

depa



# การใช้งานเทคโนโลยี Cyber Security

ในอุตสาหกรรม การเงินการธนาคาร

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล



# ขอบเขตการศึกษา

กลุ่มประเทศที่ศึกษา: กลุ่มประเทศอาเซียน ซึ่งประกอบด้วยประเทศไทย อินโดนีเซีย มาเลเซีย ฟิลิปปินส์ สิงคโปร์ และเวียดนาม

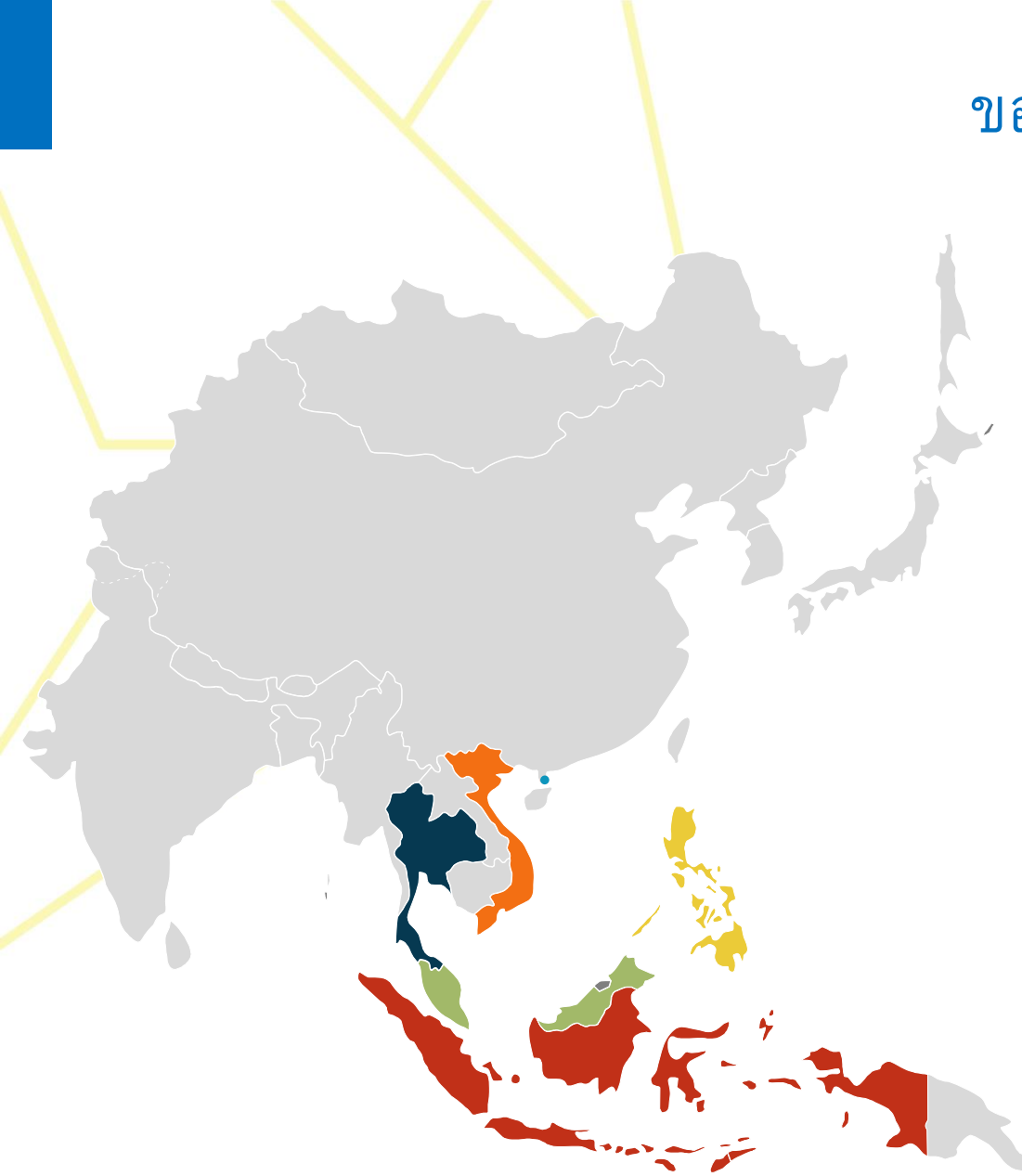
ประเทศที่ใช้ในการเปรียบเทียบ: ฮังการ

กลุ่มอุตสาหกรรมที่ศึกษา: อุตสาหกรรมการเงินการธนาคาร

กลุ่มอุตสาหกรรม	ตัวอย่างบริษัท	SIC Codes
การธนาคาร	Citigroup, Bank of America, Wells Fargo, Americorp, American Express, Bank of New York	6011, 6019, 6021, 6022, 6029, 6035, 6036, 6061, 6062, 6081, 6082, 6091, 6099, 6111, 6141, 6153, 6159, 6162, 6163
การประกัน และการลงทุน	American International Group, UnitedHealth Group, WellPoint, Allstate Corp., ALFAC, Marsh & McLennan Companies Inc., American International Group, UnitedHealth Group, WellPoint, Allstate Corp., ALFAC, Marsh & McLennan Companies Inc.	6311, 6321, 6324, 6331, 6351, 6361, 6371, 6399, 6411, 6211, 6221, 6231, 6282, 6289, 6712, 6719, 6722, 6726, 6732, 6733, 6792, 6794, 6798, 6799

เทคโนโลยีเกิดใหม่ที่ศึกษา: การรักษาความมั่นคงปลอดภัยทางไซเบอร์ยุคใหม่

คือระบบรักษาความปลอดภัยทางไซเบอร์ที่มีการนำดาต้าและเครื่องมือการวิเคราะห์ดาต้าเข้ามาใช้ ประกอบการวิเคราะห์ภัยคุกคาม เพื่อปกป้องระบบและข้อมูลที่อยู่ในดาต้าเซ็นเตอร์ อุปกรณ์เอ็นดีพอยต์ และข้อมูลที่อยู่ระหว่างการส่ง



# ระบบนิเวศน์ของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ยุคใหม่ (Cyber Security)

## ฮาร์ดแวร์รักษาความมั่นคง ปลอดภัยทางไซเบอร์

- Firewall / VPN
- IDS / IPS
- UTM
- Messaging Security Appliances
- Web Security Appliances
- WAM



## ซอฟต์แวร์รักษาความมั่นคง ปลอดภัยทางไซเบอร์

- Identity and Access Management Software
- Endpoint Security Software
- Messaging Security Software
- Web Security Software
- Network Security Software
- Security and Vulnerability Management Software



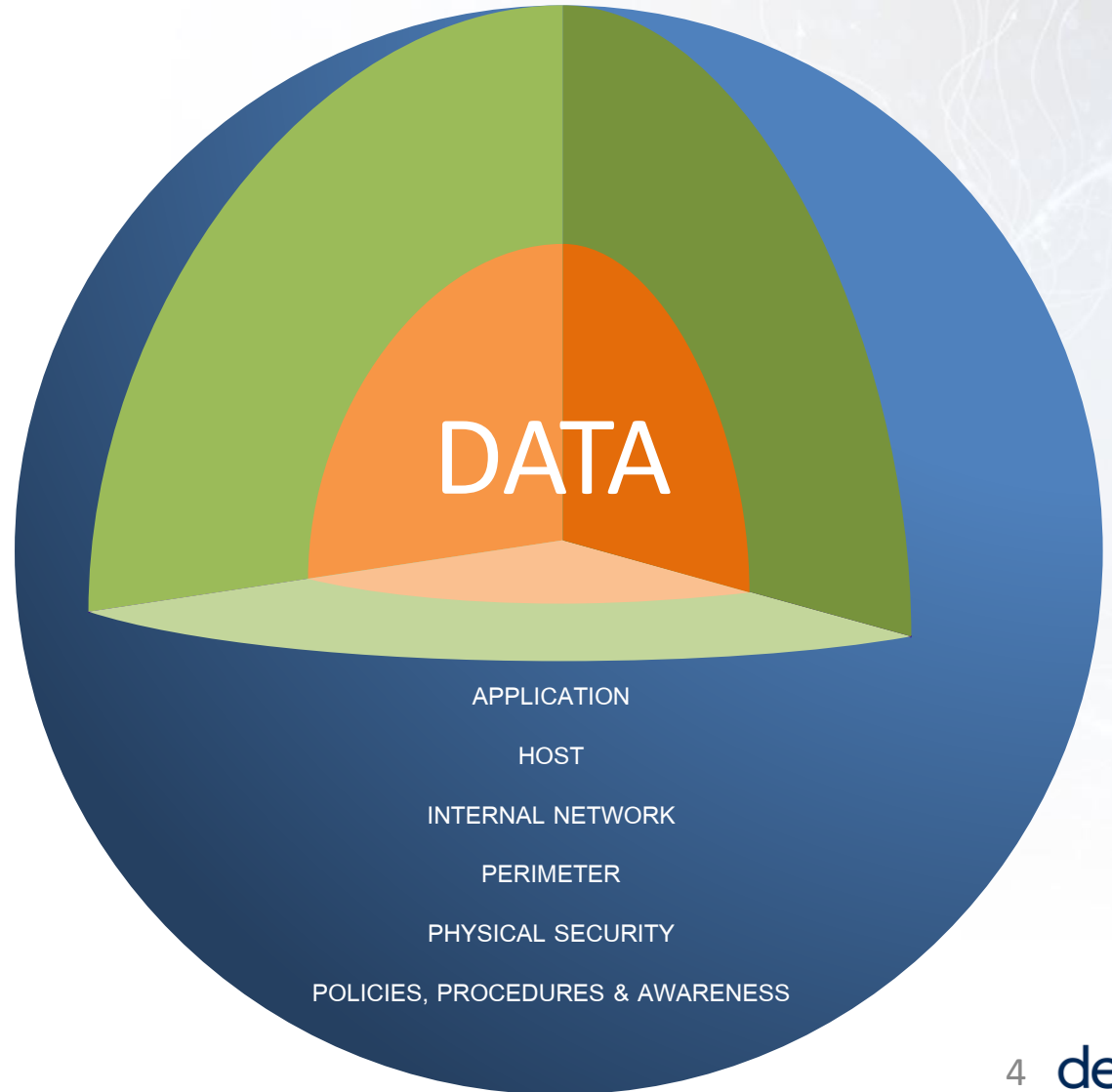
## บริการรักษาความมั่นคง ปลอดภัยทางไซเบอร์

- Security Consulting Services
- System Installation Services
- System Operation and Management Services
- Security Education and Training Services



## การป้องกันเชิงลึก

วางมาตรการรับมือการโจมตีทางไซเบอร์ ที่อยู่บนสมมติฐานที่ว่าระบบจะต้องถูกเจาะอย่างแน่นอน และวางมาตรการในการทำให้การเจาะทะลุข้างจนกระทั่งถึงจุดที่จัดการได้ในที่สุด





# ภาพรวมของอุตสาหกรรมการเงินการธนาคาร

## ไทย

การเติบโตของอุตสาหกรรมค้าปลีกของไทยมีส่วนกระตุ้นให้เกิดการพัฒนาในอุตสาหกรรมการเงิน ในแง่มุมมองที่เกี่ยวกับการชำระเงิน การรักษาสถานลูกค้า และการเพิ่มประสบการณ์การใช้งานให้ลูกค้า

โดยผู้ประกอบการในอุตสาหกรรมการเงินของไทยกำลังให้ความสนใจกับการเพิ่มช่องทางชำระเงิน กระเป๋าเงินอิเล็กทรอนิกส์ และโมบายล์แบงก์กิ้ง

กำแพงกฎระเบียบที่จำกัดการใช้งานเทคโนโลยีสารสนเทศในประเทศไทยที่น้อยกว่าประเทศอาเซียนอื่น ๆ ช่วยให้ผู้ประกอบการสามารถสร้างสรรค์นวัตกรรมได้โดยง่าย



## อินโดนีเซีย

ผู้ประกอบการในอินโดนีเซียกำลังเตรียมความพร้อมเพื่อรองรับนโยบายการค้าที่เปิดกว้างขึ้นของประเทศ และเม็ดเงินลงทุนที่ไหลเข้า/ออกมากขึ้นในขนาดอันใกล้

การเปิดเสรีทางการเงินการธนาคารมากขึ้นทำให้นักลงทุนจากต่างชาติเข้ามาลงทุนในอุตสาหกรรมการเงินการธนาคารมากขึ้นตามไปด้วย

นั่นทำให้ผู้ประกอบการเริ่มสามารถนำนวัตกรรมมาใช้และใช้ประโยชน์จากการเติบโตของ FinTech มากขึ้น



## มาเลเซีย

มาเลเซียถือเป็นบ้านของ super-regional bank ของอาเซียน และผู้ประกอบการเหล่านี้ยังคงขยายกิจการในภูมิภาคอย่างต่อเนื่อง

การแข่งขันกับคู่แข่งในประเทศอื่น และการให้บริการลูกค้าในประเทศอื่น ทำให้ผู้ประกอบการต้องมีความคล่องตัวสูง

จึงมีการลงทุนเพื่อทำดิจิทัลทรานส์ฟอร์มชันอย่างต่อเนื่อง นำไปสู่การพัฒนาช่องทางในการทำธุรกรรม การใช้ไอทีประกอบการตัดสินใจ และการสร้างผลิตภัณฑ์ทางการเงินและพันธมิตรใหม่ ๆ ได้



## สิงคโปร์

สิงคโปร์กำลังแข่งขันกับฮ่องกงเพื่อเป็นศูนย์กลางทางการเงินของเอเชีย ทำให้รัฐบาลและธนาคารกลางพยายามสร้างบรรยากาศที่เอื้อต่อการลงทุนในอุตสาหกรรมการเงินการธนาคารของประเทศให้ได้มากที่สุด

นั่นทำให้ผู้ประกอบการสามารถผลักดันการสร้างนวัตกรรมได้โดยง่าย โดยเน้นไปที่ช่องทางชำระเงินแบบดิจิทัล การยืนยันตัวตนด้วยข้อมูลชีวภาพ บล็อกเชน คลาวด์ บิ๊กดาต้า อนุโมเลกุล และระบบคอมพิวเตอร์เสมือนมนุษย์



## ฟิลิปปินส์

กฎข้อบังคับที่มักได้รับการผ่อนผันของฟิลิปปินส์เป็นหนึ่งในปัจจัยที่เอื้อให้ผู้ประกอบการสามารถพิจารณาหา นวัตกรรมใหม่ ๆ มาใช้ได้ เช่น FinTech Sandbox

ผู้ประกอบการในฟิลิปปินส์กำลังให้ความสนใจกับการเพิ่มอัตราการชำระเงินแบบอิเล็กทรอนิกส์มากขึ้นเรื่อย ๆ และได้ร่วมมือเป็นพันธมิตรกับช่องทางค้าปลีกมากขึ้น

และกำลังทำการลงทุนเพื่อปรับปรุงโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศเพื่อรองรับนวัตกรรมต่าง ๆ ต่อไป



## เวียดนาม

ทิศทางของอุตสาหกรรมการเงินการธนาคารของเวียดนามยังคงไม่ชัดเจน ผู้ประกอบการบางรายมีการพัฒนาด้านดิจิทัลอย่างก้าวกระโดด ในขณะที่บางราย (รัฐวิสาหกิจ) ยังตามหลังอยู่ค่อนข้างมาก และมีการควบรวมกิจการที่สำคัญเกิดขึ้นบ่อยครั้ง

แต่กระนั้น ตั้งแต่พ.ศ. 2559 เป็นต้นมา เวียดนามเริ่มดึงดูดเม็ดเงินลงทุนมากขึ้น โดยเฉพาะอย่างยิ่งเมื่อระบบนิเวศของ FinTech เริ่มพัฒนามากขึ้น และเริ่มมีนักลงทุนจากนิวซีแลนด์เข้ามาลงทุนอย่างจริงจังมากขึ้น เพื่อใช้เวียดนามเป็นฐานในการขยายกิจการไปยังประเทศอาเซียนต่อไป



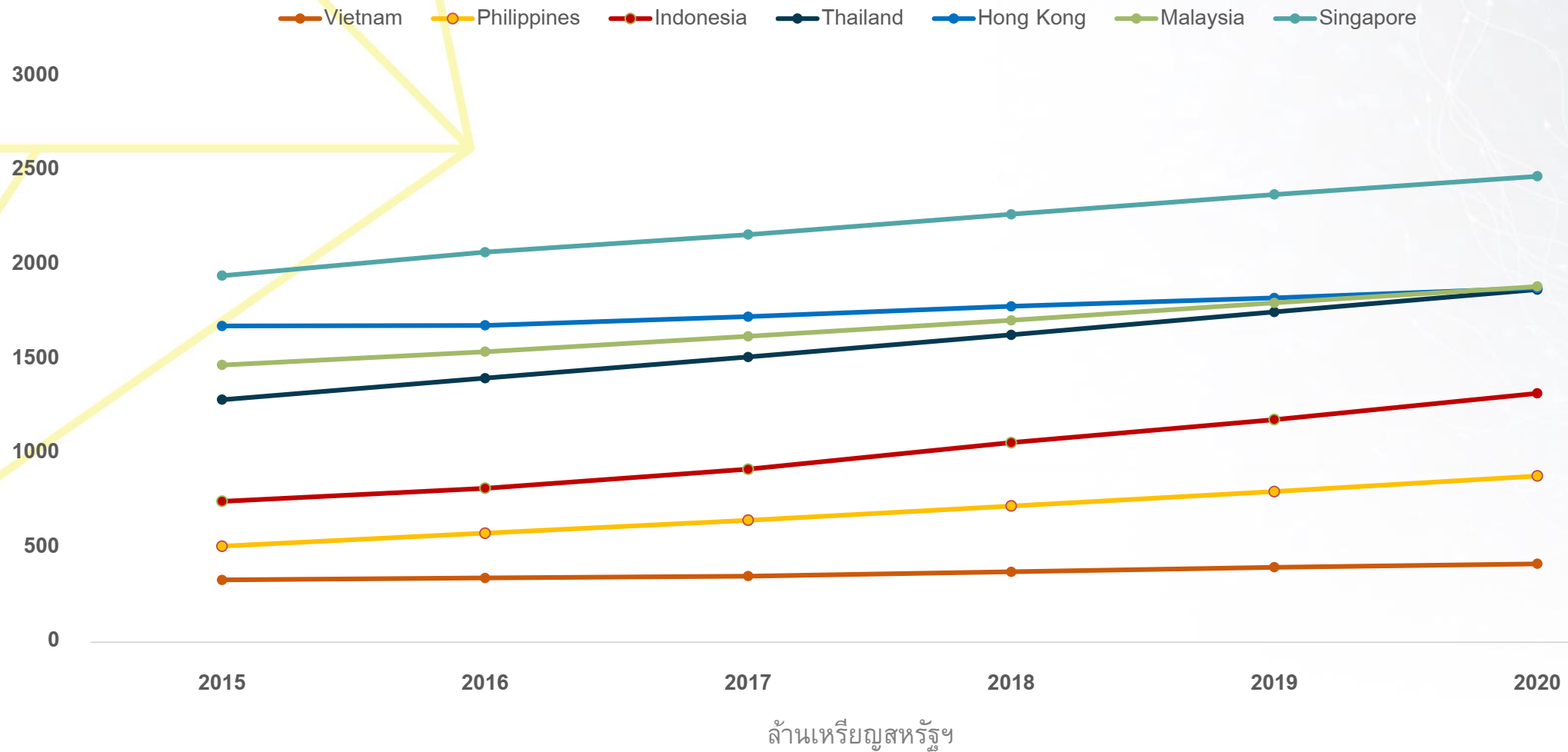
## ฮ่องกง

ผู้ประกอบการในฮ่องกงกำลังเร่งลดต้นทุน เพิ่มประสิทธิภาพ และสร้างสรรค์ผลิตภัณฑ์ทางการเงินใหม่ ๆ เพื่อกระตุ้นธุรกิจหลังจากที่อุปสงค์จากจีนแผ่นดินใหญ่เริ่มเติบโตช้าลง แต่กระนั้น กฎข้อบังคับที่ยังไม่ชัดเจนมากนักของหน่วยงานกำกับดูแล และการมีโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ค่อนข้างเก่าของผู้ประกอบการรายหลาย โดยเฉพาะผู้ประกอบการขนาดกลาง (ฮ่องกงมีสถาบันการเงินที่รับเงินฝาก 196 แห่ง) ทำให้การทำดิจิทัลทรานส์ฟอร์มเมชันเป็นไปได้ไม่ใช่ง่ายนัก





# การลงทุนในเทคโนโลยีสารสนเทศของผู้ประกอบการในภาคอุตสาหกรรมการเงิน



# ปัจจัยการขับเคลื่อนการลงทุนในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ยุคใหม่



## ไทย

- โมบายล์เฟิร์ส ผู้ประกอบการทั้งการเงินการธนาคารและประกัน ได้ใช้เทคโนโลยีโมบายล์ได้อย่างเข้มข้น ทั้งเป็นช่องทางในการทำธุรกรรม และเป็นเครื่องมือการทำงานของพนักงาน
- การปรับปรุงดาต้าเซ็นเตอร์ ผู้ประกอบการทั้งในอุตสาหกรรมการเงินและอุตสาหกรรมเทคโนโลยีสารสนเทศและโทรคมนาคม ต่างก็เพิ่มการลงทุนในการสร้างคลาวด์ดาต้าเซ็นเตอร์ ซึ่งจะทำให้เกิดการใช้บริการคลาวด์มากขึ้น



## อินโดนีเซีย

- การปรับปรุงดาต้าเซ็นเตอร์ ผู้ประกอบการทั้งในอุตสาหกรรมการเงินและอุตสาหกรรมโทรคมนาคม ต่างก็เพิ่มการลงทุนในการสร้างคลาวด์ดาต้าเซ็นเตอร์ ซึ่งจะทำให้เกิดการใช้บริการคลาวด์มากขึ้น
- กลุ่มลูกค้าใหม่และผลิตภัณฑ์ใหม่ ผู้ประกอบการกำลังเพิ่มจำนวนตู้ ATM เพื่อรองรับลูกค้าใหม่ และใช้ดาต้าในการช่วยปรับปรุงผลิตภัณฑ์ทางการเงินเพื่อตอบสนองต่ออุปสงค์ของลูกค้าเดิมให้ดีขึ้น



## มาเลเซีย

- การลดต้นทุน ผู้ประกอบการที่เป็น regional bank กำลังทำการลดต้นทุนผ่านการทำระบบอัตโนมัติและลดจำนวนพนักงานลง
- การเติบโตของ FinTech ทำให้ผู้ประกอบการร่วมเป็นพันธมิตรหรือซื้อกิจการสตาร์ทอัพมากขึ้น และนำนวัตกรรมมาใช้มากขึ้น
- การชำระเงินผ่านช่องทางดิจิทัล ซึ่งผู้ประกอบการจะต้องหาวิธีรับมือกับการรักษาความปลอดภัยของดาต้าต่าง ๆ



## สิงคโปร์

- ออมนิแชแนล ผู้ประกอบการสิงคโปร์เพิ่มช่องทางในการทำธุรกรรมกับลูกค้าที่หลากหลายมากขึ้น ซึ่งเชื่อมต่อแบบออฟไลน์และออนไลน์เข้าด้วยกัน
- ระบบบริการลูกค้าอัจฉริยะ โดยใช้เทคโนโลยีคอมพิวเตอร์เสมือนมนุษย์มาใช้ปฏิสัมพันธ์กับลูกค้า
- อาชญากรรมไซเบอร์ ผู้ประกอบการหลายรายได้เพิ่มการลงทุนเพื่อรับมือกับการโจมตีแบบ zero-day โดยการนำเทคโนโลยีเอนาไลติกส์เข้ามาช่วย



## ฟิลิปปินส์

- การชำระเงินผ่านช่องทางดิจิทัล ซึ่งผู้ประกอบการจะต้องหาวิธีรับมือกับการรักษาความปลอดภัยของดาต้าต่าง ๆ
- การควบรวมกิจการ ธนาคารกลางส่งเสริมให้ธนาคารใหญ่ซื้อกิจการธนาคารขนาดเล็กหรือธนาคารชนบท ซึ่งมักมีระบบไอทีที่ไม่ปลอดภัยพอ
- ความเสี่ยงที่เพิ่มขึ้น จากปริมาณอาชญากรรมไซเบอร์ที่เพิ่มขึ้น โดยเฉพาะอย่างยิ่งเมื่อธนาคารใหญ่อย่าง BDO โคนโจมตีเมื่อไม่นานมานี้



## เวียดนาม

- การใช้ดิจิทัลเป็นเครื่องมือในการปฏิบัติตามข้อบังคับ ธนาคารส่วนใหญ่ของเวียดนามเพิ่งผ่านหลักเกณฑ์ Basel II เท่านั้น และต้องใช้เทคโนโลยีในการเพิ่มความโปร่งใสและบริหารความเสี่ยง
- การชำระเงินผ่านช่องทางดิจิทัล ผู้ประกอบการในเวียดนามเริ่มหารายได้จากค่าทำเนียมมากขึ้น และส่งเสริมการชำระเงินผ่านสมาร์ตโฟนมากขึ้น ซึ่งต้องหาวิธีรับมือกับการรักษาความปลอดภัยของดาต้าต่าง ๆ ด้วย
- การควบรวมกิจการ ธนาคารของรัฐได้รับคำสั่งให้ซื้อกิจการธนาคารขนาดเล็กหรือธนาคารชนบท ซึ่งมักมีระบบไอทีที่ไม่ปลอดภัยพอ



## ฮ่องกง

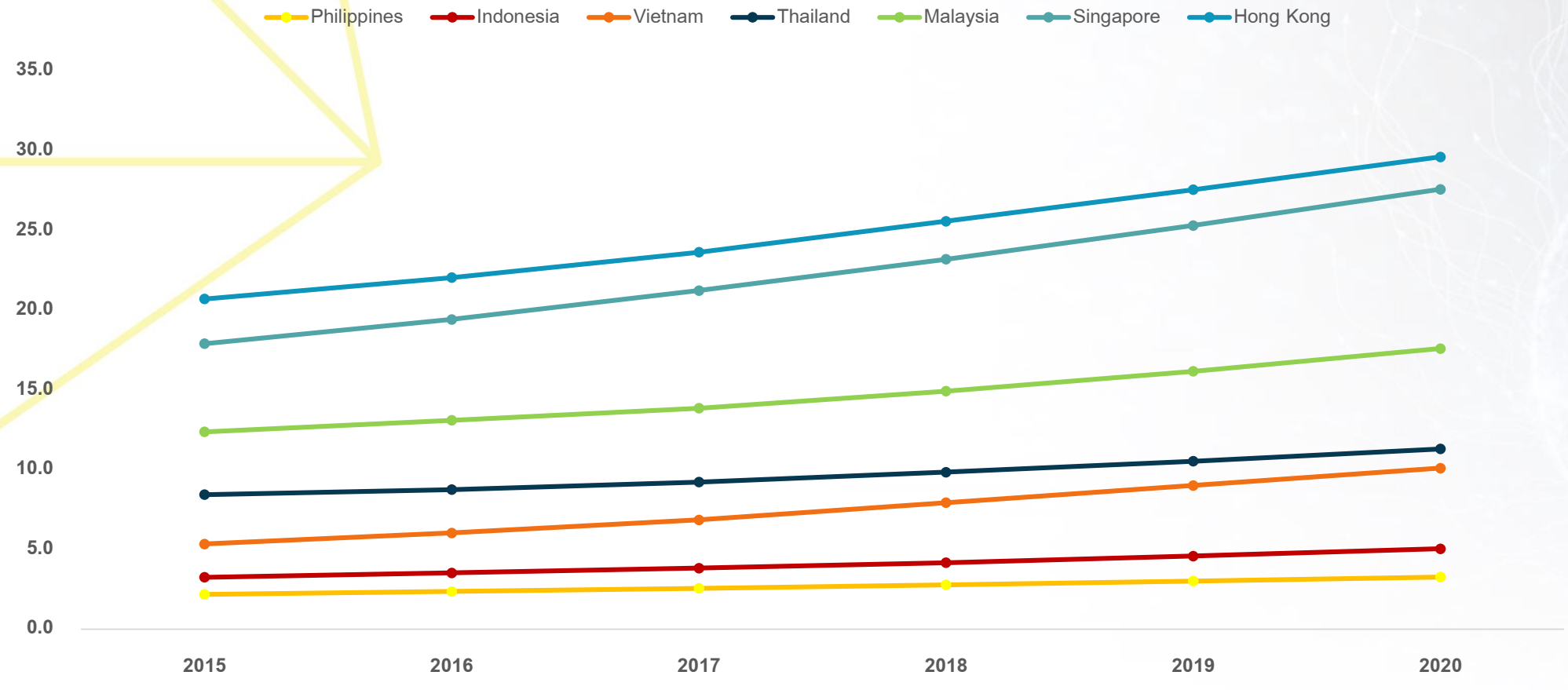
- อาชญากรรมไซเบอร์ ในช่วง 18 เดือนที่ผ่านมาทำให้ธนาคารกลางต้องเพิ่มความเข้มงวดของกฎข้อบังคับด้านไซเบอร์ซีเคียวริตี้ โดยเฉพาะเมื่อตรวจเจอช่องโหว่ของระบบ SWIFT
- ความสามารถด้านบิ๊กดาต้าออนไลน์ ผู้ประกอบการในฮ่องกงกำลังลงทุนพัฒนาขีดความสามารถด้านออนไลน์เพื่อไล่ตามสิงคโปร์และออสเตรเลีย ซึ่งออนไลน์ิกส์มีบทบาทสำคัญในระบบรักษาความปลอดภัยทางไซเบอร์ยุคใหม่
- การเพิ่มช่องทางดิจิทัล การที่ผู้ประกอบการในฮ่องกงมุ่งความสนใจไปที่การเพิ่มช่องทางดิจิทัลสำหรับการทำธุรกรรม ทำให้ต้องการระบับรักษาความปลอดภัยที่ครอบคลุมและมีประสิทธิภาพขึ้น



# การลงทุนในเทคโนโลยีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)



## ของผู้ประกอบการในอุตสาหกรรมการเงินการธนาคาร



ล้านเหรียญสหรัฐฯ





# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (1/10)

## HKMA - Cybersecurity Fortification Initiative (2016)



เป็นโครงการสร้างมาตรฐานให้กับทั้งอุตสาหกรรมการเงิน การธนาคารของฮ่องกง ในด้านการวัดประสิทธิภาพของระบบรักษาความปลอดภัยไซเบอร์ของผู้ประกอบการ และสร้างฐานข้อมูลการธุรกิจกลางขึ้นมาใช้งานร่วมกัน โดยแบ่งออกเป็น 3 โครงการย่อย

- **Cyber Resilience Assessment Framework (C-RAF)** ประเมินระดับความเสี่ยงประสิทธิภาพของระบบ และทดสอบผ่านการจำลองการโจมตี
- **Professional Development Programme (PDP)** ฝึกอบรมบุคลากรที่ทำงานด้านการรักษาความปลอดภัยไซเบอร์ โดยผู้เชี่ยวชาญจากหลายหน่วยงาน
- **Cyber Intelligence Sharing Platform (CISP)** เป็นแพลตฟอร์มที่รวบรวมข้อมูลเกี่ยวกับภัยคุกคามและการทุจริตต่าง ๆ ที่ผู้ประกอบการสามารถอัปเดตและอ่านข้อมูลได้

### ประโยชน์ที่ได้รับจากโครงการนี้

- สร้างมาตรฐานการกำกับดูแลด้านการรักษาความปลอดภัยไซเบอร์
- สร้างเครื่องมือในการวัดระดับประสิทธิภาพของระบบรักษาความปลอดภัยไซเบอร์ของผู้ประกอบการ
- เพิ่มความสามารถในการรับมือกับภัยคุกคาม ผ่านข้อมูลบนแพลตฟอร์ม CISP ทำให้ผู้ประกอบการเตรียมตัวรับมือและเรียนรู้จากกันและกันได้



# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (2/10)

## Bank Indonesia และ OJK - Laku Pandai (2014)



เป็นโครงการใช้เทคโนโลยีช่วยในการทำงานร่วมกันของสถาบันการเงินทั้งในระบบและนอกระบบ ในการบริหารจัดการการเงินฝากและเงินกู้ร่วมกัน เป็นการเพิ่มโอกาสให้ประชาชนเข้าถึงบริการทางการเงิน โดยโครงการนี้ไม่ได้เป็นการส่งเสริมการเพิ่มสาขาของผู้ประกอบการ แต่เป็นการแก้ไขนโยบายเดิม สร้างพันธมิตร และนำเทคโนโลยีที่เป็น



มาตรฐานเดียวกันมาใช้งาน ทำให้ประชาชนเปิดบัญชีโดยไม่ต้องมีเงินฝาก จัดการด้านการเงินส่วนตัว สมัครขอเงินกู้หรือสมัครประกันผ่านสมาร์ทโฟน (หรือพีเจอาร์โฟนที่ใช้งาน USSD ได้) ควบคู่ไปกับการสร้างฐานข้อมูลการประเมินความเสี่ยงสินเชื่อของประเทศ และนั่นทำให้ประชาชนสามารถทำธุรกรรมทางการเงินผ่านช่องทางออฟไลน์และออนไลน์ได้ (โดยการยืนยันตัวตนผ่านโทรศัพท์มือถือ) สำหรับช่องการดิจิทัลนั้น ผู้ประกอบการที่เข้าร่วมโครงการได้มีการใช้ระบบรักษาความปลอดภัยไซเบอร์ที่มีมาตรฐานทัดเทียมกัน

### ประโยชน์ที่ได้รับจากโครงการนี้

- สร้างมาตรฐานให้กับกระบวนการตรวจสอบความถูกต้องของบุคคลและป้องกันการฟอกเงิน และการบริการลูกค้าใหม่ ผ่านช่องทางโทรศัพท์มือถือ อีกทั้งยังเป็นการช่วยส่งเสริมการเติบโตของบริการโมบายล์แบงก์กิ้งในอนาคต
- ช่วยให้ประชาชนจำนวนมากโดยเฉพาะในเขตชนบทสามารถเข้าถึงบริการทางการเงินได้มากขึ้น โดยเป็นบริการทางการเงินที่ได้รับการกำกับดูแลโดยรัฐบาล ไม่ใช่บริการนอกระบบ



# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (3/10)

## Bank Indonesia - Financial Identity Number (2015)



เป็นโครงการเพิ่มฐานข้อมูลตัวตนของประชาชนที่ไม่ได้อยู่ในระบบธนาคารมาก่อน โดยมีการสร้าง ID ที่ผูกกับหมายเลขประจำตัวประชาชนของผู้ใช้แต่ละราย เพื่อให้เป็นเครื่องยืนยันตัวตนในการทำธุรกรรมทางการเงิน ร่วมกับการผูกกับหมายเลขโทรศัพท์มือถือเพื่อความปลอดภัย

โดยสถาบันการเงินสามารถเข้าถึงฐานข้อมูลนี้ได้ ทำให้ไม่จำเป็นต้องทำการตรวจสอบความถูกต้องของบุคคลโดยใช้เอกสารอีกต่อไป

### ประโยชน์ที่ได้รับจากโครงการนี้

- การใช้เทคโนโลยีที่รองรับการยืนยันตัวตนแบบ 2 Factor Authentication (คือ ID และหมายเลขโทรศัพท์) ทำให้ผู้ใช้งานสามารถยืนยันตัวตนผ่านโทรศัพท์มือถือได้
- ธนาคารทราบถึงประวัติการทำธุรกรรมทางการเงินและสถานะของสินทรัพย์ต่าง ๆ ของประชาชนแต่ละคนได้ เป็นการลดความเสี่ยงและลดส่วนชดเชยความเสี่ยง (risk premium) ได้ และทำให้ธนาคารสามารถตัดสินใจอนุมัติเงินกู้ได้โดยที่มีข้อมูลมากเพียงพอ



# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (4/10)

## Bank Mandiri - Rekening Hape (2015)



เป็นโครงการที่ช่วยให้ผู้ที่ไม่มียุทธินาคารสามารถใช้หมายเลขโทรศัพท์เป็นบัญชีอิเล็กทรอนิกส์ได้ โดยใช้ SMS ในการชำระบิลและการโอนเงิน ผ่านความร่วมมือกับผู้ให้บริการโทรคมนาคมไร้สายทั้ง Telekom Indonesia, Telkomsel, Indosat และ XL Axiata

โดย Rekening Hape คือการนำโทรศัพท์มาใช้งานแทนบัตร ATM และใช้หมายเลขโทรศัพท์เป็นหนึ่งในชุดข้อมูลยืนยันตัวตน ผ่านเทคโนโลยี 2 Factor Authentication ซึ่งสามารถใช้งานกับโทรศัพท์ทุกรุ่นที่มีเทคโนโลยี USSD ไม่ว่าจะเป็นสมาร์ทโฟนหรือฟีเจอร์โฟนก็ตาม ซึ่งผู้ใช้งานสามารถ

- ส่งโอนเงินผ่าน SMS ไปยังผู้รับที่มีเลขบัญชีธนาคารหรือหมายเลขโทรศัพท์
- ตรวจสอบประวัติการทำธุรกรรม
- เติมเงินเข้าบัญชี eWallet
- ถอนเงินโดยไม่ใช้บัตร

## ประโยชน์ที่ได้รับจากโครงการนี้

- โครงการนี้เป็นตัวอย่างที่ดีของการผสมผสานระหว่างระบบที่มีความปลอดภัยและรองรับการใช้งานจริงได้
- ใช้ประโยชน์จากโครงสร้างพื้นฐานเดิมและอุปกรณ์ที่ผู้ใช้งานใช้อย่างแพร่หลาย ในการสร้างระบบชำระเงินทางเลือกที่มีความปลอดภัย



# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (5/10)

## Alliance Bank – Cash2Home (2017)



เป็นโมบายล์แอปพลิเคชันที่ช่วยให้บริษัทต่าง ๆ สามารถจ่ายเงินเดือนให้กับลูกจ้างต่างชาติที่ไม่มีบัญชีธนาคารได้ โดยผู้ใช้งานไม่จำเป็นต้องมายื่นเอกสารยืนยันตัวตนที่สาขาของธนาคาร เพราะธนาคารจะส่งพนักงานไปที่บริษัทต่าง ๆ เพื่อช่วยในการเก็บรวบรวมเอกสารเหล่านั้น

ระบบรักษาความปลอดภัยของแอปพลิเคชันใช้ประโยชน์จากเทคโนโลยี biometrics ในการล็อกอินเข้าใช้งาน โดยแทนที่จะใช้ลายนิ้วมือ ธนาคารเลือกใช้เทคโนโลยีจดจำใบหน้าและเสียงแทน ซึ่งมีประสิทธิภาพมากกว่า โดยระบบจะยอมให้เข้าใช้งานผ่านเสียงก็ต่อเมื่อเอกลักษณ์ของเสียงของผู้ใช้ไม่ตรงกับที่บันทึกไว้ 100% เท่านั้น เพราะการทำให้เสียงตรงกัน 100% นั้นเป็นไปได้นอกเสียจากว่าอัดเสียงไว้เพื่อทำการทุจริตฉ้อโกง

### ประโยชน์ที่ได้รับจากโครงการนี้

- การใช้ข้อมูล biometrics และหมายเลขโทรศัพท์มาประกอบรวมกันในกระบวนการ 2 Factor Authentication มีความปลอดภัยและใช้งานง่ายกว่าแบบดั้งเดิม



# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (6/10)

## Maybank – Maybank2U Pay (2017)



เป็นการเปิด API เพื่อเชื่อมต่อเข้ากับระบบต่าง ๆ ของพาร์ทเนอร์ โดยแพลตฟอร์ม Maybank2U ช่วยให้ร้านค้าผู้จำหน่ายสินค้าสามารถพัฒนาและอินทิเกรตแอปพลิเคชันที่ใช้งานหน้าร้านเข้ากับบัญชีธนาคารของบริษัท เพื่อให้การชำระเงินมีความปลอดภัยมากขึ้น

และยังม API อื่นๆ รองรับบริการอินทิเกรตเข้ากับระบบการจัดการกระแสเงินสด การชำระเงินซัพพลายเออร์ และระบบจ่ายเงินเดือนของบริษัทด้วย

### ประโยชน์ที่ได้รับจากโครงการนี้

- สามารถสร้างแพลตฟอร์มการเชื่อมต่อกับระบบภายนอกที่มีความปลอดภัยสูงได้
- ช่วยขยายธุรกิจของ Maybank และสร้างผลประโยชน์ที่วัดปริมาณได้โดยวัดจำนวนของร้านค้าและผู้ประกอบการที่เข้าร่วม



# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (7/10)

## รัฐบาลสิงคโปร์ – MyInfo (2016)



เป็นครั้งแรกในเอเชียที่รัฐบาลมีนโยบายในการสร้างฐานข้อมูลยืนยันตัวตนของประชาชน โดยเป็นการดึงข้อมูล (ที่ได้รับคามยินยอม) ของประชาชนทุกคนจากหลายหน่วยงานรัฐเข้ามาเป็นรวมกัน เพื่อสร้างเป็น profile ของประชาชนแต่ละคน โดยประชาชนสามารถใช้

profile เหล่านี้ในการสมัครบริการ eService แทนที่จะต้องกรอกใบสมัคร ซึ่งธนาคารใหญ่ ๆ อย่าง OCBC, UOB, DBS และ Standard Chartered ต่างก็ใช้ข้อมูลยืนยันตัวตนจากแพลตฟอร์มนี้ทั้งนั้น ทั้งข้อมูลเครดิต การชำระภาษี การจ้างงาน รายได้ และข้อมูลทางการเงินอื่น ๆ

### ประโยชน์ที่ได้รับจากโครงการนี้

- สร้างมุมมองแบบ Single-citizen view ในฐานข้อมูลที่มีการรักษาความปลอดภัยอย่างแน่นหนา เพื่อช่วยในการกรอกแบบฟอร์มโดยอัตโนมัติได้
- การที่ฐานข้อมูลนี้มีระบบควบคุมการเข้าถึงตาต้า จะช่วยในการตรวจสอบความโปร่งใสได้



# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (8/10)

## กระทรวงไอซีทีสิงคโปร์ และ Cyber Security Agency (CSA) – กฎหมายความปลอดภัยไซเบอร์ (2017)



เพื่อรับมือกับปริมาณ Advanced Persistent Threat ที่เพิ่มขึ้น ทั้ง 2 หน่วยงานได้เสนอกฎหมายที่เพิ่มมาตรการรักษาความปลอดภัยให้กับโครงสร้างพื้นฐานด้านไอทีที่สำคัญของประเทศ เพื่อลดความเสี่ยงและเพิ่มความสามารถของผู้ประกอบการในการรับมือกับการโจมตี โดยมีสาระสำคัญดังนี้

- สร้างกรอบการทำงานที่ชัดเจนให้กับบริษัทเจ้าของโครงสร้างพื้นฐานไอทีที่สำคัญ ในป้องกันโครงสร้างพื้นฐานนั้น
- ให้อำนาจหน่วยงาน CSA ในการจัดการและโต้ตอบต่อภัยคุกคาม
- สร้างกรอบการทำงานสำหรับการแบ่งปันข้อมูลสำคัญด้านการรักษาความปลอดภัยไซเบอร์ กับเจ้าหน้าที่และโดยเจ้าหน้าที่ CSA
- การสร้างกรอบการทำงานในการมอบใบอนุญาตให้กับผู้ให้บริการศูนย์รักษาความปลอดภัยไซเบอร์ (SOC)

### ประโยชน์ที่ได้รับจากโครงการนี้

- ทำให้ทั่วทั้งอุตสาหกรรมได้รับข้อมูลการโจมตีในรูปแบบต่าง ๆ แบบเรียลไทม์ และเป็นการสร้างระบบแจ้งเตือนล่วงหน้าด้วยความร่วมมือจากผู้ประกอบการ





# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (9/10)

## OCBC – BCSIS Blockchain Platform (2016)



เป็นธนาคารแรกในอาเซียนที่ธนาคารนำเทคโนโลยีบล็อกเชนมาใช้ในบริการชำระเงินและโอนเงินในประเทศและข้ามประเทศ เพื่อเพิ่มประสิทธิภาพและประสบการณ์การใช้งานของลูกค้า เพิ่มความปลอดภัย ความโปร่งใส และลดต้นทุน

โดย OCBC มีแผนที่จะนำเทคโนโลยีนี้ไปใช้กับผลิตภัณฑ์ทางการเงินอื่น ๆ ด้วย เช่น smart contract

### ประโยชน์ที่ได้รับจากโครงการนี้

- เพิ่มความปลอดภัย เพราะข้อมูลธุรกรรมถูกบันทึกลงใน ledger ที่ถูกเข้ารหัสขั้นสูง และไม่สามารถแก้ไขเปลี่ยนแปลงได้
- เพิ่มประสิทธิภาพ เพราะไม่ต้องผ่าน gateway ที่เป็นตัวกลาง ทำให้ธนาคารผู้รับสามารถรับเงินจากธนาคารผู้ส่งได้โดยตรง ก่อนหน้านี้ OCBC ใช้เวลา 1 วันในการจัดการการโอนเงินระหว่างสิงคโปร์และมาเลเซีย แต่บล็อกเชนสามารถทำงานแบบเดียวกันได้ในเวลา 5 นาที
- ลดต้นทุน เพราะไม่จำเป็นต้องจ่ายค่าธรรมเนียมให้กับบริษัทที่ต้องเข้ามาเป็นตัวกลางในการกำกับดูแลการทำธุรกรรมอีกต่อไป อีกทั้งธุรกรรมยังมีความโปร่งใสนิ่งอีกด้วย



# ตัวอย่างการใช้งานและประโยชน์ที่ได้รับ (10/10)

## Citibank – Citi Developer Hub (2016)



เปิดให้พาร์ทเนอร์สามารถอ่านรายละเอียด ลงทะเบียนเข้าใช้ ลงทะเบียนแอปพลิเคชันใหม่ และเชื่อมต่อเข้ากับ API Sandbox ที่มีชุด API มากกว่า 50 ชุด ของ Citibank ได้ ซึ่งเป็นการเพิ่มความเร็วและความปลอดภัยให้การสร้างและนำนวัตกรรมมาใช้งาน

### ประโยชน์ที่ได้รับจากโครงการนี้

- สร้างแพลตฟอร์มที่สามารถควบคุมการทำงานที่เกี่ยวข้องทั้งหมดได้ และมีความปลอดภัยสูง
- ลดระยะเวลาการพัฒนาและติดตั้งแอปพลิเคชันที่พัฒนาร่วมกับพาร์ทเนอร์หรือจากผู้รับจ้างพัฒนาได้ 50%
- การใช้ Sandbox ทำให้สามารถพัฒนาแอปพลิเคชันในรูปแบบของการ fail fast ได้



**สำนักงานส่งเสริมเศรษฐกิจดิจิทัล**  
**Digital Economy Promotion Agency**

The Government Complex, Ratthaprasasanabhakti Building, 9<sup>th</sup> Floor,  
120 Chaengwattana Road, Thungsonghong, Laksi, Bangkok 10210, Thailand.



[www.depa.or.th](http://www.depa.or.th)



DEPA Thailand



Call 02-1417101