DIGITAL TRANSFORMATION, PDPA, &CYBERSECURITY

ดร.อรรถศิษฐ์ พัฒนะศิริ
ผศ.ดร.มยุรี ศรีกุลวงศ์
ดร. ชนะกัญจน์ ศรีรัตนบัลล์

August 08, 2024

ดร.อรรถศิษฐ์ พัฒนะศิริ

รองผู้อำนวยการ สำนักคอมพิวเตอร์
และ อาจารย์ประจำวิทยาลัยนวัตกรรมสื่อสารสังคม
มหาวิทยาลัยศรีนครินทรวิโรฒ

ผู้เชี่ยวชาญเฉพาะเรื่องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 บริษัทที่ปรึกษาชั้นนำ [Personal Data Protection Act (PDPA) Subject Matter Expert]

ที่ปรึกษาด้านการขับเคลื่อนเปลี่ยนแปลงสู่ดิจิทัล (Digital Transformation) กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ กระทรวงอุตสาหกรรม

ที่ปรึกษาคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) [Bangkok Dusit Medical Services (BDMS)]

B.Sc.(Computer Science), Thammasat University
M.Sc.(Computer Science), Chulalongkorn University
Ph.D.(Management of Technology), AIT

Agenda

- Digital Transformation
- PDPA
- Cybersecurity

1. DIGITAL TRANSFORMATION

100%
โลกขับเคลื่อนเปลี่ยนแปลงสู่ดิจิทัล

duval union consulting

WAVES OF DISRUPTION

1995+

Music
Photography
Video Rental
...

2010+

Print Media
TV
Travel
HR
...

2015+

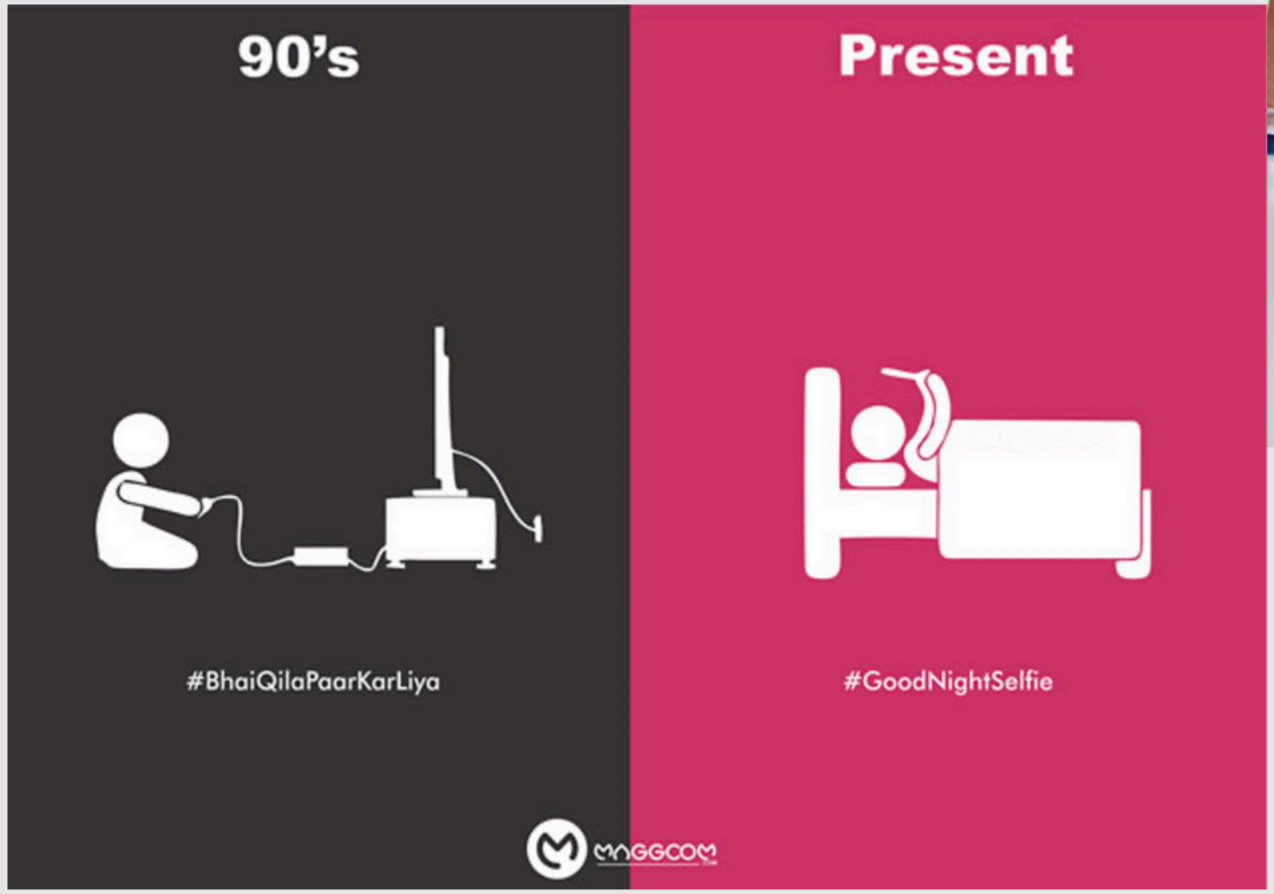
Retail
Healthcare
Automotive
Education
Telco
Food
FMCG
Banking/Insurance
...

2020

All Safe havens will be subject to digital disruption
...

ทำไมการเปลี่ยนแปลงสู่ดิจิทัลจึงสำคัญ

- Next Normal
- Next Era
- ชีวิตเปลี่ยนแปลงไปทุกด้าน
- DISRUPTIONs



PRICING TRENDS 2024

01 INCREASED USE OF AI AND MACHINE LEARNING

02 INVESTING IN PRICING COMPETENCE

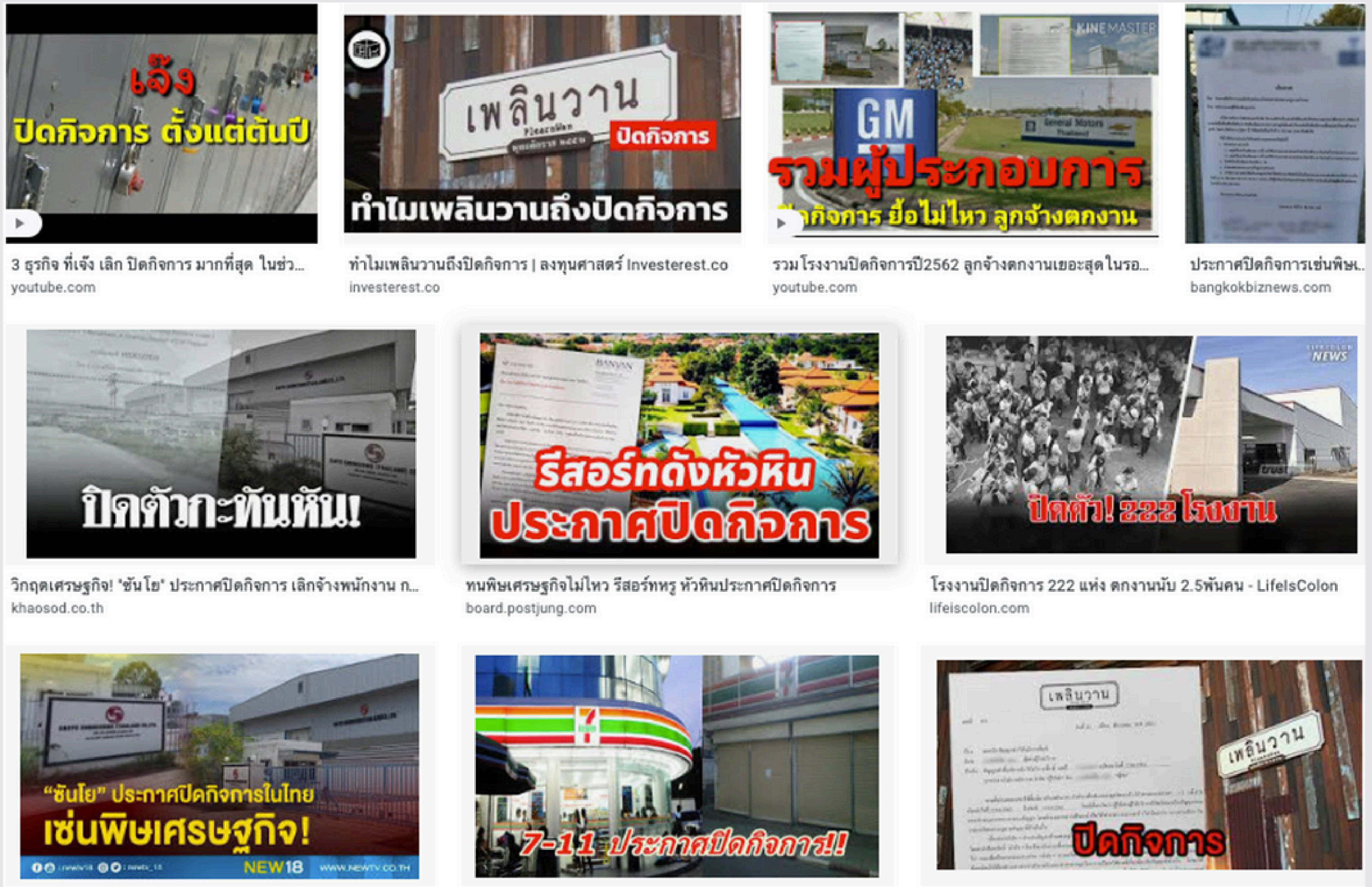
03 SUPPLY AND DEMAND MANAGEMENT

04 PROACTIVE PRICE ADJUSTMENTS

05 DISCOUNT DEPENDENCY

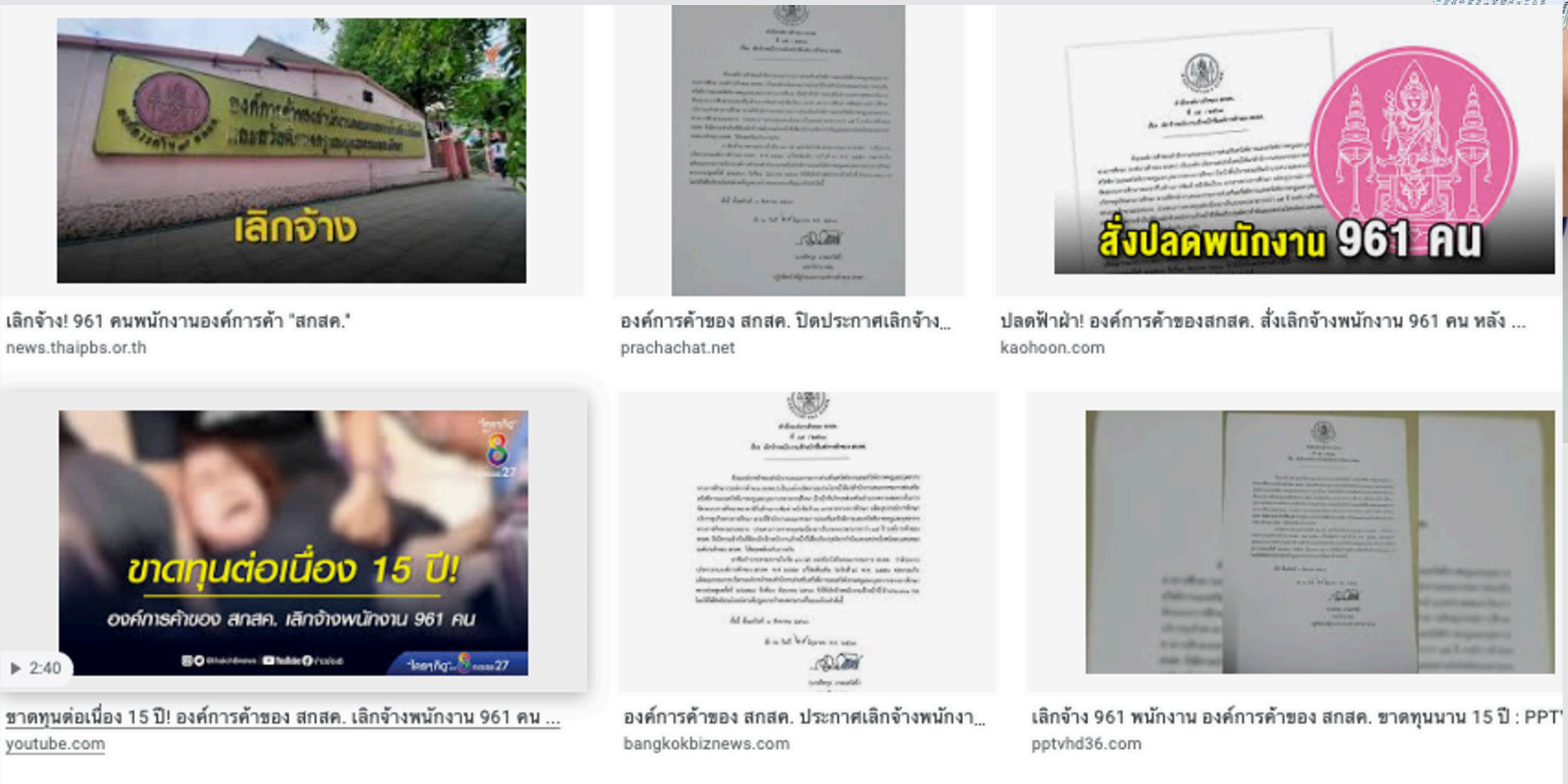
ทำไมต้องเปลี่ยน?

คำตอบคือ...เพื่ออยู่รอด



ทำไมต้องเปลี่ยน?

คำตอบคือ...เพื่ออยู่รอด



ทำไมต้องเปลี่ยน?

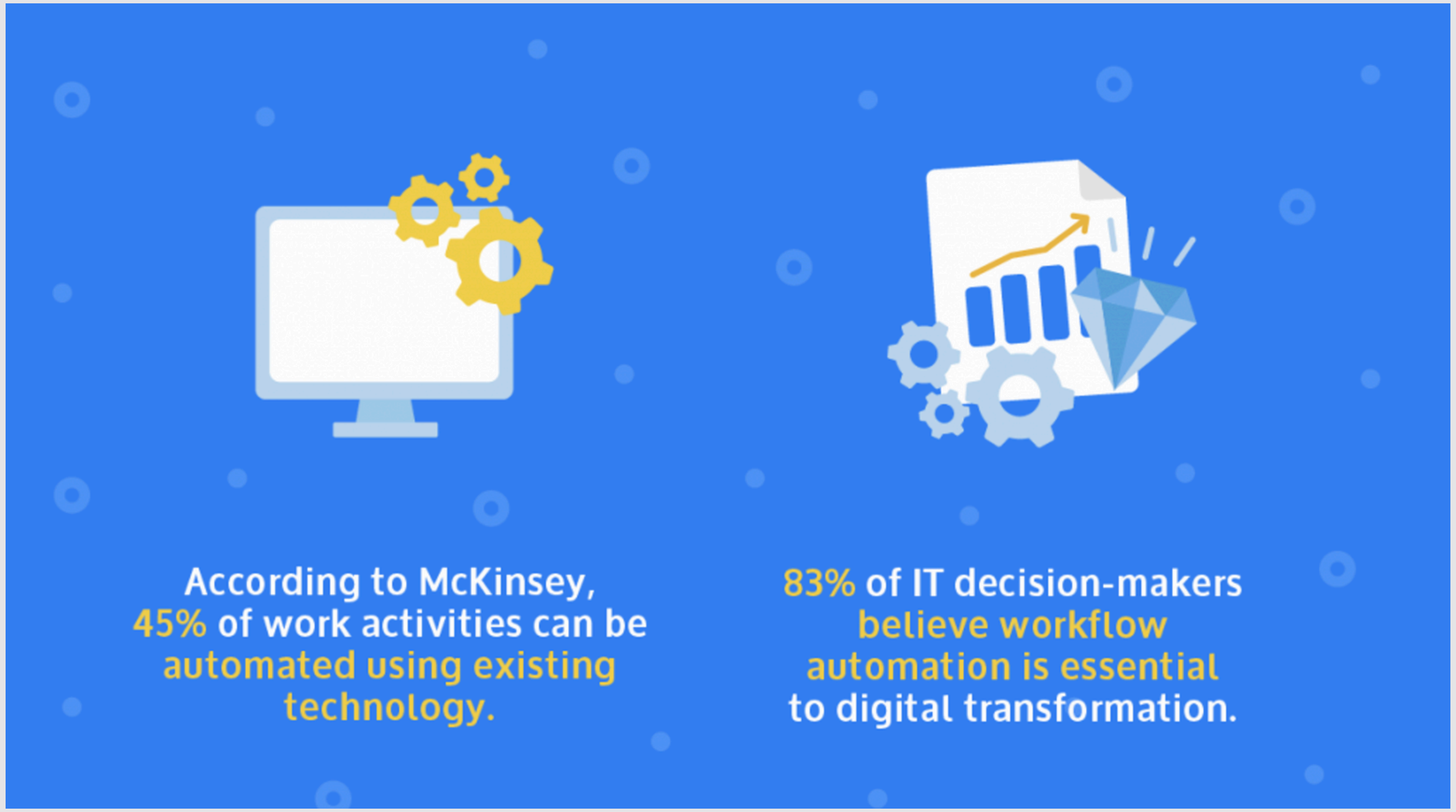
คำตอบคือ...เพื่ออยู่รอด

ทำไมต้องเปลี่ยน?

คำตอบคือ...เพื่อให้มีประสิทธิภาพ มากขึ้น

ทำไมต้องเปลี่ยน?

คำตอบคือ...เพื่อให้มีประสิทธิภาพ มากขึ้น



ทำไมต้องเปลี่ยน?

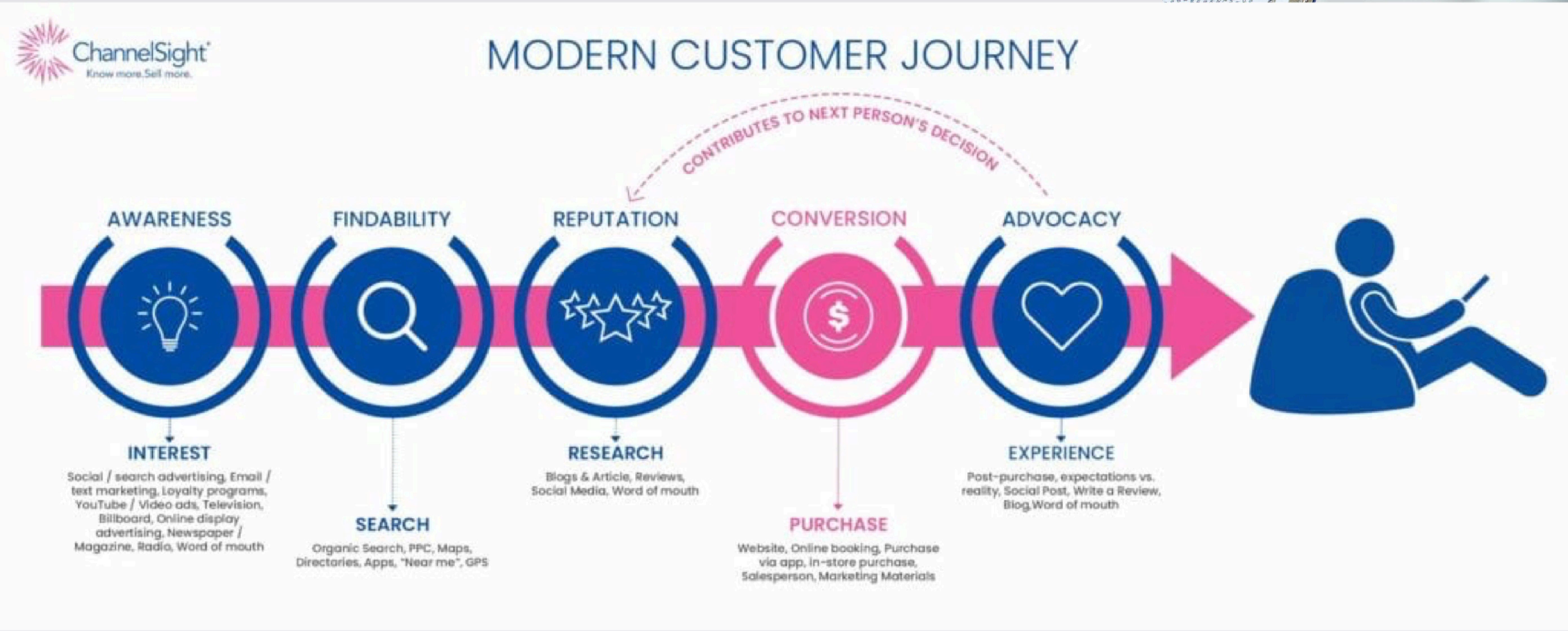
คำตอบคือ...เพื่อดึงดูดคนเก่ง และพัฒนาคนในองค์กร

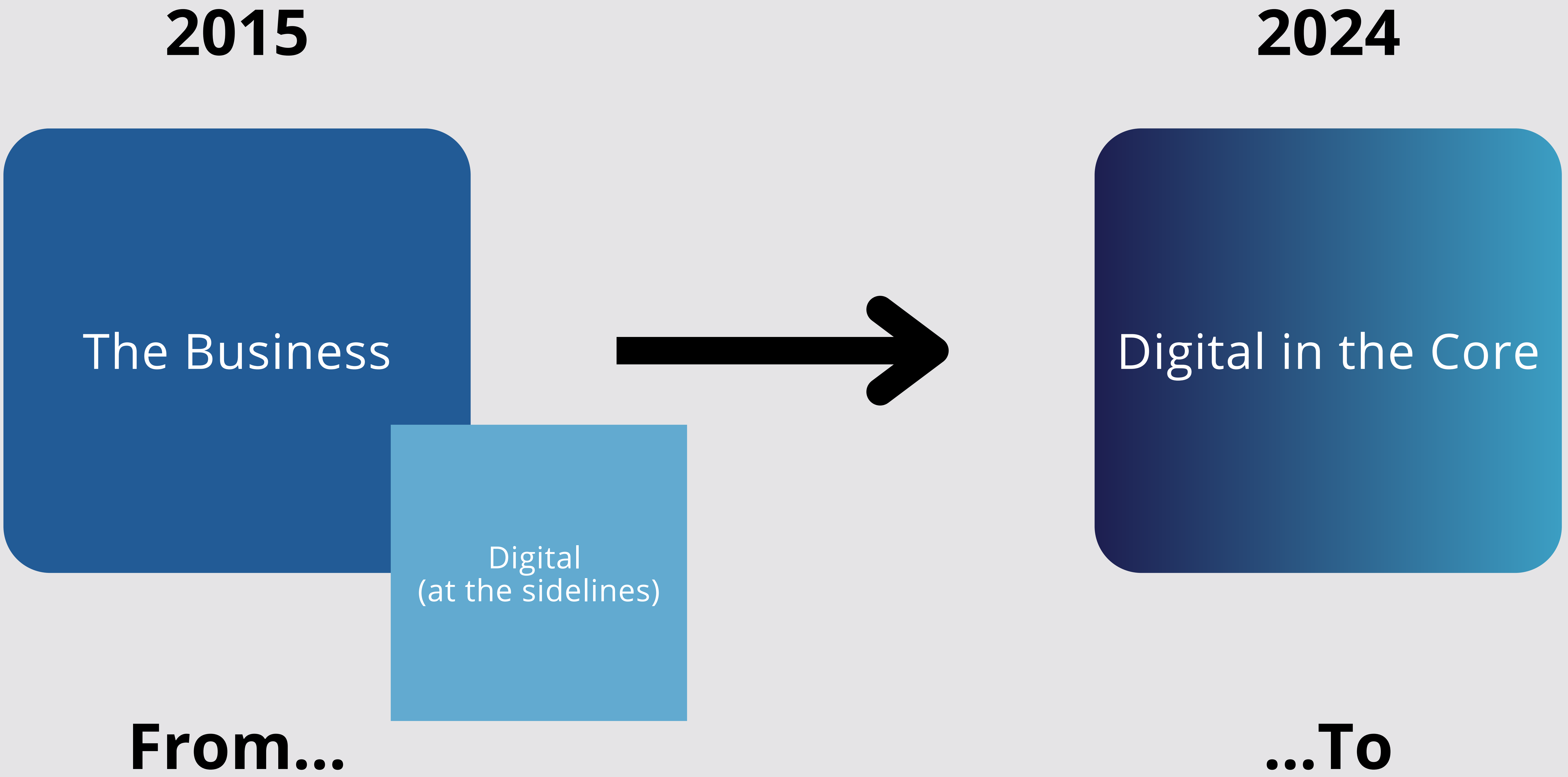
ทำไมต้องเปลี่ยน?

คำตอบคือ...เพื่อดึงดูดคนเก่ง และพัฒนาคนในองค์กร

ทำไมต้องเปลี่ยน?

คำตอบคือ...User / Customer Journey เปลี่ยนไปแล้ว




2015
2024
The Business
Digital
(at the sidelines)
Digital in the Core
From...
...To

ผลการจัดอันดับดัชนีรัฐบาลดิจิทัล ปี พ.ศ. 2563

United Nations E-Government Survey 2020 E-Government Development Index (EGDI)

ผลการจัดอันดับดัชนีรัฐบาลดิจิทัล ปี พ.ศ. 2565

United Nations E-Government Survey 2022 E-Government Development Index (EGDI)

Global Innovation Index 2021

Thailand

GII 2021 rank

43

Output rank	Input rank	Incor…	…PPP$	GII 2020 rank
46	47	Upper m…		44

	Score/ Value	Rank
Institutions	34.7	36
1.1 Political environment	37.3	51
1.1.1 Political and operational stability*		
1.1.2 Government effectiveness*		
1.2 Regulatory environment		
1.2.1 Regulatory quality*		
1.2.2 Rule of law*		
1.2.3 Cost of redundancy dismissal		
1.3 Business environment		
1.3.1 Ease of starting a business*		
1.3.2 Ease of resolving insolvency*		
Human capital and researc…		
2.1 Education		
2.1.1 Expenditure on education, % GDP		
2.1.2 Government funding/pupil, secondar…		
2.1.3 School life expectancy, years		
2.1.4 PISA scales in reading, maths and s…		

	Score/ Value	Rank
	13.8	98
	18.0	84
	0.8	27
	80.8	1
	9.9	70
	20.2	**67**
	54.4	30
	52.2	41
	0.0	83
…GDP	0.0	56
	0.1	60
	46.4	**18**
	1.7	18
	14.2	14
	0.3	116
	1.8	85
	60.8	10

WIPO
WORLD INTELLECTUAL PROPERTY ORGANIZATION

Digital Transformation
คืออะไร?

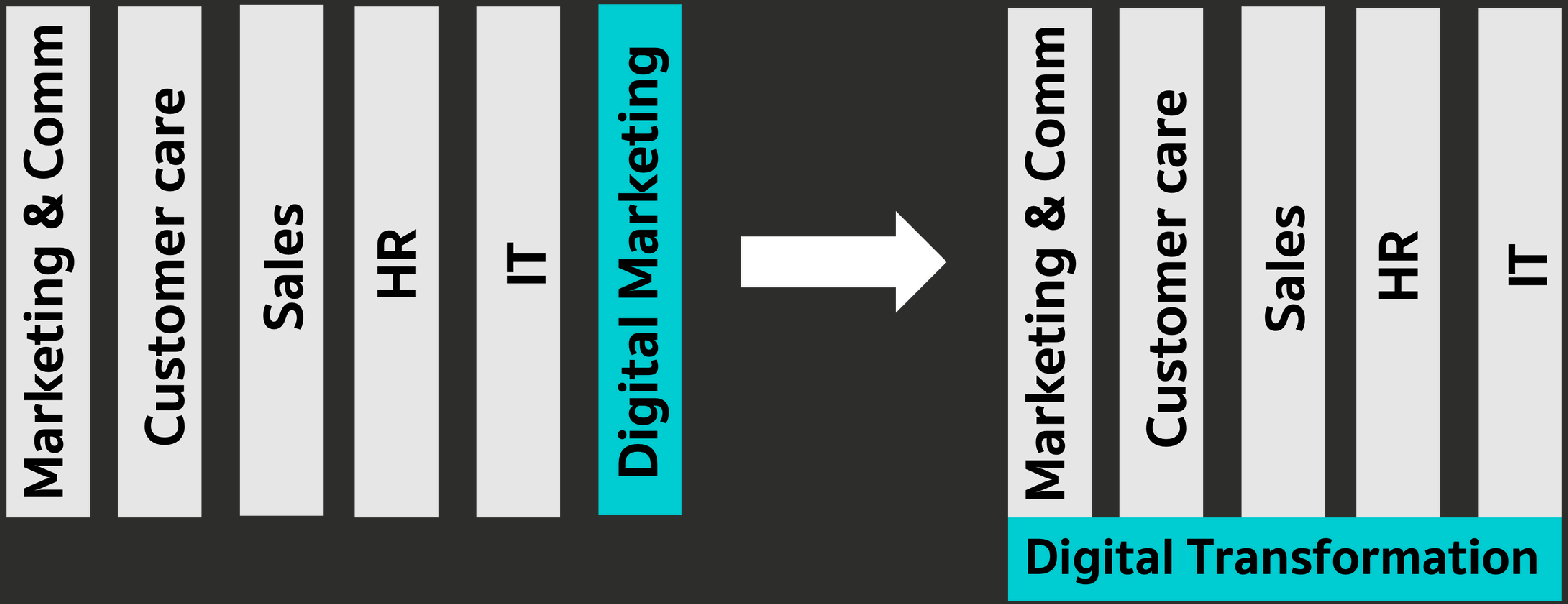
การเปลี่ยนรูปแบบองค์กรอย่างมีกลยุทธ์โดยใช้เทคโนโลยีเข้ามาช่วย เพื่อให้ทันต่อการเปลี่ยนแปลงอย่างรวดเร็วของโลกเศรษฐกิจ

The Equation

การเปลี่ยนแปลงสู่ดิจิทัลไม่ใช่แค่การปรับเปลี่ยนกระบวนการ

Digital Transformation is NOT Digitalization

Digital Transformation
ไม่ใช่งานของฝ่าย IT เพียงฝ่ายเดียว



3 ระดับการเปลี่ยนแปลงของ Digital Transformation

1. Digitization (Data)
การแปลงรูปแบบจากกระดาษสู่ดิจิทัล

2. Digitalization (Process) ปรับเปลี่ยนรูปแบบขบวนการต่าง ๆ ให้เป็นอัตโนมัติด้วยเทคโนโลยี

3. Digital Transformation (New Business Model)
ปรับเปลี่ยนรูปแบบธุรกิจโดยทำในสิ่งที่รูปแบบเดิมไม่เคยมีมาก่อน

Digital Transformation ต้องเปลี่ยนอะไรบ้าง?

กลยุทธ์ & วัฒนธรรม

STRATEGY CULTURE

+

บุคลากร & ความสัมพันธ์ลูกค้า

STAFF & CUSTOMER ENGAGEMENT

+

กระบวนการ & นวัตกรรม

PROCESS & INNOVATION

+

เทคโนโลยี

TECHNOLOGY

+

ข้อมูล & การวิเคราะห์

DATA & ANALYTICS

= Digital Transformation

Digital Transformation ต้องเปลี่ยนอะไรบ้าง?

Product & Sale

BMC จำหน่ายสินค้า
แลกเปลี่ยนกรรมสิทธิ์กับลูกค้า

From...

Customer Centric

เน้นบริการที่ให้คุณค่า
และประสบการณ์ที่ดี

...To

เอสโตเนียเปิดโอกาสให้คนทั่วโลกเป็น**“พลเมืองดิจิทัลของประเทศ”** ผ่านโปรแกรม e-Residency โดยไม่ต้องย้ายมาเอสโตเนีย

วัตถุประสงค์ *“ให้อัตลักษณ์ออนไลน์ แต่คนชาติอื่นๆ เพื่อให้ผู้คนสามารถทำงานแบบระยะไกล จากที่ไหนก็ได้ในโลก แต่มีสิทธิในเชิงการทำงานและธุรกิจแบบเดียวกับประชาชนชาวเอสโตเนีย”*

รัฐบาลเอสโตเนียวางแผนสร้างจุดเด่นให้ประเทศโดยมุ่งสู่การเป็น **“Digital Society-สังคมดิจิทัล”**อย่างแท้จริง เป็นที่มาของการทำระบบราชการดิจิทัล และมุ่งดึงดูดสตาร์ทอัพ ตามด้วย ***การออก e-Residency เป็นชาติแรกในโลก***

ส่งผลให้ประเทศเอสโตเนียเป็นประเทศที่สามารถดำเนินการเอกสารราชการดิจิทัลได้ถึง **99%** ของทั้งหมดโดยใช้ระบบลายเซ็นอิเล็กทรอนิกส์ จึงเป็นสามารถที่ทำให้สามารถดำเนินการ e-Residency

ถึงแม้ตัวจะอยู่ที่อื่นๆในโลก ก็สามารถทำธุรกิจที่เอสโตเนียได้ ทั้งการจดทะเบียนตั้งบริษัท เสียภาษี เปิดบัญชีธนาคาร หรือติดต่อราชการ

ประโยชน์ที่จะได้รับจากโปรแกรม e-Residency

สิทธิในการตั้งบริษัทสัญชาติเอสโตเนีย ซึ่งเป็นประเทศในสหภาพยุโรป โดยการดำเนินธุรกิจในเอสโตเนียจะเสมือนเป็นบริษัทสัญชาติยุโรป ซึ่งช่วยให้สามารถดำเนินธุรกิจที่มุ่งเจาะตลาดยุโรปดำเนินงานได้อย่างง่ายดาย

- Source: www.positioningmag.com

ผู้ว่าการสำนักงานการตรวจเงินแผ่นดินเอสโตเนียเปิดเผยว่า โปรแกรม e-Residency ส่งผลให้เอสโตเนีย

>

- **ประเทศสร้างงานสร้างอาชีพให้คนเอสโตเนียไปแล้ว 1,300 คน**
- **สร้างรายได้ให้ประเทศสะสมตั้งแต่เริ่มโครงการ 41 ล้านยูโร (31 ล้านยูโรในจำนวนนี้มาจากภาษี)**
- **โครงการe-Residency ยังมีผลโดยอ้อมต่อการสร้างชื่อเสียงให้เอสโตเนีย**

โดยการมีโปรแกรมรวมคนจากทั่วโลกทำให้**เอสโตเนียเคยสร้างสตาร์ทอัพระดับ ‘ยูนิคอร์น’ มาแล้ว 7 ราย** เทียบกับจำนวนประชากรเอสโตเนีย 1.3 ล้านคน

จึงกลายเป็น*ประเทศที่มีจำนวนยูนิคอร์นต่อประชากรสูงที่สุดในยุโรป และเป็นอันดับ 2 ของโลกรองจากอิสราเอล*

https://gnews.apps.go.th/news?news=20950

https://positioningmag.com/1330898

อินเดียพัฒนาระบบ **‘Aadhaar System’** ซึ่งเป็นระบบเก็บข้อมูลแบบ Biometric Database ที่ติดอันดับขนาดใหญ่ที่สุดของโลก ด้วยความร่วมมือระหว่างรัฐบาลอินเดียกับภาคเอกชน ในการเก็บข้อมูลของประชาชนและระบุตัวตน

เนื่องจากอินเดียเป็นประเทศที่มีจำนวนประชากรมากเป็นอันดับ 2 ของโลก จำนวนประชากรราว 1.38 ล้านคน (ปี 2021) คิดเป็น 17.5% ของประชากรทั่วโลก ส่งผลให้ข้อมูลที่เกี่ยวข้องกับประชากรในประเทศมีจำนวนมหาศาล จึงทำให้*การรวบรวมและดูแลข้อมูลเป็นเรื่องที่ยาก*

รัฐบาลอินเดียจึงมีแนวคิดจัดตั้ง ระบบ “Aadhaar System” ร่วมกับภาคเอกชน ซึ่งเป็นระบบฐานข้อมูลกลางแห่งชาติ โดยเก็บข้อมูลผ่าน

- **ข้อมูลประจำตัวบุคคล**
- **สแกนลายนิ้วมือ**
- **สแกนม่านตา**

ขั้นตอนการเก็บข้อมูลของผู้ลงทะเบียนใน Aadhaar ซึ่งรวมถึงการเก็บลายนิ้วมือ และสแกนม่านตา

Source: ZD Net

ผู้ที่ลงทะเบียนใน Aadhaar สามารถใช้ข้อมูลประจำตัวไปดำเนินธุรกรรมต่างๆ ได้ ไม่ว่าจะเป็นการเปิดบัญชีธนาคาร, การซื้อและจดทะเบียนซิมโทรศัพท์, การชำระค่าสาธารณูปโภค รวมทั้งลงทะเบียนเพื่อรับสวัสดิการและความช่วยเหลือทางการเงินต่างๆ จากภาครัฐ และฐานข้อมูลชุดเดียวกันนี้ยังถูกใช้โดยบริษัทใหญ่อย่าง Amazon และ Uber เพื่อระบุตัวตนลูกค้าด้วย

เกาหลีใต้รับมือกับความท้าทายของลักษณะทางประชากรที่จะมีผู้สูงอายุ เพิ่มมากขึ้นเป็น 2 เท่า ในปี 2050 โดยใช้**การพัฒนารูปแบบการจ้างงานแบบมีส่วนร่วมและการพัฒนาทักษะผู้สูงอายุ**ด้วยการอาศัยเทคโนโลยีเข้ามาช่วย

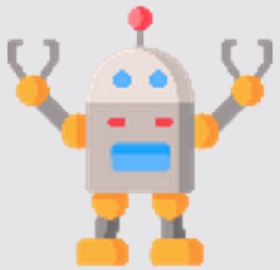
เกาหลีเริ่มการใช้หุ่นยนต์ เพื่อฝึกอบรมทักษะดิจิทัลให้กับผู้สูงอายุในกรุงโซล

กรุงโซลมีการใช้ **Humanoid robots** เพื่อช่วยผู้สูงอายุให้สามารถใช้งานอุปกรณ์ดิจิทัล สมาร์ทโฟน การส่งข้อความออนไลน์ และการบริการทางดิจิทัลต่าง ๆ ได้อย่างสะดวกสบายมากขึ้น

อีกทั้งมีการดำเนินการโปรแกรมการเรียนรู้ที่หลากหลาย เพื่อช่วยให้ประชาชนใช้อุปกรณ์ดิจิทัลได้อย่างสะดวกสบาย โดยใช้หุ่นยนต์เป็นหลัก

Liku Robots

- ฟังก์ชั่นการจดจำเสียง และการตอบกลับเพื่อถามและตอบคำถาม
- สื่อความบันเทิง
- การเรียนรู้แบบ 1:1 บนแอพพลิเคชั่น Kakaotalk



การเปิดรับคนสูงอายุทำงานด้านไอทีในบริษัทสตาร์ทอัพในเกาหลีใต้

EVERYOUNG KOREA

บริษัท EverYoung เปิดรับคนเข้าทำงาน ที่อายุ 55 ปีขึ้นไปเท่านั้น เนื่องจากบริษัทยังคงเชื่อมั่นในศักยภาพของกลุ่มคนวัยเกษียณ และต้องการต่อสู้กับวัฒนธรรมในองค์กรของเกาหลีใต้ที่มีการเลือกปฏิบัติทางอายุ

บรรดาผู้สูงอายุจะได้รับการฝึกให้ใช้แพลตฟอร์ม Naver หรือกูเกิลในเวอร์ชั่นของเกาหลีใต้ เพื่อให้คัดกรองข้อมูลหรือเนื้อหาที่ไม่เหมาะสม ทั้งบน Naver Map และในบล็อก รวมทั้งฝึกฝนทักษาด้านไอทีอื่นๆ และบางครั้งยังสอนการเขียนโค้ดให้กับเด็กนักเรียนด้วย

Source: Presentation made by the Seoul 50+ Foundation of the Seoul Metropolitan Government, Paris, 2017

Source: ITU Publications, 2020 and posttoday.com, 2019

DIGITAL TRANSFORMATION FRAMEWORK

Digital Transformation ต้องเปลี่ยนอะไรบ้าง?

กลยุทธ์ & วัฒนธรรม		บุคลากร & ความสัมพันธ์ลูกค้า		กระบวนการ & นวัตกรรม		เทคโนโลยี		ข้อมูล & การวิเคราะห์
STRATEGY & CULTURE	+	STAFF & CUSTOMER ENGAGEMENT	+	PROCESS & INNOVATION	+	TECHNOLOGY	+	DATA & ANALYTICS

= Digital Transformation

Digital Transformation

กรอบการเปลี่ยนผ่านทางดิจิทัล (Digital Transformation Framework) สามารถแบ่งออกเป็น 3 ประเภทหลัก คือ

1) ประสบการณ์ลูกค้า
2) ขับเคลื่อนองค์ด้วยข้อมูล
3) กระบวนการในการปฏิบัติงาน
4) รูปแบบธุรกิจ

กรอบการเปลี่ยนผ่านทางดิจิทัล (Digital Transformation Framework)

การเปลี่ยนแปลงประสบการณ์ลูกค้า (Customer Experience)	การเปลี่ยนแปลงการขับเคลื่อนองค์กรด้วยข้อมูล (Data Driven Organization)	การเปลี่ยนแปลงกระบวนการในการปฏิบัติงาน (Operational Process)	การเปลี่ยนแปลงรูปแบบธุรกิจ (Business Model)
ความเข้าใจลูกค้า (Customer Understanding)	การกำหนดเส้นทางการวิเคราะห์ข้อมูล (Data Analytic Pathway)	กระบวนการทางดิจิทัล (Process Digitalization)	การเปลี่ยนแปลงธุรกิจด้วยดิจิทัล (Digitally-modified Business)
การเติบโต (Top Line Growth)	การปรับมาใช้ฐานข้อมูลบนคอมพิวเตอร์ (Computerization)	ความสามารถของบุคลากร (Worker Enablement)	สร้างธุรกิจดิจิทัลใหม่ (New Digital Business)
ช่องทางในการติดต่อกับลูกค้า (Customer Touch Point)	การวิเคราะห์และเชื่อมโยงข้อมูล (Data Analytic & Integration)	ประสิทธิภาพในการจัดการ (Performance Management)	ดิจิทัลที่ใช้ร่วมกันได้ทั่วโลก (Digital Globalization)

ความสามารถทางด้านดิจิทัล (Digital Capabilities)

พื้นฐานสำคัญในการเปลี่ยนแปลงประสบการณ์ลูกค้า กระบวนการดำเนินงานภายในองค์กร และรูปแบบธุรกิจ โดยเป็นส่วนช่วยในการประสานการเปลี่ยนผ่านด้านดิจิทัลให้มีความสอดคล้องกับกลยุทธ์ขององค์กร

องค์กรที่ขับเคลื่อนด้วยข้อมูลจำเป็นต้องมีโครงสร้างพื้นฐานทางข้อมูลและการบริหารจัดการข้อมูลอย่างกว้างขวาง เพื่อให้ได้มาซึ่งข้อมูลเชิงลึกและสร้างคุณค่าทางธุรกิจด้วยการวิเคราะห์ข้อมูล

Data Driven Enterprise Strategy

1 Data Foundation

2 Data Management

3 Data Analytic

4 Value Creation

Data Platform
สำหรับข้อมูลขนาดใหญ่ (Big Data) และควรสอดคล้องกับวัตถุประสงค์ของธุรกิจ

Data Architecture
สามารถรับมือได้กับข้อมูลจำนวนมากที่มาจากแหล่งข้อมูลที่หลากหลาย

Data Governance
ควรมีมาตรฐานสำหรับการควบคุมและบริหารจัดการข้อมูลขององค์กร

Metadata Management
รับรองได้ว่าการขับเคลื่อนของข้อมูลเป็นแบบไร้รอยต่อ

Advanced Analytics
สามารถระบุเทรนด์และรูปแบบของข้อมูลเพื่อใช้ในการตัดสินใจ

AI/ML
สร้างโมเดลเพื่อการทำนายและเสนอข้อเสนอแนะ

Data-Driven Business Model
โดยใช้ข้อมูลเกี่ยวกับลูกค้า ข้อมูลตลาด และข้อมูลบริษัท

Data-Driven Performance
ใช้ข้อมูลในการฝึกอบรมพนักงาน พัฒนากระบวนการทำงานและความร่วมมือกัน

Goal
เป้าหมายคือ?

Reality
แต่ตอนนี้ สิ่งที่เป็นคือ?

Options
มีทางเลือกอะไรบ้าง?

Will
คิดว่าควรจะทำอะไร?

2.PDPA

PDPA คืออะไร?

PDPA หรือ Personal Data Protection Act หรือ พรบ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 คือ กฎหมายที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคล โดยห้ามมิให้ผู้อื่นนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในด้านใดด้านหนึ่งโดยที่เจ้าของข้อมูลไม่ยินยอม

ทำไมต้องคุ้มครองข้อมูลส่วนบุคคล?

สร้างความเชื่อมั่น **(Trust)**

Getting trust from data subjects and consumers is vital. They will be more confident when personal data management is transparent and proportionate.

ยกระดับการธรรมาภิบาลข้อมูล **(Better data governance)**

Good data governance is desirous in every organization. The more governance an organization has, the more likely they will gain trust from users and consumers.

ยกระดับสู่มาตรฐานสากล **(Connecting with global standards)**

Global data transfer needs to connected with global standards of protection to foster free flows of data.

นิยามของข้อมูลส่วนบุคคล

พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA): ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ประเภทของข้อมูลส่วนบุคคล

- ข้อมูลส่วนบุคคลทั่วไป (Genral Personal Data)
- ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data)

ข้อมูลส่วนบุคคลทั่วไป

- ชื่อ นามสกุล
- เพศ
- อายุ วันเดือนปีเกิด
- สถานภาพการสมรส
- IP address
- อีเมลส่วนตัว

ข้อมูลส่วนบุคคลอ่อนไหว

- เชื้อชาติ
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
- พฤติกรรมทางเพศ
- ข้อมูลสุขภาพ
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลความพิการ
- ข้อมูลสหภาพแรงงาน
- ข้อมูลประวัติอาชญากรรม

ข้อมูลส่วนบุคคลอยู่ในรูปแบบใดบ้าง?

เอกสาร

ข้อมูลส่วนบุคคลที่เก็บในรูปแบบ
เอกสารต่าง ๆ เช่น แบบฟอร์ม เป็นต้น

ข้อมูลอิเล็กทรอนิกส์

ข้อมูลส่วนบุคคลที่เก็บในรูปแบบอิเล็กทรอนิกส์ต่าง ๆ
เช่น ไฟล์เอกสาร ข้อมูลในฐานข้อมูล เป็นต้น

วาจา

ข้อมูลส่วนบุคคลที่จัดเก็บในรูปแบบการ
บันทึกเสียงบทสนทนา เช่น การบันทึก
เสียงสนทนาของ Call Center เป็นต้น

ภาพนิ่ง ภาพ
เคลื่อนไหว หรือวิดีโอ

ข้อมูลส่วนบุคคลที่เก็บในรูปแบบของภาพประเภทต่าง ๆ
เช่น ภาพถ่าย หรือวิดีโอบันทึกเหตุการณ์
ต่าง ๆ เป็นต้น

ผู้ที่เกี่ยวข้องกับ **PDPA** มีใครบ้าง?

ผู้ที่เกี่ยวข้องใน PDPA

Data Protection Authority	Data Controller	Data Processor	Data Subject
หน่วยงานผู้กำกับดูแล - สคส. (PDPC)	ผู้ควบคุมข้อมูลส่วนบุคคล	ผู้ประมวลผลข้อมูลส่วนบุคคล	เจ้าของข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคล (Processing):
การดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นการใช้ เก็บรวบรวม จัดเก็บ ลบ ทำลาย เปิดเผย เชื่อมโยง เปลี่ยนแปลง ส่งผ่าน หรือ Update ข้อมูล

โดยสรุป: ทุกอย่างที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลทั้งหมด

ใครคือผู้ควบคุมข้อมูลส่วนบุคคล (DATA CONTROLLER) และผู้ประมวลผลข้อมูลส่วนบุคคล (DATA PROCESSOR)?

Data controller

Data processor

สั่งการให้ Data Processor

Data controller

มีอำนาจ “ตัดสินใจ” เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของ:

ข้อมูลส่วนบุคคลของลูกค้า

ข้อมูลส่วนบุคคลของบุคลากร

ข้อมูลส่วนบุคคลของผู้มีส่วนได้ส่วนเสียอื่น ๆ

เจ้าของข้อมูลส่วนบุคคล (Data Subject) ของ Data Controller

Data processor

ดำเนินการ “ตามคำสั่งของ” Data Controller ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของ Data Subject ของ Data Controller

ยกตัวอย่าง

-ธนาคารที่ Data Controller สั่งหรือจ้างให้โอนเงินเดือนเข้าบัญชีให้กับบุคลากรของ Data Controller

PDPA กำหนดให้ Data Controller ต้องทำอะไรบ้างในกรณีนี้

Data controller **Data processor**

ทำข้อตกลงการประมวลผล
ข้อมูลส่วนบุคคล (Data Processing Agreement) กับ Data Processor

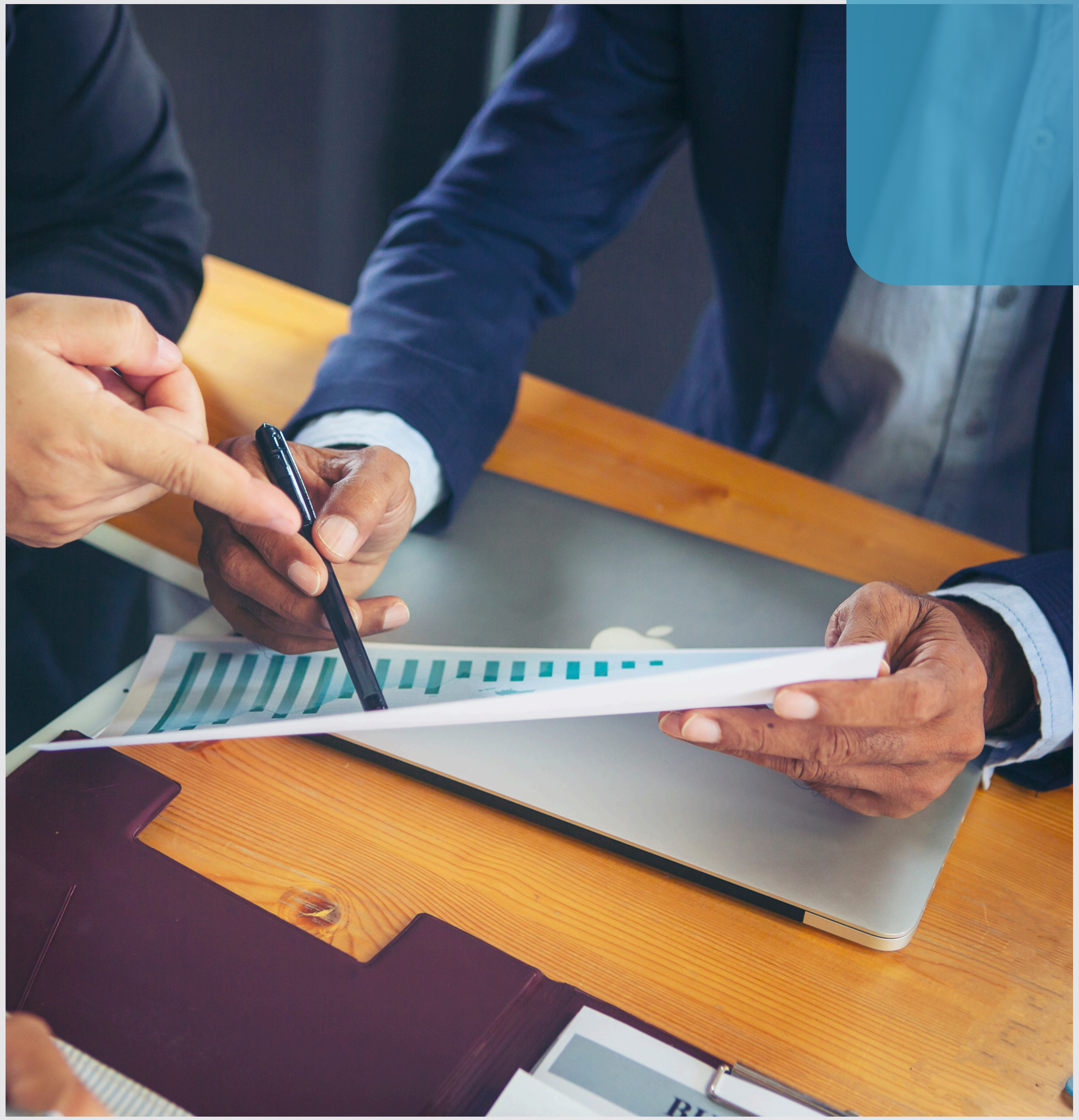
บริษัท A ได้รับการว่าจ้างโดย Data Controller
ให้สำรวจข้อมูลผู้รับบริการ
บริษัท A = Data processor

หน้าที่ของ Data Controller

- แจ้งวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล Privacy notice (ม.23)
- มีความชอบธรรมในการประมวลผล Lawful basis (ม.24, 26)
- เก็บ ใช้ เปิดเผยเท่าที่จำเป็นและตามวัตถุประสงค์ Purpose limitation (ม.22, 27)
- ทำข้อมูลส่วนบุคคลให้ถูกต้อง Data accuracy (ม.35)
- ป้องกันมิให้บุคคลหรือองค์กรอื่นที่รับข้อมูลจาก Data controller นำข้อมูลไปใช้หรือเปิดเผยโดยมิชอบ Preventing others from unlawful use or disclosure: (ม.37(2))
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม Appropriate security (ม.37 (1))

หน้าที่ของ **Data Controller (ต่อ)**

- แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ผู้กำกับดูแลทราบภายใน 72 ชั่วโมง Breach notification: (ม.37 (4))
- มีการตรวจสอบเพื่อลบข้อมูลที่ไม่จำเป็น และมีการจัดการสิทธิเจ้าของข้อมูลส่วนบุคคล Data check and Data subject rights management: (ม.37(3))
- ทำบันทึกรายการกิจกรรมที่ใช้ข้อมูลส่วนบุคคล Records of Processing Activity (RoPA) (ม.39)
- แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล - DPO (ม.41)



หน้าที่ของ Data Processor

- ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- แจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้ Data controller ทราบ
- ทำบันทึกรายการการประมวลผลข้อมูล (RoPA) (ถ้าเป็นไปตามเกณฑ์ต้องจัดทำ)
- แต่งตั้ง DPO (ถ้าเป็นไปตามเกณฑ์ต้องแต่งตั้ง)

หน่วยงานที่ต้องจัดให้มี DPO

- หน่วยงานของรัฐ
- หน่วยงานที่การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด
- หน่วยงานที่มีกิจกรรมหลักเป็นการเก็บ รวบรวม ใช้ หรือเปิดเผย Sensitive Personal Data

หน้าที่ของ DPO

- ให้คำแนะนำ Data controller
- ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล
- ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

หลักการของ **PDPA**

- Lawful Processing and Transparency มีความชอบธรรมในการประมวลผลข้อมูลส่วนบุคคลและมีความโปร่งใส
- Necessity and Purpose Limitation ใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์และเท่าที่จำเป็น
- Data Accuracy ต้องทำข้อมูลส่วนบุคคลให้ถูกต้องและเป็นปัจจุบัน
- Limitation of Storage มีระยะเวลาในการเก็บข้อมูลส่วนบุคคลที่แน่นอน
- Security มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม
- เคารพสิทธิของ Data Subject ดำเนินการตามคำร้องขอของ Data Subject ตามขอบเขตที่กฎหมายกำหนด

โทษของการไม่ปฏิบัติตาม PDPA

โทษปรับทางปกครอง - ม.82-90 (อำนาจปรับของสำนักงานคุ้มครองข้อมูลส่วนบุคคล: สคส.)

- คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งโทษปรับทางปกครองได้โดยคำนึงถึงความร้ายแรงของพฤติกรรม ขนาดของกิจการ ฯลฯ โดยอาจตักเตือนก่อนก็ได้ (ม. 90)

โทษปรับทางแพ่ง - ม.77-78 (เรียกร้องผ่านกระบวนการยุติธรรมทางแพ่ง)

- มื่อมีการเรียกร้องโดยผู้เสียหายผ่านกระบวนการทางศาลยุติธรรมเท่านั้น
- ชดใช้ค่าสินไหมทดแทนได้ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง

โทษอาญา - ม.79-80 (เรียกร้องผ่านกระบวนการยุติธรรมทางอาญา)

- (เฉพาะกรณีที่เข้าองค์ประกอบความผิดทางอาญาเท่านั้น) มีโทษอาญาถ้าความผิดเรื่อง
  - (1) แสวงหาผลประโยชน์จากข้อมูล หรือ
  - (2) ทำให้เกิดการเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรือได้รับความอับอายจากการใช้ข้อมูลส่วนบุคคลที่อ่อนไหว
- โทษอาญาสามารถยอมความได้
- โทษจำคุก 6 เดือน - 1 ปี และโทษปรับ 5 แสน - 1 ล้านบาท

PDPA มีข้อยกเว้นหรือไม่?

ข้อยกเว้นของ PDPA ตาม พรบ.

1	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น
2	การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
3	บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น
4	สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี
5	การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา
6	การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ความชอบธรรมในการประมวลผลข้อมูลส่วนบุคคล

ฐานการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย (Lawfulness of processing)

หมายถึงการที่ Data Controller ต้องสามารถอ้างความชอบธรรม (Lawful Basis) ในการประมวลผลข้อมูลส่วนบุคคลให้ได้ว่าในแต่ละกิจกรรมที่บริษัททำมีฐานการประมวลผลที่ชอบธรรมตามที่กฎหมาย PDPA กำหนดไว้อย่างไร

กฎหมาย PDPA กำหนดให้ Data Controller ต้องมี Lawful Basis ในการประมวลผลข้อมูลส่วนบุคคล

- Lawful basis สำหรับประมวลผลข้อมูลส่วนบุคคลแบบทั่วไป กำหนดใน ม. 24
- Lawful basis สำหรับประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว กำหนดใน ม. 26

โทษสำหรับ Data Controller ที่ไม่มี Lawful basis ในการประมวลผลข้อมูลส่วนบุคคลนั้น ได้แก่

- สูงสุด 3 ล้านบาท สำหรับการไม่มี Lawful basis ในการประมวลผลข้อมูลส่วนบุคคลแบบทั่วไป (ม. 83)
- สูงสุด 5 ล้านบาท สำหรับการไม่มี Lawful basis ในการประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหว (ม. 84)

ฐานการประมวลผล หรือฐานกฎหมาย **(Lawful basis)** สำหรับการประมวลผลข้อมูลส่วนบุคคลทั่วไป **(ม.24)**

- ฐานการระงับอันตรายต่อชีวิต (Vital interest)
- ฐานการจัดทำเอกสารประวัติศาสตร์เพื่อประโยชน์สาธารณะหรือการวิจัย (Historical Archive & Research)
- ฐานจำเป็นเพื่อปฏิบัติตามสัญญา (Contract)
- ฐานปฏิบัติตามกฎหมาย (Legal Obligation)
- ฐานผลประโยชน์อันชอบธรรมที่ไม่ละเมิดสิทธิขั้นพื้นฐานของ Data Subject (Legitimate Interest)
- ฐานภารกิจรัฐหรือฐานเพื่อประโยชน์สาธารณะ (Public Task)
- ฐานการขอความยินยอม (Consent)

ฐานการประมวลผล หรือฐานกฎหมาย **(Lawful basis)** สำหรับการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว **(ม.26)**

- ฐานการระงับอันตรายต่อชีวิต (Vital interest)
- ฐานดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน (Special Objectives)
- ฐานจำเป็นเพื่อปฏิบัติตามสัญญากับผู้ประกอบวิชาชีพทางการแพทย์ (Medical Contract)
- ฐานจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย (Claim of Legal Rights)
- ฐานจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์ด้านการแพทย์ ด้านสาธารณสุข การคุ้มครองแรงงาน การศึกษาวิจัย และประโยชน์สาธารณะที่สำคัญ (Legal Obligations with Specific Purposes)
- ฐานการเก็บรวบรวมประวัติอาชญากรรมภายใต้การควบคุมของหน่วยงานที่มีอำนาจด้านกฎหมาย (Criminal Records)
- ฐานการขอความยินยอมโดยชัดแจ้ง (Explicit Consent)

3.CYBERSECURITY

NCSA สกมช

ลำดับ	หน่วยงานที่ถูกโจมตี ปีพ.ศ. 2566	ม.ค	ก.พ.	มี.ค.	เม.ษ.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
0.	หน่วยงานของรัฐ ด้านอื่นๆ	45	33	72	42	68	40	39	52	22	48	0	0	**461**
1.	ความมั่นคง	3	1	4	1	1	2	7	32	8	18	0	0	**77**
2.	บริการภาครัฐ	1	4	8	5	6	3	1	8	3	1	0	0	**40**
3.	การเงินการธนาคาร	4	17	16	31	19	13	14	16	8	7	0	0	**145**
4.	เทคโนโลยีสารสนเทศและโทรคมนาคม	0	0	2	0	0	1	1	1	1	13	0	0	**19**
5.	ขนส่งและโลจิสติกส์	5	4	2	0	1	2	5	3	0	1	0	0	**23**
6.	พลังงานและสาธารณูปโภค	0	3	2	7	8	13	12	18	0	11	0	0	**74**
7.	สาธารณสุข	5	6	11	9	6	6	6	11	2	5	0	0	**67**
8.	อื่นๆ	0	0	0	0	0	3	2	6	6	3	0	0	**20**
8.1	การศึกษา	111	70	88	48	81	33	18	16	69	98	0	0	**632**
8.2	ผู้ประกอบการธุรกิจอีคอมเมิซ	0	3	2	0	0	4	0	1	1	0	0	0	**11**
8.3	เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	0	0	0	0	0	0	0	0	1	1	0	0	**2**
8.4	ผู้ประกอบการพาณิชย์ต่างประเทศที่มีที่ตั้งในประเทศไทย	1	2	2	0	1	0	0	2	0	27	0	0	**35**
8.5	ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	0	0	0	0	0	1	0	1	0	11	0	0	**13**
8.6	ผู้ผลิตซอฟแวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	1	2	3	0	0	0	0	0	1	2	0	0	**9**
8.7	กลุ่มจัดตั้ง ชมรม สมาคม	0	0	7	0	0	0	2	0	0	1	0	0	**10**
8.8	ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	14	9	19	8	0	9	17	17	8	47	0	0	**148**
8.9	ผู้ให้บริการโซเชียลมีเดีย	0	0	0	0	1	1	0	0	0	0	0	0	**2**
9.	แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ. ไซเบอร์ฯ	0	0	0	0	0	0	0	0	0	1	0	0	**1**
	รวม	**190**	**158**	**238**	**151**	**192**	**131**	**124**	**184**	**130**	**295**	**0**	**0**	**1789**

Souce: https://www.pptvhd36.com/news/%E0%B9%84%E0%B8%AD%E0%B8%97%E0%B8%B5/216557

ลำดับ	รูปแบบภัยคุกคาม ปีพ.ศ. 2566	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
1	Hacked Website (Gambling)	78	40	73	31	111	42	8	2	69	61	0	0	**515**
2	Hacked Website (Defacement)	83	60	79	17	13	20	8	5	19	32	0	0	**336**
3	Fake Website	20	28	50	49	26	26	13	50	13	26	0	0	**301**
4	จุดอ่อนช่องโหว่	1	1	4	6	4	10	45	6	1	150	0	0	**228**
5	Finance Scam - หลอกลวงการเงิน Online	0	10	7	12	19	17	15	24	5	3	0	0	**112**
6	Data Leak	0	0	2	31	3	0	4	60	0	0	0	0	**100**
7	DDoS	0	0	1	0	0	3	20	9	0	0	0	0	**33**
8	Hacked Website (Phishing)	3	6	7	1	5	4	0	4	5	3	0	0	**38**
9	Data Breach	3	2	6	0	0	3	6	7	14	6	0	0	**47**
10	Ransomware	1	6	2	3	1	4	1	5	1	3	0	0	**27**
11	Hacked Website (Malware)	0	0	3	0	5	1	0	3	0	0	0	0	**12**
12	Privileged account Compromise	0	0	0	1	0	1	1	6	3	7	0	0	**19**
13	Command and Control Server	1	0	0	0	0	0	2	2	0	1	0	0	**6**
14	Unauthorised access to information	0	0	2	0	3	0	0	0	0	1	0	0	**6**
15	Security Misconfiguration	0	0	0	0	1	0	1	0	0	2	0	0	**4**
16	Appicaltion Compromise	0	0	0	0	0	0	0	1	0	0	0	0	**1**
17	Mail Phishing	0	0	1	0	0	0	0	0	0	0	0	0	**1**
18	Malware	0	0	0	0	1	0	0	0	0	0	0	0	**1**
19	Unauthorised modification of information	0	0	1	0	0	0	0	0	0	0	0	0	**1**
20	อื่นๆ	0	1	0	0	0	0	0	0	0	0	0	0	**1**
	รวม	**190**	**154**	**238**	**151**	**192**	**131**	**124**	**184**	**130**	**295**	**0**	**0**	**1789**

Souce: https://www.pptvhd36.com/news/%E0%B9%84%E0%B8%AD%E0%B8%97%E0%B8%B5/216557

Cybersecurity ในมุมมองทั่วไป คือ การดำเนินการในการปกป้องระบบ เครือข่าย และโปรแกรมต่างๆ จากการโจมตีทางดิจิทัล ซึ่งครอบคลุมถึงเทคนิคและเทคโนโลยีหลากหลายที่ช่วยรักษาความปลอดภัยให้กับชีวิตดิจิทัลของเรา ตั้งแต่อุปกรณ์ส่วนบุคคลไปจนถึงโครงสร้างพื้นฐานที่สำคัญ

Cybersecurity ในมุมมองส่วนบุคคล คือ การที่ข้อมูลส่วนบุคคลจะไม่สามารถเข้าถึงได้โดยคนอื่นนอกจากเจ้าของข้อมูลและผู้ที่ได้รับอนุญาต รวมถึงการที่อุปกรณ์คอมพิวเตอร์ของผู้ใช้จะทำงานได้อย่างถูกต้องและปราศจากมัลแวร์

ความสำคัญของ **Cybersecurity**

1. การปกป้องข้อมูลส่วนบุคคล (Personal Data Protection)
2. การรักษาความลับขององค์กร (Confidentiality of Organizational Information)
3. การป้องกันการโจมตีทางไซเบอร์ (Protection Against Cyber Attacks)
4. การรักษาความน่าเชื่อถือ (Maintaining Trustworthiness)
5. การปฏิบัติตามกฎหมายและข้อบังคับ (Compliance with Laws and Regulations)
6. การป้องกันการสูญเสียทางการเงิน (Prevention of Financial Losses)
7. การเสริมสร้างการตอบสนองต่อเหตุการณ์ (Enhancing Incident Response)
8. การปกป้องทรัพย์สินทางปัญญา (Protection of Intellectual Property)


ทำความรู้จัก Cyberattacks

- Phishing
  - เทคนิคการหลอกลวงออนไลน์ที่พยายามขโมยข้อมูลส่วนบุคคล เช่น รหัสผ่าน, หมายเลขบัตรเครดิต หรือข้อมูลสำคัญอื่น ๆ มักจะดำเนินการผ่านอีเมล, ข้อความ, หรือเว็บไซต์ปลอมที่ดูเหมือนจริง
  - วิธีการ: แฮกเกอร์จะส่งข้อความปลอมที่ดูเหมือนมาจากแหล่งที่เชื่อถือได้ เช่น ธนาคาร, บริษัทใหญ่, หรือแพลตฟอร์มโซเชียลมีเดีย
  - จุดประสงค์: เพื่อให้เหยื่อคลิกลิงก์ที่เป็นอันตราย หรือกรอกข้อมูลสำคัญในฟอร์มที่สร้างขึ้นมาเพื่อหลอกลวง
  - อาการ: อาจมีการขอให้ยืนยันข้อมูลส่วนตัว, ขอตรวจสอบบัญชี, หรือแจ้งว่ามีปัญหาที่ต้องการการดำเนินการด่วน
  - การป้องกัน:
    - ตรวจสอบที่อยู่ URL ของเว็บไซต์ก่อนกรอกข้อมูล
    - อย่าคลิกลิงก์จากอีเมลหรือข้อความที่ไม่รู้จัก
    - ใช้การยืนยันตัวตนแบบสองขั้นตอน (2FA)

ทำความรู้จัก
Cyberattacks (ต่อ)

- Man-in-the-Middle (MitM) Attacks
  - เทคนิคการโจมตีที่ผู้โจมตีแทรกตัวเข้ามาในกระบวนการสื่อสารระหว่างผู้ใช้งานสองฝ่ายโดยไม่ให้พวกเขารู้ตัว
  - วิธีการ: ผู้โจมตีจะทำหน้าที่เป็น "กลาง" ระหว่างผู้ส่งและผู้รับข้อมูล โดยที่ข้อมูลที่ส่งไปยังปลายทางจริงจะถูกดักจับและอาจถูกเปลี่ยนแปลงได้
  - ประเภทของ MitM:
    - Wi-Fi Eavesdropping: ดักจับข้อมูลที่ส่งผ่านเครือข่าย Wi-Fi ที่ไม่ได้เข้ารหัส
    - Session Hijacking: ขโมยข้อมูลการเข้าสู่ระบบหรือเซสชันที่เปิดอยู่เพื่อเข้าถึงบัญชีของเหยื่อ
    - SSL Stripping: เปลี่ยนการเชื่อมต่อที่ปลอดภัย (HTTPS) เป็นการเชื่อมต่อที่ไม่ปลอดภัย (HTTP)

ทำความรู้จัก Cyberattacks (ต่อ)

- Man-in-the-Middle (MitM) Attacks
  - อาการ:
    - ข้อมูลที่ส่งหรือรับอาจถูกเปลี่ยนแปลงโดยไม่รู้ตัว
    - อาจมีการสื่อสารที่ไม่ปกติหรือมีปัญหาในการเชื่อมต่อ
  - การป้องกัน:
    - ใช้การเข้ารหัสข้อมูลอย่างแข็งแกร่ง เช่น HTTPS สำหรับการเชื่อมต่อเว็บ
    - หลีกเลี่ยงการเชื่อมต่อกับเครือข่าย Wi-Fi สาธารณะที่ไม่ปลอดภัย
    - ใช้การตรวจสอบใบรับรอง SSL/TLS ของเว็บไซต์ให้แน่ใจว่าเป็นของจริง
    - ติดตั้งและอัปเดตซอฟต์แวร์รักษาความปลอดภัย เช่น VPN และไฟร์วอลล์

ทำความรู้จัก
Cyberattacks (ต่อ)

- Denial-of-Service (DoS) Attacks
  - การโจมตีที่มุ่งหมายเพื่อทำให้บริการ, เซิร์ฟเวอร์, หรือระบบไม่สามารถใช้งานได้ โดยการทำให้ระบบมีการทำงานเกินขีดความสามารถ
  - วิธีการ:
    - Flooding: ส่งข้อมูลหรือคำขอจำนวนมากไปยังระบบเป้าหมายเพื่อทำให้ระบบทำงานช้าลงหรือหยุดทำงาน
    - Exploitation: ใช้ช่องโหว่ในระบบเพื่อทำให้ระบบล่มหรือไม่สามารถทำงานได้
  - ประเภทของ DoS:
    - DoS Attack: การโจมตีจากแหล่งเดียวที่ส่งข้อมูลมากเกินไป
    - Distributed Denial-of-Service (DDoS) Attack: การโจมตีที่ใช้หลายแหล่ง (เช่น คอมพิวเตอร์ที่ถูกควบคุมจากแฮกเกอร์) เพื่อโจมตีระบบเดียวกัน

ทำความรู้จัก Cyberattacks (ต่อ)

- Denial-of-Service (DoS) Attacks
  - อาการ:
    - ระบบหรือบริการไม่สามารถตอบสนองต่อคำขอของผู้ใช้งาน
    - ความเร็วในการทำงานของระบบช้าลงหรือไม่เสถียร
    - บริการที่ถูกโจมตีไม่สามารถเข้าถึงได้หรือเกิดการหยุดชะงัก
  - การป้องกัน:
    - ใช้การป้องกัน DDoS จากผู้ให้บริการเช่น การกรองคำขอที่น่าสงสัย
    - ติดตั้งซอฟต์แวร์รักษาความปลอดภัยที่สามารถตรวจจับและบล็อกการโจมตี
    - ใช้เทคโนโลยีการกระจายโหลด (Load Balancing) เพื่อจัดการกับปริมาณข้อมูลที่เข้ามา
    - การทำงานร่วมกับผู้ให้บริการอินเทอร์เน็ต (ISP) เพื่อลดผลกระทบจากการโจมตี

ทำความรู้จัก Cyberattacks (ต่อ)

- Denial-of-Service (DoS) Attacks
  - อาการ:
    - ระบบหรือบริการไม่สามารถตอบสนองต่อคำขอของผู้ใช้งาน
    - ความเร็วในการทำงานของระบบช้าลงหรือไม่เสถียร
    - บริการที่ถูกโจมตีไม่สามารถเข้าถึงได้หรือเกิดการหยุดชะงัก
  - การป้องกัน:
    - ใช้การป้องกัน DDoS จากผู้ให้บริการเช่น การกรองคำขอที่น่าสงสัย
    - ติดตั้งซอฟต์แวร์รักษาความปลอดภัยที่สามารถตรวจจับและบล็อกการโจมตี
    - ใช้เทคโนโลยีการกระจายโหลด (Load Balancing) เพื่อจัดการกับปริมาณข้อมูลที่เข้ามา
    - การทำงานร่วมกับผู้ให้บริการอินเทอร์เน็ต (ISP) เพื่อลดผลกระทบจากการโจมตี

ทำความรู้จัก
Cyberattacks (ต่อ)

- SQL Injection
  - การโจมตีที่ใช้การแทรกคำสั่ง SQL อันตรายลงไปในช่องกรอกข้อมูลหรือพารามิเตอร์ของแอปพลิเคชันเพื่อเข้าถึงหรือจัดการฐานข้อมูลโดยไม่ได้รับอนุญาต
  - วิธีการ:
    - การแทรกคำสั่ง SQL: แฮกเกอร์จะป้อนคำสั่ง SQL ลงในฟิลด์ที่ใช้กรอกข้อมูล เช่น ฟอร์มล็อกอิน หรือช่องค้นหา
    - การใช้ข้อมูลที่ไม่ผ่านการตรวจสอบ: ระบบที่ไม่ทำการตรวจสอบหรือป้องกันคำสั่ง SQL ที่ป้อนเข้ามาจะทำให้แฮกเกอร์สามารถเข้าถึงข้อมูลที่ไม่ควรเห็นหรือทำการดัดแปลงข้อมูลได้

ทำความรู้จัก
Cyberattacks (ต่อ)

- SQL Injection
    - ประเภทของ SQL Injection:
        - Error-Based SQL Injection: ใช้ข้อผิดพลาดที่เกิดจากการทำงานของฐานข้อมูลเพื่อเปิดเผยข้อมูล
        - Union-Based SQL Injection: ใช้คำสั่ง UNION SQL เพื่อรวมผลลัพธ์จากหลายคำสั่ง SQL
        - Blind SQL Injection: การใช้การสอบถามฐานข้อมูลแบบ blind เพื่อทำความเข้าใจข้อมูลที่ไม่ได้แสดงผลให้เห็นโดยตรง
    - อาการ:
        - การเข้าถึงข้อมูลที่ละเอียดอ่อน เช่น ข้อมูลผู้ใช้หรือข้อมูลทางการเงิน
        - การเปลี่ยนแปลงข้อมูลในฐานข้อมูล เช่น การลบหรือเพิ่มข้อมูล
        - ข้อผิดพลาดที่แสดงรายละเอียดเกี่ยวกับฐานข้อมูล

ทำความรู้จัก Cyberattacks (ต่อ)

- SQL Injection
  - การป้องกัน:
    - ใช้ Prepared Statements: ใช้คำสั่ง SQL ที่เตรียมไว้ล่วงหน้าเพื่อป้องกันการแทรกคำสั่ง SQL
    - ทำการตรวจสอบและกรองข้อมูล: ตรวจสอบและกรองข้อมูลที่ป้อนเข้ามาเพื่อให้แน่ใจว่าไม่มีคำสั่ง SQL ที่เป็นอันตราย
    - ใช้การเข้ารหัส: เข้ารหัสข้อมูลที่เก็บในฐานข้อมูลเพื่อลดความเสี่ยง
    - จำกัดสิทธิ์การเข้าถึงฐานข้อมูล: ใช้สิทธิ์ที่จำกัดในการเข้าถึงฐานข้อมูลเพื่อป้องกันการดัดแปลงข้อมูล

ทำความรู้จัก
Cyberattacks (ต่อ)

- Zero-day Exploit
  - การโจมตีที่ใช้ช่องโหว่ในซอฟต์แวร์หรือฮาร์ดแวร์ที่ยังไม่ถูกค้นพบหรือยังไม่มีการแก้ไข
  - วิธีการ:
    - การค้นพบช่องโหว่ใหม่: แฮกเกอร์หรือผู้โจมตีจะค้นหาช่องโหว่ที่ยังไม่มีใครรู้จัก
    - การพัฒนาและใช้งาน: สร้างโปรแกรมหรือโค้ดที่ใช้ช่องโหว่เหล่านั้นเพื่อเจาะระบบ
  - ความเสี่ยง:
    - เนื่องจากยังไม่มีการแก้ไขหรือแพตช์ ช่องโหว่นี้จึงเป็นอันตรายและยากต่อการป้องกัน
    - สามารถถูกใช้ในการโจมตีแบบต่าง ๆ เช่น การขโมยข้อมูล การควบคุมระบบ หรือการทำลายข้อมูล

ทำความรู้จัก Cyberattacks (ต่อ)

- Zero-day Exploit
  - อาการ:
    - ระบบหรือซอฟต์แวร์ทำงานผิดปกติหรือมีพฤติกรรมที่ไม่ปกติ
    - ข้อมูลสูญหายหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
    - การเข้าถึงระบบโดยไม่ได้รับอนุญาต
  - การป้องกัน:
    - อัปเดตซอฟต์แวร์อย่างสม่ำเสมอ: ตรวจสอบและติดตั้งแพตช์หรืออัปเดตที่ผู้ผลิตซอฟต์แวร์ปล่อยออกมา
    - ใช้ระบบป้องกันหลายชั้น: เช่น ไฟร์วอลล์, แอนตี้ไวรัส, และระบบตรวจจับการบุกรุก (IDS/IPS)
    - เฝ้าระวังและตรวจสอบ: ติดตามการแจ้งเตือนจากผู้ผลิตซอฟต์แวร์และองค์กรด้านความปลอดภัย
    - ฝึกอบรมพนักงาน: เพิ่มความรู้และทักษะด้านความปลอดภัยให้กับพนักงานเพื่อลดความเสี่ยงจากการถูกโจมตี

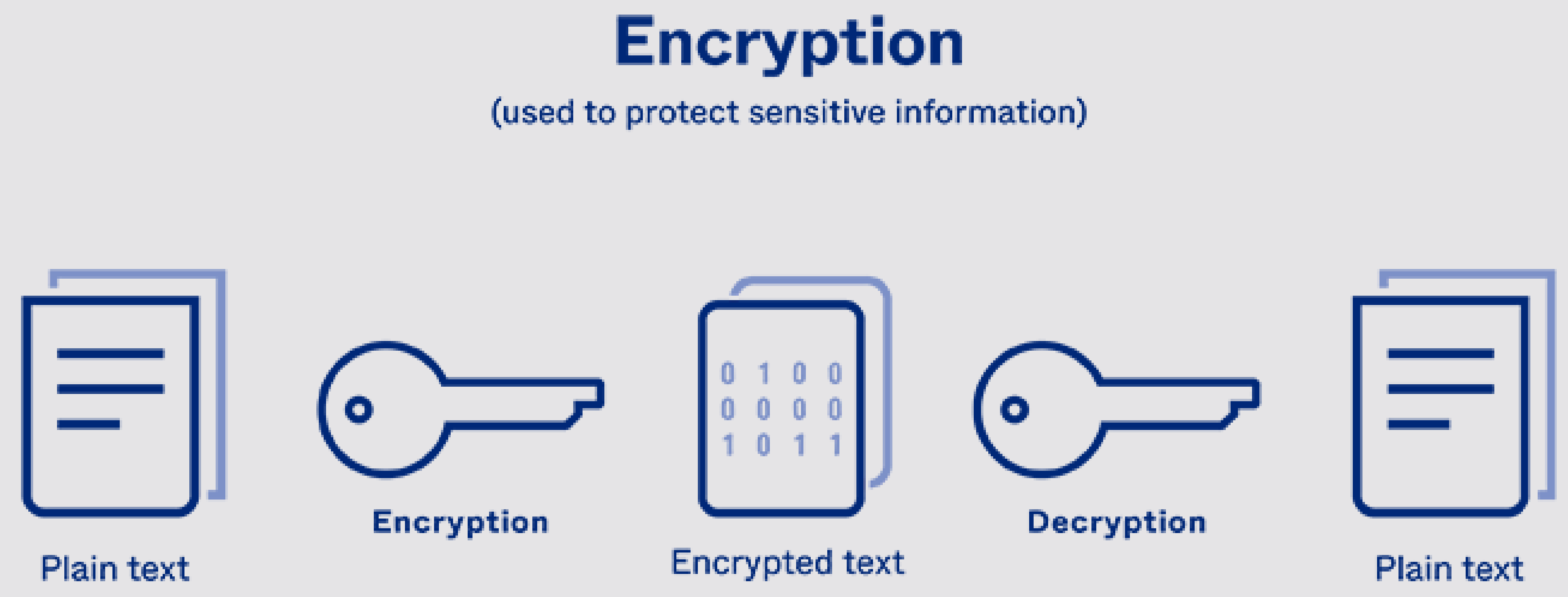
Cybersecurity Best Practices

- Use strong passwords and multi-factor authentication
- Keep software up to date
- Back up data regularly
- Educate employees about phishing
- Implement firewalls and antivirus software
- Secure your Wi-Fi network

การเข้ารหัส (Encryption)

- What is encryption?
    - กระบวนการที่ใช้ในการป้องกันข้อมูลจากการเข้าถึงที่ไม่ได้รับอนุญาต โดยการแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถเข้าใจได้ง่าย หากไม่มีการถอดรหัส (Decryption) ซึ่งเป็นกระบวนการที่ตรงกันข้าม

การเข้ารหัส (Encryption) (ต่อ)



Souce: https://www.linkedin.com/pulse/encryption-decryption-system-design-us

การเข้ารหัส (Encryption) (ต่อ)

- Types of encryption
  - การเข้ารหัสแบบสมมาตร (Symmetric Encryption)
  - การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)

การเข้ารหัส (Encryption) (ต่อ)

- การเข้ารหัสแบบสมมาตร (Symmetric Encryption)
  - การเข้ารหัสแบบสมมาตรใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัสข้อมูล ซึ่งหมายความว่าทั้งผู้ส่งและผู้รับต้องมีและรักษาความลับของกุญแจนี้ให้ดี
  - คุณสมบัติ:
    - ความรวดเร็ว: กระบวนการเข้ารหัสและถอดรหัสทำได้รวดเร็วเนื่องจากการใช้กุญแจเดียวกัน
    - การจัดการกุญแจ: การรักษาความลับของกุญแจเป็นเรื่องสำคัญมาก เนื่องจากกุญแจเดียวกันใช้ทั้งในการเข้ารหัสและถอดรหัส

การเข้ารหัส (Encryption) (ต่อ)

- การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)
  - การเข้ารหัสแบบไม่สมมาตรใช้กุญแจคู่ ซึ่งประกอบด้วย กุญแจสาธารณะ (Public Key) และ กุญแจส่วนตัว (Private Key)
  - กุญแจสาธารณะใช้ในการเข้ารหัสข้อมูล และกุญแจส่วนตัวใช้ในการถอดรหัสข้อมูล
  - คุณสมบัติ:
    - ความปลอดภัยในการจัดการกุญแจ: กุญแจสาธารณะสามารถแจกจ่ายให้กับผู้อื่นได้โดยไม่ต้องกังวลเรื่องความปลอดภัย ส่วนกุญแจส่วนตัวต้องรักษาให้เป็นความลับ
    - กระบวนการที่ช้ากว่า: การเข้ารหัสและถอดรหัสใช้ทรัพยากรมากกว่าและช้ากว่าการเข้ารหัสแบบสมมาตร

การเข้ารหัส (Encryption) (ต่อ)

- Importance of encryption in cybersecurity
    - ปกป้องความเป็นส่วนตัวของข้อมูล
        - การเข้ารหัสช่วยป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลส่วนตัว เช่น ข้อมูลการเงิน ข้อมูลทางการแพทย์ หรือข้อมูลส่วนบุคคลอื่นๆ ได้ ถ้าข้อมูลเหล่านี้ไม่ได้รับการเข้ารหัส ผู้ไม่หวังดีอาจนำไปใช้ในทางที่ผิดหรือทำลายความเป็นส่วนตัวของบุคคลได้
    - รักษาความลับของข้อมูลทางธุรกิจ
        - องค์กรธุรกิจมีข้อมูลที่มีค่ามาก เช่น แผนธุรกิจ ข้อมูลลูกค้า และข้อมูลทางการเงิน การเข้ารหัสช่วยป้องกันไม่ให้ข้อมูลเหล่านี้ถูกเข้าถึงโดยคู่แข่งหรือผู้ไม่หวังดี ซึ่งอาจนำไปสู่การสูญเสียทางธุรกิจและชื่อเสียงได้

การเข้ารหัส (Encryption) (ต่อ)

- Importance of encryption in cybersecurity
    - ป้องกันการโจมตีทางไซเบอร์
        - การเข้ารหัสช่วยป้องกันการโจมตีจากผู้ไม่หวังดีที่ต้องการดักฟังหรือแก้ไขข้อมูลที่ถูกส่งผ่านเครือข่าย การเข้ารหัสข้อมูลทำให้ผู้โจมตีไม่สามารถอ่านหรือแก้ไขข้อมูลได้ง่ายๆ
    - รับรองความถูกต้องและความสมบูรณ์ของข้อมูล
        - การเข้ารหัสร่วมกับการใช้ลายเซ็นดิจิทัล (Digital Signature) สามารถช่วยในการรับรองความถูกต้องของข้อมูลและยืนยันว่าไม่มีการแก้ไขเปลี่ยนแปลงข้อมูลตั้งแต่ต้นทางจนถึงปลายทาง
    - ปฏิบัติตามกฎหมายและข้อบังคับ
        - หลายประเทศและองค์กรมีข้อบังคับเกี่ยวกับการรักษาความปลอดภัยของข้อมูล เช่น GDPR ในสหภาพยุโรป หรือ HIPAA ในสหรัฐอเมริกา การเข้ารหัสข้อมูลเป็นหนึ่งในวิธีการที่ช่วยให้ปฏิบัติตามกฎหมายและข้อบังคับเหล่านี้ได้

การเข้ารหัส (Encryption) (ต่อ)

- Importance of encryption in cybersecurity
  - สร้างความเชื่อมั่นให้กับลูกค้าและผู้ใช้งาน
    - การใช้การเข้ารหัสข้อมูลแสดงให้เห็นถึงความใส่ใจในเรื่องความปลอดภัยของข้อมูล ซึ่งช่วยสร้างความเชื่อมั่นให้กับลูกค้าและผู้ใช้งานในการใช้บริการขององค์กร
  - ป้องกันการสูญหายของข้อมูล
    - ในกรณีที่อุปกรณ์ถูกขโมยหรือสูญหาย การเข้ารหัสข้อมูลบนอุปกรณ์นั้นๆ จะช่วยป้องกันไม่ให้ข้อมูลถูกเข้าถึงโดยผู้ไม่หวังดี

Incident Response and Management

- ขั้นตอนการเตรียมตัว (Preparation)
  - ขั้นตอนการเตรียมตัวเป็นขั้นตอนที่สำคัญที่สุด เพราะจะเป็นพื้นฐานสำหรับการตอบสนองเหตุการณ์ในอนาคต
  - ส่วนประกอบ:
    - นโยบายและขั้นตอน: การจัดทำนโยบายและขั้นตอนการตอบสนองต่อเหตุการณ์ที่ชัดเจนและครอบคลุม
    - ทีมงาน: การจัดตั้งทีมตอบสนองเหตุการณ์ (Incident Response Team) ที่มีความรู้และความสามารถ
    - การฝึกอบรม: การฝึกอบรมและทดสอบการตอบสนองเหตุการณ์ให้กับทีมงานและพนักงาน
    - เครื่องมือและทรัพยากร: การจัดหาและเตรียมเครื่องมือและทรัพยากรที่จำเป็นสำหรับการตอบสนองเหตุการณ์

Incident Response and Management (ต่อ)

- ขั้นตอนการระบุเหตุการณ์ (Identification)
  - ขั้นตอนนี้เกี่ยวข้องกับการตรวจจับและระบุเหตุการณ์ที่เกิดขึ้นว่ามีความเป็นไปได้ว่าเป็นภัยคุกคามหรือไม่
  - ส่วนประกอบ:
    - การตรวจสอบ: การตรวจสอบระบบและเครือข่ายอย่างต่อเนื่องเพื่อค้นหาสัญญาณของการถูกโจมตีหรือการเข้าถึงที่ไม่พึงประสงค์
    - การวิเคราะห์: การวิเคราะห์ข้อมูลจากระบบตรวจจับและเครื่องมือต่างๆ เพื่อยืนยันเหตุการณ์
    - การแจ้งเตือน: การแจ้งเตือนทีมตอบสนองเหตุการณ์เมื่อพบเหตุการณ์ที่น่าสงสัย

Incident Response and Management (ต่อ)

- ขั้นตอนการควบคุม (Containment)
  - การควบคุมเหตุการณ์เพื่อป้องกันการแพร่กระจายของภัยคุกคามและลดผลกระทบต่อระบบ
  - ส่วนประกอบ:
    - การควบคุมชั่วคราว: การดำเนินการทันทีเพื่อควบคุมเหตุการณ์ เช่น การตัดการเชื่อมต่อระบบที่ถูกโจมตี
    - การควบคุมระยะยาว: การวางแผนและดำเนินการเพื่อควบคุมเหตุการณ์ในระยะยาว เช่น การปรับเปลี่ยนโครงสร้างเครือข่ายหรือระบบรักษาความปลอดภัย

Incident Response and Management (ต่อ)

- ขั้นตอนการกำจัด (Eradication)
    - ขั้นตอนนี้เกี่ยวข้องกับการกำจัดภัยคุกคามออกจากระบบและแก้ไขความเสียหายที่เกิดขึ้น
    - ส่วนประกอบ:
        - การระบุสาเหตุ: การตรวจสอบและระบุสาเหตุของการโจมตีหรือการเข้าถึงที่ไม่พึงประสงค์
        - การกำจัดภัยคุกคาม: การดำเนินการเพื่อลบหรือกำจัดภัยคุกคามออกจากระบบ เช่น การลบมัลแวร์ การเปลี่ยนรหัสผ่าน
        - การแก้ไขความเสียหาย: การซ่อมแซมและฟื้นฟูระบบที่ได้รับความเสียหาย

Incident Response and Management (ต่อ)

- ขั้นตอนการกู้คืน (Recovery)
  - การนำระบบกลับมาใช้งานได้ตามปกติหลังจากเหตุการณ์ถูกควบคุมและกำจัดภัยคุกคามแล้ว
  - ส่วนประกอบ:
    - การฟื้นฟูระบบ: การนำระบบกลับมาใช้งานได้ตามปกติ เช่น การคืนค่าข้อมูลจากการสำรองข้อมูล
    - การตรวจสอบ: การตรวจสอบระบบอีกครั้งเพื่อให้แน่ใจว่าภัยคุกคามถูกกำจัดแล้วและไม่มีช่องโหว่
    - การเฝ้าระวัง: การเฝ้าระวังระบบอย่างใกล้ชิดในช่วงเวลาหลังจากการกู้คืน

Incident Response and Management (ต่อ)

- ขั้นตอนบทเรียนที่ได้เรียนรู้ (Lessons Learned)
  - การทบทวนและประเมินการตอบสนองต่อเหตุการณ์เพื่อหาข้อปรับปรุงและเพิ่มประสิทธิภาพในการตอบสนองเหตุการณ์ในอนาคต
  - ส่วนประกอบ:
    - การทบทวนเหตุการณ์: การทบทวนและวิเคราะห์เหตุการณ์ที่เกิดขึ้นโดยละเอียด
    - การประเมินผล: การประเมินประสิทธิภาพของการตอบสนองต่อเหตุการณ์และการดำเนินการที่ได้ทำ
    - การปรับปรุงแผน: การปรับปรุงแผนและขั้นตอนการตอบสนองเหตุการณ์ตามผลการทบทวน
    - การฝึกอบรมเพิ่มเติม: การฝึกอบรมเพิ่มเติมให้กับทีมงานและพนักงานตามบทเรียนที่ได้เรียนรู้

Incident Response and Management (ต่อ)

- Importance of having an incident response plan
    - การตอบสนองต่อเหตุการณ์ที่มีการวางแผนและดำเนินการอย่างมีประสิทธิภาพ จะช่วยให้องค์กรสามารถลดผลกระทบจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ได้อย่างมาก และเพิ่มความมั่นใจในความปลอดภัยของระบบและข้อมูล

THANK YOU

ดร.อรรถศิษฐ์ พัฒนะศิริ

Address มหาวิทยาลัยศรีนครินทรวิโรฒ

Email attasitp@g.swu.ac.th