



Cybersecurity and Data Protection Update for MiSSConf SP5

Thailand Understanding Thailand Cybersecurity Law/Data Protection Law and its unintended consequence.

EXECUTIVE SUMMARY

ทำความเข้าใจพ.ร.บ. องค์กรภาครัฐและเอกชนต้องเตรียมตัวอย่างไรก่อนการประกาศบังคับใช้พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

ปริญญา หอมเงenk (สุทัศน์ ณ อุยธยา)

บริษัท เอชิล โปรดักชั่นส์ จำกัด



ACIS PROFESSIONAL CENTER
YOUR SATISFACTION IS OUR PRIDE



We have been certified to

ACIS/Cybertron Privacy & Cybersecurity Research LAB

ISO 22301:2012 (BCMS)
ISO/IEC 27001:2013 (ISMS)
ISO/IEC 20000-1:2011 (IT-SMS) standards.

TOPICS

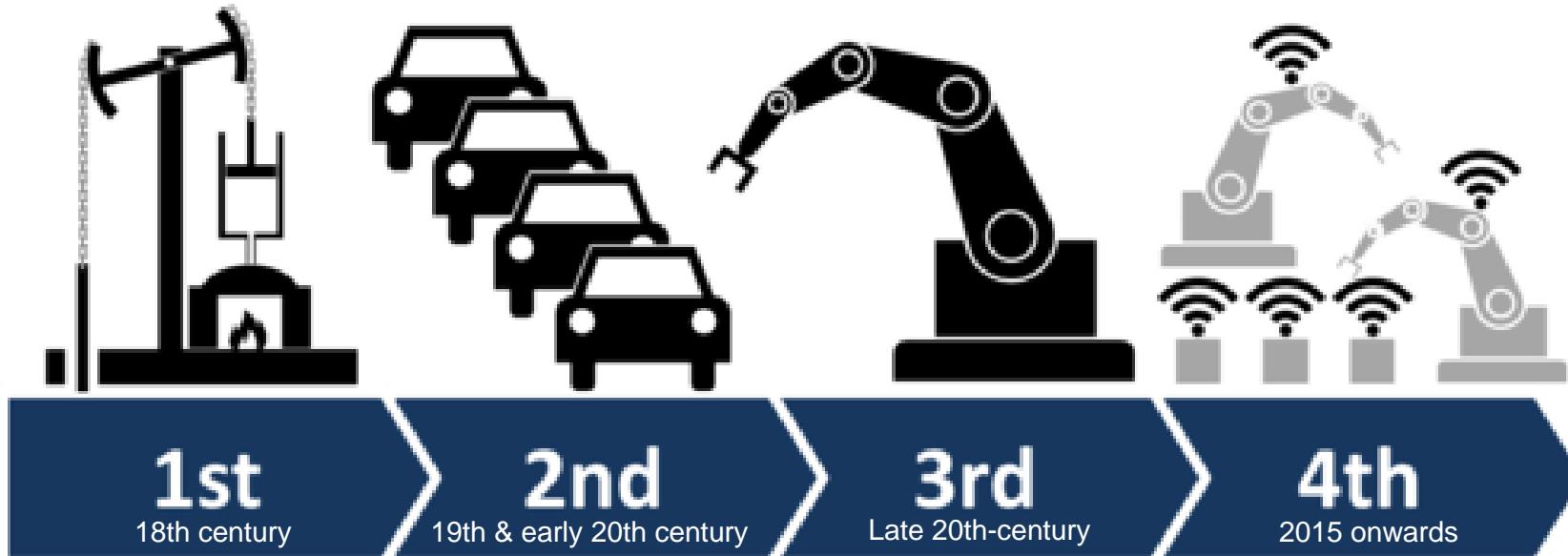
Top Ten
Cyber Threats
and Trends
for 2019

Cybersecurity Law

Personal Data Protection
(Privacy) Law

Guidance
for CI & CII

Thailand 4.0 and The fourth Industrial Revolution



Mechanisation
Water power
Steam power

Mass production
Assembly-line
Conveyor belt

Computers & Automation
The Internet
Information Age

Cyber-physical systems
Analytics
Internet of things
Artificial Intelligence
intelligent-ability

DISRUPTIVE TECHNOLOGY

THE DIGITAL TRANSFORMATION

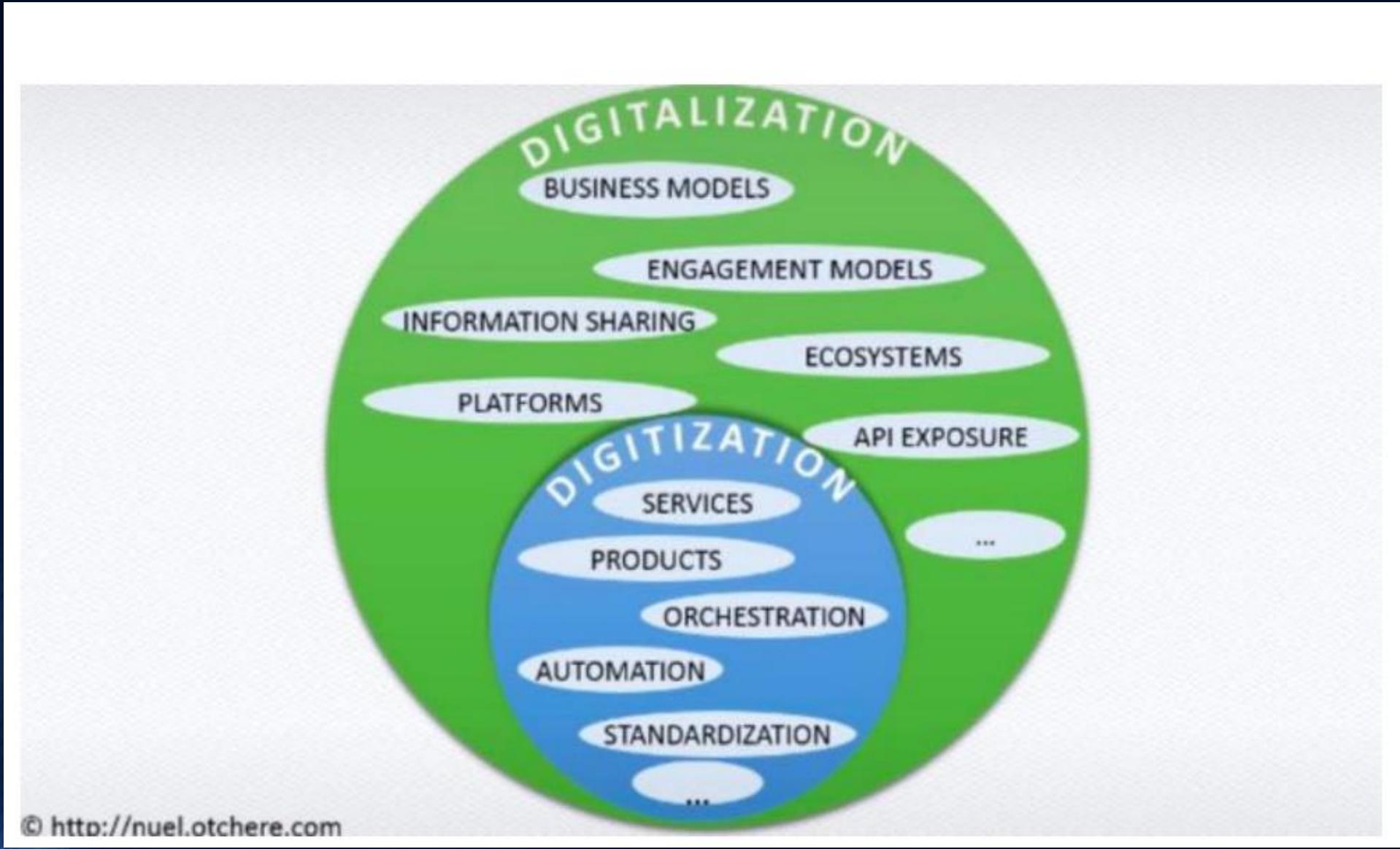
Digitization

or

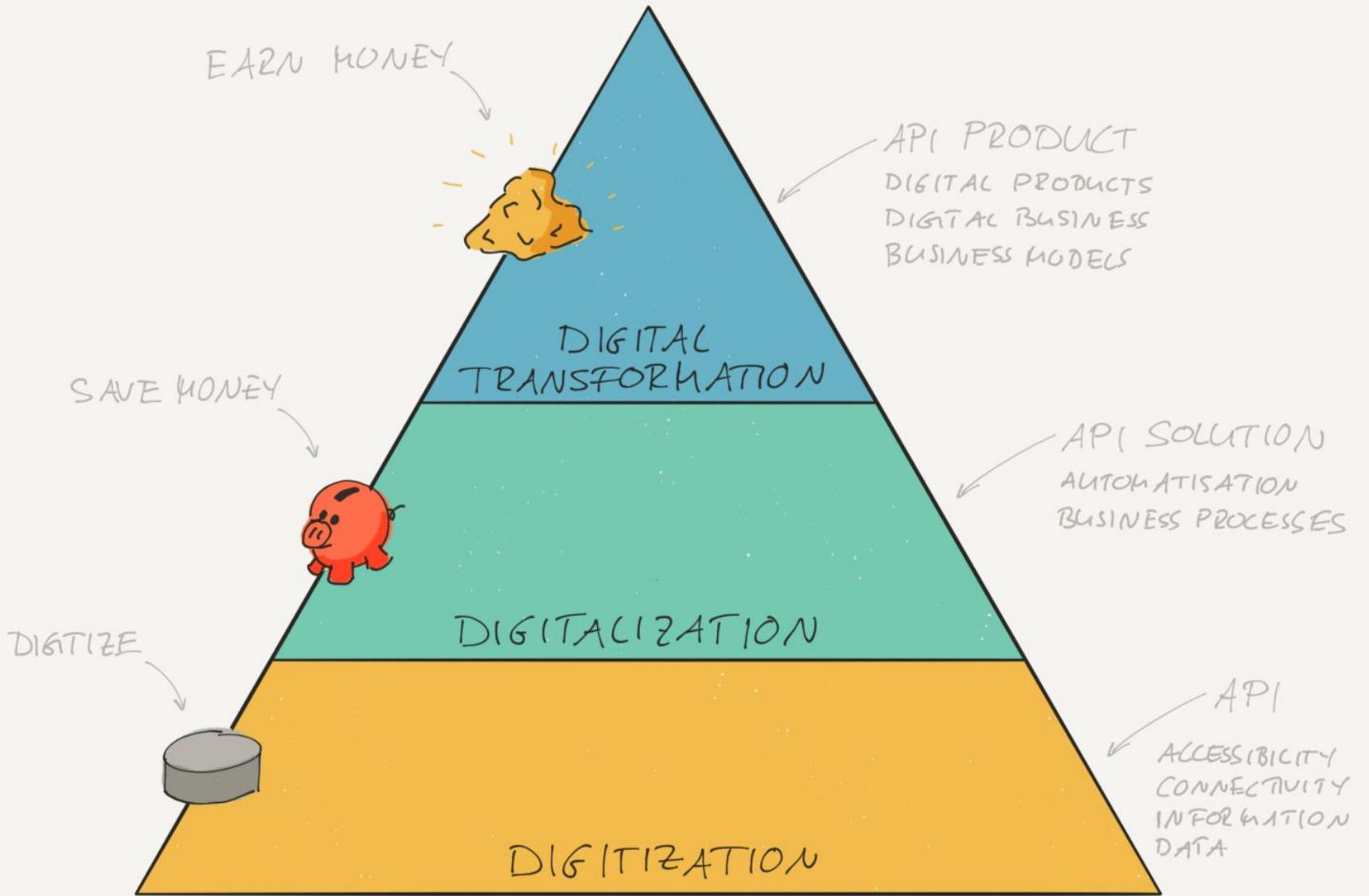
Digitalization

It defines **digitalization** as “the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business.” Similar to Wikipedia, Gartner also says, “**Digitization** is the process of changing from analog to digital form.” May 11, 2016

Source : <https://news.sap.com/>



© <http://nuel.otchere.com>



“Digital Transformation”

is the **integration** of digital **technology**

into **all areas** of a **business** resulting

in fundamental **changes** to how

businesses **operate** and how they

deliver value to customers.



DX Problems

Most organizations struggle in 4 areas



Culture

Should be an enabler
for innovation



Governance

Optimized for
Innovation



People

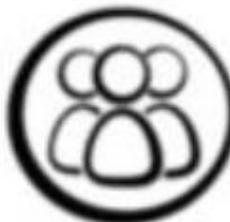
Enabling new roles
and goals



Approach

To deal with unstructured
developments

5 DOMAINS OF DIGITAL TRANSFORMATION



CUSTOMERS



VALUE



COMPETITION



INNOVATION



DATA

DOMAINS	STRATEGIC THEMES	KEY CONCEPTS
 CUSTOMERS	<i>Harness customer networks</i>	<ul style="list-style-type: none"> • reinvented marketing funnel • path to purchase • core behaviors of customer networks
 COMPETITION	<i>Build platforms, not just products</i>	<ul style="list-style-type: none"> • platform business models • (in)direct network effects • (dis)intermediation • competitive value trains
 DATA	<i>Turn data into assets</i>	<ul style="list-style-type: none"> • templates of data value • drivers of big data • data-driven decision making
 INNOVATION	<i>Innovate by rapid experimentation</i>	<ul style="list-style-type: none"> • divergent experimentation • convergent experimentation • minimum viable prototype • paths to scaling up
 VALUE	<i>Adapt your value proposition</i>	<ul style="list-style-type: none"> • concepts of market value • paths out of a declining market • steps to value prop evolution

Who should lead your digital transformation? The CEO, CIO, CMO,...?

POSTED BY :

JO AND DADO OCTOBER 29TH, 2014

LEAVE A COMMENT

IN ARTICLES

11740 VIEWS



Last month, **Harvard Business Review** published an article on why we need better managers to deal with **Digital Transformation**. In their post they mentioned several of the aspects that the digital leadership in your company needs to excel at:

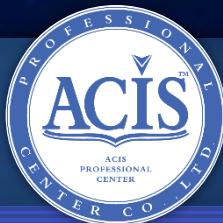
- **Creating a transformative vision** of how your firm will be different in the digital world.
- **Engaging employees** in making the vision a reality.
- Channeling an organization's energy through **digital governance**.
- **Breaking down silos** at the leadership level to drive digital transformation together.

<http://www.digitaltransformationbook.com/tag/harvard-business-review/>

Introducing COBIT 2019 – The leading framework for customising and right-sizing Enterprise Governance of I & T

Prinya Hom-anek

CISSP, CSSLP, CISA, CISM, SSCP, CFE, CBCI, CGEIT, CRISC,
(ISC)2 Asian Advisory Council Member; ISACA Thailand - Committee,
Thailand Information Security Association (TISA) – VP & Committee ,
ACIS Professional Center Co., Ltd. - President and Founder, Cybertron Co., Ltd., CEO



ACIS PROFESSIONAL CENTER
YOUR SATISFACTION IS OUR PRIDE



We have been certified to

ISO 22301:2012 (BCMS)
ISO/IEC 27001:2013 (ISMS)
ISO/IEC 20000-1:2011 (IT-SMS) standards.

ACIS/Cybertron Privacy & Cybersecurity Research LAB

IT

VS.

I & T

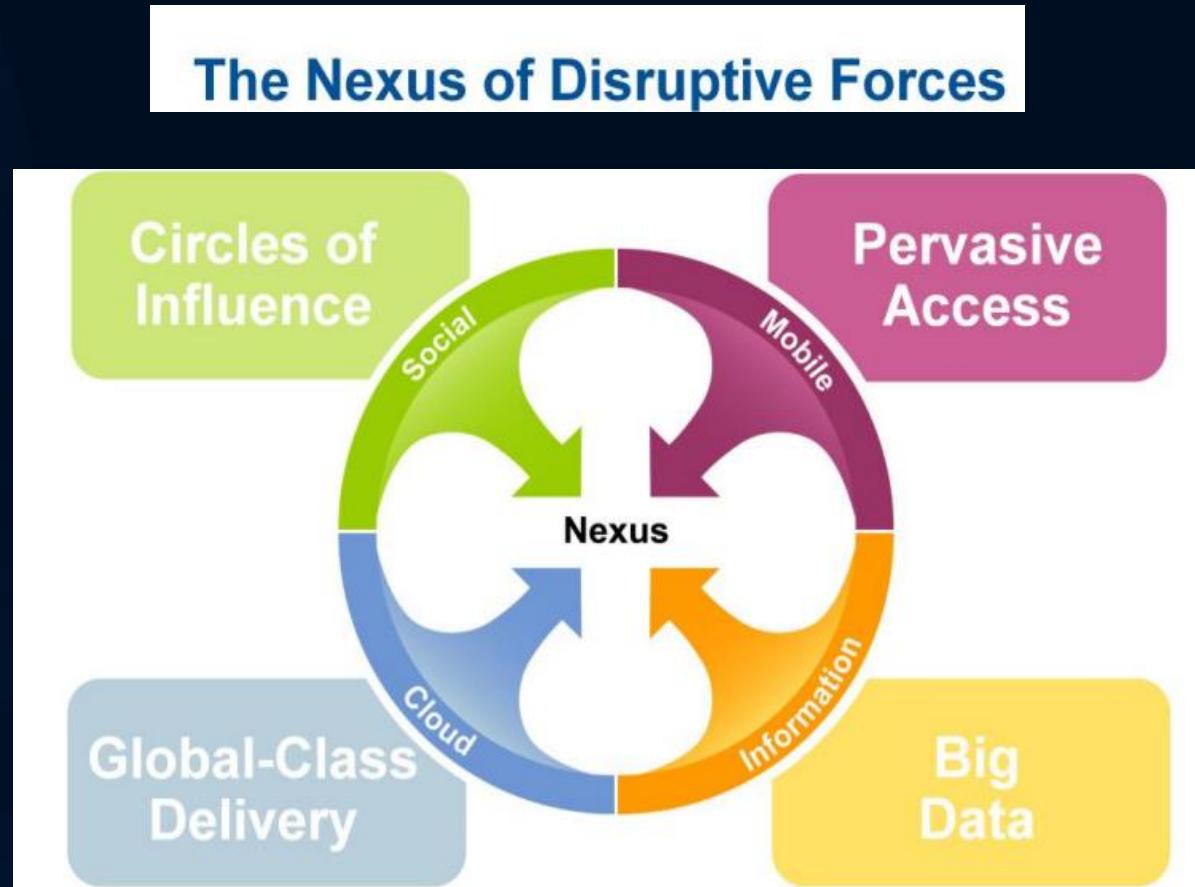
Figure 1.1—The Context of Enterprise Governance of Information and Technology



Source: De Haes, Steven; W. Van Grembergen; *Enterprise Governance of Information Technology: Achieving Alignment and Value*, Featuring COBIT 5, 2nd ed., Springer International Publishing, Switzerland, 2015, <https://www.springer.com/us/book/9783319145464>

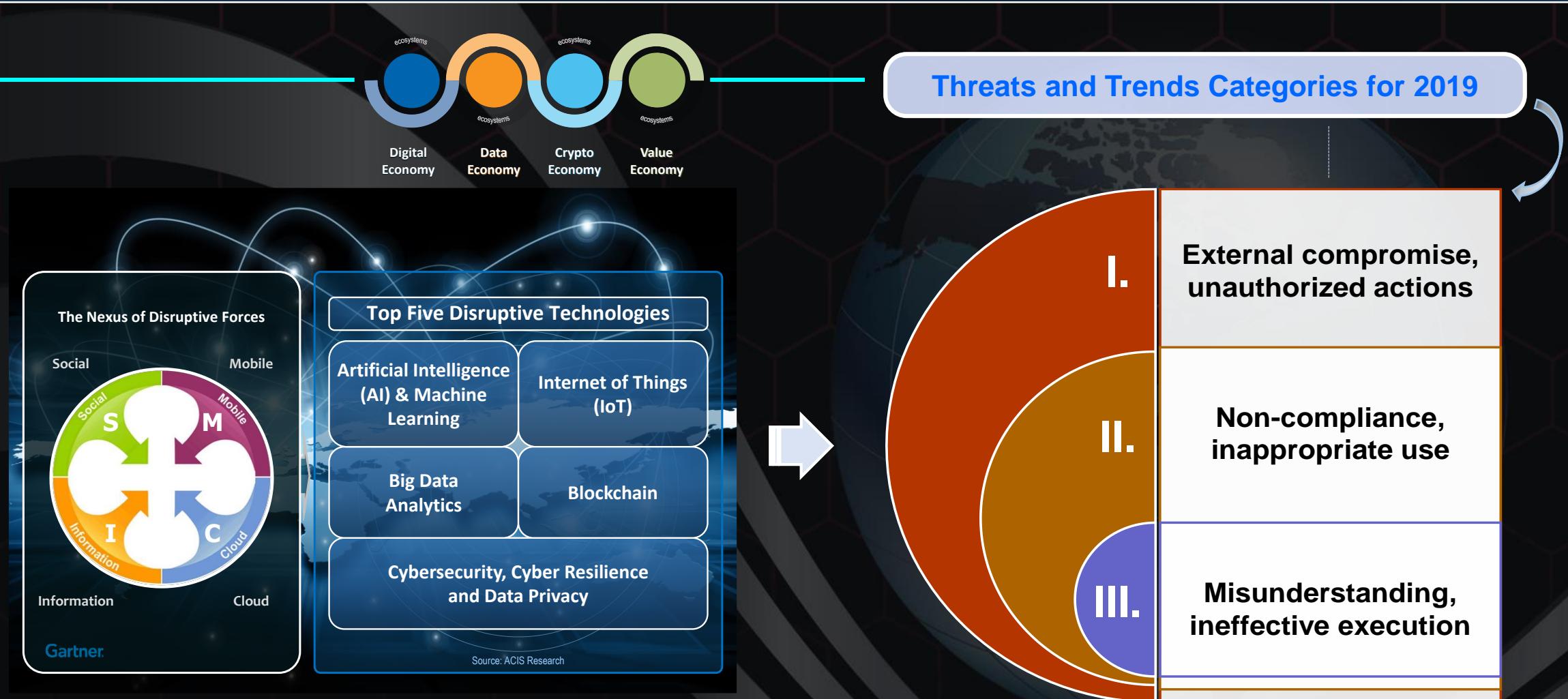
IT Trend and challenging to business

The Four IT Mega Trends : S-M-C-I Era



Source: Gartner, June 2013

Disruptive Technologies for Value Economy



Source: ACIS Research

IT-GRC, Privacy and Cybersecurity Management

Disruptive Technologies for Value Economy

Top Five Digital Disruptive Technologies

IoT (Internet
of Things)

Big Data
Analytics

AI &
Machine
Learning

Blockchain

Cybersecurity, Cyber Resilience and Data Privacy

Regulatory Compliance

Source: ACIS Research

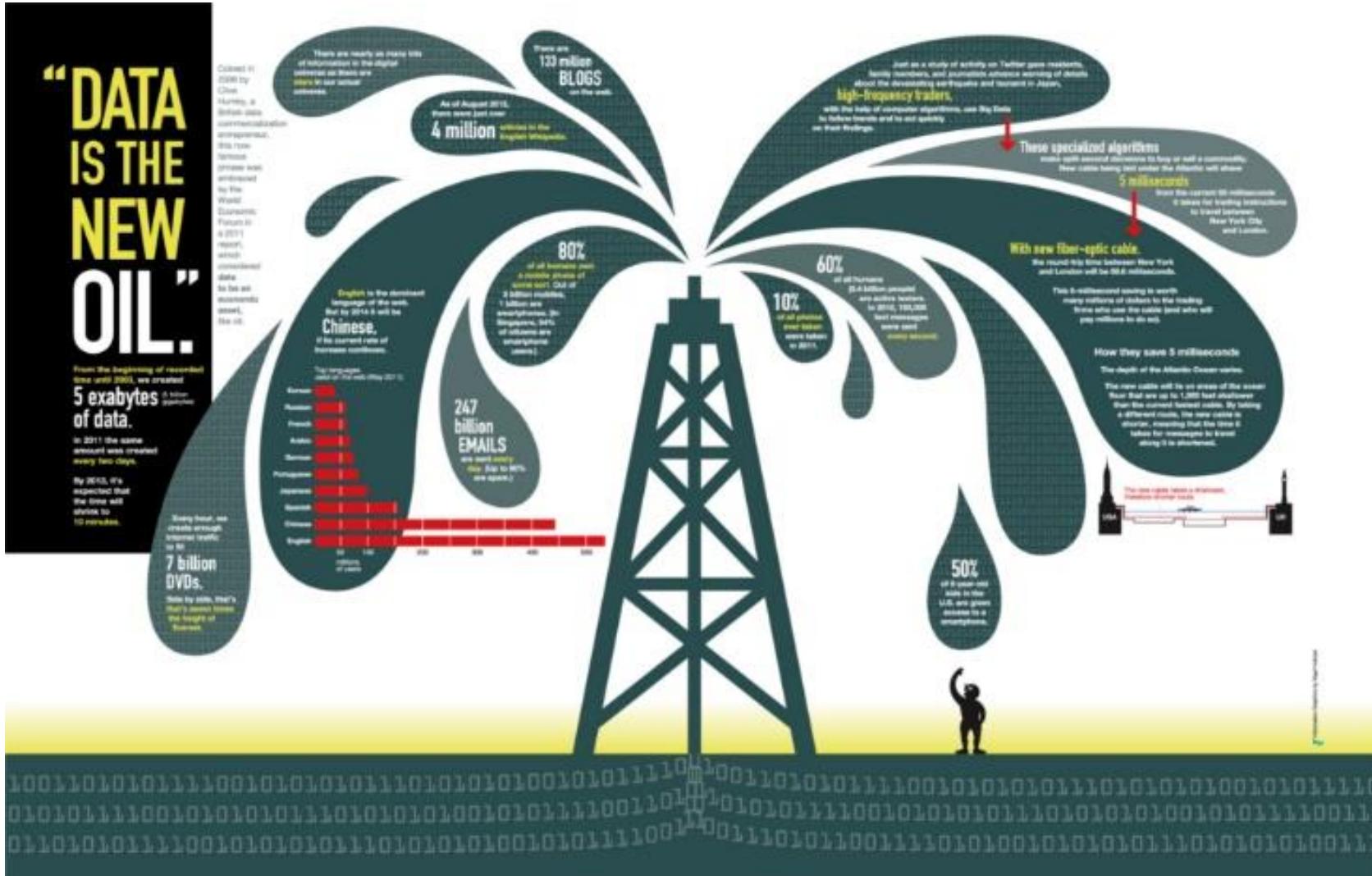
IT-GRC, Privacy and Cybersecurity Management

"About Nation Cyber Sovereignty and Hidden Privacy Threats"



David Parkins

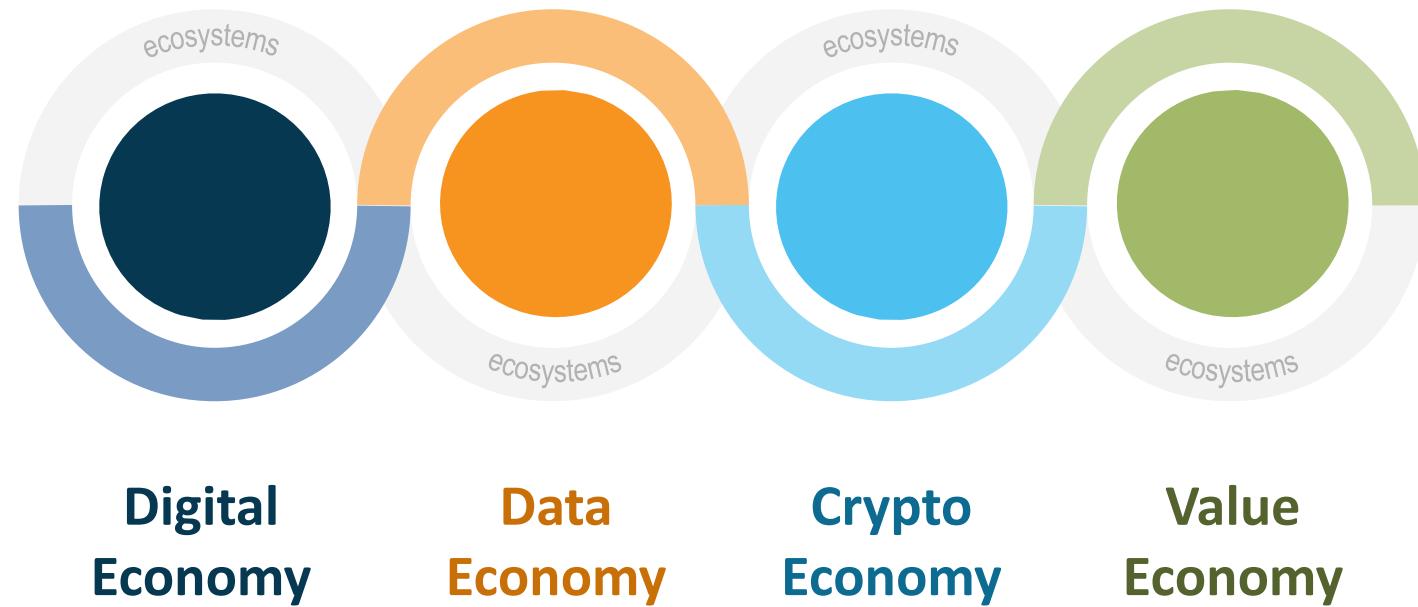
"About Nation Cyber Sovereignty and Hidden Privacy Threats"



From Digital Economy to Data Economy



Digital Economy and Ecosystems



Source: ACIS Research

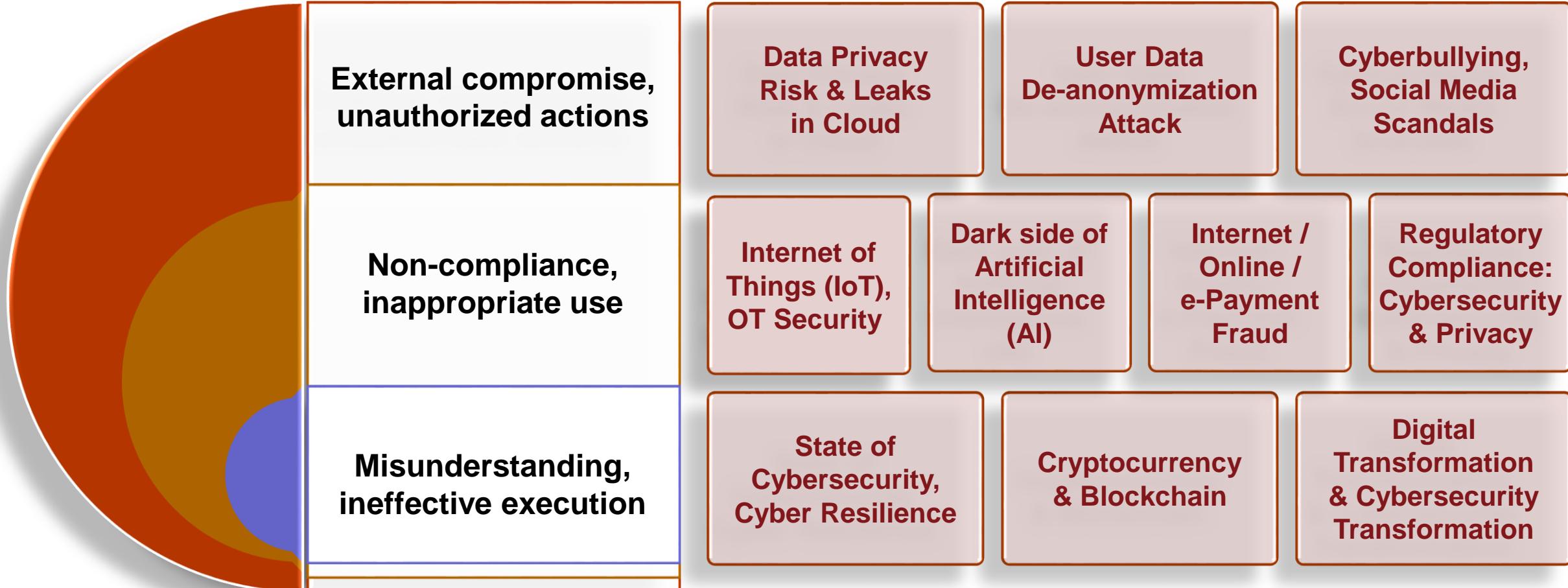


Top Ten 2019-2020

Top Ten Cyber Threats and Trends for 2019

Top Ten Cyber Threats and Trends for 2019

ACIS

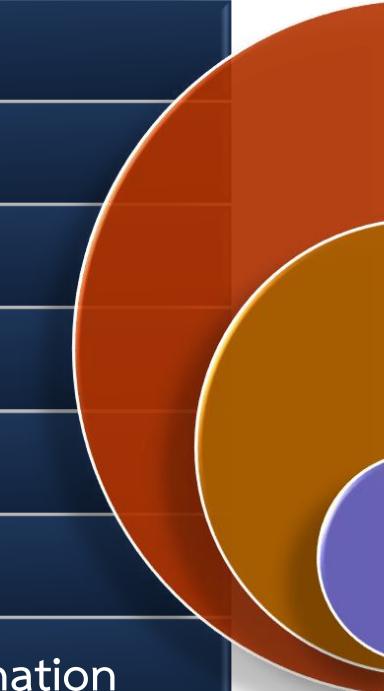


Source: ACIS Research

Top Ten Cyber Threats and Trends for 2019

ACIS

1. ภัยข้อมูลรั่วไหลจากการจัดเก็บข้อมูลในระบบคลาวด์
2. ภัยการโจมตีเอาข้อมูลส่วนบุคคลในรูปแบบ De-anonymization Attack
3. ภัยจากการกลั่นแกล้งหรือให้ร้ายป้ายสีทางโซเชียลมีเดีย (Cyberbullying)
4. ภัยจากการต่อเชื่อมอุปกรณ์กับระบบอินเทอร์เน็ตอย่างไม่ระมัดระวัง ทำให้เสี่ยงต่อการถูกโจมตีทางไซเบอร์
5. ภัยจากการนำเทคโนโลยี Artificial Intelligence (AI) มาใช้ในด้านมืด
6. ภัยจากการทุจริตในการทำธุกรรมทางอิเล็กทรอนิกส์
7. ภัยจากการท่องครั้งไม่สามารถปฏิบัติตามกฎหมายไซเบอร์และกฎหมายคุ้มครองข้อมูลส่วนบุคคล
8. ภัยจากความเข้าใจผิดในธรรมชาติของสภาวะไซเบอร์
9. ภัยจากความเข้าใจผิดในเรื่อง Cryptocurrency และ Blockchain
10. ภัยจากความไม่เข้าใจของผู้บริหารระดับสูงในเรื่อง Digital Transformation & Cybersecurity Transformation

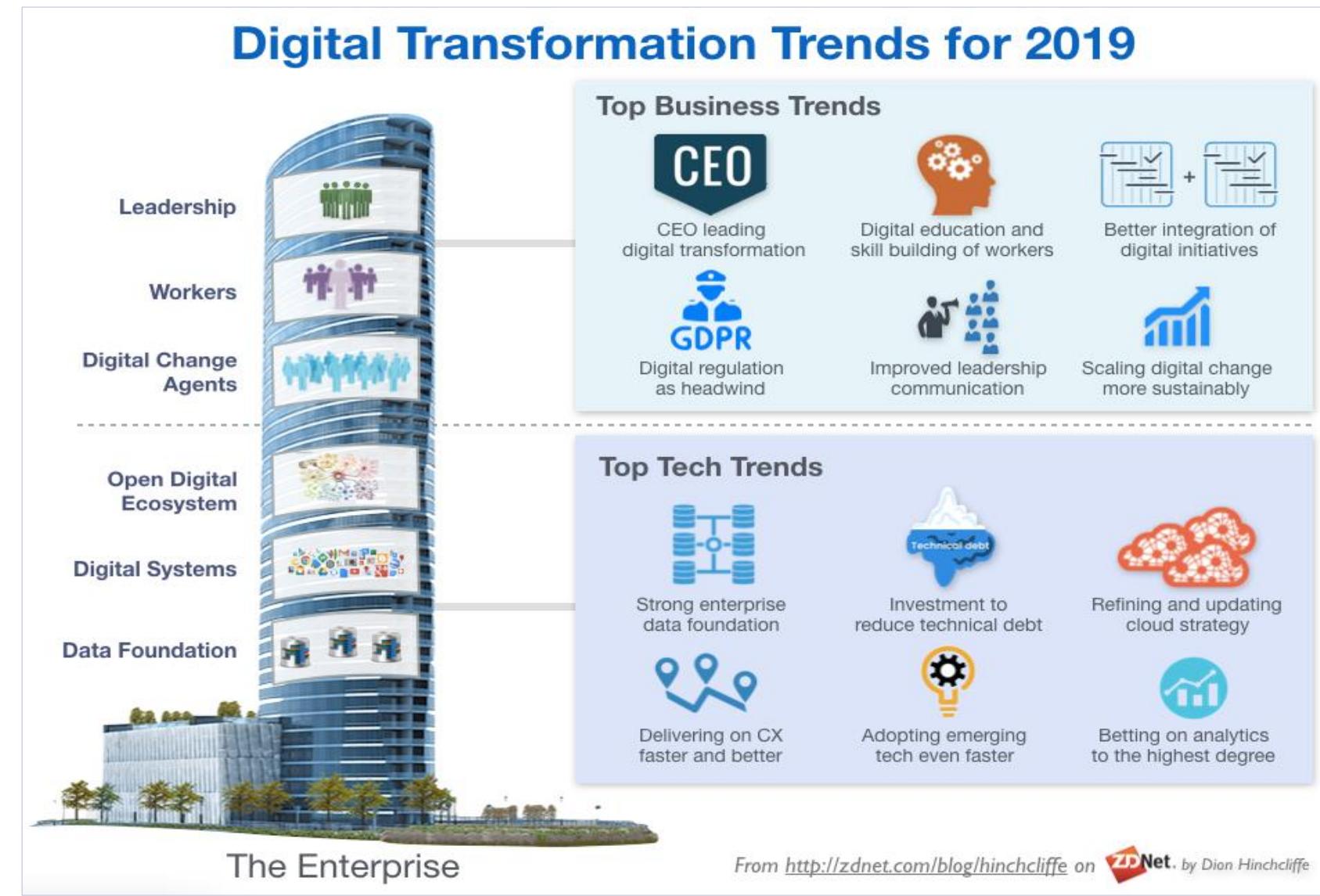


Digital Transformation Trends for 2019

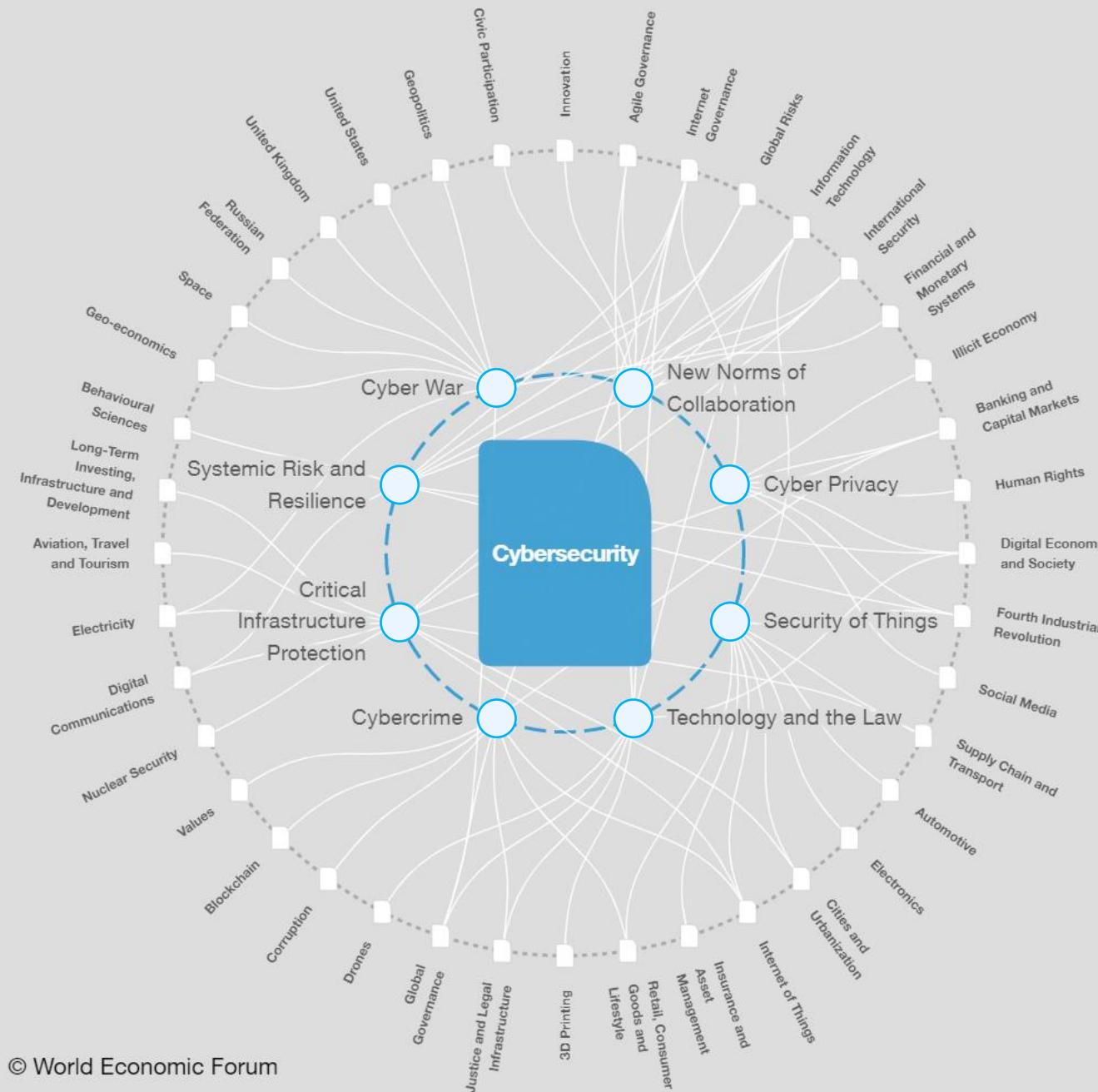
Digital Transformation: Five Domains and Key Concepts

DOMAINS	STRATEGIC THEMES
CUSTOMERS	<i>Harness customer networks</i>
COMPETITION	<i>Build platforms, not just products</i>
DATA	<i>Turn data into assets</i>
INNOVATION	<i>Innovate by rapid experimentation</i>
VALUE	<i>Adapt your value proposition</i>

Source : www.digitaltransformationplaybook.com/



Source : www.zdnet.com/article/the-biggest-lessons-learned-in-digital-transformation/



WEF Transformation Map: Cybersecurity

❖ Cybersecurity and related issues ❖

Cybercrime

Critical Infrastructure Protection

Systemic Risk and Resilience

Cyber War

New Norms of Collaboration

Cyber Privacy

Security of Things

Technology and the Law

Source: <https://toplink.weforum.org/knowledge/insight/a1Gb00000015LbsEAE/explore/summary>

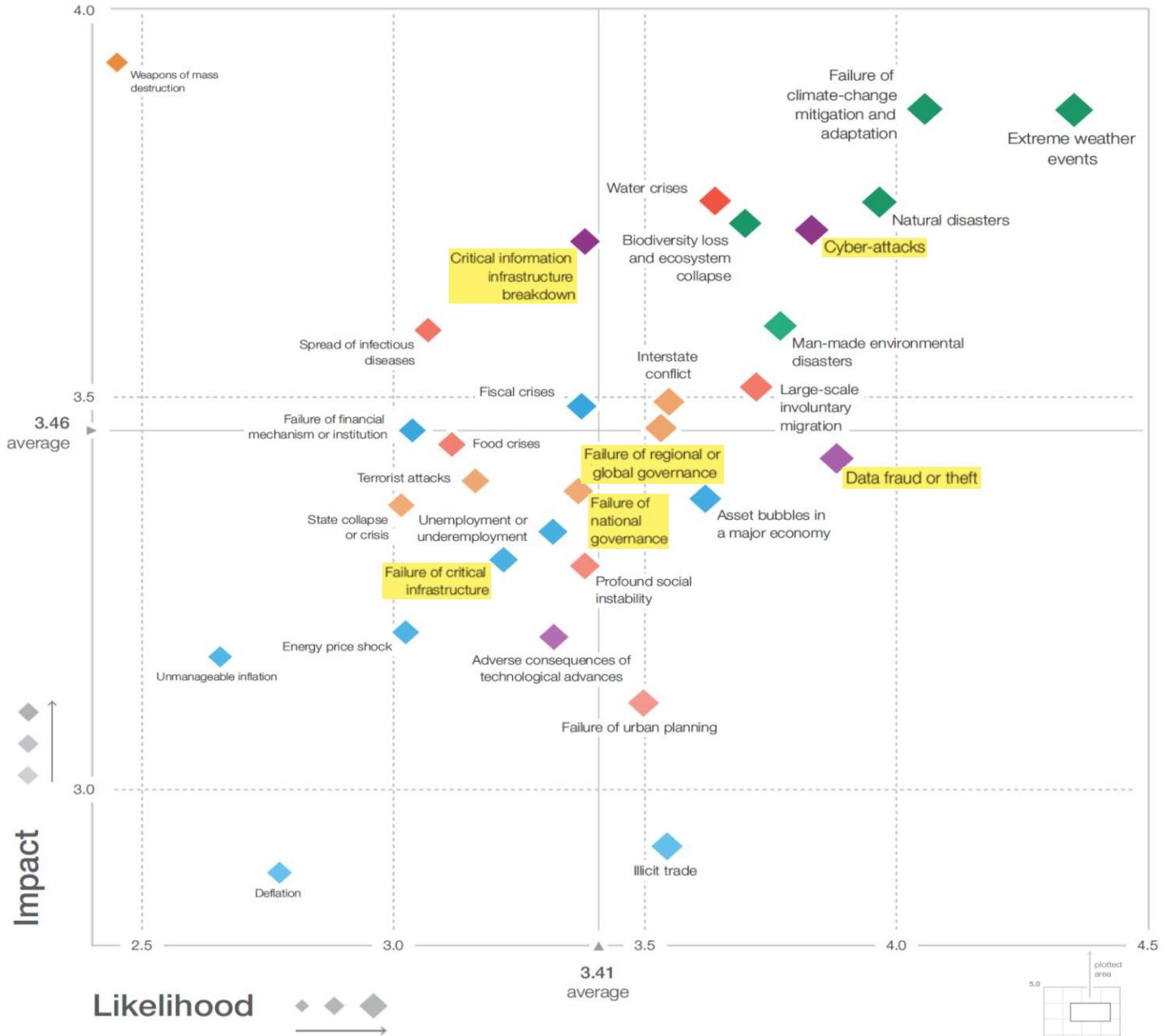
Insight Report

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The Global Risks Report 2019

14th Edition

In partnership with Marsh & McLennan Companies and Zurich Insurance Group

Source: www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

The Global Risk Outlook for 2019

THE GLOBAL RISK OUTLOOK FOR 2019

Types of Risks:



ENVIRONMENTAL



GEOPOLITICAL



SOCIETAL



TECHNOLOGICAL



ECONOMIC

Top 5 Global Risks in Terms of Impact



Top 5 Global Risks in Terms of Likelihood



SOURCE: World Economic Forum – Global Risks Report 2019

STATE OF CYBERSECURITY 2019

SECURITY SKILLS GAP BY THE NUMBERS



SKILLS GAP STILL NOT SHRINKING

69%

say their cybersecurity teams are **understaffed**.



58%

have **unfilled (open)** cybersecurity positions.



32%

say it takes six months or more to fill cybersecurity jobs at their organization.



WANTED: QUALIFIED CANDIDATES

29%

say fewer than one-quarter of job candidates are qualified for the cybersecurity position for which they applied

NEARLY 40%

say university graduates in cybersecurity are not **prepared** for the job challenges they'll face

TOP 3 REASONS CYBERSECURITY PROS ARE CHANGING JOBS

82%

Better financial incentives (salary or bonus) elsewhere

57%

Promotion and development opportunities

46%

Better work culture/environment

While these statistics may seem disheartening, they present opportunity for organizations with initiative. Today's skilled cybersecurity professionals are in high demand. Successful hiring and retention elements are attractive pay, career growth opportunities, and healthy work environments. Organizations that understand this should be able to fill open positions more quickly and better retain their current talent.

To download ISACA's 2019 State of Cybersecurity research report, visit: cybersecurity.isaca.org/state-of-cybersecurity.

CYBERSECURITY BUDGET GROWTH IS SLOWING

55%

EXPECT AN INCREASE IN CYBERSECURITY BUDGETS



1 IN 5

SAY THEIR BUDGETS ARE SIGNIFICANTLY UNDERFUNDED

DOWN 9 pts.

55%

EXPECT AN INCREASE IN CYBERSECURITY BUDGETS



1 IN 5

SAY THEIR BUDGETS ARE SIGNIFICANTLY UNDERFUNDED

THE GENDER GAP



15%

say their entire cybersecurity staff **is male**.

51%

say their cybersecurity teams have **significantly more men than women**.

79%

OF MEN SAY MEN AND WOMEN HAVE EQUAL OPPORTUNITIES for career advancement in cybersecurity roles at their organizations.

41%

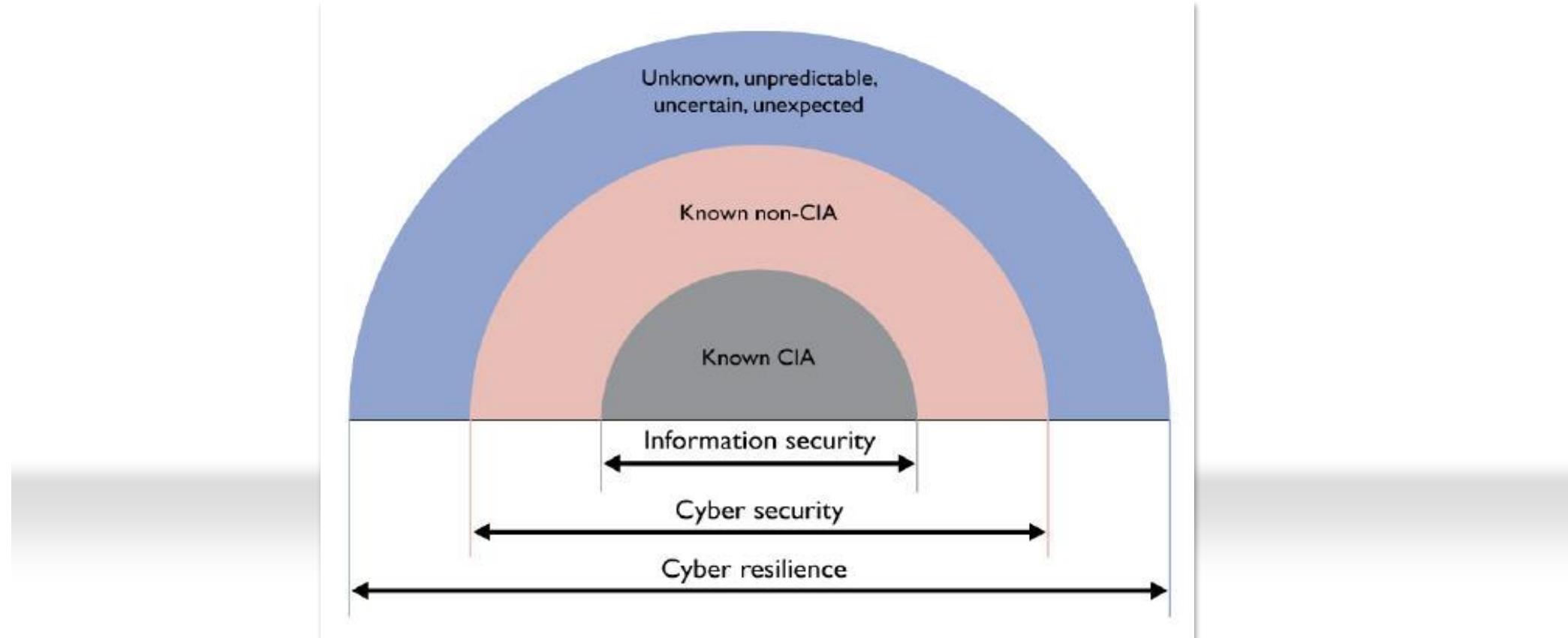
OF WOMEN AGREE. This number increases to 59% of women among organizations with diversity programs supporting women.

44%

OF ORGANIZATIONS HAVE DIVERSITY PROGRAMS that support women in cybersecurity roles.



3 Stages : Information Security, Cybersecurity and Cyber Resilience



ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยด้านต่าง ๆ กับการรับมือภัยไซเบอร์

Source: "Relationship between Cyber Resilience, Cybersecurity and Information Security, Threat Horizon 2014"



Paradigm Shift in Cybersecurity

From Preventive
To Responsive

From "Are we Secure?"
To "Are we Ready?"



SECURITY & PRIVACY

Privacy and Cybersecurity Are Converging. Here's Why That Matters for People and for Companies.



NIST Framework Core Structure

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

โครงสร้างองค์ประกอบของกรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์

Source: "Framework core structure", Framework for Improving Critical Infrastructure Cybersecurity, NIST, 12-Feb-2014

กារគាំទ្យក្នុងមាឍីកិច្ចការណ៍នៃការបង្កើតនូវការសារសុំ

Related IT & IT Security Laws: Electronic Transaction and Digital Laws

กฎหมายสำคัญด้านเทคโนโลยีสารสนเทศ/ความมั่นคงปลอดภัยสารสนเทศ

กฎหมายธุรกรรม
ทางอิเล็กทรอนิกส์

Electronic Transaction

กฎหมายการกระทำความผิด
เกี่ยวกับคอมพิวเตอร์

Computer-related Crime

กฎหมาย
ระบบการชำระเงิน

Payment System

กฎหมายดิจิทัล
เพื่อเศรษฐกิจและสังคม

Digital Economy and Society

กฎหมาย
ความมั่นคงปลอดภัยไซเบอร์

Cyber Security

กฎหมาย
คุ้มครองข้อมูลส่วนบุคคล

Personal Data Protection



กฎหมายสำคัญด้านเทคโนโลยีสารสนเทศ/ความมั่นคงปลอดภัยสารสนเทศ

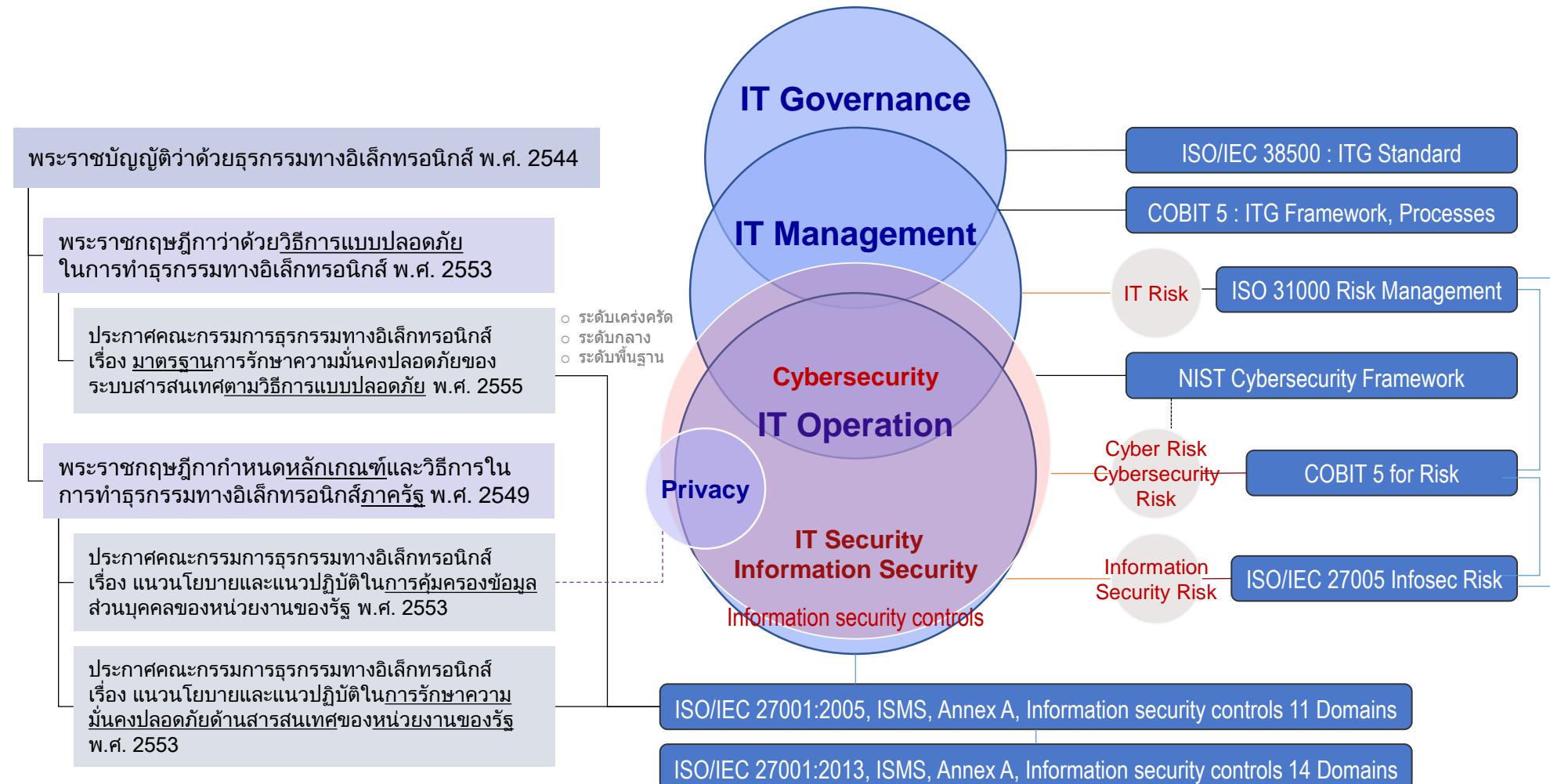
พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544		
พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551	พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 ประกาศในราชกิจจานุเบกษา 14 เมษายน 2562	พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 ประกาศในราชกิจจานุเบกษา 22 พฤษภาคม 2562
พระราชกฤษฎีกางานดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 หน่วยงานของรัฐ (ส่วนราชการ รัฐวิสาหกิจ ฯลฯ)	พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 ผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์	พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure: CI) <ul style="list-style-type: none"> ▪ ระดับเครื่องรัฐ ▪ ระดับสถาบัน ▪ ระดับพื้นฐาน
พระราชกฤษฎีกاجัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554		
พระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 ประกาศในราชกิจจานุเบกษา 14 เมษายน 2562		
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550		
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560		
พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560		
พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560		
พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562		
พระราชกฤษฎีกاجัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. 2561		
พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 2) พ.ศ. 2560		
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562		
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562		

ชุดกฎหมายดิจิทัล



Integrating IT-GRC, IT & Information Security and Cybersecurity Approach

“Regulatory Compliance” and “Standards & Best Practices”



External Regulatory Compliance

กฎหมาย
(ที่เกี่ยวข้องด้านสารสนเทศ)

พระราชบัญญัติ (พ.ร.บ.)

พระราชกฤษฎีกา (พ.ร.ก.)

ประกาศ (คณะกรรมการฯ/หน่วยงานกำกับดูแล)

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
(คธอ.)

ธนาคารแห่งประเทศไทย
(ธปท.)

ประกาศ กฎหมาย
(ของหน่วยงานกำกับดูแล)



สำนักงานคณะกรรมการนโยบายและยุทธศาสตร์
S E P O
State Enterprise Policy Office

ระบบการประเมินคุณภาพธุรกิจ
(State Enterprise Performance Appraisal: SEPA)



ธนาคารแห่งประเทศไทย
(ธปท.)



สำนักงานคณะกรรมการ
กำกับหลักทรัพย์และ
ตลาดหลักทรัพย์ (ก.ล.ต.)



สำนักงานคณะกรรมการ
กำกับและส่งเสริมการประกอบ
ธุรกิจประกันภัย (คปภ.)

ข้อตกลง สัญญา
(พันธมิตร คู่ค้า ผู้ให้บริการ)

MOU

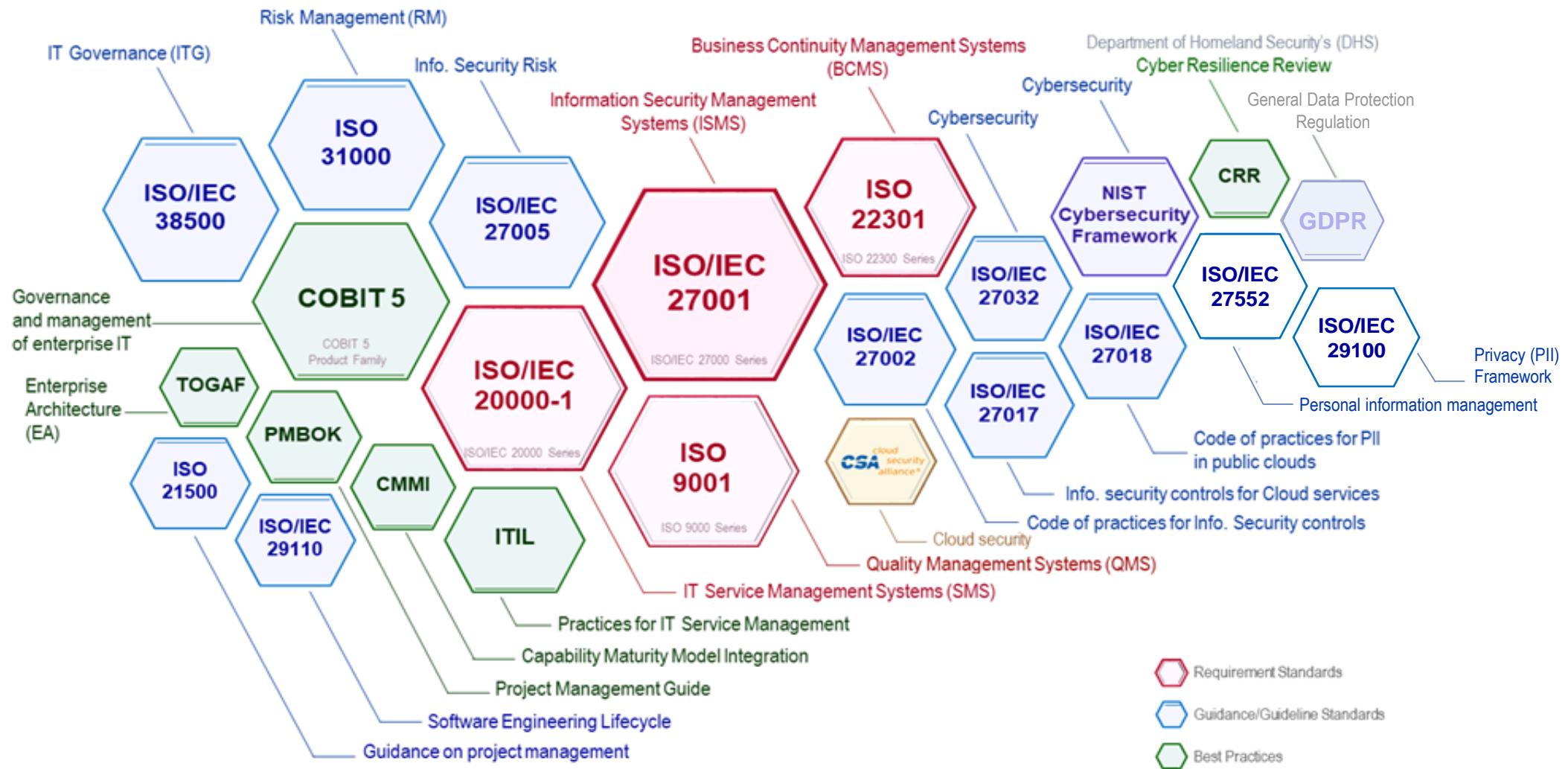
AGREEMENT

CONTRACT

Business Partnership / Service Provider / Supplier / Vendor / Contractor / Subcontractor / Seller / ...

Risk-based IT-GRC Standards and Best Practices

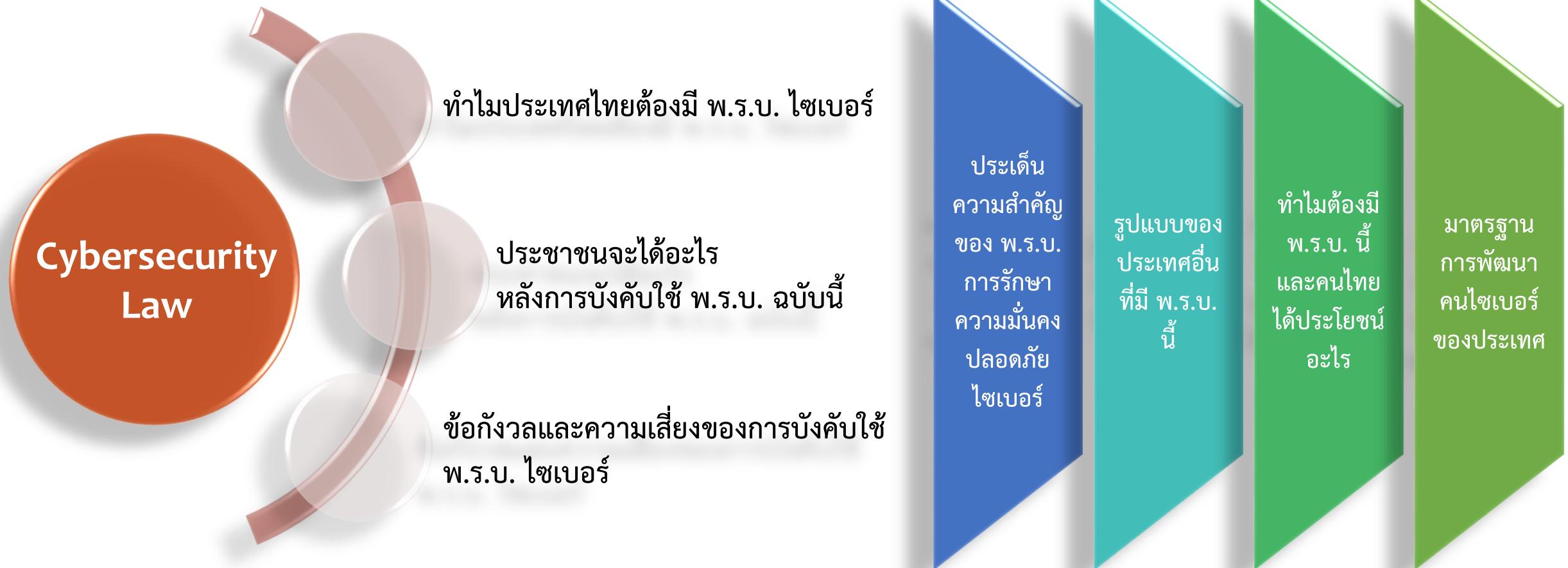
for IT-GRC, Privacy, Cybersecurity and Information Security Management



สาระสำคัญ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

Thailand Cybersecurity Laws

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์



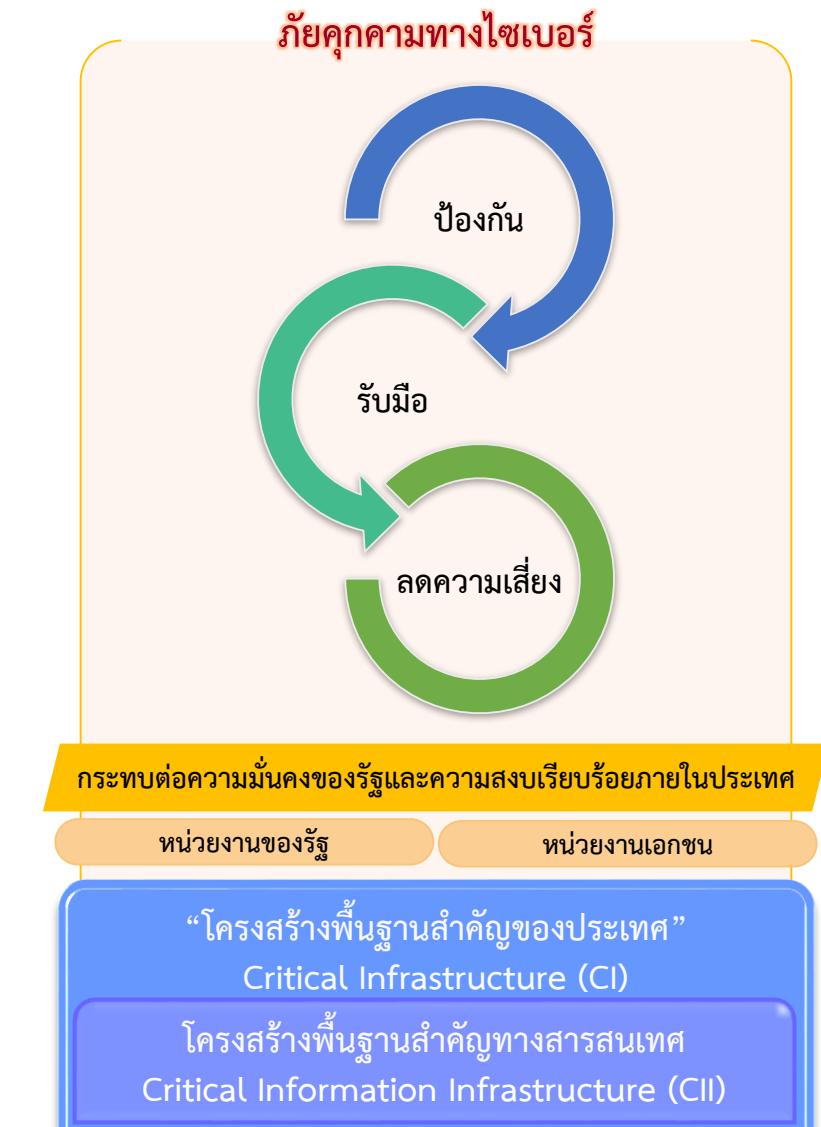
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

▶ เหตุผลและความจำเป็น

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ และเพื่อให้มี มาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

เพื่อให้สามารถป้องกันภัยคุกคามดังกล่าวได้อย่างทันท่วงที่ โดยไม่ปล่อยให้นานจนเกิดผลกระทบกับประชาชน

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป



เหตุผลและความจำเป็น : การปกป้องโครงสร้างพื้นฐานสำคัญ

หน่วยงานของรัฐ

หน่วยงานเอกชน



The European Commission Directive, 2008/214/CE set out the guidelines for EU member states to create national laws for the Protection of Critical Infrastructures

Source: <https://temigroup.wordpress.com/2014/01/24/temi-group-partners-participate-in-the-creation-of-critical-infrastructures-standard/>

เหตุผลและความจำเป็น : การปกป้องโครงสร้างพื้นฐานสำคัญ

หน่วยงานของรัฐ

หน่วยงานเอกชน

CI

“โครงสร้างพื้นฐานสำคัญของประเทศ”
Critical Infrastructure

“โครงสร้างพื้นฐานสำคัญของประเทศ” (Critical Infrastructure)

หมายความว่า บรรดาหน่วยงานหรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้น มีผลเกี่ยวนেื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณะ

ที่มา : พระราชบัญญัติวิธีการแบบปลอดภัยในการทำธุกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๓

CII

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ”
Critical Information Infrastructure

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” (Critical Information Infrastructure)

หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐ หรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานทางสารสนเทศ

ที่มา : พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

เหตุผลและความจำเป็น : การปกป้องโครงสร้างพื้นฐานสำคัญ

หน่วยงานของรัฐ

หน่วยงานเอกชน

▶ “หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ” : Critical Infrastructure (CI)

ปัญหาที่อาจเกิดขึ้นกับประชาชนในอนาคตอันใกล้ และเคยเกิดมาแล้วก็คือ

- ปัญหาน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศดังที่กล่าวมาแล้ว
 - ระบบคอมพิวเตอร์ล่ม **ใช้งานไม่ได้**
 - ปัญหาระบบสารสนเทศถูกแฮกเกอร์เจาะเข้ามาก moy ข้อมูลหรือทำลายข้อมูล **ทำให้ระบบหยุดชะงัก ไม่สามารถให้บริการประชาชนได้**

เมื่อพิจารณาให้ละเอียดพบว่า ระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญดังกล่าว ล้วนทำงานด้วยระบบคอมพิวเตอร์อยู่เบื้องหลัง

- โดยใน พ.ร.บ.ไซเบอร์ เรียก ระบบคอมพิวเตอร์นั้นว่า “โครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ” หรือ “Critical Information Infrastructure (CII)” ซึ่งถ้าโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกิดปัญหา ก็จะส่งผลกระทบต่อ การให้บริการประชาชนอย่างหลีกเลี่ยงไม่ได้

ทำให้เกิดผลกระทบต่อประชาชน

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”
Critical Information Infrastructure (CII)



- (1) ด้านความมั่นคงของรัฐ
- (2) ด้านบริการภาครัฐที่สำคัญ
- (3) ด้านการเงินการธนาคาร
- (4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- (5) ด้านการขนส่งและโลจิสติกส์
- (6) ด้านพลังงานและสาธารณูปโภค
- (7) ด้านสาธารณสุข
- (8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

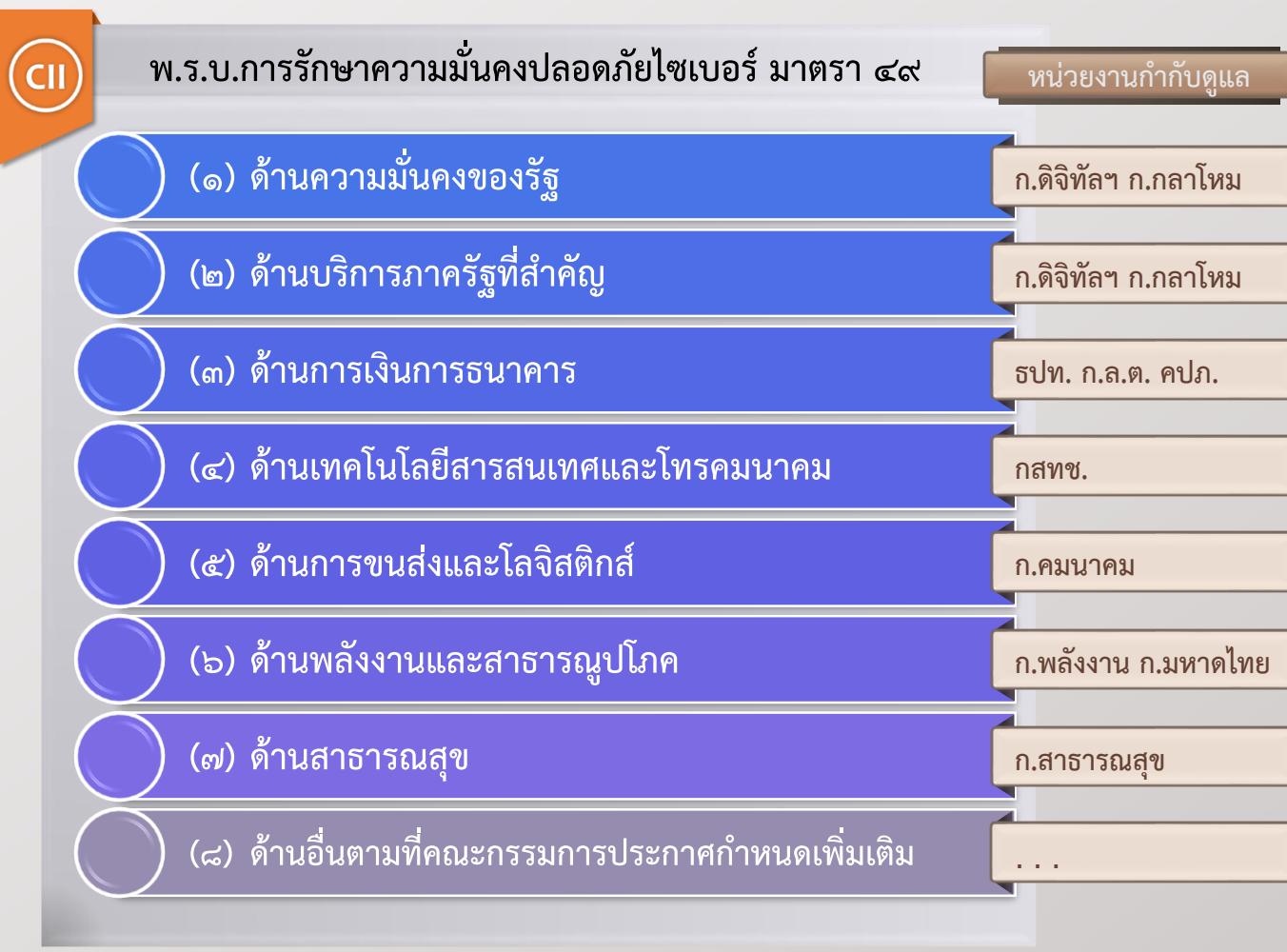
* คณะกรรมการประกาศความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Cybersecurity Law

ที่มา : พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“Critical Information Infrastructure (CII)”



มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

การพิจารณาประกาศกำหนดภารกิจหรือบริการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด โดยประกาศในราชกิจจานุเบกษา ทั้งนี้ คณะกรรมการจะต้องพิจารณาทบทวนประกาศกำหนดภารกิจ หรือบริการดังกล่าวเป็นคราว ๆ ไปตามความเหมาะสม

* (มาตรา ๕) คณะกรรมการ : คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)
National Cyber Security Committee (NCSC) นายกรัฐมนตรีเป็นประธานกรรมการ



Source: <https://temigroup.wordpress.com/2014/01/24/temi-group-partners-participate-in-the-creation-of-critical-infrastructures-standard/>

การจัดการความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ

ทั้งนี้ การตรวจสอบ การประเมินความเสี่ยง การปฏิบัติตามแนวทางปฏิบัติที่ได้มาตรฐาน และการปฏิบัติตามมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

- จำเป็นต้องมี “เจ้าภาพ” หรือ หน่วยงานที่กำหนดขึ้นมา เพื่อรับผิดชอบงานด้านไซเบอร์ในระดับชาติโดยเฉพาะ
- หน่วยงานนี้จะทำหน้าที่หลายประการด้วยกัน ตั้งแต่
 - กำหนดนโยบาย
 - กำหนดมาตรฐานขั้นต่ำ
 - ตรวจสอบ
 - ช่วยรับมือ **ภัยคุกคามทางไซเบอร์** ซึ่งกำหนดเป็น 3 ระดับ



ประชาชนจะได้อะไร หลังการบังคับใช้ พ.ร.บ. ไซเบอร์ ?

ประชาชนที่อยู่เบื้องหลังการตรากฎหมาย พ.ร.บ. ไซเบอร์ ก็คือ การทำให้น่วยงาน โครงสร้างพื้นฐานสำคัญ ของประเทศที่ไม่สามารถให้บริการประชาชนได้ สามารถดูแลตนเองด้านไซเบอร์ และ สามารถรับมือกับภัยคุกคามไซเบอร์ได้ ด้วยตนเอง เมื่อน่วยงานมีความแข็งแรง มีภูมิคุ้มกันภัยคุกคามไซเบอร์มากขึ้น ย่อมส่งผลต่อความมั่นคงโดยรวมของ ประเทศในที่สุด



1. ลดความเสี่ยงและผลกระทบจากการที่หน่วยงานโครงสร้างพื้นฐานสำคัญ ของประเทศที่ไม่สามารถให้บริการประชาชนได้



2. มีหน่วยงานหลักรับหน้าที่เป็นเจ้าภาพในการช่วยเหลือหน่วยงานโครงสร้าง พื้นฐานสำคัญของประเทศในการรับมือภัยคุกคามไซเบอร์



3. มีการสนับสนุนในการให้ความรู้แก่ประชาชนโดยทั่วไป และฝึกอบรมบุคลากร เพื่อรองรับการปฏิบัติหน้าที่ในการดำเนินงานของหน่วยงาน CII

โดย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่

- เป็นผู้คุมกฎ ผู้ตรวจสอบและประเมิน ผู้กำหนดกรอบมาตรฐานและมาตรฐานขั้นต่ำ รวมถึงประมวลแนวทางปฏิบัติ
- เป็นผู้คลักดัน ผู้สนับสนุน ให้หน่วยงานมีระเบียบวินัย มีความตั้งใจจริงในการพัฒนาบุคลากร ปฏิบัติตามประมวลแนวทางปฏิบัติ และปฏิบัติตามกรอบมาตรฐานและมาตรฐานขั้นต่ำที่ควรปฏิบัติอย่างสม่ำเสมอและต่อเนื่อง ตลอดจน
- ส่งเสริมสนับสนุนให้หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศเกิดความตระหนักรักภัยคุกคามไซเบอร์ที่จะส่งผลกระทบต่อการดำเนินชีวิตของประชาชน จึงจำเป็นต้องตรา พ.ร.บ.นี้ ขึ้นมา เพื่อเป็นประโยชน์ต่อประชาชนทั้งในปัจจุบันและอนาคตอันใกล้นี้

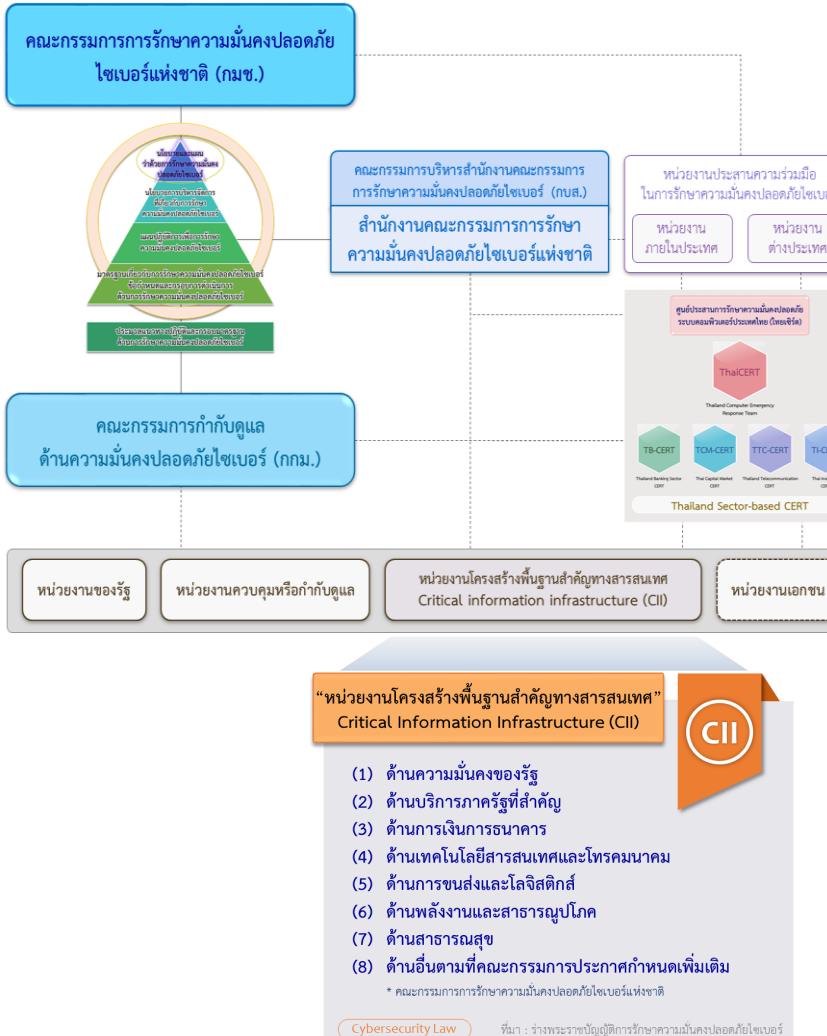
ประชาชนจะได้อะไร หลังการบังคับใช้ พ.ร.บ. ไซเบอร์ ?



1. ลดความเสี่ยงและผลกระทบจากการที่หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศที่ไม่สามารถให้บริการประชาชนได้

ลดความเสี่ยงและผลกระทบที่ไม่สามารถให้บริการประชาชนได้ ซึ่งทำให้ประชาชนเสียโอกาส เสียเวลา และอาจมีผลกระทบไปถึงการเสียทรัพย์ หรือเสียชีวิต หากภัยคุกคามไซเบอร์นั้นส่งผลกระทบในวงกว้างระดับประเทศ
เนื่องจากหลังการบังคับใช้ พ.ร.บ.ไซเบอร์ ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ จะต้องปฏิบัติตาม **ประมวลแนวทางปฏิบัติ** และมาตรฐานขั้นต่ำ ที่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กำหนด มีการตรวจสอบ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้แน่ใจว่าระบบสามารถให้บริการได้อย่างต่อเนื่อง ไม่ทำให้ประชาชนเดือดร้อน

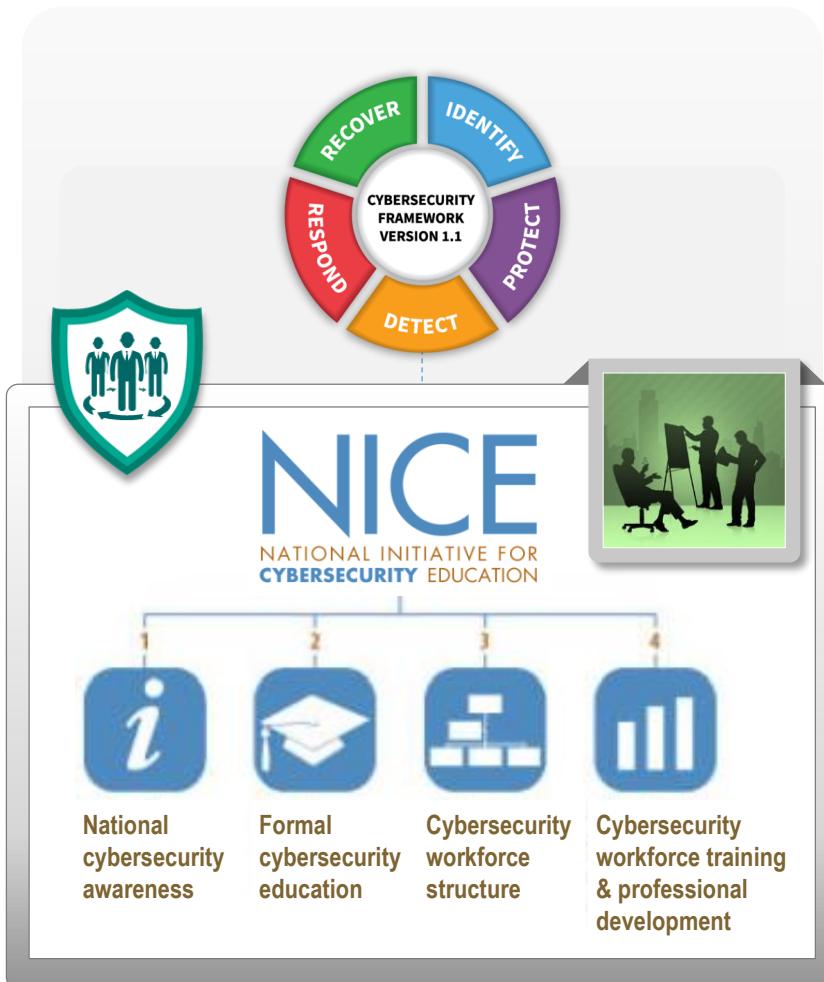
ประชาชนจะได้อะไร หลังการบังคับใช้ พ.ร.บ. ไซเบอร์ ?



2. มีหน่วยงานหลักรับหน้าที่เป็นเจ้าภาพในการช่วยเหลือหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศไทยในการรับมือภัยคุกคามไซเบอร์

แต่เดิมเวลาที่เกิด **เหตุการณ์ไม่สงบ** กับหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศไทย เช่น สนามบิน ธนาคาร ระบบไฟฟ้า-ประปา ระบบโทรศัพท์ ระบบอินเทอร์เน็ต ที่ผ่านมาเมื่อเกิดเหตุการณ์ระบบล่มไม่สามารถทำงานได้ หรือ มีเหตุการณ์ถูกโจมตีจากแฮกเกอร์ รวมทั้งการขโมยข้อมูลจากการทั้งภาครัฐและเอกชน ประเทศไทยของเราไม่เคยมีหน่วยงานที่เป็นเจ้าภาพอุบัติเหตุสัมภารณ์นักข่าว หรือทำหน้าที่รับภัยคุกคามไซเบอร์ดังกล่าว แต่เป็นไปในลักษณะที่เรียกว่า “**ต่างคนต่างทำ เท่าที่กำลังจะมี**” หลังจาก พ.ร.บ.ไซเบอร์ มีผลบังคับใช้แล้ว ประเทศไทยของเราจะมีหน่วยงานภาครัฐ ได้แก่ **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ** จะเข้ามารับหน้าที่เป็นเจ้าภาพในการช่วยเหลือหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศไทยในการรับมือภัยคุกคามไซเบอร์ ดังกล่าว

ประชาชนจะได้อะไร หลังการบังคับใช้ พ.ร.บ. ไซเบอร์ ?



- มีการสนับสนุนในการให้ความรู้แก่ประชาชนโดยทั่วไป และฝึกอบรมบุคลากรรองรับการปฏิบัติหน้าที่ในการดำเนินงานของหน่วยงาน CII

เนื่องจากวัตถุประสงค์ในการตรา พ.ร.บ.ไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจจะกระทบต่อการดำเนินชีวิตของประชาชนไปจนถึงความมั่นคงของรัฐ นับเป็นเรื่องใหม่สำหรับทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน และภาคประชาชน จึงมีความจำเป็นที่ต้องจัดให้มีการสนับสนุนในเรื่อง การให้ความรู้แก่ประชาชนโดยทั่วไป และ การฝึกอบรมบุคลากร เพื่อให้รองรับการปฏิบัติหน้าที่ทั้งนี้ เพื่อให้การดำเนินงานของ หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศไทยสามารถให้บริการประชาชนอย่างต่อเนื่อง

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๓ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่และอำนาจ ดังต่อไปนี้

(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ในการกำหนดกรอบมาตรฐานตามวรคหนึ่ง (๔) ให้คำนึงถึง **หลักการบริหารความเสี่ยง** โดยอย่างน้อยต้องประกอบด้วย **วิธีการและมาตรการ** ดังต่อไปนี้

(๑) การ**ระบุความเสี่ยง**ที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการ**ป้องกันความเสี่ยง**ที่อาจจะเกิดขึ้น

(๓) มาตรการ**ตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์**

(๔) มาตรการ**เชิงเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์**

(๕) มาตรการรักษาและ**ฟื้นฟูความเสียหาย**ที่เกิดจากภัยคุกคามทางไซเบอร์



NIST Cybersecurity Framework

Source: "NIST Framework for improving critical infrastructure cybersecurity", www.nist.gov/

Functions

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Cybersecurity Framework (CSF) Core Functions:

Identify—Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.

Protect—Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond—Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

5 ข้อกังวลและความเสี่ยงของการบังคับใช้ พ.ร.บ. ไซเบอร์

1. การประชาสัมพันธ์จากทางภาครัฐต้องทำอย่างต่อเนื่อง

เหตุผลก็คือ พ.ร.บ. ไซเบอร์ ถือว่าเป็นของใหม่สำหรับประชาชน เพราะมีแนวทางในการตรวจสอบและประเมินความเสี่ยง ป้องกันก่อนภัยคุกคามไซเบอร์จะมีผลกระทบ และ ยังรวมถึง เรื่องการรับมือผลกระทบที่เกิดขึ้นจากภัยคุกคามไซเบอร์ที่อุบัติขึ้นแล้ว จึงจำเป็นต้องให้ความรู้และปรับเปลี่ยนแนวคิดในรูปแบบเดิม ๆ กัน พอกสมควร

ผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
Critical Information Infrastructure (CII)

Cybersecurity
Mindset

“Are we ready?”
“Are we secure?”

ความรู้
ความเข้าใจ

การประเมินความเสี่ยง การป้องกัน
ก่อนภัยคุกคามไซเบอร์จะมีผลกระทบ

Professional
Development
(Organizations
&
Certifications)

Education

Specialists
& Professionals

Training

Functional Roles
& Responsibilities

Awareness Training

Security Basics
& Literacy

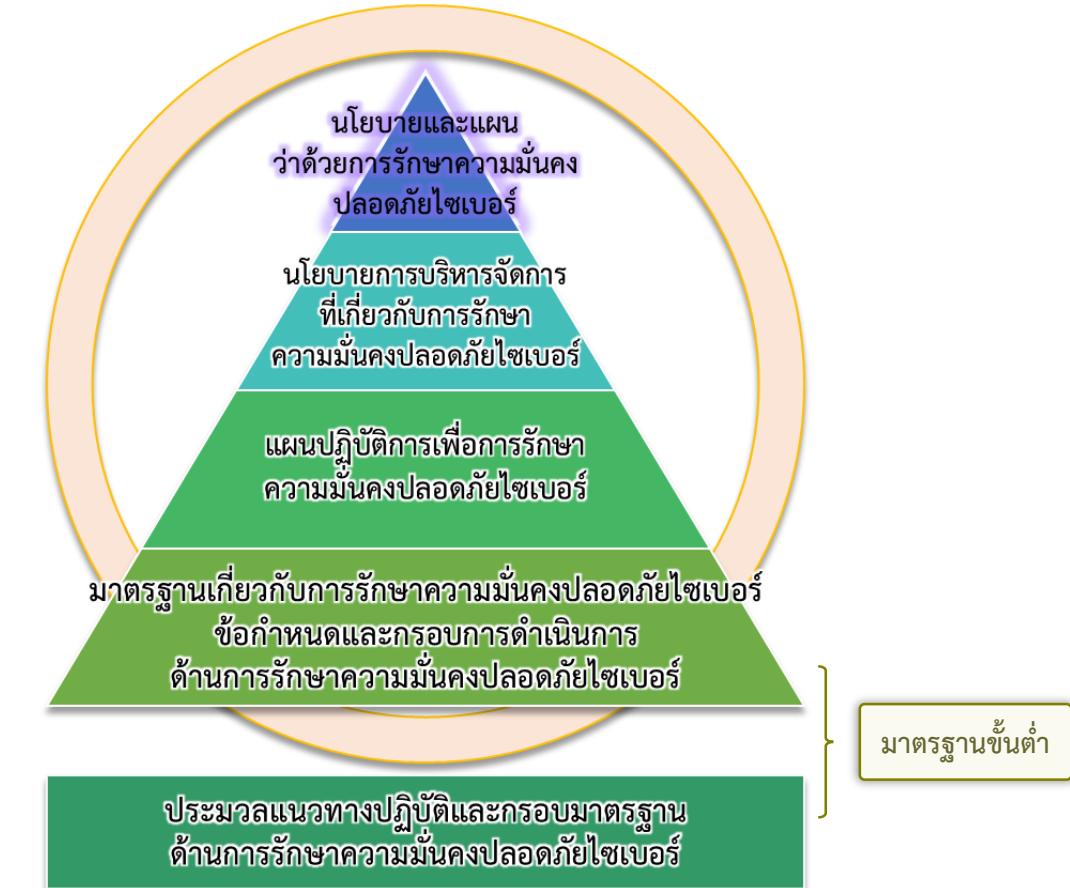
Awareness

Security Awareness
for All Users

5 ข้อกังวลและความเสี่ยงของการบังคับใช้ พ.ร.บ. ไซเบอร์

2. การพัฒนากฎหมายลูก ของ พ.ร.บ. ไซเบอร์

การพัฒนากฎหมายลูก ประกาศสำนักงานฯ เพื่อการบังคับใช้จริงภาคปฏิบัติ ต้องทำด้วยความรู้ความเข้าใจ ผู้พัฒนาควรมีความเข้าใจอย่างลึกซึ้ง มีประสบการณ์เข้าใจสภาวะไซเบอร์ในระดับหนึ่ง เพื่อไม่ให้เกิดปัญหาในทางปฏิบัติจริงกับหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศไทย



5 ข้อกังวลและความเสี่ยงของการบังคับใช้ พ.ร.บ. ไซเบอร์

3. การให้ความรู้ความเข้าใจและการพัฒนาศักยภาพ

การให้ความรู้ความเข้าใจกับประชาชนและการพัฒนาศักยภาพบุคลากร
การพึ่งพาตนเองของบุคลากรที่ต้องปฏิบัติหน้าที่ตาม พ.ร.บ. ฉบับนี้
ต้องให้ความสำคัญเป็นอันดับต้น ๆ



Table 1: Function and Category Unique Identifiers			
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
		DE.RP	Response Planning
RS	Respond	RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
		RC.RP	Recovery Planning
RC	Recover	RC.IM	Improvements
		RC.CO	Communications



5 ข้อกังวลและความเสี่ยงของการบังคับใช้ พ.ร.บ. ไซเบอร์

4. การสื่อสารและทำความเข้าใจกับผู้บริหารระดับสูง

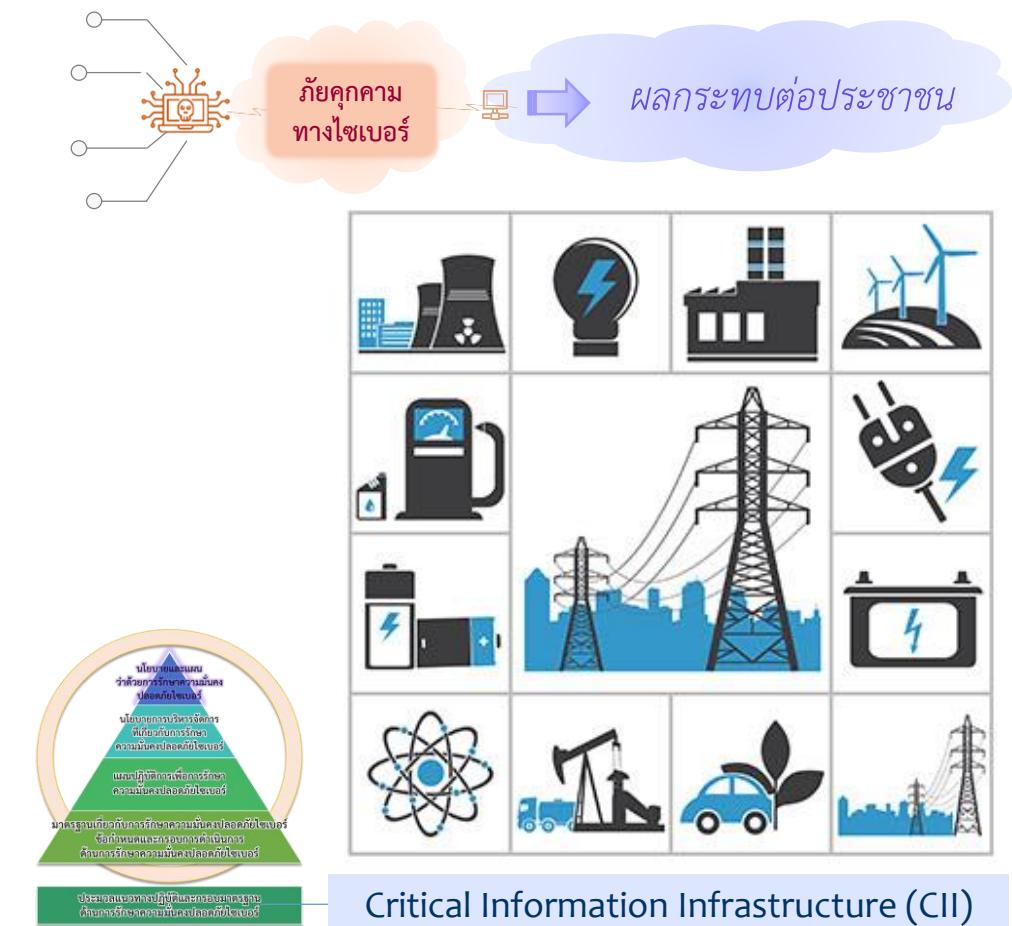
การสื่อสารและทำความเข้าใจกับผู้บริหารระดับสูงในหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศไทย ให้ทราบที่มาที่ไปของ พ.ร.บ. และตระหนักถึงผลกระทบต่อประชาชนจากภัยคุกคามทางไซเบอร์ ต้องทำอย่างจริงจังและต่อเนื่อง

The Real Meaning of Cybersecurity

Cybersecurity is “A Full Time Activity”

Cybersecurity is “A Business Imperative”

Cybersecurity is “An Executive-Level Concern”



5 ข้อกังวลและความเสี่ยงของการบังคับใช้ พ.ร.บ. ไซเบอร์

5. การคัดเลือกรัฐธรรมนูญและการพนักงานเจ้าหน้าที่

การคัดเลือกที่เป็นธรรมจากคุณสมบัติที่เหมาะสมของพนักงานเจ้าหน้าที่ ตลอดจนคณะกรรมการผู้ทรงคุณวุฒิ และเลขานุการของสำนักงานฯ ต้องทำด้วยความโปร่งใส ตรวจสอบได้ และคัดคนที่มีความรู้ความสามารถ มีประสบการณ์ ที่สำคัญมีทัศนคติที่ดี มีความซื่อสัตย์สุจริต และความเสียสละ ในการทำงานภาครัฐที่มีความสำคัญต่อประเทศชาติและประชาชน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พนักงานเจ้าหน้าที่

เลขานุการ

เลขานุการฝ่ายอัยยวัฒน์ตามแบบที่กำหนดไว้ เลขานุการซึ่งพ้นจากตำแหน่งตาม วาระอาจได้รับแต่งตั้งอีกได้ แต่ต้องไม่เกินสองวาระ

ผู้ช่วยรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้ พิจารณาแต่งตั้งจาก ผู้มีความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ + ระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามที่คณะกรรมการ (กมช.) ประกาศกำหนด + บัตรประจำตัวพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่ กกม. ประกาศกำหนด

คณะกรรมการ
การรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ (กมช.)

คณะกรรมการกำกับดูแลด้าน
ความมั่นคงปลอดภัยไซเบอร์
(กกม.)

สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์ (กบส.)

นายรัฐมนตรี เป็นประธานกรรมการ
กรรมการโดยตำแหน่ง จำนวน 6 คน
+ กรรมการผู้ทรงคุณวุฒิ *
จำนวนไม่เกิน 7 คน
ซึ่งคุณรัฐมนตรีแต่งตั้ง^{จากผู้มีความรู้ความเชี่ยวชาญ}
และประสบการณ์เป็นที่ประจักษ์

รัฐมนตรี ก.ดิจิทัลฯ เป็นประธานกรรมการ
กรรมการโดยตำแหน่ง จำนวน 13 คน
+ กรรมการผู้ทรงคุณวุฒิ *
จำนวนไม่เกิน 4 คน
คณะกรรมการ (กมช.) แต่งตั้งจาก
ผู้มีความรู้ความเชี่ยวชาญ ประสบการณ์
เป็นที่ประจักษ์และเป็นประโยชน์ต่อการ
รักษาความมั่นคงปลอดภัยไซเบอร์

รัฐมนตรี ก.ดิจิทัลฯ เป็นประธานกรรมการ
กรรมการโดยตำแหน่ง จำนวน 5 คน
+ กรรมการผู้ทรงคุณวุฒิ *
จำนวนไม่เกิน 6 คน
ให้รัฐมนตรีแต่งตั้งจากบุคคล ซึ่งมีความรู้
ความเชี่ยวชาญ และความสามารถ
เป็นที่ประจักษ์

บทกำหนดโทษ พ.ร.บ. ไซเบอร์

มาตรา ๗๐ - มาตรา ๗๗

มาตรา ๗๐
พนักงานเจ้าหน้าที่
ฝ่าฝืน/กระทำความผิด

- ▶ ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นใดที่เกี่ยวข้องกับระบบคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด

จำคุกไม่เกิน สามปี
หรือปรับเกิน หกหมื่นบาท
หรือทั้งจำทั้งปรับ

มาตรา ๗๑
พนักงานเจ้าหน้าที่
กระทำโดยประมาท

- ▶ พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ผู้ใดกระทำโดยประมาท เป็นเหตุให้ผู้อื่นล่วงรู้ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการ หรือข้อมูลอื่นใด ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่ได้มาตามพระราชบัญญัตินี้

จำคุกไม่เกิน หนึ่งปี
หรือปรับไม่เกิน สองหมื่นบาท
หรือทั้งจำทั้งปรับ

มาตรา ๗๒
บุคคลอื่น
เปิดเผยข้อมูลโดยมิชอบ

- ▶ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการ หรือข้อมูลอื่นใดที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มา ตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ

จำคุกไม่เกิน สองปี
หรือปรับไม่เกิน สี่หมื่นบาท
หรือทั้งจำทั้งปรับ

มาตรา ๗๓
หน่วยงาน CII
ไม่รายงานเหตุฯ

- ▶ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ ตามมาตรา ๕๗ โดยไม่มีเหตุอันสมควร

ปรับไม่เกิน สองแสนบาท

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

บทกำหนดโทษ พ.ร.บ. ไซเบอร์

มาตรา ๗๐ - มาตรา ๗๗

มาตรา ๗๔
ผู้ไม่ปฏิบัติ
ตามหนังสือเรียก

- ▶ ผู้ใดไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่ หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ ตามมาตรา ๖๒ (๑) หรือ (๒) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี



ปรับไม่เกิน หนึ่งแสนบาท

มาตรา ๖๒ ในการดำเนินการตามมาตรา ๖๑ [ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง] เพื่อประโยชน์ในการวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการ ดังต่อไปนี้
 (๑) มีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้อง เพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสมและตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์
 (๒) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสาร ซึ่งอยู่ในความครอบครองของผู้อื่นด้านเป็นประโยชน์แก่การดำเนินการ

มาตรา ๗๕
ผู้ฝ่าฝืนหรือไม่ปฏิบัติ
ตามคำสั่งของ กกม.

- ▶ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๑) และ (๒) โดยไม่มีเหตุอันสมควร
- ▶ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๓) และ (๔) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๕ (๕)

ปรับไม่เกิน สามแสนบาท และปรับอีกไม่เกินวันละ หนึ่งหมื่นบาท นับแต่วันที่ครบกำหนดระยะเวลาที่ กกม. ออกคำสั่งให้ปฏิบัติจนกว่าจะปฏิบัติให้ถูกต้อง จำคุกไม่เกิน หนึ่งปี หรือปรับไม่เกิน สองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖๕ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้และระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ ดำเนินการ ดังต่อไปนี้
 (๑) ผู้ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง
 (๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์ เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์
 (๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์ เพื่อจัดการข้อบกพร่องที่เกิดขึ้น หรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือรับผลกระทบจากภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่
 (๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์
 (๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

บทกำหนดโทษ พ.ร.บ. ไซเบอร์

มาตรา ๗๐ - มาตรา ๗๗

มาตรา ๗๖
ผู้ขัดขวางหรือ^{ไม่ปฏิบัติตามคำสั่ง}

- ▶ ผู้ใดขัดขวาง หรือไม่ปฏิบัติตามคำสั่งของ กกม. หรือพนักงานเจ้าหน้าที่ ซึ่งปฏิบัติการตามคำสั่งของ กกม. ตามมาตรา ๖๖ (๑) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๖ (๒) (๓) หรือ (๔) โดยไม่มีเหตุอันสมควร

จำคุกไม่เกิน สามปี
หรือปรับไม่เกิน หกหมื่นบาท
หรือทั้งจำทั้งปรับ

มาตรา ๖๖ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่องดังต่อไปนี้

- (๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของ หรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์
- (๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์
- (๓) ทดสอบการทำงานของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายใต้ประโยชน์จากคอมพิวเตอร์ หรือระบบคอมพิวเตอร์นั้น
- (๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เนพาที่จำเป็น ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าว ให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์ หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์ในการดำเนินการตาม (๒) (๓) และ (๔) ให้ กกม. ยึนคำร้องต่อศาลที่มีเขตอำนาจ เพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต่อระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องได้ส่วนคำร้องฉุกเฉินและให้ศาลพิจารณาได้ส่วนโดยเร็ว

มาตรา ๗๗
ผู้กระทำความผิด
เป็นนิติบุคคล

- ▶ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้ เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้น เกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการ จนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

รับโทษตามความผิด
มาตรา ๗๐ ถึง มาตรา ๗๖
แล้วแต่กรณี

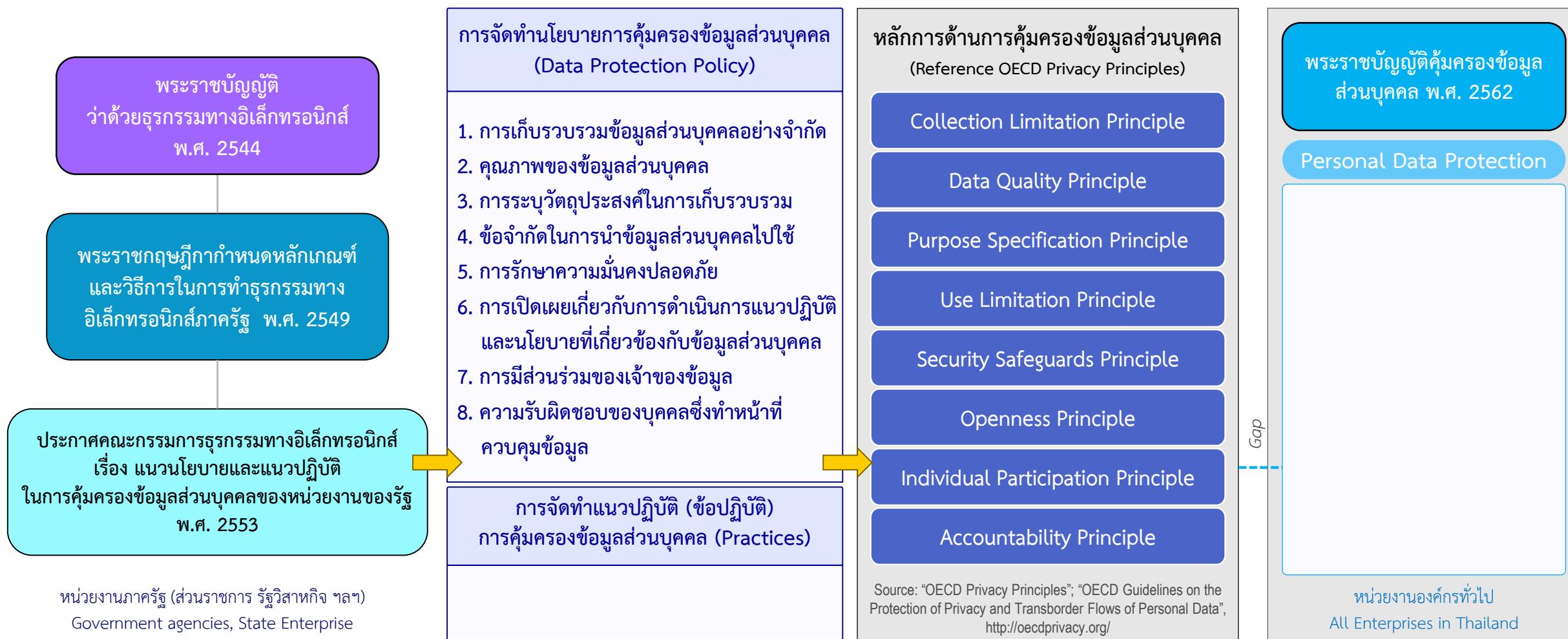
สาระสำคัญ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

Thailand Data Protection Laws



กฎหมายสำคัญที่เกี่ยวข้องด้านการคุ้มครองข้อมูลส่วนบุคคล

Data Protection Laws



หลักการคุ้มครองข้อมูลส่วนบุคคล

Principles for Personal Information/Data Protection (Privacy)



ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวโน้มฯและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
ข้อ 1 ให้จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร (อ้างอิงหลักการคุ้มครองข้อมูลส่วนบุคคล 8 ประการ)

1. Collection Limitation Principle

หลักการรวบรวมข้อมูลอย่างจำกัด :

- การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

2. Data Quality Principle

หลักการคุณภาพของข้อมูล :

- คุณภาพของข้อมูลส่วนบุคคล

3. Purpose Specification Principle

หลักการระบุวัตถุประสงค์ :

- การระบุวัตถุประสงค์ในการเก็บรวบรวม

4. Use Limitation Principle

หลักการใช้ข้อมูลอย่างจำกัด :

- ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

5. Security Safeguards Principle

หลักการรักษาความปลอดภัยของข้อมูล :

- การรักษาความมั่นคงปลอดภัย

6. Openness Principle

หลักการเปิดเผย :

- การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

7. Individual Participation Principle

หลักการมีส่วนร่วมของเจ้าของข้อมูล :

- การมีส่วนร่วมของเจ้าของข้อมูล

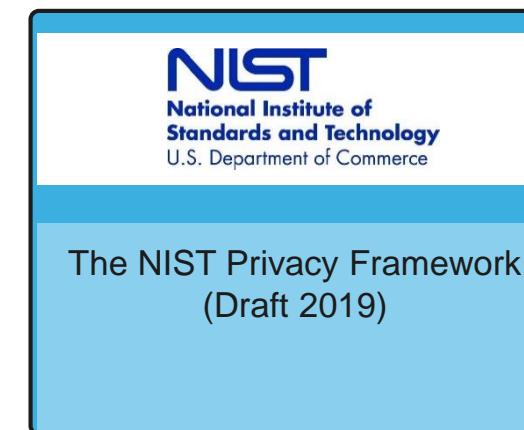
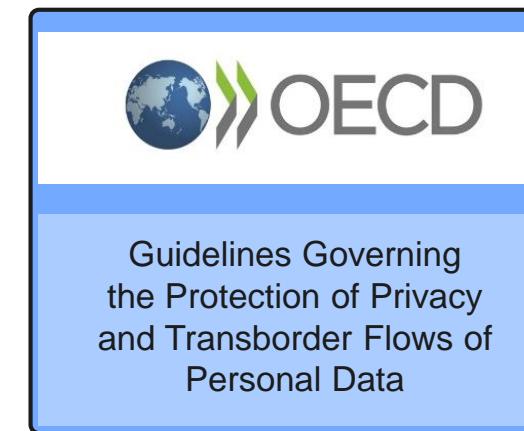
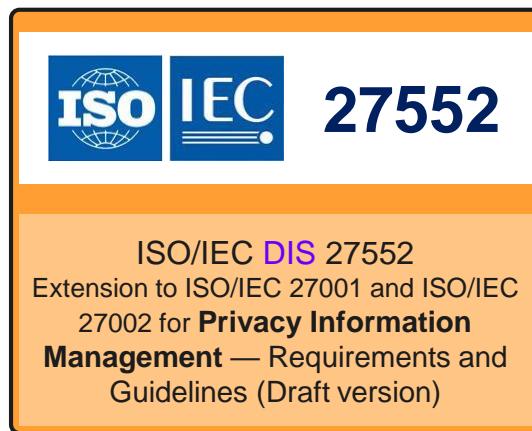
8. Accountability Principle

หลักการความรับผิดชอบ :

- ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

หลักการคุ้มครองข้อมูลส่วนบุคคล

Principles for Personal Information/Data Protection (Privacy)



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล vs. GDPR

สิทธิของเจ้าของข้อมูลส่วนบุคคล



The EU General Data Protection Regulation (GDPR)

- Right to be informed** Article 13 Article 14
- Right of access by the data subject** Article 15
- Right to be rectification** Article 16
- Right to erasure ('Right to be forgotten')** Article 17
- Right to restrict processing** Article 18
- Notification obligation regarding rectification or erasure of personal data or restriction of processing** Article 19
- Right to data portability** Article 20
- Right to object** Article 21
- Right of automated decision making and profiling** Article 22



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- สิทธิในการได้รับแจ้งข้อมูล**
- สิทธิในการเข้าถึงข้อมูล**
- สิทธิในการแก้ไขข้อมูล**
- สิทธิในการขอลบข้อมูล**
- สิทธิในการจำกัดการให้ข้อมูล**
- สิทธิในการได้รับการแจ้งเตือนที่เกี่ยวข้องกับสิทธิด้านต่างๆ**
- สิทธิในการโอนย้ายข้อมูล**
- สิทธิที่จะปฏิเสธการให้ใช้ข้อมูล**
- สิทธิไม่อนุญาตให้ระบบการตัดสินใจดำเนินการอัตโนมัติ**

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

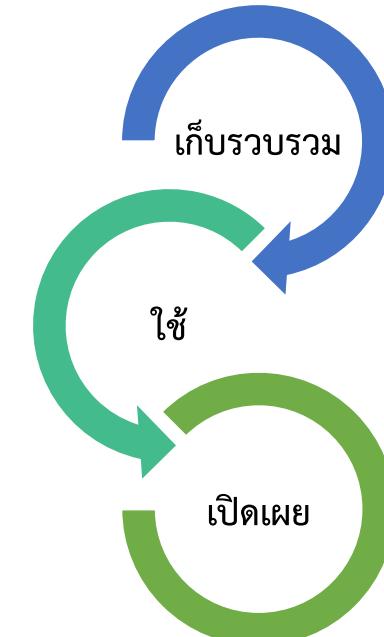
▶ เหตุผลและความจำเป็น

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการ
เยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล
ซึ่งการพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัตไว้ในมาตรา ๒๖
ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

เพื่อกำหนดหลักเกณฑ์ กลไก
หรือมาตรการกำกับดูแลเกี่ยวกับ
การให้ความคุ้มครองข้อมูลส่วนบุคคล
ที่เป็นหลักการโดยทั่วไป

สอดคล้อง
ตามหลักการสากล
และ GDPR

การคุ้มครองข้อมูลส่วนบุคคล

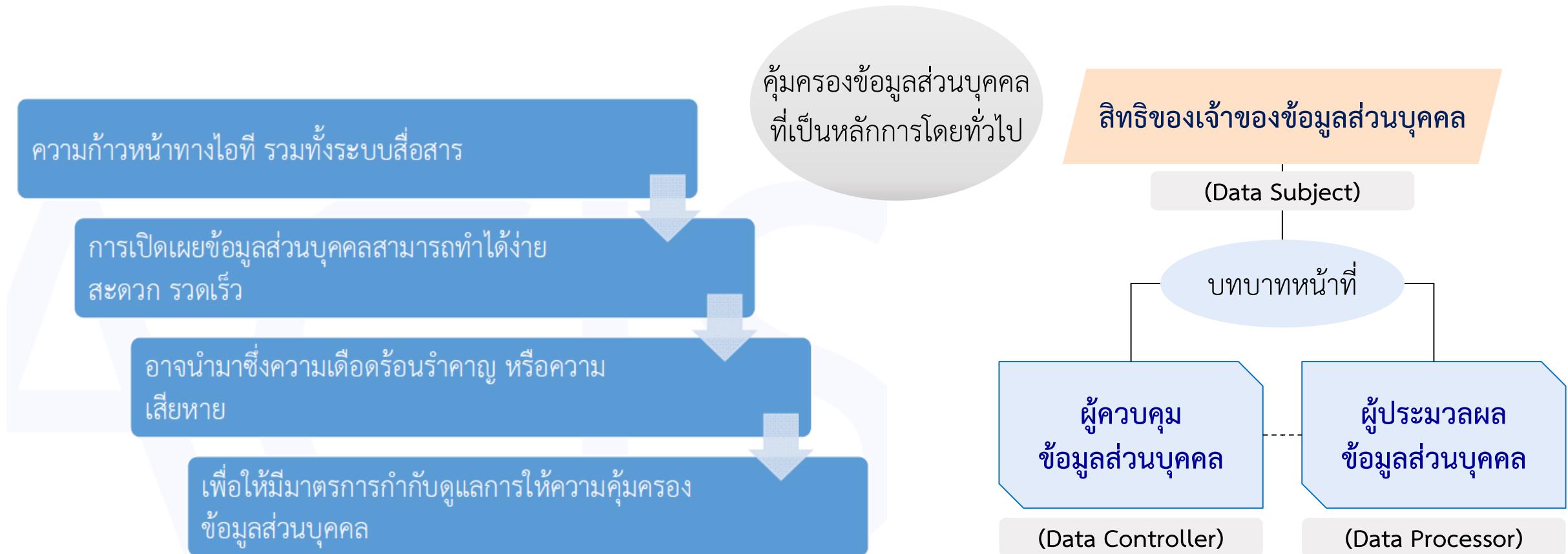


สิทธิของเจ้าของข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล

เหตุผลและความจำเป็น : การคุ้มครองข้อมูลส่วนบุคคล



นิยามสำคัญ

มาตรา 6 ในพระราชบัญญัตินี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าว ไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“บุคคล” หมายความว่า บุคคลธรรมดा

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

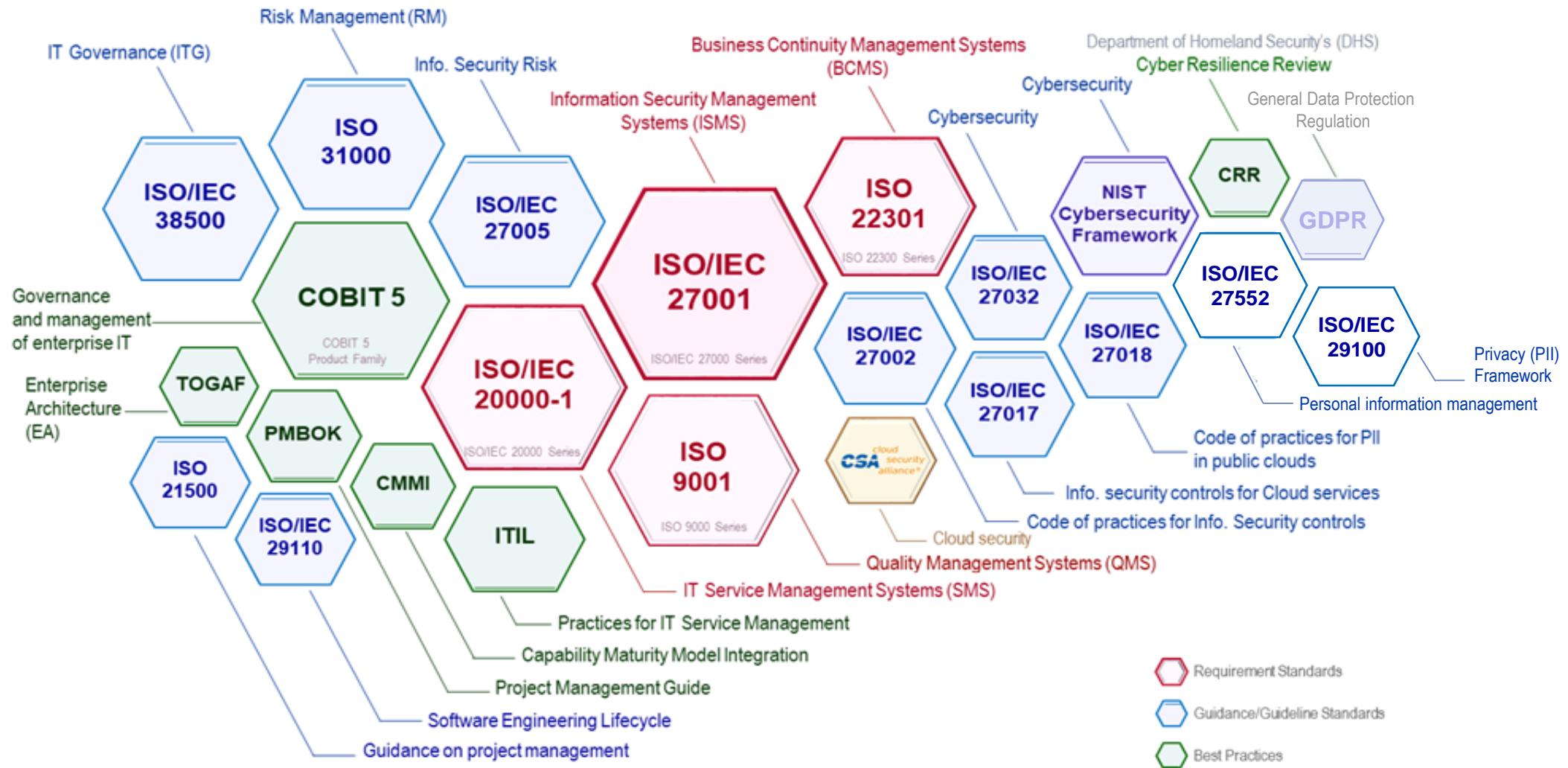
“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“เลขาริการ” หมายความว่า เลขาธิการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้ (รัฐมนตรี ก.ดิจิทัลฯ)

Key Risk-based Standards and Best Practices

for IT-GRC, Privacy, Cybersecurity and Information Security Management



ขอบคุณครับ



Thailand Information Security Association (TISA)
www.TISA.or.th



Cyber Defense Initiative Conference
www.cdicconference.com



ACIS Professional Center Co., Ltd.
www.acisonline.net



www.youtube.com/thehackertyv



www.youtube.com/thecyber911



Prinya.ho@acisonline.net



[www.twitter.com/prinyaACIS \(@prinyaacis\)](http://www.twitter.com/prinyaACIS)



www.facebook.com/acisonline

www.facebook.com/prinyah

Facebook search : prinya hom-anek



ACIS Professional Center Co., Ltd.
YOUR SATISFACTION IS OUR PRIDE

140/1 Kian Gwan Building 2, 18th Floor, Wireless Road, Lumpini,
Pathumwan, Bangkok 10330, Thailand
Tel: +66 2 253 4736, Fax: +66 2 253 4737 www.acisonline.net



"Security Intelligence"



ACIS Professional Center Co., Ltd.
YOUR SATISFACTION IS OUR PRIDE

140/1 Kian Gwan Building 2, 18th Floor, Wireless Road, Lumpini, Pathumwan, Bangkok 10330, Thailand
Tel: +66 2 253 4736, Fax: +66 2 253 4737 www.acisonline.net