DGA Digital Government Development Agency

TDGA THAILAND DIGITAL GOVERNMENT ACADEMY

LIVE TALK

ภัยคุกคามไซเบอร์ กับวิถีชีวิตรูปแบบใหม่

Cyber Threats in New Normal

แนะไอเดียรับมือยุคดิจิทัลไลฟ์ ด้วย 2 ผู้เชี่ยวชาญในวงการ IT

วันที่ 3 กรกฎาคม 2563 เวลา 14.00 – 15.00 น.

ดร.ปริญญา หอมเอนก
กรรมการผู้ทรงคุณวุฒิ
ในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ดร.ธัชพล โปษยานนท์
ผู้อำนวยการศูนย์ความเป็นเลิศด้านดิจิทัล มหาวิทยาลัยหอการค้าไทย

LIVE

ชมสดผ่านทาง
DGA THAILAND

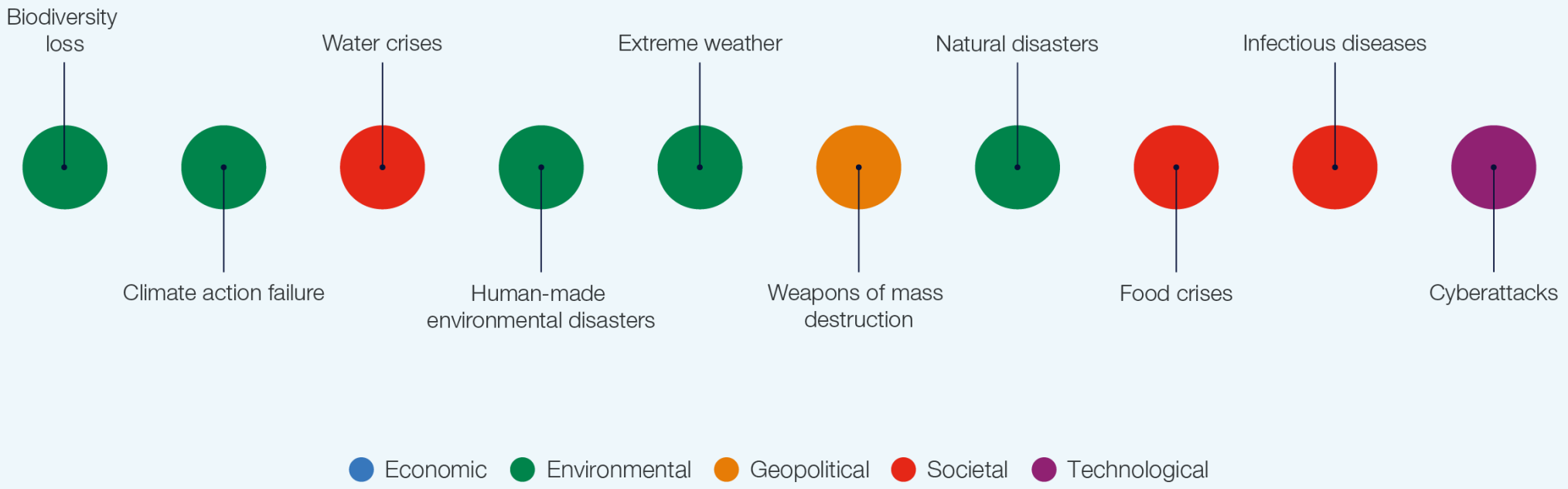
นำเสนอโดย
สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
หรือ TDGA ร่วมกับ ฝ่ายปฏิบัติการ สพร.

TOP 10 RISKS OVER THE NEXT 10 YEARS

Long-Term Risk Outlook: Impact

WORLD ECONOMIC FORUM

Global Shapers



Global Risks Report 2020

Note: The Global Shapers Community is the World Economic Forum's network of young people driving dialogue, action and change.

http://reports.weforum.org/global-risks-report-2020/shareable-infographics/

ACIS © All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

Thailand Update 2019/2021

- Privacy and Cybersecurity are Converging around the World (and in Thailand)
- Thailand Cybersecurity Act : 27 May 2019
- Thailand Personal Data Protection Act (PDPA) : 27 May 2019 => 31 May 2021
- **Thailand Cybersecurity Minimum Requirement for PDPA (July 2020)**
- NIST Cybersecurity Framework Implementation for Thai CI/CII
- ISO/IEC TR 27103 : Cybersecurity and ISO and IEC Standards (ref. NIST CSF)
- ISO/IEC 27001 (ISMS) as Fundamental Standard for Information Security and Cybersecurity
- ISO/IEC 27701, ISO/IEC 29100, GDPR, NIST Privacy Framework as Reference Principle Knowledges
- Thailand Industry is moving from Cybersecurity to Cyber Resilience
- NICE Framework (NIST SP800-181) for Cybersecurity Workforce Development
- **Digital Transformation needs Cybersecurity Transformation**

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

The New Normal

© ACIS Professional Center Company Limited All right reserved.

Towards: "Responsive Security"

Responsive & Readiness Mentality

Fortress Mentality

Are we ready ?

Are we secure ?

Risk-based: Value Preservation

Source: ACIS Research

ACIS © All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

SAGEFOX

Top Ten Cybersecurity and Privacy Trends

2020

ACIS © All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

Top Ten Cybersecurity and Privacy Trends 2020

1. **Cyber Fraud with a Deepfake**
   (Cyber Fraud with the Deepfake and the Dark side of AI)
2. **Beyond Fake News**
   (It's a Real News based-on a True Story that intentionally attack someone/some organization)
3. **Cyber Sovereignty and National Security Issues in the Long Run**
   (That include rising in state sponsor attacks; Data Sovereignty: What's Next for Data Privacy)
4. **'Cyberattack and Data Breach' : A New Normal in Cybersecurity**
   (Cybersecurity Mindset of Top Managements need to be changed)
5. **Tighten in Cybersecurity and Data Protection Regulatory Compliance**
   (Focus on Cyber Resilience, Data Governance, Data Sovereignty when Value Preservation is crucial topic)

Source: ACIS / Cybertron Research LAB

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

Top Ten Cybersecurity and Privacy Trends 2020

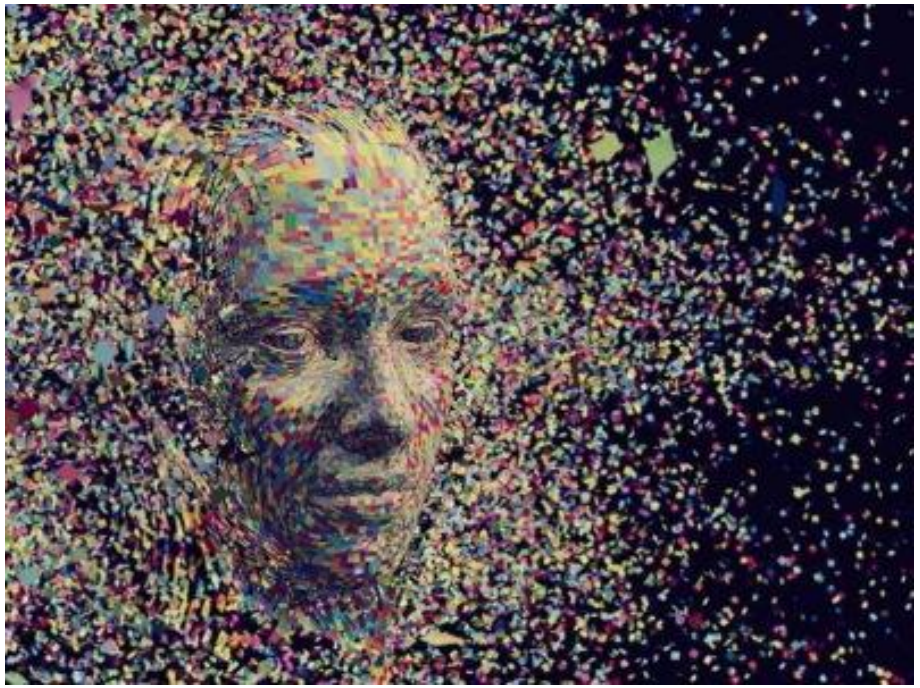
6. **"Data Breaches" as Top Concerns for Business**
   (Zero Day Exploitation, Cloud Misconfigurations including Human Errors/Digital Footprint in the Clouds)
7. **Orchestration & Automation Boosting Security Staff Effectiveness**
   (From MSSP to MDR, Using AI and Automation to improve IR Capability)
8. **Increasing on Impact of State-Sponsored Cyberattacks**
   (Cyberattack on Critical Infrastructure for example Energy Grids are at risk)
9. **The Cybersecurity Skills Gap Crisis**
   (More CISOs Earning a Seat at the Table)
10. **5G Networks require New Approaches to Cybersecurity**
    (EU Report Highlights Cybersecurity Risks in 5G Networks: Securing the Transition to 5G)

Source: ACIS / Cybertron Research LAB

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

1. Cyber Fraud with a Deepfake

(Cyber Fraud with the Deepfake and the Dark side of AI)



Source: digital image retrieved from https://www.securityworldmarket.com/int/News/Business-News/panda-shines-a-light-on-the-dark-side-of-ai#.XczqbVczY5s

การหลอกลวงได้อย่างแนบเนียนด้วยเทคโนโลยี Deepfake

Deepfake Technology เป็นการนำด้านมืดของ AI มาใช้ในการหลอกลวงด้วยการสร้างวิดีโอปลอมแปลงเป็นบุคคลนั้น ๆ จากจุดแข็งของ AI ที่สามารถเก็บข้อมูลมาประมวลผล วิเคราะห์ และเรียนรู้สิ่งต่าง ๆ ทำให้สามารถสร้างวิดีโอปลอมแปลงขึ้นมาได้ค่อนข้างเหมือนจริง เช่น การปลอมแปลงเป็น ประธานาธิบดี ดอนัลด์ จอห์น ทรัมป์ สามารถทำได้โดยการตัดต่อใบหน้าจากคนอื่นเป็น ประธานาธิบดีทรัมป์ โดย AI จะเรียนรู้สีหน้าใบหน้า การขยับปากเมื่อพูด หรือการขยับใบหน้าต่าง ๆ จาก ประธานาธิบดีทรัมป์ มาตัดต่อแทนที่ใบหน้าคนอื่น ซึ่งในความเป็นจริงบุคคลนั้นสามารถพูดอะไรก็ได้แล้วตัดต่อให้เป็นใบหน้าของประธานาธิบดีทรัมป์ได้โดยดูแทบไม่ออกเลย

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

2. Beyond Fake News

(It's a Real News based-on a True Story that intentionally attack someone/some organization)

Source digital image: Shutterstock

กระบวนการสร้างความเชื่อ Beyond Fake News

ภัยที่น่ากลัวกว่าข่าวปลอม (Fake News) เปรียบได้กับกระบวนการล้างสมอง (Brainwashing) สามารถทำได้โดยทำการสร้างภาพการ์ตูนด้านลบ หรือ อินโฟกราฟฟิคด้านลบของบุคคลหรือสถาบันใดสถาบันหนึ่งขึ้นมาลงสื่อสังคมโซเชียลอย่างต่อเนื่อง และ เผยแพร่ออกไปเป็นระยะๆ ในเวลาที่ค่อนข้างยาว เช่น หลายเดือน หรือเป็นปี เพื่อตอกย้ำภาพด้านลบของบุคคลหรือสถาบันนั้นๆ โดยมีเป้าหมายให้คนที่ได้เห็นภาพการ์ตูนหรืออินโฟกราฟฟิคดังกล่าว เกิดความเชื่อทีละเล็กทีละน้อยสะสมไปเรื่อยๆ จนกระทั่งเป็นความเชื่ออย่างถาวร

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

3. Cyber Sovereignty & National Security Issues

in the long run

(That include rising in state sponsor attacks; Data Sovereignty: What's Next for Data Privacy)

Source digital image: Shutterstock

อธิปไตยไซเบอร์และระบบรักษาความปลอดภัยแห่งชาติ

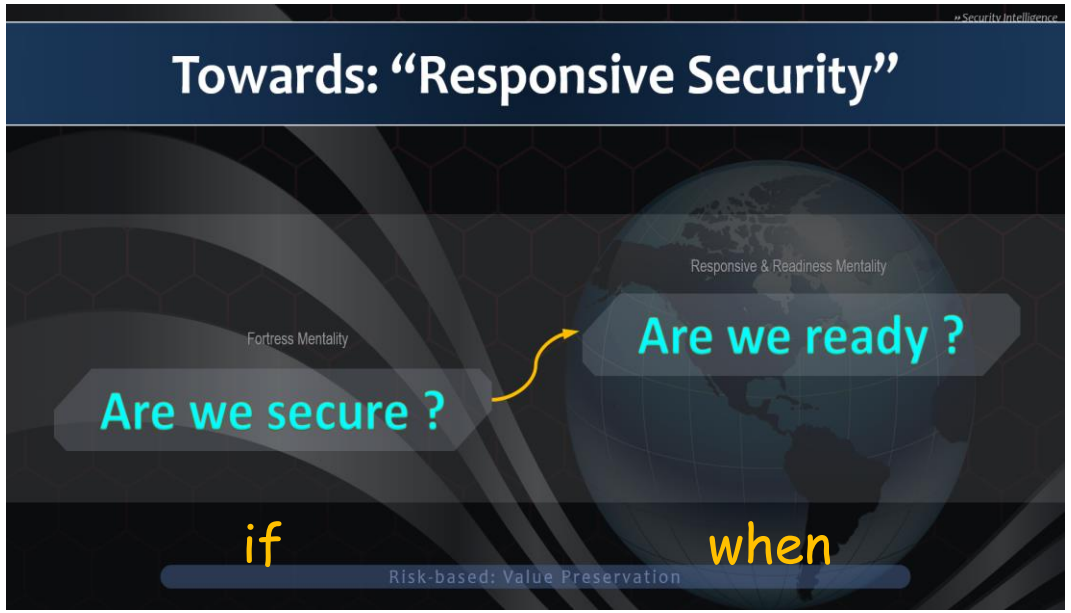
ในยุคข้อมูลคือ ขุมทรัพย์แห่งใหม่ หรือ การที่มีผู้กล่าวไว้ว่า "Data is the New Oil" นั้นแฝงมาด้วยปัญหาอธิปไตยไซเบอร์ (Cyber Sovereignty) ที่ผู้คนบนโลกใบนี้ล้วนนำข้อมูลส่วนหนึ่งของชีวิตตนไปเก็บไว้บนโลกออนไลน์ที่เราเรียกว่า "Digital Footprint" ไม่ว่าจะเป็นการใช้แพลตฟอร์มใดก็ตาม ข้อมูลเหล่านั้นล้วนเป็นข้อมูลส่วนตัว ข้อมูลทางธุรกิจ หรือ ข้อมูลอื่นๆ ที่เจ้าของแพลตฟอร์มสามารถนำไปศึกษาวิเคราะห์เพื่อใช้ประโยชน์ต่อไปได้หากผู้ใช้บริการยินยอม (customer consent) ซึ่งอาจเป็นการรุกล้ำความเป็นส่วนตัว หรือ การรุกล้ำข้อมูลทางธุรกิจที่ผู้ใช้บริการไม่รู้ตัวหรือไม่อาจจะหลีกเลี่ยงได้

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

4. ‘Cyberattack and Data Breach’ : A New Normal in Cybersecurity

(Cybersecurity Mindset of Top Managements need to be changed)

(ต่อ)



ดังนั้น mindset ของผู้บริหารระดับสูงคงต้องเปลี่ยนจาก “if” เป็น “when”

ความปกติใหม่ – The New Normal in Cybersecurity

ดังนั้น องค์กรต้องเตรียมพร้อมและบริหารจัดการความเสี่ยงที่จะเกิดขึ้น ผู้บริหารจึงจำเป็นต้องมีการวางแผนสำรองเมื่อถูกจู่โจมทางไซเบอร์ เนื่องจากทุกวันนี้ เราอยู่บนโลกที่เรียกว่า VUCA World คืออยู่กับ “ความไม่แน่นอน” ที่กลายเป็นความแน่นอนที่เราต้องเผชิญ ได้แก่

- Volatility- ความผันผวน
- Uncertainty- ความไม่แน่นอน
- Complexity – ความซับซ้อน
- Ambiguity – ความคลุมเครือ

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

5. Tighten in Cybersecurity & Data Protection Regulatory Compliance

(Focus on Cyber Resilience, Data Governance, Data Sovereignty when Value Preservation is crucial topic)

(ต่อ)

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

หน้า ๒๐
เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

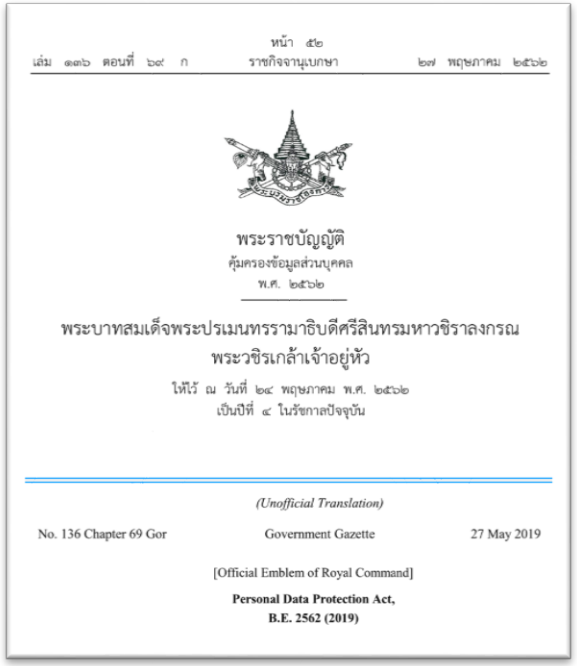
(Unofficial Translation)

No. 136 Chapter 69 Kor Government Gazette 27 May 2019

[Official Emblem of Royal Command]

Cybersecurity Act,
B.E. 2562 (2019)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



หน้า ๕๒
เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

(Unofficial Translation)

No. 136 Chapter 69 Gor Government Gazette 27 May 2019

[Official Emblem of Royal Command]

Personal Data Protection Act,
B.E. 2562 (2019)

การประกาศบังคับใช้ของกฎหมาย

ดังนั้น ประเทศไทยจึงมีความจำเป็นจะต้องมีกฎหมายด้านไซเบอร์ไม่ว่าจะเป็น พระราชบัญญัติการรักษาความปลอดภัยมั่นคงไซเบอร์ และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงพระราชบัญญัติฉบับอื่นๆ ที่เกี่ยวกับดิจิทัล

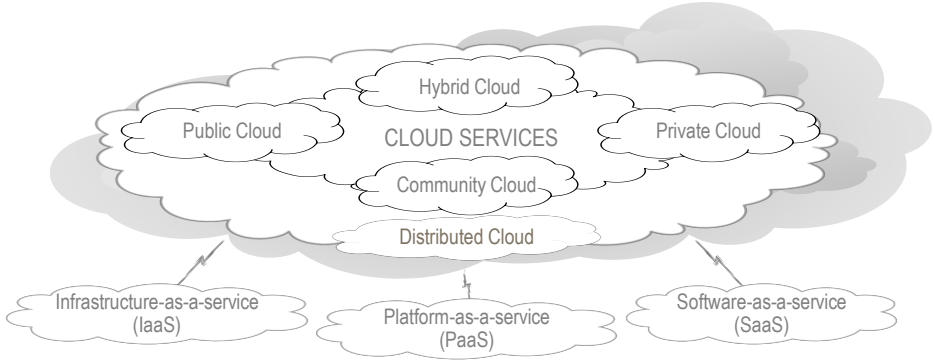
© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

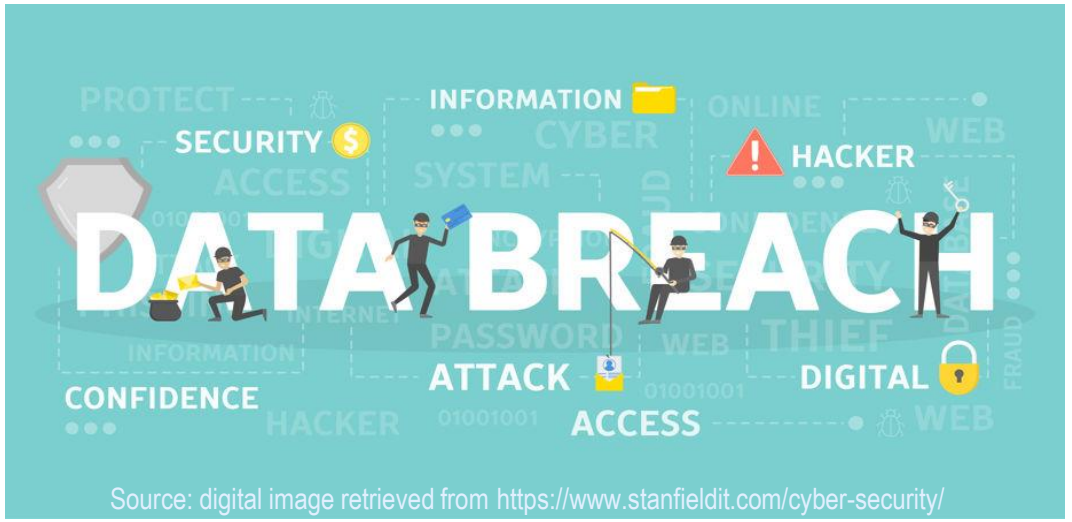
6. “Data Breaches” as Top Concerns for Business

(Zero Day Exploitation, Cloud Misconfigurations including Human Errors/Digital Footprint in the Clouds)

การเจาะขโมยข้อมูลเป็นปัญหาใหญ่ขององค์กร

การเจาะช่องโหว่เพื่อขโมยข้อมูลจะเป็นประเด็นที่ธุรกิจต้องให้ความสนใจ ทั้งนี้ สาเหตุส่วนใหญ่มักเกิดจากการตั้งค่าบนระบบ Cloud ที่ไม่รัดกุมหรือไม่มั่นคงปลอดภัยเพียงพอ รวมไปถึงความผิดพลาดอันเนื่องมาจากตัวบุคคลที่ไม่ตระหนักในเรื่อง Cybersecurity หรือ Data Privacy องค์กรจึงควรเพิ่มมาตรการควบคุม เช่น การเข้ารหัสข้อมูล ตลอดจนการสร้างความตระหนักรู้ด้านภัยคุกคามและด้านการรักษาความมั่นคงปลอดภัยให้แก่บุคลากรภายในองค์กร



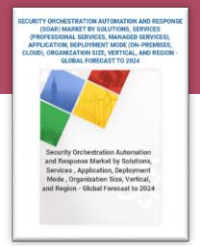


Source: digital image retrieved from https://www.stanfieldit.com/cyber-security/

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

7. Orchestration & Automation Boosting Security Staff Effectiveness

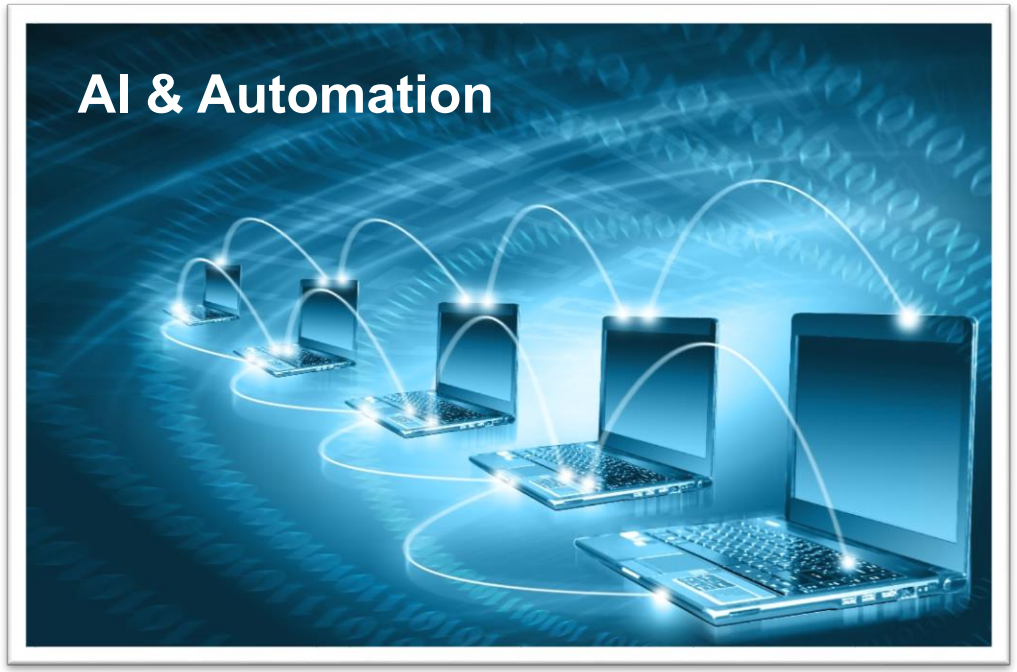
(From MSSP to MDR, Using AI and Automation to improve IR Capability)



https://www.researchandmarkets.com/reports/4833635/security-orchestration-automation-and-response

การใช้เทคโนโลยีในการรับมือกับภัยคุกคาม

การใช้เทคโนโลยี AI & Automation ในการรับมือกับภัยคุกคาม เนื่องจากปัจจุบันภัยคุกคามและการจู่โจมฉลาดขึ้น ทำให้ระบบรักษาความมั่นคงปลอดภัยมีความซับซ้อนและยุ่งยากเพิ่มขึ้นตามวิวัฒนาการของภัยคุกคาม ผู้ดูแลระบบต้องเผชิญกับการแจ้งเตือนและเหตุการณ์ด้านความมั่นคงปลอดภัยปริมาณมหาศาล จนเริ่มรับมือไม่ไหว



Source digital image: Shutterstock

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

8. Increasing on Impact of State-Sponsored Cyberattacks

(Cyberattack on Critical Infrastructure for example Energy Grids are at risk)

(ต่อ)

การโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญเพิ่มมากขึ้น

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) จำเป็นต้องมีกลไกในการปกป้องระบบโครงสร้างพื้นฐาน เพื่อป้องกันและบริหารจัดการตอบสนองต่อภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยการโจมตีในรูปแบบนี้อาจเปรียบเป็นเสมือนการทำสงครามรูปแบบใหม่ก็ว่าได้ ซึ่งการโจมตี “ทางไซเบอร์” ถูกกำหนดให้เป็น The Fifth domain หรือ โดเมนที่ 5 นอกจาก ทางบก, ทางน้ำ, ทางอากาศ และ ทางอวกาศ

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/

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

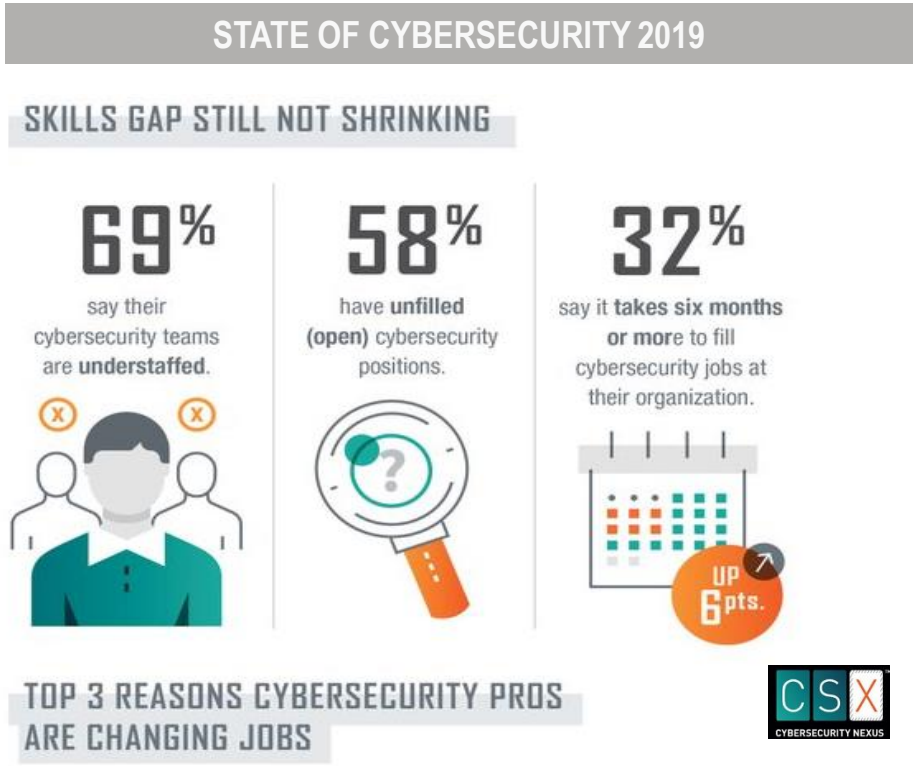
9. The Cybersecurity Skills Gap Crisis

(More CISOs Earning a Seat at the Table)

(ต่อ)

การขาดแคลนบุคลากร และบทบาทของ CISO ในองค์กร

เมื่อมีภัยไซเบอร์มากขึ้น และฉลาดขึ้น การขาดแคลนบุคลากรเป็นเรื่องที่ตามมา จากที่มีการขาดแคลนบุคลากรด้านระบบความมั่นคงปลอดภัยไซเบอร์อยู่แล้ว องค์กรจะยิ่งเผชิญกับการขาดแคลนบุคลากรที่มีทักษะด้านนี้อย่างหนักหน่วง เนื่องจากการโจมตีไซเบอร์จะกลายเป็นเรื่องปกติสามัญและกฎหมายดิจิทัลหลายฉบับได้ถูกบังคับใช้ ส่งผลให้ตลาดต้องการผู้ที่มีความสามารถด้านนี้เป็นอย่างมาก ในขณะที่ CISO (Chief Information Security Officer) จะถูกยกระดับขึ้นมาให้มีตำแหน่งเทียบเท่า CIO/CTO และขึ้นตรงกับ CEO แทน



Source: "State of Cybersecurity 2019", https://cybersecurity.isaca.org/state-of-cybersecurity www.isaca.org

10. 5G Networks require New Approaches to Cybersecurity

(EU Report Highlights Cybersecurity Risks in 5G Networks: Securing the Transition to 5G)

ความเร็วสูง 5G ทางด่วนของผู้ใช้และแฮกเกอร์

การมาถึงแห่งยุคของเครือข่าย 5G ทำให้เป็นการเปิดช่องทางใหม่ ๆ ให้แฮกเกอร์อย่างไม่ตั้งใจ โดยแฮกเกอร์สามารถโจมตีผู้ใช้โดยตรงได้มากยิ่งขึ้น เนื่องจากผู้ใช้สามารถ เชื่อมต่ออินเทอร์เน็ตความเร็วสูงได้โดยตรงง่ายขึ้น ไม่จำเป็นต้องผ่านระบบป้องกันหรือ Security Gateway ที่ช่วยกลั่นกรองอีกต่อไป อีกทั้งการที่อินเทอร์เน็ตมีความเร็วเพิ่มขึ้น ทำให้การมาถึงของภัยคุกคามก็ย่อมเร็วขึ้นมากเท่านั้น

Source: digital image retrieved from https://windstreetz.com/upcoming-5g-security-having-huge-security-threatstroubling-new-security-flaws-emerge/93184/

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

10. 5G Networks require New Approaches to Cybersecurity

(EU Report Highlights Cybersecurity Risks in 5G Networks: Securing the Transition to 5G)

(ต่อ)

ความเร็วสูง 5G ทางด่วนของผู้ใช้และแฮกเกอร์

สิ่งสำคัญที่ผู้ใช้ 5G จะป้องกันตนเองให้อยู่รอดปลอดภัยได้ดีที่สุด คือ การรู้เท่าทันเทคโนโลยี ด้วยการหมั่นหาความรู้เพิ่มเติม หมั่นสังเกต ตรวจสอบความผิดปกติของอุปกรณ์อยู่ตลอดเวลา

Source digital image: Shutterstock

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

ACIS © All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

The 11 Cyber Defense Tips to Stay Secure at Work and Home

credit : Center for Internet Security

Implementation: Stay secure at work and home

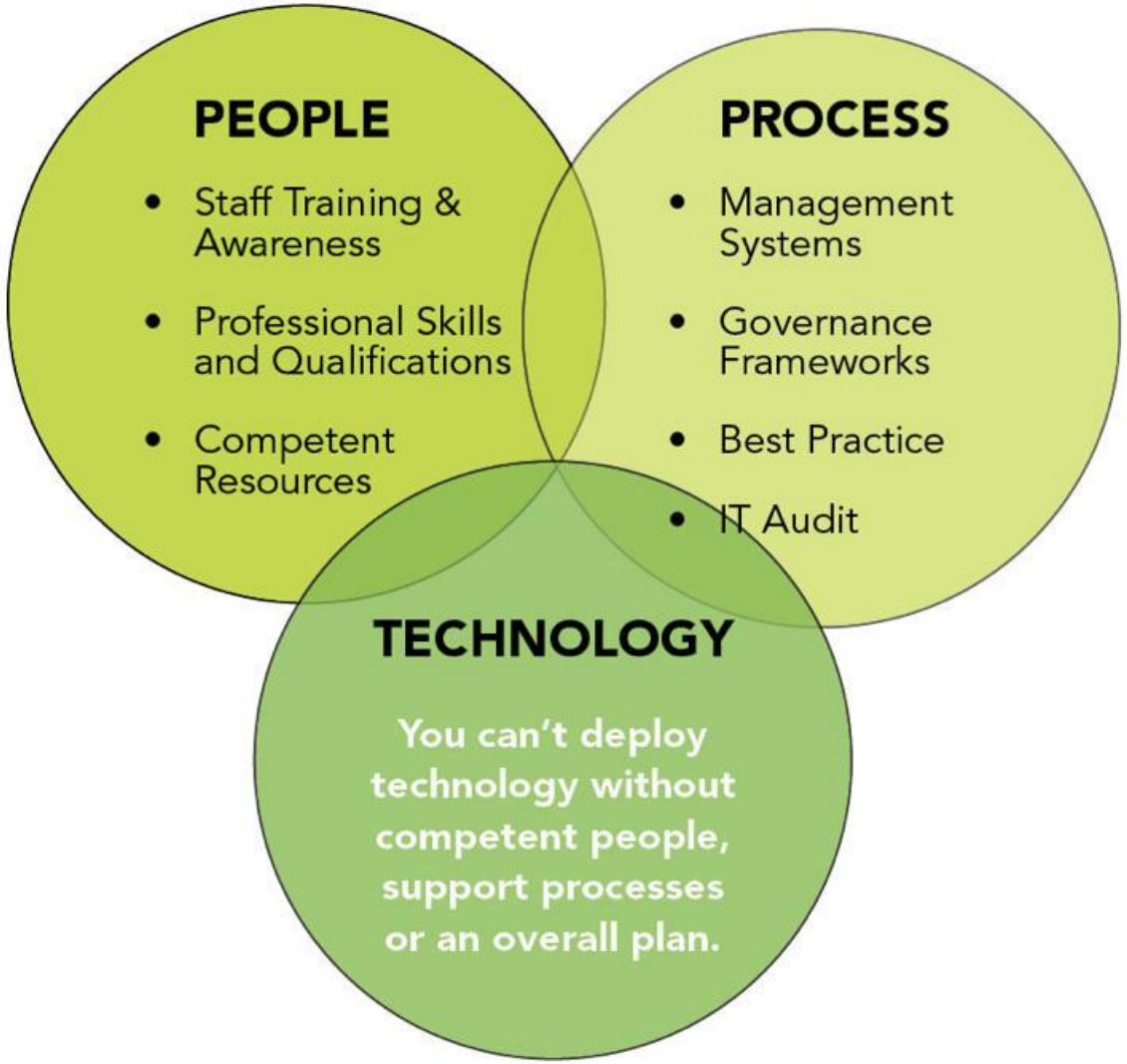
Stay secure at work and home with these 11 tips.

The line between our on- and off-line lives is shifting as technologies bring the internet into our workplaces, homes, and everywhere in between. Here are 11 cyber defense best practices for securing your digital systems and data.

1. Set some priorities.
2. Think before you click.
3. Don't get phished.
4. Go beyond the password.
5. Keep it fresh.
6. Reflect, then connect.
7. Shop smart, shop secure.
8. Avoid configuration confusion.
9. Don't be the bully.
10. Charge with caution.
11. If it matters, use multifactor.

© All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance

Back to the Basic : People Process Technology



ACIS © All rights reserved. IT-GRC, Cybersecurity, Privacy and Regulatory Compliance