้องกันระบบของธนาคารสมาชิกได้แบบเชิงรุก รวมถึงการร่วมกำหนดมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ในหัวข้อต่าง ๆ ร่วมกันกับธนาคารแห่งประเทศไทย เพื่อให้ธนาคารสมาชิกใช้เป็นแนวทางในการปฏิบัติงานอย่างเป็นระบบ นอกเหนือจากการทำงานร่วมกันอย่างใกล้ชิดในภาคธนาคารแล้ว การทำงานร่วมกันกับหน่วยงานที่เกี่ยวข้อง ทั้งภายในประเทศ และต่างประเทศ เป็นเรื่องที่สำคัญ ที่ TB-CERT เดินหน้าผลักดันอย่างต่อเนื่องให้เป็นรูปธรรมมากยิ่งขึ้น

ท้ายสุดนี้ขอให้ทุกท่านใช้ชีวิตอย่างมีสติ นอกเหนือจากการมีเทคโนโลยีที่เพียบพร้อม การมีบุคลากรที่มีทักษะที่ดีแล้ว การมีสติก็เป็นเรื่องสำคัญที่จะทำให้ภาคการเงินการธนาคารของประเทศไทย และพวกเราทุกคนแคล้วคลาดจากภัยไซเบอร์ ภัยทุจริตทางดิจิทัล และภัยจาก COVID-19 และพร้อมจะเดินหน้าสู่ยุคดิจิทัลไปได้อย่างมั่นคงต่อไป ....

ชัชวัฒน์ อัศวรักวงศ์

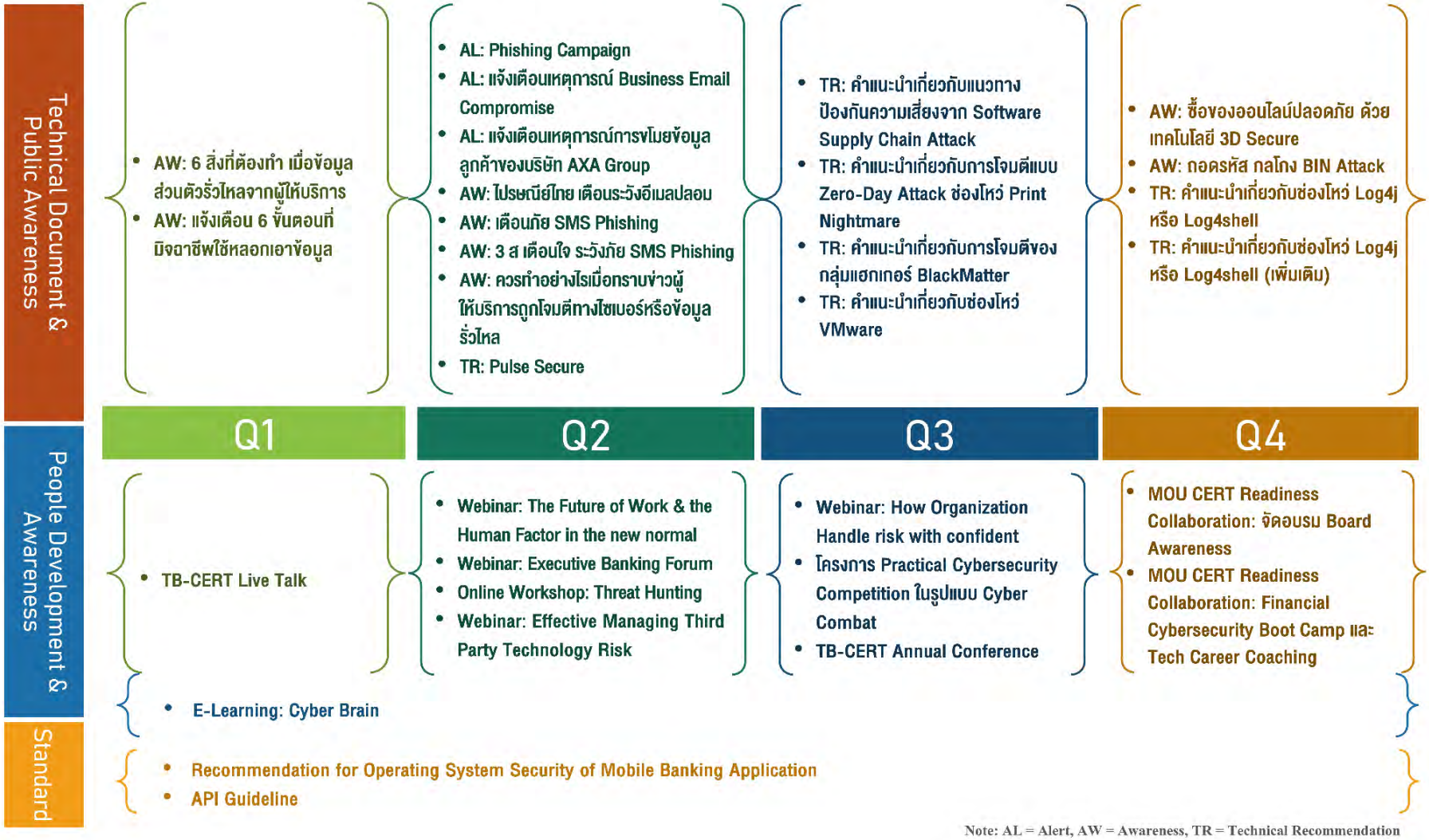
ประธานกรรมการ TB-CERT

บทนำ

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือทีบีเซิร์ต (Thailand Banking Sector CERT: TB-CERT) สมาคมธนาคารไทย มีภารกิจหลายด้านโดยได้มุ่งเน้นที่ 5 ส่วนหลัก ๆ อันได้แก่ 1. พัฒนาบุคลากรด้าน Cybersecurity ของภาคการธนาคาร 2. กำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคการธนาคาร 3. สร้างความตระหนักรู้ถึงภัยคุกคามด้าน Cybersecurity สำหรับสมาชิกและประชาชน 4. ศึกษาและวิจัยเพื่อพัฒนาและสร้างองค์ความรู้ด้าน Cybersecurity ให้กับภาคการธนาคาร 5. ให้บริการแก่ธนาคารสมาชิกในการวิเคราะห์และแจ้งเตือนเพื่อบรรเทาจากเหตุภัยไซเบอร์แบบเชิงรุก ตลอดระยะเวลา 5 ปีของ TB-CERT การรักษาคุณภาพของการเป็น TB-CERT นั้นเป็นสิ่งที่ท้าทายมาก โดยเฉพาะในยุคของ COVID-19 ที่ทำให้กลไกการสร้างเครือข่าย การแลกเปลี่ยนข้อมูล ของสมาชิก TB-CERT นั้นเป็นไปได้อย่างยากลำบากมาก การแลกเปลี่ยนข้อมูลโดยเฉพาะข้อมูลที่มีความอ่อนไหวนั้นเป็นสิ่งที่เกิดขึ้นจากความไว้วางใจของสมาชิกที่เชื่อว่าสมาชิกที่ได้รับข้อมูลจะปฏิบัติต่อข้อมูลหรือข่าวสารนั้นอย่างถูกต้องตามข้อตกลงที่ได้ให้ไว้ร่วมกัน หากขาดความเชื่อใจกันและกันแล้วนั้นจะส่งผลกระทบต่อการแลกเปลี่ยนข้อมูลภายในกลุ่มสมาชิกทันที ดังนั้นในสภาพการณ์ของยุค COVID-19 ที่ทำให้หลาย ๆ หน่วยงาน หลาย ๆ องค์กรต้องปรับตัวในการทำงานกัน และสมาชิกส่วนใหญ่ของ TB-CERT นั้นทำงานในรูปแบบของออนไลน์กันหมด การพบปะพูดคุยกัน การประชุมแบบเจอกันตามสถานที่ต่าง ๆ ก็ถูกตัดไป ทำให้มีความจำเป็นต้องปรับเปลี่ยนรูปแบบกิจกรรมเพื่อให้ยังยึดโยง trust relationship ระหว่างสมาชิก ในขณะที่ยังมีการรับสมาชิกใหม่เข้ามาอย่างต่อเนื่อง ทำให้ความคล่องตัวในการที่จะแลกเปลี่ยนข้อมูลระหว่างสมาชิกซึ่งกันและกันลดลง เพราะเกรงว่าจะส่งผลกระทบต่อองค์กรหากข้อมูลที่อ่อนไหวหลุดออกไป ดังนั้น ความไว้เนื้อเชื่อใจกันที่สมาชิกต้องทำตามข้อกำหนดและหลักปฏิบัติของกลุ่ม จะต้องแข็งแกร่งและยึดมั่นในหลักการแลกเปลี่ยนข้อมูลภายในสมาชิกอย่างเข้มงวด การสร้างความไว้เนื้อเชื่อใจนั้นไม่ได้เกิดขึ้นในวันเดียวหรือการพูดคุยกันเพียงครั้งเดียว หากแต่สิ่งเหล่านั้นล้วนเกิดจากการที่กลุ่มคนเหล่านั้นได้ทำกิจกรรมร่วมกัน ได้พบปะพูดคุยกันแลกเปลี่ยนความรู้และประสบการณ์ร่วมกัน เข้าอกเข้าใจซึ่งกันและกันเป็นระยะเวลาใดเวลาหนึ่ง ตลอดระยะเวลาการทำงานที่ผ่านมา TB-CERT ได้สร้างสายสัมพันธ์ ความไว้วางใจซึ่งกันและกันมาได้เป็นอย่างดี หากแต่สถานการณ์ COVID-19 ที่เกิดขึ้นทั่วโลกที่ทำให้เราต้องปรับเปลี่ยนวิถีการดำเนินชีวิตและการทำงานใหม่อย่างหลีกเลี่ยงไม่ได้ เราไม่สามารถจัดกิจกรรมเพื่อมาพบปะพูดคุยแลกเปลี่ยนข้อมูลกันได้อย่างใกล้ชิดกันอย่างเช่นอดีตที่ผ่านมา จึงเป็นเรื่องที่ท้าทายอย่างยิ่งว่าทำอย่างไรเรายังคงรวมกลุ่มสร้างความสัมพันธ์ที่ดีและรักษาคุณภาพเช่นนี้ไว้ได้ ในปี 2021 TB-CERT ได้

ทำภารกิจหลายอย่างไม่ว่าจะเป็นการจัดสัมมนาออนไลน์รูปแบบใหม่ ๆ ที่ให้ความรู้และความตระหนักรู้ในหลากหลายมิติ การจัดหาแพลตฟอร์มสำหรับสมาชิกเรียนออนไลน์ผ่านโครงการ Cyber Brain ที่จัดทำขึ้นเพื่อพัฒนาทักษะของบุคลากรด้านไอทีให้มีความรู้ความเชี่ยวชาญเฉพาะทางมากขึ้น โดยได้สอดแทรกกิจกรรมระหว่างการเรียนให้กับผู้ที่เข้ามาเรียนด้วย การประชุมสมาชิกประจำเดือน แม้ว่าจะเป็นออนไลน์เราก็ได้เสริมกิจกรรมที่สร้างความคุ้นเคย การพูดคุยแลกเปลี่ยนกันอย่างเป็นกันเองตลอดในทุกเดือน อีกทั้งการจัดตั้งคณะทำงานจากหน่วยงานสมาชิกให้เข้ามามีส่วนร่วมในกิจกรรมต่าง ๆ เช่น Banking Cyber Drill รวมไปถึงการสร้างมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ในหลาย ๆ เรื่อง เช่น API Security Standard และอีกหลากลายกิจกรรมตามภารกิจของ TB-CERT ก็เป็นส่วนหนึ่งของการสร้างความสัมพันธ์ระหว่างสมาชิกให้แน่นแฟ้นยิ่งขึ้น รวมถึงการที่เมื่อเกิดเหตุการณ์โจมตีสำคัญที่เกิดขึ้นกับหน่วยงานภายนอกในประเทศไทย สมาชิกได้มีการปรึกษาหารือกันตลอดและแบ่งปันความรู้ประสบการณ์แนวทางการรับมือได้อย่างน่าชื่นชม ทำให้ทุกคนใน TB-CERT ได้มีการเรียนรู้และยกระดับความมั่นคงปลอดภัยไซเบอร์ไปพร้อม ๆ กัน ทำให้ภาพรวมความมั่นคงปลอดภัยไซเบอร์ระดับภาคการธนาคารนั้นเข้มแข็งขึ้น ตลอดระยะเวลาของปี 2021 ที่ TB-CERT ต้องเผชิญกับความท้าทายดังกล่าวและได้พยายามปรับแนวทางการทำงานให้เป็นวิถีชีวิตใหม่ผ่านกิจกรรมต่าง ๆ นั้นทำให้ผ่านอุปสรรคและความท้าทายนั้นมาได้ คงไว้ซึ่งความเป็นน้ำหนึ่งใจเดียวกันและความไว้เนื้อเชื่อใจกันมาตลอดจนถึงปัจจุบัน

กิจกรรมและผลงานสำคัญในปี 2021

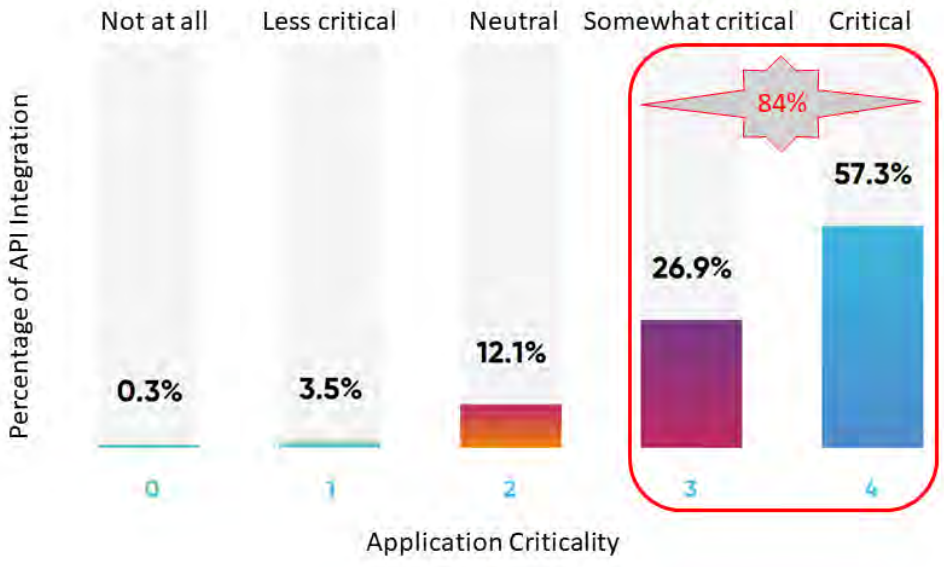


Note: AL = Alert, AW = Awareness, TR = Technical Recommendation

งานด้านมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัย

1. กรอบมาตรฐานด้านความมั่นคงปลอดภัยสำหรับเทคโนโลยี API (API Security Standard)

ในยุคดิจิทัลที่เทคโนโลยีเข้ามามีบทบาทสำคัญในการดำเนินชีวิตประจำวัน ข้อมูลสามารถถูกเปลี่ยนแปลงได้ตลอดเวลาอย่างรวดเร็ว ระบบ ผลิตภัณฑ์ และอุปกรณ์ต่าง ๆ สามารถเชื่อมโยงสื่อสารกันและทำงานร่วมกันได้อย่างอัตโนมัติภายใต้การทำงานของเทคโนโลยีที่เรียกว่า API ซึ่งย่อมาจาก Application Programming Interface นั่นคือ API จะทำหน้าที่เสมือน “ปลั๊ก” สำหรับผู้พัฒนาระบบที่ใช้เชื่อมต่อกันระหว่างอุปกรณ์หรือเชื่อมต่อระหว่างแอปพลิเคชันในการรับส่งข้อมูลและคำสั่งต่าง ๆ ทำให้ทำงานร่วมกันมีความสะดวกและรวดเร็วมากยิ่งขึ้น ส่งผลให้การใช้เทคโนโลยี API มีการเติบโตที่เพิ่มสูงขึ้นและนำไปสู่การพัฒนาสิ่งใหม่ ๆ และการเปลี่ยนแปลงอย่างรวดเร็ว



รูปที่ 1 แสดงสัดส่วนร้อยละการใช้งาน API Integration บนระบบงานสำคัญ

อ้างอิง: ที่มา The State of API Integration Report 2020

จากรูปที่ 1 อ้างอิงผลสำรวจจากรายงาน The State of API Integration ปี 2020 พบว่า องค์กรมีการใช้งาน API Integration ในระบบงานที่มีความสำคัญสูงถึงร้อยละ 84 และในจำนวนนั้นร้อยละ 60 เป็นการใช้เทคโนโลยี API ที่เกี่ยวข้องกับการเชื่อมต่อระหว่างองค์กรไปยังระบบคลาวด์ ในขณะที่บทบาทการใช้งาน API มีจำนวนเพิ่มสูงขึ้นและมีความสำคัญมากขึ้น แต่ในส่วนของผู้พัฒนา API อาจไม่ได้คำนึงถึงความเสี่ยงที่อาจเกิดจากภัยคุกคามทางไซเบอร์ ทำให้ขาดความระมัดระวังด้านการควบคุมความมั่นคงปลอดภัยในการใช้งาน API อย่างเหมาะสม จากสถิติภัยคุกคามทางไซเบอร์ที่เกิดขึ้นช่วง 2 ปีที่ผ่านมา พบว่าแนวโน้มภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับการใช้งาน API มีอัตราเพิ่มสูงขึ้นและส่งผลกระทบก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร รวมถึงส่งผลกระทบก่อให้เกิดความเสียหายกับข้อมูลของลูกค้าในวงกว้าง ทั้งนี้ TB-CERT เล็งเห็นความสำคัญของเทคโนโลยี API ที่เข้ามามีบทบาทอย่างมากในอุตสาหกรรมภาคการธนาคารในประเทศไทย เพื่อให้องค์กรสามารถออกแบบและพัฒนาการใช้งาน API ที่มีการควบคุมด้านความมั่นคงปลอดภัยที่เหมาะสมเพียงพอ สามารถป้องกันภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นจากการใช้งาน API และทำให้เกิดการยกระดับด้านความมั่นคงปลอดภัยสำหรับผู้ให้บริการ API ที่เป็นมาตรฐานเดียวกัน ในปี 2021 TB-CERT ได้จัดตั้งกลุ่มคณะทำงาน API Security ประกอบด้วยบุคลากรที่มีความรู้ ความเชี่ยวชาญและมีประสบการณ์เกี่ยวกับการออกแบบและพัฒนา API รวมถึงบุคลากรทางด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศจากหน่วยงานสมาชิก เพื่อร่วมมือกันจัดทำกรอบมาตรฐานด้านความมั่นคงปลอดภัยของ API หรือ API Security Standard

จากการทำงานร่วมกันของคณะทำงาน API Security Standard ได้รวบรวมลักษณะของ API ที่องค์กรให้บริการหรือมีการใช้งานอยู่ โดยแต่ละลักษณะของ API ที่ให้บริการก็จะมีระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่แตกต่างกัน สามารถสรุปเป็นปัจจัยความเสี่ยงพื้นฐาน 5 ด้าน ได้แก่

ปัจจัยความเสี่ยงด้านที่ 1: การเปิดเผย API Specification เป็นปัจจัยเสี่ยงโดยพิจารณาถึงขอบเขตการเปิดเผย API Specification ที่ให้บริการ เช่น

1.1 ขอบเขตการเปิดเผย API Specification เฉพาะภายในองค์กร คือ API Specification ที่ไม่ได้เปิดเผยให้นิติบุคคล หรือบุคคลภายนอก

1.2 ขอบเขตการเปิดเผย API Specification ระหว่างองค์กรที่เกี่ยวข้อง คือ API Specification ที่มีการควบคุมการเปิดเผยต่อนิติบุคคล หรือบุคคลภายนอก

1.3 ขอบเขตการเปิดเผย API Specification ให้กับสาธารณะ คือ API Specification ที่มีการเปิดเผยต่อสาธารณะโดยทั่วไป

ซึ่งแต่ละแบบอาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในรูปแบบที่แตกต่างกันตามปัจจัยแวดล้อม เช่น การเปิดเผยค่าพารามิเตอร์ในการใช้งานและการทำงานของแอพพลิเคชันสู่สาธารณะ ซึ่งอาจก่อให้เกิดความเสี่ยงด้านไซเบอร์ที่สูงกว่า API Specification ที่เปิดเผยในวงจำกัด

ปัจจัยความเสี่ยงด้านที่ 2: ลักษณะข้อมูลการให้บริการ เป็นปัจจัยเสี่ยงโดยพิจารณาถึงลักษณะของข้อมูลที่ให้บริการด้วย API หมายถึงการให้สิทธิ์แก่ผู้ใช้บริการ API ในการเข้าถึงข้อมูลลักษณะต่าง ๆ ได้แก่

2.1 ข้อมูลสาธารณะ เช่น ข้อมูลรายละเอียดของบริการ ข้อมูลช่วงเวลาที่เปิดให้บริการ ข้อมูลค่าธรรมเนียมการใช้บริการ และข้อมูลสาขาที่ให้บริการ เป็นต้น

2.2 ข้อมูลที่เกี่ยวข้องกับธุรกรรมของธนาคาร เช่น ข้อมูลรายละเอียดการโอนเงิน/การชำระเงิน ข้อมูลเกี่ยวกับข้อมูลส่วนบุคคล (PII) เป็นต้น

2.3 ข้อมูลสำคัญ ข้อมูลส่วนบุคคลที่อ่อนไหว หรือข้อมูลที่มีชั้นความลับระดับสูงสุดขององค์กร เช่น PIN/Password ข้อมูล Biometric หรือ แผนกลยุทธ์การตลาดขององค์กร เป็นต้น เพราะข้อมูลแต่ละแบบอาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับความรุนแรงที่แตกต่างกันไปตามความสำคัญของข้อมูลนั้น

ปัจจัยความเสี่ยงด้านที่ 3: สิทธิ์สำหรับการดำเนินการ เป็นปัจจัยเสี่ยงโดยพิจารณาถึงการให้สิทธิ์การดำเนินการแก่ผู้ใช้บริการ API กล่าวถึงการกำหนดสิทธิ์ให้ผู้ใช้บริการ API เช่น ให้สามารถอ่านข้อมูลได้อย่างเดียว หรือให้สามารถอ่านและเขียนข้อมูลได้ และการให้สิทธิ์ในการบริหารจัดการสิทธิ์ได้ เช่น การเปลี่ยนแปลงแก้ไขสิทธิ์การเข้าใช้งานจากสิทธิ์ผู้ใช้งานเป็นสิทธิ์ของผู้ดูแลระบบ เป็นต้น ทั้งนี้หากการเรียกใช้งาน API มีการกำหนดสิทธิ์อนุญาตให้ทำงานตามฟังก์ชันที่แตกต่างกัน อาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในรูปแบบและระดับความรุนแรงที่แตกต่างกันไป ตามสิทธิ์สำหรับการดำเนินการที่อนุญาตให้เข้าถึงการใช้บริการ API นั้น ๆ

ปัจจัยความเสี่ยงด้านที่ 4: ลักษณะการเชื่อมต่อ เป็นปัจจัยเสี่ยงโดยพิจารณาถึงลักษณะการติดต่อสื่อสารหรือการเชื่อมต่อ API ผ่านเครือข่ายประเภทต่าง ๆ ทั้งภายในและภายนอกองค์กร เช่น การเชื่อมต่อเครือข่ายภายในองค์กร การเชื่อมต่อเครือข่ายภายนอกองค์กรที่มีการจำกัดการเข้าถึง และการเชื่อมต่อเครือข่ายภายนอกองค์กรแบบสาธารณะที่ไม่มีการจำกัดการเข้าถึง ซึ่งลักษณะการเชื่อมต่อรูปแบบต่าง ๆ มีการควบคุมความปลอดภัยที่แตกต่างกัน อาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในรูปแบบและระดับความรุนแรงที่แตกต่างกันไป

ปัจจัยความเสี่ยงด้านที่ 5: ปริมาณข้อมูล เป็นปัจจัยเสี่ยงโดยพิจารณาถึงขนาดของข้อมูลที่เกี่ยวข้องสำหรับการใช้งาน API เช่น การระบุปริมาณจำนวน Records ของ Data source หรือ ขนาดของ Data source สำหรับใช้งาน API เป็นต้น โดยปริมาณข้อมูลขนาดใหญ่อาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับความรุนแรงที่สูงกว่าการให้บริการ API ที่มีปริมาณข้อมูลขนาดเล็กกว่า ทั้งนี้หลักเกณฑ์การพิจารณาปริมาณข้อมูลควรสอดคล้องตามนโยบายของแต่ละองค์กร

จากลักษณะการให้บริการ API ตามปัจจัยพื้นฐาน 5 ด้านที่กล่าวข้างต้น สามารถนำมาพิจารณาระดับความเสี่ยง 3 ระดับ ได้แก่ ต่ำ ปานกลาง สูง สรุปเป็นตารางได้ดังนี้

ปัจจัย	ระดับความเสี่ยง		
	ต่ำ	ปานกลาง	สูง
1. การเปิดเผย API Specification			
2. ลักษณะข้อมูลการให้บริการ			
3. สิทธิ์สำหรับการดำเนินการ			
4. ลักษณะการเชื่อมต่อ			
5. ปริมาณข้อมูล			

ตารางที่ 1 แสดงปัจจัยและระดับความเสี่ยง 3 ระดับ ต่ำ ปานกลาง สูง

เพื่อให้การควบคุมด้านความมั่นคงปลอดภัยของ API มีความเหมาะสมสอดคล้องกับความเสี่ยงตามปัจจัยพื้นฐานของ API ที่ใช้งานจริง การกำหนดแนวทางปฏิบัติการควบคุมด้านความมั่นคงปลอดภัยควรอ้างอิงตามระดับความเสี่ยงของปัจจัยพื้นฐานนั้น โดยมีกรอบมาตรฐานด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการพัฒนา API มาทั้งหมด 7 หลักการ ประกอบด้วย

หลักการที่ 1: กระบวนการยืนยันตัวตน (Authentication) เพื่อควบคุมการเข้าถึงข้อมูล และป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การบริหารจัดการกระบวนการยืนยันตัวตน ประกอบด้วย การสร้าง บริหารจัดการ การแสดงผล เพิกถอน ต่ออายุ และการให้สิทธิ์อย่างเหมาะสมปลอดภัย สำหรับปัจจัยที่ใช้ในการยืนยันตัวตน โดยมีแนวปฏิบัติดังต่อไปนี้

1.1 มีกลไกการยืนยันตัวตนผู้ใช้งานในระดับ Application authentication เพื่อให้สามารถควบคุมและระบุตัวตนในระดับ Client หรือ User ที่เรียกใช้งานเข้ามา ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

1.2 มีกลไกการยืนยันตัวตนผู้ใช้งานในระดับ Server authentication เพื่อตรวจสอบความถูกต้องของผู้ให้บริการว่าเป็นผู้ให้บริการตัวจริงก่อนเรียกใช้บริการต่าง ๆ เช่น การตรวจสอบใบรับรองอิเล็กทรอนิกส์ (Certificate)

1.3 มีการออกแบบการใช้งาน Token อย่างปลอดภัย (Token strength) เช่น การใช้งาน Token แบบใช้ครั้งเดียวหรือ กำหนดอายุการใช้งานของ Token แบบจำกัด (Short-lived token) รวมถึงการเลือกใช้ Strong encryption algorithm สำหรับการสร้าง Token

1.4 มีกลไกการยืนยันตัวตนโดยการใช้ Token ที่มีการลงนามทางดิจิทัล (Digitally signed) หรือจากแหล่งตรวจสอบที่เชื่อถือได้ (Authoritative source)

1.5 มีการใช้ Multi-Factor authentication เพิ่มความมั่นคงปลอดภัยของกระบวนการยืนยันตัวตนเพื่อป้องกันการเข้าถึงบัญชีผู้ใช้โดยไม่ได้รับอนุญาต

หลักการที่ 2: กระบวนการตรวจสอบสิทธิ์การใช้งาน (Authorization) เพื่อกำหนดทรัพยากรที่ผู้ใช้บริการสามารถเข้าถึงได้ ได้แก่ ความสามารถในการจัดการทรัพยากรและการกำหนดสิทธิ์ รวมถึงควบคุมการเข้าถึงได้เฉพาะข้อมูลที่มีสิทธิ์เท่านั้น หรือเฉพาะฟังก์ชันที่กำหนดเท่านั้น โดยมีแนวปฏิบัติดังต่อไปนี้

2.1 มีการกำหนดสิทธิ์หรือระบุขอบเขตฟังก์ชันของ API ที่อนุญาตให้ใช้งานอย่างชัดเจนตามหลักการ “Least privilege” และ “Deny all access by default”

2.2 มีกลไกการตรวจสอบสิทธิ์การขอดำเนินการในทุกฟังก์ชันอย่างชัดเจน

2.3 การออกแบบ Token ต้องเป็นค่าที่ไม่สามารถคาดเดาได้

2.4 มีการกำหนดขอบเขตการร้องขอการใช้งานในวงจำกัด เพื่อลดความเสี่ยงที่อาจเกิดขึ้น โดยการจำกัดเฉพาะ IP address และ Port ที่อนุญาตเชื่อมต่อ หรือการจำกัดการเชื่อมต่อด้วยอุปกรณ์ปลายทางที่ได้รับอนุญาตเท่านั้น เป็นต้น

หลักการที่ 3: การรักษาความลับของข้อมูลและการคงความถูกต้องสมบูรณ์ของข้อมูล (Data Confidentiality and Integrity) เพื่อควบคุมการเข้าถึงข้อมูล เพื่อคงความลับของข้อมูล และเพื่อคงความถูกต้องสมบูรณ์ของข้อมูลไม่ให้ถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต ซึ่งเป็นการป้องกันข้อมูลสำคัญรั่วไหล เช่น ข้อมูล Credential, ชื่อ-สกุล, เลขบัตรประชาชน เป็นต้น โดยมีแนวปฏิบัติดังต่อไปนี้

3.1 มีการป้องกันการฝังข้อมูลสำคัญ (Sensitive Information) ใน Source Code และใน Audit Log

3.2 มีการป้องกันไม่ให้มีการเปิดเผยข้อมูลจากการประมวลผลเกินความจำเป็น (Excessive Data Exposure)

3.3 มีการเข้ารหัสข้อมูลในระดับเครือข่าย (Network Layer Standard and Strong Encryption)

3.4 มีการเข้ารหัสข้อมูลในระดับแอปพลิเคชัน (Application Layer Standard and Strong Encryption) และป้องกันข้อมูลถูกเปลี่ยนแปลงแก้ไข เช่น การทำ Hash+Salt หรือ Signing เพื่อตรวจสอบความถูกต้องของข้อมูล เป็นต้น

หลักการที่ 4: การรักษาความมั่นคงปลอดภัยด้านการสื่อสาร (Secure Communication) เพื่อป้องกันการถูกขโมย ดักจับ หรือรั่วไหลของข้อมูลระหว่างการส่งผ่านในช่องทางการสื่อสาร โดยมีแนวปฏิบัติดังต่อไปนี้

4.1 มีกลไกการเชื่อมต่อบนระบบเครือข่ายการเข้ารหัสอย่างปลอดภัยตามมาตรฐานสากล (Transport Layer Security)

4.2 มีการเชื่อมต่อเครือข่ายการเข้ารหัสด้วยการใช้งาน Strong cipher suite และยกเลิกการใช้งาน Weak cipher suite

4.3 มีกลไกการตรวจสอบใบรับรอง Certificate จากแหล่งตรวจสอบที่เชื่อถือได้ (Local Trusted CA) เช่น Certificate ที่ออกโดยผู้ให้บริการใบรับรองที่ได้รับการรับรองจากผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (National Root Certification Authority of Thailand) หรือ Enterprise Trusted CA ที่ออกโดยหน่วยงานภายในองค์กร เป็นต้น

4.4 มีกลไกการตรวจสอบใบรับรอง Certificate จากแหล่งตรวจสอบที่เป็นมาตรฐานสากล (Global Trusted CA) เช่น Certificate ที่ออกโดยหน่วยงานสากล เป็นต้น

4.5 มีแนวทางในการป้องกันความเสี่ยงที่เกิดจากภัยคุกคามประเภท MITM (Man In The Middle) เช่น mutual TLS, Certificate Pinning เป็นต้น

หลักการที่ 5: การพัฒนาโปรแกรมและการกำหนดค่าที่ปลอดภัย (Secure Coding and Configuration) เพื่อเป็นมาตรฐานด้านความมั่นคงปลอดภัยในการพัฒนาระบบเทคโนโลยีสารสนเทศ ช่วยลดความเสี่ยงที่อาจเกิดภัยคุกคามทางไซเบอร์ได้ โดยยึดหลักการกำหนดให้มีการใช้งานเฉพาะเท่าที่จำเป็นและตรวจสอบความถูกต้องของข้อมูลทั้งก่อนและหลังการประมวลผล โดยมีแนวปฏิบัติดังต่อไปนี้

5.1 มีการตรวจสอบ Input Validation ทั้งในส่วนของ Client และ Server เพื่อป้องกันการใส่ค่าไม่ตรงกับเงื่อนไข หรือ ป้องกันการโจมตีแบบ Injection

5.2 มีการตรวจสอบการแสดงผลลัพธ์ของการประมวลผลให้อยู่ในรูปแบบที่ถูกต้อง (Output Encoding) และมีการกำหนดขอบเขตการแสดงผล เพื่อป้องการการโจมตีแบบ Injection และการเปิดเผยข้อมูลที่มากเกินไป

5.3 มีการจัดการการแสดงความผิดพลาดของระบบ (Error Message Handling) เพื่อไม่ให้เปิดเผยข้อมูลเชิงเทคนิคที่สำคัญของระบบ เช่น ชื่อฐานข้อมูล , โครงสร้างข้อมูล , โครงสร้าง Source code, หมายเลข IP ภายใน และ ชื่อรุ่นของซอฟต์แวร์ที่ใช้ เป็นต้น

5.4 มีการกำหนด HTTP Request Method ที่อนุญาตให้ดำเนินการได้ และปิด HTTP Request Method อื่นที่ไม่จำเป็น

5.5 มีการตั้งค่า CORS (Cross-Origin Resource Sharing) อย่างปลอดภัย เพื่อป้องกันไม่ให้มีการละเมิดการเข้าถึงข้อมูลจากโดเมนอื่นที่ไม่ได้รับอนุญาต

หลักการที่ 6: การจัดเก็บข้อมูลบันทึกเหตุการณ์ และการเฝ้าระวัง (Audit Log and Monitoring) เพื่อใช้เป็นข้อมูลในการเฝ้าระวังและตรวจสอบเหตุการณ์ต่าง ๆ ที่อาจมีความผิดปกติเกิดขึ้น รวมถึงการปฏิบัติตามข้อกำหนดตามกฎหมายทางคอมพิวเตอร์ โดยมีแนวปฏิบัติดังต่อไปนี้

6.1 การจัดเก็บ Log ต้องปฏิบัติตามนโยบายการเก็บรักษาข้อมูลขององค์กรและปฏิบัติตามด้วยกฎหมาย รวมถึงข้อบังคับที่เกี่ยวข้อง เช่น จะต้องเก็บรักษาข้อมูลบันทึกเหตุการณ์ไว้ไม่ต่ำกว่า 90 วัน หรืออาจจะมากกว่า ขึ้นกับนโยบายของทางองค์กร

6.2 การจัดเก็บ Log ต้องมีการควบคุมการเข้าถึง เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลง แก้ไข หรือทำลาย

6.3 การจัดเก็บ Log ต้องพิจารณาถึงความสมบูรณ์ของข้อมูลที่ถูกบันทึก เพื่อให้สามารถใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานตามกฎหมาย

6.4 มีกระบวนการหรือเครื่องมือสำหรับตรวจสอบและวิเคราะห์ข้อมูลความมั่นคงปลอดภัยระบบเครือข่ายขององค์กร

หลักการที่ 7: ความเพียงพอของทรัพยากร (Resource Sufficiency) เพื่อให้การจัดการทรัพยากรเป็นไปอย่างมีประสิทธิภาพ ป้องกันการใช้งานทรัพยากรที่มากเกินไปที่อาจส่งผลทำให้การบริการหยุดชะงักได้ โดยมีแนวปฏิบัติดังต่อไปนี้

7.1 มีการตั้งค่า Timeout เพื่อป้องกันระบบหยุดชะงักจากทรัพยากรที่ถูกจองให้คงค้างในปริมาณมาก

7.2 มีการตั้งค่า Throttling หรือ Rate Limit เพื่อป้องกันระบบหยุดชะงักจากการถูกเรียกใช้งาน API ในปริมาณมาก

7.3 มีแนวทางในการตัดการเชื่อมต่อ (Circuit Breaker) เพื่อลดและป้องกันปัญหาจากการเกิดผลกระทบสืบเนื่อง จากปัญหาการใช้งานในปริมาณมาก เช่น การปิดบางบริการเพื่อลดปัญหาจากการเรียกใช้งานในปริมาณมาก เป็นต้น รวมทั้ง แนวทางการกลับมาเปิดให้บริการเมื่อสถานการณ์กลับมาสู่ภาวะปกติ

7.4 มีแนวทางในการป้องกันความเสี่ยงที่เกิดจาก API DDoS ระดับ Network layer หรือระดับ Application layer เพื่อป้องกันการหยุดชะงักของ API Server จากการถูกโจมตี

จากกรอบมาตรฐานด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการพัฒนา API ทั้ง 7 หลักการที่กล่าวมาข้างต้น ในแต่ละหลักการประกอบด้วยแนวทางปฏิบัติที่องค์กรสามารถนำไปประยุกต์ใช้อ้างอิงตามระดับความเสี่ยงจากลักษณะปัจจัยพื้นฐานทั้ง 5 ด้าน เพื่อให้ธนาคารสามารถใช้เป็นหลักเกณฑ์สำหรับการพัฒนา API ในองค์กร รวมถึงใช้เป็นข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยให้กับผู้ใช้งาน API ที่เชื่อมต่อกับระบบของธนาคาร เพื่อให้เกิดการยกระดับความมั่นคงปลอดภัยเกี่ยวกับการใช้งาน API ในภาคการธนาคารต่อไป

2. การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management)

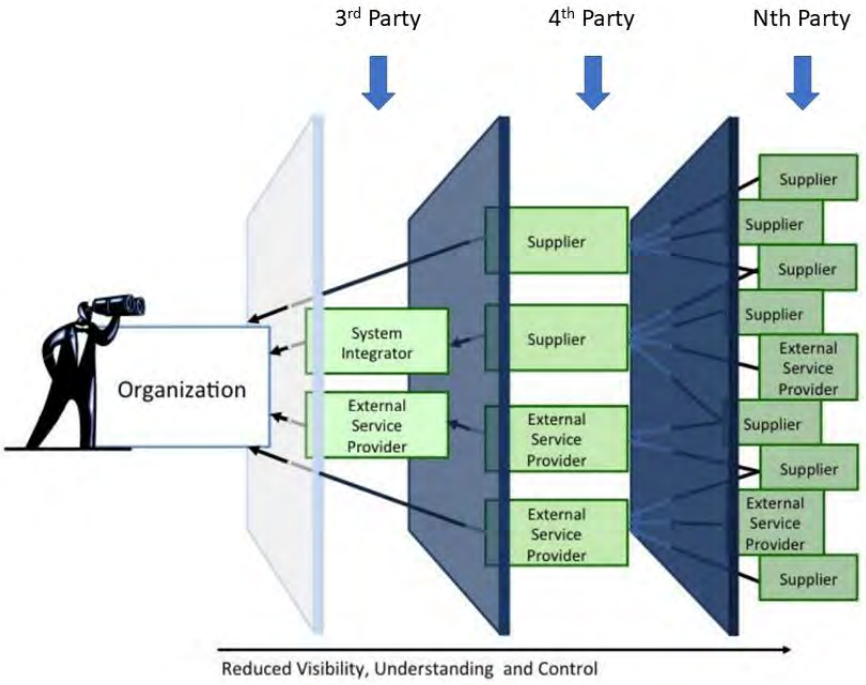
ในยุค Digital Transformation คือการนำเทคโนโลยีดิจิทัลเข้ามาประยุกต์ใช้งานเพื่อสร้างสิ่งใหม่ ๆ หรือการนำเทคโนโลยีดิจิทัลเข้ามาใช้งานเพื่อปรับปรุงการดำเนินงานให้สอดคล้องกับการเปลี่ยนแปลงที่เกิดขึ้นอยู่ตลอดเวลา รวมถึงความจำเป็นด้านการวิเคราะห์ข้อมูลธุรกิจร่วมกันระหว่างองค์กรเพื่อกำหนดการให้บริการผลิตภัณฑ์ที่เหมาะสม ตอบโจทย์การดำเนินธุรกิจตามการเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็ว สามารถให้บริการผลิตภัณฑ์ได้อย่างรวดเร็วและมีประสิทธิภาพมากที่สุด ทำให้การเลือกใช้บริการและการทำความร่วมมือกับบุคคลภายนอกเข้ามามีบทบาทมากขึ้น อย่างไรก็ตามหากบุคคลภายนอกนั้นดำเนินการบางอย่างผิดพลาด หรือมีกระบวนการควบคุมมาตรฐานการดำเนินงานที่ต่ำกว่ามาตรฐานขององค์กร สิ่งเหล่านี้ก่อให้เกิดความเสี่ยงที่สำคัญหลายประการและอาจส่งผลกระทบมาสู่องค์กรได้ เช่น ความเสี่ยงด้านปฏิบัติการ (Operation Risk) กรณีที่บุคคลภายนอกเกี่ยวข้องกับการดำเนินงานขององค์กรและไม่สามารถดำเนินการให้บริการตามที่ได้ทำสัญญาไว้ ความเสี่ยงด้านกฎหมายและข้อกำหนด (Compliance Risk) กรณีบุคคลภายนอกละเลยการปฏิบัติตามกฎระเบียบข้อบังคับ และกระบวนการภายในที่องค์กรต้องปฏิบัติตามสำหรับดำเนินธุรกิจ ความเสี่ยงด้านชื่อเสียง กรณีการดำเนินงานของบุคคลภายนอกเกี่ยวข้องกับการรับรู้ขององค์กรหรือให้บริการในนามขององค์กร อาจกระทำการบางอย่างที่ส่งผลกระทบต่อชื่อเสียงขององค์กรได้ และความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยภัยคุกคามทางไซเบอร์ที่มีโอกาสเกิดขึ้นตลอดเวลา หากบุคคลภายนอกไม่มีกระบวนการด้านการควบคุมความปลอดภัยที่เป็นมาตรฐาน หรือขาดการดูแลความปลอดภัยการใช้งานระบบที่มีช่องโหว่ ก็อาจส่งผลกระทบให้เกิดความเสียหายแก่ระบบหรือข้อมูลขององค์กรได้ เป็นต้น จากตัวอย่างความเสี่ยงเหล่านี้สะท้อนให้เห็นว่าการบริหารจัดการความเสี่ยงจากบุคคลภายนอกเป็นเรื่องสำคัญที่แต่ละองค์กรควรต้องพิจารณา และมีความเกี่ยวข้องกับหลายหน่วยงานทั่วทั้งองค์กร

เพื่อให้รับทราบถึงความเสี่ยงที่อาจจะเกิดขึ้น และสามารถควบคุมความเสี่ยงด้านต่าง ๆ อย่างเหมาะสม เอกสารฉบับนี้จะกล่าวถึงกรอบการบริหารจัดการความเสี่ยงจากบุคคลภายนอกและความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระบบห่วงโซ่อุปทาน (Supply Chain)

ขอบเขตความสัมพันธ์ของบุคคลภายนอก

บุคคลภายนอกในที่นี้หมายถึงผู้ขาย ผู้ผลิต ผู้รับเหมา คู่ค้าพันธมิตร รวมถึงบุคคลภายนอกที่มีสิทธิ์เข้าถึงข้อมูลภายในของบริษัท ข้อมูลลูกค้า หรือข้อมูลที่เป็นเอกสิทธิ์อื่น ๆ ขององค์กร สามารถเข้าถึงระบบหรือเป็นส่วนหนึ่งของขั้นตอนกระบวนการทำงานของบริษัทได้ และในความเป็นจริงองค์กรสามารถทำงานร่วมกันกับบุคคลภายนอกมากกว่า 1 ราย หรือมีความสัมพันธ์กับบุคคลภายนอกมากกว่า 1 รายต่อการพัฒนา

ผลิตภัณฑ์หรือบริการใด ๆ ก็ตาม ตั้งแต่กระบวนการติดต่อผู้ขายหรือผู้ผลิต เพื่อสร้างวัตถุดิบจนเข้าสู่กระบวนการผลิตด้วยเทคโนโลยีต่าง ๆ การจัดเก็บ จนถึงขั้นตอนการนำเสนอผลิตภัณฑ์ส่งถึงมือลูกค้า ทั้งหมดนี้เป็นขอบเขตความสัมพันธ์ของบุคคลภายนอก ซึ่งเป็นการสร้างระบบห่วงโซ่อุปทาน (Supply Chain)



รูปที่ 2 แสดงความสัมพันธ์ระหว่างองค์กรกับบุคคลภายนอกในระบบห่วงโซ่อุปทาน (Supply Chain)
อ้างอิง: ที่มา Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST.SP.800-161

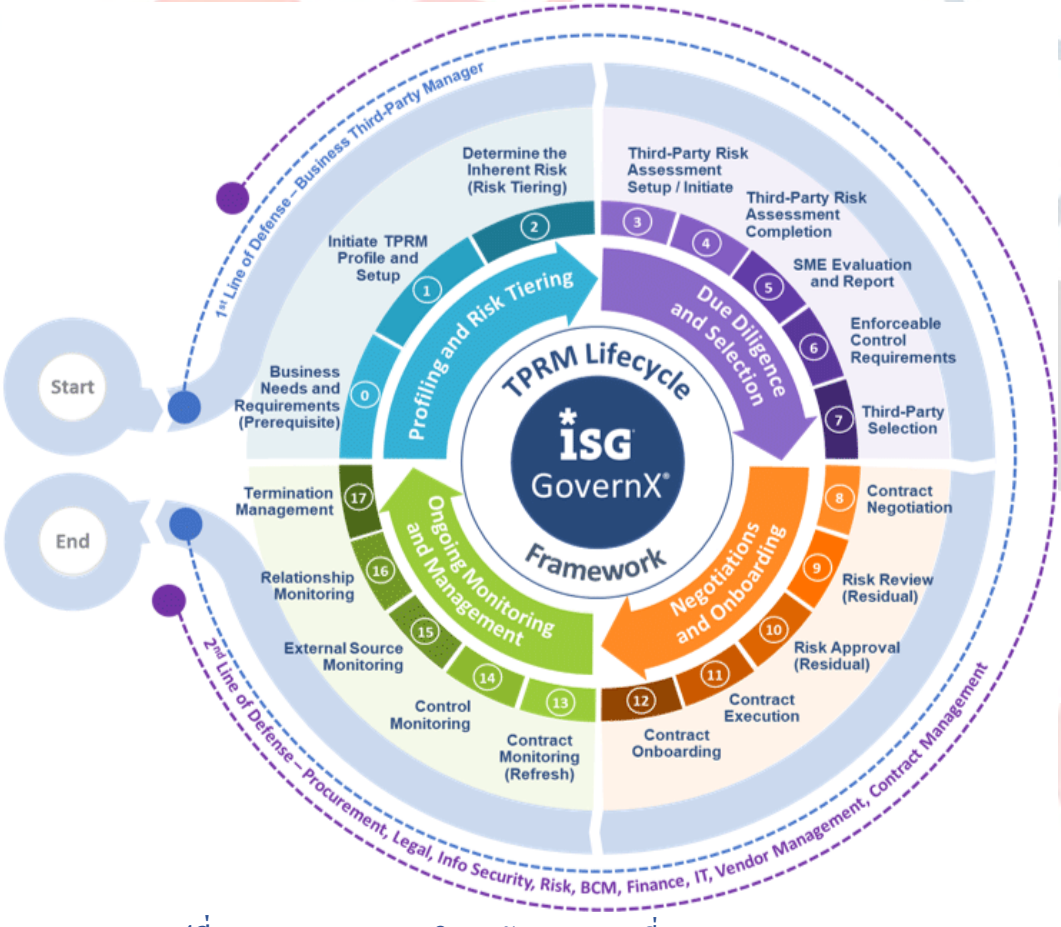
เมื่อบุคคลภายนอกเข้ามามีบทบาทสำคัญในการสนับสนุนผลิตภัณฑ์และบริการต่าง ๆ เพื่อให้องค์กรสามารถดำเนินงานให้บรรลุตามเป้าหมายที่ได้วางไว้ และบุคคลภายนอกตลอดทั้งระบบห่วงโซ่อุปทานสามารถมีความสัมพันธ์กันมากกว่า 1 ราย จากรูปที่ 2 แสดงให้เห็นถึงความสัมพันธ์ระหว่างองค์กรกับบุคคลภายนอกในระบบห่วงโซ่อุปทาน กำแพงขั้นที่ 1 คือการเชื่อมต่อหรือการทำงานที่มีความเกี่ยวข้องกันโดยตรงระหว่างองค์กรกับบุคคลภายนอกที่ถูกเรียกว่า บุคคลที่สาม (3rd Party) ในขั้นนี้องค์กรจะสามารถเห็นบุคคลภายนอกที่มีความเกี่ยวข้องโดยตรงอย่างชัดเจนที่สุด ลำดับถัดไปกำแพงขั้นที่ 2 คือการเชื่อมต่อหรือการทำงานระหว่างบุคคลภายนอกที่เป็นบุคคลที่สามกับบริษัทอื่นที่ทำงานร่วมกันภายใต้ชื่องาน บริการหรือผลิตภัณฑ์เดียวกันเพื่อที่จะส่งมอบให้กับองค์กร บุคคลภายนอกที่อยู่ภายใต้กำแพงขั้นที่ 2 นี้จะถูกเรียกว่า บุคคลที่สี่ (4th Party) เนื่องจากการทำงานระหว่างองค์กรกับบุคคลที่สี่ไม่ได้ติดต่อกันโดยตรง ดังนั้นการดำเนินงานในส่วนของบุคคลที่สี่นี้ องค์กรอาจจะไม่รับทราบหรือไม่สามารถมองเห็นได้ และยิ่งไปกว่านั้นอาจจะมีบริษัทอื่น ๆ ที่มีความเกี่ยวข้องและมาทำงานร่วมกันอยู่เบื้องหลังบุคคลที่สี่ในระดับชั้นที่ลึกลงไป จากรูปที่ 2 ลำดับชั้นที่ N จะถูกเรียกว่า Nth Party หมายถึงระดับชั้นของบุคคลภายนอกที่อยู่เบื้องหลังในลำดับที่ลึกถัดลงไป ความซับซ้อนของการทำงานหรือการให้บริการจากบุคคลภายนอกเหล่านี้ทำให้การระบุ

ความเสี่ยงจากบุคคลภายนอกเป็นเรื่องที่ท้าทาย ยกตัวอย่างความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หากองค์กรขาดความเข้าใจความเสี่ยงด้านเทคโนโลยีที่สอดคล้องภายใต้ผลิตภัณฑ์ที่ดำเนินงานร่วมกับบุคคลภายนอก ซึ่งอาจเป็นช่องทางทำให้ผู้โจมตีสามารถใช้ประโยชน์ได้ กล่าวคือในขณะที่องค์กรมีมาตรการรักษาความปลอดภัยทางไซเบอร์ที่รัดกุมและแผนการแก้ไขป้องกันภัยคุกคามไซเบอร์ที่แข็งแกร่ง แต่สำหรับบุคคลภายนอกอาจไม่ได้รักษามาตรการความปลอดภัยอยู่ในระดับมาตรฐานเดียวกัน การโจมตีไปยังช่องโหว่ของบุคคลภายนอกจึงอาจเกิดขึ้นได้ง่ายกว่า ทำให้เป็นสาเหตุของภัยคุกคามไซเบอร์ที่เกิดจากบุคคลภายนอกได้ ดังนั้นการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของทั้งระบบห่วงโซ่อุปทานจึงจำเป็น เพื่อทำให้มั่นใจว่ากระบวนการรักษาความปลอดภัยนั้นครบถ้วนสมบูรณ์

ดังนั้น คำนิยามของความเสี่ยงจากบุคคลภายนอก (Third Party Risk) คือ ความเสี่ยงใด ๆ ที่เกิดจากบุคคลภายนอกทั้งระบบห่วงโซ่อุปทาน ครอบคลุมถึงบุคคลภายนอกอื่น ๆ ที่อาจเกี่ยวข้องในการจัดหาผลิตภัณฑ์หรือบริการขององค์กร บุคคลภายนอกที่มีการแลกเปลี่ยนข้อมูลที่สำคัญเชิงธุรกิจกับองค์กร โดยมีสิทธิ์เข้าถึงระบบหรือมีข้อมูลขององค์กร และส่งผลกระทบมาสู่องค์กร ก่อให้เกิดภัยคุกคามที่มีความสำคัญ โดยอาจเกิดขึ้นกับทั้งข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลทางการเงิน หรือการดำเนินงานบนระบบห่วงโซ่อุปทานขององค์กรได้

กรอบการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Framework)

จากรูปที่ 3 แสดงภาพรวมองค์ประกอบที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงจากบุคคลภายนอก โดยครอบคลุมวัฏจักรการบริหารจัดการบุคคลภายนอก (Third Party Management Lifecycle) ตั้งแต่การจัดหา และการทำสัญญาไปจนถึงการตรวจสอบ และการตัดสินใจของระดับผู้บริหาร ความสัมพันธ์ในกระบวนการบริหารจัดการความเสี่ยงขององค์กร การกำหนดกรอบงานความเสี่ยงตามกลยุทธ์ของทั้งองค์กร การติดตามมาตรการควบคุม การบริหารความเสี่ยงด้านระบบปฏิบัติการ ทั้งหมดนี้เกี่ยวข้องกับการดำเนินงานทั้งภายในและภายนอก รวมถึงความสัมพันธ์ระหว่างบุคคลภายนอก วัฏจักรของการบริหารจัดการความเสี่ยงจากบุคคลภายนอกในแต่ละองค์กรอาจมีความแตกต่างกันในรายละเอียดตามแต่กลยุทธ์และนโยบายขององค์กรนั้น ๆ อย่างไรก็ตามองค์ประกอบพื้นฐานสำคัญที่ทุกองค์กรต้องคำนึงถึงในกระบวนการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ประกอบด้วย 4 ขั้นตอน ได้แก่



รูปที่ 3 แสดงกรอบการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

(Third Party Risk Management Framework)

อ้างอิง: ที่มา https://isg-one.com/articles/managing-enterprise-risk-the-tprm-lifecycle-framework

ขั้นตอนที่ 1 Profiling and Risk Tiering คือกระบวนการระบุและกำหนดขอบเขตความเสี่ยงที่เกี่ยวข้องกับบุคคลภายนอก ข้อกำหนดแผนธุรกิจ กำหนดความต้องการในด้านต่าง ๆ เช่น ด้านกระบวนการด้านบริการ ด้านผลิตภัณฑ์ เป็นต้น รวมถึงข้อการกำหนดของสัญญาธุรกิจ การกำหนดทีมงานผู้ดูแลรับผิดชอบด้านปฏิบัติงานตามบทบาท เพื่อทำหน้าที่สำคัญในการระบุ ประเมิน จัดการ และควบคุมความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้บริการจากบุคคลภายนอก ผลที่ได้จะนำไปใช้เพื่อประเมินความเสี่ยงที่มาพร้อมกับความต้องการนั้น ๆ และแบ่งระดับความเสี่ยงตามลักษณะบริการจากบุคคลภายนอก ซึ่งในองค์กรขนาดใหญ่อาจมีบุคคลภายนอกที่เกี่ยวข้องในจำนวนค่อนข้างมาก การจัดระดับความเสี่ยงเหล่านี้จะทำให้องค์กรสามารถที่จะบริหารจัดการการใช้บริการจากบุคคลภายนอกได้อย่างมีประสิทธิภาพ ทั้งนี้ควรจะนำเอาปัจจัยพื้นฐานดังต่อไปนี้มาใช้ในการประเมินความเสี่ยงดังกล่าว

ปัจจัยพื้นฐานในการประเมินความเสี่ยงการใช้บริการจากบุคคลภายนอก

1. **การเข้าถึงข้อมูล (Access to Information)** เพื่อระบุความเสี่ยงของวิธีและช่องทางในการเข้าถึงข้อมูล

2. **ชั้นความลับของข้อมูล (Information Classification) ที่ใช้ในการประมวลผล** เพื่อระบุระดับชั้นความลับของข้อมูลที่ใช้ในการประมวลผลซึ่งจะนำไปสู่ระดับความเสี่ยงในการประมวลผลดังกล่าว
3. **ความพร้อมใช้งาน (Availability)** เพื่อใช้ในการประเมินความเสี่ยงที่อาจจะเกิดจากการที่ข้อมูลสูญหาย หรือไม่พร้อมเมื่อต้องการใช้งาน
4. **ขอบเขต หรือปริมาณสินทรัพย์ที่เกี่ยวข้อง (Assets Associated/Volume)** เพื่อใช้ประเมินระดับความเสี่ยงจากปริมาณสินทรัพย์ที่อยู่ภายในกรอบการให้บริการของบุคคลภายนอกซึ่งจะเชื่อมโยงไปสู่ระดับผลกระทบต่อองค์กรผู้ว่าจ้างหากเกิดเหตุการณ์

องค์กรจะต้องพิจารณากำหนดหลักเกณฑ์ความเสี่ยงตามแต่ละปัจจัยข้างต้นโดยนำเอาค่าความเสี่ยงที่องค์กรสามารถรับได้ (Risk Appetite) ในการจัดแบ่งระดับขั้นความเสี่ยง เพื่อให้มีความสอดคล้องกับการลงทุนทรัพยากรที่จำเป็น รวมถึงมีความสอดคล้องกับทิศทางการดำเนินการทางธุรกิจ

ขั้นตอนที่ 2 Due Diligence and Selection คือกระบวนการคัดกรองความเสี่ยงจากบุคคลภายนอกเชิงลึกด้านต่าง ๆ ตั้งแต่กลยุทธ์นโยบายของบริษัทบุคคลภายนอก ชื่อเสียง ความมั่นคงทางการเงิน มาตรการควบคุมความปลอดภัยด้านเทคโนโลยีสารสนเทศ มาตรการบริหารจัดการความเสี่ยง การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือต่อภัยหรือเหตุการณ์ต่าง ๆ เป็นต้น โดยผู้เชี่ยวชาญแต่ละด้านจะรับบทบาทเป็นผู้ประเมินการตอบกลับจากแบบสอบถามการคัดกรองความเสี่ยงของบุคคลภายนอก สิ่งสำคัญคือบุคคลภายนอกที่ถูกจัดอยู่ในระดับความเสี่ยงสูงควรจะต้องได้รับการตรวจสอบเพิ่มเติมและติดตามการดำเนินงานอย่างใกล้ชิด เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นและทำให้การบริหารจัดการความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ แนวปฏิบัติเพื่อให้เกิดการคัดกรองความเสี่ยงจากบุคคลภายนอกอย่างมีประสิทธิภาพ คือ

(1) ทำความเข้าใจเกี่ยวกับกับความสัมพันธ์ระหว่างองค์กรและบุคคลภายนอกที่องค์กรได้ดำเนินงานร่วมกันอยู่ ยิ่งองค์กรมีความเข้าใจในความสัมพันธ์ระหว่างบุคคลภายนอกชัดเจนเท่าไหร่ สิ่งนี้จะเป็นสิ่งสำคัญที่จะช่วยให้การคัดกรอง ตรวจสอบ และวิเคราะห์ความเสี่ยงจากบุคคลภายนอกนั้นได้อย่างถูกต้องครบถ้วนและมีประสิทธิภาพ เป็นพื้นฐานสำคัญสำหรับการบริหารจัดการความเสี่ยงในลำดับถัดไป การไม่เข้าใจในความสัมพันธ์ระหว่างองค์กรและบุคคลภายนอก อาจทำให้องค์กรไม่สามารถวิเคราะห์ความเสี่ยงได้อย่างถูกต้อง หรืออาจขาดการวิเคราะห์ความเสี่ยงในบางเรื่องได้

(2) ประเมินความเสี่ยงจากบุคคลภายนอกตามกลุ่มความสำคัญหรือตามลักษณะความเสี่ยงที่ได้จัดกลุ่มไว้ อย่างที่กล่าวไปข้างต้นว่าบุคคลภายนอกทุกรายไม่ได้มีความสำคัญหรือความเสี่ยงเท่ากัน บุคคลภายนอกที่อยู่ในระดับความสำคัญสูงหรือความเสี่ยงสูง จะต้องได้รับการติดตามการดำเนินงานอย่างใกล้ชิด

(3) ดำเนินการตรวจคัดกรองและวิเคราะห์บุคคลภายนอกตามกลุ่มโปรไฟล์ที่ได้จัดไว้ บุคคลภายนอกที่มีความเสี่ยงสูงกว่าจะถูกตรวจสอบและวิเคราะห์ข้อมูลอย่างละเอียดถี่ถ้วนมากกว่าบุคคลภายนอกที่มีความเสี่ยงต่ำ

(4) กำหนดแผนการติดตามการดำเนินงานของบุคคลภายนอกอย่างต่อเนื่อง เนื่องจากความเสี่ยงจากบุคคลภายนอกมีแนวโน้มที่จะเปลี่ยนแปลงเมื่อเวลาผ่านไป ดังนั้นการติดตามการดำเนินงานของบุคคลภายนอกอย่างต่อเนื่อง จะช่วยให้สามารถรับทราบถึงการเปลี่ยนแปลงที่เกี่ยวข้องกับความเสี่ยงที่อาจเกิดขึ้นอย่างรวดเร็ว

พัฒนาระบบการจัดการบุคคลภายนอก การทำงานด้วยระบบการจัดการบุคคลภายนอกจะช่วยปรับปรุงประสิทธิภาพการทำงานของพนักงานในองค์กร ช่วยลดโอกาสที่พนักงานจะทำงานผิดพลาดหรือมีพฤติกรรมไม่เหมาะสม ช่วยให้เกิดความเป็นธรรมและความสม่ำเสมอในกระบวนการคัดกรอง และยังช่วยให้กระบวนการคัดกรองสามารถควบคุมได้จากส่วนกลาง มีศูนย์รวมการบันทึก การตรวจสอบ และการวิเคราะห์สถานะบุคคลภายนอกทั้งหมดขององค์กร

(5) ประเมินกระบวนการตรวจสอบและวิเคราะห์สถานะของบุคคลภายนอกอีกครั้งเมื่อเวลาผ่านไป นั่นคือ เมื่อเวลาผ่านไปองค์กรอาจเผชิญกับความต้องการหรือความท้าทายใหม่ ๆ ที่เกี่ยวข้องกับความสัมพันธ์ของบุคคลภายนอก อาจทำให้มีการปรับปรุงรายละเอียดการตรวจสอบคัดกรอง มีการระบุประเด็นข้อกังวลใหม่ ๆ ดังนั้นจึงควรดำเนินการตรวจสอบและวิเคราะห์สถานะบุคคลภายนอกสม่ำเสมอ เพื่อให้มั่นใจว่าความเสี่ยงที่เกี่ยวข้องกับองค์กรนั้นถูกนำมาพิจารณาอย่างครบถ้วน

ขั้นตอนที่ 3 Negotiations and Onboarding ประกอบด้วย (1) กระบวนการจัดทำสัญญาหรือข้อตกลง (2) การประเมินความเสี่ยงที่เหลืออยู่ และ (3) การเชื่อมต่อหรือการเข้าถึงข้อมูลโดยบุคคลภายนอก

(1) กระบวนการจัดทำสัญญาหรือข้อตกลง ข้อสัญญาควรระบุลักษณะและขอบเขตของการมีส่วนร่วม การมีสิทธิ์ในทรัพย์สินทางปัญญา การมีสิทธิ์ในการตรวจสอบ การรักษาความลับ และความเป็นส่วนตัวของข้อมูล ทั้งหมดเหล่านี้ควรระบุในเอกสารสัญญาเป็นลายลักษณ์อักษร

(2) การประเมินความเสี่ยงที่เหลืออยู่ ผลการประเมินความเสี่ยงที่เหลืออยู่ คือ ความเสี่ยงสุดท้ายที่ยังคงอยู่หลังจากพิจารณาการควบคุมด้านความปลอดภัยแล้ว และการประเมินความเสี่ยงควรดำเนินการอย่างสม่ำเสมอตามความถี่ที่เหมาะสม เพื่อให้แน่ใจว่าการควบคุมที่บังคับใช้นั้นเพียงพอต่อการจัดการและลดความเสี่ยงที่อาจเกิดขึ้นได้

(3) การเชื่อมต่อหรือการเข้าถึงข้อมูลโดยบุคคลภายนอก การเชื่อมต่อกับบุคคลภายนอกถือเป็นกระบวนการสำคัญในโครงสร้างการพัฒนาระบบขององค์กรในระยะยาว จึงควรต้องดำเนินการอย่างถูกต้องและมีแนวปฏิบัติที่เหมือนกันทั่วทั้งองค์กร

โดยทั่วไปข้อตกลงที่ถูกกำหนดในสัญญาจะเป็นข้อกำหนดจากสัญญามาตรฐาน อย่างไรก็ตาม สัญญาจะต้องถูกเปลี่ยนแปลงเมื่อการเจรจามีความคืบหน้า ถือเป็นส่วนสำคัญของกระบวนการเพื่อให้แน่ใจว่าความต้องการของทุกฝ่ายที่เกี่ยวข้องได้รับการพิจารณาและถูกจัดการเรียบร้อย หัวข้อต่อไปนี้คือสิ่งที่ควรนำมาพิจารณาเจรจาตามความต้องการขององค์กร ได้แก่

1. มาตรฐานประสิทธิภาพ หรือข้อตกลงระดับการให้บริการ (SLA)
2. ข้อกำหนดด้านความมั่นคงปลอดภัยและการรักษาความลับ
3. ขั้นตอนการตรวจสอบและวิเคราะห์สถานะของการปฏิบัติงาน
4. เงื่อนไขและราคา
5. การยกเลิกใช้งาน หรือใช้บริการ

ขั้นตอนที่ 4 Ongoing Monitoring and Management คือกระบวนการติดตามสถานะของการปฏิบัติงานและการบริหารจัดการประสิทธิภาพการปฏิบัติงานตามข้อตกลงที่กำหนดไว้ในสัญญากับบุคคลภายนอก นอกจากนั้นกระบวนการติดตามความเสี่ยงเป็นส่วนที่สำคัญของการจัดการความเสี่ยงของบุคคลภายนอกให้มีประสิทธิภาพ สำหรับระบบหรือบริการที่มีความสำคัญควรมีการติดตาม ตรวจสอบความเสี่ยงและมาตรการควบคุมที่ครอบคลุมในรายละเอียดที่มากขึ้น รวมถึงติดตามและตรวจสอบการจัดการอื่น ๆ ที่เกี่ยวข้องกับบุคคลภายนอก ได้แก่ การบริหารจัดการสัญญา การจัดเตรียมกระบวนการ เครื่องมือ สิ่งที่ส่งมอบ ภาระผูกพัน การเปลี่ยนแปลงต่าง ๆ และการตรวจสอบสิ่งที่ได้รับตามที่ได้กำหนดไว้ในสัญญา สุดท้ายคือการจัดการเกี่ยวกับกระบวนการยกเลิกการใช้บริการหรือยกเลิกความร่วมมือระหว่างกันกับบุคคลภายนอก รวมถึงการทำลายข้อมูล การโอนระบบหรือบริการไปยังบุคคลภายนอกรายอื่น เพื่อให้เกิดการยุติความสัมพันธ์หรือการยกเลิกใช้บริการของบุคคลภายนอกอย่างมีประสิทธิภาพ กระบวนการติดตามและตรวจสอบอย่างต่อเนื่องควรพิจารณาเรื่องดังต่อไปนี้

1. การจัดการเกี่ยวกับการกำหนดค่าต่าง ๆ (Configuration management) และกระบวนการควบคุมด้านความปลอดภัยขององค์กร
2. การประเมินความเสี่ยงสำหรับการเปลี่ยนแปลงต่อระบบ และต่อสภาพแวดล้อมที่เกี่ยวข้องกับการทำงานนั้น
3. การประเมินการควบคุมตามที่กำหนดอย่างต่อเนื่อง
4. การรายงานผลด้านการรักษาความปลอดภัยและนโยบายความเป็นส่วนตัวต่อเจ้าหน้าที่ที่เกี่ยวข้องอย่างเหมาะสม
5. การมอบอำนาจให้เจ้าหน้าที่มีส่วนร่วมอย่างจริงจังในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวอย่างต่อเนื่อง

นอกจากกระบวนการต่าง ๆ ที่กล่าวมาข้างต้นเป็นสิ่งที่ควรต้องพิจารณาเกี่ยวกับการบริหารจัดการความเสี่ยงจากบุคคลภายนอกแล้วนั้น ยังมีกฎหมายหรือระเบียบข้อบังคับปฏิบัติอื่นที่เกี่ยวข้อง เช่น กฎหมายเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายเรื่องการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายเรื่องการป้องกันและปราบปรามการฟอกเงิน ที่องค์กรต้องขยายแนวทางปฏิบัติในการบริหารความเสี่ยงไปยังความสัมพันธ์กับบุคคลภายนอกด้วย เพื่อให้การบริหารจัดการความเสี่ยงจากบุคคลภายนอกเป็นไปอย่างมีประสิทธิภาพและประสิทธิผลยิ่งขึ้น

แนวโน้มผลกระทบที่เกิดขึ้นต่อองค์กรในปัจจุบันมีสาเหตุมาจากบุคคลภายนอกในอัตราที่สูงขึ้น ดังนั้นการสร้างความเข้าใจเกี่ยวกับความเสี่ยงจากบุคคลภายนอกจึงเป็นเรื่องที่หลายองค์กรและหลายหน่วยงานให้ความสำคัญ ทั้งหน่วยงานด้านความมั่นคงปลอดภัย หน่วยงานด้านความเสี่ยง และหน่วยงานด้านกำกับดูแล เป็นต้น จากที่กล่าวมาข้างต้นเป็นกรอบการบริหารจัดการความเสี่ยงบุคคลภายนอก เพื่อให้เกิดความเข้าใจและตระหนักเกี่ยวกับการบริหารจัดการความเสี่ยงบุคคลภายนอกตามกรอบการบริหารจัดการความเสี่ยง

3. มาตรฐานด้านความมั่นคงปลอดภัยระบบปฏิบัติการโทรศัพท์มือถือสำหรับโมบายแบงก์กิ้งแอปพลิเคชัน

บริการธนาคารออนไลน์ผ่านแอปพลิเคชันบนโทรศัพท์มือถือได้รับความนิยมในการใช้งานเพิ่มสูงขึ้นอย่างต่อเนื่องในยุคปัจจุบัน ทั้งนี้ TB-CERT ได้เล็งเห็นถึงความสำคัญในเรื่องการดูแลความปลอดภัยของระบบปฏิบัติการโทรศัพท์มือถือที่ให้บริการสำหรับโมบายแบงก์กิ้งแอปพลิเคชัน จึงได้พัฒนาเอกสารเกี่ยวกับการกำหนดมาตรฐานความปลอดภัยของโทรศัพท์มือถือที่อนุญาตให้ผู้ใช้บริการสามารถติดตั้งโมบายแบงก์กิ้งแอปพลิเคชันได้ เผยแพร่วันที่ 10 พฤษภาคม 2021 เอกสารฉบับนี้มีวัตถุประสงค์เพื่อแสดงให้เห็นถึงความเสี่ยงด้านความปลอดภัยของระบบปฏิบัติการในกรณีที่ผู้ใช้บริการใช้งาน โมบายแบงก์กิ้งแอปพลิเคชันบนระบบปฏิบัติการที่ล้าสมัยหรือไม่มีการสนับสนุนจากเจ้าของผลิตภัณฑ์ เพื่อให้เกิดความเข้าใจและมีแนวทางป้องกันเบื้องต้นในระหว่างการวางแผนอัปเดตระบบปฏิบัติการให้ทันสมัยในเวลาที่เหมาะสม โดยแนวทางการพิจารณามาตรฐานความปลอดภัยได้อ้างอิงข้อมูลจากการพัฒนาแอปพลิเคชัน OWASP Mobile Application Security Verification Standard (MASVS) และการทดสอบความปลอดภัย OWASP Mobile Security Testing Guide (MSTG) ที่สอดคล้องกับเทคโนโลยีและแนวโน้มภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในปัจจุบันและอนาคต

เกณฑ์การประเมินเวอร์ชันของระบบปฏิบัติการขั้นต่ำที่ธนาคารอนุญาตให้ใช้งานโมบายแบงก์กิ้งแอปพลิเคชัน พิจารณาจากปัจจัยที่ใช้ป้องกันภัยคุกคามทางไซเบอร์ที่มีผลต่อการใช้งาน โมบายแบงก์กิ้งแอปพลิเคชันอย่างปลอดภัย ประกอบด้วย

1. **ความปลอดภัยในการรับส่งข้อมูล** เนื่องด้วยการทำงานของโมบายแบงก์กิ้งแอปพลิเคชันจะต้องมีการรับส่งข้อมูลระหว่างเครื่องโทรศัพท์มือถือของผู้ใช้งานและระบบผู้ให้บริการของธนาคารผ่านเครือข่ายอินเทอร์เน็ต ซึ่งอาจเกิดความเสี่ยงที่ข้อมูลสำคัญจะถูกดักจับหรือถูกเปลี่ยนแปลงแก้ไขได้ ดังนั้นอุปกรณ์โทรศัพท์มือถือที่ใช้งานจะต้องรองรับโพรโทคอลที่ได้มาตรฐานความปลอดภัยเพียงพอ

2. **ความปลอดภัยในการจัดเก็บข้อมูลบนเครื่องโทรศัพท์มือถือ** เนื่องจากข้อมูลที่เก็บบนอุปกรณ์โทรศัพท์มือถือมีความสำคัญ ดังนั้นการจัดเก็บข้อมูลและการบริหารจัดการข้อมูลบนโทรศัพท์มือถือจึงจำเป็น ควรเลือกใช้เทคโนโลยีการเข้ารหัสข้อมูลบนอุปกรณ์ที่เหมาะสม หากแอปพลิเคชันมีความจำเป็นต้องเก็บข้อมูลสำคัญ ข้อมูลเหล่านั้นก็ควรต้องเก็บอยู่ในพื้นที่บันทึกข้อมูลที่ปลอดภัย (Secure Storage Device)

3. **ความปลอดภัยของระบบปฏิบัติการ** โดยพิจารณาจากความรุนแรงของช่องโหว่ที่เกิดขึ้นและการดูแลแก้ไขช่องโหว่นั้น ๆ หากระบบปฏิบัติการเวอร์ชันใดที่ล้าสมัย หรือไม่มีการสนับสนุนจากเจ้าของ

ผลิตภัณฑ์ และมีช่องโหว่ระดับรุนแรง (Critical) ที่อาจส่งผลทำให้เกิดการทำงานข้ามสิทธิ์ (Bypass Authorization) หรือทำให้แอปพลิเคชันอื่นมีสิทธิ์สามารถรันข้าม Sandbox ได้ ระบบปฏิบัติการเวอร์ชันนั้นก็ไม่ควรถูกอนุญาตให้ติดตั้งและใช้งานโมบายแบงก์กิ้งแอปพลิเคชันได้

4. **ความปลอดภัยของเทคโนโลยีที่ใช้ในการพัฒนาแอปพลิเคชัน** กล่าวคือเทคโนโลยี ไลบรารี หรือคอมโพเนนท์ที่ใช้พัฒนาแอปพลิเคชันอาจมีช่องโหว่ เช่นการใช้งานคอมโพเนนท์ WebView ในการพัฒนาแอปพลิเคชัน หากเทคโนโลยี ไลบรารี หรือคอมโพเนนท์ที่นำมาใช้พัฒนาแอปพลิเคชันมีช่องโหว่ระดับรุนแรงที่ไม่สามารถแก้ไขได้ ส่งผลทำให้ผู้ใช้งานโมบายแบงก์กิ้งแอปพลิเคชันมีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ได้ ดังนั้นระบบปฏิบัติการเวอร์ชันที่มีช่องโหว่ระดับรุนแรงนี้จึงไม่ควรจะถูกอนุญาตให้ติดตั้งและใช้งานโมบายแบงก์กิ้งแอปพลิเคชัน

จากปัจจัยที่ใช้ป้องกันภัยคุกคามทางไซเบอร์ที่มีผลต่อการใช้งานโมบายแบงก์กิ้งแอปพลิเคชัน อย่างปลอดภัยที่กล่าวมาข้างต้น สามารถสรุปเวอร์ชันขั้นต่ำของแต่ละระบบปฏิบัติการได้ดังนี้

ปัจจัยพิจารณา	ตัวเลือกที่ใช้พิจารณา
ความปลอดภัยในการรับส่งข้อมูล	TLS 1.2
ความปลอดภัยในการจัดเก็บข้อมูลบนโทรศัพท์มือถือ	KeyChain
	KeyStore
ความปลอดภัยของระบบปฏิบัติการ	Sandbox ที่ไม่มีช่องโหว่ระดับรุนแรง
ความปลอดภัยของเทคโนโลยีที่ใช้ในการพัฒนาแอปพลิเคชัน	WebView ที่ไม่มีช่องโหว่ระดับรุนแรง

ดังนั้นแม้ว่าธนาคารจะสามารถอนุญาตให้ผู้ใช้บริการใช้งานโมบายแบงก์กิ้งแอปพลิเคชันบนระบบปฏิบัติขั้นต่ำที่ไม่มีการสนับสนุนจากเจ้าของผลิตภัณฑ์ หรือเรียกว่าล้าสมัยนั้น แต่ในเวอร์ชันที่ล้าสมัยเหล่านี้ยังคงมีความเสี่ยงทางด้านการใช้เทคโนโลยีที่ล้าสมัยและขาดประสิทธิภาพทางด้านการพัฒนาฟังก์ชันต่าง ๆ โดยเฉพาะหากพบปัญหาด้านความปลอดภัยจะไม่ได้รับการสนับสนุนจากเจ้าของผลิตภัณฑ์ ดังนั้น เพื่อควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น การยกระดับความเข้าใจและเล็งเห็นความสำคัญของการอัปเดตระบบปฏิบัติการให้ทันสมัยอยู่เสมอจึงเป็นสิ่งสำคัญที่ควรปฏิบัติ

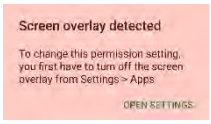
รูปที่ 4 แสดงผลสำรวจเวอร์ชันระบบปฏิบัติการขั้นต่ำที่ธนาคารอนุญาต
เทียบกับเวอร์ชันระบบปฏิบัติการที่ยังได้รับการสนับสนุนจากเจ้าของผลิตภัณฑ์

นอกจากการพิจารณาความปลอดภัยของโมบายแบงก์กิ้งแอปพลิเคชันจากด้านผู้ให้บริการหรือผู้พัฒนาระบบแล้ว สำหรับผู้ใช้บริการหรือผู้ใช้งาน โมบายแบงก์กิ้งแอปพลิเคชัน การสร้างความตระหนักเพื่อให้เกิดการใช้งานอย่างปลอดภัยก็เป็นสิ่งสำคัญ สามารถช่วยลดความเสี่ยงที่อาจเกิดภัยคุกคามทางไซเบอร์ได้ ดังคำแนะนำต่อไปนี้

คำแนะนำสำหรับผู้ใช้งาน ระบบปฏิบัติการ iOS

	1. ใช้งานบนระบบปฏิบัติการที่ยังได้รับการสนับสนุนจากเจ้าของผลิตภัณฑ์ และอัปเดตเวอร์ชันให้ทันสมัยอยู่เสมอ เพื่อเพิ่มประสิทธิภาพด้านการทำงานของฟังก์ชัน และประสิทธิภาพด้านการควบคุมความปลอดภัยจากการใช้งานตามเทคโนโลยีใหม่ ๆ ที่เกิดขึ้น
	2. หลีกเลี่ยงการ Jailbreak เพื่อไม่ให้ความมั่นคงปลอดภัยของระบบปฏิบัติการลดลง และถูกใช้เป็นช่องทางในการโจมตีเข้าสู่โทรศัพท์
	3. ดาวน์โหลด และติดตั้งแอปพลิเคชันจากแหล่งที่มาที่น่าเชื่อถือ เช่น App Store เท่านั้น เพื่อลดความเสี่ยงที่อาจจะถูกติดตั้งโปรแกรมอันตรายและถูกใช้เป็นช่องทางในการโจมตีเข้าสู่โทรศัพท์ต่อไป
	4. ตรวจสอบการร้องขอสิทธิ์ที่แอปพลิเคชันร้องขอตอนติดตั้ง และพยายามทบทวนสิทธิ์อยู่สม่ำเสมอ

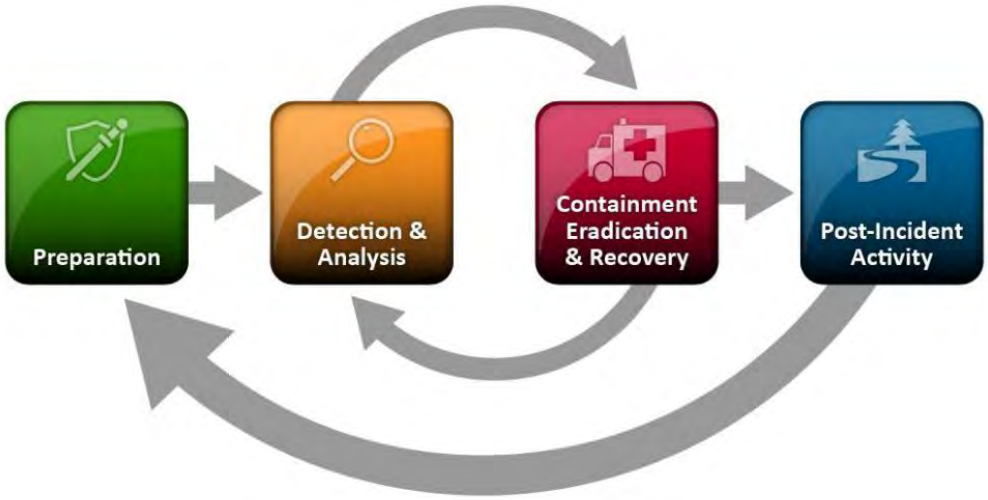
คำแนะนำสำหรับผู้ใช้งาน ระบบปฏิบัติการ Android ในกรณีที่ไม่สามารถอัปเดตระบบปฏิบัติการได้

	1. ใช้งานบนระบบปฏิบัติการที่ยังได้รับการสนับสนุนจากเจ้าของผลิตภัณฑ์ และอัปเดตเวอร์ชันให้ทันสมัยอยู่เสมอ เพื่อเพิ่มประสิทธิภาพด้านการทำงานของฟังก์ชัน และประสิทธิภาพด้านการควบคุมความปลอดภัยจากการใช้งานตามเทคโนโลยีใหม่ ๆ ที่เกิดขึ้น
	2. หลีกเลี่ยงการ Rooted เพื่อไม่ให้ความมั่นคงปลอดภัยของระบบปฏิบัติการลดลง และถูกใช้เป็นช่องทางในการโจมตีเข้าสู่โทรศัพท์
	3. ดาวน์โหลด และติดตั้งแอปพลิเคชันจากแหล่งที่มาที่น่าเชื่อถือ เช่น Play Store เท่านั้น เพื่อลดความเสี่ยงที่อาจจะถูกติดตั้งโปรแกรมอันตรายและถูกใช้เป็นช่องทางในการโจมตีเข้าสู่โทรศัพท์ต่อไป
	4. ปิดการใช้งานฟังก์ชันซ้อนทับหน้าจอ (Screen Overlay) กับแอปพลิเคชันที่ไม่อนุญาตให้ใช้งานฟังก์ชันนี้ เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการซ่อนการทำงานบางอย่างไว้เบื้องหลังภายใต้หน้าจอการใช้งานบนโมบายแบงก์กิ้งแอปพลิเคชัน
	5. เปิดใช้งาน Google Play Protect หรือติดตั้งโปรแกรมป้องกันมัลแวร์สำหรับระบบปฏิบัติการ Android
	6. หลีกเลี่ยงการใช้งานผ่าน Wi-Fi สาธารณะที่ไม่รู้จัก โดยเฉพาะอย่างยิ่งเมื่อทำธุรกรรมด้านการเงินผ่านโมบายแบงก์กิ้งแอปพลิเคชัน
	7. ปิดการเชื่อมต่อ เช่น NFC, Wi-Fi, และ Bluetooth หากไม่จำเป็นต้องใช้ เพื่อลดความเสี่ยงที่อาจถูกใช้เป็นช่องทางในการโจมตีเข้าสู่โทรศัพท์
	8. ตรวจสอบบัญชีผู้ใช้งานในเครื่องอยู่เสมอ หากพบบัญชีรายชื่อที่ผิดปกติให้ลบทิ้งทันที (เลือกที่ การตั้งค่า (Settings) -> ผู้ใช้งานและบัญชี (Users & Accounts) -> ผู้ใช้งาน (Users)) เพื่อลดความเสี่ยงที่อาจจะถูกติดตั้งโปรแกรมอันตรายและถูกใช้เป็นช่องทางในการโจมตีเข้าสู่โทรศัพท์
	9. ตรวจสอบการร้องขอสิทธิ์ที่แอปพลิเคชันร้องขอตอนติดตั้งโดยอนุญาตเท่าที่จำเป็นเท่านั้น และมีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

4. แนวทางการรับมือเมื่อเกิดการปลอมแปลงหน้าเว็บไซต์ของหน่วยงานสมาชิก (Web Phishing Handling Guide)

ปัจจุบันภัยคุกคามทางไซเบอร์มีเพิ่มมากขึ้นอย่างต่อเนื่อง ซึ่งหนึ่งในประเภทภัยคุกคามที่เกิดขึ้นบ่อยครั้งและเป็นที่นิยมของเหล่ามิจฉาชีพเพื่อหลอกเอาข้อมูลของประชาชนคือ การโจมตีแบบฟิชชิง (Phishing) ซึ่งเป็นวิธีการหลอกลวงแบบหนึ่ง ที่เหล่ามิจฉาชีพจะทำการสร้างเว็บไซต์ปลอมของหน่วยงานเป้าหมายขึ้นมาเพื่อหลอกลวงลูกค้าของหน่วยงานนั้นให้หลงเชื่อว่าเป็นเว็บไซต์หน่วยงานจริงและทำการกรอกข้อมูลส่วนบุคคลต่าง ๆ ไม่ว่าจะเป็นชื่อ นามสกุล ที่อยู่ อีเมล พาสเวิร์ด เลขที่บัญชี เลขบัตรเครดิตและอื่น ๆ มากมาย เนื่องด้วยธนาคารมีฐานลูกค้าจำนวนมาก ก็มักจะถูกเป็นเป้าในการโจมตีด้วยฟิชชิง ซึ่งจะทำให้ลูกค้าและธนาคารได้รับความเสียหายในรูปแบบของมูลค่าที่เป็นตัวเงิน หรือชื่อเสียง และความเชื่อมั่นต่อระบบสถาบันการเงิน จากการที่ TB-CERT ได้รับรายงานการกรณีของเว็บไซต์ปลอมหรือเว็บฟิชชิงของธนาคารสมาชิกในช่วงปีที่ผ่านมานั้นล้วนเป็นการส่งผ่าน SMS เป็นส่วนมาก

TB-CERT ได้จัดทำแนวทางปฏิบัติให้กับสมาชิกเพื่อใช้เป็นแนวทางการดำเนินการเมื่อตรวจพบ Phishing Website ของหน่วยงานสมาชิกของ TB-CERT โดยมีวัตถุประสงค์หลักเพื่อให้สมาชิกได้ทราบถึงกระบวนการรับมือและประสานงานเมื่อเกิดเหตุภัยคุกคามประเภทนี้ขึ้นและสามารถรับมือกับเหตุการณ์เบื้องต้นได้ด้วยตนเองอย่างทันท่วงที โดยถือหลักการ กระบวนการรับมือ ตามแบบ NIST Framework เป็นกรอบในการพัฒนาแนวทางปฏิบัติ



รูปที่ 5 Incident Response process-NIST

อ้างอิง NIST 800-181

ขั้นที่ 1 ขั้นเตรียมการ ในช่วงที่สถานการณ์สงบ สมาชิกควรเตรียมการรับมือกับเหตุการณ์การโจมตีด้วยฟิชชิง โดยสมาชิกควรมีการเตรียมความพร้อมสำหรับการสื่อสารภายในและสื่อสารภายนอกให้พร้อม เช่น ข้อมูลการติดต่อ ข้อความที่จะใช้สื่อสารและช่องทางการสื่อสารกับหน่วยงานที่เกี่ยวข้องกับการจัดการการโจมตีด้วยฟิชชิง และควรต้องมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ และนอกจากเตรียมการเรื่องการสื่อสารแล้ว ยังเตรียมเรื่องของสถานที่ อุปกรณ์ สิ่งอำนวยความสะดวกต่าง ๆ ที่จำเป็นในการประสานงาน สื่อสาร และรับมือกับเหตุการณ์ที่จะเกิดขึ้น

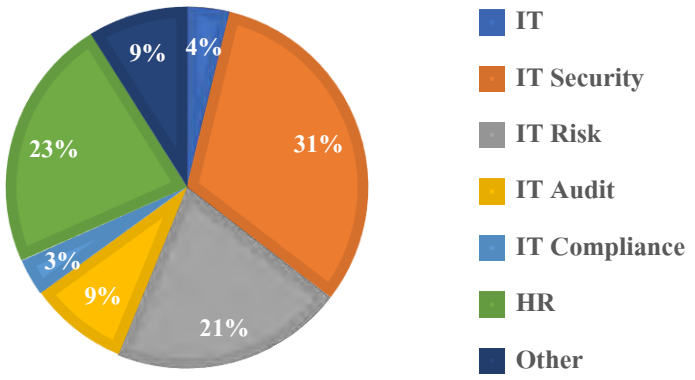
ขั้นที่ 2 ขั้นตรวจสอบและวิเคราะห์ข้อมูล ผู้ที่ทำหน้าที่รับผิดชอบในการรับมือกับเหตุกาณ์การโจมตีทางไซเบอร์ (Incident Response Handler) จะต้องสามารถระบุช่องทางและรูปแบบการโจมตีของเหตุการณ์ฟิชชิงเพื่อรวบรวมข้อมูลบ่งชี้อื่นเพิ่มเติมจากเครื่องมือตรวจจับที่เกี่ยวข้องได้ รูปแบบการโจมตีที่แตกต่างกัน กลยุทธ์ในการวิเคราะห์เหตุการณ์จะแตกต่างกันด้วย ดังนั้นการตรวจสอบเหตุการณ์การโจมตีด้วยฟิชชิงจะต้องสามารถระบุรูปแบบการโจมตี Location ของ Phishing Website ข้อมูลเป้าหมาย และทำการรวบรวมข้อมูลที่เกี่ยวข้องของเหตุการณ์เพื่อการวิเคราะห์ในรายละเอียด เพื่อหารูปแบบและความสัมพันธ์ของ Phishing Website ที่เกิดขึ้นในช่วงเวลาเดียวกัน และจะนำไปสู่จัดลำดับความสำคัญของเหตุการณ์ตามกรอบความรุนแรงและแจ้งให้ผู้ที่เกี่ยวข้องทราบ ทั้งนี้การตรวจสอบค้นหาข้อมูล Phishing Website นั้น ควรต้องมีความระมัดระวังมิให้เป็นการให้ข้อมูลอ่อนไหวหรือเป็นเหตุทำให้ติดมัลแวร์ และที่สำคัญไม่ควรใช้เน็ตเวิร์คขององค์กรที่เป็นเน็ตเวิร์คที่ให้บริการออนไลน์อยู่ด้วย

ขั้นที่ 3 ขั้นตอนการทำ Containment, Eradication และ Recovery ตามมาตรฐานการจัดการเหตุการณ์ทางคอมพิวเตอร์ของ NIST ที่ใช้อ้างถึงนี้ ขั้นตอนที่ 3 นี้ถือได้ว่าเป็นขั้นตอนที่สำคัญขั้นตอนหนึ่ง ซึ่งหลาย ๆ องค์กรอาจเลือกแนวทาง วิธีการ ในการจำกัดผลกระทบ (Containment) กำจัดภัยคุกคาม (Eradication) และกู้คืนระบบ (Recovery) ของตนเองแตกต่างกันไปตามผลการประเมินความเสี่ยงขององค์กรนั้น แต่สำหรับเหตุการณ์การโจมตีด้วยฟิชชิงนั้น วิธีการจำกัดผลกระทบ (Containment) สำหรับลูกค้าคือจะต้องแจ้งข้อมูลให้ลูกค้าทราบถึงรูปแบบของ Phishing นั้นโดยเร็ว (User Awareness) ในขณะที่จะไม่ลืมที่จะลดผลกระทบจากการโจมตีนั้นให้กับพนักงานในองค์กรด้วยวิธีการเช่น Automated filtering, Blocking user access หรือ User awareness เป็นต้น จากนั้นให้เร่งรัดในการแจ้งเพื่อดำเนินการปิด Phishing website และแจ้งให้ browser vendor ขึ้นข้อความเตือนเพื่อปิดกันการเข้าถึง Phishing website นั้น ๆ ด้วย browser ทุกราย

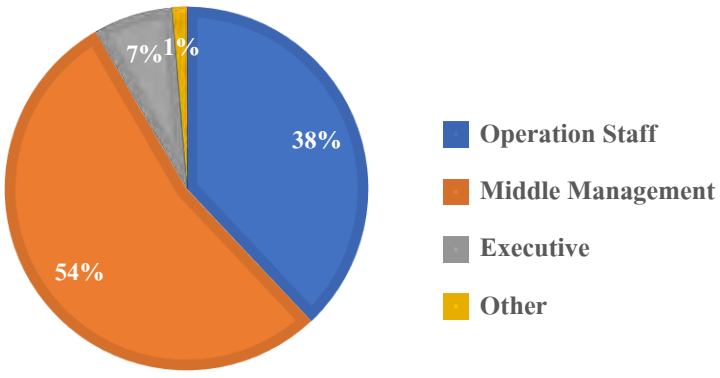
ขั้นสุดท้ายเป็นขั้นตอนหลังจากจัดการกับเหตุการณ์การโจมตีเป็นที่เรียบร้อย องค์กรจะต้องทบทวนการจัดการกับเหตุการณ์ที่เกิดขึ้น และจัดเตรียมรายงานเหตุการณ์โดยจะต้องตอบให้ได้ว่า ใคร ทำอะไร ที่ไหน อย่างไร เมื่อไหร่ และที่ขาดไม่ได้ผู้ที่เกี่ยวข้องในการจัดการกับเหตุการณ์ที่เกิดขึ้นจะต้องนำผลจากการทบทวนนั้นไปพิจารณาเพื่อการปรับปรุงต่าง ๆ ให้ดีขึ้น ไม่ว่าจะเป็น กระบวนการรับมือ แนวทางการปฏิบัติงานที่พบจากเหตุการณ์ที่เกิดขึ้น สำหรับการทบทวนการจัดการกับเหตุการณ์การโจมตีด้วยฟิชชิงนั้นอาจจะนำไปสู่การรับรู้ถึงเทคนิคของการหลอกลวงหรือการตรวจจับแบบใหม่ ๆ ได้อีกด้วย

งานด้านการสร้างความตระหนักรู้ด้านภัยไซเบอร์สำหรับธนาคารสมาชิก
Cybersecurity Proficiency Development Program (Webinar & Workshop)

ภารกิจของ TB-CERT ในการพัฒนาบุคลากรภาคธนาคารในปีที่ผ่านมา ได้จัดหาผู้เชี่ยวชาญด้านเทคโนโลยี ไม่ว่าจะเป็นด้านความมั่นคงปลอดภัยไซเบอร์ หรือการนำเทคโนโลยีมาใช้ในการจัดการต่าง ๆ รวมทั้งการบริหารความเสี่ยง ผ่านการจัด Webinar และ Online Workshop จำนวน 4 ครั้ง ในปี 2021 มีจำนวนผู้เข้าร่วมทั้งหมด 395 คน มาจากสายงานต่าง ๆ ทั้งสิ้น 6 สายงาน ได้แก่ IT, IT Security, IT Risk, IT Audit, IT Compliance, Human Resources และสามารถแบ่งระดับตำแหน่งงานของผู้เข้าร่วมงานออกเป็น 3 ระดับ ได้แก่ Executive, Middle Management และ Operation Staff



รูปที่ 6 แผนภาพแสดงสัดส่วนของบุคลากรที่เข้าร่วม Webinar แบ่งตามระดับตำแหน่งงาน (เปอร์เซ็นต์)



รูปที่ 7 แผนภาพแสดงสัดส่วนของบุคลากรที่เข้าร่วม Webinar แบ่งตามส่วนงานต่าง ๆ (เปอร์เซ็นต์)

การจัดสัมมนาเชิงวิชาการออนไลน์เพื่อพัฒนาบุคลากรด้านไซเบอร์ ผ่านโครงการ Cybersecurity Development Program

ซึ่งแบ่งเป็น 2 ส่วนหลักคือ การบรรยายเชิงทฤษฎีและการบรรยายเชิงปฏิบัติ มีรายละเอียดดังนี้

1. โครงการ Cybersecurity Development Program (Webinar)

เป็นการจัดสัมมนาเชิงวิชาการให้กับธนาคารสมาชิก ในรูปแบบ webinar ดังนี้

1.1 งานสัมมนาออนไลน์ The Future of Work & the Human Factor in the new normal

TB-CERT ร่วมกับบริษัท SAP Thailand จัดงานสัมมนาออนไลน์ The Future of Work & the Human Factor in the new normal ในวันที่ 19 พฤษภาคม 2021 โดยเป็นการแชร์ความรู้และประสบการณ์จากผู้บริหารระดับสูงด้านทรัพยากรบุคคล ถึงความท้าทายและแนวทางของงานด้านทรัพยากรบุคคลในยุคโควิด รวมทั้งการอัพเดทเทคโนโลยีที่จะมาช่วยให้การทำงานด้านบุคลากรในยุคนี้มีประสิทธิภาพและตรงตามความต้องการมากขึ้น

1.2 งานสัมมนาออนไลน์ Effectively Managing Third Party Technology Risk

TB-CERT ร่วมกับบริษัท Akamai Technologies Singapore Pte จัดงานสัมมนาออนไลน์ Effectively Managing Third Party Technology Risk เมื่อวันที่ 1 มิถุนายน 2021 ซึ่งผู้เข้าร่วมได้รับความรู้จากผู้เชี่ยวชาญในหัวข้อ Digital Banking and Third-Party Technology Risk และเปลี่ยนประสบการณ์ร่วมกับวิทยากรจากธนาคารพาณิชย์และหน่วยงานกำกับดูแลเกี่ยวกับการจัดการ Third Party ซึ่งจะช่วยให้ผู้เข้าร่วมสัมมนานำไปปรับใช้กับองค์กรได้

1.3 งานสัมมนาออนไลน์ Executive Banking Forum

TB-CERT ร่วมกับบริษัท FireEye จัดงานสัมมนาออนไลน์ Executive Banking Forum ในวันที่ 15 มิถุนายน 2021 โดยช่วงบรรยาย Management Track เป็นการอัพเดทเทรนด์ด้านภัยคุกคามไซเบอร์และการบริหารจัดการความเสี่ยงสำหรับผู้บริหาร

1.4 งานสัมมนาออนไลน์ How Organizations Handle risk with confident

TB-CERT ร่วมกับบริษัท ServiceNow จัดงานสัมมนาออนไลน์ How organizations handle risks with confidence ขึ้นในวันที่ 4 สิงหาคม 2021 ซึ่งได้อัพเดทความรู้และทักษะเกี่ยวกับการจัดการความเสี่ยงด้านเทคโนโลยีในแง่มุมของการจัดการความเสี่ยงด้านไอทีขององค์กร ที่จะช่วยให้การดำเนินงานขององค์กรเป็นไปอย่างราบรื่นและมีประสิทธิภาพ

2. โครงการ Cybersecurity Development Program (Workshop)

เป็นการจัดอบรมเชิงปฏิบัติการให้กับธนาคารสมาชิกด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

2.1 Threat Hunting Workshop

TB-CERT ร่วมกับบริษัท FireEye จัด Online Workshop เกี่ยวกับ threat hunting ในวันที่ 15 มิถุนายน 2021 ซึ่งเป็น Technical Track ของงาน Executive Banking Forum เพื่อให้ธนาคารสมาชิกและผู้ปฏิบัติงานที่เกี่ยวข้องได้เรียนรู้จากประสบการณ์ของผู้เชี่ยวชาญโดยเฉพาะ

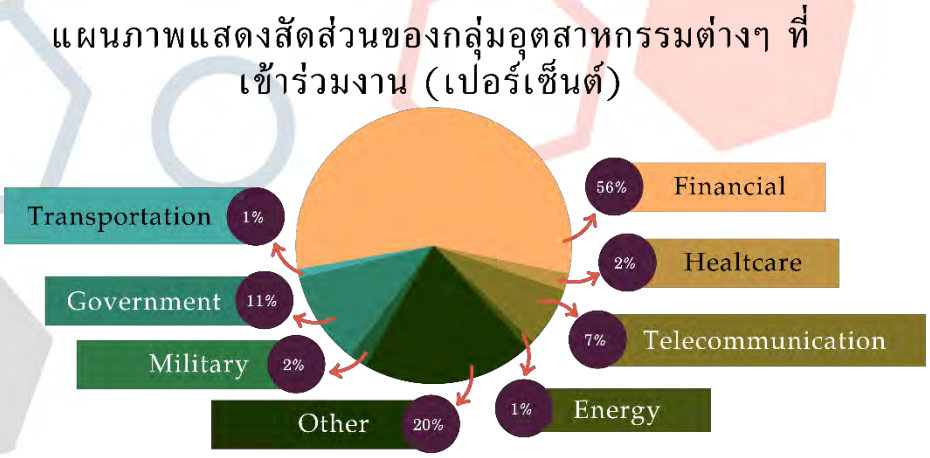
งานด้านการสร้างความตระหนักรู้ด้านไซเบอร์สำหรับธนาคารสมาชิก ภาคการเงิน และหน่วยงานภายนอก

1. Live Talk: Phishing ตระหนักแต่อย่าตระหนก

TB-CERT ได้จัดงานเสวนาออนไลน์ ผ่าน TB-CERT Facebook Live ในหัวข้อ Phishing ตระหนักแต่อย่าตระหนก ในวันที่ 10 กุมภาพันธ์ 2021 โดยมีผู้เชี่ยวชาญจากภาคธนาคารร่วมสนทนาและให้ความรู้เกี่ยวกับภัยฟิชชิ่ง เพื่อให้ผู้ชมได้รู้เท่าทันและมีแนวทางป้องกันภัยฟิชชิ่งได้ ซึ่งมีผู้รับชมสดผ่าน Facebook Live และวิดีโอกว่า 4,000 ครั้ง

2. งานสัมมนาออนไลน์ TB-CERT Annual Conference 2021

TB-CERT จัดงานสัมมนาออนไลน์ TB-CERT Annual Conference 2021: Vaccinate Your Cybersecurity, Now or Never เมื่อวันที่ 22 กันยายน 2021 ร่วมกับหน่วยงานด้านเทคโนโลยีชั้นนำที่มาให้ความรู้และอัปเดทเทคโนโลยีใหม่ ๆ เพื่อเสริมสร้างภูมิคุ้มกันด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงสร้างความเข้าใจในสถานการณ์ภัยคุกคามทางไซเบอร์เพื่อเป็นการเตรียมพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ให้กับสมาชิก และบุคลากรในอุตสาหกรรมภาคการเงินการธนาคาร การลงทุน ประกันภัย โทรคมนาคม รวมถึงหน่วยงานภาครัฐที่เกี่ยวข้อง โดยมีผู้เข้าร่วมงานรวม 754 คน จากผู้ที่ลงทะเบียนเข้ามา 779 คน ซึ่งแบ่งเป็นสัดส่วนของผู้เข้าร่วมงานตามภาคอุตสาหกรรมต่าง ๆ ได้ตามภาพ



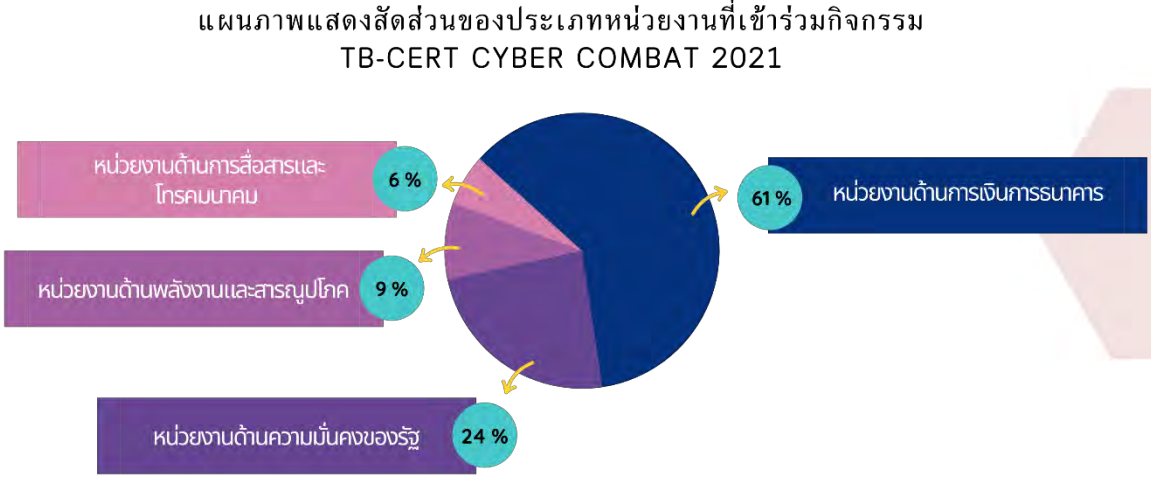
รูปที่ 8 แผนภาพแสดงสัดส่วนของกลุ่มอุตสาหกรรมต่าง ๆ ที่เข้าร่วมงาน (เปอร์เซ็นต์)

และจากแบบประเมินพบว่าผู้เข้าร่วมงานมีความพึงพอใจมากและมากที่สุดในการจัดงานครั้งนี้มากถึง 93%

การพัฒนาศักยภาพในการรับมือภัยไซเบอร์

1. โครงการ Cyber Combat

ในปี 2021 ทีมงาน TB-CERT ยังคงมุ่งเน้นด้านการพัฒนาศักยภาพในการรับมือภัยไซเบอร์อย่างต่อเนื่อง โดยจัดการแข่งขัน TB-CERT Cyber Combat ซึ่งเป็นกิจกรรมหลักกิจกรรมหนึ่งของภาคการธนาคารที่จัดอย่างต่อเนื่องเป็นประจำทุกปี ในกิจกรรมนี้จะเน้นการฝึกอบรมและแข่งขัน ที่เรียกว่า CTF (Capture The Flag) ในรูปแบบการทำโจทย์หาคำตอบ แบบ Jeopardy เพื่อพัฒนาทักษะทั้งด้านการคิดวิเคราะห์และเข้าใจการรับมือการโจมตีด้วยเทคนิคใหม่ ๆ รวมถึงการพัฒนาศักยภาพที่จำเป็นต่อการรับมือภัยไซเบอร์ที่ความซับซ้อนมากขึ้น นอกจากจะมุ่งเน้นที่การพัฒนาทักษะของผู้เข้าแข่งขันที่เป็นกำลังพลหลักขององค์กรแล้วนั้น TB-CERT ยังมุ่งเน้นการสร้างความสัมพันธ์กับหน่วยงานภายนอกเช่นกัน นอกจากหน่วยงานสมาชิกเข้าร่วมการแข่งขันครั้งนี้ TB-CERT ได้เชิญหน่วยงานภายนอกต่าง ๆ ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้แก่ หน่วยงานด้านความมั่นคงของรัฐ หน่วยงานด้านเทคโนโลยีสารสนเทศและโทรคมนาคม หน่วยงานด้านพลังงานและสาธารณูปโภค เข้าร่วมอบรมและแข่งขัน รวมทั้งหมดมีหน่วยงานเข้าร่วมกิจกรรมทั้งสิ้น 33 หน่วยงาน นับเป็นจำนวนทีมทั้งหมดจากการแข่งขัน 2 ครั้งรวม 87 ทีม โดยแบ่งเป็นประเภท Blue team จำนวน 46 ทีม 137 คน และ ประเภท Red team จำนวน 41 ทีม 122 คน



รูปที่ 9 แผนภาพแสดงสัดส่วนของประเภทหน่วยงานที่เข้าร่วมกิจกรรม TB-CERT Cyber Combat 2021

การฝึกอบรมทักษะ ความรู้ทั้งทฤษฎีและปฏิบัติช่วยให้ผู้เข้าแข่งขัน สามารถนำไปปรับใช้กับการแข่งขันและการทำงานจริงได้ โดยจะแบ่งกลุ่มผู้เรียนและผู้แข่งขันออกเป็น 2 กลุ่มคือ 1. กลุ่มทักษะเชิงรับ (Blue Team) ซึ่งมุ่งเน้นความสามารถในวิเคราะห์และตรวจจับผู้บุกรุก 2. กลุ่มทักษะเชิงรุก (Red Team) ซึ่งมุ่งเน้นความสามารถในการค้นหาและตรวจสอบช่องโหว่ของระบบ

TB-CERT ได้ร่วมการอบรมและออกแบบโจทย์ทักษะเชิงรับ (Blue Team) กับบริษัท Splunk ซึ่งได้จัดการอบรมเป็นเวลา 2 วัน โดยแบ่งเป็นระดับพื้นฐาน (Basic) และ ระดับกลางถึงสูง (Intermediate & Advance) เพื่อเตรียมความพร้อมให้ผู้แข่งขัน ในปีนี้โจทย์เชิงรับได้มุ่งเน้นพัฒนาทักษะการตรวจจับภัยคุกคามที่สำคัญต่อการทำงานของธนาคารในยุคปัจจุบัน ประกอบด้วย Enterprise security, Cloud security, Secure remote working และ Modern infrastructure อย่าง Kubernetes

โจทย์ปัญหาประเภททักษะเชิงรับ (Blue Team) 3 อันดับแรกที่ผู้เข้าแข่งขันส่วนใหญ่สามารถแก้ไข ดังนี้

อันดับที่ 1 โจทย์ประเภท Enterprise security เป็นโจทย์ที่ผู้แข่งทำคะแนนได้สูงสุด ซึ่งชี้ให้เห็นถึงทักษะของผู้แข่งขันในการวิเคราะห์และตรวจจับการโจมตีในระดับองค์กรได้เป็นอย่างดี

อันดับที่ 2 โจทย์ประเภท Cloud security ซึ่งชี้ให้เห็นถึงทักษะของผู้แข่งขันที่มีความรู้ ความเข้าใจในการวิเคราะห์และตรวจจับการโจมตี รวมถึงการตั้งค่าความปลอดภัยบนเครือข่ายคลาวด์

อันดับที่ 3 โจทย์ประเภท Kubernetes ซึ่งชี้ให้เห็นถึงทักษะของผู้แข่งขันว่ามีความรู้และความเข้าใจ เรื่องความมั่นคงปลอดภัยในการใช้งาน Kubernetes ซึ่งเป็น Modern infrastructure ที่ได้รับการยอมรับและใช้งานอย่างแพร่หลายในปัจจุบัน

สำหรับกลุ่มทักษะเชิงรุก (Red Team) ทีมงาน TB-CERT ได้ทำงานร่วมกับทีมงาน Hack the Box จากประเทศอังกฤษ อบรมและออกแบบโจทย์ร่วมกัน ซึ่งทีมงาน Hack the Box เป็นทีมที่ยอมรับในการจัดแข่งขันฝึกทักษะด้านไซเบอร์ในระดับสากล และได้นำหลักการออกแบบโจทย์ตามกรอบ MITRE ATT&CK และ OWASP Top 10 มาใช้เป็นแนวทางในการพัฒนาทักษะ และได้จัดการอบรม 2 วัน โดยทีมงาน TB-CERT เป็นผู้อบรมและเตรียมความพร้อมให้กับผู้แข่งขัน ในปีนี้โจทย์เชิงรุกได้มุ่งเน้นพัฒนาทักษะของผู้แข่งขัน ในการใช้เทคนิคการค้นหาช่องโหว่และเจาะระบบตามกรอบของ MITRE ATT&CK ดังต่อไปนี้ Active Scanning, Exploitation for Credential Access, Exploit Public-Facing Application, Scheduled Task/Job, Steal Web Session Cookie, Exploit Public-Facing Application, Credentials from Password Stores, Abuse Elevation Control Mechanism, Exploitation for Privilege Escalation, Access token manipulation, Steal or Forge Kerberos Tickets, OS Credential dumping ซึ่งโจทย์ในการแข่งขันเป็นระบบที่เกี่ยวข้องกับ Web application โดยมีหัวข้อที่สอดคล้องกับ OWASP Top 10 เวอร์ชัน 2017 และ 2021 ดังนี้ Injection, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security

Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, Server Side Request Forgery

โจทย์ปัญหาประเภททักษะเชิงรุก (Red Team) 3 อันดับแรกที่ผู้เข้าแข่งขันส่วนใหญ่สามารถแก้ไข ดังนี้

อันดับที่ 1 ประเภท Security Misconfiguration ผู้แข่งขันสามารถแก้ไขโจทย์ได้ถึง 80 เปอร์เซ็นต์ (ผู้แข่งขันแก้ปัญหาได้ 33 ทีม จากทั้งหมด 41 ทีม) ซึ่งชี้ให้เห็นถึงทักษะของผู้แข่งขันในการค้นหาและวิเคราะห์ช่องโหว่ที่เกิดจากการตั้งค่าความปลอดภัยที่ผิดพลาดและไม่เหมาะสม

อันดับที่ 2 ประเภท XML External Entities (XXE) ผู้แข่งขันสามารถแก้ไขโจทย์ได้ 46 เปอร์เซ็นต์ (ผู้แข่งขันแก้ปัญหาได้ 19 ทีม จากทั้งหมด 41 ทีม) ซึ่งชี้ให้เห็นถึงทักษะของผู้แข่งขันในการค้นหาและวิเคราะห์ช่องโหว่ที่สามารถเพิ่มเนื้อหาอันตรายเข้าไปใน XML โดยถูกนำไปประมวลที่ฝั่งเครื่องแม่ข่าย ส่งผลให้เข้าถึงไฟล์สำคัญ หรือทรัพยากรอื่นๆ บนเครื่องแม่ข่ายได้

อันดับที่ 3 ประเภท Server Side Request Forgery ผู้แข่งขันสามารถแก้ไขโจทย์ได้ 41 เปอร์เซ็นต์ (ผู้แข่งขันแก้ปัญหาได้ 17 ทีม จากทั้งหมด 41 ทีม) ซึ่งชี้ให้เห็นถึงทักษะของผู้แข่งขันในการค้นหาและวิเคราะห์ช่องโหว่ที่สามารถทำการปลอมแปลงและเปลี่ยนแปลงคำขอ (request) จากฝั่งเครื่องแม่ข่ายได้

2. โครงการ Cyber Brain

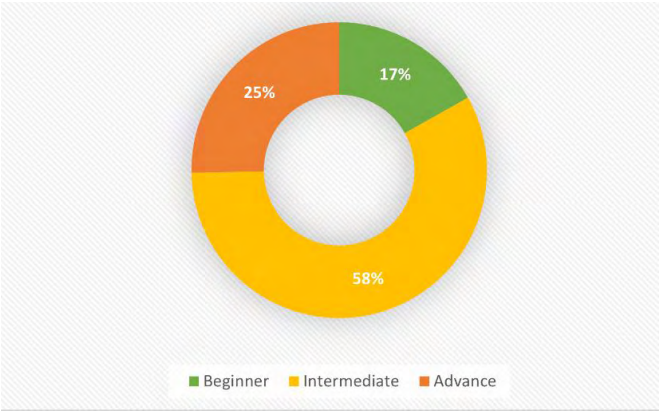
ปี 2021 TB-CERT เริ่มโครงการ Cyber Brain โดยมีเป้าหมายในการพัฒนาหลักสูตรการเรียนรู้ด้าน Cybersecurity แบบออนไลน์ เพื่อพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ตามเป้าหมาย ของ TB-CERT คือ เป็นศูนย์รวมของผู้เชี่ยวชาญระดับ Professional ด้าน Cybersecurity รวมถึงภารกิจหลักของ TB-CERT คือ เพิ่มพูนศักยภาพและจำนวนบุคลากรที่มีความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับภาคการธนาคารในประเทศไทย ให้เพียงพอต่อความต้องการในปัจจุบันและอนาคต โดยหลักสูตรในโครงการนี้ถูกออกแบบให้มีการเรียนเชิงทฤษฎีควบคู่กับการยกตัวอย่างเชิงปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ ผ่านระบบแพลตฟอร์มแบบออนไลน์ มุ่งเน้นความรู้ความเข้าใจและทักษะด้าน Cybersecurity เฉพาะทาง เตรียมความพร้อมทางด้านความมั่นคงปลอดภัยไซเบอร์ในยุคดิจิทัลที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ตลอดจนให้ผู้เรียนสามารถนำองค์ความรู้ไปประยุกต์ใช้เพื่อให้เกิดประโยชน์ต่อตนเองและองค์กรในการรับมือภัยไซเบอร์ที่อาจเกิดขึ้นในอนาคต

หลักสูตรของโครงการ Cyber Brain ออกแบบพัฒนาตามกรอบการพัฒนาความรู้และความสามารถของบุคลากรด้าน Cybersecurity จาก NIST Workforce Framework for Cybersecurity (NICE Framework) ซึ่งเป็นพื้นฐานในการกำหนดความรู้ ทักษะความเชี่ยวชาญ และความสามารถของบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ที่จำเป็นต้องมีในแต่ละบทบาทหน้าที่การปฏิบัติงานต่าง ๆ ในปี 2021 โครงการ Cyber Brain ได้พัฒนาหลักสูตรทางด้าน Cybersecurity ให้กับสมาชิก จำนวนทั้งสิ้น 25 หลักสูตร โดยจัดกลุ่มหลักสูตรเป็น 3 ระดับ คือ

1. **Beginner Level** คือ หลักสูตรด้านความมั่นคงปลอดภัยระดับพื้นฐาน เหมาะสำหรับผู้เริ่มทำงานในสายงาน Cybersecurity มีความรู้พื้นฐานทางด้านเทคโนโลยีและเครือข่าย โดยระดับพื้นฐานนี้จะเน้นองค์ความรู้พื้นฐานทางด้าน Cybersecurity และการสร้างทักษะแนวคิดให้เกิดความตระหนักทางด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้สามารถนำไปประยุกต์ในการปฏิบัติงานในองค์กรได้อย่างมีประสิทธิภาพ
2. **Intermediate Level** คือ หลักสูตรด้านความมั่นคงปลอดภัยระดับผู้ชำนาญ เหมาะสำหรับผู้ที่มีประสบการณ์การทำงานด้าน Cybersecurity มาแล้วระยะหนึ่ง ระดับผู้ชำนาญนี้จะเน้นองค์ความรู้เชิงลึกและทักษะความรู้ทางเทคนิคเฉพาะทางในแต่ละด้าน เพื่อสร้างความรู้ความเข้าใจและสร้างทักษะให้เกิดความชำนาญ เพื่อให้สามารถปฏิบัติงานในองค์กรได้อย่างมีประสิทธิภาพและพร้อมรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคตได้

3. **Advanced Level** คือ หลักสูตรด้านความมั่นคงปลอดภัยระดับผู้เชี่ยวชาญ เหมาะสำหรับผู้ที่มีประสบการณ์การทำงานด้าน Cybersecurity มากกว่า 5 ปีขึ้นไป ระดับผู้เชี่ยวชาญนี้จะเน้นองค์ความรู้ทาง Cybersecurity ด้านการบริหารจัดการ Cybersecurity ที่เกี่ยวข้องกับสายงาน 2nd line และ 3rd line เพื่อให้สามารถนำไปเสริมสร้างกลยุทธ์ด้านความมั่นคงปลอดภัย กำหนดนโยบาย รวมถึงการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กรให้มีประสิทธิภาพยิ่งขึ้น

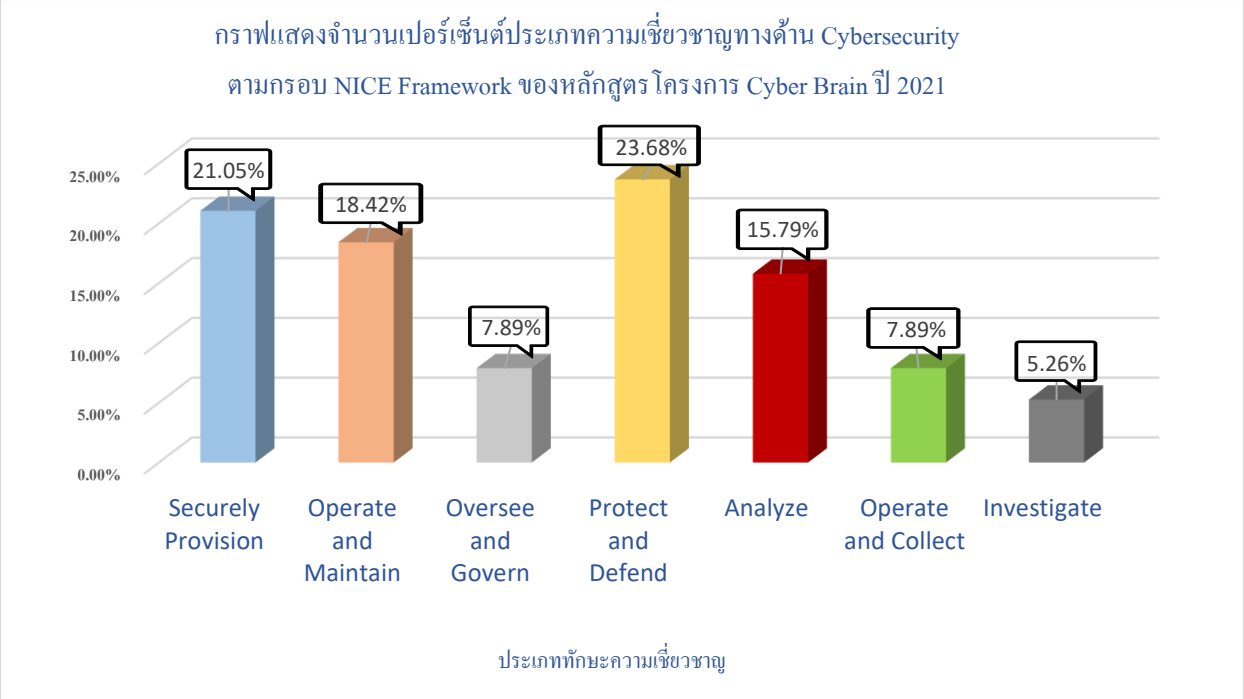
จากผลการดำเนินงานของโครงการ Cyber Brain ในปี 2021 มีผู้ลงทะเบียนเข้าเรียนในโครงการทั้งสิ้น 107 ท่านจากสมาชิก TB-CERT ทั้งหมด 25 องค์กร มีผู้ลงทะเบียนเรียนตามหลักสูตรของแต่ละระดับคิดเป็น หลักสูตรระดับพื้นฐาน 17%, หลักสูตรระดับผู้ชำนาญ 58% และหลักสูตรระดับผู้เชี่ยวชาญ 25% ดังรูปที่ 6 แสดงเปอร์เซ็นต์ความสนใจของบุคลากรภาคการธนาคารจากหลักสูตรทั้ง 3 ระดับ หลักสูตรที่มีความสนใจมากที่สุดคือ หลักสูตรระดับผู้ชำนาญ ซึ่งสอดคล้องกับผลสำรวจความต้องการบุคลากรด้าน Cybersecurity ภาคการเงินในปี 2021 ที่พบว่า จำนวนความต้องการบุคลากรที่มีประสบการณ์ด้าน Cybersecurity ตั้งแต่ 3-5 ปี มีอัตราความต้องการมากที่สุดถึง 43% แสดงให้เห็นว่า สายงานทางด้าน Cybersecurity มีอัตราการเติบโตที่สูงขึ้น มีความต้องการบุคลากรทางด้าน Cybersecurity เพิ่มมากขึ้น โดยเฉพาะความต้องการบุคลากรที่มีความรู้ทางเทคนิคเฉพาะด้าน มีทักษะกระบวนการคิดวิเคราะห์ มีความเข้าใจเกี่ยวกับกฎหมายและข้อกำหนดต่างๆ ที่เกี่ยวข้อง และมีความสามารถในการออกแบบประยุกต์ใช้เทคโนโลยีให้มีความมั่นคงปลอดภัยอย่างเหมาะสม ดังนั้นภาคการธนาคารจึงมีความต้องการมุ่งเน้นที่จะพัฒนาศักยภาพบุคลากรให้มีความรู้ทางด้าน Cybersecurity เชิงลึกและสร้างทักษะความรู้ทางเทคนิคเฉพาะทางให้เกิดความชำนาญ เพื่อให้สามารถพัฒนาระบบที่มีความมั่นคงปลอดภัย และมีความพร้อมรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต



รูปที่ 10 แสดงเปอร์เซ็นต์ความสนใจของบุคลากรภาคการธนาคารจากหลักสูตรทั้ง 3 ระดับ

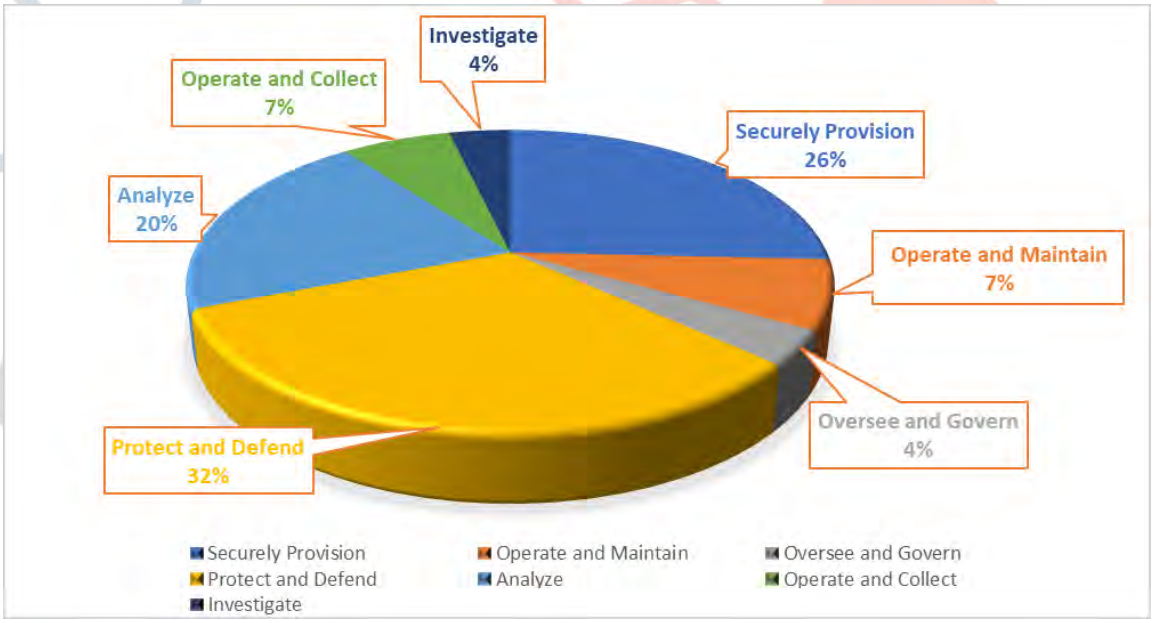
นอกจากนี้จากทั้ง 25 หลักสูตรของโครงการ Cyber Brain เมื่อนำมาจัดกลุ่มตามหมวดหมู่ประเภทความเชี่ยวชาญทางด้าน Cybersecurity ของ NICE Framework ทั้ง 7 กลุ่ม ได้แก่ Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Operate and Collect และ Investigate จากรูปที่ 10 แสดงจำนวนเปอร์เซ็นต์ประเภทความเชี่ยวชาญทางด้าน Cybersecurity ตามกรอบ NICE

Framework ของหลักสูตรโครงการ Cyber Brain ปี 2021 ซึ่งชี้ให้เห็นว่าหลักสูตรมุ่งเน้นการพัฒนาศักยภาพบุคลากรเกี่ยวกับทักษะด้าน **Protect and Defend** มากที่สุด เพราะบทบาทความรับผิดชอบเกี่ยวกับการป้องกัน และรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศถือเป็นด่านสำคัญหน้าสุด เป็นเสมือนชุดเกราะชั้นแรกสุดสำหรับป้องกันการเกิดความเสี่ยงจากภัยคุกคามทางไซบอร์และช่วยบรรเทาผลกระทบจากภัยคุกคามทางไซเบอร์ต่าง ๆ เนื่องด้วยแนวโน้มการเกิดภัยคุกคามทางไซเบอร์ที่มีจำนวนเพิ่มมากขึ้น และมีความซับซ้อนมากขึ้น ทำให้การตรวจจับทำได้ยากขึ้น ดังนั้นหลักสูตรของโครงการ Cyber Brain จึงมุ่งเน้นทักษะทางด้าน **Protect and Defend** โดยทักษะกลุ่มนี้จะเกี่ยวข้องผู้วิเคราะห์แนวทางการป้องกันเครือข่ายและระบบเทคโนโลยีสารสนเทศ กลุ่มงานที่เป็นผู้รับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ และผู้ดูแลบริหารจัดการช่องโหว่ของระบบเทคโนโลยีสารสนเทศ เพื่อให้บุคลากรมีความรู้ ความเข้าใจเท่าทันตามเทคโนโลยีและภัยคุกคามที่อาจจะเกิดขึ้นในอนาคต และสามารถรับมือกับภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิภาพ ทักษะในลำดับถัดมาที่มุ่งเน้นของโครงการ Cyber Brain คือ ทักษะทางด้าน **Securely Provision** และ ทักษะทางด้าน **Operate and Maintain** เพราะการวางโครงสร้างหรือการสร้างพื้นฐานทางด้านความมั่นคงปลอดภัยที่แข็งแกร่งจะช่วยลดโอกาสเกิดภัยจากการโจมตีทางไซเบอร์ได้เป็นอย่างมาก นั่นคือ แม้ว่าองค์กรจะพบว่ามีการโจมตีทางไซเบอร์เกิดขึ้น แต่หากองค์กรมีมาตรการควบคุมความมั่นคงปลอดภัยที่แข็งแรงตั้งแต่โครงสร้างสถาปัตยกรรมด้านความมั่นคงปลอดภัยและกระบวนการดูแลควบคุมความปลอดภัยของระบบเทคโนโลยีสารสนเทศภายใน ทำให้โอกาสที่จะได้รับผลกระทบจากการโจมนี้ทางไซเบอร์ก็จะลดลง



รูปที่ 11 แสดงจำนวนเปอร์เซ็นต์ประเภทความเชี่ยวชาญทางด้าน Cybersecurity ตามกรอบ NICE Frameworkของหลักสูตรโครงการ Cyber Brain ปี 2021

ในจำนวนสมาชิกผู้เข้าเรียนทั้งหมด 107 ท่าน สามารถสรุปจำนวนเปอร์เซ็นต์หลักสูตรที่สมาชิกสนใจเลือกเรียนเพื่อเสริมทักษะความรู้ความสามารถตามหมวดหมู่ประเภทความเชี่ยวชาญทางด้าน Cybersecurity ดังรูปที่ 11 ปรากฏผลองค์ความรู้และทักษะความสามารถใน 3 อันดับแรกที่สมาชิกได้เรียนรู้และพัฒนาศักยภาพทางด้าน Cybersecurity คือ ด้าน **Protect and Defend** ลำดับถัดมาคือ **Securely Provision** และ **Analyze** ตามลำดับ นั่นแสดงให้เห็นว่าทั้ง TB-CERT และองค์กรสมาชิกเล็งเห็นความสำคัญต่อบทบาทหน้าที่ทางด้านการป้องกัน เฝ้าระวัง และเตรียมพร้อมรับมือต่อเหตุการณ์ภัยคุกคามที่อาจเกิดขึ้น เป็นหัวใจสำคัญด้านหนึ่งของการดูแลรักษาความมั่นคงปลอดภัยของภาคการธนาคาร และยังสอดคล้องกับผลสำรวจความต้องการบุคลากรทางด้าน Cybersecurity ของภาคการธนาคารตลอด 2 ปีที่ผ่านมา ที่มีอัตราส่วนความต้องการบุคลากรทางด้าน **Protect and Defend** สูงถึง 45% เพื่อป้องกันภัยคุกคามและการโจมตีทางไซเบอร์ที่ยังคงเพิ่มขึ้นอย่างต่อเนื่อง ทั้งนี้ ความต้องการในการพัฒนาศักยภาพและทักษะความเชี่ยวชาญทางด้าน Cybersecurity ในด้านอื่น ๆ สำหรับภาคการธนาคารยังคงมีแนวโน้มที่จะยังเติบโตอย่างต่อเนื่องเช่นกัน นอกจากนี้องค์ความรู้และทักษะความสามารถที่ผู้เข้าเรียนให้ความสนใจของโครงการ Cyber Brain ในลำดับถัดมาคือ **Securely Provision** และ **Analyze** ซึ่งเป็นทักษะทางด้านการสร้างแนวคิดออกแบบ และพัฒนาความมั่นคงปลอดภัยบนระบบเทคโนโลยีสารสนเทศ และทักษะทางด้านการตรวจสอบ วิเคราะห์และประเมินผล โดยใช้ทักษะการวิเคราะห์เชิงลึกที่เน้นความเชี่ยวชาญพิเศษเฉพาะด้านที่เกี่ยวข้องกับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ จากทั้ง 3 อันดับที่มีเปอร์เซ็นต์ผู้เข้าเรียนมากที่สุด พบว่าองค์ความรู้และทักษะทางเทคนิคยังคงเป็นทักษะที่บุคลากรของภาคการธนาคารให้ความสนใจและเน้น การพัฒนาศักยภาพให้มีความสามารถในเชิงคิดวิเคราะห์ คิดเป็นระบบ และการคิดอย่างมีเหตุผล กระบวนการคิดเหล่านี้เป็นสิ่งสำคัญของการทำงานทางด้าน Cybersecurity เพื่อให้สามาถสามารถออกแบบพัฒนาปรับปรุงกระบวนการทำงานบนระบบเทคโนโลยีสารสนเทศให้มีความมั่นคงปลอดภัย พร้อมรับมือและแก้ไขปัญหาได้อย่างมีประสิทธิภาพ



รูปที่ 12 แสดงจำนวนเปอร์เซ็นต์หลักสูตรที่สมาชิกสนใจเลือกเรียน
เพื่อเสริมทักษะความรู้ความสามารถตามหมวดหมู่ประเภทความเชี่ยวชาญทางด้าน Cybersecurity

บทสรุปตามเป้าหมายของโครงการ Cyber Brain คือ มุ่งเน้นการออกแบบหลักสูตร เพื่อพัฒนาศักยภาพบุคลากรทางสายอาชีพ Cybersecurity ตามกรอบมาตรฐานสากล ออกแบบหลักสูตรให้มีการเรียนรู้สอดคล้องกับบทบาทหน้าที่ความรับผิดชอบในการปฏิบัติงานจริง สอดคล้องกับความต้องการบุคลากรทางด้าน Cybersecurity ของภาคการธนาคาร และตามเท่าทันเทคโนโลยีต่าง ๆ ที่เกิดขึ้นอย่างรวดเร็ว เพื่อให้บุคลากรมีความรู้ ความเข้าใจ ความสามารถรับผิดชอบตามบทบาทหน้าที่ในสายงาน Cybersecurity รวมถึงพร้อมรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพและทันท่วงที และส่งเสริมภาพรวมของอุตสาหกรรมภาคการธนาคารให้มีบุคลากรที่เป็นกำลังสำคัญขององค์กรในด้าน Cybersecurity ให้มีปริมาณและศักยภาพที่เพิ่มมากขึ้น

งานด้านการสร้างความร่วมมือ

1. ความร่วมมือกับมหาวิทยาลัย

ด้วยเป้าหมายหลักข้อหนึ่งของ TB-CERT คือ การพัฒนาบุคลากรและเพิ่มพูนบุคลากรให้มีความรู้และทักษะความสามารถทางด้าน Cybersecurity ที่เพิ่มมากขึ้น นอกจากมุ่งเน้นการพัฒนาบุคลากรขององค์กรในภาคการธนาคารแล้ว TB-CERT ยังเล็งเห็นความสำคัญของการพัฒนาบัณฑิตเพื่อให้เกิดความตระหนักและความเข้าใจพื้นฐานเกี่ยวกับความมั่นคงปลอดภัยทาง Cybersecurity เพราะบัณฑิตในวันนี้จะเป็นกำลังสำคัญของบุคลากรในวันข้างหน้า และการสร้างความตระหนักรู้ทางด้าน Cybersecurity ก็ยังเป็นพื้นฐานสำคัญที่สามารถนำไปประยุกต์ใช้ รวมถึงต่อยอดการเรียนรู้ทักษะในแขนงอื่น ๆ ต่อไปได้ ทั้งนี้การสร้างความตระหนักรู้ทางด้าน Cybersecurity ไม่เพียงแค่เฉพาะในองค์การภาคการธนาคาร การให้ความรู้ทางด้าน Cybersecurity ให้กับหน่วยงานอื่น ๆ รวมถึงบุคคลทั่วไป จะช่วยส่งเสริมให้เกิดการยกระดับความมั่นคงปลอดภัยภาพรวมในระดับประเทศ ในปี 2021 ทาง TB-CERT ได้มีโอกาสเข้าร่วมบรรยายให้ความรู้แก่นักศึกษาชั้นปีที่ 2 และปีที่ 3 คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (สจล.) ในหลักสูตรวิศวกรรมนวัตกรรมคอมพิวเตอร์ (หลักสูตรนานาชาติ) จำนวน 40 ท่าน หัวข้อในการบรรยาย คือ บทบาทการใช้เทคโนโลยี API (Application Programming Interface) ในผลิตภัณฑ์และบริการปัจจุบัน เพื่อให้เกิดความเข้าใจเทคโนโลยี API บทบาทการใช้งาน ความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น โดยในการบรรยายได้เปิดโอกาสให้นักศึกษานำเสนอบทบาท API ในชีวิตประจำวันและการใช้เทคโนโลยี API ให้มีความปลอดภัย จากการนำเสนอผลงานของนักศึกษา เราเห็นศักยภาพของนักศึกษาในด้านต่าง ๆ ไม่ว่าจะเป็น การค้นคว้าหาความรู้ การคิดวิเคราะห์ การแก้ปัญหาตอบคำถาม และมีการศึกษาเชิงลึกในรายละเอียดทางเทคนิคที่น่าสนใจ คงปฏิเสธไม่ได้เลยว่านักศึกษาหรือบัณฑิตในวันนี้เป็นบุคลากรที่มีกำลังสำคัญในวันข้างหน้า ศักยภาพของเด็กในวันนี้สามารถเรียนรู้ได้เร็ว และมีการวิเคราะห์ความเข้าใจได้ดี ยิ่งการศึกษาที่เน้นหลักสูตรส่งเสริมให้เกิดทักษะที่จำเป็นกับการทำงาน จะยิ่งสร้างทรัพยากรบุคลากรที่มีคุณภาพให้กับประเทศต่อไป นอกจากนี้ TB-CERT ยังได้รับนักศึกษาฝึกงาน จากคณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (สจล.) เพื่อให้โอกาสน้องได้เรียนรู้และมีประสบการณ์การทำงานด้าน Cybersecurity โดยได้ให้โจทย์ในการทำวิทยานิพนธ์ เรื่อง Mobile security และ Wireless security ซึ่งจากหัวข้อดังกล่าวนักศึกษาฝึกงานได้ออกแบบโจทย์การเจาะระบบ และจำลองระบบโจทย์ขึ้นมาเพื่อใช้ในการทำวิทยานิพนธ์ ภายใต้การดูแลและให้คำแนะนำจากพี่ ๆ TB-CERT อย่างใกล้ชิด

2. ความร่วมมือกับหน่วยงาน MOU

TB-CERT ภายใต้สมาคมธนาคารไทย ได้มีการลงนามบันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย เมื่อวันที่ 22 กันยายน 2016 ร่วมกับ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงานคณะกรรมการ ก.ล.ต.) และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ร่วมกันจัดกิจกรรมภายใต้แผนการดำเนินงานตามข้อตกลงและขอบเขตของความร่วมมือเพื่อส่งเสริมและสนับสนุนระหว่างกันในด้านการรับมือภัยคุกคามทางไซเบอร์ ดังนี้

แผนงานด้าน Capability Building & Awareness : ดำเนินการจัดหลักสูตรพัฒนาบุคลากรด้านไซเบอร์

1. **การจัดหลักสูตรอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับคณะกรรมการภาคการเงิน (Board Awareness)** เมื่อวันที่ 12 ตุลาคม 2021 เวลา 9.00-12.00 น. ทางออนไลน์ร่วมกับ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และ สำนักงานคณะกรรมการกำกับและส่งเสริม การประกอบธุรกิจประกันภัย มีวัตถุประสงค์เพื่อสนับสนุนให้คณะกรรมการขององค์กรภาคการเงิน มีความรู้และตระหนักรู้ภัยคุกคามไซเบอร์ รวมทั้งเพิ่มโอกาสในการแลกเปลี่ยนมุมมองภัยคุกคามไซเบอร์ระหว่างองค์กร และสามารถนำไปปรับใช้ในการกำกับดูแลการบริหารจัดการความเสี่ยงของแต่ละองค์กร โดยมีกลุ่มเป้าหมาย ได้แก่ คณะกรรมการขององค์กรภาคการเงิน ภายใต้การกำกับดูแลของ ก.ล.ต. คปภ. ธปท. โดยมีผู้เข้าร่วมอบรมจากภาคการธนาคาร ระดับกรรมการ จำนวน 99 คน ภาคการลงทุน ระดับกรรมการ ประธานเจ้าหน้าที่บริหาร ระดับผู้ช่วยกรรมการ ระดับผู้บริหารสายงานไอที จำนวน 109 คน ภาคประกันภัย ระดับกรรมการ ประธานเจ้าหน้าที่บริหาร ระดับผู้บริหารสายงานไอที 72 คน รวมผู้เข้าร่วมอบรมทั้งสิ้น 280 คน

การจัดงานเป็นลักษณะของการจัดอบรมออนไลน์ ในหัวข้อ Cyber Resilience Leadership: Herd Immunity ดำเนินการโดยบริษัท ACIS โดยแบ่งช่วงการสัมมนาเป็น 3 ช่วง ได้แก่ ช่วงที่ 1 บรรยายให้ความรู้ในเรื่องของ Cybersecurity & Cyber Resilience ให้เห็นภาพในระดับ global landscape และแนวโน้มด้าน Cybersecurity ช่วงที่ 2 เสวนาหัวข้อ The Future of Privacy and Cybersecurity, Forecast to 2030 โดยมีตัวแทนของภาคการธนาคาร การลงทุน และประกันภัย มาร่วมแชร์มุมมองเกี่ยวกับสถานการณ์ในปัจจุบันที่ส่งผลกระทบต่อ Cybersecurity รวมทั้งการเตรียมความพร้อมในการรับมือต่อการบังคับใช้เรื่องข้อมูลส่วนบุคคล และช่วงที่ 3 การอบรม

ภาคปฏิบัติในหัวข้อ Privacy and Cybersecurity Risks Every Board of Directors Needs To Know แบ่งเป็น 3 ห้องตามภาคอุตสาหกรรมต่าง ๆ โดยวิทยากรบรรยายถึง กรอบการบริหารจัดการ ของแต่ละภาคอุตสาหกรรมที่ควรทราบ รวมถึง Case study ที่น่าสนใจและแลกเปลี่ยนมุมมองกับผู้เข้าร่วมอบรม และสรุป Key Takeaway จากงานสัมมนาในช่วงท้ายงาน

2. **โครงการ Financial Cybersecurity Boot Camp** จัดขึ้นต่อเนื่องเป็นครั้งที่ 5 ด้วยความร่วมมือระหว่าง สมาคมธนาคารไทย ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) มีวัตถุประสงค์หลักเพื่อส่งเสริมและพัฒนาความรู้ด้าน Cybersecurity ให้กับนิสิต นักศึกษา ให้มีศักยภาพที่พร้อมเข้าร่วมงานในภาคการเงิน โดยในปีนี้ด้วยสถานการณ์โควิด-19 ได้ปรับเป็นการจัดงานออนไลน์ 100% ในลักษณะหลักสูตรการเรียนการสอนออนไลน์ผ่าน Zoom Meeting และ Lab ภาคปฏิบัติ โดยเนื้อหาแบ่งเป็น 5 บทเรียน ได้แก่ 1) Core Security Principles 2) Network and Devices Security 3) Fundamental Cryptography 4) Operation System Security และ 5) Policy and Risk Management จัดหลักสูตรการสอนและการทดสอบโดยวิทยากรและคณะทำงานจากบริษัท ARIT ร่วมกับกิจกรรมเกมส์ด้าน Cybersecurity และการแชร์ประสบการณ์จากผู้เชี่ยวชาญที่ทำงานในภาคการเงิน ดำเนินโครงการเป็นระยะเวลา 3.5 วัน ตั้งแต่วันที่ 16-17 และ 23-24 ตุลาคม 2021 โดยมีนิสิต นักศึกษา สนใจเข้าร่วมโครงการทั้งสิ้น 130 คน

3. **จัดงาน Tech Career Coaching** จัดขึ้นเมื่อวันที่ 24 ตุลาคม เวลา 13.00-16.00 น. ในรูปแบบออนไลน์ โดยเป็นครั้งที่ 3 ของการจัดงานดังกล่าว มีวัตถุประสงค์หลักเพื่อเปิดโอกาสให้ผู้ที่สนใจในสายงานด้าน Cybersecurity ในภาคการเงินเข้ามาทำงาน ฝึกงาน หรือสมัครเข้ารับทุนการศึกษา ซึ่งได้รับการสนับสนุนและความร่วมมือด้วยดีจากฝ่ายบุคลากรของหน่วยงานภาคการเงินภายใต้การกำกับดูแลของ ธปท. สำนักงาน คปภ. และสำนักงาน ก.ล.ต. กว่า 30 องค์กร รวมทั้งวิทยากรจากภาคการเงินเพื่อแชร์ความรู้และประสบการณ์ในการทำงานด้าน Cybersecurity ภาคการเงิน แนวทางการสมัครงาน และการให้คำปรึกษาจากฝ่ายบุคลากรของหน่วยงานภาคการเงินผ่าน LINE Open chat มีผู้ลงทะเบียนเข้าร่วมงานทั้งสิ้น 449 คน

3. ความร่วมมือกับหน่วยงานภายนอก ในการรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

TB-CERT ได้มีการสร้างความร่วมมือกับหน่วยงานภายนอกภาคการธนาคารในการรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ซึ่งได้สร้างความร่วมมือกับบริษัทและองค์กรต่าง ๆ ได้แก่

1. **LINE Thailand** เพื่อช่วยในการประสานงานเมื่อเกิดเหตุ Line account official ของธนาคารถูกปลอมแปลง
2. **Operators: AIS, TRUE, DTAC, NT** เพื่อช่วยกันรับมือกับภัยไซเบอร์เมื่อเกิด SMS Phishing โดยการ Block SMS Fake sender ซึ่งกรณีเมื่อเกิดเหตุ TB-CERT ได้มีการตกลงแนวปฏิบัติร่วมกับ Operators ทั้ง 4 ราย
3. ร่วมมือกับ **กสทช.** และ **Telecom CERT** จัดทำแนวทางการทำงานการลงทะเบียนชื่อผู้ส่ง SMS และการรับมือเหตุการณ์ (SMS Sender name Registration and Incident Handling Process) เพื่อป้องกันภัยคุกคามอันเกี่ยวกับ SMS Phishing ของภาคส่วนโทรคมนาคมและภาคการธนาคาร
4. **ThaiCERT** เพื่อช่วยในการประสานงานกรณี Take down website ปลอมของธนาคารซึ่งเป็นเครือข่ายความสัมพันธ์ CERT

4. ความร่วมมือกับหน่วยงานสำคัญระดับประเทศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
(National Cyber Security Agency - NCSA)

อย่างที่เราทราบกันดีว่าปี 2021 เป็นอีกหนึ่งปีที่หลายองค์กรยังต้องพบกับความท้าทายทางธุรกิจประกอบกับสถานการณ์ของ COVID-19 ที่ยังแพร่ระบาดไม่หยุดยั้ง ทำให้อาชญากรไซเบอร์ใช้ประโยชน์เหตุการณ์นี้เข้าถึงประชาชนในประเทศไทยและทั่วโลกมากขึ้น Threat Intelligence หรือข้อมูลภัยคุกคาม เป็นสิ่งสำคัญและพูดถึงกันอย่างแพร่หลายในแวดวงความมั่นคงปลอดภัยไซเบอร์ การครอบครองข้อมูลภัยคุกคามนั้นยิ่งข้อมูลมีคุณภาพมากเท่าไหร่และมาถึงเราเร็วมากเท่าไหร่ ความเป็นต่อในการรักษาความมั่นคงปลอดภัยของระบบยิ่งมีมากขึ้นเท่านั้น ดังนั้น TB-CERT จึงเร่งสร้างความร่วมมือกับหน่วยงานต่าง ๆ ไม่ว่าจะเป็นความร่วมมือภายในประเทศ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Agency - NCSA) ซึ่งเป็นหน่วยงานหลักของประเทศที่มีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) หรือ ความร่วมมือกับต่างประเทศเช่น CERTFin, FS-ISAC, F-ISAC TW, FIRST เพื่อให้เกิดการแลกเปลี่ยนข้อมูลภัยคุกคามได้อย่างรวดเร็วและครอบคลุมมากขึ้น

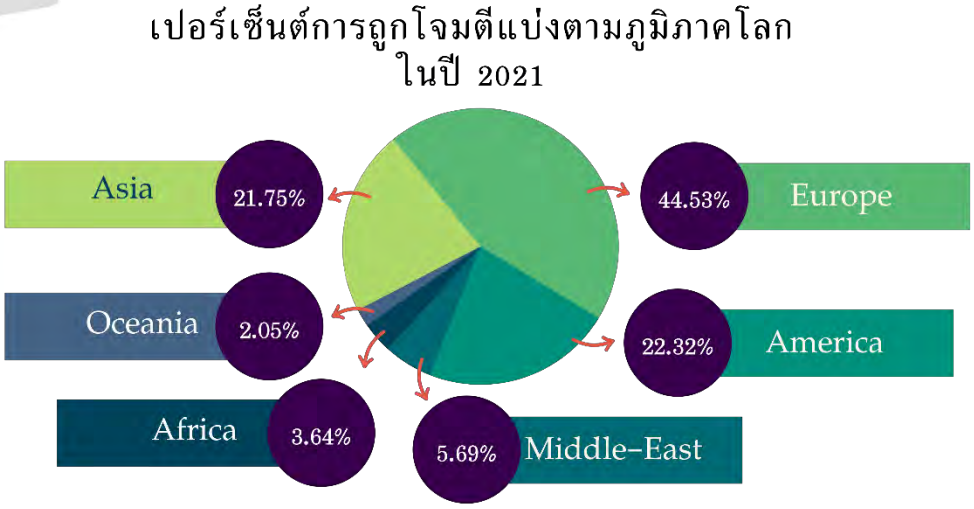
นอกจากการสร้างความร่วมมือในการแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์แล้วนั้น กระบวนการรับมือกับภัยไซเบอร์เมื่อเกิดเหตุการณ์ขึ้นก็ต้องอาศัยความร่วมมือจากทุกภาคส่วนที่เกี่ยวข้องด้วยเช่นกัน การซักซ้อมรับมือภัยไซเบอร์ซึ่งหากเปรียบเทียบให้เข้าใจง่าย ก็เหมือนกับการซ้อมหนีไฟ ที่ทุกอาคารจำเป็นต้องฝึกฝนประจำทุกปีเพื่อเป็นการเตรียมความพร้อมในการรับมือกับเหตุการณ์ที่คาดไม่ถึง ดังนั้นการซ้อมรับมือภัยคุกคามทางไซเบอร์ก็เช่นเดียวกัน จำเป็นต้องเตรียมพร้อมบุคลากรในองค์กรให้พร้อมกับการรับมือต่อเหตุการณ์ด้านไซเบอร์ เช่น เมื่อองค์กรเกิดโดนโจมตีด้วย Ransomware องค์กรนั้นจะมีแนวทางในการรับมืออย่างไรหากเกิดขึ้นจริง ซึ่งการซักซ้อมรับมือภัยคุกคามทางไซเบอร์นี้จะช่วยให้องค์กรนั้นมีความเข้าใจในการประเมินสถานการณ์และตอบสนองต่อเหตุการณ์ได้รวดเร็วทันเวลา ลดผลกระทบที่อาจจะเกิดขึ้นและสร้างความเสียหายในวงกว้างได้ ดังนั้นการซ้อมรับมือต่อเหตุการณทางไซเบอร์ในรูปแบบต่าง ๆ จึงเป็นส่วนสำคัญหนึ่งที่ช่วยเสริมสร้างความแข็งแกร่งให้กับองค์กร อีกทั้งเมื่อ

ผู้ปฏิบัติงานด้านไซเบอร์และผู้ที่เกี่ยวข้องทราบถึงกระบวนการ แนวทางในการตอบสนองต่อเหตุการณ์ต่าง ๆ ที่เกิดได้อย่างมีประสิทธิภาพได้แล้วนั้นจะช่วยให้เกิดการรับมือกับภัยต่าง ๆ เหล่านั้นได้อย่างรวดเร็ว ทันต่อเหตุการณ์ได้อย่างมีประสิทธิภาพ

สำหรับการซ้อมรับมือภัยไซเบอร์ภาคการธนาคารประจำปี 2021 ได้มีแนวคิดของการสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้องต่อเหตุการณ์ภัยไซเบอร์ และเพื่อให้การซ้อมครั้งนี้เสมือนจริงหรือใกล้เคียงกับความเป็นจริงมากที่สุด TB-CERT จึงได้สร้างแพลตฟอร์มที่ใช้ในการซ้อมครั้งนี้ และออกแบบสถานการณ์จำลองขึ้นโดยได้รับการสนับสนุนจากหน่วยงานสมาชิกของ TB-CERT ส่งบุคลากรเข้ามาร่วมพัฒนาและออกแบบสถานการณ์จำลองของการซ้อมครั้งนี้ และที่สำคัญได้รับการอนุเคราะห์จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Agency - NCSA) เข้ามาเป็นส่วนหนึ่งของคณะทำงานและพัฒนาสถานการณ์จำลองร่วมกัน ทำให้ทราบถึงกระบวนการการรับมือ การประสานงานเชื่อมโยงกันระหว่างหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศภาคการธนาคารธนาคารแห่งประเทศไทยซึ่งเป็นหน่วยงานกำกับดูแลสถาบันการเงิน TB-CERT และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Agency - NCSA) ซึ่งหนึ่งในวัตถุประสงค์หลักของการซ้อมรับมือภัยคุกคามทางไซเบอร์ในปีนี้ที่ต้องการเน้นคือ เตรียมความพร้อมในเรื่องของการประสานงานข้ามองค์กรเมื่อเกิดเหตุการณ์ภัยไซเบอร์ขึ้น ดังนั้นการสร้างความร่วมมือกับหลายภาคส่วนที่เกี่ยวข้อง จึงจำเป็นอย่างยิ่งในการสนับสนุนกระบวนการประสานงานให้เป็นไปอย่างราบรื่นและมีประสิทธิภาพ

บทวิเคราะห์ภัยคุกคามทางไซเบอร์ 2021

ในปี 2021 TB-CERT ได้รวบรวมสถิติภัยคุกคามทางไซเบอร์จากระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence หรือ CTI) ของ TB-CERT จากข้อมูลพบว่า ภูมิภาคยุโรป เป็นภูมิภาคของโลกที่ถูกโจมตีในปี 2021 มากเป็นอันดับ 1 คิดเป็นสัดส่วน 44.53% รองลงมาเป็นภูมิภาคอเมริกา เป็นสัดส่วน 22.32% และภูมิภาคเอเชีย เป็นสัดส่วน 21.75% ตามลำดับ ดังรูปที่ 13

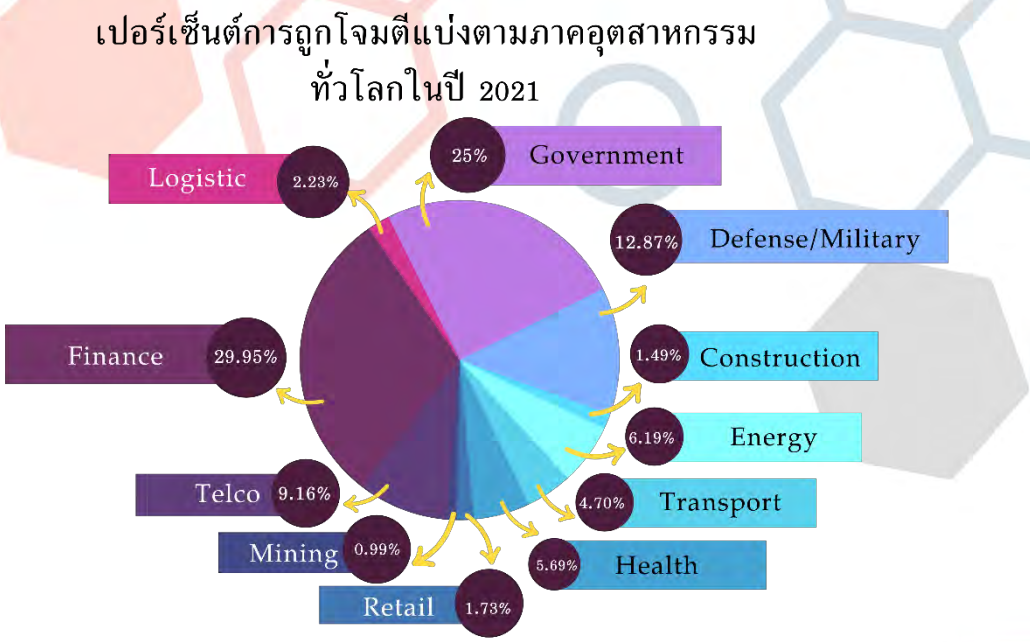


รูปที่ 13 เปอร์เซ็นต์การถูกโจมตีแบ่งตามภูมิภาคโลกในปี 2021

อ้างอิง ข้อมูลจากระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence หรือ CTI) ของ TB-CERT

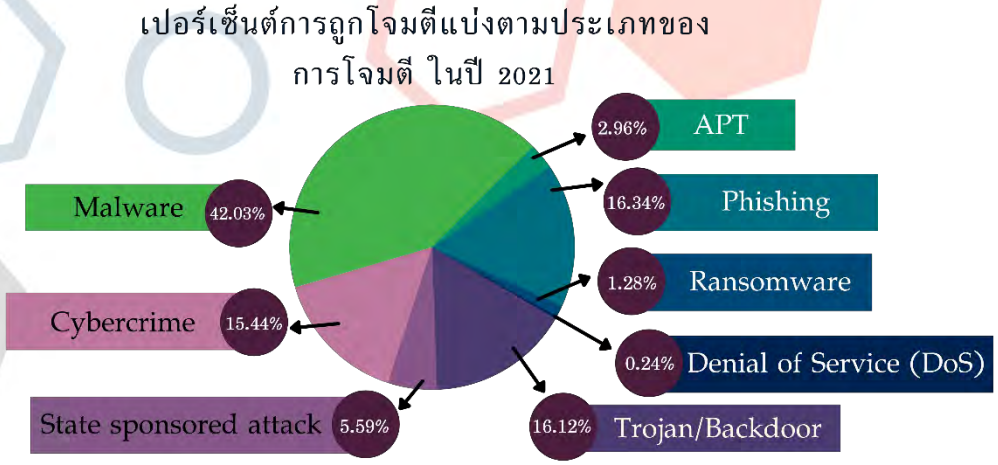
จากสถิติภัยคุกคามทางไซเบอร์ในปี 2021 ภาคการเงินนั้นพบเหตุการณ์การโจมตีมากเป็นอันดับ 1 คิดเป็นสัดส่วน 29.95% ดังรูปที่ 14 ถึงแม้ว่าภาคการเงินเป็นภาคอุตสาหกรรมที่มีการลงทุนด้านการรักษาความมั่นคงปลอดภัยในระดับสูงทั้งทางด้านบุคลากร เทคโนโลยี และกระบวนรับมือภัยคุกคามทางไซเบอร์ แต่แรงจูงใจหลักของการโจมตียังคงเป็นเรื่องเงิน ที่กลุ่มผู้โจมตีคาดหวังว่าจะได้รับมากกว่าการโจมตีในภาคอุตสาหกรรมอื่น

ลำดับถัดมาเป็นภาครัฐบาล คิดเป็นสัดส่วน 25% และภาคความมั่นคง คิดเป็นสัดส่วน 12.87% ดังรูปที่ 14 ซึ่งเห็นได้ชัดเจนจากประกาศแจ้งเตือนจากหน่วยงานความมั่นคงต่าง ๆ เช่น Cybersecurity and Infrastructure Security Agency (CISA) **[1]**, The Federal Bureau of Investigation (FBI), The Australian Cyber Security Centre (ACSC), และ The United Kingdom's National Cyber Security Centre (NCSC) **[2]** ถึงภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นและการโจมตีที่ได้รับการสนับสนุนจากภาครัฐ (State-sponsored attack)



รูปที่ 14 เปอร์เซ็นต์การถูกโจมตีแบ่งตามภาคอุตสาหกรรมทั่วโลกในปี 2021
อ้างอิง ข้อมูลจากระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence หรือ CTI) ของ TB-CERT

สถิติแบ่งประเภทของการโจมตีอันดับ 1 คือ มัลแวร์ (Malware) ที่สัดส่วน 42.03% และลำดับถัดมา คือ ฟิชชิง (Phishing) ที่สัดส่วน 16.34% และ Trojan/Backdoor ที่สัดส่วน 16.12% ตามลำดับ ดังรูปที่ 15 ซึ่งใช้เทคนิคการหลอกลวงแบบผสมผสานที่ซับซ้อนมากขึ้น ในปี 2021 เทคนิคที่เห็นชัดเจนจากกลุ่ม Threat actors ได้นำมาใช้กัน คือการใช้เทคนิคที่เรียกว่า Initial Access Brokers (IABs) เป็นการว่าจ้างคนภายในองค์กรให้คลิกลิงก์หรือติดตั้งโปรแกรมมัลแวร์ (Malware) หรือ Trojan/Backdoor ที่ทางกลุ่ม Threat actors ได้จัดเตรียมไว้ในการเข้าถึงระบบเบื้องต้นขององค์กรได้จากภายนอก เพื่อขยายผลการโจมตีไปยังระบบสำคัญต่อไป จากข้อมูลดังกล่าวสอดคล้องกับข้อมูลของ Group-IB **[3]** รายงานทางสถิติเรื่อง HI-TECH Crime Trends 2021/2022: Access Brokers พบว่าในปี 2020 มีจำนวนการขาย Initial access จำนวน 724 ครั้ง เพิ่มขึ้นจากปี 2019 มีจำนวนการขาย Initial access จำนวน 130 ครั้ง ซึ่งเพิ่มขึ้นคิดเป็น 457 เปอร์เซ็นต์ และจากรายงานดังกล่าวพบว่าในปี 2021 เพียงครึ่งปีแรก พบว่ามีจำนวนการขาย Initial access จำนวน 652 ครั้ง ซึ่งเกือบเทียบเท่ากับปี 2020 ทั้งปีรวมกัน จากข้อมูลดังกล่าวเห็นได้ชัดเจนถึงเทคนิคการโจมตีที่เริ่มปรับเปลี่ยนไปของกลุ่ม Threat actors ในปัจจุบัน



รูปที่ 15 เปอร์เซ็นต์การถูกโจมตีแบ่งตามประเภทของการโจมตี ในปี 2021

อ้างอิง ข้อมูลจากระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence หรือ CTI) ของ TB-CERT

สรุปเหตุการณ์สำคัญที่ TB-CERT ช่วยในการประสานงานแก้ไขรับมือ

ในปี 2021 TB-CERT ได้รวบรวมสรุปเหตุการณ์สำคัญและการรับมือภัยไซเบอร์ในระดับภาคการธนาคาร ที่ได้รับการร้องขอจากหน่วยงานสมาชิกให้ช่วยประสานงาน เพื่อยับยั้งภัยคุกคามภัยทางไซเบอร์ ซึ่งสรุปได้ดังนี้

เหตุการณ์ที่ 1 ในช่วงไตรมาสที่ 1 พบว่ามีปริมาณ SMS phishing หลอกลวงประชาชนจำนวนมาก ในรูปแบบที่มีการตั้งชื่อผู้ส่ง SMS (SMS Sender) เป็นชื่อคล้ายรวมถึงการใช้ชื่อเหมือนกับที่ทางธนาคารใช้งานอยู่ ทางทีมงาน TB-CERT จึงได้หารือร่วมกับผู้รับผิดชอบหน่วยงานภาคโทรคมนาคม เพื่อหาแนวทางการป้องกันในระดับภาคการธนาคาร

เหตุการณ์ที่ 2 สืบเนื่องจากการร่วมมือกับผู้รับผิดชอบหน่วยงานภาคโทรคมนาคม ทำให้เกิดแนวทางการป้องกันเชิงรุกเพื่อยับยั้งภัยคุกคามที่จะเกิดกับประชาชน เกิดการจัดทำทะเบียนชื่อผู้ส่ง (SMS Sender) และการแจ้งระงับเหตุ SMS Phishing ส่งผลให้จำนวนเหตุการณ์ใช้ SMS ในการหลอกลวงประชาชนลดลงอย่างมีนัยสำคัญ ในขณะเดียวกันช่วงไตรมาสที่ 2 พบการประกาศช่องโหว่การโจมตี Pulse Secure และ PrintNightmare แบบ Zero-day attack ระดับรุนแรง TB-CERT จึงได้ออกคำแนะนำทางเทคนิค (Technical Recommendation) เพื่อให้หน่วยงานสมาชิกใช้เป็นข้อมูลในการรับมือ

เหตุการณ์ที่ 3 ในช่วงของไตรมาสที่ 3 พบการโจมตีทางไซเบอร์กับบริษัทผู้ให้บริการไอที ภายนอก (3rd party attack) โดยการใช้มัลแวร์เรียกค่าไถ่ (Ransomware) จากกลุ่มแฮกเกอร์ชื่อกลุ่ม BlackMatter ที่อาจจะส่งผลต่อเนื่องกับภาคการธนาคาร ซึ่งเป็นเหตุการณ์ที่สำคัญเหตุการณ์หนึ่งของปี TB-CERT จึง ได้ประสานงานบริษัทผู้ให้บริการไอทีภายนอกดังกล่าว เพื่อร่วมกันหาแนวทางป้องกันที่อาจจะส่งผลกระทบในวงกว้าง ต่อภาคการธนาคาร และได้ออกคำแนะนำทางเทคนิค (Technical Recommendation) รวมถึงข้อมูลสัญญาณบ่งชี้การบุกรุก (Indicator of Compromise) เพื่อให้หน่วยงานสมาชิกใช้เป็นข้อมูลในการรับมือและป้องกันไม่ให้เกิดการโจมตีในรูปแบบห่วงโซ่อุปทาน (Supply Chain Attack) จากเหตุการณ์ดังกล่าว

เหตุการณ์ที่ 4 ในช่วงของไตรมาสที่ 4 พบการโจมตีที่มีรูปแบบผสมผสานและมีความซับซ้อนมากขึ้นมีการผสมผสานหลายเทคนิคในรูปแบบการหลอกลวงทางดิจิทัล (Digital Fraud) โดยพบว่ามิจฉาชีพเริ่มมีการปรับเปลี่ยนรูปแบบการหลอกลวงโดยสร้างบัญชี LINE ปลอมเป็นบริษัทผู้ให้บริการเงินกู้ หลอกประชาชนให้หลงเชื่อว่าเป็นบริษัทที่ปล่อยเงินกู้จริง พบมีการแอบอ้างข้อมูลการจดทะเบียนนิติบุคคล รวมถึงการใช้ข้อมูลส่วนบุคคล รูปถ่าย บัตรประชาชนของผู้อื่นมาแอบอ้างเป็นพนักงานบริษัทเงินกู้นั้น พอเหยื่อหลงเชื่อก็จะทำธุกรรมกู้เงินกับบริษัทนั้นทันที สิ่งที่ TB-CERT ดำเนินการกรณีเช่นนี้คือประสานขอความร่วมมือไปยังบริษัท LINE คอร์ปอเรชั่นเพื่อทำการปิดบัญชีหลอกลวงดังกล่าว และยังพบสัญญานบ่งชี้ว่ามีการใช้เซิร์ฟเวอร์หลากหลายประเทศมากขึ้นในการสร้างเว็บไซต์ปลอม เช่น จีน อเมริกา ไอซ์แลนด์ กัมพูชา รวมถึงประเทศไทยเป็นฐานในการโจมตี โดย TB-CERT ได้ประสานหน่วยงาน CERT ตามความร่วมมือเพื่อ Takedown เซิร์ฟเวอร์ดังกล่าวอีกด้วย

เหตุการณ์ที่ 5 ในช่วงเดือนตุลาคม พบการโจมตีแบบ BIN Attack ที่ขยายวงกว้างและมีประชาชนได้รับความเดือดร้อนจำนวนมาก โดยกลุ่มมิจฉาชีพจะใช้ข้อมูลรูปแบบจากบัตรจริง และสร้างเลขบัตรเพิ่มขึ้นโดยสุ่มเลขบัตรและวันหมดอายุ ในการโจมตีดังที่ปรากฏเป็นข่าว TB-CERT จึงออกประกาศ Security Awareness เรื่อง "ถอดรหัส กลโกง BIN Attack" เพื่อให้ประชาชนชนทราบถึงแนวทางการรับมือและการป้องกันภัย

เหตุการณ์ที่ 6 ในช่วงเดือนธันวาคม พบการประกาศช่องโหว่ Log4Shell (CVE-2021-44228) ซึ่งเป็นช่องโหว่ระดับวิกฤต (Critical) ของ Apache Log4j Library ที่มีผลกระทบต่อผลิตภัณฑ์หรือแอปพลิเคชันที่มีการใช้งาน Library ดังกล่าวในวงกว้างหลายผลิตภัณฑ์ TB-CERT ได้ออกประกาศแจ้งเตือนและคำแนะนำทางเทคนิค (Technical Recommendation) รวมถึงข้อมูลสัญญาณบ่งชี้การบุกรุก (Indicator of Compromise) จากเหตุการณ์การโจมตีดังกล่าวที่เกิดขึ้นทั่วโลก รวมถึงข้อมูลการพยายามโจมตีจากหน่วยงานสมาชิก เพื่อใช้เป็นข้อมูลในการรับมือเชิงรุก (Proactive Action) ในระดับภาคธนาคาร

Reference

[1] https://www.cisa.gov/uscert/northkorea

[2] https://www.cisa.gov/uscert/ncas/current-activity/2021/11/17/iranian-government-sponsored-apt-cyber-actors-exploiting-microsoft

[3] รายงานทางสถิติเรื่อง HI-TECH Crime Trends 2021/2022: Access Brokers

https://www.group-ib.com/resources/threat-research/2021-reports.html

แนวโน้มภัยไซเบอร์ในปี 2022

จากการรวบรวมข้อมูลเหตุการณ์ที่เกิดขึ้นในปีที่ผ่านมา ประกอบกับการวิเคราะห์สถานการณ์และแนวโน้มจากรายงานหลายแหล่ง TB-CERT ได้คาดการณ์แนวโน้มรูปแบบการโจมตีทางไซเบอร์ สำหรับปี 2022 ดังนี้

1. **ภัยไซเบอร์จากห่วงโซ่อุปทาน (Supply Chain Attack)**

ปลายปี 2020 มีเหตุการณ์การโจมตีบริษัท Solarwinds ซึ่งเป็นบริษัทที่พัฒนาระบบการเฝ้าระวังระบบงานไอที (IT Monitoring Solution) ที่มีการใช้งานอย่างกว้างขวางทั่วโลกโดยการโจมตีดังกล่าวทำให้มีการส่งผ่านมัลแวร์ผ่านกลไกของการ Update Hotfix ไปยังลูกค้า ซึ่งในปี 2021 จากเหตุการณ์กลุ่มแฮกเกอร์ชื่อกลุ่ม BlackMatter โจมตีบริษัทผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (3rd Party Service Provider) และเหตุการณ์พบช่องโหว่ของ Log4shell นั้น เป็นสิ่งที่ทุกอุตสาหกรรมเกิดการตื่นตัวอย่างมากในการดูแลและยกระดับการป้องกันภัยไซเบอร์จากการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ รวมถึงแอปพลิเคชันและอุปกรณ์ด้านเทคโนโลยีสารสนเทศที่ผลิตและพัฒนาโดยบริษัทอื่น ซึ่งผลกระทบจากการโจมตีประเภทนี้ใช้กลไกของการเชื่อถือระหว่างธุรกิจในยุคที่ธุรกิจมีการเชื่อมโยงกันเป็นห่วงโซ่อุปทาน (Supply Chain) ทำให้มีการตรวจสอบความเสี่ยงที่น้อยกว่าช่องทางอินเทอร์เน็ต ด้วยเหตุนี้จึงสามารถหลบระบบป้องกันภัยเข้าไปยังระบบเครือข่ายขององค์กรเป้าหมาย เพื่อกระทำการขโมยข้อมูล แพร่กระจายมัลแวร์ หรือควบคุมการทำงานระบบสำคัญ ซึ่งการโจมตีลักษณะนี้ส่งผลกระทบในวงกว้างกับหลายภาคอุตสาหกรรม รวมถึงภาคการเงินการธนาคาร แต่หากมองอีกมุมหนึ่งเหตุการณ์ดังกล่าวก็เป็นตัวเร่งให้ทุกภาคส่วนพร้อมใจกันในการยกระดับมาตรการรับมือและป้องกันภัยไซเบอร์ให้มีความเข้มแข็งมากขึ้น

2. **การโจมตีแพลตฟอร์มแลกเปลี่ยน Cryptocurrency กระเป๋าเงินอิเล็กทรอนิกส์ และระบบการเงินแบบไร้ศูนย์กลาง (Cryptocurrency Exchange, eWallet and Decentralized Finance (DeFi)**

จากกระแสความนิยมต่อการใช้งานและการลงทุนใน คริปโทเคอร์เรนซี (Cryptocurrency) ที่เพิ่มขึ้นเป็นทวีคูณ ส่งผลให้เป็นที่ดึงดูดความสนใจจากกลุ่มมิจฉาชีพ หรือกลุ่ม Threat Actors มากขึ้นเช่นกัน ดังจะเห็นได้จากเหตุการณ์อาชญากรรมไซเบอร์ที่เกี่ยวข้องกับคริปโทเคอร์เรนซีมีจำนวนเพิ่มสูงขึ้น เช่น

เหตุการณ์ที่ 1 บริษัทแลกเปลี่ยน Crypto ชื่อ BitMart เกิดความเสียหายจากการถูกเจาะระบบ โดยสูญเสียเงินในระบบ Crypto รวมมูลค่ากว่า 150 ล้านดอลลาร์สหรัฐ หรือกว่า 5 พันล้านบาท [1]

[1] https://www.bbc.com/news/business-58163917

เหตุการณ์ที่ 2 PolyNetwork ซึ่งเป็นแพลตฟอร์มผู้ให้บริการเกี่ยวกับ Decentralized Finance (DeFi) ถูกโจมตีแพลตฟอร์มและขโมยเหรียญ Crypto ไป เป็นมูลค่ารวมกว่า 600 ล้านดอลลาร์สหรัฐ หรือเกือบ 20,000 ล้านบาท ซึ่งถือเป็นจำนวนเงินที่สูงสุดเป็นประวัติการณ์[2]

กระแสอาชญากรรมไซเบอร์ที่เกี่ยวข้องกับ Cryptocurrency ที่เพิ่มสูงขึ้นนั้น สอดคล้องกับรายงานของ Chainalysis ซึ่งเป็นบริษัทด้านการวิจัยบล็อกเชน ได้ระบุว่า กลุ่มอาชญากรไซเบอร์จากเกาหลีเหนือได้ปฏิบัติการโจมตีแพลตฟอร์มแลกเปลี่ยนสกุลเงินดิจิทัล ทั้งหมด 7 ครั้งในปี 2021 มูลค่าความเสียหายรวมแล้วเกือบ 400 ล้านดอลลาร์สหรัฐ หรือประมาณ 13,270 ล้านบาท[3]

TB-CERT คาดการณ์ว่า เหตุการณ์อาชญากรรมไซเบอร์ที่เกี่ยวข้องกับ Cryptocurrency จะยังคงเพิ่มสูงขึ้นอย่างต่อเนื่อง ในปี 2022 และเป็นความท้าทายต่อภาคการเงินการธนาคาร ผู้ที่ให้บริการทางการเงิน หรือ ผู้ที่จะนำ Cryptocurrency ไปใช้งานนั้นได้เตรียมการรับมือ สร้างมาตรฐานด้านความมั่นคงปลอดภัยของระบบแลกเปลี่ยนคริปโทเคอร์เรนซี (Cryptocurrency Exchange) และกระเป๋าเงินอิเล็กทรอนิกส์ (eWallet) รวมถึงการเร่งให้ความรู้ต่อภาคประชาชน เพื่อให้รู้เท่าทันภัยไซเบอร์ที่เกี่ยวข้องกับ Cryptocurrency

3. ช่องว่างของความรู้ (Knowledge Gaps) ในการใช้เทคโนโลยีอุบัติใหม่ (Emerging Technology)

การเกิดขึ้นใหม่ของเทคโนโลยี หรือ เทคโนโลยีอุบัติใหม่ (Emerging Technology) จะยังคงมีบทบาทสำคัญที่ทำให้เกิดการพัฒนาหลากหลายด้านในอนาคตอันใกล้ ทำให้เกิดการเปลี่ยนแปลงทั้งทางด้านสังคมและเศรษฐกิจ ตัวอย่างเช่น กระแสโลกเสมือนจริง (Metaverse) ทำให้เกิดธุรกรรมใหม่ ๆ และการซื้อขายสินค้า บริการ ที่ดินในโลกเสมือนจริง (Metaverse) ในยุคดิจิทัลนี้เราคงหลีกเลี่ยงไม่ได้ถึงการเปลี่ยนแปลงของเทคโนโลยีใหม่ ๆ ในหลายด้าน (Emerging Technology) แต่การเปลี่ยนที่รวดเร็วมักจะทำให้เกิดช่องว่างของความรู้ (Knowledge Gaps) ต่อผู้ใช้งานและเป็นช่องโหว่ให้กลุ่มมิจฉาชีพใช้ในการโจมตีจากการไม่รู้เท่าทันเทคโนโลยีในการหลอกลวงผู้ใช้งานได้ จึงเป็นความท้าทายของผู้ใช้งานและผู้พัฒนาเทคโนโลยีใหม่ ๆ ในการเติมเต็มความรู้ให้มีการใช้งานอย่างถูกต้องและมีความปลอดภัย เพื่อลดช่องว่างของความรู้ (Knowledge Gaps) และทำให้เกิดการพัฒนาด้านสังคมและเศรษฐกิจอย่างยั่งยืน

[2] https://www.reuters.com/technology/defi-platform-poly-network-reports-hacking-loses-estimated-600-million-2021-08-11/
[3] https://markets.businessinsider.com/news/currencies/cryptocurrency-ransomware-attacks-russian-cybercriminals-revenue-400-million-blockchain-chainanlysis-2022-2

4. ช่องโหว่ในระบบอัตโนมัติ (Autonomous System)

การใช้งานระบบอัตโนมัติต่าง ๆ มีการใช้กันอย่างแพร่หลายทั้งในชีวิตประจำวันเพื่อความสะดวกสบาย ในภาคอุตสาหกรรมและในโครงสร้างพื้นฐานสำคัญระดับประเทศ ระบบอัตโนมัติจะยังคงเป็นกระแสหลักต่อไปในการพัฒนาเศรษฐกิจและขับเคลื่อนประเทศในปัจจุบัน แต่การพัฒนาระบบอัตโนมัติเหล่านี้ส่วนใหญ่ต้องมีการเชื่อมต่อหรือการเรียกใช้งาน API (Application Programming Interface) ในการเชื่อมโยง และรับ-ส่งข้อมูลระหว่างกัน ดังนั้นการออกแบบระบบ ผู้พัฒนาจำเป็นต้องคำนึงถึงเรื่องความมั่นคงปลอดภัย เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ในการโจมตีระบบอัตโนมัติ ให้เกิดความเสียหายได้ ซึ่งอาจจะทำให้เกิดผลกระทบที่ขยายขอบเขตไปได้อย่างรวดเร็วและสร้างผลกระทบต่อคู่ค้าทางธุรกิจและลูกค้าในวงกว้างได้

5. การโจมตีจากรูปแบบการทำงานที่เปลี่ยนแปลงไปเป็นแบบ Work From Anywhere (WFA)

จากการแพร่ระบาดของโรคไวรัสโคโรนา 2019 (COVID-19) ทำให้เห็นการเปลี่ยนแปลงรูปแบบการทำงานทั่วโลก หลายองค์กรได้ปรับเปลี่ยนให้พนักงาน ทำงานจากที่ไหนก็ได้ (Work From Anywhere) ซึ่งหลายองค์กรได้ผลลัพธ์ในด้านประสิทธิภาพการทำงานดีขึ้น จึงได้เริ่มปรับนโยบายให้พนักงานสามารถทำงานในรูปแบบนี้ได้ ซึ่งก็อาจจะกลายเป็นเรื่องปกติของการทำงาน แต่การทำงานรูปแบบนี้พนักงานยังคงมีความจำเป็นเข้าถึงข้อมูลขององค์จากภายนอก การที่พนักงานเข้าถึงข้อมูลหรือระบบขององค์กรจากที่ไหนก็ได้อาจจะเป็นช่องโหว่สำคัญที่กลุ่ม Threat Actors ใช้โจมตีองค์กรได้ จึงเป็นเรื่องสำคัญทั้งพนักงานเองที่จะต้องปฏิบัติตามนโยบายความปลอดภัยอย่างเคร่งครัด และองค์กรที่จะต้องมีมาตรการความปลอดภัยที่เหมาะสมกับรูปแบบการทำงานจากที่ไหนก็ได้ (Work From Anywhere)

6. การใช้ Social Network เป็นเครื่องมือในการโจมตี

ในปีที่ผ่านมาพบว่ากลุ่มมิจฉาชีพมีการใช้งานช่องทาง Social Network เป็นเครื่องมือในการหลอกลวงประชาชนเพิ่มมากขึ้น พบการสร้างตัวตนปลอมในโลกออนไลน์ แอบอ้างชื่อบุคคล ชื่อหน่วยงาน และปลอมแปลงเอกสารสำคัญ เพื่อให้ดูน่าเชื่อถือในการหลอกเหยื่อให้หลงเชื่อโดยง่าย รวมถึงการหลอกให้ติดตั้งแอปพลิเคชันอันตราย ขโมยข้อมูลส่วนบุคคลหรือนำข้อมูลไปทำธุรกรรมต่าง ๆ ในรูปแบบ Digital Fraud ซึ่งในปีนี้แนวโน้มการใช้ Social Network เป็นเครื่องมือในการโจมตีและหลอกลวงจะยังคงเกิดขึ้นอย่างต่อเนื่อง และยังเป็นความท้าทายร่วมกันทุกภาคส่วนในการให้ความรู้กับภาคประชาชนในการใช้งาน Social Network ให้มีความปลอดภัย ไม่ให้ตกเป็นเหยื่อของกลุ่มมิจฉาชีพ

References:

https://go.chainalysis.com/2021-Crypto-Crime-Report.html

https://www.reuters.com/technology/defi-platform-poly-network-reports-hacking-loses-estimated-600-million-2021-08-11/

เป้าหมายการดำเนินการของ TB-CERT ในปี 2022

แม้ว่าจะเจอความท้าทายที่ยากลำบากในสถานการณ์ COVID-19 แต่ในหลายภาคธุรกิจก็ได้ปรับตัวให้เข้ากับสถานการณ์และรักษาธุรกิจนั้นให้อยู่รอดได้ TB-CERT ก็เช่นเดียวกัน เราได้ดำเนินการตามภารกิจหลักอย่างต่อเนื่อง เพื่อยกระดับความมั่นคงปลอดภัยของภาคการธนาคารในรูปแบบวิถีชีวิตและการทำงานใหม่ให้ตอบรับต่อสถานการณ์เช่นนี้ได้อย่างมีประสิทธิภาพและมีคุณภาพ ไม่ว่าจะเป็นการประชุมออนไลน์ การจัดสัมมนาออนไลน์ เรายังคงดำเนินการตามภารกิจเช่นเดิมแม้อาจจะต้องปรับเปลี่ยนรูปแบบไปบ้างก็ตาม สิ่งสำคัญหนึ่งของการเป็น CERT (Computer Emergency Response Team) ของ TB-CERT คือ การสร้างความไว้เนื้อเชื่อใจกัน (Build Trust) เพื่อประโยชน์ต่อทุกฝ่ายในการแลกเปลี่ยนข้อมูลกัน และเป็นการสร้างสภาพแวดล้อมที่ดีของกลุ่ม รวมถึงการมีทีมที่ดี ที่สามารถรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงทีและมีประสิทธิภาพ เพื่อประโยชน์ต่อองค์กรและสาธารณะ แต่การคงไว้ซึ่งประสิทธิภาพและคุณภาพของ TB-CERT นั้นจำเป็นต้องอาศัยสมาชิกของ TB-CERT ร่วมมือกันเป็นน้ำหนึ่งใจเดียวกัน รักษากฎระเบียบของการอยู่ร่วมกันได้อย่างดี และที่สำคัญคือทักษะความรู้ของบุคลากรด้านไซเบอร์ที่ต้องอาศัยประสบการณ์ในการทำงาน การเรียนรู้ร่วมกันซึ่งเป็นอีกเส้นทางหนึ่งในการเรียนรู้ได้เร็วขึ้นเท่าทันต่อโลกดิจิทัลในปัจจุบันที่ภัยคุกคามทางไซเบอร์ได้พัฒนาขึ้นอย่างรวดเร็วเฉกเช่นเดียวกันกับเทคโนโลยีที่เปลี่ยนแปลงตลอดเวลา ในสภาวการณ์ของภัยคุกคามทางไซเบอร์ในปัจจุบัน ในปี 2022 นี้ ทาง TB-CERT ได้มุ่งเน้นเป้าหมายในการดำเนินการใน 4 ด้านดังนี้

1. **วิเคราะห์ Threat เชิงลึก**ให้กับสมาชิกซึ่งเป็นแนวทางการนำ CERT ไปสู่ CERT Maturity ที่ Level 4 และเป็นหัวใจสำคัญของการพัฒนา CERT ให้มีประสิทธิภาพและเกิดประโยชน์สูงสุดต่อสมาชิก
2. **ขยายเครือข่ายความร่วมมือ** เพื่อให้เกิดการแชร์ข้อมูลที่หลากหลายและมากขึ้นทำให้เรามีข้อมูลเพื่อใช้ในการวิเคราะห์ได้ดีขึ้น เป็นประโยชน์ต่อการรับรู้ข่าวสารที่รวดเร็วทันต่อเหตุการณ์ที่อาจจะเกิดขึ้นและช่วยให้สมาชิกสามารถป้องกันภัยได้ทันท่วงที
3. **กำหนดมาตรฐาน**สำหรับเทคโนโลยีใหม่ที่ใช้ในธุรกิจธนาคาร
4. **พัฒนาบุคลากร**ที่มีอยู่ให้มีศักยภาพเพิ่มขึ้น โดยเน้นการฝึกอบรมแบบเน้นไปที่การลงมือปฏิบัติหลังจากมีการอบรมเชิงทฤษฎีแล้ว ซึ่งกลยุทธ์นี้จะช่วยให้สมาชิกสามารถนำไปปรับใช้งานได้จริง

บทสรุป

สังคมที่อุดมไปด้วยการพัฒนาของเทคโนโลยีที่เป็นไปอย่างรวดเร็วและการนำเอาเทคโนโลยีดังกล่าวไปใช้ในหลากหลายอุตสาหกรรมเป็นการยกระดับความเป็นอยู่ เพิ่มประสิทธิผลในการสร้างสรรค์ และสร้างเสริมความคิดนวัตกรรม ซึ่งจะทำให้เป็นการต่อยอดผลผลิตต่าง ๆ อย่างก้าวกระโดด สภาพการณ์เช่นนี้ การพัฒนาศักยภาพของบุคคลากรเป็นสิ่งสำคัญอันดับแรก เนื่องจากมีการนำเอาเทคโนโลยีใหม่เข้ามาใช้กันอย่างแพร่หลายมากขึ้น จึงจำเป็นต้องมีการพัฒนาความรู้ด้านใหม่ ๆ ให้เท่าทันเทคโนโลยีที่นำไปใช้งาน นอกจากจะต้องทราบถึงวิธีการนำไปใช้งานแล้ว จะต้องเข้าใจความเสี่ยงที่จะเกิดจากเทคโนโลยีนั้นด้วย ไม่ว่าจะเป็นความเสี่ยงด้านข้อมูลส่วนบุคคล ความเสี่ยงด้านความเป็นส่วนตัว หรือความเสี่ยงที่เกิดจากห่วงโซ่อุปทาน (Supply Chain Risk) เนื่องจากเป็นการใช้เทคโนโลยีของบุคคลภายนอกและเชื่อมต่อแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นอีกด้วย

ด้านของรูปแบบการโจมตีในปี 2021 นอกจากจำนวนที่มีแนวโน้มเพิ่มขึ้นแล้ว เทคนิคที่เรียกว่า Social Engineering หรือการเจาะช่องโหว่ด้านความรู้ความเข้าใจของผู้ใช้งาน ยังคงถูกนำมาใช้อย่างต่อเนื่อง แต่ที่น่าสนใจคือเป้าหมายของการโจมตีจะเน้นไปที่การใช้งานของเทคโนโลยีใหม่ที่ผู้ใช้งานอาจจะยังไม่มีความเข้าใจเพียงพอ เช่น Crypto-wallet รวมถึงการสร้างผลกระทบในห่วงโซ่อุปทานเพื่อให้เกิดผลกระทบไปยังเป้าหมายที่ต้องการเนื่องจากมีการเชื่อมโยงทางธุรกิจและระบบงานเทคโนโลยีสารสนเทศเดียวกัน (Business Ecosystem)

การเตรียมความพร้อมให้กับหน่วยงานต่าง ๆ รวมถึงการเป็นส่วนหนึ่งในการสร้างความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของประเทศนั้น TB-CERT ยังคงมุ่งเน้นในการพัฒนาบุคลากร กำหนดมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานสมาชิกให้มีแนวปฏิบัติไปในทิศทางเดียวกัน เพื่อยกระดับความมั่นคงปลอดภัยให้กับภาคการเงินการธนาคาร การสร้างเครือข่ายแลกเปลี่ยนข้อมูลและประสบการณ์ เพื่อให้มีการเตรียมความพร้อมรับมือกับภัยไซเบอร์ในทุกสถานการณ์ การเสริมสร้างทักษะผ่านการซักซ้อมรับมือภัยไซเบอร์เป็นประจำ ทั้งหมดนี้จะทำให้เกิดการบริหารจัดการความเสี่ยงแบบองค์รวมในยุคดิจิทัล

ภาคผนวก

เอกสารเผยแพร่

ในปี 2021 TB-CERT ได้มีการจัดทำเอกสารเพื่อแจ้งเตือนหน่วยงานสมาชิก คำแนะนำด้านเทคนิค รวมถึงการสร้างความตระหนักรู้ให้กับภาคประชาชนได้เข้าใจภัยคุกคามทางด้านไซเบอร์ในรูปแบบต่าง ๆ โดยแบ่งตามประเภทของเอกสารดังนี้

1. **เอกสาร Public Awareness** มีเนื้อหาเกี่ยวกับการสร้างความตระหนักรู้ให้กับภาคประชาชนได้เข้าใจภัยคุกคามทางด้านไซเบอร์ จำนวน 9 เรื่อง ได้เผยแพร่ที่เว็บไซต์สมาคมธนาคารไทย (https://www.tba.or.th/tb-cert-document-report/tb-cert-public-awareness/) และโซเชียลมีเดียของ TB-CERT (https://www.facebook.com/TBCERT.Official/) ดังนี้
   1. 6 สิ่งที่ต้องทำเมื่อข้อมูลส่วนตัวรั่วไหลจากผู้ให้บริการ
   2. แจ้งเตือน 6 ขั้นตอนที่มิจฉาชีพใช้หลอกเอาข้อมูล
   3. ไปรษณีย์ไทยเตือนระวังอีเมลปลอม
   4. เตือนภัย SMS Phishing
   5. 3 ส. เตือนใจระวังภัยฟิชชิง
   6. ควรทำอย่างไรเมื่อทราบข่าวผู้ให้บริการถูกโจมตีทางไซเบอร์หรือข้อมูลรั่วไหล
   7. ซื้อของออนไลน์ปลอดภัย ด้วยเทคโนโลยี 3D Secure
   8. ถอดรหัส-กลโกง-BIN-Attack
   9. “10 แนวทาง” ทำธุรกรรมออนไลน์อย่างปลอดภัย


6 สิ่งที่ต้องทำ เมื่อข้อมูลส่วนตัวรั่วไหลจากผู้ให้บริการ
TLP: WHITE
เผยแพร่วันที่ 17 มกราคม 2564
ปัจจุบันมีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้นมากมาย ทั้งภัยไซเบอร์ที่เกิดขึ้นกับผู้ใช้งานโดยตรงและภัยไซเบอร์ที่เกิดจากผู้ให้บริการแต่ส่งผลกระทบวงกว้างมายังผู้ใช้งาน โดยจุดมุ่งหมายหลักของกลุ่มแฮกเกอร์คือ การพยายามเข้าถึงระบบและข้อมูลสำคัญ หนึ่งในข้อมูลสำคัญที่แฮกเกอร์ให้ความสนใจคือ การเข้าถึงข้อมูลส่วนตัวหรือการหลอกลวงเอาข้อมูลส่วนตัวของเราเพื่อนำไปใช้งานเสมือนเป็นเจ้าของข้อมูลนั้น ๆ ด้วยข้อมูลส่วนตัวหรือข้อมูลส่วนบุคคลเป็นข้อมูลที่บ่งบอกถึงลักษณะเฉพาะของบุคคลนั้น เพื่อเข้าใช้งานบริการของหน่วยงานต่าง ๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชน โดยเฉพาะอย่างยิ่งสถาบันการเงิน มักจะใช้ข้อมูลนี้เพื่อประกอบการยืนยันตัวตน ดังนั้นข้อมูลส่วนบุคคลจึงมีความสำคัญ เพราะหากมีผู้ไม่หวังดีล่วงรู้ก้อาจจะใช้สวมรอยในการทำธุรกรรมแทนและสร้างความเสียหายให้แก่เจ้าของข้อมูลได้ หากพบว่ามีข้อมูลส่วนตัวรั่วไหลจากผู้ให้บริการ ควรปฏิบัติดังนี้
1. ตรวจสอบและประเมินความสำคัญของข้อมูลที่ใช้งานกับผู้ให้บริการรายนั้น
2. เปลี่ยนรหัสผ่านที่ใช้ในการเข้าระบบของผู้ให้บริการรายนั้น
3. หากมีการใช้รหัสผ่านเดียวกันกับระบบอื่น ๆ เช่น อีเมล Facebook หรือ LINE ควรเปลี่ยนรหัสผ่านดังกล่าวด้วย
****
4. หลีกเลี่ยงการตั้งรหัสผ่านด้วยข้อมูลส่วนตัว เช่น วันเดือนปีเกิด หรือ หมายเลขโทรศัพท์ เป็นต้น
5. ตรวจสอบความน่าเชื่อถือของผู้ขอข้อมูล ระมัดระวังการให้ข้อมูลส่วนตัวทางช่องทางต่าง ๆ เช่น เว็บไซต์ หรือโทรศัพท์
6. หากสงสัยในการกรอกข้อมูลใด ๆ บนธุรกรรมออนไลน์หรือเว็บไซต์ ควรติดต่อสอบถามกับเจ้าหน้าที่ที่เกี่ยวข้องโดยตรง
เวอร์ชัน 1.0
มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง
TB-CERT


แจ้งเตือน!!!!!
6 ขั้นตอนที่มิจฉาชีพใช้หลอกเอาข้อมูล
TLP: WHITE
เผยแพร่วันที่ 17 มีนาคม 2564
1. มิจฉาชีพแอบอ้างช่วยเหลือ
2. มิจฉาชีพขอข้อมูลเพื่อใช้ลงทะเบียนรับเงินเยียวยา
3. มิจฉาชีพนำข้อมูลที่ได้ไปทำการยื่นขอภาษีคืนจากสรรพากร
- ชื่อ นามสกุล
- วันเดือนปีเกิด
- เลขบัตรประชาชน
- บัญชีเงินฝากพร้อมเพย์
- เอกสารอื่นภาษีอื่นๆ
อย่าให้ข้อมูลส่วนตัวกับคนที่ไม่รู้จัก
4. สรรพากรคืนเงินเข้าบัญชีเหยื่อ
5. มิจฉาชีพอ้างว่าเงินที่ได้จากภาครัฐนั้นเกิน ...ให้โอนคืน
6. ผู้หลงเชื่อโอนเงินเกินให้กับมิจฉาชีพ
TB-CERT
มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง
เวอร์ชัน 1.0

โปรดระวัง!!!

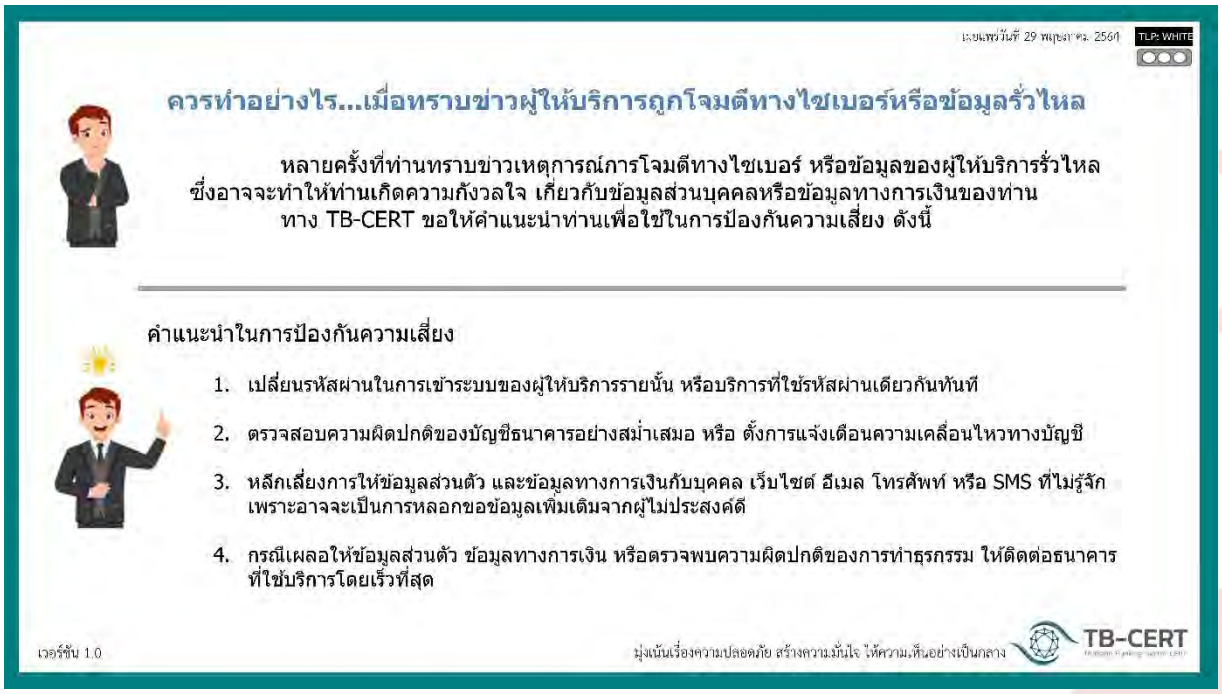
เวอร์ชั่น 1.0

ไปรษณีย์ไทย เตือนระวัง **อีเมลปลอม**
ย้ำไม่มีนโยบายส่งอีเมล แจ้งเรียกเก็บค่าดำเนินการหรือแจ้งส่งพัสดุ

บริษัท ไปรษณีย์ไทย จำกัด แจ้งเตือนผู้ใช้บริการระวังมิจฉาชีพแอบอ้างส่งจดหมายอิเล็กทรอนิกส์ ระบุว่าเป็นอีเมลจาก ไปรษณีย์ไทย แจ้งว่าไม่สามารถจัดส่งพัสดุของลูกค้าได้ เนื่องจากไม่มีการชำระภาษีศุลกากร หรือเหตุผลอื่น ๆ พร้อมแนบลิงก์เพื่อหลอกลวงขอข้อมูลบัตรเครดิต และข้อมูลส่วนบุคคลของผู้ใช้บริการ

วิธีป้องกันตนเอง

1. ระมัดระวังการให้ข้อมูลส่วนตัว รวมถึงข้อมูลบัตรเครดิตผ่านช่องทางต่าง ๆ เช่น อีเมล์ เว็บไซต์แอบอ้าง และทางโทรศัพท์
2. ติดตามความคืบหน้าผ่านช่องทางการสื่อสารที่หน่วยงานกำหนด เช่น เว็บไซต์ หรือเบอร์โทรของหน่วยงานโดยตรง
   สำหรับไปรษณีย์ไทยสามารถติดตามและตรวจสอบได้ที่
   www.thailandpost.co.th และแอปพลิเคชัน Track&Trace Thailand Post
3. หากสงสัยสามารถติดต่อ โทรสายตรงไปรษณีย์ไทย 1545


TLP: WHITE
ควรทำอย่างไร...เมื่อทราบข่าวผู้ให้บริการถูกโจมตีทางไซเบอร์หรือข้อมูลรั่วไหล
หลายครั้งที่ท่านทราบข่าวเหตุการณ์การโจมตีทางไซเบอร์ หรือข้อมูลของผู้ให้บริการรั่วไหล ซึ่งอาจจะทำให้ท่านเกิดความกังวลใจ เกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินของท่าน ทาง TB-CERT ขอให้คำแนะนำท่านเพื่อใช้ในการป้องกันความเสี่ยง ดังนี้
คำแนะนำในการป้องกันความเสี่ยง
1. เปลี่ยนรหัสผ่านในการเข้าระบบของผู้ให้บริการรายนั้น หรือบริการที่ใช้รหัสผ่านเดียวกันทันที
2. ตรวจสอบความผิดปกติของบัญชีธนาคารอย่างสม่ำเสมอ หรือ ตั้งการแจ้งเตือนความเคลื่อนไหวทางบัญชี
3. หลีกเลี่ยงการให้ข้อมูลส่วนตัว และข้อมูลทางการเงินกับบุคคล เว็บไซต์ อีเมล โทรศัพท์ หรือ SMS ที่ไม่รู้จัก เพราะอาจจะเป็นการหลอกขอข้อมูลเพิ่มเติมจากผู้ไม่ประสงค์ดี
4. กรณีเผลอให้ข้อมูลส่วนตัว ข้อมูลทางการเงิน หรือตรวจพบความผิดปกติของการทำธุรกรรม ให้ติดต่อธนาคารที่ใช้บริการโดยเร็วที่สุด
เวอร์ชัน 1.0
มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง
TB-CERT

3 ส. เตือนใจ ระวังภัย SMS Phishing

TLP: WHITE

เผยแพร่วันที่ 21 เมษายน 2564

สงสัย: ดูชื่อผู้ส่ง

สังเกต: เนื้อหาข้อความ

ส่งข่าว: แจ้ง call center หรือช่องทางติดต่อธนาคาร

จากข่าวที่ปรากฏเมื่อช่วงปลายปีที่แล้ว เกี่ยวกับภัย SMS Phishing ที่แพร่หลาย ซึ่งเหตุการณ์ดังกล่าวยังคงเกิดขึ้นต่อเนื่อง และหลายท่านคงได้เห็นมีการส่งต่อเพื่อเตือนภัยกันอีกมากในช่วงนี้

TB-CERT ขอแนะนำ

คาถา 3 ส.

เพื่อให้ทุกคนร่วมกันระวังภัย ดังนี้

สงสัย ชื่อผู้ส่งที่ไม่ใช่ชื่อธนาคาร หรือที่ใช้ชื่อคล้ายธนาคาร

สังเกต เนื้อหาข้อความเชิญชวนเกินจริง และมีลิงก์แนบ

ส่งข่าว ให้ธนาคารที่ถูกปลอมแปลงทราบ เพื่อยับยั้งความเสียหาย

TB-CERT Thailand Banking Sector CERT

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

Version 1.0

ซื้อของออนไลน์ปลอดภัย ด้วยเทคโนโลยี 3D Secure

TLP: WHITE

เผยแพร่วันที่ 27 ตุลาคม 2564

ปัจจุบันโลกออนไลน์ได้เข้ามามีบทบาทอย่างมากในชีวิตประจำวัน การซื้อของเปลี่ยนไปอยู่ในรูปแบบออนไลน์มากขึ้น ดังนั้นการซื้อสินค้าออนไลน์ และชำระเงินด้วยบัตรเครดิตและบัตรเดบิตแบบออนไลน์จึงได้รับความนิยมเพิ่มมากขึ้น เพื่อให้ตอบโจทย์กับการใช้งานบนโลกออนไลน์และยังคงมีความปลอดภัยที่ทำให้มั่นใจได้ว่าเจ้าของบัตรเป็นผู้ทำรายการซื้อของออนไลน์เอง จึงเป็นที่มาของการนำเทคโนโลยี 3D Secure มาใช้งาน

3D Secure คืออะไร

3D Secure เป็นโครงสร้างความปลอดภัยบนระบบการชำระเงินธุรกรรมออนไลน์ที่ช่วยป้องกันการฉ้อโกงในธุรกรรมบัตรเครดิตและบัตรเดบิต สำหรับการทำงานของเทคโนโลยี 3D Secure (Verified by VISA/ MasterCard SecureCode) มีขั้นตอนดังนี้

1. ลูกค้าเลือกซื้อของบนร้านค้าออนไลน์ และเมื่อต้องการ ชำระค่าสินค้า ร้านค้าออนไลน์จะแสดงหน้าจอให้ลูกค้ากรอกข้อมูลบัตรเครดิตหรือบัตรเดบิต สำหรับร้านค้าที่รองรับเทคโนโลยี 3D Secure บนหน้าจอที่ให้กรอกข้อมูลบัตรเครดิตหรือบัตรเดบิต จะแสดงสัญลักษณ์ Verified by VISA หรือ MasterCard SecureCode
2. ด้วยความปลอดภัยแบบ 3D Secure ธนาคารผู้ออกบัตรจะส่งรหัสผ่าน OTP ไปยังมือถือของลูกค้าเจ้าของบัตร กรณีลูกค้าทำรายการชำระสินค้าแล้วไม่ได้รับรหัสผ่าน OTP ลูกค้าสามารถติดต่อสอบถามข้อมูลได้จากธนาคารผู้ออกบัตรนั้น
3. ลูกค้ากรอกรหัสผ่าน OTP ที่ได้รับบนหน้าจอทำรายการชำระค่าสินค้า เพื่อยืนยันตัวตนในการทำรายการชำระเงิน
4. ระบบ 3D Secure ทำการตรวจสอบข้อมูล หากตรวจสอบแล้วข้อมูลถูกต้อง ธนาคารก็จะอนุมัติการทำรายการ สำหรับกรณีที่มีข้อมูลผิดพลาด ธนาคารก็จะปฏิเสธการทำรายการ และส่งผลลัพธ์ให้กับการร้านค้าออนไลน์เพื่อดำเนินการต่อไป

TB-CERT มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง TB-CERT Version 1.0

ถอดรหัส กลโกง BIN Attack

TLP: WHITE

เผยแพร่วันที่ 10 พฤศจิกายน 2564

เมื่อรูปแบบการชำระเงินได้มีการเปลี่ยนแปลงไปสู่การชำระเงินทางอิเล็กทรอนิกส์มากขึ้น และการชำระเงินด้วยบัตรเครดิตและบัตรเดบิตก็มีอัตราการใช้งานบนโลกออนไลน์เพิ่มสูงขึ้น เพื่อให้เกิดความตระหนักในการใช้งานบัตรเครดิตและบัตรเดบิตอย่างปลอดภัย บทความนี้จะมาอธิบาย BIN Attack คืออะไร ลักษณะการทำงานเป็นอย่างไร และเราจะป้องกันกลโกง BIN Attack นี้ได้อย่างไร

BIN Attack คืออะไร

การโกงด้วยวิธีการใช้ข้อมูล BIN (Banking Identification Number) เป็นค่าตั้งต้น แล้วใช้โปรแกรมสร้างชุดตัวเลขที่เหลือจนได้ชุดตัวเลขครบทั้ง 16 หลัก ของบัตรเครดิตหรือบัตรเดบิต

โจรจะนำชุดตัวเลข 16 หลักนี้ พร้อมกับการสุ่มเดือนปีที่หมดอายุของบัตรไปลองใช้กับกลุ่มร้านค้าออนไลน์ที่ไม่ได้ใช้เทคโนโลยี 3D Secure

สุดท้ายเมื่อโจรสุ่มจนได้ข้อมูลบัตรที่ถูกต้องครบถ้วน ได้แก่ เบอร์บัตร 16 หลัก และเดือนปีที่บัตรหมดอายุ ก็จะนำชุดข้อมูลนี้ไปทำรายการซื้อสินค้าและบริการที่ต้องการ กับร้านค้าออนไลน์ที่ไม่ได้ใช้เทคโนโลยี 3D Secure

แนวทางป้องกัน BIN Attack

1. **ตั้งค่าวงเงิน**สำหรับการชำระสินค้าให้เหมาะสมกับการทำธุรกรรมการเงิน **หรือปรับลดวงเงิน**ชำระสินค้าเป็นศูนย์ชั่วคราว หากยังไม่มีความจำเป็นต้องใช้ ซึ่งสามารถดำเนินการผ่านช่องทางดังนี้
   - ติดต่อศูนย์บริการสมาชิกบัตรผ่านระบบอัตโนมัติ (เบอร์ติดต่อศูนย์บริการจะปรากฏบนหลังบัตร) หรือ Call Center ของธนาคาร
   - เปลี่ยนแปลงแก้ไขวงเงินบนแอปพลิเคชัน Mobile Banking ของธนาคาร
2. **สังเกตการแจ้งเตือนเงินเข้า-เงินออก**จากบัญชีธนาคาร และหมั่น**ตรวจสอบยอดการใช้จ่าย**ผ่านบัตรเครดิตและบัตรเดบิตอย่างสม่ำเสมอ
3. **หากพบรายการบัญชีผิดปกติ**หรือมีข้อสงสัย **ควรติดต่อธนาคาร**เจ้าของบัตรโดยตรง
4. **ติดตามข่าวสาร**จากช่องทางที่เป็นทางการของธนาคาร และ TB-CERT

TB-CERT มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง TB-CERT Version 1.0

10 แนวทาง

ทำธุรกรรมออนไลน์อย่างปลอดภัย

สมาคมธนาคารไทย ได้รวบรวมแนวทางการทำธุรกรรมออนไลน์ ที่จะช่วยให้ทำธุรกรรมอย่างปลอดภัย เพื่อให้ลูกค้าสามารถทำธุรกรรมได้อย่างมั่นใจและปลอดภัย ดังนี้

1. ทำธุรกรรมกับร้านค้าออนไลน์ที่น่าเชื่อถือ

2. ควรทำธุรกรรมบนระบบที่มีการยืนยันตัวตน ด้วย OTP หรือใช้เทคโนโลยี 3D Secure

3. ไม่ส่งต่อ OTP ให้กับบุคคลอื่น ไม่ว่ากรณีใดๆ

4. ตั้งรหัสผ่านที่ยากต่อการคาดเดา

5. ไม่ใช้รหัสผ่านร่วมกัน ในการทำธุรกรรม และร้านค้าออนไลน์

6. ไม่เปิดเผยข้อมูลส่วนตัว ข้อมูลทางการเงิน แก่บุคคลอื่น เช่น เลขบัญชี เลขบัตรเดบิต เลขบัตรเครดิต เลข CVV

7. ปรับวงเงินสำหรับการชำระสินค้า ให้เหมาะสมกับการทำธุรกรรม

8. หมั่นสังเกตและตรวจสอบ ยอดเงินเข้า-เงินออก ยอดการใช้จ่ายบัตรเครดิต และบัตรเดบิตอยู่เสมอ

9. หากพบรายการบัญชีผิดปกติ ควรติดต่อ ธนาคารเจ้าของบัตรโดยตรงทันที

10. ติดตามข่าวสารจาก TB-CERT และช่องทางที่เป็นทางการของทางธนาคาร

สมาคมธนาคารไทย ขอให้ความมั่นใจว่า การให้บริการแก่ลูกค้าธนาคารพาณิชย์ของไทย มีความมั่นคงปลอดภัย ในระดับมาตรฐานสากล โดยขอให้ลูกค้าดำเนินการตาม 10 ข้อแนะนำ อย่างสม่ำเสมอ หากพบรายการผิดปกติ ให้ติดต่อธนาคารทันที โดยธนาคารพร้อมให้บริการที่ดี และมีความรับผิดชอบ

2. **เอกสาร Technical Recommendation** เกี่ยวกับคำแนะนำด้านเทคนิคในการรับมือกับเหตุการณ์โจมตีทางไซเบอร์ ดังนี้

   TR21-001 เรื่อง Pulse Secure ส่งให้สมาชิก

   TR21-002 เรื่อง Pulse Secure – IOC ส่งให้ NCERT

   TR21-003 เรื่อง คำแนะนำเกี่ยวกับแนวทางการป้องกันความเสี่ยงจาก Software Supply Chain Attack

   TR21-004 เรื่อง Black Matter

   TR21-005 เรื่อง Vmware CVE-2021-22005

   TR21-006 เรื่อง คำแนะนำเกี่ยวกับช่องโหว่ Log4j หรือ Log4shell CVE-2021-442228

   TR21-007 เรื่อง คำแนะนำเกี่ยวกับช่องโหว่ Log4j หรือ Log4shell CVE-2021-442228 (เพิ่มเติม)

3. **Cybersecurity alerts to members** แจ้งเตือนภัยคุกคามไซเบอร์ ให้หน่วยงานสมาชิกรับทราบข่าวสารอย่างรวดเร็ว

   AL21-001 – Phishing campaign

   AL21-002 - แจ้งเตือนเหตุการณ์ Business Email Compromise (BEC)

   AL21-003 - แจ้งเตือนเหตุการณ์การขโมยข้อมูลลูกค้าของบริษัท AXA Group

รายนามคณะกรรมการ TB-CERT วาระปี 2021-2023

ประธานกรรมการ	**คุณชัชวัฒน์ อัศวรักวงศ์** Managing Director and Chief Information Security Officer ธนาคารกสิกรไทย
รองประธานกรรมการ	**คุณสมภพ สุรัตนกวีกุล** Director, IT Security Office, Information Technology Department ธนาคารแห่งประเทศไทย
ที่ปรึกษากิตติมศักดิ์และกรรมการด้านสื่อสาร	**ดร. กิตติ โฆษะวิสุทธิ์** Senior Vice President, Head of Security Management ธนาคารกรุงเทพ
กรรมการด้านสื่อสาร	**คุณนิโรจน์ ผิวพรรณ** First Vice President, IT Security, Technology Group ธนาคารกรุงไทย
กรรมการด้านวิชาการ	**คุณพาวิต ศักดิ์สูง** Head of Digital Technology Security ธนาคารไทยพาณิชย์
กรรมการด้านวิชาการ	**คุณประกลกฤษ แสงชูวงศ์** Team Head of Information, Security Detection and Response ธนาคารทหารไทยธนชาต
กรรมการด้านเทคนิค	**คุณภคพงศ์ จุลวงศาศิลป์** Head of Cyber Security Department ธนาคารกรุงศรีอยุธยา
กรรมการด้านเทคนิค	**คุณวชิราวัชร์ มหาทัพกฤษ** Inspector general, Chief Information Security Officer ธนาคารออมสิน
กรรมการ	**คุณยศ กิมสวัสดิ์** Head of Payment System Office สมาคมธนาคารไทย
คณะเลขานุการ	**คุณปรมินทร์ ช่วงมณี** CERT Manager
	คุณปิลันญา เชิญถนอมวงศ์ CERT Manager
	คุณธาวินี วงศ์วิศว์ CERT Relations Manager

หน่วยงานสมาชิก TB-CERT

	ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร Bank of Agriculture and Agricultural Cooperatives		ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน) Kiatnakin Phatra Bank Plc.
	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) Bank of Ayudhya Public Company Limited (Krungsri)		ธนาคารกรุงไทย จำกัด (มหาชน) Krung Thai Bank Public Company Limited
	ธนาคารกรุงเทพ จำกัด (มหาชน) Bangkok Bank Public Company Limited		ธนาคารแลนด์ แอนด์ เฮ้าส์ จำกัด (มหาชน) Land and Houses Bank Public Company Limited
	ธนาคารแห่งประเทศไทย Bank of Thailand		ธนาคารมิซูโฮ จำกัด สาขากรุงเทพฯ Mizuho Bank Bangkok Branch
	ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน) CIMB Thai Bank Public Company Limited		บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด National Credit Bureau Company Limited
	ธนาคารซิตี้แบงก์ Citibank N.A.		บริษัท ศูนย์ประมวลผล จำกัด Processing Center Company Limited
	ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย Export-Import Bank of Thailand		ธนาคาร ไทยพาณิชย์ จำกัด (มหาชน) The Siam Commercial Bank Public Company Limited
	ธนาคารอาคารสงเคราะห์ Government Housing Bank		ธนาคารสแตนดาร์ดชาร์เตอร์ด (ไทย) จำกัด (มหาชน) Standard Chartered Bank (Thai) Public Company Limited
	ธนาคารออมสิน Government Savings Bank		ธนาคารไทยเครดิต เพื่อรายย่อย จำกัด (มหาชน) The Thai Credit Retail Bank Public Company Limited
	ธนาคารอิสลามแห่งประเทศไทย Islamic Bank of Thailand		ธนาคารทิสโก้ จำกัด (มหาชน) TISCO Bank Public Company Limited
	ธนาคาร ไอซีบีซี (ไทย) จำกัด (มหาชน) Industrial and Commercial Bank of China (Thai) Public Company Limited (ICBC Thai)		ธนาคารทหารไทยธนชาต จำกัด (มหาชน) TMB Thanachart Bank Public Company Limited
	บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด National ITMX Company Limited		ธนาคารยูโอบี จำกัด (มหาชน) United Overseas Bank (Thai) Public Company Limited
	ธนาคารกสิกรไทย จำกัด (มหาชน) KASIKORNBANK Public Company Limited		

The Thai Bankers' Association

4th Fl., 5/13 Moo 3, Chaengwattana Rd., Pakkret, Nonthaburi 11120
Phone : 025587500 Website : www.tba.or.th