Digital Transformation, Data Economy, Cybersecurity/Cyber Sovereignty and Data Privacy

EXECUTIVE SUMMARY

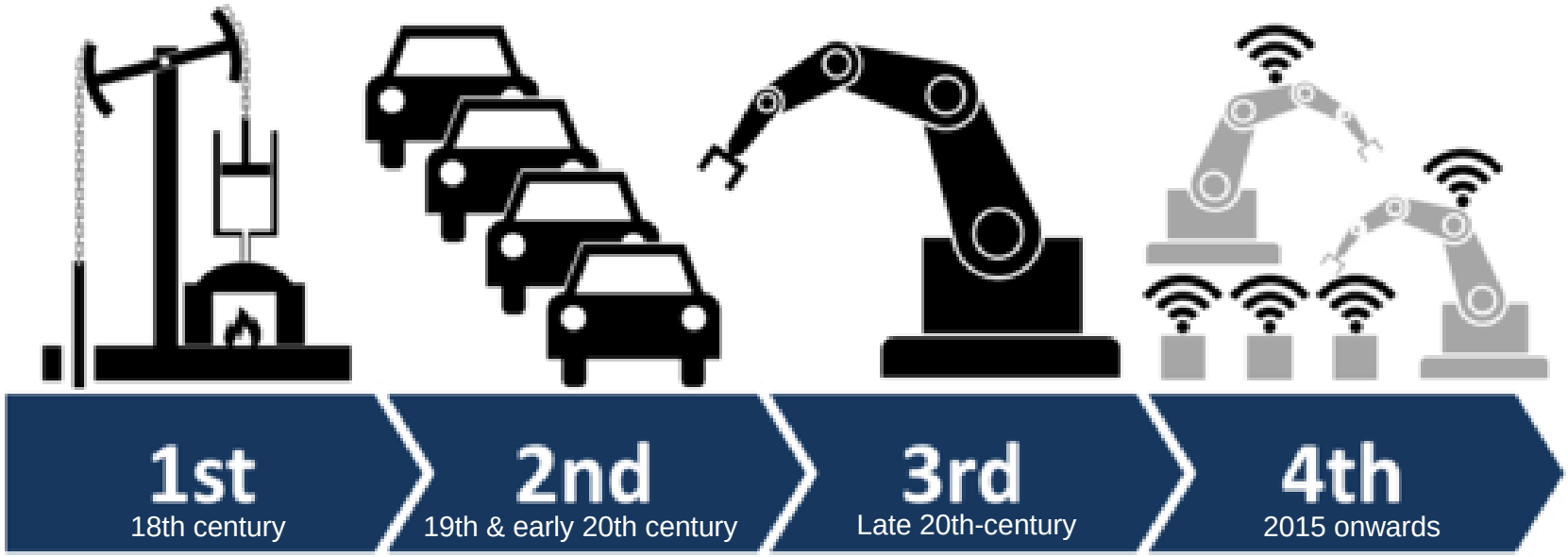
PRINYA HOM-ANEK

CISSP, CSSLP, SSCP, CASP, CFE, CBCI, CGEIT, CRISC, CISA, CISM, CSX, ITIL Expert,
COBIT 5 Foundation, COBIT 5 Implementation, ISMS Lead Auditor, ITSMS and BCMS Auditor
Eisenhower Fellowships 2013, (ISC)^2 Asian Advisory Board,
ISACA Thailand Board Member, itSMF Thailand Board Member,
Thailand Information Security Association (TISA), Board Member

Cybertron Co., Ltd. - CEO
ACIS Professional Center Co., Ltd. – President and Founder

ACIS/Cybertron Privacy & Cybersecurity Research LAB

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

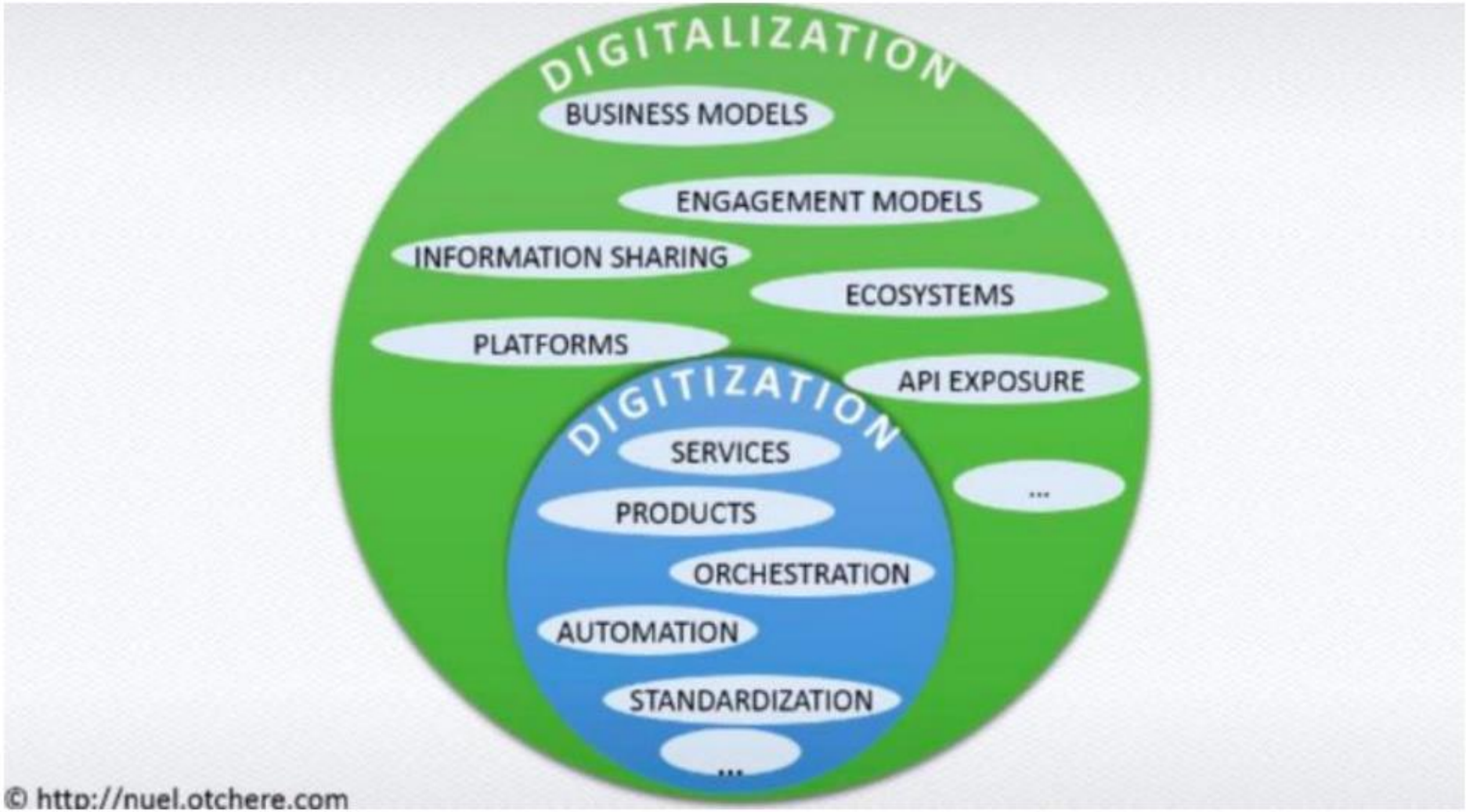
THE DIGITAL TRANSFORMATION

Digitization

or

Digitalization

Source : http://www.digitaltransformationplaybook.com/



Digital Transformation (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

Source : http://www.digitaltransformationplaybook.com/

DOMAINS	STRATEGIC THEMES	KEY CONCEPTS
 CUSTOMERS	*Harness customer networks*	• reinvented marketing funnel • path to purchase • core behaviors of customer networks
 COMPETITION	*Build platforms, not just products*	• platform business models • (in)direct network effects • (dis)intermediation • competitive value trains
 DATA	*Turn data into assets*	• templates of data value • drivers of big data • data-driven decision making
 INNOVATION	*Innovate by rapid experimentation*	• divergent experimentation • convergent experimentation • minimum viable prototype • paths to scaling up
 VALUE	*Adapt your value proposition*	• concepts of market value • paths out of a declining market • steps to value prop evolution

Source : http://www.digitaltransformationplaybook.com/

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

Harvard Business Review

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/

IT

vs.

I & T

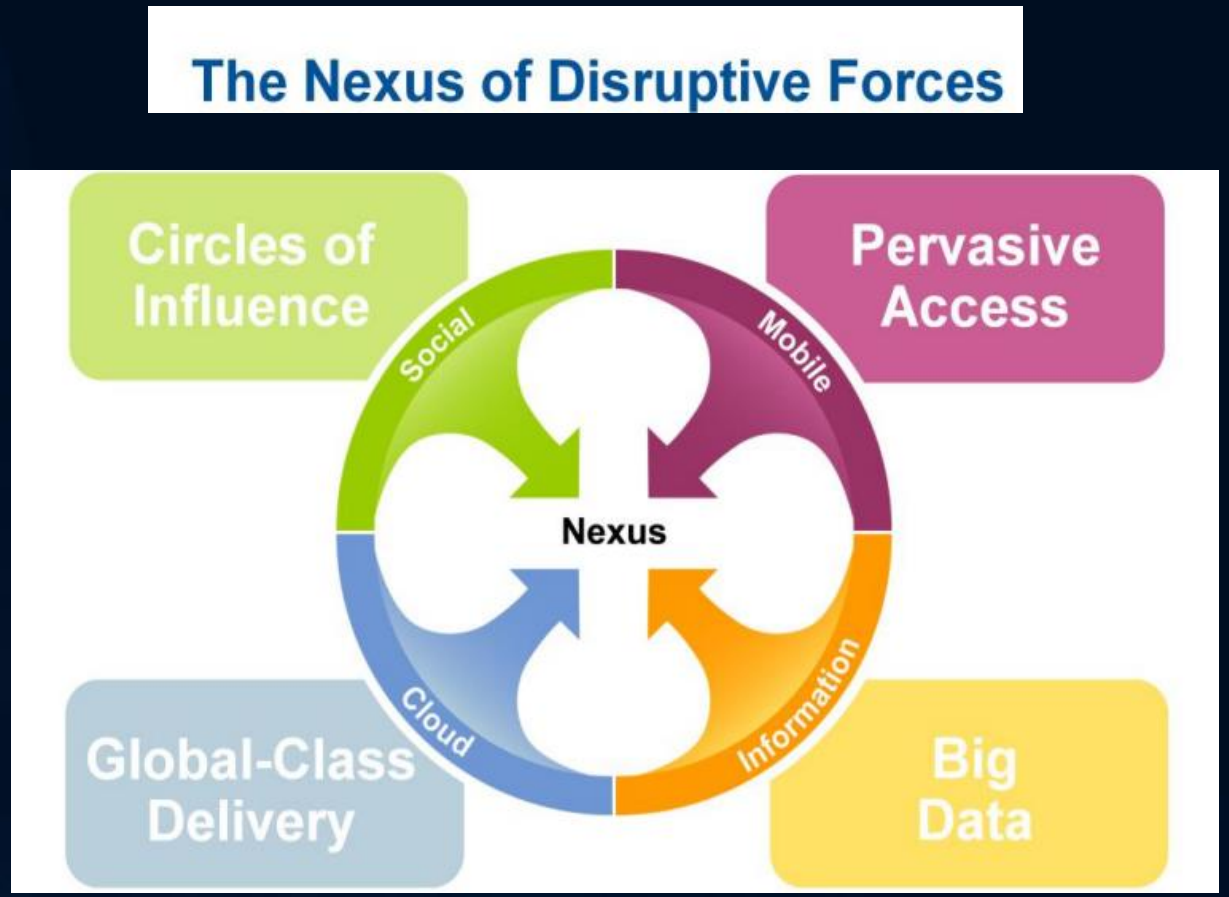
Source : http://www.digitaltransformationplaybook.com/

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*

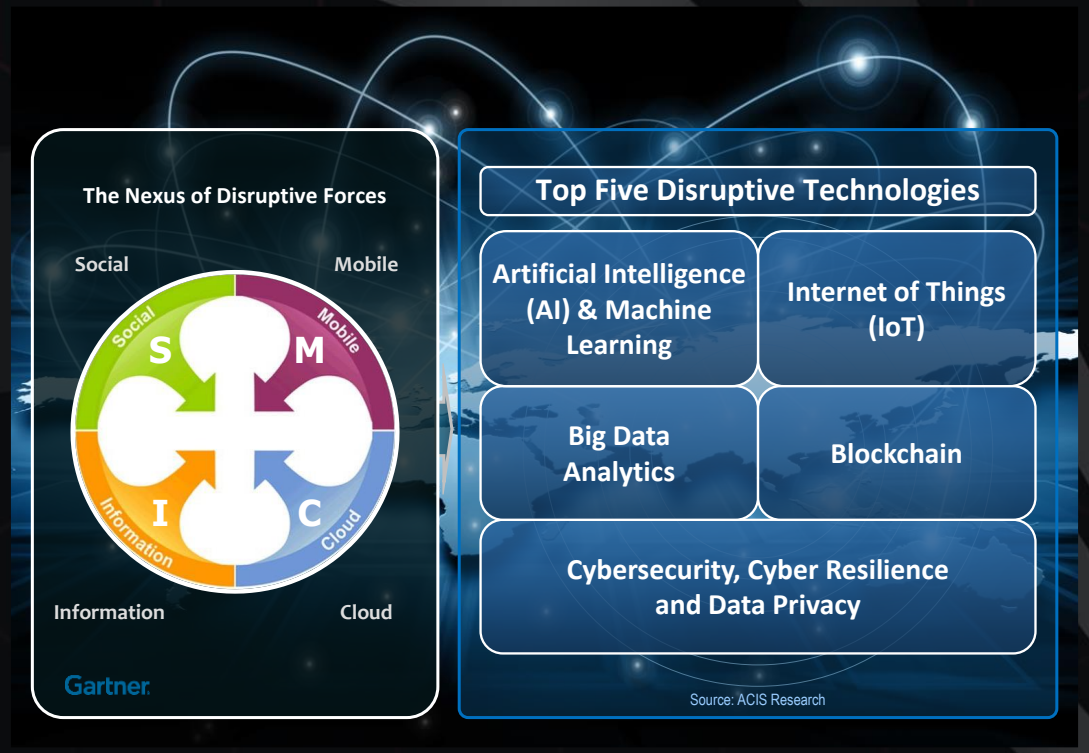
IT Trend and challenging to business

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

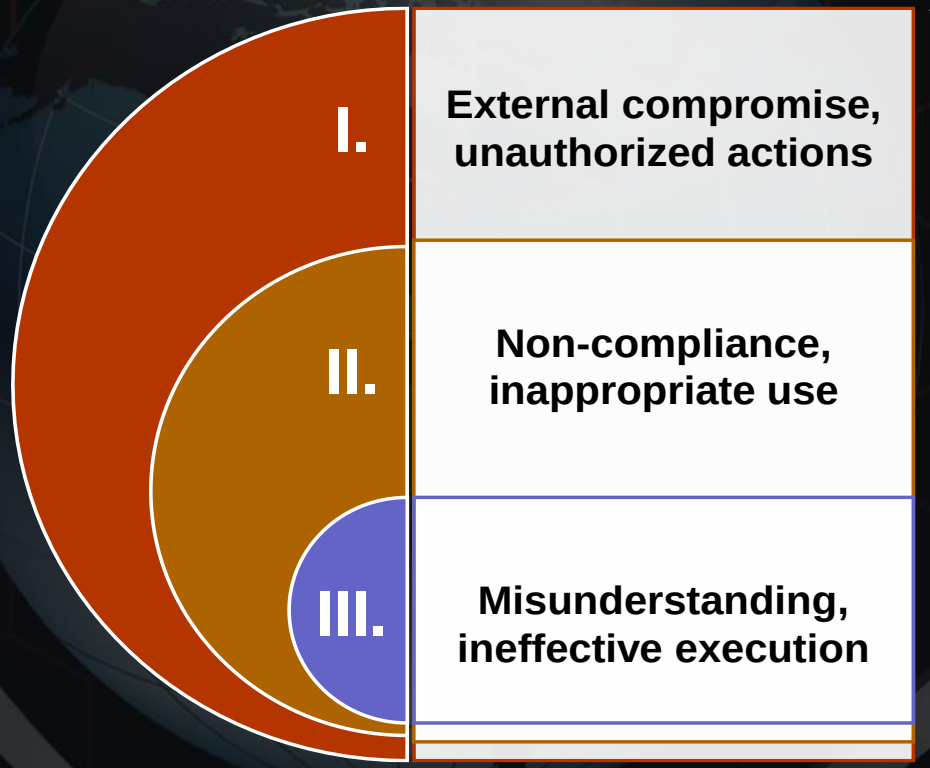


Source: Gartner, June 2013

Disruptive Technologies for Value Economy

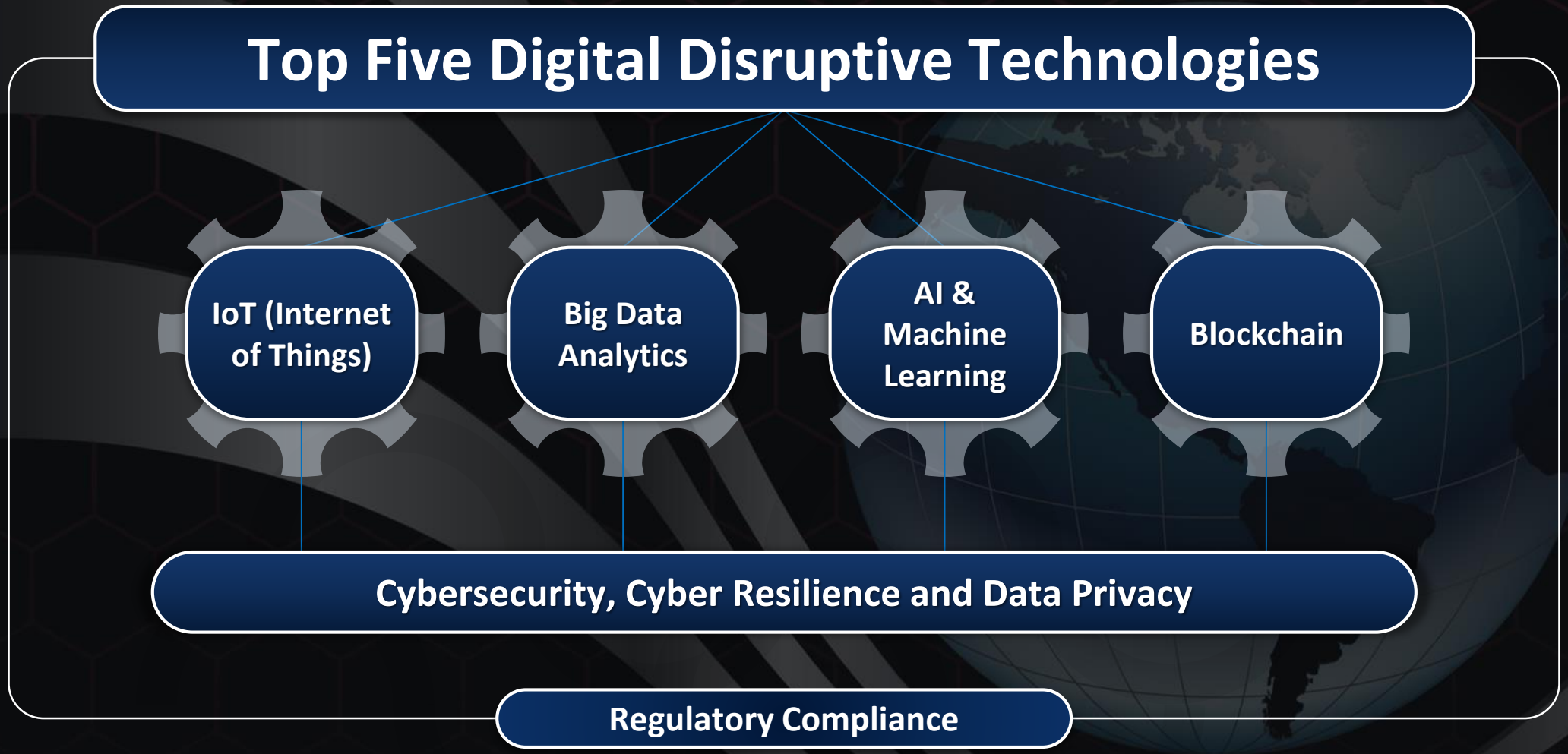


Threats and Trends Categories for 2019



Source: ACIS Research

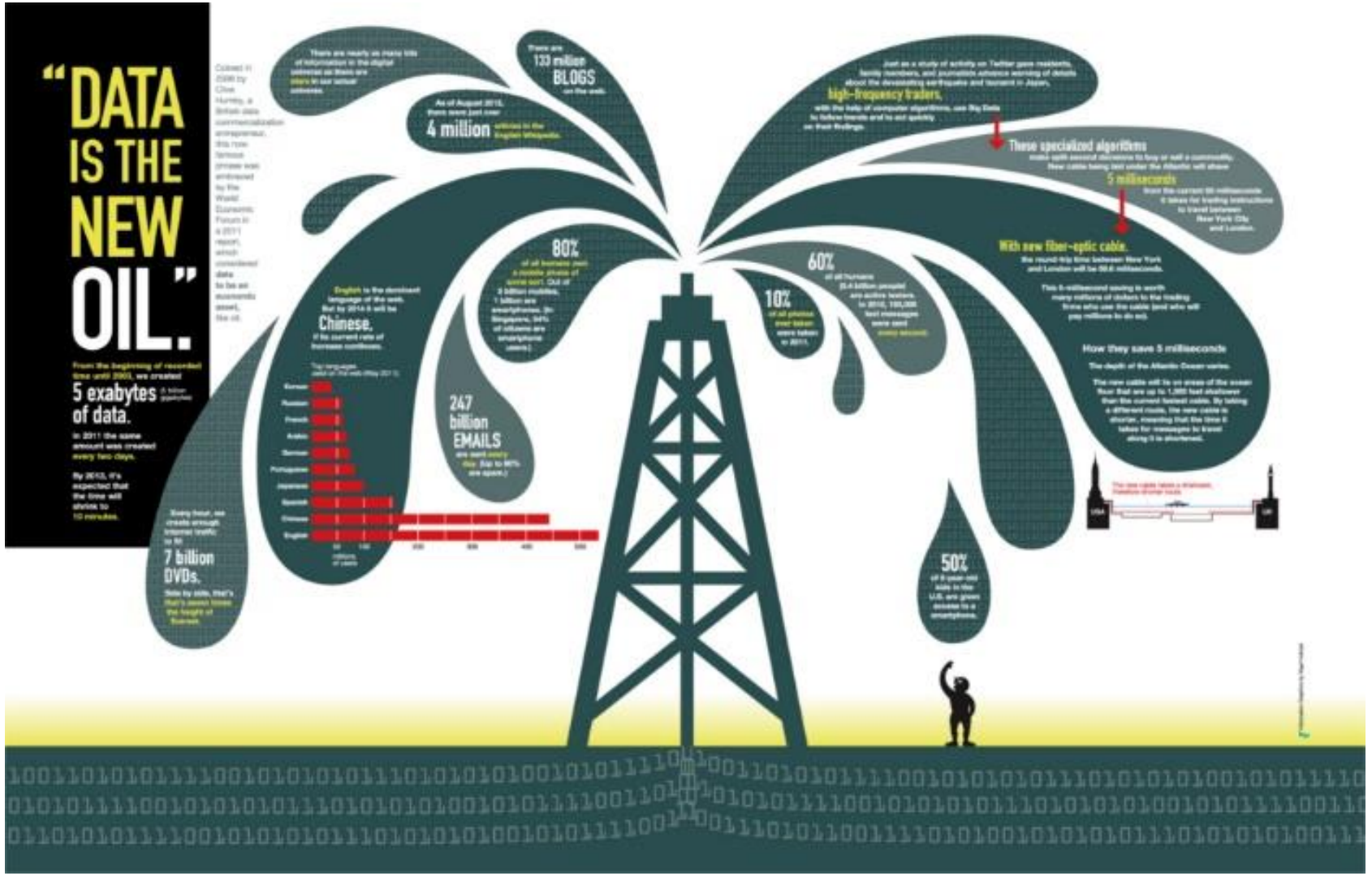
Disruptive Technologies for Value Economy



Source: ACIS Research

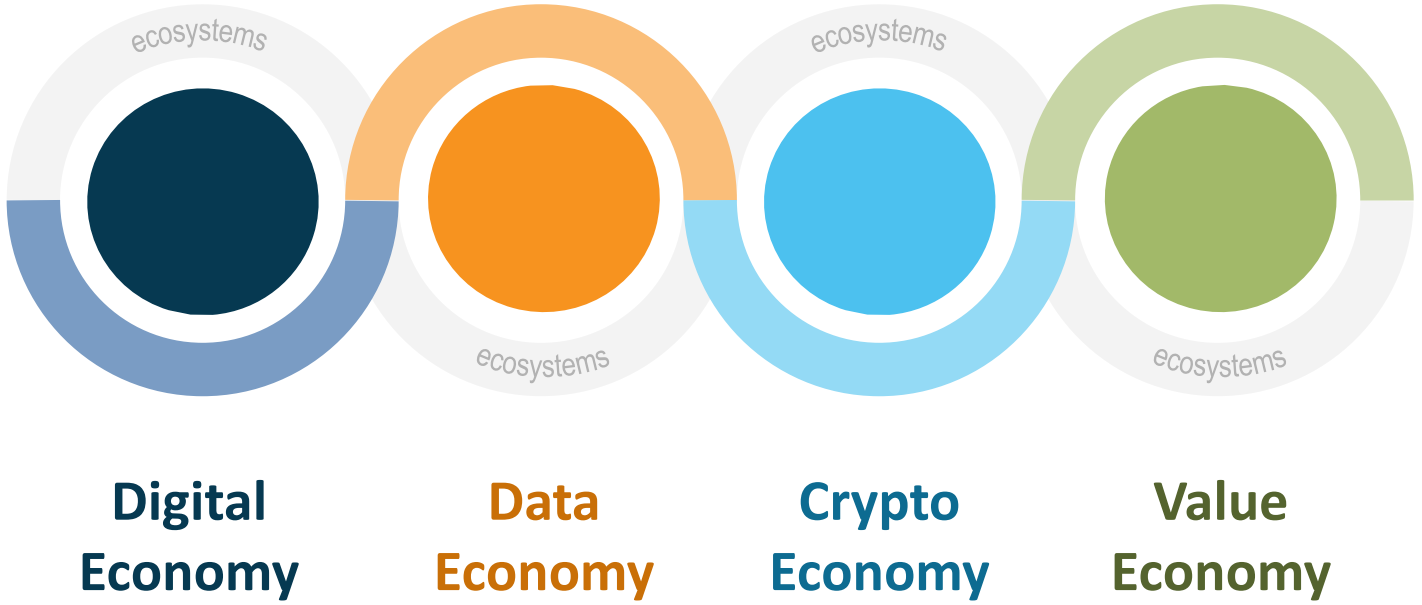
"About Nation Cyber Sovereignty and Hidden Privacy Threats"

"About Nation Cyber Sovereignty and Hidden Privacy Threats"



From Digital Economy to Data Economy

Digital Economy and Ecosystems



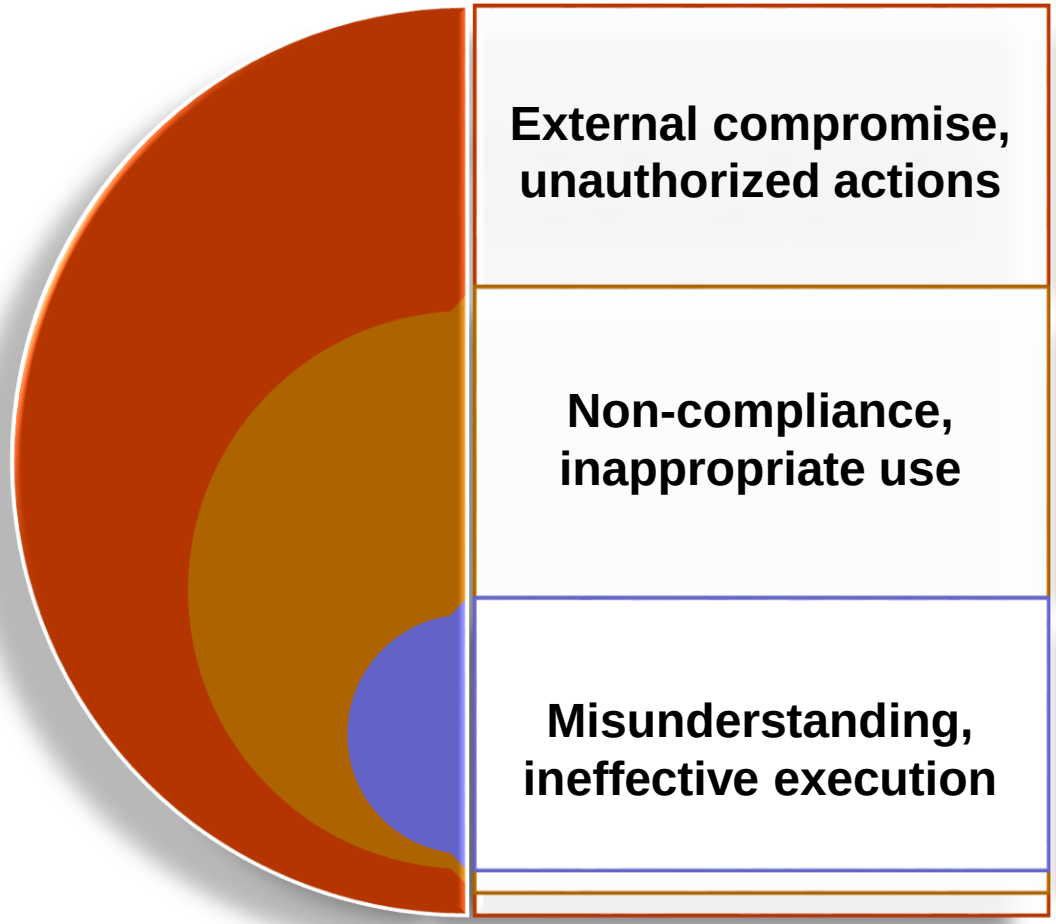
Source: ACIS Research

Top Ten 2019-2020

Top Ten Cyber Threats and Trends for 2019

Top Ten Cyber Threats and Trends for 2019

ACIS



- Data Privacy Risk & Leaks in Cloud
- User Data De-anonymization Attack
- Cyberbullying, Social Media Scandals
- Internet of Things (IoT), OT Security
- Dark side of Artificial Intelligence (AI)
- Internet / Online / e-Payment Fraud
- Regulatory Compliance: Cybersecurity & Privacy
- State of Cybersecurity, Cyber Resilience
- Cryptocurrency & Blockchain
- Digital Transformation & Cybersecurity Transformation

Source: ACIS Research

Top Ten Cyber Threats and Trends for 2019

ACIS

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

Source: ACIS Research, www.acisonline.net

Data Privacy Risk & Leaks in Cloud

ภัยข้อมูลรั่วไหลจากการจัดเก็บข้อมูลในระบบคลาวด์

การใช้บริการคลาวด์ได้รับความนิยมมากขึ้น องค์กรมักจะนำข้อมูลสำคัญขึ้นสู่คลาวด์ จึงเกิดปัญหาที่ข้อมูลสำคัญขององค์กรรั่วไหล ส่งผลกระทบต่อชื่อเสียงและภาพลักษณ์ขององค์กรอย่างหลีกเลี่ยงไม่ได้

ปัญหาเรื่อง “Security” และ “Privacy” กำลังจะกลายเป็นปัญหาใหญ่ หากไม่มีการวางแผนและการเตรียมการที่ดีพอในการรองรับปัญหาที่จะเกิดขึ้นดังกล่าว

User Data De-anonymization Attack

ภัยการโจมตีเจาะข้อมูลส่วนบุคคลในรูปแบบ De-anonymization Attack

ผู้ใช้บริการบริการโซเชียลมีเดีย ควรระมัดระวังการป้อนข้อมูลเข้าไปในระบบ ไม่ว่าจะ Post หรือ Upload ข้อมูลส่วนบุคคลเข้าไปในคลาวด์ เพราะแฮ็กเกอร์สามารถหาข้อมูลเพิ่มเติมประกอบที่เชื่อมโยงกับข้อมูลหลักของเรา จนสามารถระบุตัวตนของเป้าหมายได้ในที่สุด

จึงควรฝึกให้มีสติทุกครั้งในการป้อนข้อมูล โดยใช้หลักการง่าย ๆ สองข้อ คือ “Think before you post” (คิดก่อนโพสต์) และ “You are what you post” (คุณเป็นคนอย่างไรคุณก็โพสต์อย่างนั้น)

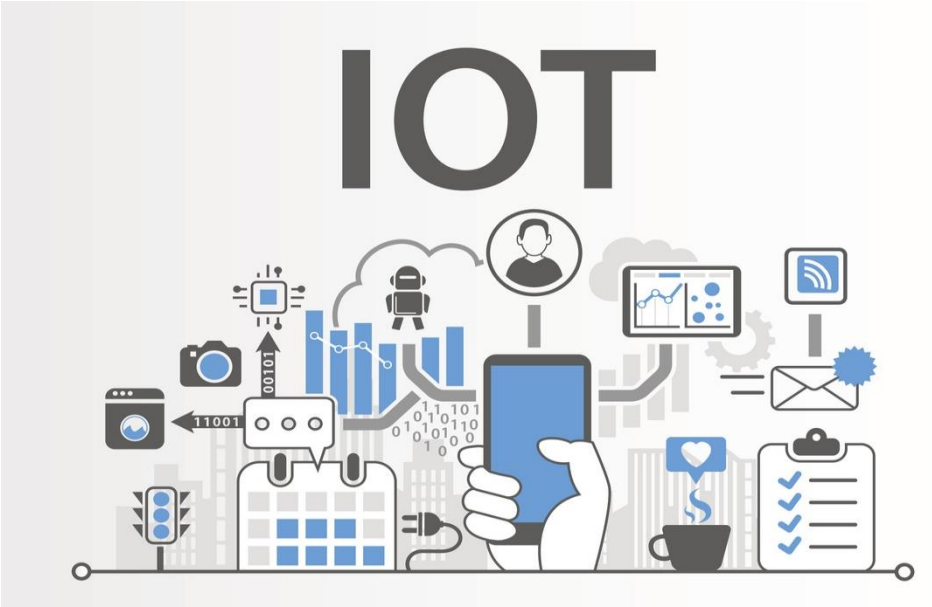
Cyberbullying, Social Media Scandals

ภัยจากการกลั่นแกล้งหรือให้ร้ายป้ายสีทางโซเชียลมีเดีย (Cyberbullying)

> บุคคลและองค์กรจำเป็นต้องวางแผนและมีการเฝ้าระวังสื่อสังคมออนไลน์อย่างต่อเนื่อง องค์กรต้องมีศักยภาพหรือขีดความสามารถในการโต้ตอบ ให้ข้อมูลเชิงบวกกับสาธารณชนให้ทันเวลา ก่อนที่ข่าวสารเชิงลบซึ่งทั้งจริงและไม่เป็นความจริง จะทำให้ชื่อเสียงของบุคคลและองค์กร มีผลกระทบต่อความน่าเชื่อถือ และความเชื่อมั่นของลูกค้าและประชาชน

IT, IoT and OT Security

ภัยจากการต่อเชื่อมอุปกรณ์ IoT กับระบบอินเทอร์เน็ตอย่างไม่ระมัดระวัง ทำให้เสี่ยงต่อการถูกโจมตีทางไซเบอร์



> อุปกรณ์ที่ต่อเชื่อมกับอินเตอร์เน็ต “IoT” หรือ “Internet of Things” ไม่จำเป็นต้องเป็นเครื่องคอมพิวเตอร์หรือแค่เพียงสมาร์ทโฟนอีกต่อไป เช่น กล้องวงจรปิด โทรทัศน์ ตู้เย็น นาฬิกาเพื่อสุขภาพ และอุปกรณ์ไฟฟ้าที่ใช้ในครัวเรือน ฯลฯ
>
> ขณะที่ “OT” หรือ “Operational Technology” หมายถึงอุปกรณ์ที่ถูกนำมาใช้ในระบบอุตสาหกรรม หรือ อุปกรณ์ควบคุมระบบ SCADA/ICS ซึ่งล้วนถูกออกแบบมาให้ชื่อผู้ใช้และรหัสผ่านถูกกำหนดมาจากผู้ผลิตอุปกรณ์เป็นค่าเริ่มต้น แฮกเกอร์จึงเข้าถึงอุปกรณ์เหล่านี้ได้โดยไม่ยากเย็นนัก

Dark side of Artificial Intelligence (AI)

ภัยจากการนำเทคโนโลยี Artificial Intelligence (AI) มาใช้ในด้านมืด

Should We Worry About Artificial Intelligence (AI)?

Source: https://www.codingdojo.com/blog/dark-side-of-artificial-intelligence-ai

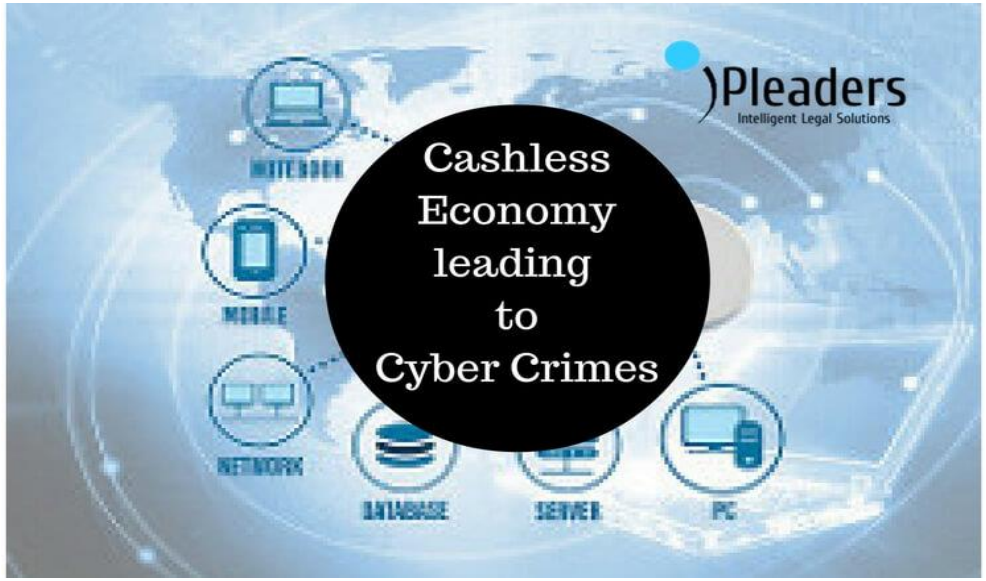
"ผู้ให้บริการโซเชียลมีเดีย" หรือ "Tech Giant" มีการนำเทคโนโลยี "AI" มาใช้วิเคราะห์พฤติกรรมของพวกเรา โดยที่เราทราบหรือไม่ทราบ ยินยอมหรือไม่ยินยอม นำข้อมูลในโซเชียลมีเดียของเราไปใช้หรือไปขายเพื่อประโยชน์ทางธุรกิจ โดยที่เรามิได้ยินยอมหรือไม่ทราบ

EU ต้องออกกฎหมาย "GDPR" มาจัดการเรื่องความเป็นส่วนตัวของผู้ใช้โดยเฉพาะ ทุกคนมีสิทธิที่จะจัดการหรือลบข้อมูลความเป็นส่วนตัว สิทธิที่จะถูกลืม "Right to be forgotten" หรือ "Right to erasure" นับเป็นสิทธิขั้นพื้นฐาน

Internet / Online / e-Payment Fraud

ภัยจากการทุจริตในการทำธุรกรรมทางอิเล็กทรอนิกส์

Is Cashless Economy Eliciting Cyber Crimes?



Source: https://blog.ipleaders.in/cashless-economy-eliciting-cyber-crime/

ปัจจุบันทั่วโลกกำลังมุ่งสู่ “สังคมไร้เงินสด” หรือ “Cashless Society” หากแต่ “Internet Fraud” หรือการฉ้อโกงทางอินเทอร์เน็ต ก็มีสถิติที่เริ่มมากขึ้นเป็นเงาตามตัวไปกับความนิยมในการทำธุรกรรมออนไลน์ ประชาชนถูกโกงเงิน หรือ เงินหายออกจากบัญชี ฯลฯ ความรับผิดชอบในเรื่องนี้ควรจะอยู่ใคร

ผู้ใช้จำเป็นต้องปรับแนวคิด และพฤติกรรมเสี่ยงดังกล่าวด้วยตนเอง เปลี่ยนแนวคิดที่ว่า “เรื่องนี้คงไม่เกิดกับเรา” หรือ “มีการป้องกันที่ดีที่สุดแล้ว” มาเป็น “สักวันเรื่องนี้คงเกิดกับเราอย่างแน่นอน” การป้องกันได้ดีที่สุด คือ “การใช้สติ” และ “ความไม่ประมาท” ของตัวเราเอง

Regulatory Compliance: Cybersecurity & Privacy

ภัยจากการที่องค์กรไม่สามารถปฏิบัติตามกฎหมายไซเบอร์และกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎระเบียบต่าง ๆ และกฎหมายที่เกี่ยวข้องกับไซเบอร์จะมีความเข้มงวดมากขึ้นทั่วโลก และประเทศไทยกำลังจะมีกฎหมายใหม่ที่ถูกนำมาบังคับใช้สองฉบับ ได้แก่ พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ซึ่งจะมีผลกระทบในส่วนหน่วยงานโครงสร้างพื้นฐานทั้งภาครัฐและเอกชน ตลอดจนมีผลกระทบต่อประชาชนทั่วไป ซึ่งในภาพรวมประชาชนจะได้ประโยชน์มากขึ้นจากการบังคับใช้ พ.ร.บ.ทั้งสองฉบับนี้ แต่สำหรับผู้บริหารระบบสารสนเทศ ตลอดจนผู้ตรวจสอบระบบสารสนเทศกลับมีเรื่องที่ต้องทำมากขึ้น

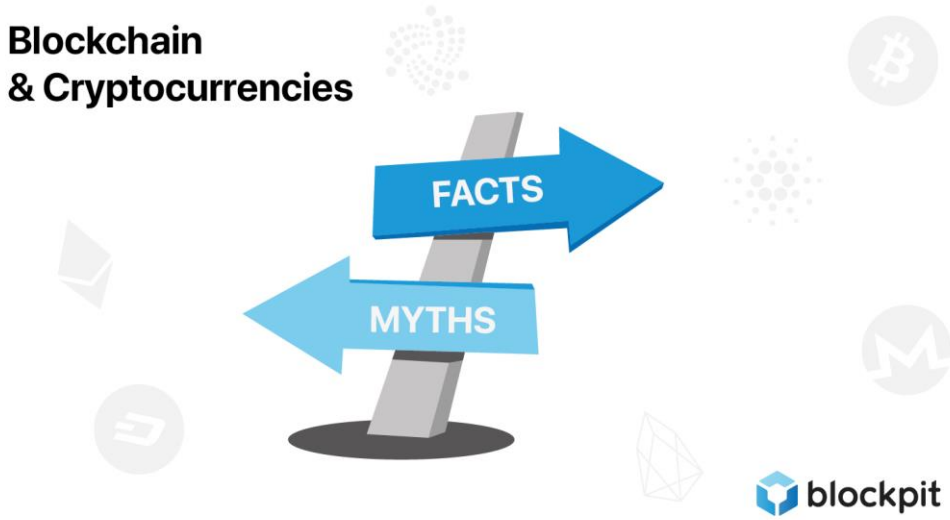
State of Cybersecurity, Cyber Resilience

ภัยจากความเข้าใจผิด ในธรรมชาติของสภาวะไซเบอร์

> คำว่า “Cybersecurity” เป็นคำยอดนิยมที่ถูกนำมาใช้อย่างแพร่หลายในแทบทุกวงการ แต่จะมีสักกี่คนที่เข้าใจธรรมชาติของ “สภาวะไซเบอร์” ได้อย่างถูกต้อง หากเรายังมีคำถามว่า “ระบบนั้นระบบนี้ ปลอดภัยไหม” (Are we secure?) ก็คงต้องทำความเข้าใจเสียใหม่ว่า ไม่มีคำว่า “ระบบที่ปลอดภัย 100%” ต่อให้เราลงทุนด้านการรักษาความปลอดภัยไซเบอร์ไปมากเพียงใด เราก็ยังไม่สามารถรอดพ้น 100% จากการโจมตีทางไซเบอร์ได้ ดังนั้น เรามีความจำเป็นต้องปรับเปลี่ยน Mindset จาก “Are we secure?” เป็น “Are we ready?”

Cryptocurrency and Blockchain Myths

ภัยจากความเข้าใจผิดในเรื่อง Cryptocurrency และ Blockchain



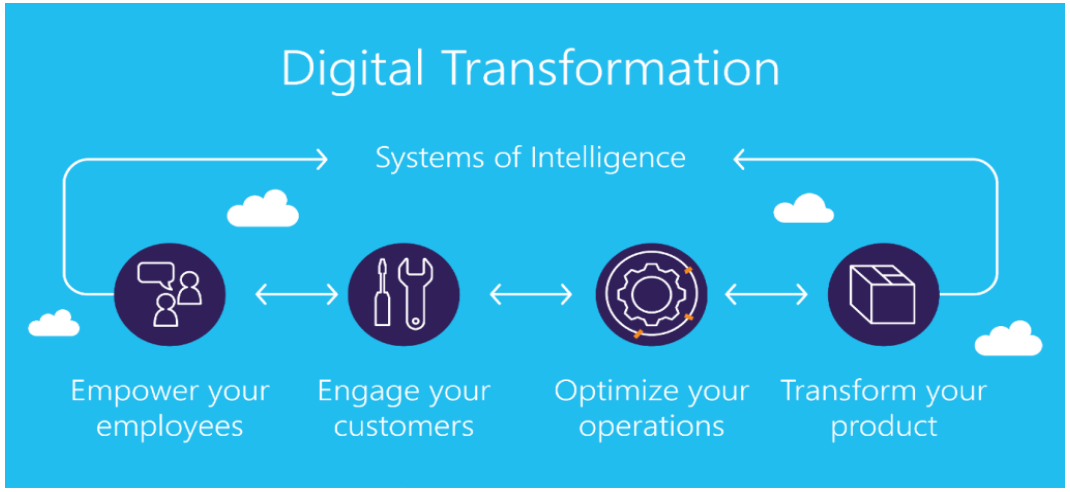
Source: https://medium.com/@blockpit/the-top-6-myths-about-blockchain-and-cryptocurrencies-3c23ca6bf9a6

“Blockchain เป็นหนึ่งในเทคโนโลยีเปลี่ยนโลกที่กำลังมีอนาคต หลายองค์กรกำลังศึกษาหาทางนำเทคโนโลยี Blockchain มาใช้ให้เกิดประโยชน์สูงสุดต่อองค์กร ขณะที่อีกมุมหนึ่งมีผู้สนใจใน Cryptocurrency ที่เกิดจากการนำเทคโนโลยี Blockchain มาประยุกต์ใช้ สร้างเป็น “Coin” หรือ “Token” ไปจนถึง “ICO” “STO” ฯลฯ หลายคนมีความเชื่อว่า จาก Data Economy เรากำลังจะไปสู่ Crypto Economy

หากแต่เทคโนโลยี Blockchain ยังสามารถนำมาทำสิ่งอื่น ที่ไม่ใช่เฉพาะเรื่อง Cryptocurrency ได้อีกมากมายโดยที่เรายังไม่ได้คิด ถือเป็นเรื่องใหม่ๆ ที่อาจเกิดขึ้นในอนาคต”

Digital Transformation and Cybersecurity Transformation

ภัยจากความไม่เข้าใจของผู้บริหารระดับสูงในเรื่อง Digital Transformation and Cybersecurity Transformation



Source: "Microsoft's 4 pillars of digital transformation", Microsoft

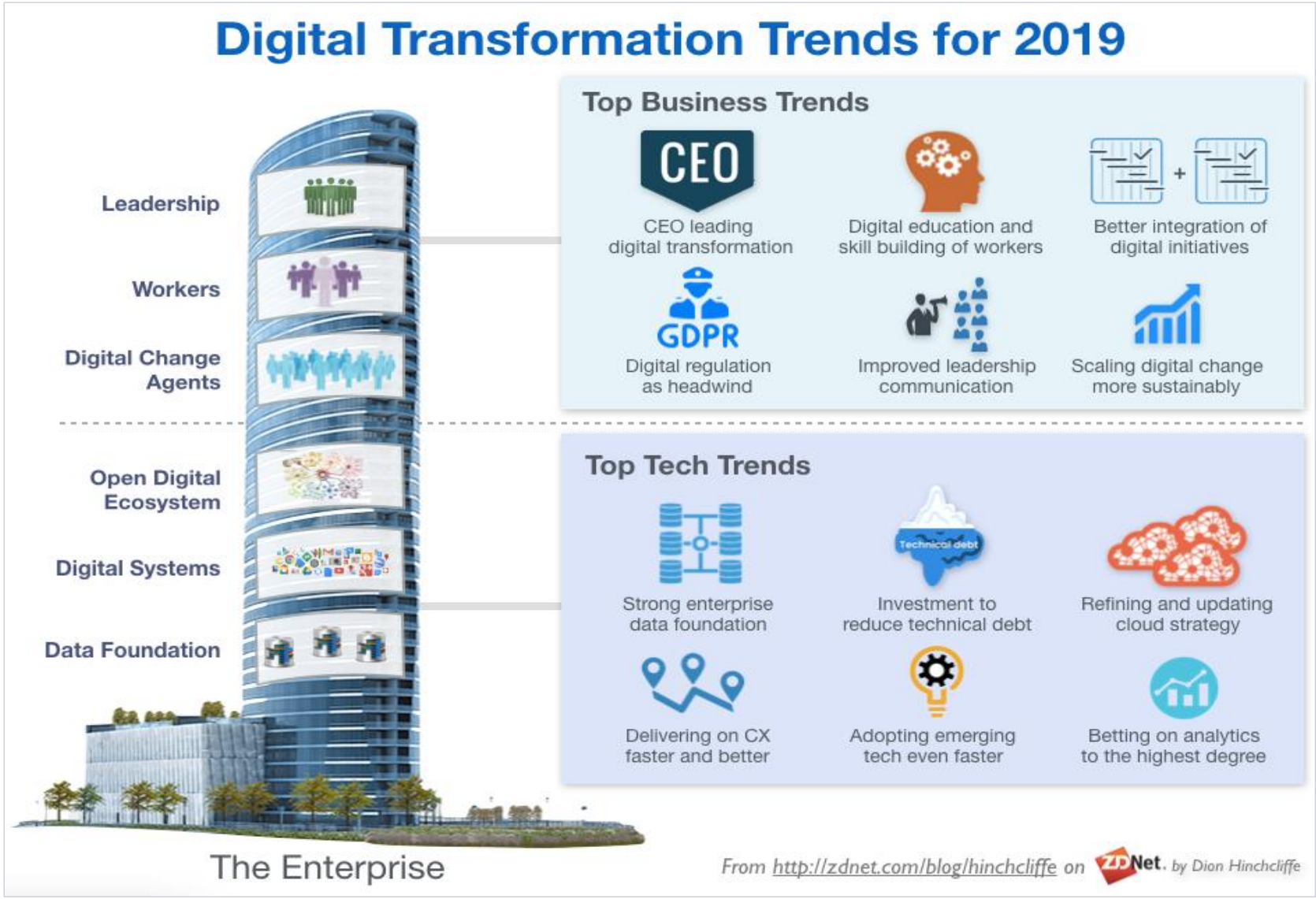
> การปรับองค์กรตามแนวทาง "Digital Transformation" ไม่ใช่เพียงการนำเอาเทคโนโลยีดิจิทัลมาใช้ แต่ต้องปรับเปลี่ยนองค์กรตั้งแต่เรื่อง "Leadership" ไปจนถึง "Customer Experience" ซึ่งจำเป็นต้อง Transform เรื่องการบริหารจัดการ Security และ Privacy ในองค์กรด้วย การนำหลักการ Cyber Resilience มาประยุกต์ใช้ เป็นเรื่องที่สำคัญมากสำหรับองค์กรในยุคใหม่ที่สามารถเตรียมพร้อมรับกับสิ่งไม่คาดคิดที่อาจจะเกิดขึ้น ขณะเดียวกันองค์กรยังสามารถรักษาระดับการให้บริการกับลูกค้าไว้ได้โดยไม่มีผลกระทบต่อชื่อเสียงและภาพลักษณ์ขององค์กร

Digital Transformation Trends for 2019

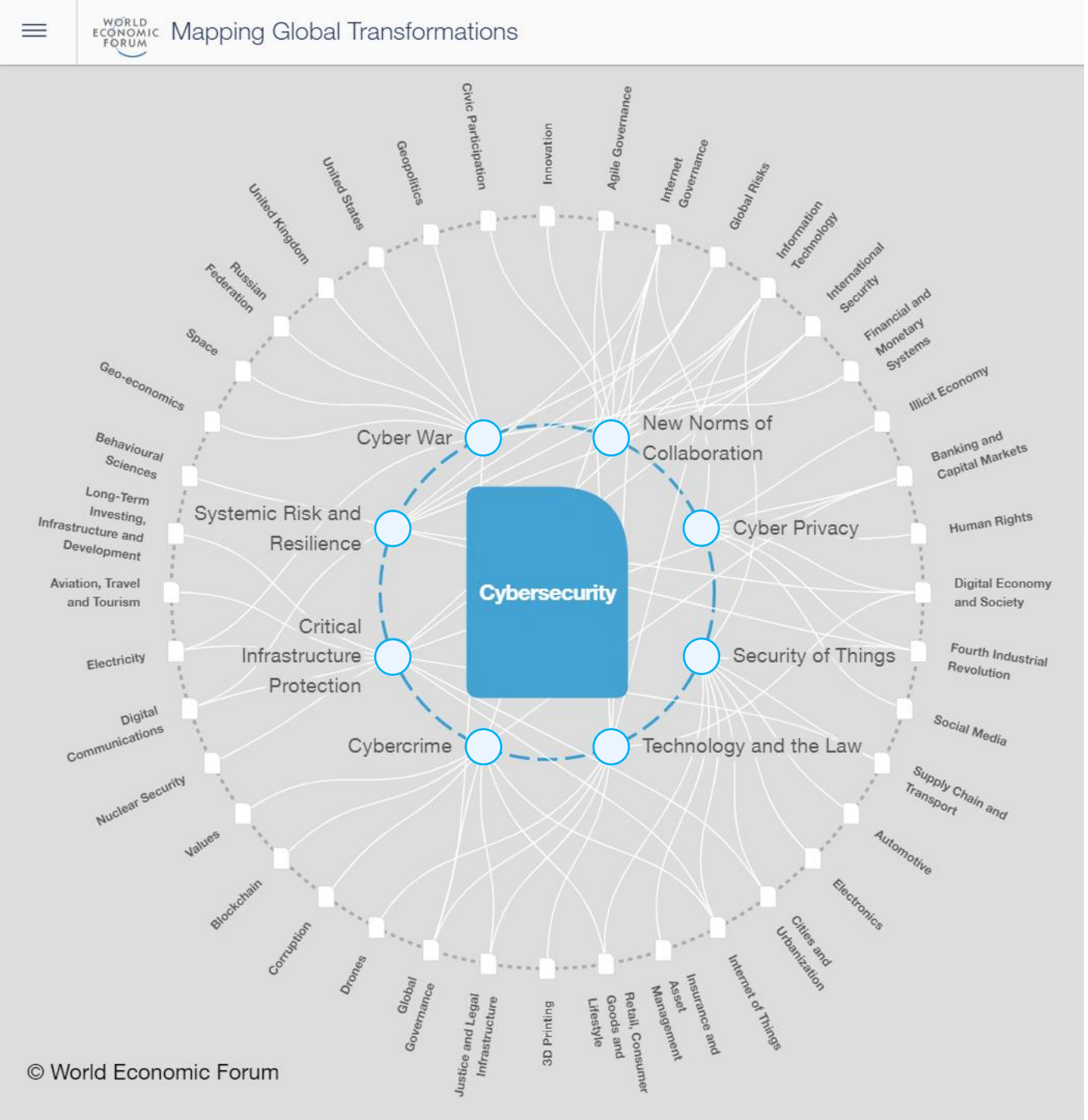
Digital Transformation:
Five Domains and Key Concepts

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

Source : www.digitaltransformationplaybook.com/



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

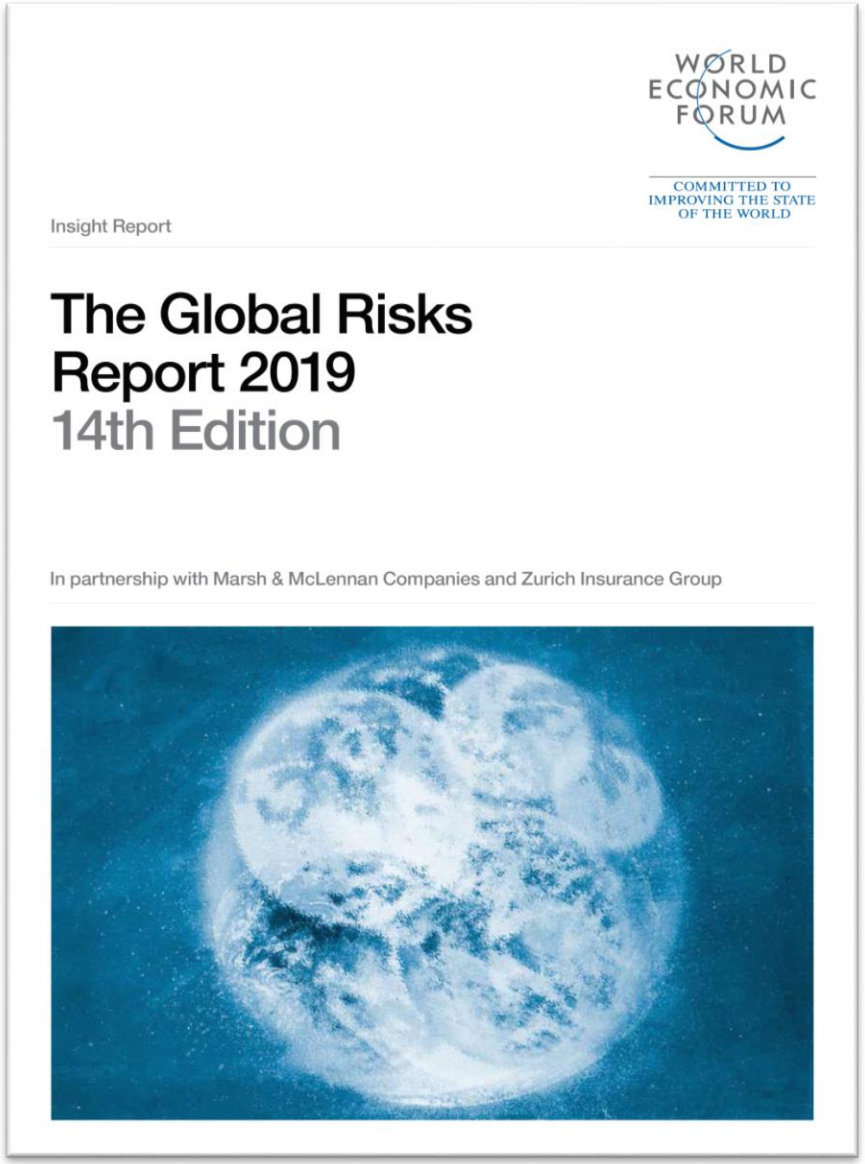


WEF Transformation Map: Cybersecurity

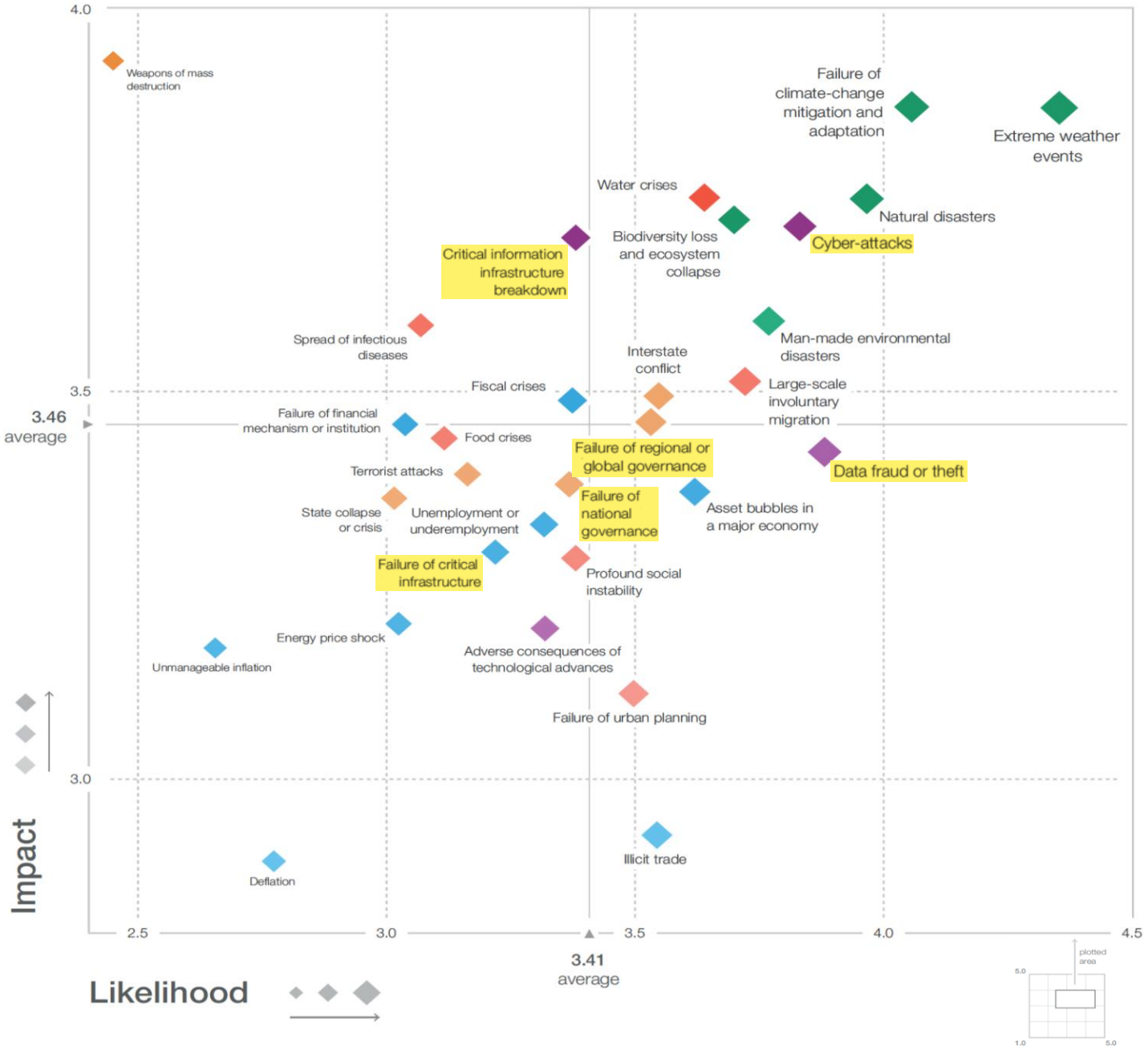
✧ Cybersecurity and related issues ✧

- 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



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



The Global Risk Outlook for 2019

STATE OF CYBERSECURITY 2019

SECURITY SKILLS GAP BY THE NUMBERS

CSX CYBERSECURITY NEXUS

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*.

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.

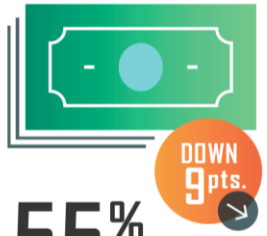
TOP 3 REASONS CYBERSECURITY PROS ARE CHANGING JOBS

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

CYBERSECURITY BUDGET GROWTH IS SLOWING



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.**

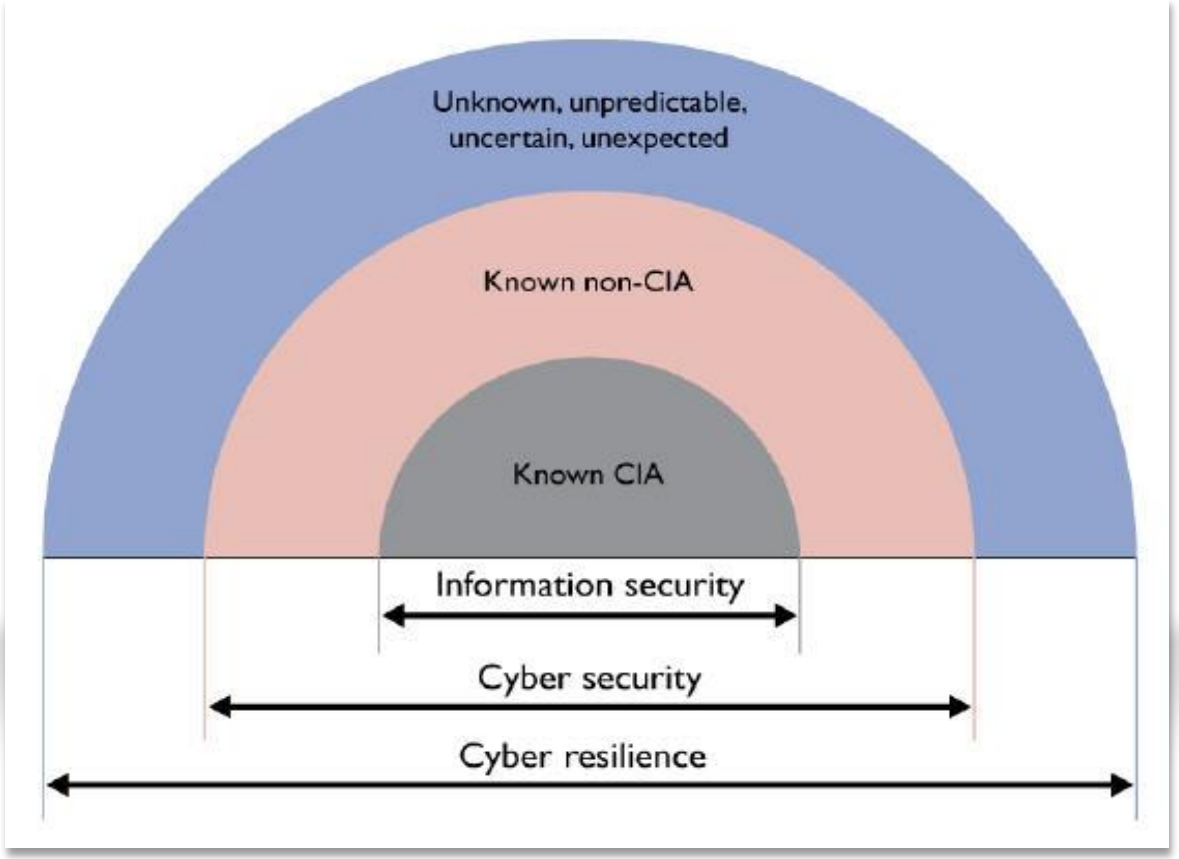
79% OF MEN SAY MEN AND WOMEN HAVE EQUAL OPPORTUNITIES for career advancement in cybersecurity roles at their organizations.

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.

SOURCE: ISACA's 2019 State of Cybersecurity Study, https://cybersecurity.isaca.org/state-of-cybersecurity

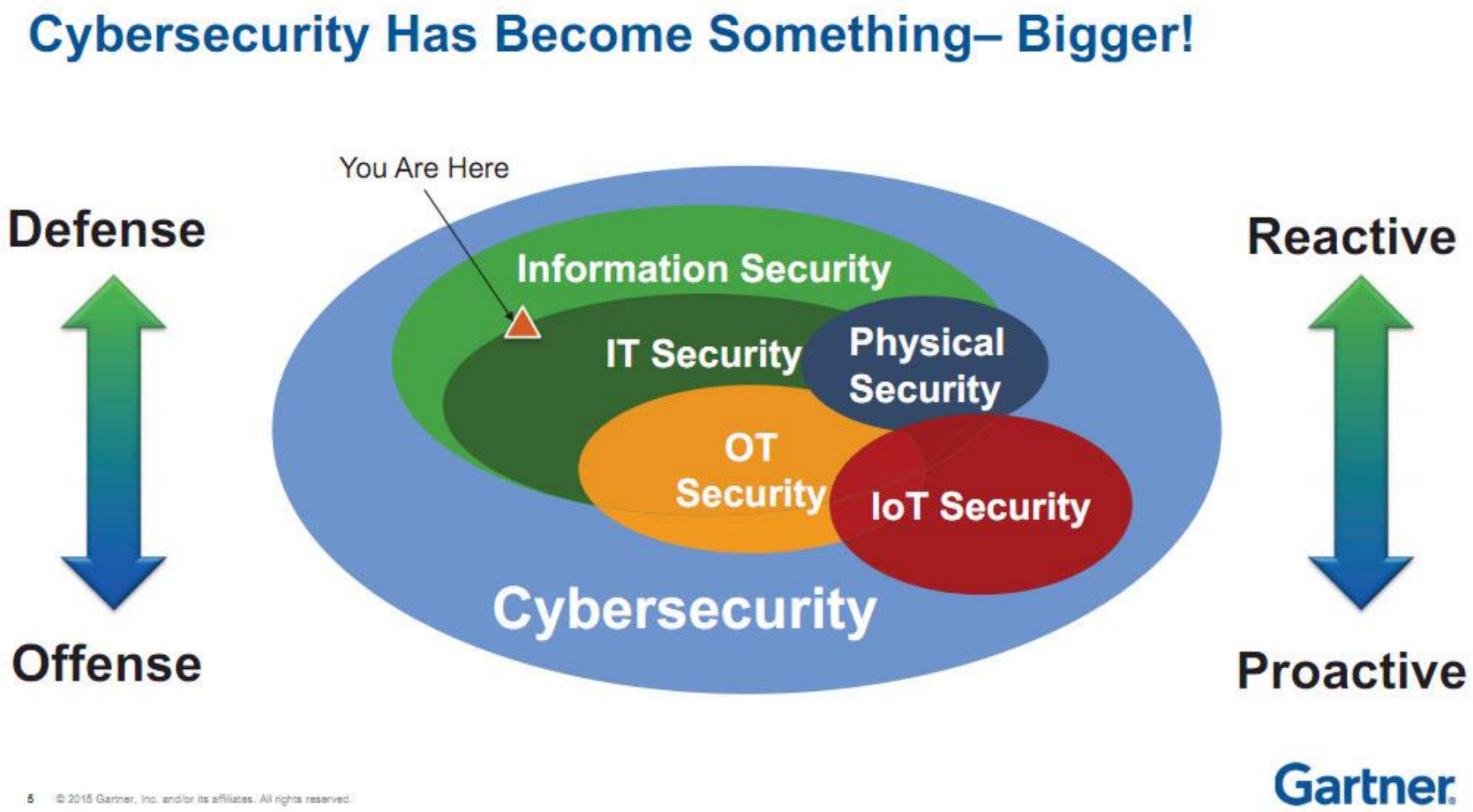
3 Stages : Information Security, Cybersecurity and Cyber Resilience



ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยด้านต่าง ๆ กับการรับมือภัยไซเบอร์

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

Not only IT security and Information Security

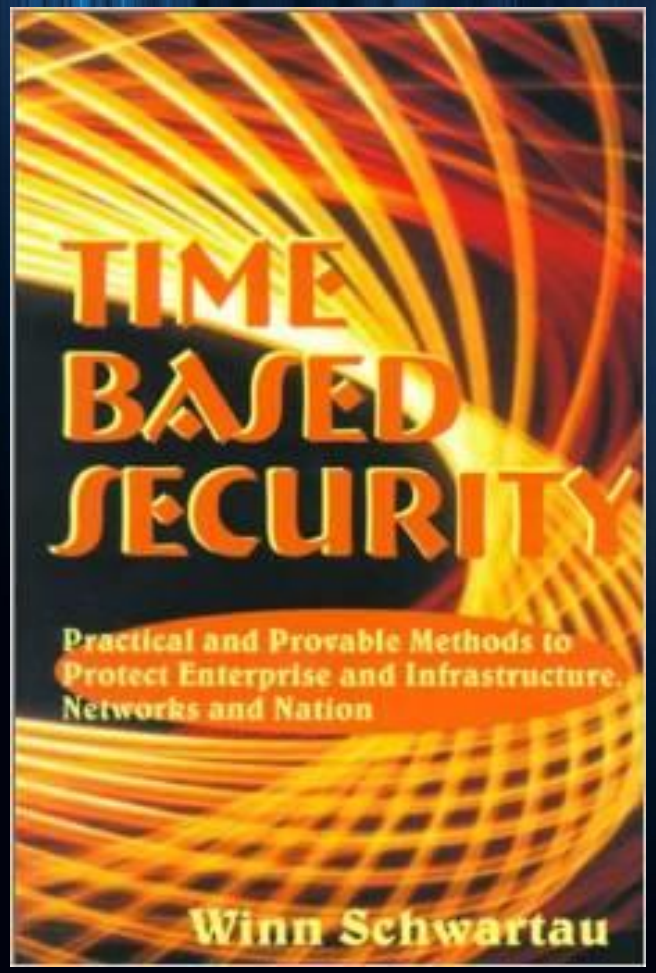


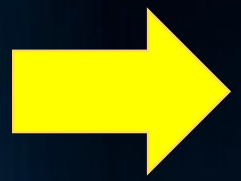
Gartner

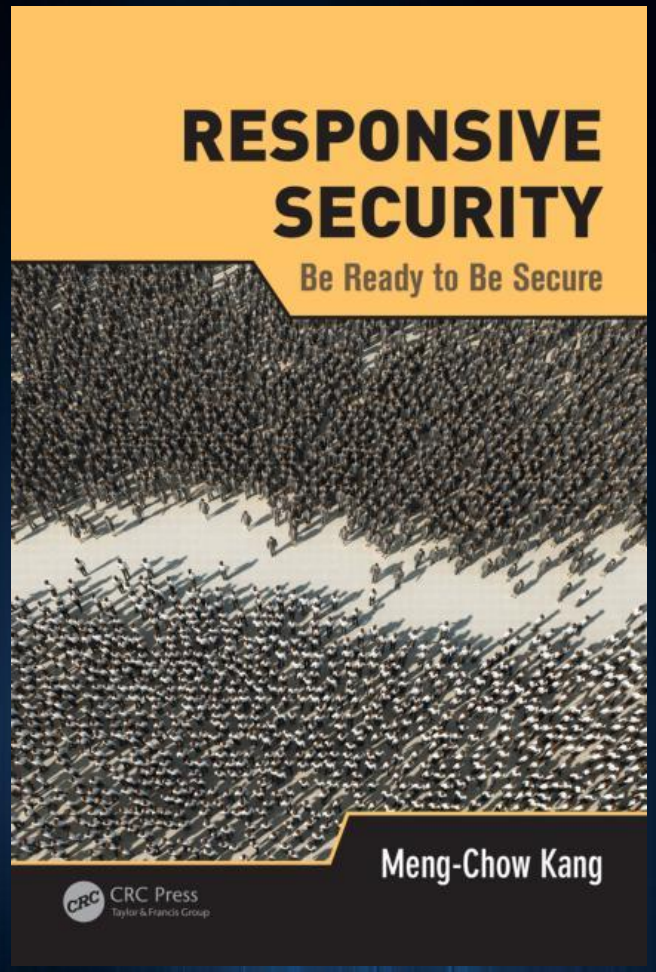
Paradigm Shift in Cybersecurity

“From Preventive to Responsive”

From “Time-based Security” to “Responsive Security”
credit: Dr. Meng-Chow Kang

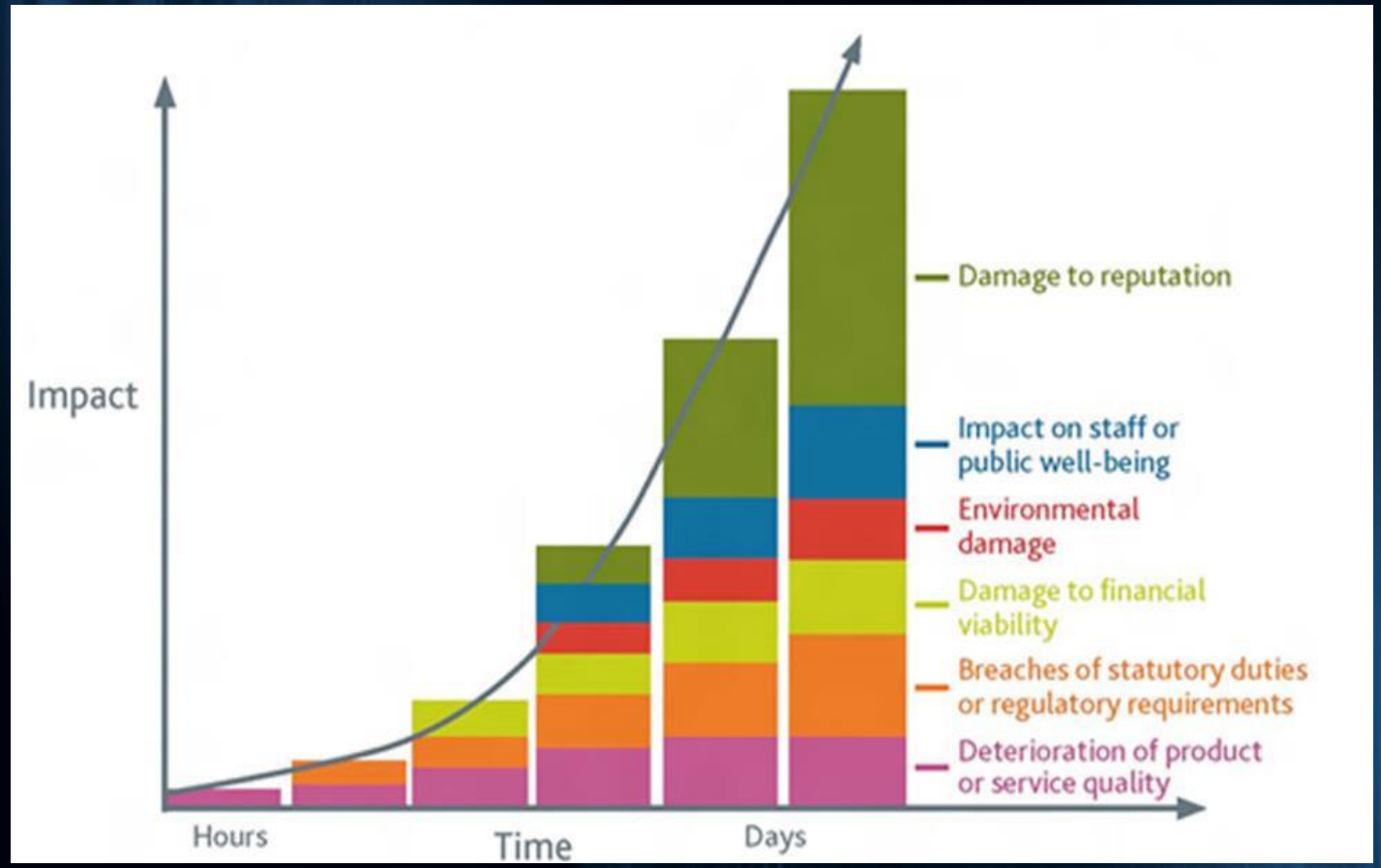






From “Preventive Security” to “Responsive Security”

Relationship about Business Impact and Time



CYBERTRON

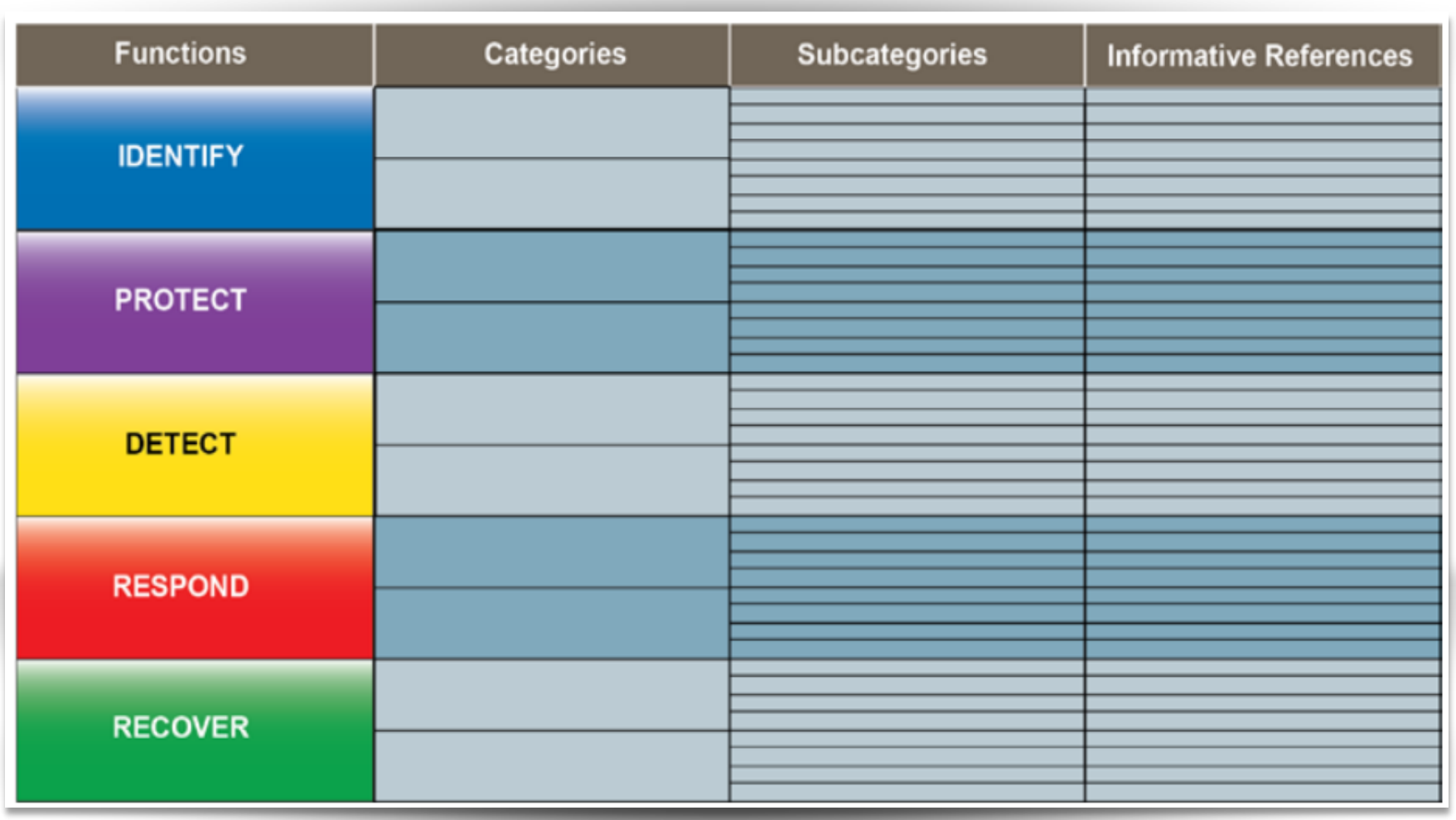
Manage and Mitigate #1 risk in 21st century

“REPUTATIONAL RISK”

“Cyber Drill” : Testing User Responsive & Readiness

การเตรียมความพร้อมของผู้ใช้ระบบสารสนเทศทั่วไป (User Readiness and Responsiveness by performing Cyber Drill) และการให้ความรู้ด้านภัยสารสนเทศ (User Information Security Awareness Training by performing Information Security Awareness Training) จึงเป็นเรื่องจำเป็นที่องค์กรต้องทำเป็นประจำ ทุกปี
ยกตัวอย่าง เรื่องการซ้อมหนีไฟ (Fire Drill) องค์กรยังมีการซ้อมอยู่เป็นประจำทุกปี แล้วทำไมองค์กรไม่ทำการซ้อมรับมือภัยทางไซเบอร์ที่เรียกว่า “ Cyber Drill” เพื่อให้ผู้ใช้คอมพิวเตอร์ในองค์กรตลอดจนผู้บริหารทั้งระดับกลางและระดับสูงได้ตระหนักรู้และสร้างประสบการณ์ในการรับมือกับภัยคุกคามอย่างได้ผลในทางปฏิบัติ มีความพร้อมต่อการรับมือ “ Incident” ต่าง ๆ ที่จะเกิดขึ้น

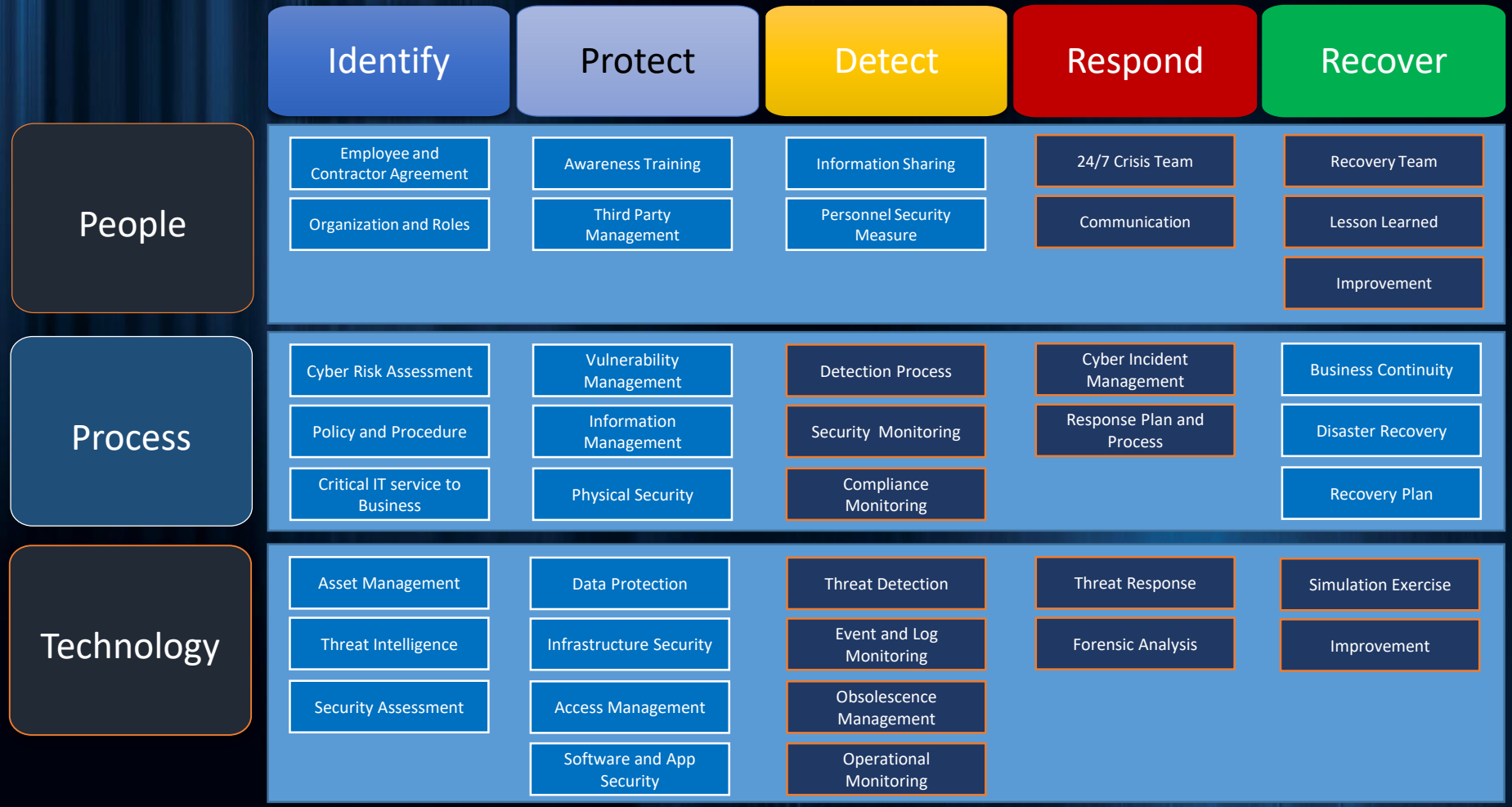
NIST Framework Core Structure



โครงสร้างองค์ประกอบของกรอบการดำเนินงานหลักด้านความมั่นคงปลอดภัยไซเบอร์

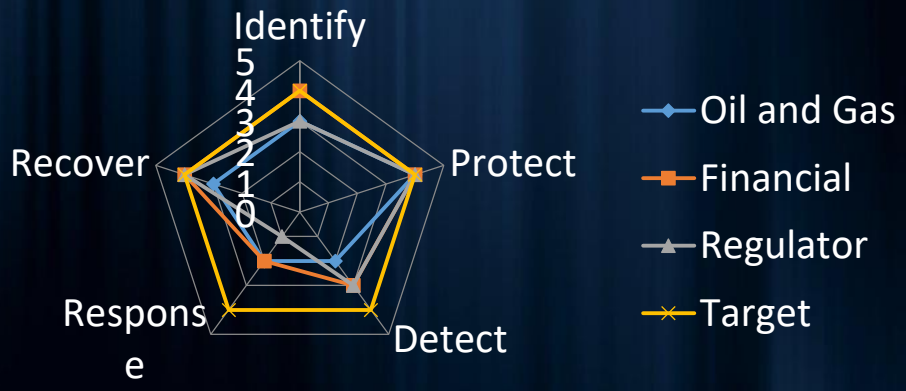
Source: “Framework core structure”, Framework for Improving Critical Infrastructure Cybersecurity, NIST, 12-Feb-2014

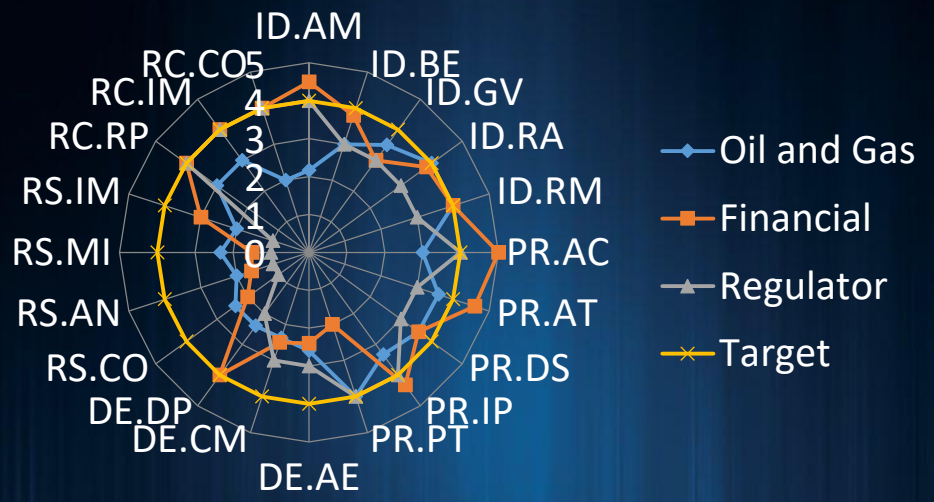
CYBERTRON


Identify
Protect
Detect
Respond
Recover
People
Employee and Contractor Agreement
Organization and Roles
Awareness Training
Third Party Management
Information Sharing
Personnel Security Measure
24/7 Crisis Team
Communication
Recovery Team
Lesson Learned
Improvement
Process
Cyber Risk Assessment
Policy and Procedure
Critical IT service to Business
Vulnerability Management
Information Management
Physical Security
Detection Process
Security Monitoring
Compliance Monitoring
Cyber Incident Management
Response Plan and Process
Business Continuity
Disaster Recovery
Recovery Plan
Technology
Asset Management
Threat Intelligence
Security Assessment
Data Protection
Infrastructure Security
Access Management
Software and App Security
Threat Detection
Event and Log Monitoring
Obsolescence Management
Operational Monitoring
Threat Response
Forensic Analysis
Simulation Exercise
Improvement

CYBERTRON

Benchmarking between your organization and Industries

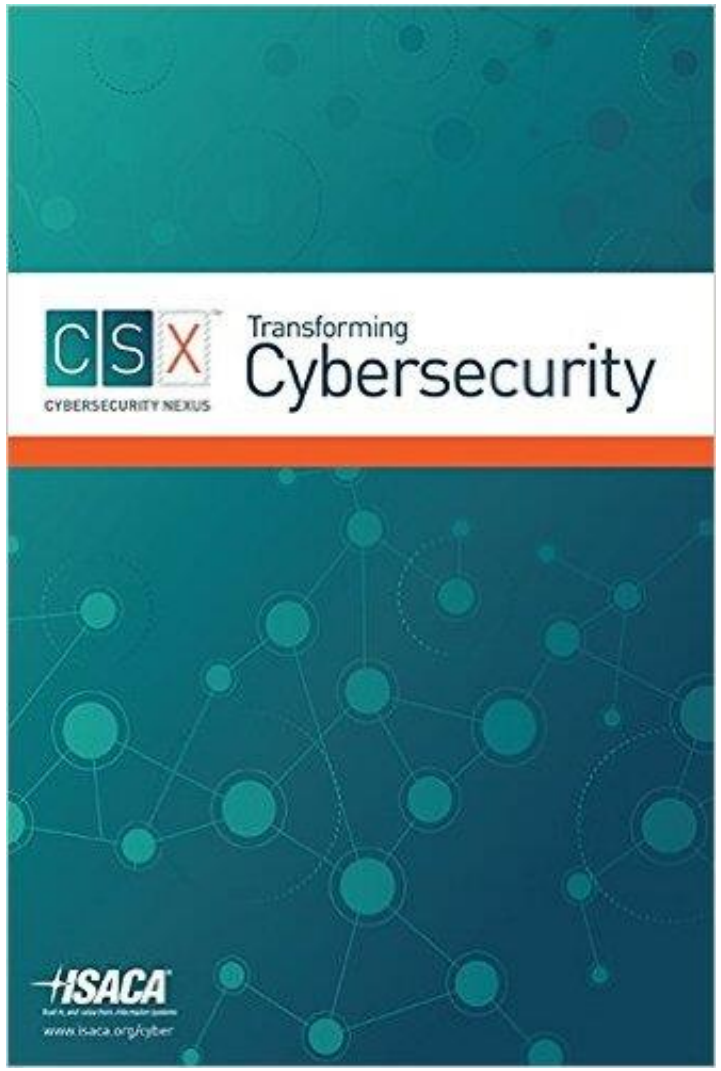




Cybersecurity Transformation Strategy

ACIS - CYBERTRON
CYBERSECURITY RESILIENCE FRAMEWORK

ISACA



TRANSFORMING
CYBERSECURITY
USING COBIT®5

COBIT 5 AN ISACA® FRAMEWORK ISACA

CONTENTS

CYBERTRON

DHS/SEI/CMU
Cyber Resilience Review (CRR)

Cyber Resilience Review (CRR):
Method Description and
Self-Assessment User Guide

February 2016

Homeland Security

CYBERTRON

DHS/SEI/CMU
Cyber Resilience Review (CRR) 10 Domains

WHAT DOES THE CRR MEASURE?

The CRR measures an organization's operational resilience capabilities through examining cybersecurity practices across ten domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

ภาพรวมกฎหมายที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ

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

กฎหมายสำคัญด้านเทคโนโลยีสารสนเทศ/ความมั่นคงปลอดภัยสารสนเทศ

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

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
หน่วยงานของรัฐ (ส่วนราชการ รัฐวิสาหกิจ ฯลฯ)

พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551
ผู้ประกอบธุรกิจให้บริการการชำระเงินทางอิเล็กทรอนิกส์

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553
- ระดับเคร่งครัด
- ระดับกลาง
- ระดับพื้นฐาน

หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure: CI)

พระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (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

พระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. 2561

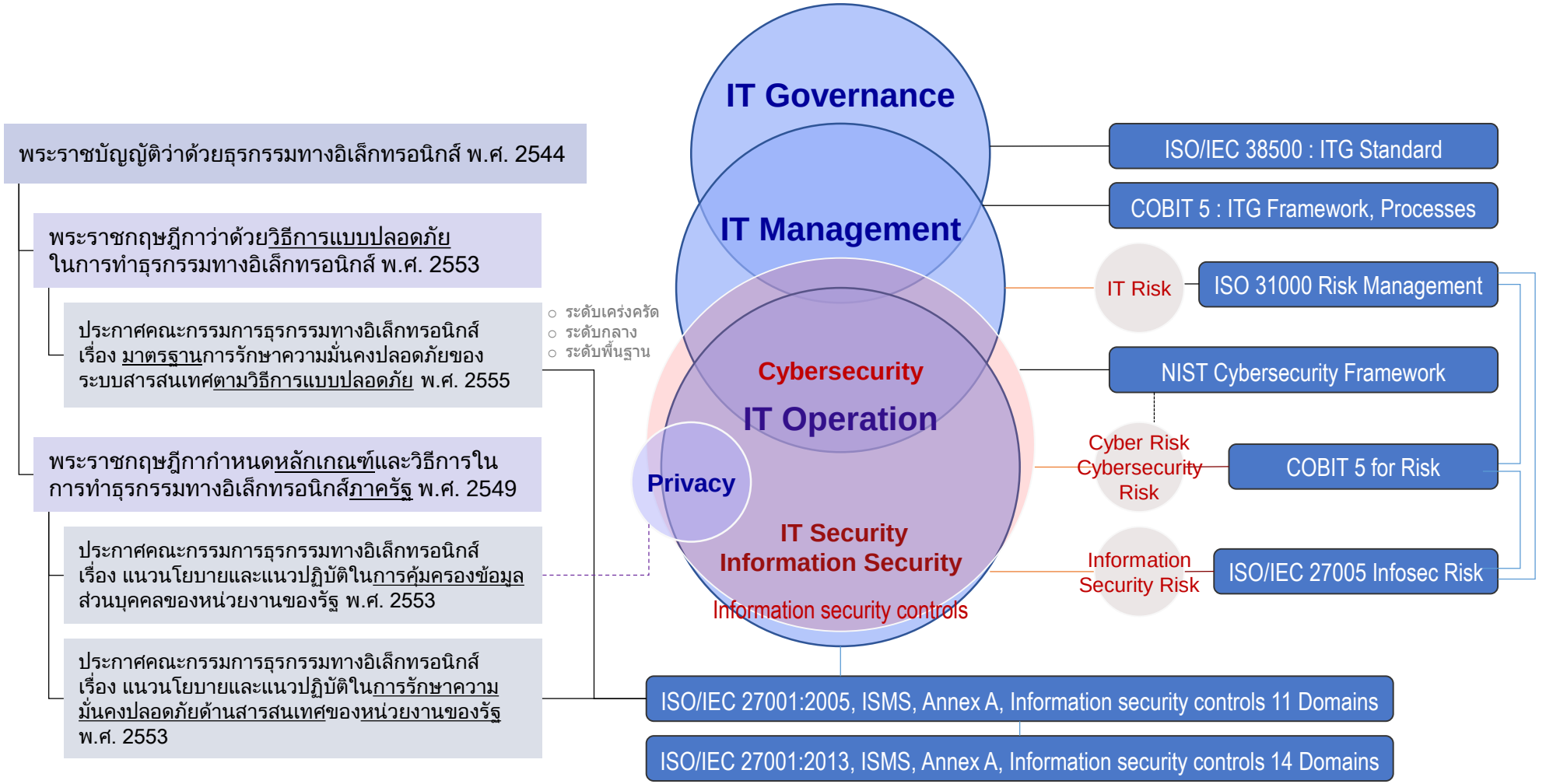
พระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม (ฉบับที่ 2) พ.ศ. 2560

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562

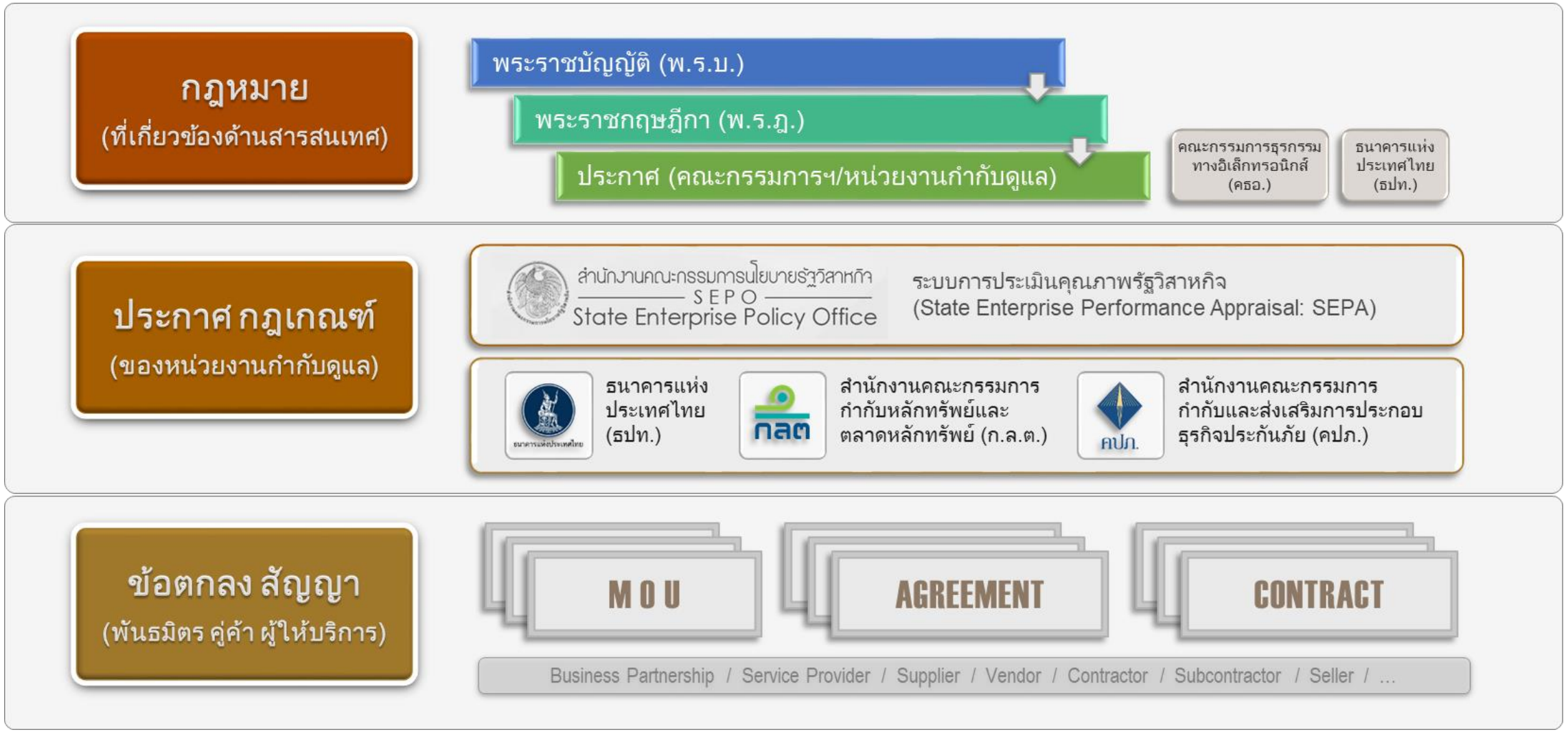
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ประกาศในราชกิจจานุเบกษา 27 พฤษภาคม 2562

ชุดกฎหมายดิจิทัล

Integrating IT-GRC, IT & Information Security and Cybersecurity Approach "Regulatory Compliance" and "Standards & Best Practices"

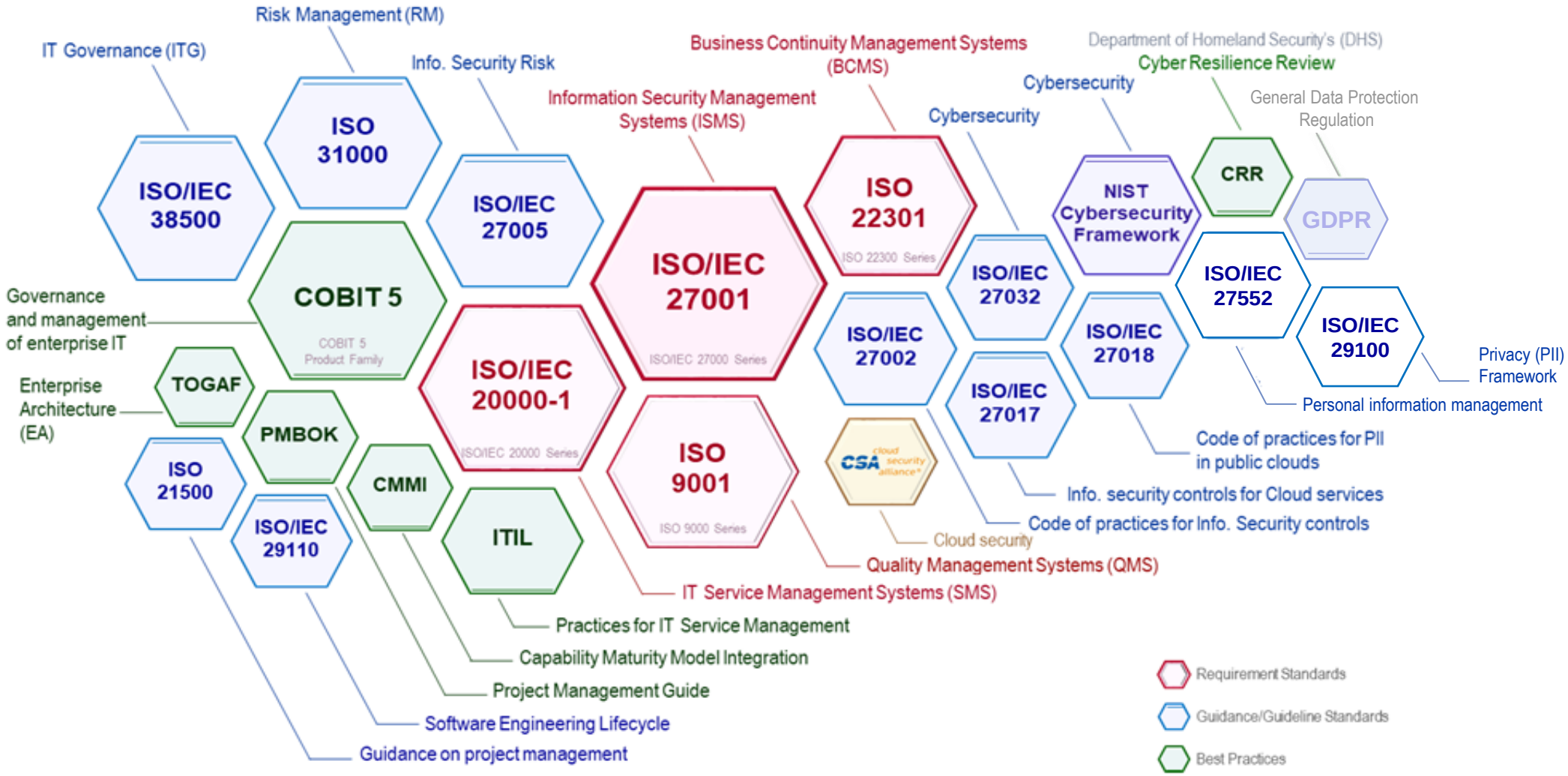


External Regulatory Compliance



Risk-based IT-GRC Standards and Best Practices

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



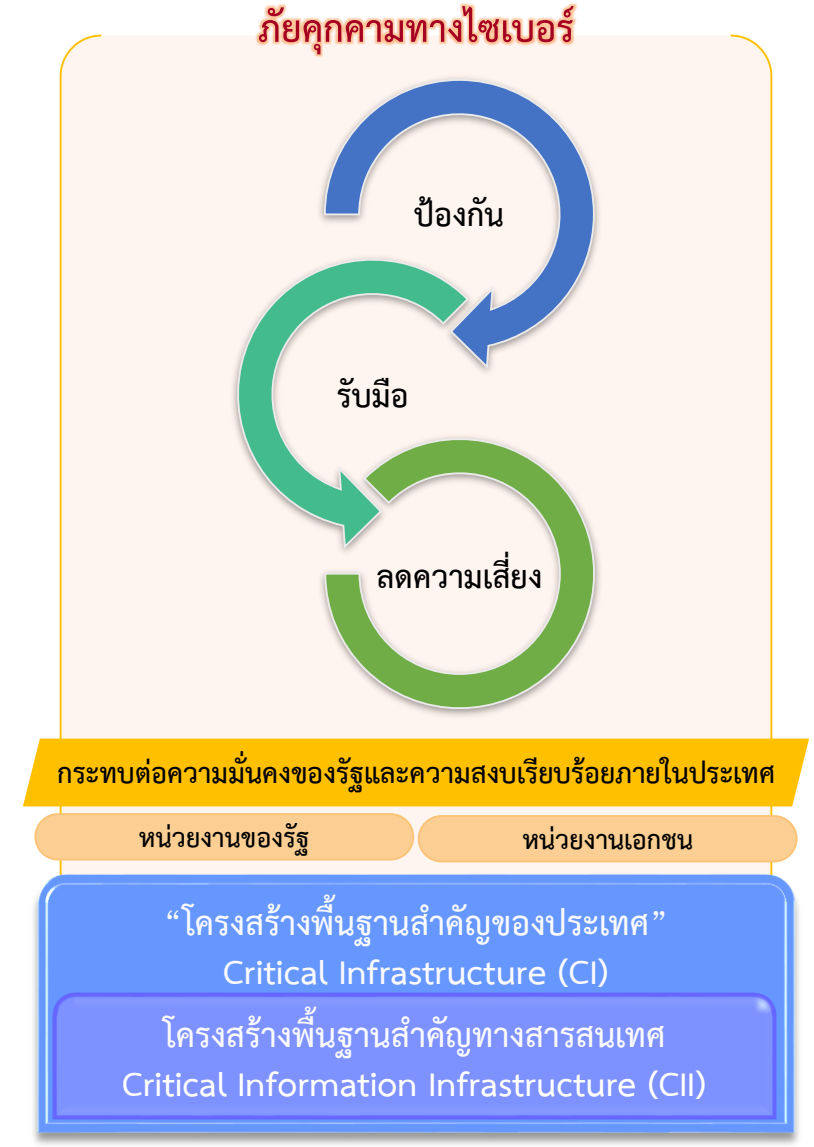
Source: ACIS research, www.acisonline.net

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

เหตุผลและความจำเป็น

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ
ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

เพื่อให้สามารถป้องกันภัยคุกคามดังกล่าวได้อย่างทันท่วงที
โดยไม่ปล่อยให้นานจนเกิดผลกระทบกับประชาชน



มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับ ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๓ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่และอำนาจ ดังต่อไปนี้
(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ในการกำหนด**กรอบมาตรฐาน**ตามวรรคหนึ่ง (๔) ให้คำนึงถึง**หลักการบริหารความเสี่ยง** โดยอย่างน้อยต้องประกอบด้วย**วิธีการและมาตรการ** ดังต่อไปนี้

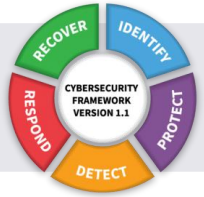
(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์



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.

NIST Cybersecurity Framework

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPONSE	RECOVER
Asset Management	Identity Management and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Strategy	Protective Technology			
What processes and assets need protecton?	What safeguards are available?	What techniques can identify incidents?	What techniques can contain impacts of incidents?	What techniques can restore capabilities?
พ.ร.บ. ไซเบอร์	การระบุความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น	มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์	มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	มาตรา 13 (4)

กฎหมายสำคัญที่เกี่ยวข้องด้านการคุ้มครองข้อมูลส่วนบุคคล

Data Protection Laws

1.0 พระราชบัญญัติ ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

1.1 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

1.1.2 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

หน่วยงานภาครัฐ (ส่วนราชการ รัฐวิสาหกิจ ฯลฯ)
Government agencies, State Enterprise

การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy)

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด
2. คุณภาพของข้อมูลส่วนบุคคล
3. การระบุวัตถุประสงค์ในการเก็บรวบรวม
4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้
5. การรักษาความมั่นคงปลอดภัย
6. การเปิดเผยเกี่ยวกับการดำเนินการแนวปฏิบัติและนโยบายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
7. การมีส่วนร่วมของเจ้าของข้อมูล
8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

การจัดทำแนวปฏิบัติ (ข้อปฏิบัติ) การคุ้มครองข้อมูลส่วนบุคคล (Practices)

หลักการด้านการคุ้มครองข้อมูลส่วนบุคคล
(Reference OECD Privacy Principles)

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Source: "OECD Privacy Principles"; "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", http://oecdprivacy.org/

Gap

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Personal Data Protection

หน่วยงานองค์กรทั่วไป
All Enterprises in Thailand

หลักการคุ้มครองข้อมูลส่วนบุคคล

Principles for Personal Information/Data Protection (Privacy)

OECD The OECD Privacy Principles

Electronic Transactions Commission ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ 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	หลักการการระบุวัตถุประสงค์ :	• 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

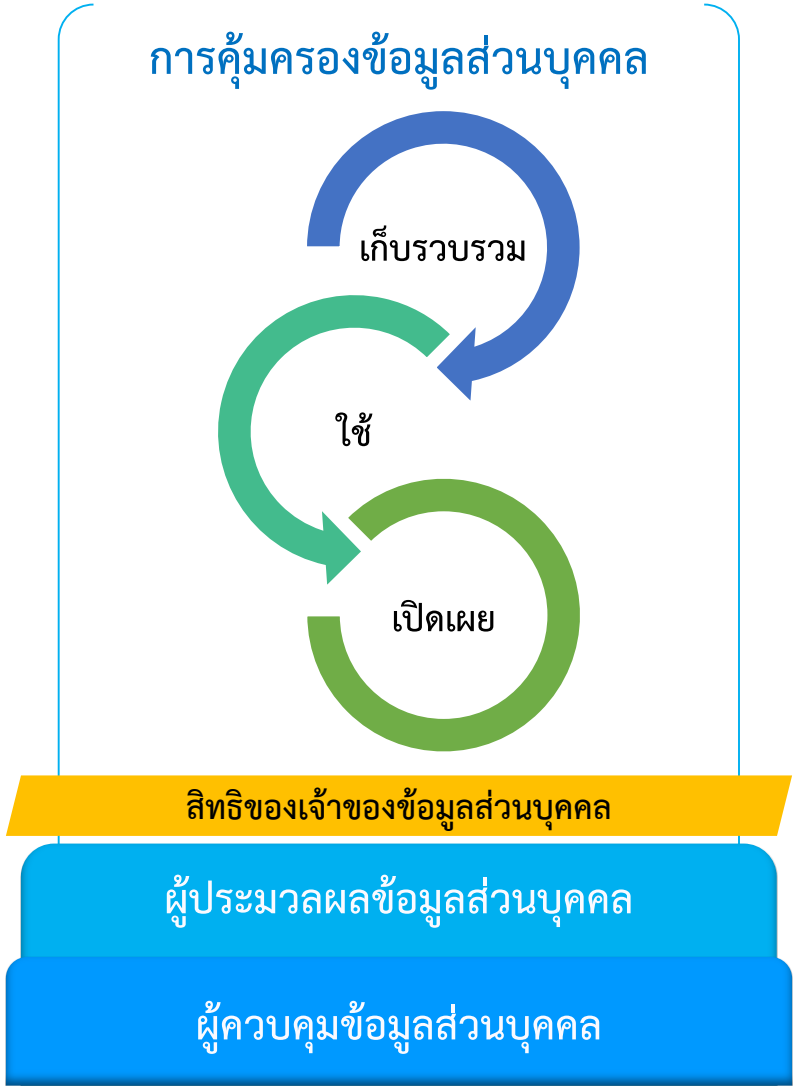
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

เหตุผลและความจำเป็น

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการโดยทั่วไป

สอดคล้องตามหลักการสากล และ GDPR



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

Cyber Defense Initiative Conference
www.cdicconference.com

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

ขอบคุณครับ

www.youtube.com/thehackertv

www.youtube.com/thecyber911

Prinya.ho@acisonline.net

www.twitter.com/prinyaACIS (@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

BBC | Sign in | News | Sport | Reel | Worklife | Travel | Future | Mo

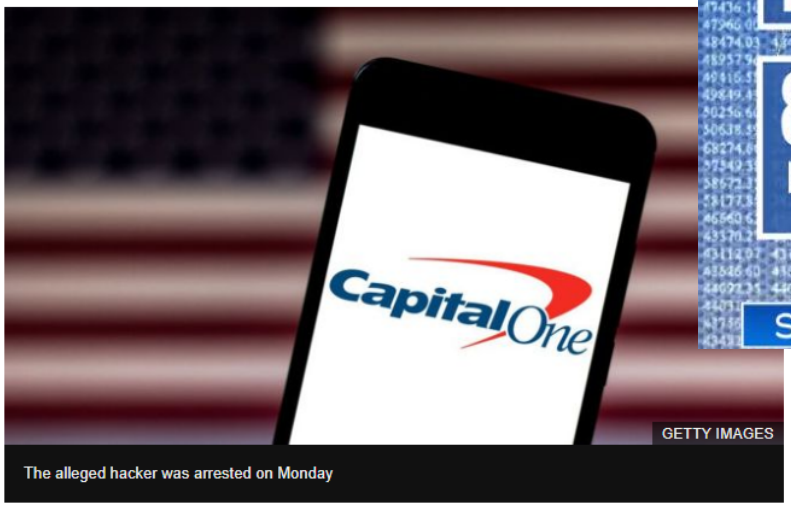
NEWS

Home | Video | World | Asia | UK | Business | Tech | Science | Stories | Entertainment &

US & Canada

Capital One data breach: Arrest after details of 106m people stolen

30 July 2019



The alleged hacker was arrested on Monday

The personal details of about 106 million individuals across the US and Canada were stolen in a hack targeting financial services firm Capital One, the company has revealed.

The alleged hacker, Paige Thompson, was arrested on Monday after reportedly boasting about the breach online.

Capital One said the data included names, addresses and phone numbers of people who applied for its products.

But the hacker did not gain access to credit card account numbers, it said.

The data breach is believed to be one of the largest in banking history.

- 106 million personal data (income, birth date) who apply for credit card are hacked
  80,000 bank account number
  140,000 social security number

GDPR (General Data Protection Regulation) cased

DATAINSIDER
Digital Guardian's Blog

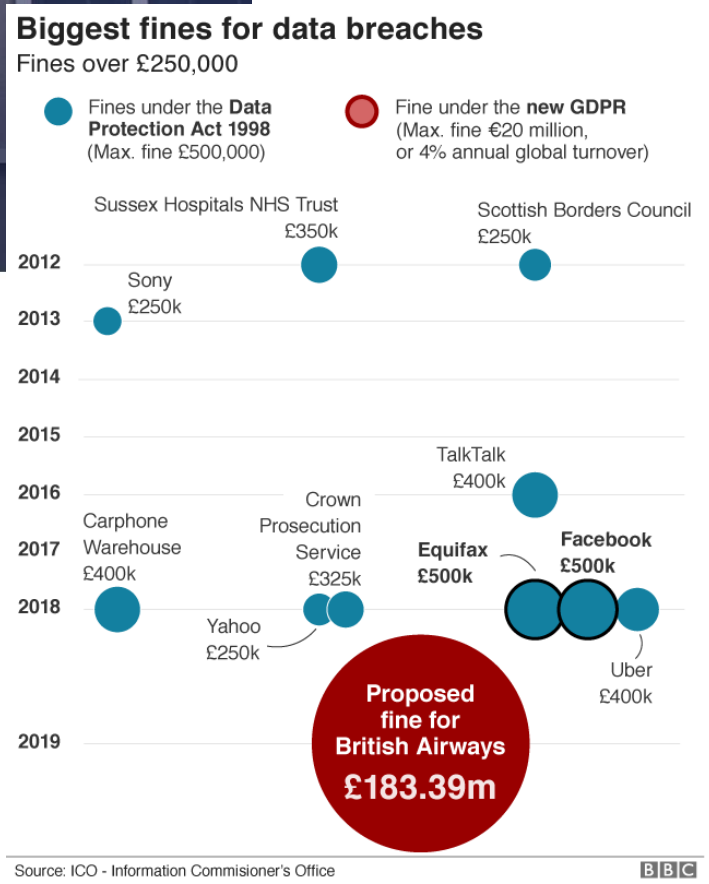
Popular Topics: Data Protection | Security News | Threat Research | Industry Insights | Search Digital Guardian

GlobalSign Blog

14 Nov 2018

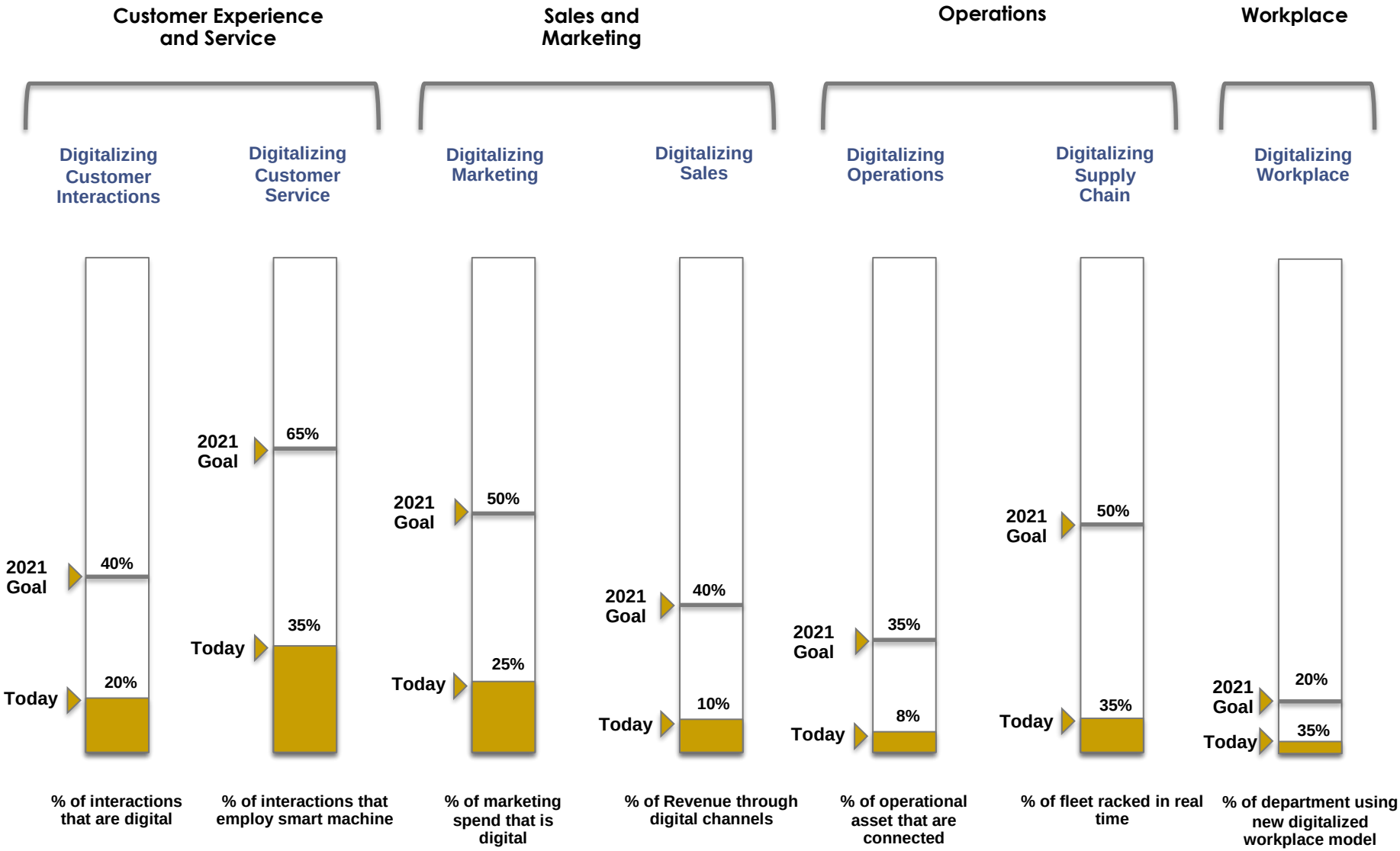
How Well did British Airways Handle Their Data Breach? A GDPR Case Study

In September 2018, leading airline British Airways announced that it had suffered a data breach and that customer data had been lost. The company released details that the theft had occurred between 21 August 2018 and 5 September 2018, and that as many as 380,000 transactions had been affected.



DBS Digital Strategy

Digital Business KPIs for Optimizing Current Business Model



Digital Business KPIs for New Revenue and Business Models