สมาคมธนาคารไทย

ANNUAL REPORT 2019

รายงานผลการดำเนินงาน 2562

สำนักงานระบบการชำระเงิน
Payment System Office (PSO)

สารบัญ

[สำนักงานระบบการชำระเงิน]

สารบัญ

บทนำ

จาก แผนกลยุทธ์ระบบการชำระเงินฉบับที่ 4 (พ.ศ. 2562-2564) ที่ประกาศโดยธนาคารแห่งประเทศไทย ซึ่งได้ให้ความสำคัญในการพัฒนาระบบการชำระเงินของประเทศ โดยดำเนินงานอย่างต่อเนื่องจากแผนกลยุทธ์ระบบการชำระเงินฉบับก่อนหน้านี้ รวมถึงแผนยุทธศาสตร์การพัฒนาโครงสร้างพื้นฐานระบบการชำระเงินแบบอิเล็กทรอนิกส์แห่งชาติ หรือ National e-Payment Master Plan

สำนักงานระบบการชำระเงินได้ร่วมดำเนินการผลักดันการชำระเงินทางอิเล็กทรอนิกส์ หรือ Digital Payment ของธนาคารให้มีการพัฒนาอย่างต่อเนื่องตามการเปลี่ยนแปลงของเทคโนโลยี และพฤติกรรมของผู้บริโภค โดยคำนึงถึงความมั่นคงปลอดภัยและได้มาตรฐานสากล ซึ่งจะเห็นได้ว่าการที่สำนักงานระบบการชำระเงินได้ร่วมมือกับธนาคารสมาชิกและภาครัฐมาอย่างต่อเนื่อง ตั้งแต่ปี 2558 เรื่อยมานั้นส่งผลให้ในปี 2562 ภาครัฐและภาคเอกชนได้ใช้โครงสร้างการชำระเงินแบบ Digital Payment ในการกระตุ้นเศรษฐกิจของประเทศ โดยจะเห็นได้จากหลายโครงการของภาครัฐ โดยเริ่มตั้งแต่การคืนภาษีบุคคลธรรมดาผ่านระบบพร้อมเพย์ การจ่ายสวัสดิการต่าง ๆ ไปจนถึงการกระตุ้นการจับจ่ายใช้สอยผ่านมาตรการชิมช้อปใช้ และโครงการอื่น ๆ

ในการดำเนินงานปี 2562 รูปแบบการชำระเงินของไทยได้มีการเปลี่ยนแปลงไปสู่การชำระเงินแบบ Digital Payment อย่างชัดเจน โดยตั้งแต่ปี 2559 จนถึงปี 2562 จะพบว่าการใช้ Smartphone ในการทำธุรกรรมทางการเงินมีการพัฒนา และเติบโตอย่างรวดเร็ว มีการใช้บริการชำระเงินและโอนเงินผ่านโทรศัพท์มือถืออย่างแพร่หลาย จะเห็นได้ว่ามีการทำธุรกรรมทางการเงินผ่านโทรศัพท์มือถือเพิ่มขึ้นถึง 588.31% จากปี 2559 ถึงปี 2561 ซึ่งปัจจัยสำคัญมาจากการขับเคลื่อนภายใต้แผน National e-Payment Master Plan โครงการระบบพร้อมเพย์และโครงการขยายการใช้บัตร

สำนักงานระบบการชำระเงินมุ่งเน้นในการพัฒนาสนับสนุนให้มีบริการทางการเงินและการชำระเงินทางอิเล็กทรอนิกส์อย่างต่อเนื่อง ทั้งภาครัฐ ภาคธุรกิจ และภาคประชาชน การพัฒนาการเชื่อมโยงระบบ Digital Payment กับต่างประเทศ รวมถึงการพัฒนา Interoperable QR Code for ASEAN การเปลี่ยนบัตรแถบแม่เหล็กเป็นบัตรชิปการ์ด และการให้ความสำคัญเรื่องความปลอดภัยในการทำธุรกรรมทางการเงิน การพัฒนามาตรฐาน Thai QR payment การบริการเตือนเพื่อจ่าย (PayAlert) รองรับการขายของออนไลน์ และบริการ e-Donation

ต้นปี 2562 สำนักงานระบบการชำระเงินได้ตั้งเป้าหมายที่จะผลักดันให้ Digital Payment มีการขยายตัวและพัฒนาอย่างต่อเนื่องภายใต้การดำเนินงานที่มีประสิทธิภาพ มีต้นทุนที่เหมาะสม มีความปลอดภัยสูง และคำนึงถึงความต้องการของผู้ใช้บริการ โดย มีเป้าหมายหลัก ดังนี้

เป้าหมายหลัก
■ สนับสนุนการเชื่อมโยงระบบการชำระเงินกับต่างประเทศ (Payment Connectivity) โดยนำนวัตกรรมหลายรูปแบบมาใช้ เช่น Thai QR Payment ในรูปแบบ Sponsor Bank Model ในรูปแบบ Switch-to-Switch Model การร่วมมือกับประเทศใน ASEAN พัฒนา Interoperable QR Payment for ASEAN
■ ส่งเสริมการพัฒนาและการใช้มาตรฐานข้อความสากล ISO20022 สำหรับการชำระเงินทั้งภายในประเทศและต่างประเทศ
■ การผลักดันการพัฒนามาตรฐาน API
■ เปิดให้บริการ MyPromptQR (B scan C) ซึ่งใช้มาตรฐานข้อความ ISO20022
■ ร่วมกำหนด Business Rules รูปแบบและมาตรฐาน สำหรับบริการใหม่ที่เกี่ยวข้องกับการชำระเงินทางอิเล็กทรอนิกส์
■ พัฒนาและเปิดให้บริการ Digital Payment ในรูปแบบใหม่ ๆ บน โครงสร้างพร้อมเพย์ เช่น บริการ BillAlert
■ ร่วมกำหนดมาตรฐาน e-KYC เพื่อสนับสนุน National Digital ID Project
■ ส่งเสริมการรับรู้และสร้างความเชื่อมั่นในการโอนเงินและการชำระเงินทางอิเล็กทรอนิกส์
■ การเปลี่ยนบัตรเดบิตและบัตรเอทีเอ็มแบบแถบแม่เหล็กเป็นบัตรแบบชิปการ์ด
■ จัดการการอบรมสัมมนาเพื่อพัฒนาบุคลากรของธนาคารในเรื่องการชำระเงินทางอิเล็กทรอนิกส์

ในการดำเนินงานของสำนักงานระบบการชำระเงินปี 2562 เป็นการดำเนินงานต่อเนื่องจากปี 2561 ซึ่งมีการวางรากฐานรูปแบบการชำระเงินแบบ Digital Payment ไว้หลายด้าน ซึ่งการดำเนินงานอย่างต่อเนื่องที่สำคัญ คือการพัฒนาโครงสร้างการชำระเงินในประเทศให้เติบโตและขยายสู่ทุกภาคส่วนก้าวสู่สังคมไร้เงินสดอย่างต่อเนื่อง และพัฒนาการเชื่อมโยงในอาเซียนโดยดำเนินตามกรอบของธนาคารแห่งประเทศไทย เพื่อลดต้นทุนการชำระเงิน/โอนเงินระหว่างประเทศ เพิ่มโอกาสการเข้าถึงบริการทางการเงิน สนับสนุนการท่องเที่ยว การค้าขายในพื้นที่ชายแดน รวมถึง การลงทุน และการเคลื่อนย้ายแรงงานในภูมิภาค

สนับสนุนการเชื่อมโยงระบบการชำระเงินกับต่างประเทศ (Payment Connectivity)

ในปัจจุบันธุรกรรมชำระเงินระหว่างประเทศมีแนวโน้มสูงขึ้นอย่างต่อเนื่องจากการเติบโตของการค้าและการลงทุนระหว่างประเทศ การท่องเที่ยวและแรงงานต่างชาติการค้าชายแดนกับประเทศมาเลเซีย เมียนมา ลาว และกัมพูชา ธนาคารแห่งประเทศไทยได้ให้ความสำคัญในการร่วมมือของสถาบันการเงิน (Bank) ผู้ให้บริการชำระเงินอิเล็กทรอนิกส์ไทย Non-bank) และผู้ให้บริการบัตรเครดิต/เดบิต ในการพัฒนาบริการชำระเงินระหว่างประเทศด้วยเทคโนโลยีใหม่ เช่น QR Code, Distributed Ledger Technology (Blockchain), Application Programming Interface (API) และ Card Network การพัฒนานวัตกรรมทางการเงิน จะช่วยเพิ่มประสิทธิภาพของระบบการเงิน และทำให้ภาคธุรกิจ และภาคประชาชน ได้รับความสะดวกในการทำธุรกรรมทางการเงิน รวมทั้งเพิ่มการเข้าถึงบริการทางการเงินของประชาชนที่จะเพิ่มมากขึ้น ส่งผลโดยตรงต่อความเจริญก้าวหน้าของเศรษฐกิจในภูมิภาคอาเซียน

ในการพัฒนาให้มีบริการชำระเงินที่สะดวกมากขึ้น ต้นทุนต่ำซึ่งจะช่วยสนับสนุนการทำธุรกรรมระหว่างประเทศ และการเติบโตของเศรษฐกิจไทย สำนักงานระบบการชำระเงินได้มีส่วนร่วมสำคัญในการผลักดันการเชื่อมโยงระบบการชำระเงินหลัก ๆ ดังต่อไปนี้

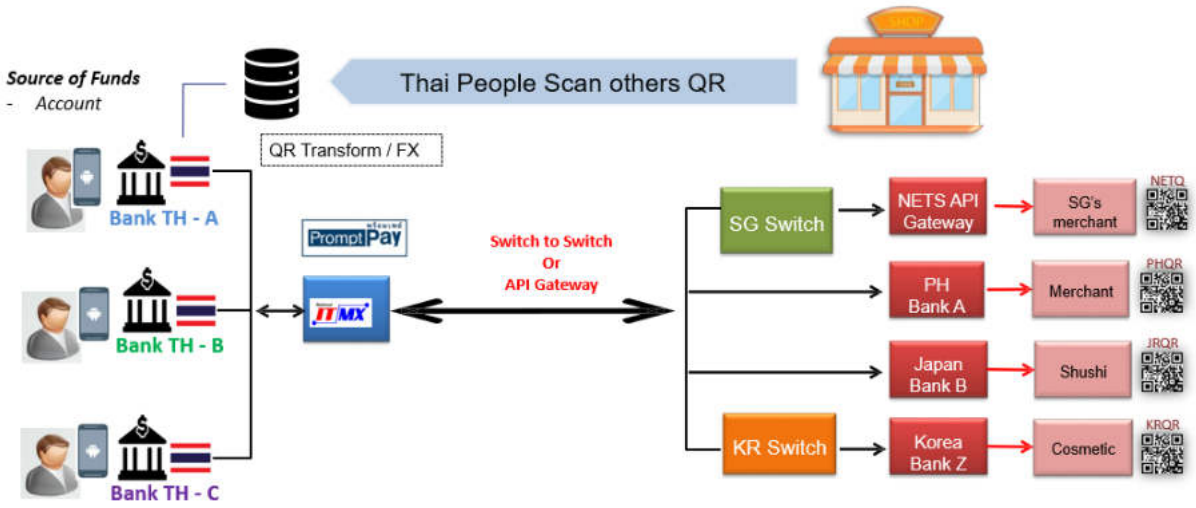
การให้บริการการชำระเงินในกลุ่มประเทศอาเซียน ในปี 2562

➢ Interoperable QR Code ใน ASEAN

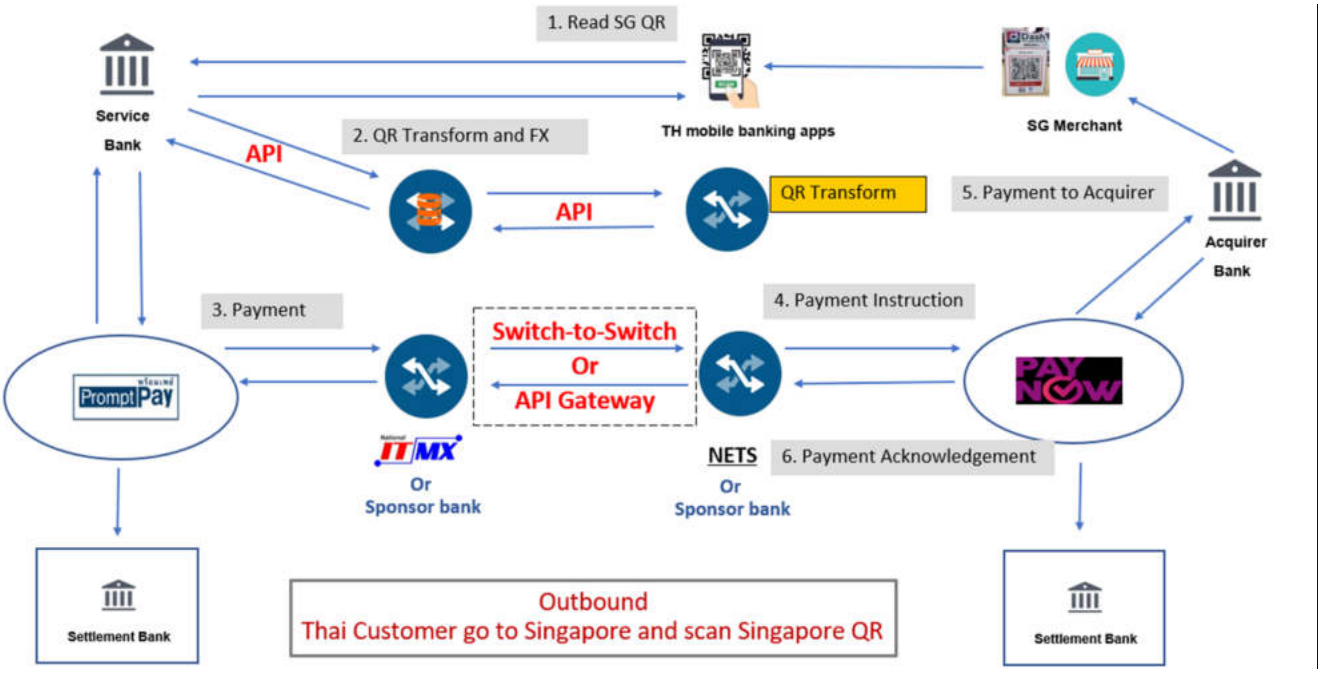
สืบเนื่องจากในการประชุม Financial Connectivity - Interoperable QR Code for Cross-Border (“ASEAN QR”) ในงาน “5th ASEAN Finance Ministers’ and Central Bank Governors’ and Related Meetings” ระหว่างวันที่ 2 – 5 เมษายน 2562 ที่ Riverie by Katathani จังหวัดเชียงราย โดยมีผู้ว่าการธนาคารแห่งประเทศไทยเป็นประธานในที่ประชุม ประเด็นสำคัญในการประชุมคือการสนับสนุนให้มีการศึกษาแนวทางที่ประเทศใน ASEAN สามารถชำระเงินระหว่างประเทศด้วย Mobile Banking ผ่านระบบ QR Code ได้สะดวก รวดเร็ว และปลอดภัย สำนักงานระบบการชำระเงินภายใต้สมาคมธนาคารไทยได้รับมอบหมายให้เป็นผู้ขับเคลื่อน Interoperable QR Code ใน ASEAN

- ✓ การชำระเงินผ่าน QR Code มีการเติบโตอย่างรวดเร็ว และต่อเนื่องในภูมิภาคอาเซียน และเป็นที่ยอมรับอย่างกว้างขวางของผู้ค้าและผู้บริโภค
- ✓ การชำระเงินผ่าน QR code เป็นวิธีที่รวดเร็ว ยืดหยุ่นสามารถตรวจสอบได้ และต้นทุนต่ำ เพื่อให้บริการชำระเงินทางอิเล็กทรอนิกส์สำหรับลูกค้าในและต่างประเทศ
- ✓ การชำระเงินผ่าน QR Code จะช่วยลดต้นทุนการชำระเงินภายในอาเซียน
- ✓ ในบางประเทศการนำ QR code มาใช้เป็น Digital Launchpad ก้าวกระโดดไปสู่การสร้างระบบ Digital Payment หลักของประเทศ และเปิดโอกาสให้ ประชาชนระดับล่างมีโอกาส เข้าถึงบริการทางการเงิน

ภาพตัวอย่าง ด้านเทคนิคกรณีคนไทยเดินทางไปใช้ QR Payment ในต่างประเทศ



User Journey

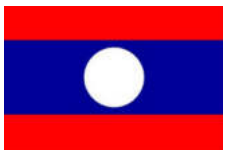


นอกจากนี้ธนาคารแห่งประเทศไทยได้นำเสนอนวัตกรรมทางการเงิน และระบบการชำระเงินระหว่างประเทศไทยและประเทศอื่น ๆ ในงาน “5th ASEAN Finance Ministers’ and Central Bank Governors’ and Related Meetings” ที่จัดขึ้นที่จังหวัดเชียงราย ดังนี้

1) การชำระเงินระหว่างประเทศด้วย Interoperable QR Payment


ประเทศไทย และประเทศกัมพูชา

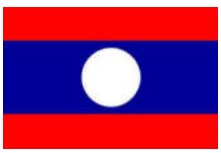
โดยธนาคารพาณิชย์ไทยได้พัฒนาและทดสอบการให้บริการชำระเงินด้วย Interoperable QR Payment ข้ามประเทศ ซึ่งสอดคล้องกับมาตรฐาน EMV โดยร่วมกับสาขาของธนาคารนั้นในประเทศกัมพูชา บริการนี้จะช่วยอำนวยความสะดวกสำหรับการชำระเงินรายย่อยระหว่างลูกค้าและร้านค้าของทั้งสองประเทศ บริการนี้ทำให้นักท่องเที่ยวไทยสามารถใช้ Mobile Application ของธนาคารไทย ในการสแกน QR Code เพื่อชำระเงินค่าสินค้าและบริการให้กับร้านค้าในกัมพูชาที่ร่วมให้บริการ ซึ่งจะมีการเปิดให้บริการจริงในระยะต่อไป

ประเทศไทย และ สปป. ลาว

โดยธนาคารของไทยและ Banque Pour Le Commerce Exterieur Lao Public (BCEL) ได้ร่วมพัฒนาการบริการชำระเงินระหว่างประเทศด้วย QR Payment บริการดังกล่าวจะช่วยให้ลูกค้าของ BCEL สามารถชำระเงินในประเทศไทยและมีผลทันทีด้วยการสแกน QR Code ที่ร้านค้าไทยด้วย Mobile Application ของ BCEL และยังช่วยให้คนไทยซึ่งเป็นลูกค้าของธนาคารในประเทศไทยที่เดินทางไป สปป. ลาว สามารถชำระเงินที่ร้านค้าของ BCEL ผ่าน Mobile Application ของแต่ละธนาคาร ซึ่งเชื่อมโยงไปยังบัญชีของลูกค้าได้โดยตรง

2) Blockchain Interledger: การโอนเงินระหว่างประเทศแบบ Real-time สำหรับภาคธุรกิจ

ประเทศไทย และ สปป. ลาว

ธนาคารพาณิชย์ไทยได้เริ่มบุกเบิกการใช้นวัตกรรม Blockchain สำหรับธุรกิจยุคใหม่ โดยเปิดให้บริการโอนเงินระหว่างประเทศแบบ Real-time สำหรับภาคธุรกิจในการโอนเงินจาก สปป. ลาว มายังประเทศไทย และส่งต่อจากประเทศไทยไปยังประเทศสิงคโปร์ในเวลาที่รวดเร็ว ช่วยเพิ่มประสิทธิภาพในการแข่งขันในด้านการบริหารจัดการลดต้นทุน และช่วยลดความเสี่ยงของอัตราแลกเปลี่ยน

ประเทศไทย และประเทศเมียนมา


โดยธนาคารพาณิชย์ในประเทศไทยและ Shwe Bank ประเทศเมียนมาได้ร่วมกับ Everex ซึ่งเป็นพันธมิตรทางธุรกิจ พัฒนาบริการส่งเงินระหว่างประเทศที่มีความสะดวก ปลอดภัยและมีผลทันที โดยใช้ Blockchain Platform ซึ่งจะให้ลูกค้าสามารถ โอนเงินโดยไม่จำกัดสถานที่และเวลา ด้วยอัตราแลกเปลี่ยนที่แข่งขันได้ ผ่านบริการ Mobile Application ของธนาคาร โดยผู้รับเงินในประเทศเมียนมาสามารถเลือกรับเงินได้หลายช่องทาง เช่น การส่งเงินถึงบ้าน หรือรับเงินจากสาขาของธนาคาร Shwe Bank หรือการโอนเข้าบัญชี Shwe Bank โดยตรง

3) การโอนเงินระหว่างประเทศผ่าน API


ประเทศไทย และประเทศสิงคโปร์

โดยธนาคารพาณิชย์ในประเทศไทยและ DBS ได้ร่วมพัฒนาบริการโอนเงินระหว่างประเทศโดยใช้เทคโนโลยี API (API-Based Funds Transfer Service) เพื่อรองรับการโอนเงินจากสิงคโปร์มาไทย บริการดังกล่าวมีความพิเศษที่อนุญาตให้ผู้โอนสามารถตรวจสอบสถานะบัญชีของผู้รับโอนก่อนการโอนเงิน และสามารถโอนเงินได้สูงสุด 1.5 ล้านบาทต่อรายการ

4) การชำระเงินระหว่างประเทศด้วย Interoperable QR Payment

ประเทศไทย และประเทศสิงคโปร์


โดยธนาคารพาณิช์ในประเทศไทย ร่วมกับ Non-Bank เปิดให้บริการ Interoperable QR Payment ของในต่างประเทศ โดยเป็นการเริ่มให้บริการ GLOBAL Pay ซึ่งเป็น Mobile Wallet Application ที่ช่วยให้ลูกค้าคนไทย ที่ใช้ e-Wallet ของ GLOBAL Pay ให้สามารถใช้บริการชำระเงินผ่าน QR Code เมื่อเดินทางไปต่างประเทศผ่านเครือข่าย VIA Network ภายใต้กลุ่ม Singtel Group ซึ่งในการทำธุรกรรมนี้จะได้รับความสะดวก ปลอดภัย และมีอัตราแลกเปลี่ยนที่แข่งขันได้ผ่าน Mobile Wallets ของประเทศนั้น ๆ

➢ โครงการการเชื่อมโยงระหว่าง PromptPay และ PayNow


ประเทศใน ASEAN ได้มีการพัฒนาระบบการชำระเงินหลักของประเทศเพื่อรองรับการเติบโตของ Digital Payment ซึ่งหลายประเทศได้นำระบบ Faster Payment มาพัฒนา ใช้งานกันในช่วง 3-4 ปีที่ผ่านมา ซึ่งสำหรับประเทศไทยนั้นได้มีการพัฒนาระบบ PromptPay ขึ้นในปี 2559 และประเทศสิงคโปร์ได้มีการพัฒนาระบบ PayNow ขึ้นในปีเดียวกัน การที่ประเทศต่าง ๆ มีระบบ Faster Payment นี้ทำให้เปิดโอกาสให้การเชื่อมโยงการชำระเงินระหว่างประเทศสามารถจัดสร้างในรูปแบบ Switch-to-Switch ทำให้สามารถมีการเปิดให้บริการโอนเงิน/ชำระเงินข้ามประเทศในรูปแบบ Proxy (เช่น เบอร์โทรศัพท์มือถือ) ซึ่งง่าย สะดวก ปลอดภัย และมีค่าบริการที่ต่ำกว่าการให้บริการของ International Payment Service Provider

ธนาคารแห่งประเทศไทยและธนาคารชาติสิงคโปร์ได้มีการตกลงร่วมมือในการพัฒนาการเชื่อมโยงระบบการชำระเงินของทั้งสองประเทศในรูปแบบ Switch-to-Switch (PromptPay-PayNow) เพื่อที่จะให้บริการในการโอนเงิน/การชำระเงินในรูปแบบใหม่ ซึ่งในการพัฒนาการเชื่อมโยงระบบการชำระเงินระหว่าง ไทยและสิงคโปร์นี้ ได้มีการกำหนดหลักการเบื้องต้นดังนี้

1. ส่งเสริมการเชื่อมต่อการชำระเงินของอาเซียนโดยใช้รูปแบบ Switch-to-Switch
2. ส่งเสริมการแข่งขันและบริการที่เป็นนวัตกรรมที่ใช้ประโยชน์จากการเชื่อมโยงโครงสร้างพื้นฐานนี้
3. โครงสร้างพื้นฐานนี้ต้องปฏิบัติตามกฎหมายและระเบียบข้อบังคับของ AML / CFT
4. พัฒนาโครงสร้างพื้นฐานและการทำงานร่วมกัน เพื่ออำนวยความสะดวกในการชำระเงินผ่านช่องทางที่สะดวก และต้นทุนต่ำ

ธนาคารแห่งประเทศไทย ธนาคารพาณิชย์ และสำนักงานระบบการชำระเงินภายใต้สมาคมธนาคารไทย คาดว่ารูปแบบการเชื่อมโยง PromptPay-PayNow นี้ จะทำให้ประชาชาชนทั้งสองประเทศสามารถโอนเงินและชำระเงินได้ง่ายขึ้น สามารถนำไปเป็นต้นแบบในการพัฒนาการเชื่อมโยงกับประเทศอื่น ๆ ได้ง่าย เพื่อความสะดวก ความรวดเร็ว มีความปลอดภัย และประหยัดค่าใช้จ่าย

โครงการนี้ธนาคารพาณิชย์ในประเทศไทย ได้มีธนาคารนำร่อง 4 ธนาคารทาง คือ ธนาคารกรุงเทพ ธนาคารกสิกรไทย ธนาคารกรุงไทย และธนาคารไทยพาณิชย์ ทางธนาคารสิงคโปร์มีธนาคารนำร่อง 3 ธนาคาร คือ DBS UOB และ OCBC ซึ่งกำลังร่วมกันพัฒนา และคาดว่าจะเปิดให้บริการได้ในราวเดือนมิถุนายน 2563

การต่อยอดการให้บริการจากโครงสร้างพื้นฐานพร้อมเพย์

➢ MyPromptQR (B Scan C): The New Chapter of QR Payment

MyPromptQR (B scan C) เป็นบริการชำระเงินรูปแบบใหม่ที่พัฒนาบนระบบโครงสร้างพื้นฐานการชำระเงินดิจิทัลที่ใช้มาตรฐาน ISO20022 รองรับการส่งข้อมูลระหว่างสถาบันการเงินและภาคธุรกิจได้อย่างมีประสิทธิภาพ โดยสามารถส่งข้อมูลทางธุรกิจไปพร้อมกับการชำระเงิน สนับสนุนการปรับไปสู่ Digital Business อย่างครบวงจร

โดยธนาคารได้มีการพัฒนา MyPromptQR มาตั้งแต่เดือนสิงหาคม 2562 เพื่อให้ร้านค้าสามารถรองรับการจ่ายเงินจากลูกค้าผ่าน mobile applicationได้ เป็นการตอบโจทย์ความต้องการของธุรกิจที่มีขนาดใหญ่ขึ้นและมีเครือข่ายสาขาจำนวนมาก เช่น ร้านสะดวกซื้อ และห้างสรรพสินค้า โดย MyPromptQR จะช่วยให้ภาคธุรกิจรับชำระเงินได้สะดวกและรวดเร็วขึ้น สามารถเชื่อมโยงระบบการรับชำระเงินกับระบบ Point of Sale ที่จุดรับชำระเงินของร้านค้าได้อัตโนมัติ สะดวกขึ้นจากการให้บริการ QR Code แบบเดิม เป็นบริการที่ลดขั้นตอนและเวลาของแคชเชียร์ในการรับชำระเงิน อีกทั้งยังสามารถเชื่อมโยงกับระบบส่งเสริมการขาย ช่วยเพิ่มโอกาสทางธุรกิจได้ในอนาคต

และในอนาคตสามารถรองรับการเชื่อมโยงกับต่างประเทศ อีกทั้งยังช่วยเพิ่มความสามารถในการแข่งขันด้วยการใช้ประโยชน์จากการวิเคราะห์ข้อมูลชำระเงินเพื่อต่อยอดนวัตกรรมที่หลากหลาย และตอบสนองความต้องการของลูกค้าได้ดี

➢ BillAlert บริการเตือนเพื่อจ่าย

บริการที่ให้ให้กับ Biller ใช้เป็นบริการแจ้งเตือนการชำระบิลกับลูกค้า ที่มาสมัครใช้บริการ โดยสามารถยกเลิกการใช้งานได้ตามความต้องการ โดย Biller Bank ที่ได้รับคำสั่งจาก Biller ก็จะส่ง PayAlert (Request-to-Pay) ให้กับผู้รับด้วย Proxy (เช่น หมายเลขโทรศัพท์มือถือ หรือ หมายเลขบัตรประชาชน หรือ หมายเลขนิติบุคคล) โดยมีหลักว่า Biller Bank ต้องมีกระบวนการเปิดให้บริการกับ Biller ในระดับที่มีความน่าเชื่อถือ

ในด้านลูกค้า ที่ต้องการได้รับแจ้งเตือนจ่ายบิล ต้องไปสมัครบริการกับ Biller โดยไม่ต้องให้ Consent ไว้กับธนาคาร แต่ลูกค้าต้องมีการสมัครบริการพร้อมเพย์ด้วย หมายเลขโทรศัพท์มือถือ หรือ หมายเลขบัตรประชาชน หรือหมายเลขนิติบุคคล

การเปลี่ยนบัตรเดบิตและบัตรเอทีเอ็มแบบแถบแม่เหล็กเป็นบัตรแบบชิปการ์ด

ตามที่ฝ่ายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน ธนาคารแห่งประเทศไทย (ธปท.) มีนโยบายผลักดันการปรับเปลี่ยนบัตรเดบิตและบัตรเอทีเอ็มจากรูปแบบบัตรแถบแม่เหล็ก (Magnetic Card) ให้เป็นบัตรแบบชิปการ์ด (Chip Card) เพื่อยกระดับความความปลอดภัยในการทำธุรกรรมทางการเงินจากการใช้บัตรอิเล็กทรอนิกส์ป้องกันความเสี่ยงจากภัยไซเบอร์ที่เพิ่มมากขึ้น

โดยสำนักระบบการชำระเงินได้ร่วมกับ ธปท. ธนาคารสมาชิก ธนาคารรัฐ และธนาคารต่างประเทศ ที่ให้บริการในประเทศไทย ดำเนินงานตามนโยบาย พร้อมทั้งประชาสัมพันธ์ให้ผู้ที่ยังใช้บัตรเดบิตหรือบัตรเอทีเอ็มแบบแถบแม่เหล็กอยู่ในปัจจุบันติดต่อที่สาขาธนาคารเพื่อขอเปลี่ยนบัตรเป็นบัตรชิปการ์ดให้แล้วเสร็จในวันที่ 15 มกราคม 2563 โดยมีการเตรียมความพร้อมของสถาบันการเงินดังต่อไปนี้

1. การวิเคราะห์ข้อมูลลูกค้าที่ยังไม่เปลี่ยนบัตร
2. Implementation Plan สำหรับ ATM และ EDC
3. จัดเตรียม FAQs เรื่องการเปลี่ยนบัตรแถบแม่เหล็กเป็นชิปการ์ดให้แก่พนักงานสาขา และ Call Center
4. จัดเตรียมคู่มือกระบวนการเปลี่ยนบัตรให้กับลูกค้า เพื่อให้พนักงานสาขาปฏิบัติต่อลูกค้าในแนวทางเดียวกันและสร้างประสบการณ์ที่ดีในการมาใช้บริการ
5. จัดเตรียมวิธีการรับมือกับลูกค้าที่ยังไม่เปลี่ยนบัตรและไม่สามารถใช้งานบัตรแบบเดิมได้หลังวันที่ 15 ม.ค. 63

จำนวนบัตร ATM ลดลงจาก 18.38 ล้านใบในปี 2560 เหลือ เพียง 17.39 ในสิ้นปี 2561 แต่จำนวนบัตร Debit Card ได้เพิ่มขึ้นจาก 59.03 ล้านใบในปี 2560 เป็นจำนวน 62.06 ล้านใบในปี 2561 และจำนวนการใช้บัตร Debit Card ในการชำระค่าสินค้าและบริการได้มีจำนวนเพิ่มขึ้นจาก 224 ครั้งต่อบัตร/ปี ในปี 2560 เป็น 241 ครั้งต่อบัตร/ปี

ปรับปรุงมาตรฐานไทยแบงก์ชิปการ์ด (Thai Bank Chip Card – TBCC)

ในส่วนของ มาตรฐานไทยแบงก์ชิปการ์ด (Thai Bank Chip Card – TBCC) ได้มีการประกาศ เพิ่มมาตรฐาน Security CA & Root CA จากเดิมในปัจจุบันอยู่ใน Level 3 – Length 1408 เป็น Level 4 – Length 1984 โดยเริ่มดำเนินการตั้งแต่ ตุลาคม 2561 โดยทาง NITMX, TPN ได้ประกาศยกเลิกการ Support Key Length 1408 ซึ่งจะสิ้นสุดวันที่ 31 ธันวาคม 2562 นี้ ทั้งนี้บัตรที่อยู่ในท้องตลาด ที่ใช้ Key length แบบเดิม จะใช้งานได้จนถึงถึงวันที่ 31 ธันวาคม 2567

การพัฒนา EDC เพื่อรองรับเทคโนโลยี NFC (Near Field Communication)

สำนักงานระบบการชำระเงินได้ดำเนินงานร่วมกับธนาคารสมาชิกในการพัฒนา Terminal EDC ให้รองรับมาตรฐานบัตร Contactless – Pay Wave ด้วยมาตรฐานไทย เพื่อเตรียมรองรับการใช้งานกับไทย เพื่อเตรียมรองรับการใช้งานกับระบบงาน Transit ตั้งแต่ กุมภาพันธ์ 2562 โดยในปัจจุบัน มีการใช้งานบัตร Contact และ Contactless กับรถเมล์ ขสมก. แต่ยังเป็นรูปแบบ Online ซึ่งได้มีการประกาศ ใช้งาน ในเดือนเมษายน 2562

โครงการร่วมกับภาครัฐ

ในปี 2562 ภาครัฐให้ความสำคัญกับการปรับเปลี่ยนรูปแบบการรับ-จ่ายเงินไปสู่ Digital Payment อย่างชัดเจน ซึ่งเป็นผลมาจากการการพัฒนาโครงสร้างพื้นฐานระบบการชำระเงินตามแผนยุทธศาสตร์ National e-Payment Master Plan ตามแผนนี้มีโครงการมากมายบรรลุวัตถุประสงค์ตามที่วางไว้ ซึ่งหนึ่งในความสำเร็จคือการปรับเปลี่ยนการรับจ่ายเงินของภาครัฐให้มีความทันสมัยและลดการใช้เงินสดมาอย่างต่อเนื่อง

สนับสนุนและส่งเสริมการนำข้อมูลแบบอิเล็กทรอนิกส์มาร่วมใช้กับโครงการภาครัฐ (Government)

ภาครัฐมีส่วนสำคัญอย่างยิ่งในการขับเคลื่อนการใช้ Digital Payment ของไทย โดยที่ผ่านมาหน่วยงานภาครัฐให้ความสำคัญกับการปรับเปลี่ยนรูปแบบการรับจ่ายเงินไปสู่ Digital Payment อย่างชัดเจน โดยมีการดำเนินงานที่สำคัญ ได้แก่

1. ด้านการจ่ายเงิน
    - มีการจ่ายเงินสวัสดิการให้กับประชาชนโดยตรงทั้งผ่านบัตรสวัสดิการแห่งรัฐหรือจ่ายตรงเข้าบัญชีผู้มีสิทธิ
    - การคืนภาษีเงินได้บุคคลธรรมดากว่าร้อยละ 70 ด้วยพร้อมเพย์แทนการใช้เช็คในปี 2560 ช่วยลดค่าใช้จ่ายและเพิ่มประสิทธิภาพในการให้บริการประชาชน
2. ด้านการรับเงิน
    - มีการติดตั้งเครื่องรับบัตรและมาตรฐาน Thai QR Payment ที่หน่วยงานราชการกว่า 8,000 แห่ง (ข้อมูลเดือนสิงหาคม 2561)
    - Mobile Application ถุงเงินประชารัฐที่รองรับการชำระเงินจากผู้มีบัตรสวัสดิการแห่งรัฐด้วยต้นทุนต่ำ
    - แผนพัฒนาบริการของภาครัฐทางอิเล็กทรอนิกส์ (e-Government Service) ที่รองรับการชำระเงินทางอิเล็กทรอนิกส์ เช่น การชำระค่าธรรมเนียมการขอใบอนุญาตประกอบธุรกิจ

นโยบายส่งเสริมการใช้ Digital Payment ของภาครัฐ มีการกำหนดให้หน่วยงานภาครัฐรับเงินผ่านช่องทางอิเล็กทรอนิกส์ตั้งแต่เดือนมีนาคม 2561 รวมถึงการส่งเสริมให้มีการประยุกต์ใช้เทคโนโลยี (Contactless/ Near Field Communication: NFC6) ในระบบชำระค่าโดยสารสาธารณะที่สามารถใช้ได้กับระบบขนส่งหลากหลายประเภท เพื่อสนับสนุนการใช้ Digital Payment

ร่วมกำหนดข้อตกลงด้านธุรกิจ Business Rules และมาตรฐานสากล สำหรับบริการที่เกี่ยวข้องกับการชำระเงินอิเล็กทรอนิกส์

สำนักงานระบบการชำระเงินทำหน้าที่เป็นผู้ประสานงานหลักระหว่างธนาคารแห่งประเทศไทย ธนาคารพาณิชย์ ธนาคารต่างประเทศ ธนาคารรัฐ และผู้ให้บริการชำระเงินอิเล็กทรอนิกส์ไทย (Non-Bank) เพื่อให้การดำเนินการด้าน Digital Payment เติบโตอย่างต่อเนื่องอย่างมีเสถียรภาพ

โดยการริเริ่มโครงการต่าง ๆ เกี่ยวกับ Digital Payment นั้นต้องอาศัยความร่วมมือจากทุกหน่วยงานและทุกภาคส่วนเพื่อกำหนดข้อตกลงด้านธุรกิจให้เป็นไปในทางทิศทางเดียวกัน เพื่อให้การดำเนินงานเป็นไปอย่างคล่องตัว รวมทั้งภาคประชาชน ภาครัฐ และภาคธุรกิจ ได้ใช้งานอย่างสะดวกและปลอดภัย

การกำหนดข้อตกลงด้านธุรกิจนั้น จำเป็นต้องคำนึงถึงผู้ให้บริการและผู้รับบริการให้ได้รับผลประโยชน์สูงสุด ข้อจำกัดต่าง ๆ เช่น ข้อจำกัดด้านเทคนิค ด้านการใช้งาน ด้านกฎหมาย และเนื่องจากธนาคาร และผู้ให้บริการชำระเงินอิเล็กทรอนิกส์ไทย (Non-Bank) มีข้อจำกัดและการดำเนินงานที่แตกต่างกัน จึงจำเป็นอย่างยิ่งที่สำนักงานระบบการชำระเงิน จะทำหน้าที่เป็นตัวกลางในการประสานงาน การจัดประชุม ร่วมแสดงความคิดเห็น และ ชี้ให้เห็นถึงข้อจำกัดต่าง ๆ ที่แต่ละหน่วยงานมีความแตกต่างกัน โครงการที่มีการกำหนดข้อตกลงด้านธุรกิจมีดังนี้

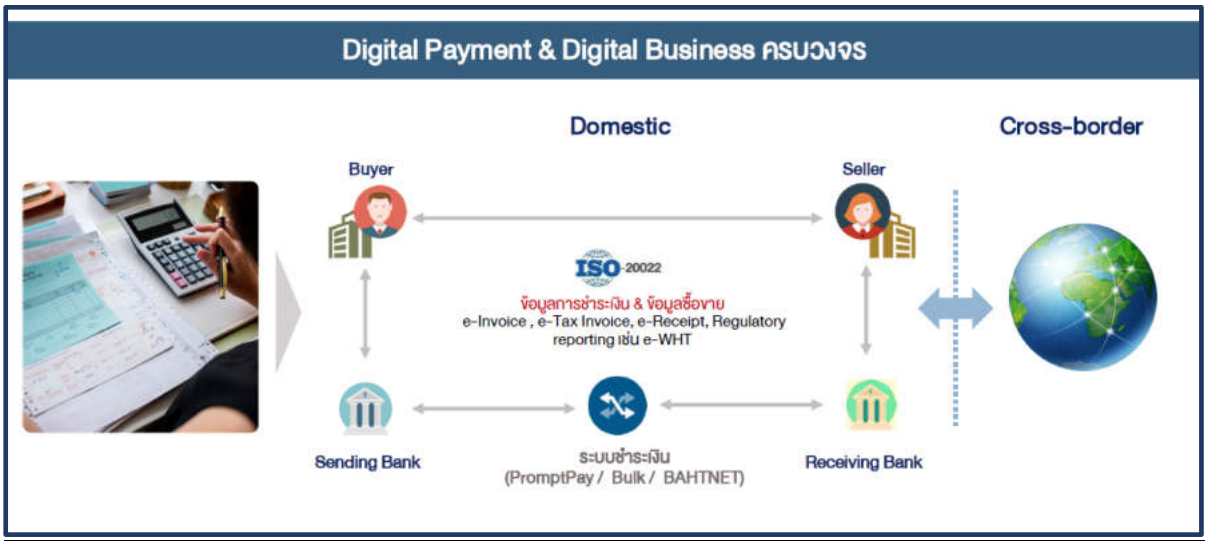
1. Business Rule ที่มีการนำมาปรับปรุงในปี 2562
    - Thai QR Payment (Domestic)

2. Business Rule ที่มีการดำเนินการในปี 2562
    - Cross border QR Payment (C scan B): Sponsor Model
    - Cross border Remittance: Sponsor Model (Inward)
    - MyPromptQR (B scan C Domestic)

3. Business Rule ที่เริ่มดำเนินการในปี 2562 (คาดว่าเสร็จสิ้นในปี 2563)
    - Cross border QR Payment (C scan B): Switch Model
    - BillAlert
    - ปรับ General Rule ของ PromptPay เพื่อรองรับบริการที่เกี่ยวกับนิติบุคคล

ในระบบการชำระเงินของไทยมีการใช้มาตรฐาน ISO 8583 มาเป็นเวลานาน ซึ่ง ISO 8583 มีข้อจำกัดต่อการพัฒนานวัตกรรม และขาดมาตรฐานกลางที่เชื่อมโยง e-Business แบบ End-to-End จึงเป็นเรื่องจำเป็นที่ธนาคารจะต้องมีการพัฒนามาตรฐานข้อความสากล ISO 20022 ซึ่งสำนักงานระบบการชำระเงิน และธนาคารได้ร่วมดำเนินการพัฒนาและส่งเสริมการใช้มาตรฐานข้อความสากล ISO 20022 เพื่อรองรับการรับส่งข้อมูลทางธุรกิจไปพร้อมกับการชำระเงิน ที่เป็นพื้นฐานสำคัญของการพัฒนาบริการชำระเงิน พร้อมทั้งสนับสนุนการพัฒนานวัตกรรมและการเชื่อมโยงกับต่างประเทศ

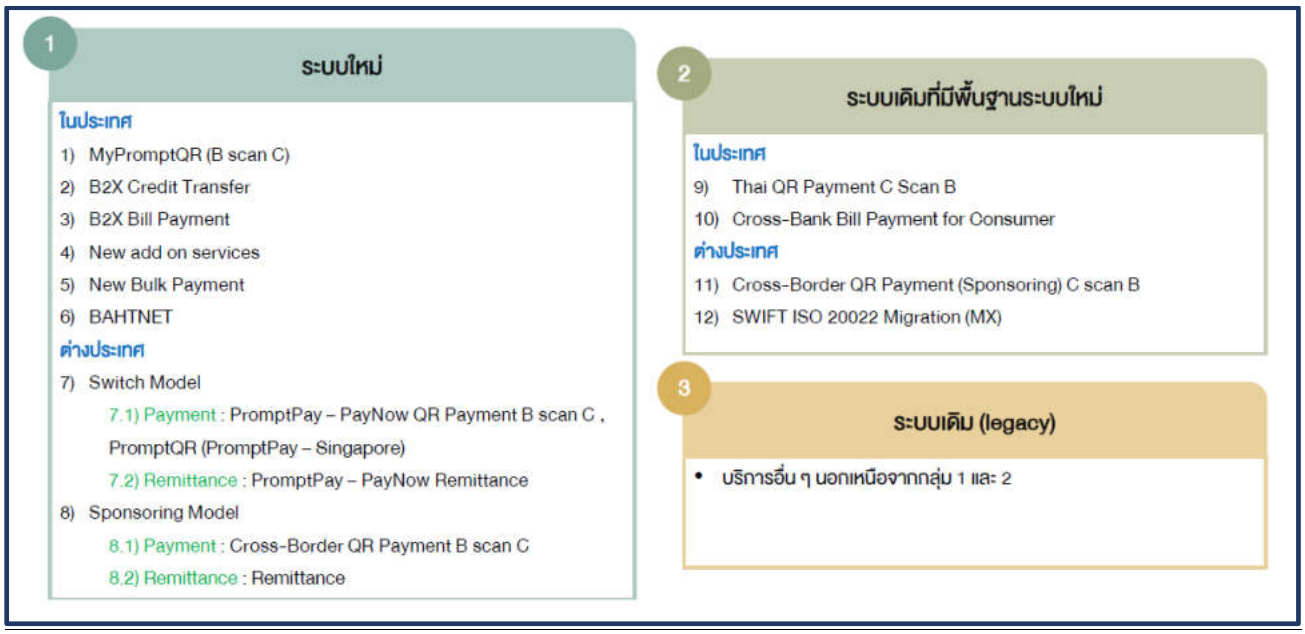
แนวทางการใช้มาตรฐานข้อความ ISO 20022 ในระบบการชำระเงิน



Guiding Principles การปรับใช้มาตรฐานข้อความ ISO 20022

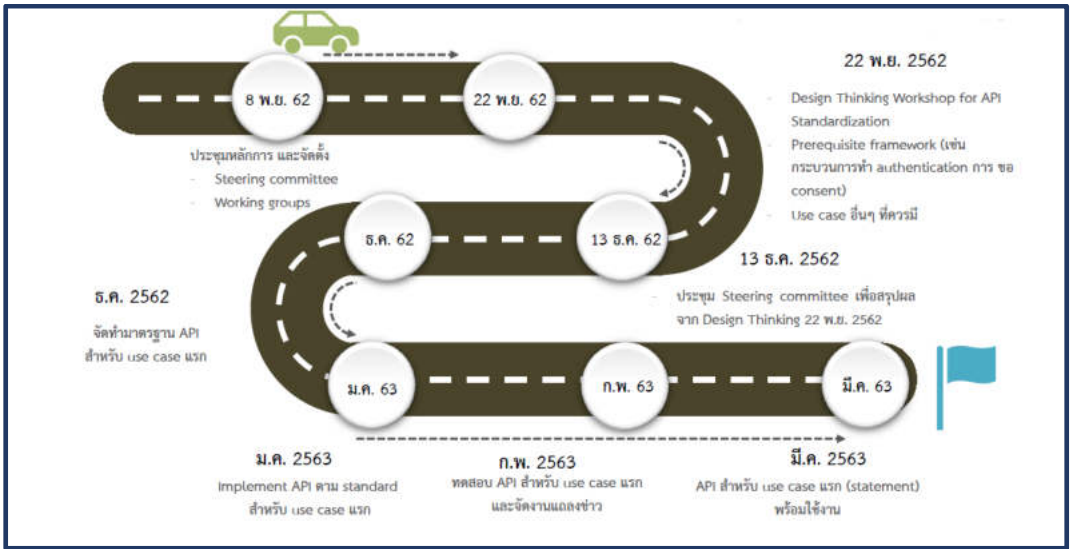
สำนักงานระบบการชำระเงินร่วมกับคณะทำงานพัฒนาและส่งเสริมการใช้ ISO 20022 การปรับใช้มาตรฐาน ISO 20022 ในระบบการชำระเงินแบ่งเป็น 3 กลุ่ม ได้แก่ (1) ระบบใหม่ (2) ระบบเดิมที่มีพื้นฐานระบบใหม่ และ (3) ระบบเดิม (Legacy) ซึ่งธนาคารพาณิชย์จะพิจารณาจัดกลุ่มบริการของทั้ง 3 ระบบ พร้อมเรียงลำดับการปรับใช้มาตรฐาน ISO 20022 ของแต่ละบริการตามความสำคัญและความพร้อมของธนาคารพาณิชย์แต่ละแห่ง โดยพิจารณาทั้งประเด็นด้านธุรกิจและด้านเทคนิค

การปรับใช้มาตรฐาน ISO 20022 แบ่งออกเป็น 3 ส่วน



การพัฒนามาตรฐาน API เป็นการส่งเสริมการเชื่อมโยงบริการร่วมกัน เพื่อเพิ่มความสะดวกและสร้างความเชื่อมั่นในการใช้บริการ Digital Payment มากขึ้น การเชื่อมโยงข้อมูลเพื่อนำไปสู่การยกระดับการให้บริการทางการเงินดิจิทัล (Digital Financial Services) ซึ่งจะช่วยเพิ่มประสิทธิภาพในการพัฒนาผลิตภัณฑ์และบริการทางการเงินร่วมกัน ทั้งยังช่วยลดต้นทุนการพัฒนาระบบและต้นทุนด้านปฏิบัติการของบริการทางการเงินทั้งระบบในระยะยาว อันจะเป็นประโยชน์ให้ลูกค้าสามารถเข้าถึงบริการทางการเงินได้ดีขึ้น สะดวก รวดเร็ว ปลอดภัย และตรงกับความต้องการของลูกค้าในระบบเศรษฐกิจดิจิทัลมากยิ่งขึ้น พร้อมทั้งรองรับการพัฒนาบริการต่อยอดอื่น ๆ ได้เช่น ตรวจสอบยืนยันรายการชำระเงินข้ามธนาคาร ตรวจสอบความเป็นเจ้าของหมายเลขโทรศัพท์มือถือก่อนการลงทะเบียนพร้อมเพย์และบริการอื่น ๆ

<u>แผนการจัดทำมาตรฐานAPI</u>



➢ ร่วมกำหนด มาตรฐาน e-KYC เพื่อสนับสนุน National Digital ID Project

หลังจากที่ได้มีการจัดตั้ง บริษัทเนชั่นแนลดิจิทัล ไอดี จำกัด (National Digital ID Co., Ltd.: NDID) ซึ่งเป็นหนึ่งใน 5 โครงสร้างพื้นฐานของประเทศที่จะช่วยพัฒนาและขับเคลื่อนประเทศให้เกิดสังคมดิจิทัล (Thailand 4.0 – Digital Economy) ซึ่งในเรื่องเกี่ยวกับระบบกลางได้มีการพัฒนาเป็นที่เรียบร้อยแล้ว และใน Phase 1 ได้มี 3 บริการที่ได้ดำเนินการ คือ 1) การเปิดบัญชีบุคคลธรรมดา 2) การบริการ Digital Lending และ 3) การเปิดบัญชี บล. บลจ. ผ่าน FinNet Proxy ในปี 2562 มีการดำเนินการดังต่อไปนี้

1. ออกแบบและพัฒนา Platform โดยคณะทำงานด้านเทคนิค
2. ร่วมพิจารณากฎหมายที่รองรับ
3. การกำหนด Business Model โดยคณะทำงานนำร่อง

ข้อมูลทางสถิติ

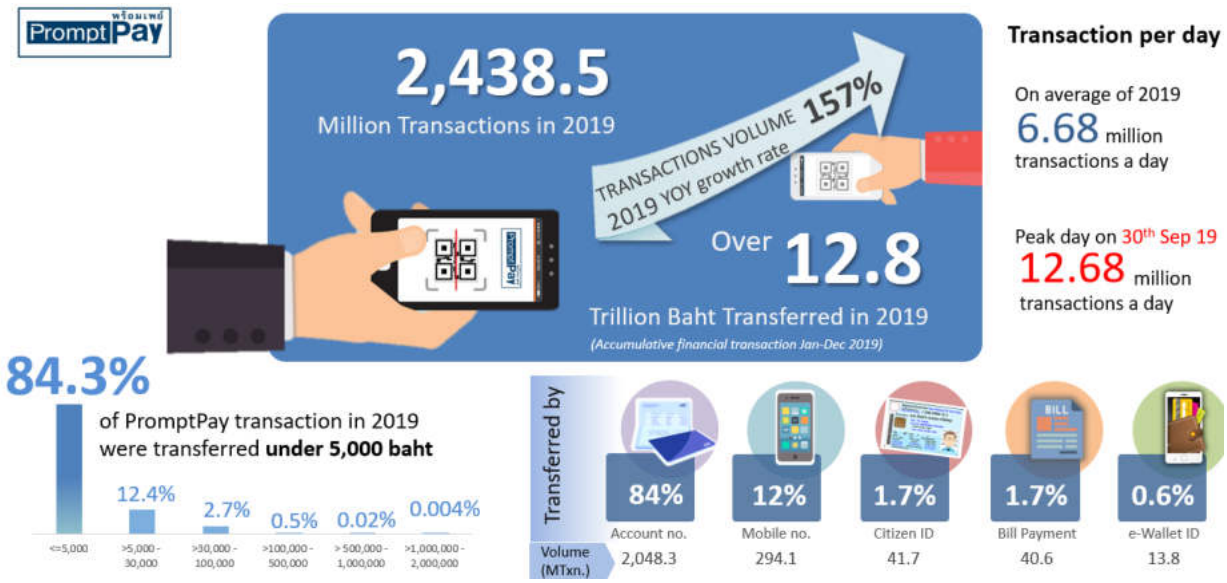
ในช่วงที่ผ่านมาการชำระเงินของไทยมีการเปลี่ยนแปลงไปสู่การชำระเงินทางอิเล็กทรอนิกส์ หรือ Digital Payment อย่างชัดเจน ซึ่งเริ่มต้นตั้งแต่แผนยุทธศาสตร์ National e-Payment ที่ประกาศปี 2558 โดยตั้งแต่นั้นมาพบว่าการใช้ Digital Payment ของประเทศมีกาพัฒนาขึ้นอย่างรวดเร็ว จากข้อมูลสถิติชี้ให้เห็นว่าการใช้ Digital Payment มีการเติบโตในทุกภาคส่วน ทั้งภาครัฐ ภาคการธนาคาร ภาคธุรกิจ รวมทั้งภาคประชาชน ถึงแม้ว่า ครม. เห็นชอบยุติบทบาท คกก. ขับเคลื่อนแผนยุทธศาสตร์ National e-Payment ภายหลังบรรลุเป้าหมายเรียบร้อยแล้ว แต่ ธปท. ยังคงมีการดำเนินการต่อตามแผนกลยุทธ์ระบบการชำระเงินฉบับที่ 4 (พ.ศ. 2562-2564) ธปท. ซึ่งมีวิสัยทัศน์คือ "***Digital Payment เป็นทางเลือกหลักในการชำระเงินภายใต้ระบบการชำระเงินที่มีประสิทธิภาพ ปลอดภัย ต้นทุนต่ำ ตรงกับความต้องการของผู้ใช้บริการ***"

จำนวนผู้ลงทะเบียน ในระบบพร้อมเพย์ ยังเพิ่มขึ้นอย่างต่อเนื่องจากปลายปี 2561 ซึ่งมีผู้ลงทะเบียนรวม 46.17 ล้านเลขหมาย ที่เป็นเลขหมายโทรศัพท์มือถือ 16.8 ล้าน และเลขประจำตัวประชาชน รวมถึงเลขประจำตัวนิติบุคคล 29.3 ล้าน เพิ่มขึ้นมาเป็น ณ. สิ้นปี 2562 จำนวนผู้ลงทะเบียนรวม 49.16 ล้านเลขหมาย ซึ่งเป็นเลขหมายโทรศัพท์มือถือ 18.86 ล้าน และเลขประจำตัวประชาชน รวมถึงเลขประจำตัวนิติบุคคล 30.29 ล้าน

ข้อมูลสถิติ การให้บริการพร้อมเพย์

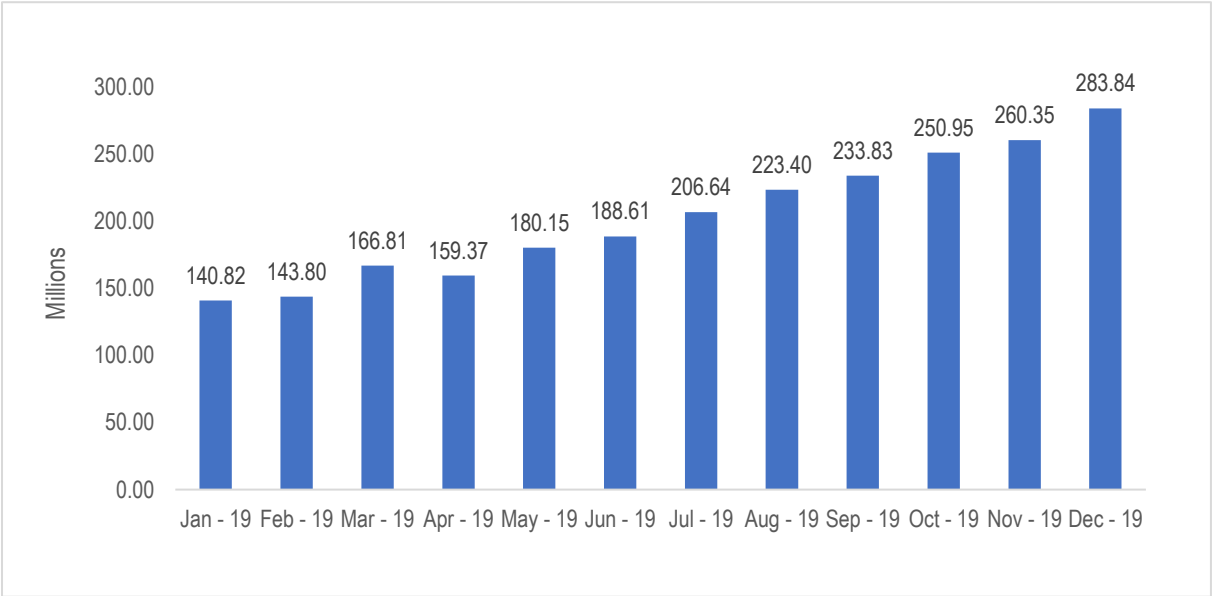
** ข้อมูลและภาพประกอบจาก บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด (NITMX) ข้อมูล ณ วันที่ 31 ธันวาคม 2562*

ข้อมูลสถิติ การให้บริการพร้อมเพย์



** ข้อมูลและภาพประกอบจาก บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด (NITMX) ข้อมูล ณ วันที่ 31 ธันวาคม 2562*

ธุรกรรมการโอนเงินข้ามธนาคารด้วยระบบพร้อมเพย์ ได้เพิ่มขึ้นมากจากจำนวน 140.82 ล้านรายการในเดือนมกราคม 2562 สูงขึ้น 101.25% เป็นจำนวน 283.4 ล้านรายการในเดือนธันวาคม 2562



จากข้อมูลธนาคารแห่งประเทศไทยตั้งแต่ปี 2558 ถึง 2561จะพบว่าปริมาณการชำระเงินผ่านช่องทางอิเล็กทรอนิกส์มีการเจริญเติบโตถึงราว 129.94% และโดยเฉพาะการชำระเงินด้วย Internet and Mobile Phone มีการเจริญเติบโตสูงถึง 588.31%

การประชาสัมพันธ์ การส่งเสริมการชำระเงินแบบอิเล็กทรอนิกส์

ASEAN Payment Connectivity

MyPromptQR

การให้ความรู้ด้าน Digital Payment

จัดการการอบรมสัมมนาเพื่อพัฒนาบุคลากรของธนาคารในเรื่องการชำระเงินทางอิเล็กทรอนิกส์

วันที่	หัวข้อในการบรรยาย	ผู้เข้าร่วมรับฟัง
16 ส.ค. 62	วิทยากรให้ความรู้ในหัวข้อ Digital Payment	ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
4 ก.ย. 62	■ Digital Banking Journey and Ecosystem in Thailand ■ Digital banking and digital economy initiatives to migrate Thailand into a cashless society	The Association of Banks in Malaysia
10 ต.ค. 62	Asia-Global Payment Summit (Asia-GPS)-discussing & Debate focused on the National EID Project	อินโดนีเซีย
29 ต.ค. 62	■ Commercial Banks' Contributions to PromptPay and Thai QR Payment and the Plan Going Forward ■ Applications of PromptPay and Thai QR Payment: Business Use Cases	Bank Indonesia
30 ต.ค. 62	จัดทำ Workshop ร่วมกันระหว่างกรมสรรพากร และภาคธนาคารเรื่องการนำส่งข้อมูล e- Withholding Tax	กรมสรรพากร
15 พ.ย. 62	วิทยากรใน Workshop เรื่อง Retail Payment Systems (Chip card and QR code standard)	National Bank of Cambodia: (NBC)
25 พ.ย. 62	ASEAN Payment Connectivity through QR Interoperability	กัมพูชา

สำนักงานระบบการชำระเงิน ปี 2563

- ผลักดันการพัฒนา MyPromptQR ให้มีการใช้งานให้กว้างขวาง
- ขับเคลื่อนแผน Payment Roadmap 4 ตามที่ได้กำหนดแผนงานร่วมกับภาคธนาคารและ NITMX
- พัฒนาการเชื่อมโยงระบบ Digital Payment กับต่างประเทศ (Cross-border Payment)
  - Interoperable QR Code for ASEAN
  - Switch-to-Switch Model
  - Sponsor Bank model through ITMX Switch
- ผลักดันการใช้มาตรฐาน API
- ขับเคลื่อน Payment Collaboration Alignment
- วางโครงสร้างและกำหนดแนวทางการพัฒนาระบบการชำระเงิน และการนำส่งข้อมูลการชำระเงิน ผ่านระบบอิเล็กทรอนิกส์เพื่อรองรับมาตรการของภาครัฐ
- สนับสนุนให้มีบริการทางการเงินและการชำระเงินทางอิเล็กทรอนิกส์อย่างต่อเนื่อง ทั้งภาครัฐ ภาคธุรกิจ และภาคประชาชน


สำนักงานระบบการชำระเงิน มุ่งมั่นในการพัฒนาระบบการชำระเงินของไทย
ให้เกิดขึ้นอย่างเป็นรูปธรรม โดยสถาบันการเงิน ภาครัฐ รวมถึงผู้มีส่วน
เกี่ยวข้องในระบบการชำระเงินของประเทศ มีการพัฒนาอย่างต่อเนื่อง เพื่อให้
ประชาชนในประเทศเข้าถึงบริการทางการเงินที่ทันสมัย มีความปลอดภัย ซึ่ง
จะเป็นส่วนสำคัญในการพัฒนาเศรษฐกิจของประเทศให้เติบโตอย่างมี
ประสิทธิภาพ
สำนักงานระบบการชำระเงิน
Payment System Office

TB-CERT

Thailand Banking Sector CERT

TB-CERT
Thailand Banking Sector CERT

ANNUAL REPORT 2

Thailand Banking Sector CERT (TB-CERT)

ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร [Thailand Banking Sector CERT -TB-CERT]

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 ด้านที่สำคัญ คือ

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

Organizational resilience เพื่อการเตรียมความพร้อมรับมือภัยด้านไซเบอร์ในยุคเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

การพัฒนาของเทคโนโลยีในช่วง 4-5 ปีที่ผ่านมาจะเห็นได้ว่าเป็นไปในอัตราเร่งและมักจะถูกเรียกกันว่าเป็นช่วงเวลาหรือยุคของ disruption ซึ่งให้ความหมายในมุมของผลกระทบจากการเปลี่ยนแปลงในเชิงลบ ขณะที่การเปลี่ยนแปลงดังกล่าวในอีกหลายด้านจะเป็นไปในทางสร้างสรรค์และเป็นการพัฒนาสังคมให้มีประสิทธิผลที่ดีขึ้นในยุคดิจิทัล อย่างไรก็ตามด้วยสภาพการเปลี่ยนแปลงที่รวดเร็วซึ่งเกิดจากการนำเทคโนโลยีที่ได้สร้างสมไว้เป็นพื้นฐานนำมาประกอบรวมกัน และด้วยความพร้อมของโครงสร้างพื้นฐานไม่ว่าจะเป็นระบบคลาวด์ การเชื่อมต่ออินเทอร์เน็ตความเร็วสูง และการเข้าถึงจำนวนผู้ใช้งานอุปกรณ์เคลื่อนที่ที่มีมากถึง 5.17 พันล้านคน หรือประมาณ 66% ของประชากรโลกในปัจจุบัน จึงก่อให้เกิดการนำเทคโนโลยีไปประยุกต์ใช้ในรูปแบบที่สร้างการเปลี่ยนแปลงได้ใน scale ขนาดใหญ่ จึงทำให้เกิดการเปลี่ยนแปลงสภาพแวดล้อมและการนำไปใช้งานแบบพลิกผันไปในรูปแบบที่ไม่เคยเป็นมาก่อน สภาพการณ์นี้จึงก่อให้เกิดผลกระทบทั้งธุรกิจและบุคคลธรรมดาที่ยังไม่เข้าใจเทคโนโลยี ยังไม่สามารถปรับเปลี่ยนวิธีการทำงานหรือวิถีการดำรงชีวิตได้เร็วเพียงพอกับการเปลี่ยนแปลงเหล่านั้น

การที่เทคโนโลยีถูกนำมาสร้างนวัตกรรมใหม่ ๆ บริการใหม่ ๆ และสร้างการเปลี่ยนแปลงอย่างรวดเร็วนั้น สภาพการใช้งานเทคโนโลยีเหล่านั้นจะกลายเป็นบรรทัดฐานใหม่ในการดำเนินของสังคม เช่น การใช้งาน chat หรือสื่อสารผ่าน mobile application แทนการส่งจดหมายและโทรศัพท์ ความเปลี่ยนแปลงของบรรทัดฐานในยุคดิจิทัลนี้จะแตกต่างจากช่วงก่อน กล่าวคือ ผู้ที่กำหนดบรรทัดฐานของสังคมนั้นไม่ใช่คนในสังคมแต่กลับเป็นบริษัทเทคโนโลยีผู้ที่นำเทคโนโลยีมาใช้ในการให้บริการ นั่นจึงเป็นปัจจัยหลักหนึ่งในการเร่งการเปลี่ยนแปลงให้เร็วขึ้น เนื่องจากไม่จำเป็นต้องใช้เวลาในการพัฒนาบรรทัดฐานของสังคม ยิ่งอัตราการนำเอาเทคโนโลยีมาใช้เป็นไปอย่างรวดเร็วเท่าใด โอกาสในการที่จะเตรียมการรับมือการเปลี่ยนแปลงดังกล่าวให้ได้มีประสิทธิภาพก็เป็นไปได้ยากขึ้นเท่านั้น โดยไม่ได้จำกัดที่ระดับปัจเจกบุคคลแต่จะส่งผลถึงการเตรียมความพร้อมในระดับองค์กรอีกด้วย ผู้ไม่ประสงค์ดีโดยเฉพาะที่เป็นภัยคุกคามทางไซเบอร์ก็มักจะใช้ช่องว่างของความเข้าใจสภาพการณ์ที่เปลี่ยนแปลงเร็วนี้ในการโจมตี หลอกขโมยข้อมูล หรือฝังตัวในองค์กรเพื่อรอโอกาสที่เหมาะสมต่อไป

ระดับความรุนแรงของเหตุการณ์การโจมตีทางไซเบอร์นั้น มีแนวโน้มที่จะมีความซับซ้อนมากขึ้น จากที่ทาง TB-CERT ได้มีการเก็บข้อมูลและเฝ้าระวังจะเห็นได้ว่า รูปแบบการโจมตีในหลายครั้งจะใช้เทคนิคแบบผสมผสานซึ่งอาจจะหมายถึงมีความร่วมมือหรือแลกเปลี่ยนข้อมูลระหว่างกลุ่มผู้โจมตี หากติดตามเหตุการณ์ต่าง ๆ ทั่วโลกจะเห็นว่าเป้าหมายที่สำคัญในช่วงปีที่ผ่านมามีแนวโน้มมุ่งไปที่หน่วยงานที่มีความสำคัญทางสารสนเทศของประเทศหรือที่เรียกกันว่า CII – Critical Information Infrastructure อีกทั้งยังมุ่งไปที่การขโมยข้อมูล ซึ่งนอกจากจะสร้างผลกระทบกับเจ้าของข้อมูลแล้วยังกระทบกับภาพพจน์ชื่อเสียงขององค์กรนั้น ๆ อีกด้วย นี่เป็นปัจจัยสำคัญหนึ่งที่ประเทศไทยพยายามผลักดันกฎหมายสำคัญ 2 ฉบับซึ่งมีความสำคัญมากในการที่ประเทศไทยจะก้าวสู่ยุคดิจิทัลและเป็นช่วงเวลาที่สำคัญในการสร้างความมั่นใจให้กับคนไทยและประเทศอื่น ๆ ที่จะต้องมีการเชื่อมต่อและทำธุรกรรมทั้งภาครัฐและภาคเอกชน นั่นคือ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ซึ่งได้ประกาศลงในราชกิจจานุเบกษาในวันที่ 27 พฤษภาคม 2562 โดย พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ นั้น มีวัตถุประสงค์เพื่อที่จะสนับสนุนให้หน่วยงาน CII มีมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สูงขึ้น มีความพร้อมรับมือภัยไซเบอร์ด้วยตนเอง อีกทั้งยังจะสร้างเครือข่ายความร่วมมือระหว่าง CII เพื่อสามารถที่จะติดต่อสื่อสารแลกเปลี่ยนข้อมูล แจ้งเตือน ไปจนถึงร่วมมือกันรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดย TB-CERT ถือว่ามีบทบาทที่สำคัญภายใต้ พ.ร.บ.ฉบับนี้ในการที่จะช่วยประสานงานกับหน่วยงานภาคการเงินและหน่วยงานที่เกี่ยวข้องเพื่อเตรียมความพร้อม อีกทั้งวิเคราะห์แนวทางการรับมือหรือลดความเสียหายจากภัยคุกคามทางไซเบอร์ ส่วน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ถือเป็นข้อกฎหมายที่จำเป็นในการที่จะยกสิทธิให้เจ้าของข้อมูลในการป้องกันดูแลข้อมูลของตนเองที่ถูกนำไปใช้เพื่อประโยชน์ เพื่อความสะดวกในการใช้บริการของเจ้าของข้อมูลเอง และยังเป็นการเพิ่มสิทธิในการควบคุมไม่ให้ถูกละเมิดได้ ในขณะเดียวกันก็เป็นการกำหนดมาตรการดูแลข้อมูลส่วนบุคคลให้กับหน่วยงานที่เก็บรักษาข้อมูลส่วนบุคคลนั้นให้สูงขึ้น นั่นก็หมายความว่าจะเป็นการเสริมสร้างมาตรการป้องกันดูแลข้อมูลให้กับทุกหน่วยงานในประเทศ

ด้วยเหตุนี้ การสร้างให้องค์กรมี resilience หรือมีความยืดหยุ่นรับมือกับภัยทางไซเบอร์จึงมีความสำคัญยิ่งยวดโดยเฉพาะในช่วงสภาพการณ์ที่มีความเปลี่ยนแปลงอย่างรวดเร็ว (disruption) ภัยคุกคามทางไซเบอร์มีรูปแบบที่ยากที่จะคาดเดาได้ องค์กรจะต้องมีการเตรียมพร้อมตั้งแต่ระดับนโยบาย การกำหนดบทบาทหน้าที่ความรับผิดชอบ การพัฒนาแผนการรับมือหากเกิดภัยทางไซเบอร์ขึ้น รวมไปถึงจะต้องนำแผนการรับมือนั้นไปซ้อมภายใต้สถานการณ์ต่าง ๆ เพื่อให้ผู้ที่เกี่ยวข้องตั้งแต่ผู้บริหารระดับสูงจนถึงผู้ปฏิบัติงานมีความคุ้นเคยในการตอบสนองรับมือต่อสถานการณ์ภัยคุกคามทางไซเบอร์โดยไม่ตระหนกจนเกินไป ผู้ปฏิบัติงานที่เกี่ยวข้องจะต้องมีทักษะในการจัดการกับปัญหาที่ไปในแนวทางเดียวกัน ผู้บริหารจะต้องสามารถกำหนดทิศทางขององค์กร

ภายใต้สถานการณ์การคุกคามทางไซเบอร์ได้ ส่งผลให้องค์กรสามารถปรับตัวรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพมากขึ้น

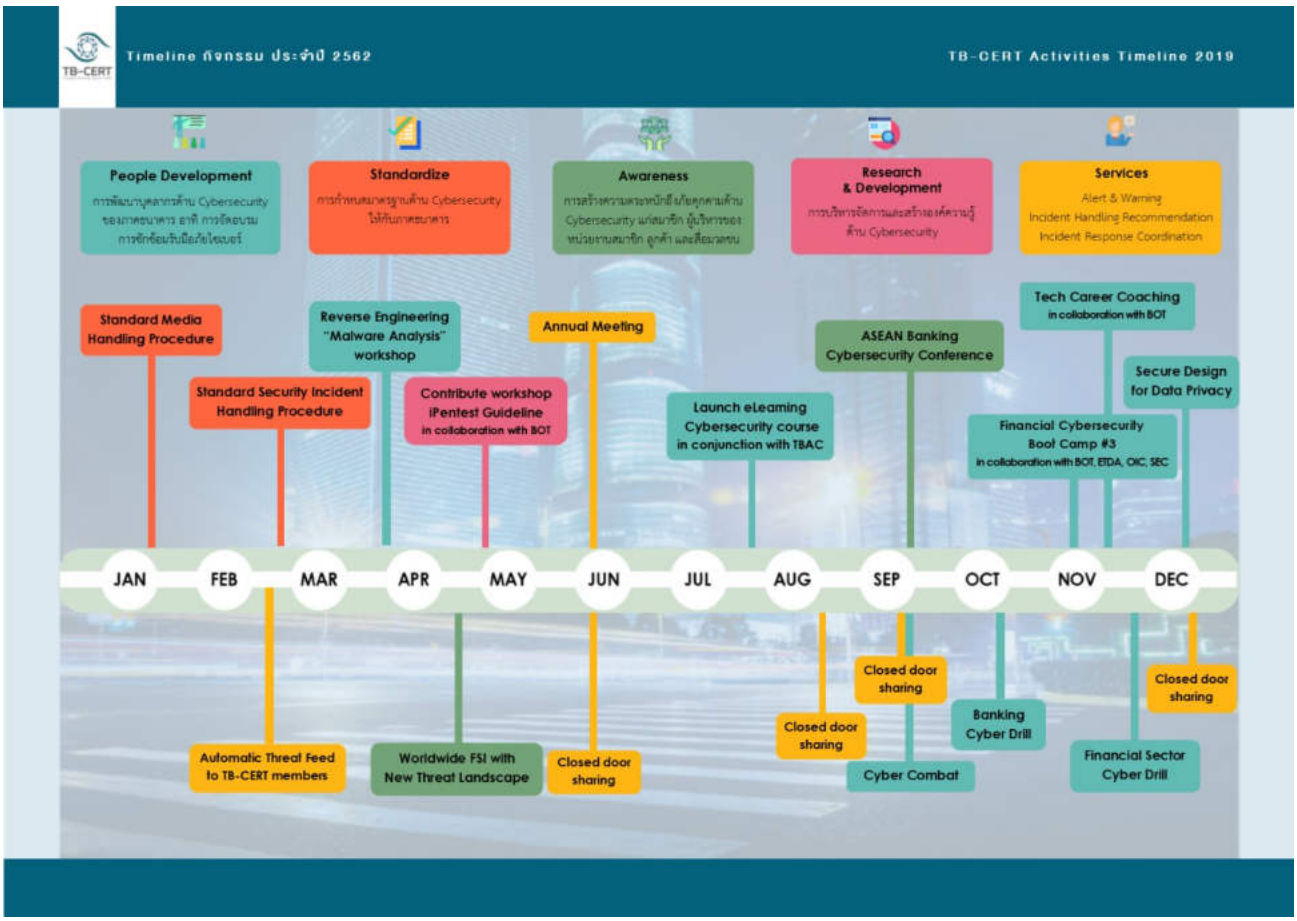
ในปี 2561 TB-CERT ได้เน้นยกระดับในเรื่องของ Incident Response ซึ่งถือเป็นกรอบการดำเนินการตอบสนองต่อเหตุการณ์อย่างมีมาตรฐาน ส่วนกิจกรรมในปี 2562 TB-CERT ได้เน้นที่จะช่วยธนาคารสมาชิกในการเตรียมความพร้อมรับมือภัยไซเบอร์ ให้มี resilience ในระดับขององค์กร ผ่านกิจกรรมที่หลากหลายต่อเนื่องทั้งปี ไม่ว่าจะเป็นการเตรียมความพร้อมให้กับผู้ปฏิบัติงานให้มีทักษะทางเทคนิคในเชิงลึกจากการจัด hands on workshop ไปจนถึงการจัดการแข่งขัน cyber combat และงานสัมมนาที่มุ่งเน้นไปในหัวข้อหลักในเรื่องของการพัฒนา organizational resilience โดยจะเห็นว่าภาคการธนาคารในภาพรวมมีความพร้อมมากขึ้น และด้วยการสนับสนุนจากทางธนาคารแห่งประเทศไทย ทำให้เกิดการสร้างความตระหนักหรือการให้ความสำคัญในการเตรียมความพร้อมรับมือภัยไซเบอร์ในระดับผู้บริหารระดับสูง ซึ่งเป็นการเติมเต็มองค์ประกอบสำคัญของ organizational resilience development

นอกจากนั้น TB-CERT ยังมีการขยายความร่วมมือกับองค์กรนอกภาคการเงิน ไม่ว่าจะเป็นหน่วยงานด้าน telecommunication หน่วยงานด้านความมั่นคง โดยการเชิญเข้าร่วมกิจกรรมของ TB-CERT เพื่อเสริมสร้างความสัมพันธ์ที่ดี และช่วยกันยกระดับความพร้อมในการเตรียมการป้องกันภัยคุกคามทางไซเบอร์ในวงกว้างขึ้น ซึ่งนอกจากจะเป็นการสนับสนุน พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์แล้ว ยังเป็นการสร้างเครือข่ายของความร่วมมือระหว่างอุตสาหกรรมต่าง ๆ ในประเทศไทย ด้วยภัยทางไซเบอร์มีแนวโน้มที่จะไม่จำกัดขอบเขตเฉพาะอุตสาหกรรมใดอุตสาหกรรมหนึ่ง แต่จะสร้างผลกระทบเชื่อมโยงข้ามอุตสาหกรรมอย่างหลีกเลี่ยงไม่ได้ ฉะนั้นการพัฒนา organizational resilience จึงมีความจำเป็นที่จะต้องขยายขอบเขตสู่ country wide resilience เพื่อให้มีความพร้อมรับมือภัยไซเบอร์ในระดับประเทศต่อไป

ดร.กิตติ โฆษะวิสุทธิ์
ประธานกรรมการ TB-CERT

Timeline กิจกรรมในปี 2562

ตลอด 3 ปี ที่ผ่านมา TB-CERT พัฒนาบุคลากรของสมาชิกอย่างต่อเนื่อง เราได้เน้นการสร้างรากฐานของ TB-CERT ให้มีความมั่นคงแข็งแรงเพื่อให้สมาชิกมีกรอบในการแลกเปลี่ยนข้อมูลอย่างไว้วางใจซึ่งกันและกัน รวมถึงการยกระดับความมั่นคงปลอดภัยไซเบอร์ให้กับทุกภาคส่วนของหน่วยงานสมาชิก โดยการพัฒนาบุคลากร สร้างความตระหนักรู้ให้กับสาธารณะ สร้างมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ทุกธนาคารมีหลักการหลักปฏิบัติร่วมกัน และพยายามผลักดันการสร้างวัฒนธรรมองค์กรให้มี Resilience ผ่านกิจกรรมต่าง ๆ ดังนี้



การพัฒนาบุคลากร (Human Resource Development)

Reverse Engineering “Malware Analysis” workshop

28-29 March 2019, Bangkok Bank Rama 3

Reverse Engineering “Malware Analysis” เป็นการอบรมเชิงปฏิบัติการต่อเนื่อง 2 วัน โดยวิทยากรบริษัท Group IB Mr. Vitaliy Trifonovis ในวันแรกผู้เข้าอบรมได้เรียนรู้เกี่ยวกับ Theory of Reverse Engineering และวันที่สองเป็นการลงมือปฏิบัติ ในหัวข้อ Dynamic and Static Malware Analysis

Secure Design for Data Privacy

17 December 2019,

National Credit Bureau Head Office

การสัมมนา Secure Design for Data Privacy TB-CERT ได้รับเกียรติจากวิทยากร คุณนฤดม รุ่งศิริวงศ์ ผู้อำนวยการอาวุโส หัวหน้าฝ่าย IT Security ธนาคารเกียรตินาคิน ที่ได้มาให้ความรู้เกี่ยวกับแนวคิด Privacy by Design แนวทางในการออกแบบเพื่อการจัดเก็บข้อมูลส่วนบุคคล เพื่อให้รองรับกับกรอบของกฎหมายคุ้มครองข้อมูลส่วนบุคคล และ GDPR พื้นฐานการออกแบบด้าน Information Security รวมทั้ง Design Pattern ที่สามารถนำไปใช้ได้

Cyber Combat

6 September 2019, The Athenee Hotel - A Luxury Collection Hotel


การแข่งขันการแข่งขัน Cyber Combat จัดขึ้นต่อเนื่องเป็นครั้งที่ 2 เพื่อพัฒนาทักษะของผู้ปฏิบัติงานด้านการป้องกันภัยไซเบอร์โดยมีผู้เข้าแข่งขันจากภาคการธนาคาร โทรคมนาคม และหน่วยงานความมั่นคง รวม 30 ทีม

Banking Cyber Drill

2 October 2019, Bank of Thailand Learning Center


การซ้อมรับมือภัยไซเบอร์ภาคการธนาคาร หรือ Banking Cyber Drill จัดขึ้นต่อเนื่องเป็นครั้งที่ 4 มีวัตถุประสงค์ดังนี้

- เพื่อยกระดับการซ้อมรับมือภัยไซเบอร์ ให้ผู้บริหารได้มีปฏิสัมพันธ์กับผู้ปฏิบัติงาน โดยจำลองสถานการณ์การซ้อมให้มีการร่วมกันตัดสินใจแก้ไขสถานการณ์
- เพื่อประเมินทักษะในการวิเคราะห์การโจมตีทางไซเบอร์ การประเมินแนวทางแก้ไขและป้องกันเหตุ
- เพื่อซักซ้อมการตอบสนองต่อเหตุการณ์แจ้งเตือนภัยคุกคามที่ได้รับจากระบบ Threat Intelligence

- เพื่อซักซ้อมขั้นตอนการตอบสนองต่อเหตุการณ์ผิดปกติจากการโจมตีทางไซเบอร์ กระบวนการประสานงาน ทั้งภายในหน่วยงาน ระหว่างหน่วยงานกับ TB-CERT หรือกับหน่วยงานภายนอกและสาธารณะ
- เพื่อพัฒนากระบวนการรับมือภัยไซเบอร์ให้มีประสิทธิภาพ เหมาะสมกับภาคการธนาคาร รวมทั้งเสริมสร้างความร่วมมือระหว่างธนาคารสมาชิกและ TB-CERT

โดยในปีนี้เป็นการซักซ้อมในรูปแบบ Hybrid Exercise แบ่งการซักซ้อมออกเป็น 2 ส่วน คือ

1. ช่วงเช้า เป็นการฝึกซ้อมของทีมปฏิบัติงาน มีผู้เข้าร่วมงาน 124 คนจากองค์กรสมาชิก TB-CERT
2. ช่วงบ่าย เป็นการฝึกซ้อมของทีมบริหาร มีผู้เข้าร่วมงาน 131 คนจากองค์กรสมาชิก TB-CERT และหน่วยงานที่เกี่ยวข้อง

Financial Cybersecurity Boot Camp #3

1-3 November 2019, Bank of Thailand Learning Center

TB-CERT สมาคมธนาคารไทย ร่วมกับหน่วยงานภายใต้บันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจ การเงิน การลงทุน และการประกันภัย ได้แก่ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จัดโครงการ Financial Cybersecurity Boot Camp ครั้งที่ 3 โดยมีวัตถุประสงค์เพื่อเพิ่มโอกาสในการพัฒนาทักษะด้าน Cybersecurity และเป็นการสร้างเครือข่ายบุคลากรรุ่นใหม่ที่มีความสนใจงานด้าน Cybersecurity ในภาคการเงิน รวมทั้งฝึกทักษะผ่านการแข่งขันทั้งในด้านการโจมตีและป้องกันระบบ ซึ่งในปีนี้มีผู้เข้าร่วมโครงการจำนวน 17 ทีม รวมทั้งสิ้น 64 คน ส่วนใหญ่กำลังศึกษาระดับปริญญาตรีชั้นปีที่ 3 และปีที่ 4 จากผู้สมัครทั้งสิ้น 30 ทีม รวม 109 คน

Tech Career Coaching

30 November 2019, Krungsri Ploenchit Office


TB-CERT ร่วมกับธนาคารแห่งประเทศไทย และฝ่ายบุคลากรของ 15 ธนาคารสมาชิกสมาคมธนาคารไทย ในการจัดงานแนะแนวอาชีพด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นโครงการต่อเนื่องจากโครงการ Financial Cybersecurity Boot Camp โครงการ Tech Career Coaching ได้จัดขึ้นเป็นครั้งแรก โดยมีวัตถุประสงค์เพื่อให้องค์กรภาคการเงินได้มีโอกาสให้ข้อมูลด้านวิชาชีพ การฝึกงาน และทุนการศึกษาด้าน IT และเป็นการสร้างเครือข่ายระหว่างฝ่ายบุคลากรขององค์กรภาคการเงินในการสร้างบุคลากรใหม่ด้าน IT เข้าสู่ภาคการเงินร่วมกันผ่านเวทีเสวนา และบูธให้คำปรึกษาจากองค์กรภาคการเงิน การจัดงานดังกล่าวได้รับการตอบรับเป็นอย่างดีจากผู้เข้าร่วมงานกว่า 250 คน ซึ่งมาจากผู้เข้าร่วมโครงการ Financial Cybersecurity Boot Camp จำนวน 24 คน

การสร้างการตระหนักรู้และเข้าใจภัยไซเบอร์ให้กับสมาชิก (Awareness Building)

Executive Banking Forum: Worldwide FSI with New Threat Landscape

25 April 2019, Intercontinental Bangkok

งานสัมมนา Worldwide FSI with New Threat Landscape ในครั้งนี้ ได้จัดขึ้นสำหรับผู้บริหารสายงานเทคโนโลยี รวมทั้งหัวหน้าฝ่ายด้านการรักษาความปลอดภัยของระบบและข้อมูลของหน่วยงานสมาชิก โดยได้รับเกียรติจากผู้เชี่ยวชาญบริษัท FireEye ซึ่งเป็นผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ มาบรรยายแลกเปลี่ยนมุมมองด้านความซับซ้อนของภัยคุกคามในปัจจุบัน แนวทางในการป้องกัน ตรวจจับ และรับมือกับภัยคุกคาม รวมทั้งกรณีศึกษาจากธนาคารต่างประเทศ

ASEAN Banking Cybersecurity Conference

6 September 2019, The Athenee Hotel - A Luxury Collection Hotel

กล่าวต้อนรับและกล่าวเปิดงานโดย คุณชาติศิริ โสภณพนิช ที่ปรึกษาสมาคมธนาคารไทย และ ดร.วิรไท สันติประภพ ผู้ว่าการธนาคารแห่งประเทศไทย

งานสัมมนาประจำปี ASEAN Banking Cybersecurity Conference จัดขึ้นภายใต้หัวข้อหลัก “Building A Resilient Organizational Culture” เพื่อเป็นการพัฒนาบุคลากรให้มีความตระหนักในเรื่องของ Cyber Resilience โดยแบ่งการจัดงานออกเป็น 2 ส่วน ได้แก่ งานสัมมนาเชิงวิชาการ ประกอบด้วยหัวข้อสัมมนาทั้งด้าน Technical และ Management รวมถึงการแสดง solution จากบริษัทผู้สนับสนุน ซึ่งมีผู้สนใจเข้าร่วมงานกว่า 400 คนจากภาคการเงินการธนาคาร ทั้งในประเทศไทยและอาเซียน รวมทั้งหน่วยงานด้านการลงทุนและการประกันภัย

การวิจัยและการพัฒนามาตรฐานด้านไซเบอร์ (Research and Development)

iPentest Guideline Workshop

26 April 2019, Bank of Thailand Learning Center

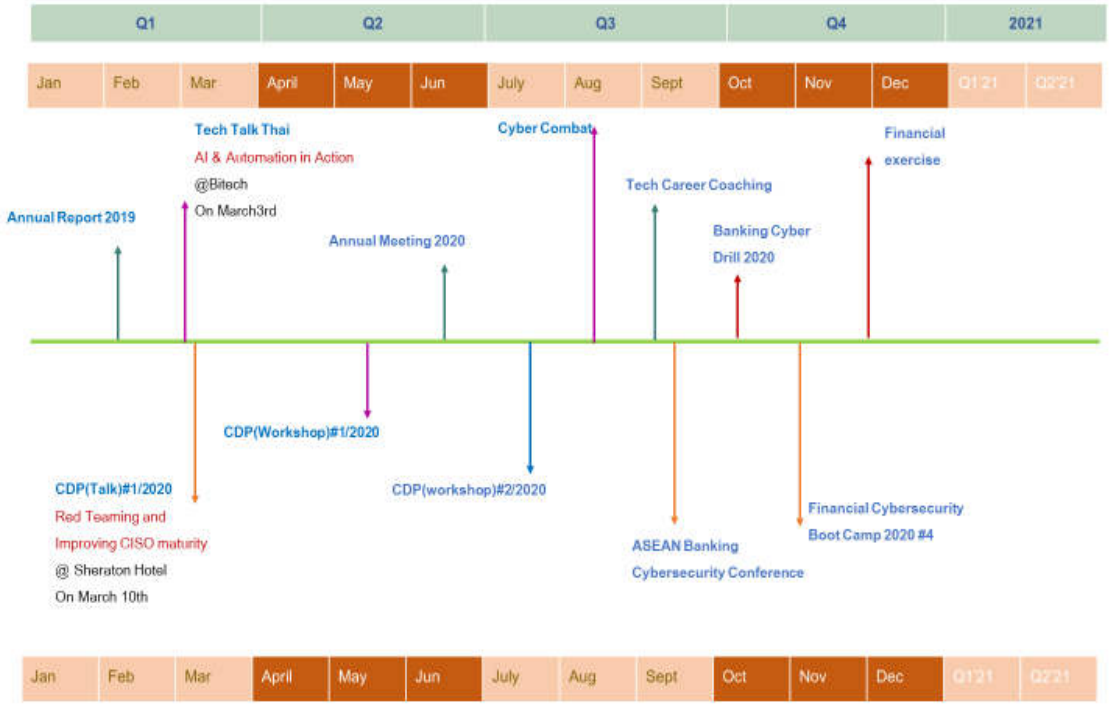
TB-CERT ร่วมกับธนาคารแห่งประเทศไทย ในการจัดทำแนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led (Intelligence-led Penetration Testing Guideline: iPentest) ซึ่งเป็นการทดสอบเจาะระบบในลักษณะเสมือนจริงหรือ Red Teaming ตามมาตรฐานสากล เพื่อยกระดับความพร้อมของสถาบันการเงินในการป้องกันและรับมือภัยคุกคามไซเบอร์ ให้มีการป้องกันที่แข็งแรง ตรวจจับภัยคุกคามทางไซเบอร์ได้ทันการณ์ สามารถตอบสนองต่อเหตุการณ์และกู้คืนระบบและบริการได้รวดเร็ว รวมทั้งได้จัดให้มีการอบรมเพื่อสร้างความรู้ความเข้าใจในเรื่องดังกล่าว

TB-CERT Annual Meeting

24-26 May 2019, Siam Commercial Bank Training Center, Chonburi

TB-CERT ได้จัดงานประชุมสมาชิกประจำปี ซึ่งเป็นกิจกรรมกลุ่มสัมพันธ์เชิงวิชาการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นการระดมสมองและวางแผนงานประจำปีของ TB-CERT การแชร์ความรู้ทางเทคนิค ให้สมาชิกได้มีโอกาสพบปะ ทำกิจกรรม และเสริมสร้างความสัมพันธ์ระหว่างสมาชิกอีกด้วย

แผนการดำเนินการในปี 2563

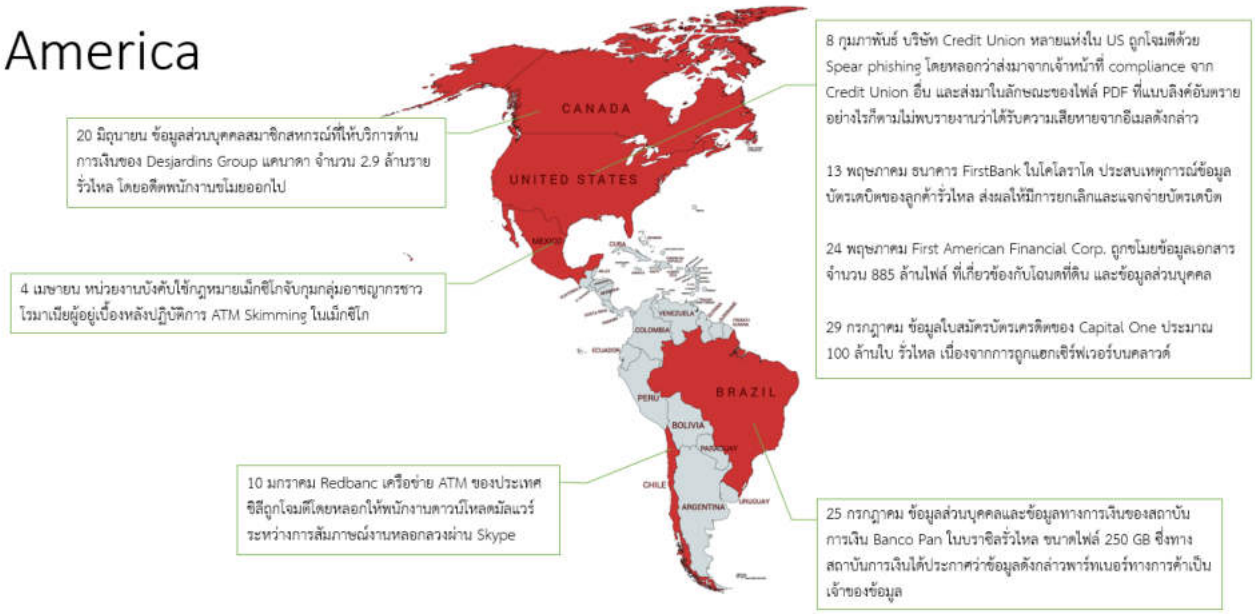


TB-CERT มีแผนการการดำเนินงาน โดยผ่านกิจกรรมการพัฒนาบุคลากรให้มีคุณภาพมากขึ้นเพื่อนำไปสู่ CERT level 4 ในปี 2563 นี้ โดยกิจกรรมที่เสริมสร้างให้ Cybersecurity ของ ภาคการธนาคารแข็งแกร่งขึ้น ได้แก่

1. กิจกรรมที่พัฒนาทักษะความรู้ด้านไซเบอร์ให้กับสมาชิก ได้แก่ CDP[1](Talk), CDP[1](workshop), Cyber Combat
2. กิจกรรมที่ช่วยสร้างความตระหนักถึงภัยคุกคามด้าน Cybersecurity ให้กับภาคประชาชน ได้แก่ ASEAN Banking Cybersecurity Conference, Tech Talk Thai Ai & Automation in action,
3. ฝึกซ้อมการรับมือภัยไซเบอร์เมื่อเกิดเหตุการณ์ ด้าน Cybersecurity ให้กับภาคการเงินการธนาคาร ได้แก่ Banking Cyber Drill และ Financial Sector Exercise
4. กิจกรรมที่เสริมสร้างบุคลากรเข้าสู่ภาคการเงินการธนาคาร ในด้าน cybersecurity ได้แก่ Tech career coaching, Financial Cybersecurity Boot Camp
5. กิจกรรมที่เสริมสร้างความสัมพันธ์ระหว่างสมาชิก และสร้างความเชื่อมั่น ไว้วางใจซึ่งกันและกัน ได้แก่ การจัดประชุมใหญ่ประจำปี Annual Meeting

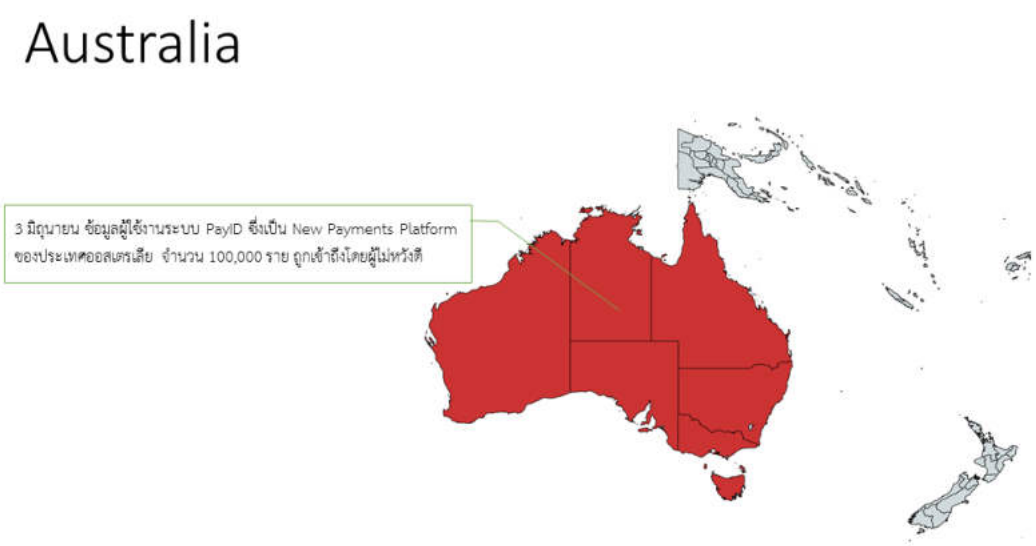
เหตุการณ์สำคัญด้านภัยไซเบอร์ในปี 2562

สรุปเหตุการณ์โลกที่น่าสนใจตามทวีปต่าง ๆ ปี 2562



จากเหตุการณ์แนวโน้มการโจมตีสถาบันการเงินในทวีปอเมริกา เป็นการโจมตีเพื่อขโมยข้อมูลเป็นสำคัญ โดยส่วนใหญ่จะเป็นข้อมูลส่วนบุคคลของลูกค้าโดยเทคนิคของ social engineering เช่น phishing หรือการส่งไฟล์แนบที่มีมัลแวร์ไปกับอีเมลก็ยังเป็นเทคนิคที่ยังคงใช้งานได้ดี อีกทั้งในบางเหตุการณ์นั้นเกิดจากผู้ดูแลระบบปรับแต่งค่าการป้องกันการเข้าถึงที่ผิดพลาด ทำให้แฮกเกอร์สามารถเข้าถึงฐานข้อมูลที่อยู่กับผู้ให้บริการคลาวด์ภายนอกได้อย่างง่ายดาย ส่วนเหตุการณ์การโจมตีบริการ ATM ก็ยังพบอยู่แต่จะมีวิธีการที่เปลี่ยนแปลงไป โดยหันไปมุ่งโจมตีไปยังบริษัทผู้ให้บริการเครือข่าย ATM โดยมีเหตุการณ์หนึ่งที่เกิดขึ้นในประเทศชิลีซึ่งเป็นฝีมือของกลุ่มแฮกเกอร์ Lazarus จุดเริ่มต้นของการโจมตีอยู่ที่พนักงานของบริษัท Redbanc ได้ทำการสมัครงานผ่าน LinkedIn ในตำแหน่ง Developer พนักงานดังกล่าวถูกหลอกให้ดาวน์โหลดและเปิดไฟล์แนบชื่อ ApplicationPDF.exe โดยถูกหลอกว่าเป็นแอปพลิเคชันที่ช่วยในการสร้าง Resume ในรูปแบบของบริษัทที่สมัครงาน ซึ่งภายหลังมีการวิเคราะห์พบว่าเป็นมัลแวร์ชื่อ PowerRatankba และมัลแวร์นี้ได้รวบรวมข้อมูลภายต่าง ๆ ในเครื่องและส่งกลับไปยังเซิร์ฟเวอร์ ได้แก่ รายละเอียดของระบบปฏิบัติการ การตั้งค่า Proxy รายการ Process ปัจจุบัน การเชื่อมต่อ RPC และ SMB รวมถึงสถานะของการเชื่อมต่อ RDP ด้วย หลังจากนั้นเมื่อแฮกเกอร์สามารถเข้าถึงเครื่องดังกล่าวได้แล้วได้ดำเนินการในขั้นตอนต่อ ๆ ไปเพื่อขโมยเงิน

เหตุการณ์ด้านความปลอดภัยสารสนเทศที่พบในทวีปยุโรปส่วนใหญ่เป็นภัยคุกคามที่เกี่ยวข้องกับข้อมูลรั่วไหลเช่นกันกับทวีปอเมริกา แม้ว่าจะมีเหตุการณ์ที่ข้อมูลถูกขโมยจากระบบคลาว์ดน้อยกว่าของทวีปอเมริกาก็ตาม ข้อมูลส่วนบุคคลของลูกค้าสถาบันการเงินที่ถูกขโมยแล้ว ยังมีข้อมูล Biometrics เช่น ลายนิ้วมือและใบหน้ารั่วไหลอีกด้วย ซึ่งข้อมูลประเภทนี้ต้องให้ความสำคัญเนื่องจากข้อมูลดังกล่าวไม่สามารถถูกเปลี่ยนแปลงได้ โดยใน พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล 2562 ของไทยหรือ GDPR – General Data Protection Regulation ของ EU ยังระบุให้ข้อมูล Biometrics นี้เป็นข้อมูลประเภทอ่อนไหว (Sensitive information) ต้องให้การคุ้มครองป้องกันเป็นพิเศษเพื่อมิให้เกิดผลกระทบกับเจ้าของข้อมูล นอกจากนี้ยังมีเหตุการณ์ที่แฮกเกอร์พยายามขโมยเงินจากธนาคาร Bank of Valletta (BOV) ประเทศ Malta จำนวน 13 ล้านยูโร ถึงแม้ว่าความพยายามครั้งนี้จะไม่ประสบความสำเร็จ แต่ก็ทำให้ธนาคารหยุดให้บริการ ซึ่งสร้างความเสียหายให้แก่ธนาคาร



ในประเทศออสเตรเลียพบเหตุการณ์ข้อมูลผู้ใช้งาน PayID ซึ่งเป็นแพลตฟอร์มการโอนเงินของประเทศออสเตรเลีย (New Payments Platform-NPP) ที่อนุญาตให้โอนเงินด้วยหมายเลขโทรศัพท์หรืออีเมล (คล้ายกับระบบพร้อมเพย์ของประเทศไทย) โดยผู้ไม่หวังดีจะทำการโอนเงินโดยใช้หมายเลขโทรศัพท์หรืออีเมลที่ต้องการทราบข้อมูล จากนั้นระบบจะแจ้งข้อมูลส่วนบุคคลของผู้ที่รับโอนเงินกลับมา อย่างไรก็ตามทางธนาคาร CUA – Credit Union Australia ได้ประกาศถึงผลกระทบว่า ข้อมูลชื่อเต็ม หมายเลขโทรศัพท์มือถือ และเลขบัญชีธนาคารถูกเข้าถึงด้วยวิธีดังกล่าว จากข้อมูลที่ถูกเก็บรวบรวมด้วยวิธีดังกล่าวผู้ไม่หวังดีจะใช้ข้อมูลนั้นมาใช้ในการส่งอีเมล phishing หรือโทรติดต่อเพื่อหลอกข้อมูลอื่น ๆ เพิ่มเติมก่อนดำเนินการสร้างความเสียหายในรูปแบบอื่น ๆ ต่อไป

ในปี 2562 ที่ผ่านมา หน่วยงานและสถาบันการเงินในทวีปเอเชียถูกโจมตีจากกลุ่มแฮกเกอร์ต่าง ๆ โดยแฮกเกอร์มักจะเลือกเป้าหมายโจมตีเป็นประเทศอินเดีย โดยส่วนใหญ่จะเป็นการขโมยข้อมูลด้วยการสร้างมัลแวร์ ATMDtrack เพื่อโจมตี ATM นอกจากนี้ธนาคารในบังคลาเทศเองก็ถูกขโมยเงินกว่า 3,000,000 เหรียญสหรัฐผ่านตู้ ATM ซึ่งเชื่อว่าเป็นฝีมือของกลุ่มแฮกเกอร์ที่ชื่อ Silence ส่วนในประเทศญี่ปุ่นพบมัลแวร์ Ursnif ที่โจมตีธนาคารหลายแห่งและมีเหตุการณ์ที่กลุ่มแฮกเกอร์ Fancy Bear ส่งอีเมลข่มขู่เพื่อที่จะโจมตีแบบ DDoS หากไม่จ่ายเงินด้วย ในเหตุการณ์นั้นทำให้ JPCERT/CC (CERT ประเทศญี่ปุ่น) ได้ออกมาประกาศแจ้งเตือน แต่ในเหตุการณ์ครั้งนั้นไม่ได้รับรายงานแจ้งความเสียหาย

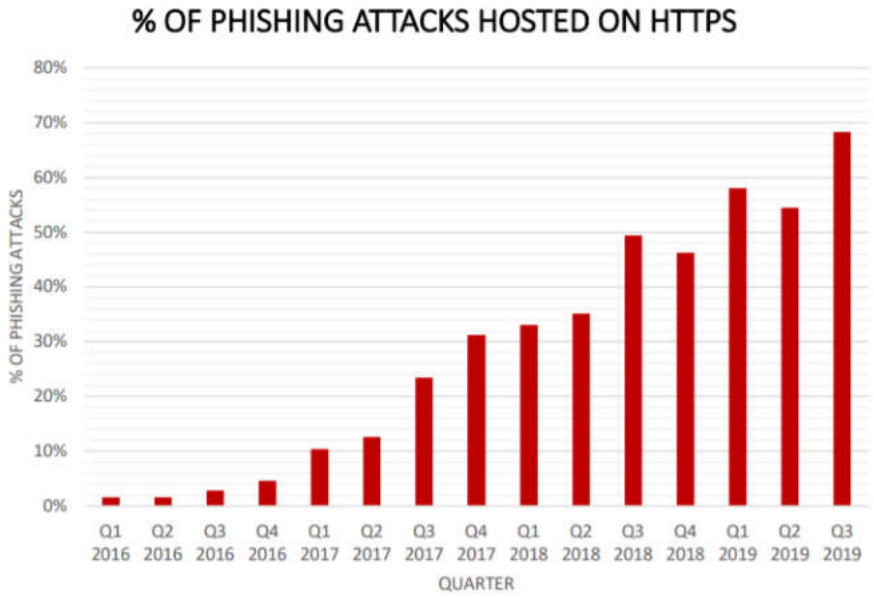
สำหรับประเทศไทยนั้น ถึงแม้ว่าธนาคารและสถาบันการเงินในประเทศไทยจะไม่เกิดเหตุการณ์ถูกโจมตีจนทำให้เกิดผลกระทบโดยตรง แต่ก็มีเหตุการณ์ข้อมูลรั่วไหลจากเว็บพนันออนไลน์ และเว็บสายการบิน ซึ่งเป็นข้อมูลส่วนบุคคลที่รั่วไหลออกไปและบุคคลเหล่านั้นก็เป็นลูกค้าธนาคาร จึงอาจจะทำให้มีผู้ไม่หวังดีใช้ข้อมูลดังกล่าวแอบอ้างเพื่อหลอกลวงเป็นเจ้าของข้อมูลและมาทำธุรกรรมกับธนาคาร ซึ่งถือเป็นการสร้างผลกระทบทางอ้อมแก่ธนาคาร

วิเคราะห์เหตุการณ์ในปี 2562 เทียบกับปี 2561

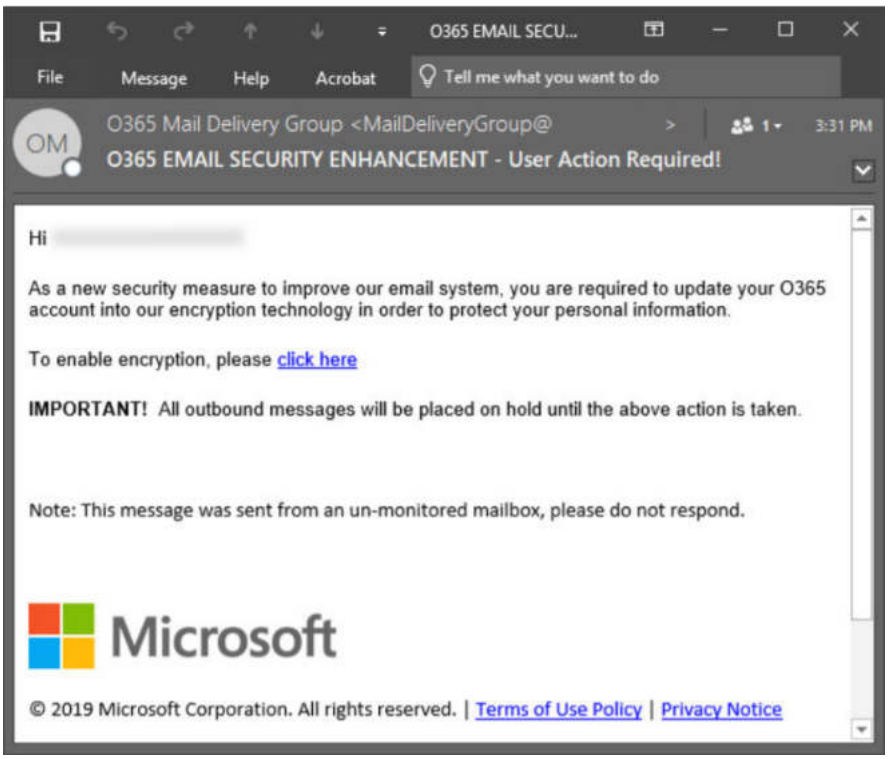
ในปี 2562 มีเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับภาคการธนาคารทั่วโลก โดย

1. **ฟิชชิงที่ตรวจจับและปิดกั้นได้ยากขึ้น** จากรายงานเหตุการณ์ฟิชชิงที่เกี่ยวข้องกับธนาคารในประเทศไทยที่ TB-CERT ได้รับแจ้งมานั้นพบว่าปริมาณเว็บไซต์ฟิชชิงที่มีการใช้ https เพื่อให้เว็บไซต์นั้นดูน่าเชื่อถือมากขึ้น มีมากถึง 77% ดังรูปที่ 1 และเมื่อเปรียบเทียบกับสัดส่วนจากรายงานสถิติฟิชชิงทั่วโลกจาก AntiPhishing Working Group (APWG) พบว่าในช่วงไตรมาสที่ 3 ของปีนี้มีปริมาณเว็บฟิชชิงที่ใช้ HTTPS ถึง 68% [1] ดังรูปที่ 2 ซึ่งมีความสอดคล้องกับสถิติเว็บฟิชชิงที่เกี่ยวข้องกับธนาคารในประเทศไทยที่ TB-CERT ได้รับแจ้ง และยังมีแนวโน้มเพิ่มขึ้นในทุก ๆ ไตรมาสอีกด้วย อีกทั้งแฮกเกอร์จะเลือกใช้ผู้ให้บริการรับฝากเว็บไซต์กับบริษัทเล็กหรือก่อตั้งใหม่ เนื่องจากบริษัทเหล่านี้จะมีช่วงเวลาการให้บริการไม่ตลอด 24 ชั่วโมง และบางบริษัทติดต่อยาก หรือไม่สนใจในการแก้ไขปัญหาดีพอ และเมื่อพบเว็บไซต์ฟิชชิงถูกจัดเก็บที่โฮสติ้งดังกล่าว ทำให้ takedown ได้ช้า นอกจากนี้ในปี 2562 พบฟิชชิงที่หลอกลวงว่าเป็นระบบอื่น นอกจากระบบของธนาคาร เช่น O365, Facebook รวมถึงบัญชีผู้ใช้ Line ปลอม เพื่อใช้หลอกถามข้อมูลส่วนตัวด้วย [2] ดังตัวอย่างในรูปที่ 3 ซึ่งในปัจจุบันบัญชีของระบบต่าง ๆ อาจจะมีความเชื่อมโยงกัน เช่นใช้อีเมล office จาก O365 ไปสมัครใช้งาน Facebook หรือเครือข่ายสังคมออนไลน์ต่าง ๆ นอกจากนี้ผู้ใช้งานบางคนยังมีการใช้ชื่อบัญชีและรหัสผ่านเดียวกันในทุกระบบอีกด้วย ทำให้เมื่อแฮกเกอร์สามารถขโมยรหัสผ่านของระบบใดระบบหนึ่งได้ก็จะสามารถยึดครองทุกบัญชีผู้ใช้งานของเหยื่อได้ด้วย ดังนั้นผู้ใช้งานควรเพิ่มมาตรการป้องกัน เช่น การใช้ระบบยืนยันตัวด้วยหลายปัจจัย (Multi factors authentication) ใช้รหัสผ่านที่แตกต่างกันในแต่ละบัญชี รวมถึงการไม่ใช้อีเมลขององค์กรไปสมัครใช้งานเครือข่ายสังคมออนไลน์ เป็นต้น

รูปที่ 1 แสดงปริมาณร้อยละการใช้ HTTPS บนเว็บไซต์ฟิชชิงเทียบกับ HTTP ที่ TB-CERT ได้รับแจ้งทั้งหมดในปี 2562



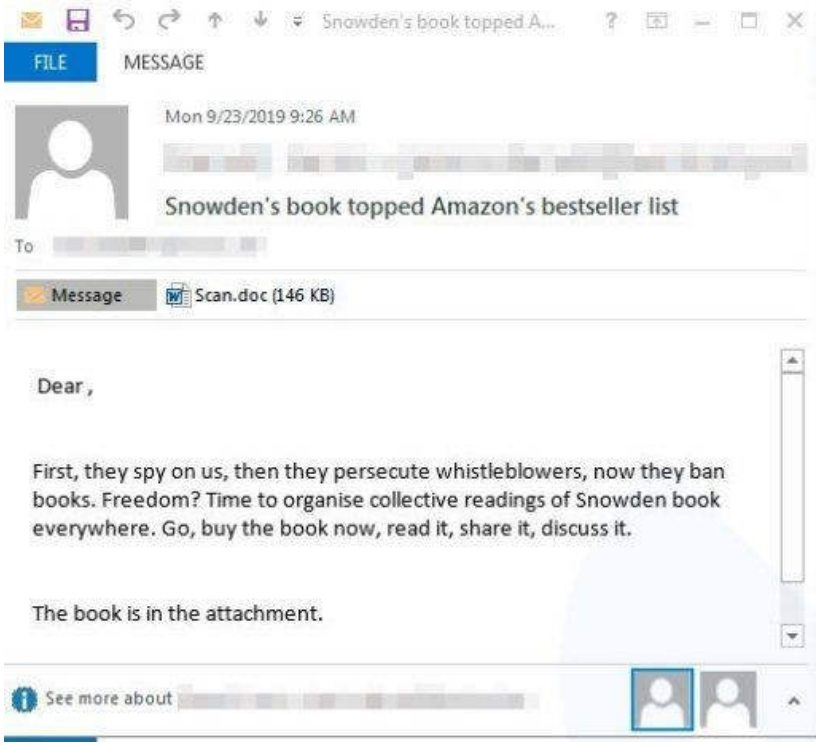
รูปที่ 2 แสดงปริมาณร้อยละของเว็บไซต์ฟิชชิงที่ใช้ HTTPS ทั่วโลก โดย Anti-Phishing Working Group (APWG)



รูปที่ 3 แสดงตัวอย่างฟิชชิงที่หลอกลวงว่าเป็น O365

2. **มัลแวร์ไร้ไฟล์ (Fileless Malware) กลายเป็นเทคนิคหลักที่แฮกเกอร์นิยมใช้** ในปีนี้กลุ่มแฮกเกอร์ส่วนใหญ่มักสร้างมัลแวร์ไร้ไฟล์เพื่อใช้ในการโจมตี ซึ่งสอดคล้องกับการคาดการณ์ในปีที่ผ่านมาของ TB-CERT โดยการเปลี่ยนแปลงที่พบคือมีการเปลี่ยนเทคนิคจาก Script-base (คือใช้ powershell script ฝังในไฟล์) เปลี่ยนมาเป็นใช้เทคนิคฝังในหน่วยความจำโดยตรง หรือ Memory code injection [3] มากขึ้น โดยไม่จำเป็นต้องเขียนไฟล์มัลแวร์ลงในฮาร์ดดิสก์ ส่งผลทำให้โปรแกรมป้องกันมัลแวร์ตรวจจับได้ยากขึ้นกว่าเดิม นอกจากนี้ยังมีการสร้างมัลแวร์ไร้ไฟล์ที่ทำงานบนระบบปฏิบัติการอื่นที่ไม่ใช่ Windows อีกด้วย โดยแฮกเกอร์กลุ่ม Lazarus ได้สร้างมัลแวร์ไร้ไฟล์บนระบบปฏิบัติการ MacOS เพื่อขโมยข้อมูลบนหน่วยความจำ ยังมีการพัฒนา Framework สำหรับสร้างมัลแวร์ไร้ไฟล์บน Linux ชื่อ FireELF [4] และแจกจ่ายอยู่บนอินเทอร์เน็ตด้วย ทำให้มีโอกาสที่แฮกเกอร์จะสามารถสร้างมัลแวร์ไร้ไฟล์บน Linux ได้ง่ายขึ้น อย่างไรก็ตามถึงแม้ว่าจะไม่พบรายงานความเสียหายเกิดขึ้นแต่ก็ต้องให้ความสนใจเพื่อเตรียมการป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นในอนาคตได้

3. **มัลแวร์ที่ผสมผสานความสามารถในการโจมตี** ในปี 2562 มีการค้นพบมัลแวร์ที่มีความสามารถในการโจมตีที่หลากหลาย เห็นได้ชัดเจนจากการกลับมาของมัลแวร์ Emotet [5][6] ในเดือนกันยายน ซึ่งก่อนหน้านี้ Emotet เป็นแบงค์กิ้งโทรจัน แต่ครั้งนี้เพิ่มขีดความสามารถของตัวเองให้มีความสามารถทั้งการเป็นโทรจัน และบ็อตเน็ต นอกจากนี้ในบางสายพันธุ์ยังเป็นมัลแวร์เรียกค่าไถ่ (Ransomware) อีกด้วย โดย Emotet จะใช้เทคนิคการแพร่กระจายตัวผ่านทางอีเมล ซึ่งอาจจะส่งเป็นไฟล์แนบ หรือลิงก์ให้ดาวน์โหลดได้ จากตัวอย่างของ Emotet ในปี 2562 นี้ เป็นแคมเปญหลอกลวงว่ามีการแจกหนังสือ “Permanent Record” ที่ถูกสั่งห้ามขาย ของ Edward Snowden อดีตที่ปรึกษาทางเทคนิคให้กับสำนักงานความมั่นคงแห่งชาติของสหรัฐ (NSA-National Security Agency) เมื่อเหยื่อหลงเชื่อดาวน์โหลดและเปิดไฟล์แนบแล้ว มัลแวร์จะทำการขโมยข้อมูลการล็อกอินใช้งานอีเมลและส่งอีเมลต่อไปตามรายชื่อผู้ติดต่อที่พบในเครื่องอีกด้วย นอกจากนี้จากสถิติของเว็บไซต์ที่ให้บริการวิเคราะห์พฤติกรรมมัลแวร์ (Sandbox) ชื่อ ANY.RUN พบว่า Emotet ยังเป็นมัลแวร์ที่พบมากที่สุดในรอบปี 2562 [7] อีกด้วย ดังรูปที่ 5



รูปที่ 4 ตัวอย่างอีเมลที่แนบไฟล์มัลแวร์ Emotet [6]

รูปที่ 5 สถิติแสดงจำนวน sample ที่ถูกวิเคราะห์ใน Any.run ซึ่งเป็น sandbox ที่ใช้วิเคราะห์พฤติกรรมของมัลแวร์

4. **ข้อมูลรั่วไหลจากคลาวด์และฐานข้อมูล** ในปี 2562 ที่ผ่านมาข้อมูลส่วนบุคคลเป็นเป้าหมายของแฮกเกอร์ ยิ่งในปีนี้มีการประกาศใช้งาน GDPR-General Data Protection Regulation และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 ยิ่งทำให้ประเด็นนี้ยิ่งน่าสนใจมากยิ่งขึ้น ถึงแม้ว่าข้อมูลส่วนบุคคลนั้นไม่ได้รั่วไหลจากสถาบันการเงิน แต่ข้อมูลดังกล่าวสามารถถูกนำมาใช้ในการแอบอ้างเพื่อการฉ้อโกงสถาบันการเงินได้ จากข่าวเหตุการณ์การโจมตีเพื่อขโมยข้อมูลจากหน่วยงานต่าง ๆ นั้น พบว่ามีเหตุการณ์การขโมยข้อมูลที่ใช้บริการคลาวด์ เช่น S3 bucket เป็นต้น อีกทั้งฐานข้อมูลที่อนุญาตให้เข้าถึงจากสาธารณะ เช่น Elasticsearch และ MongoDB เป็นต้น ซึ่งสาเหตุหลักนั้นมาจากผู้ดูแลระบบปรับแต่งค่า configuration ไม่ดีเพียงพอ ทำให้บุคคลภายนอกสามารถเข้าถึงได้โดยไม่ต้องได้รับอนุญาต อีกทั้งไม่ได้ใช้การเข้ารหัสข้อมูลในการจัดเก็บ ทำให้เมื่อมีผู้ไม่หวังดีขโมยข้อมูลออกไปได้ก็สามารถเห็นข้อมูลได้ทั้งหมด ดังนั้นการปรับแต่ง ตรวจสอบ configuration สำหรับควบคุมการเข้าถึงระบบฐานข้อมูล ไม่ว่าจะเป็นระบบที่อยู่ในดาต้าเซ็นเตอร์หรือระบบคลาวด์และการอัพเดตซอฟต์แวร์ที่ใช้ต่าง ๆ จะช่วยลดความเสี่ยงจากการถูกขโมยข้อมูลได้อย่างมีประสิทธิภาพ

5. **การขโมยข้อมูลไบโอเมทริกซ์ (Biometrics)** ในปี 2562 มีเหตุการณ์ที่น่าสนใจเกี่ยวข้องกับการขโมยข้อมูลไบโอเมทริกซ์ ได้แก่ ข้อมูลลายนิ้วมือ และข้อมูลระบบจดจำใบหน้าของผู้ใช้จำนวน 27.8 ล้านรายการ ซึ่งถูกใช้สำหรับควบคุมการเข้าออกอาคารของบริษัท Suprema นอกจากนี้ยังมีเหตุการณ์ที่มีแฮกเกอร์พยายามขโมยข้อมูลของลูกค้าบริษัท Veritas Genetics ซึ่งเป็นผู้ให้บริการทดสอบ DNA อย่างไรก็ตามทางบริษัทได้มาประกาศแล้วว่าข้อมูลที่รั่วไหลนั้น ไม่มีข้อมูลที่ sensitive เช่น ชื่อ นามสกุล หรือ รหัสพันธุกรรม (DNA) เป็นต้น ยิ่งไปกว่านั้นมีการนำเอาข้อมูลไบโอเมทริกซ์มาใช้เพื่อการยืนยันตัวตนเพิ่มมากขึ้นอย่างมาก ดังนั้นหน่วยงานที่จะเก็บข้อมูลไบโอเมทริกซ์จะต้องใช้ความระมัดระวังให้มาก เนื่องจากว่าข้อมูลเหล่านี้เป็นข้อมูลที่ Sensitive อีกทั้งเจ้าของข้อมูลไม่สามารถเปลี่ยนข้อมูลนี้ได้อีกด้วย

เทคนิคของกลุ่มแฮกเกอร์สถาบันการเงินที่น่าสนใจ

1. **Lazarus**

กลุ่มแฮกเกอร์สัญชาติเกาหลีเหนือ Lazarus เป็นกลุ่มแฮกเกอร์ที่พุ่งเป้าโจมตีสถาบันการเงินในหลายประเทศ ในปีนี้แฮกเกอร์กลุ่มนี้ได้สร้างมัลแวร์ประเภทไร้ไฟล์ (Fileless Malware) สายพันธุ์ใหม่ที่มีผลกระทบบนระบบปฏิบัติการ MacOS ซึ่งทำงานอยู่ในหน่วยความจำ และไม่ต้องติดตั้งลงฮาร์ดดิสก์ ทำให้สามารถหลบเลี่ยงการตรวจจับของโปรแกรมป้องกันมัลแวร์ได้ โดยมีจุดประสงค์ในการขโมยข้อมูลที่อยู่ในหน่วยความจำ นอกจากนี้ยังมีการสร้างมัลแวร์ที่มุ่งขโมยเงินจากตู้ ATM โดยการนำโทรจัน DTrack มาผสมผสาน ซึ่งมัลแวร์ DTrack จัดอยู่ในประเภทโทรจันที่ถูกควบคุมได้จากระยะไกล (Remote Access Trojan – RAT) ที่มีความสามารถในการเรียกดูข้อมูลที่อยู่ในหน่วยความจำ (Memory Dump) ได้ ซึ่งมัลแวร์ ATMDTrack นั้นจึงมีความสามารถอ่านและเก็บข้อมูลในบัตรที่ใช้บริการจากตู้ที่ถูกมัลแวร์ดังกล่าวคุกคามได้

2. **TA505**

กลุ่มแฮกเกอร์ TA505 เป็นกลุ่มแฮกเกอร์ที่พุ่งเป้าโจมตีสถาบันการเงินในหลายประเทศ เช่น สหราชอาณาจักร ฝรั่งเศส ญี่ปุ่น อินเดีย ฟิลิปปินส์ และอาร์เจนตินา เป็นต้น อย่างไรก็ตามประเทศไทยเองก็ตกเป็นเป้าหมายด้วยเช่นกัน แต่ได้รับผลกระทบน้อยมาก ในปี 2562 นี้แฮกเกอร์กลุ่มนี้สร้างมัลแวร์หลากหลายสายพันธุ์ โดยส่วนใหญ่จะมีลักษณะคล้ายกันคือส่งอีเมลพร้อมไฟล์แนบที่มีนามสกุล .xls เมื่อเหยื่อหลงเชื่อเปิดไฟล์ xls ดังกล่าว มัลแวร์จะดาวน์โหลดไฟล์มัลแวร์ที่จะทำอันตรายผ่านลิงค์บน Dropbox และการสร้าง Tunnel ผ่านทางโพรโตคอล Remote Desktop เป็นต้น โดยมีวัตถุประสงค์เพื่อฝังตัว ขโมยข้อมูลสำคัญ และควบคุมเครื่องคอมพิวเตอร์ที่ถูกมัลแวร์คุกคามจากระยะไกลได้

3. **Cobalt**

กลุ่มแฮกเกอร์ Cobalt ในปีนี้มีเทคนิคที่น่าสนใจคือการอาศัยการหลอกลวงโดยใช้ไฟล์ PDF แล้ว Redirect ไปยัง Google App Engine ผ่านทางโพรโตคอล HTTPS ทำให้เหยื่อเข้าใจว่ากำลังเข้าถึงข้อมูลจาก Google จริง ๆ จากนั้นจะดาวน์โหลดไฟล์ Word ที่ฝังมาโครเพื่อจะโจมตีต่อไป นอกจากนี้แฮกเกอร์กลุ่มนี้ยังได้สร้างมัลแวร์เรียกค่าไถ่ชื่อ PureLocker ที่มีจุดเด่นด้านความสามารถในการเข้ารหัสไฟล์และทำงานได้บนทุกระบบปฏิบัติการหลัก ได้แก่ Windows, Linux, และ MacOS

4. Fancy Bear

ในปีนี้แฮกเกอร์สัญชาติรัสเซียอย่าง Fancy Bear (APT28) ส่งอีเมลข่มขู่เพื่อเรียกค่าไถ่จากหน่วยงานในสถาบันการเงิน หน่วยงานราชการ และกลาโหม เป็นต้น ซึ่งเหตุการณ์นี้เกิดขึ้นในหลายประเทศ อย่างไรก็ตามยังไม่พบอีเมลข่มขู่ในประเทศไทย เทคนิคที่แฮกเกอร์กลุ่มนี้ใช้โจมตีเป็นลักษณะการทำ DDoS โดยโจมตีผ่านโพรโตคอลต่าง ๆ ได้แก่ DNS NTP และ CLDAP รวมไปถึงโพรโตคอล WS Discovery (UDP/3702 multicast address 239.255.255.250) และ ARMS-Apple Remote Management Service (UDP/3283) ด้วย ซึ่งโพรโตคอล WS Discovery (UDP/3702 multicast address 239.255.255.250) เคยพบการเพิ่มปริมาณทราฟฟิกได้ถึง 15,300%

5. Silence

กลุ่มแฮกเกอร์ Silence กลุ่มแฮกเกอร์สัญชาติรัสเซีย และมีเป้าหมายโจมตีสถาบันการเงินในรัสเซียเป็นหลัก ในปีนี้ได้ใช้เทคนิคการส่งอีเมลฟิชชิงและหลอกว่าเป็นอีเมลตอบกลับอัตโนมัติ เพื่อรวบรวมบัญชีอีเมลที่ยังมีการใช้งานอยู่ อีกทั้งยังเป็นการยืนยันอีเมลของเหยื่อด้วย ซึ่งจากรายงานพบว่ามีการส่งอีเมลถึง 170,000 ฉบับ ทั้งในทวีปยุโรป เอเชีย และประเทศในกลุ่มสหภาพโซเวียต ในจำนวนนี้ส่งมายังทวีปเอเชียถึง 80,000 ฉบับใน 12 ประเทศ ซึ่ง TB-CERT ไม่ได้รับรายงานผลกระทบดังกล่าวของกลุ่มการเงินในประเทศไทย เมื่อมัลแวร์ดังกล่าวสามารถคุกคามเครื่องคอมพิวเตอร์ในสถาบันการเงินได้แล้วจะพยายาม Lateral movement ไปยังเครื่องคอมพิวเตอร์ที่ประมวลผลข้อมูลบัตร อีกทั้งยังพยายามควบคุม ATM โดยไม่จำเป็นต้องติดตั้งมัลแวร์ในตู้ ATM เพื่อที่จะขโมยเงินอีกด้วย

6. FIN7

กลุ่มแฮกเกอร์ FIN7 สัญชาติรัสเซีย ที่มีเป้าหมายหลักในการโจมตีสถาบันการเงินในยุโรปและสหรัฐอเมริกา แม้ประเทศไทยจะไม่ใช่เป้าหมาย แต่ในปีนี้ก็มีเทคนิคของมัลแวร์ที่น่าสนใจ คือมัลแวร์ BOOSTWRITE เป็น dropper ที่ทำงานในหน่วยความจำเท่านั้น (หรือเป็นมัลแวร์ประเภทไร้ไฟล์) และสามารถถอดรหัส payload ที่ฝังตัวมาด้วยกุญแจที่ได้รับจากเซิร์ฟเวอร์ นอกจากนี้ยังมี RDFSNIFFER ซึ่งเป็น payload ของมัลแวร์นี้ จะถูกโหลดเข้ากับโพรเซสเดียวกันกับโพรเซสของ NCR Aloha Command ซึ่งเป็นซอฟต์แวร์ที่ใช้บริหารจัดการและแก้ไขปัญหาของการประมวลผลการชำระเงินผ่านบัตร ในลักษณะของ DLL เพื่อควบคุมระบบบริหารจัดการดังกล่าว

อ้างอิง

1. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf
2. https://www.cisco.com/c/dam/en/us/products/collateral/security/2019-threats-of-the-year-cybersecurity-series-dec-2019.pdf
3. https://resources.infosecinstitute.com/malware-spotlight-fileless-malware/
4. https://kalilinuxtutorials.com/fireelf/
5. https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-exploring-emotet-elaborate-everyday-enigma/
6. https://fossbytes.com/top-malware-2019/
7. https://any.run/malware-trends/emotet
8. https://www.globenewswire.com/news-release/2019/11/12/1945147/0/en/October-2019-s-Most-Wanted-Malware-the-Decline-of-Cryptominers-Continues-as-Emotet-Botnet-Expands-Rapidly.html
9. https://securelist.com/biometric-data-processing-and-storage-system-threats/95364/
10. https://www.pcsecurity-99.com/2019/12/07/infamous-lazarus-apt-hackers-group-attack-mac-computers-with-fileless-malware/
11. https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf
12. https://securelist.com/kaspersky-security-bulletin-2019-statistics/95475/

คาดการณ์แนวโน้มการโจมตีในปี 2563

จากการรวบรวมข้อมูลเหตุการณ์ที่เกิดขึ้นในปีที่ผ่านมาประกอบกับการวิเคราะห์สถานการณ์และแนวโน้มจากรายงานหลายแหล่ง TB-CERT จึงได้ทำการคาดการณ์แนวโน้มรูปแบบการโจมตีทางไซเบอร์สำหรับปี 2563 นี้ ดังนี้

- **การขโมยข้อมูลบัตรที่ใช้ชำระเงินผ่านช่องทางอิเล็กทรอนิกส์ (e-skimming)** การซื้อขายของออนไลน์เป็นที่นิยมอย่างมากในปัจจุบัน และนับวันยิ่งจะมีปริมาณการใช้บริการซื้อขายของออนไลน์มากขึ้น ทำให้แฮกเกอร์นั้นพยายามที่จะขโมยข้อมูลบัตรที่ใช้ชำระเงิน ไม่ว่าจะเป็นบัตรเครดิตและบัตรเดบิตหรือบัตรในรูปแบบอื่น ๆ ที่ต่างพัฒนาให้มีความสะดวกในการใช้งานมากขึ้น โดยการฝังมัลแวร์ไว้ที่เครื่องคอมพิวเตอร์ที่ทำหน้าที่ Point of Sale (POS) หรือระบบคอมพิวเตอร์ของร้านค้าที่ให้บริการขายของออนไลน์ เพื่อที่จะดักขโมยข้อมูลบัตรของผู้ถือบัตร ที่ชำระเงินผ่านเครื่อง POS หรือ ผ่านเว็บไซต์ e-commerce ที่แฮกเกอร์เจาะระบบแล้วฝังมัลแวร์ไว้ได้ ดังนั้นเจ้าของร้านค้าที่ใช้งาน POS และเจ้าของเว็บไซต์ e-commerce ต่าง ๆ ต้องระมัดระวัง ตรวจสอบความปลอดภัยของระบบอย่างสม่ำเสมอ จึงมีความพยายามที่จะผลักดันมาตรฐาน PCI DSS หรือ Payment Card Industry Data Security Standard มาอย่างต่อเนื่องเพื่อให้เกิดแนวปฏิบัติที่ให้องค์กร ผู้ให้บริการ และ ร้านค้ามีการดูแลป้องกัน การบริหารจัดการความมั่นคงปลอดภัยข้อมูลของลูกค้าที่มีประสิทธิภาพมากขึ้น

- **ระบบปฏิบัติการ MacOS, Linux และ Unix เป็นเป้าหมายมากขึ้น** จากเดิมที่กลุ่มแฮกเกอร์ต่าง ๆ มักจะอาศัยช่องโหว่บนระบบปฏิบัติการ Windows และซอฟต์แวร์ต่าง ๆ ดังนั้นผู้ดูแลระบบจึงให้ความสนใจกับเครื่องที่ติดตั้งระบบปฏิบัติการ Windows มากกว่า แต่มีงานวิจัยของผู้ผลิตโปรแกรมป้องกันไวรัสบางแห่งรายงานว่า ในปี 2562 พบว่ามีมัลแวร์ที่แพร่กระจายตัวบนระบบปฏิบัติการ MacOS เพิ่มมากขึ้น อีกทั้งเมื่อปลายปี 2562 กลุ่มแฮกเกอร์เกาหลีเหนืออย่าง Lazarus ก็ได้สร้างมัลแวร์ที่แพร่กระจายบนระบบปฏิบัติการ MacOS ด้วย ดังนั้นในองค์กรที่มีการใช้งานระบบปฏิบัติการอื่นที่นอกเหนือจาก Windows แล้วต้องให้ความสำคัญในการรักษาความปลอดภัยมากขึ้น

- **การแฮกระบบ IoT – Internet of Things** ปัจจุบันเทคโนโลยีที่เกี่ยวข้องกับ IoT ได้พัฒนาไปอย่างมาก อีกทั้งราคาก็ลดลง ทำให้เครื่องใช้ไฟฟ้า อุปกรณ์อำนวยความสะดวก อุปกรณ์เพื่อสุขภาพติดตามตัว รวมถึงของเล่น ส่วนใหญ่มักจะเริ่มเชื่อมต่อสู่อินเทอร์เน็ตได้แล้ว อย่างเช่นกล้องวงจรปิด สมาร์ททีวี เครื่องซักผ้า อุปกรณ์ช่วยเหลืออัจฉริยะในบ้าน เป็นต้น จึงเป็นแรงจูงใจที่ทำให้แฮกเกอร์พยายามโจมตีอุปกรณ์เหล่านี้ที่ไม่ได้รับการป้องกันอย่างดีเพียงพอ ซึ่งผลกระทบที่อาจจะพบได้อย่างเช่นการเผยแพร่ข้อมูลส่วนตัว เช่นภาพจากกล้องวงจรปิดในบ้าน หรือแม้กระทั่งการข่มขู่กรรโชกเพื่อเรียกร้องเงินและทรัพย์สินของเหยื่อ ดังนั้นการใช้เทคโนโลยี IoT จึงควรคำนึงถึงความปลอดภัยและความเป็นส่วนตัวของผู้ใช้งานด้วย รวมถึงการศึกษาคุณสมบัติของอุปกรณ์ที่เลือกใช้ด้วย

- **มัลแวร์เรียกค่าไถ่ (Ransomware) จะผสมผสานการเผยแพร่ข้อมูลที่อ่อนไหว (Extortion) ด้วย** มัลแวร์เรียกค่าไถ่ที่ผ่านมาจะเข้ารหัสข้อมูลไฟล์สำคัญขององค์กร แต่องค์กรส่วนใหญ่ที่ถูกมัลแวร์เรียกค่าไถ่คุกคามนี้มักจะไม่จ่ายเงินค่าไถ่ ดังนั้นแฮกเกอร์จะหาวิธีในการข่มขู่ที่รุนแรงขึ้น เช่น การข่มขู่ว่าจะทำลายข้อมูลที่อ่อนไหว เปิดเผยข้อมูลที่อ่อนไหวขององค์กรสู่สาธารณะ การนำไปขายในตลาดมืด รวมไปถึงการแจ้งไปยังหน่วยงานกำกับขององค์กรนั้น ๆ ได้

- **การใช้คลาวด์สาธารณะ (Public Cloud) ในการโจมตีมากขึ้น** ความสะดวกสบายในการใช้บริการ คลาวด์สาธารณะต่าง ๆ ด้วยเหตุผลด้านความประหยัด ความรวดเร็ว และประสิทธิภาพในการใช้งาน ทำให้แฮกเกอร์ส่วนใหญ่มักจะเลือกลงทุนใช้คลาวด์สาธารณะเป็นฐานในการโจมตี ไม่เพียงเท่านี้องค์กรส่วนใหญ่ไม่สามารถปิดกั้นการเข้าถึงคลาวด์สาธารณะเหล่านี้ด้วย เนื่องจากจะกระทบการใช้งานของผู้ใช้ในองค์กรได้ ตัวอย่างเช่น แฮกเกอร์เปิดเว็บไซต์ฟิชชิงบนผู้ให้บริการคลาวด์สาธารณะ ถ้าผู้ดูแลระบบขององค์กรปิดกั้นการเข้าถึง แฮกเกอร์ก็จะเปลี่ยนแปลงค่าหมายเลขไอพีได้ใหม่ได้อย่างง่ายดาย ทำให้ผู้ดูแลระบบขององค์กรปิดกั้นการเข้าถึงได้ลำบากมากยิ่งขึ้น

- **ข้อมูลรั่วไหลบนเว็บ Repository ต่าง ๆ** เว็บ Repository เป็นเว็บที่มีไว้สำหรับเก็บข้อมูลควบคุมเวอร์ชันและแชร์โค้ดที่พัฒนาขึ้น เช่น Github และ Pastebin เป็นต้น เพื่อเพิ่มประสิทธิภาพในการทำงานร่วมกันของนักพัฒนาซอฟต์แวร์ต่าง ๆ อย่างไรก็ตามแฮกเกอร์เองก็มักจะอาศัยเว็บเหล่านี้ในการแจกจ่ายโค้ดในการเจาะระบบ หรือแม้แต่การแชร์ข้อมูลความลับต่าง ๆ ที่ขโมยมาได้เผยแพร่บนเว็บเหล่านั้นได้ ข้อมูลรั่วไหลที่มักพบได้บ่อยบนเว็บ Repository ได้แก่ ชื่อบัญชีผู้ใช้ รหัสผ่าน รวมถึงเลขที่บัตรเครดิต เป็นต้น ดังนั้นการเฝ้าระวังข้อมูลรั่วไหลจึงควรค้นหาข้อมูลจากเว็บเหล่านี้ด้วย

อ้างอิง

1. https://www.rsa.com/content/dam/en/e-book/20-predictions-for-2020.pdf
2. https://documents.trendmicro.com/assets/rpt/rpt-the-new-norm-trend-micro-security-predictions-for-2020.pdf
3. https://hello.global.ntt/en-us/insights/future-disrupted-2020-technology-trends
4. https://securityintelligence.com/posts/ibm-x-force-security-predictions-for-2020/
5. https://www.technologyrecord.com/Article/which-technologies-could-change-enterprise-it-in-2020-101253
6. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
7. https://www.crowdstrike.com/blog/4-cyber-threat-predictions-for-2020/
8. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/11/20151759/KSB2019_APT-predictions-2020_web.pdf
9. https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/top-9-cybersecurity-trends-for-2020.pdf
10. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-2020-threats-predictions-report/
11. https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/
12. https://ww2.frost.com/news/press-releases/artificial-intelligence-seen-as-key-technology-game-changer-but-implementation-challenges-remain-finds-frost-sullivan/

บทสรุป

การเตรียมความพร้อมในการรับมือภัยคุกคามไซเบอร์ จำเป็นต้องมีการพัฒนาบุคลากร กระบวนการรับมือ และการพัฒนามาตรฐานความมั่นคงปลอดภัยอย่างต่อเนื่อง เพื่อให้เกิดการสร้างวัฒนธรรมองค์กรให้มีความเข้าใจในเรื่อง Cyber Resilience และเกิดผลอย่างยั่งยืนในยุคดิจิทัล TB-CERT เล็งเห็นว่าการพัฒนาทักษะความรู้พื้นฐานให้กับหน่วยงานสมาชิกโดยผ่านกิจกรรมการจัดฝึกอบรมทั้งภาคทฤษฎีและปฏิบัติอย่างต่อเนื่องจะเพิ่มความรู้ความเชี่ยวชาญให้กับบุคลากรที่เกี่ยวข้องให้สามารถรับมือภัยไซเบอร์ได้อย่างทันท่วงที และเป็นมาตรฐานเดียวกันทั้งอุตสาหกรรม การซักซ้อมกระบวนการรับมือภัยคุกคามอย่างสม่ำเสมอหรือที่เราเรียกกันว่า Banking Cyber Drill ประจำปีนั้นช่วยให้หน่วยงานสมาชิกได้ฝึกทดสอบประสิทธิภาพของกระบวนการรับมือภัยคุกคามของตนในสถานการณ์ต่าง ๆ นอกจากนั้นการร่วมฝึกซ้อมของสมาชิกในกลุ่มการเงินก็ถือเป็นการซักซ้อมความเข้าใจของหน่วยงานทั้งอุตสาหกรรม จะช่วยให้หน่วยงานสมาชิกที่อาจจะยังไม่มีกระบวนการชัดเจน สามารถนำผลการฝึกซ้อมไปปรับใช้ได้อย่างมีประสิทธิภาพมากขึ้น และเป็นโอกาสที่ดีที่ทุกหน่วยงานจะได้แลกเปลี่ยนเรียนรู้จากประสบการณ์จากสมาชิกอื่น ๆ อันจะเป็นกระบวนการเรียนรู้แบบอัตราเร่ง โดย cTB-CERT ได้มีบทบาทในการส่งเสริมการพัฒนากระบวนการแลกเปลี่ยนข้อมูลเหตุการณ์การโจมตีในรูปแบบต่าง ๆ ของแฮกเกอร์ ระหว่างหน่วยงานสมาชิกด้วยกัน ให้ทุก ๆ หน่วยงานได้รับข้อมูลเดียวกันอย่างรวดเร็ว ทันต่อเหตุการณ์ เพื่อเป็นการป้องกันภัยที่อาจจะเกิดขึ้นกับหน่วยงานใดหน่วยงานหนึ่งในภาคอุตสาหกรรมได้ทันที ทั้งยังมีการแลกเปลี่ยนข้อมูลจากหน่วยงาน CERT ทั้งในและนอกประเทศภายใต้พันธะสัญญาแลกเปลี่ยนข้อมูลซึ่งเป็นแหล่งข้อมูลที่น่าเชื่อถือได้อีกแหล่งหนึ่งให้กับหน่วยงานสมาชิก

นอกจากการผลักดันให้องค์กรมีความเข้าใจและทักษะในการรับมือกับภัยไซเบอร์อย่างยืดหยุ่นแล้วนั้น TB-CERT ยังเน้นการพัฒนามาตรฐานด้าน cyber security ร่วมกันซึ่งจะช่วยให้สมาชิกและหน่วยงานกำกับดูแลมีความเข้าใจบนพื้นฐานเดียวกัน และเป็นส่วนหนึ่งของการทำให้ภาคอุตสาหกรรมธนาคารมีความเข้มแข็งขึ้นอย่างยั่งยืน พร้อมที่จะยกระดับให้เป็น resilience industry ได้อย่างมั่นคง

TB-CERT
Thailand Banking Sector CERT

Thailand Banking Sector CERT: TB-CERT

ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร

สมาคมธนาคารไทย

สำนักงานระบบการชำระเงิน
Payment System Office (PSO)

THE THAI BANKERS' ASSOCIATION
4th Floor, 5/13 Moo 3, Chaengwattana Rd.
Khlong-Kluea, Pakkret
Nonthaburi 11120
Tel: +66 2558 7500
www.tba.or.th