Cyber Risk ที่เกี่ยวข้องกับผู้สอบบัญชี

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

นายพิรุฬน์ กิตติเดชปรีชา

Director – Risk Advisory บริษัท ดีลอยท์ ทู้ช โธมัทสุ ไชยยศ ที่ปรึกษา จำกัด

นายกษิภัท ธนิตธนาคุณ

กรรมการผู้จัดการ บริษัท เคที ไอที โซลูชั่น จำกัด

คณะทำงานศูนย์ความรู้ด้านการสอบบัญชีในธุรกิจที่มีระบบ IT ที่ซับซ้อน ในคณะกรรมการวิชาชีพบัญชีด้านการสอบบัญชี - สภาฯ

หัวข้อเสวนา

- ประเภทของความเสี่ยงด้าน IT
- ประเภทของความเสี่ยงด้าน Cyber
- ความเสี่ยงด้าน IT และ Cyber ที่มีผลกระทบต่อการสอบบัญชี

วัตถุประสงค์

เนื่องจากสถานการณ์ Covid-19 ทำให้ผู้สอบบัญชีและผู้ปฏิบัติงานด้านการสอบบัญชีต้องปรับเปลี่ยนการทำงานมาเป็นรูปแบบออนไลน์มากขึ้น คณะกรรมการวิชาชีพบัญชีด้านการสอบบัญชี โดยคณะทำงานศูนย์ความรู้ด้านการสอบบัญชีในธุรกิจที่มีระบบ IT ที่ซับซ้อน ซึ่งเป็นคณะทำงานภายใต้คณะสอบบัญชี ได้เล็งเห็นประเด็นจากการสอบบัญชีในรูปแบบออนไลน์ จึงเห็นควรให้จัดการเสวนานี้เพื่อให้ความรู้ด้านไอทีที่เกี่ยวกับการปฏิบัติงานด้านการสอบบัญชีในรูปแบบที่เข้าใจง่าย และสามารถนำไปปฏิบัติได้ **เพื่อให้ผู้สอบบัญชีเข้าใจถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) รวมถึง Cyber Risk ที่เกี่ยวข้องกับการสอบบัญชี และนำไปใช้ในการประเมินผลกระทบที่มีต่อแผนการตรวจสอบบัญชี**


1
Malware
2
www
Web-based attacks
3
Phishing
4
Web application attacks
5
Spam
TOP 15 CYBER THREATS
enisa
2020
European Union Agency for Cybersecurity.
6
DDoS
7
Identity theft
8
Data breach
9
Insider threat
10
Botnets
11
Physical manipulation, damage, theft and loss
12
Information leakage
13
Ransomware
14
Cyberespionage
15
Cryptojacking

Top Security and Risk Trends for 2021

01 Cybersecurity mesh

02 Cyber-savvy boards

03 Vendor consolidation

04 Identity-first security

05 Managing machine identities becoming a critical security capability

06 “Remote work” now just “work”

07 Breach and attack simulation

08 Privacy-enhancing computation techniques

gartner.com

Gartner®

CASE STUDY: Relevance of Cybersecurity Risk and Cyber Attacks to Financial Statements Audits

Deletion of Financial Reporting Data

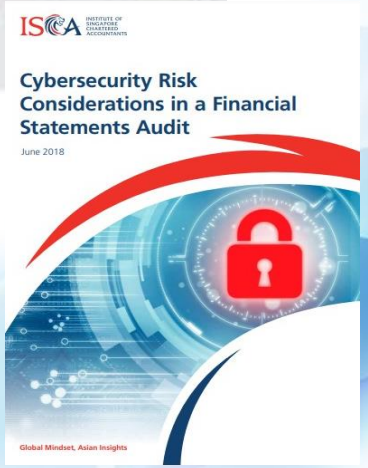
A manufacturing company was subject to a cyber attack, which deleted some of its financial reporting data. Without appropriate data backup and recovery controls, the company may not be able to present complete and accurate financial information.

DoS Attack to Online Retail Platform

An online retailer experienced a distributed DoS attack to its online retail platform, an attack to make the online service unavailable by overwhelming it with traffic from multiple sources. This resulted in customers being unable to place online orders for an extended period. This represents a business risk to the retailer with an opportunity cost of lost revenue when the system is down rather than a direct impact to the financials of the entity.

Loss of Customer Information

A financial institution experienced a cyber attack which resulted in the loss of sensitive customer information (credit card information). There appear to be no direct impact to the financial statements or the entity's assets. However, there may be other consequences arising such as penalties for breaching data privacy, potential lawsuits from affected customers, reputation damage, or even potential impairment and going concern issues, especially when the breach is material.



ที่มา https://isca.org.sg/media/2240014/isca-cyber-security-risk-report.pdf

“**IT (information technology) security** refers to protecting **data and information** systems from unauthorized access. It involves implementing processes that prevent the misuse, modification, or theft of sensitive company information. On the other hand, **cybersecurity** covers the protection of data on the internet- particularly from hackers and other cybercriminals.”

ที่มา https://securityboulevard.com

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk)

- ความเสี่ยงด้านธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance)
- ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)
- ความเสี่ยงด้านการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)
- ความเสี่ยงด้านการบริหารโครงการ (IT Project Management)
- ความเสี่ยงด้านการใช้บริการจากบุคคลภายนอก (IT Outsource)

ที่มา → ISO27001, BOT,SEC และ OIC

ความเสี่ยงด้านไซเบอร์ (Cyber Risk)

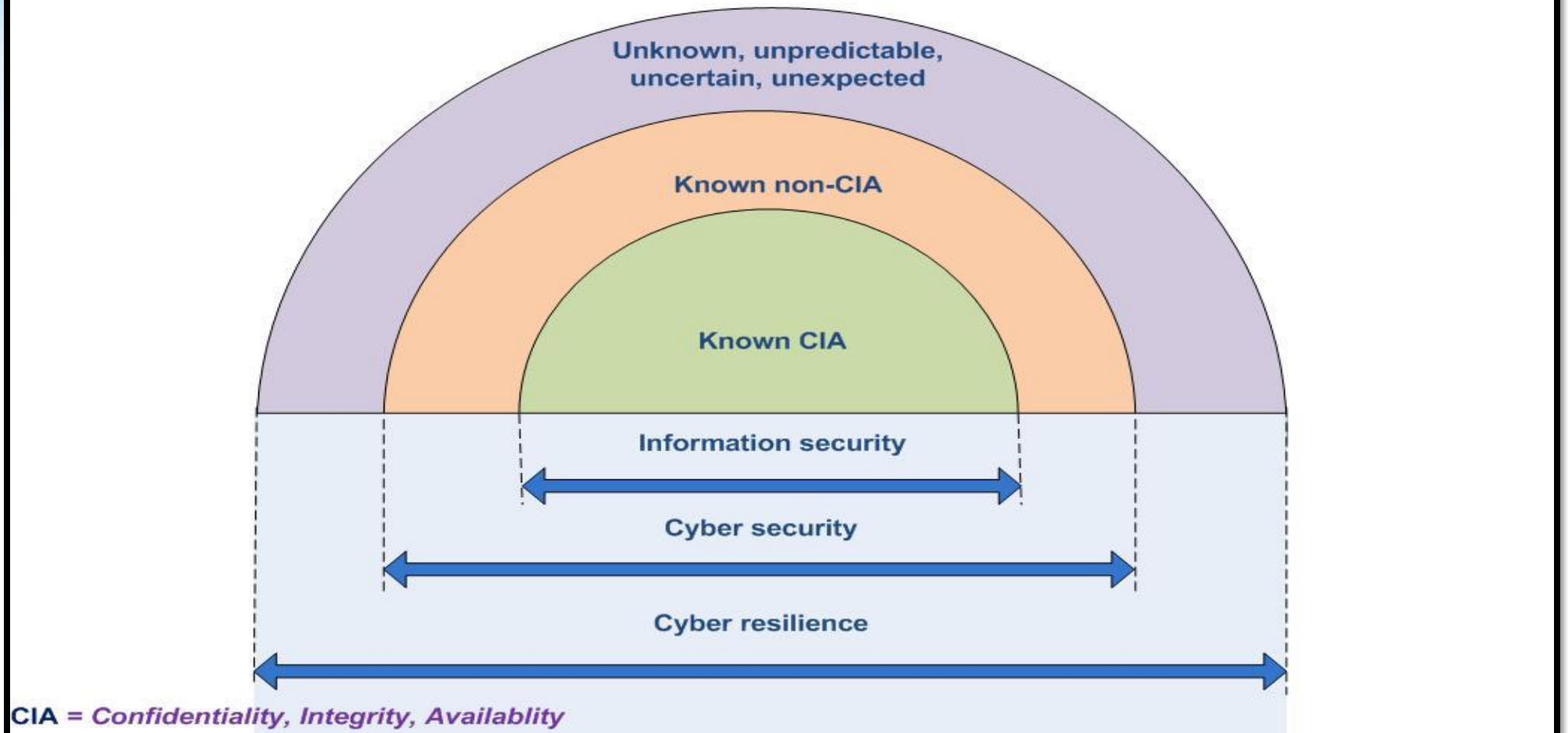
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของ **ไซเบอร์ (Cyber)** คือ คำที่กร่อนมาจากคำว่า**ไซเบอร์เนติกส์ (Cybernetics)** และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก

- Critical infrastructure security หรือการรักษาความปลอดภัยของโครงสร้างพื้นฐาน
- Application security หรือความปลอดภัยของแอปพลิเคชัน
- Network security หรือความปลอดภัยของเครือข่าย
- Cloud security หรือความปลอดภัยบนคลาวด์
- Internet of things (IoT) security หรือความปลอดภัยของ IoT.

กรอบการประเมินความพร้อมด้าน Cyber Resilience ของ ธปท. (Link download)

https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/FSINotifications/Cyber%20resilience%20framework%202019.pdf

IT/Information Security, Cyber Security, and Cyber Resilience



CIA = *Confidentiality, Integrity, Availablity*

Source: "Cyber Security strategic achieving cyber resilience", Information Security Forum (ISF), www.securityforum.org

หัวข้อ	BOT สนส. 21/62	SEC สธ. 37/2559 นป. 3/2559	OIC แนวปฏิบัติ IT Risk
1. ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance)	✓	✓	✓
2. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security)			
(2.1) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (information security policy)	✓	✓	✓
(2.2) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management)	✓	✓	✓
(2.3) การจัดโครงสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ (organization of information security)	✓	✓	✓
(2.4) การควบคุมการเข้าถึง (access control)	✓	✓	✓
(2.5) การควบคุมการเข้ารหัสข้อมูล (cryptographic control)	✓	✓	✓

หัวข้อ	BOT สนส. 21/62	SEC สธ. 37/2559 นป. 3/2559	OIC แนวปฏิบัติ IT Risk
(2.6) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)	✓	✓	✓
(2.7) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร(communications security)	✓	✓	✓
(2.8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security)	✓	✓	✓
(2.9) การจัดหาและการพัฒนาระบบ (system acquisition and development)	✓	✓	✓
(2.10) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management)	✓	✓	✓
(2.11) การจัดทาแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (disaster recovery plan)	✓	✓	✓

หัวข้อ	BOT สนส. 21/62	SEC สธ. 37/2559 นป. 3/2559	OIC แนวปฏิบัติ IT Risk
(2.12) การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management)	✓	✓	✓
(2.13) การบริหารจัดการความมั่นคงปลอดภัยด้านทรัพยากรบุคคล (human resource security)	✓	✓	✓
3. การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)	✓	✓	✓
4. การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance)	✓	✓	✓
5. การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit)	✓	✓	✓
6. การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT project management)	✓	-	✓
7. การกำกับดูแลและบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)	✓	✓	✓

เสวนาประเด็นคำถามหรือข้อสงสัยที่เกี่ยวข้องกับ Cyber risk

ที่ได้รับจากผู้เข้าร่วมฟังเสวนา

อ้างอิง

- สนส.21/2562 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ธนาคารแห่งประเทศไทย
- สธ. 37/2559 เรื่องข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ก.ล.ต.
- นป. 3/2559 เรื่องแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ก.ล.ต.
- แนวปฏิบัติ เรื่อง การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันชีวิต / ประกันวินาศภัย พ.ศ. 2564 ค.ป.ภ.

THANK YOU

https://www.tfac.or.th

@TFAC.FAMILY

tfac@tfac.or.th

https://www.facebook.com/TFAC.FAMILY

https:// www.youtube.com/TFACFamily

02 685 2500