ACINFOTEC

E-Commerce Law 2544

E-Transaction Law 2553

Security Standard & Regulations 2556

สถานการณ์โลกในปัจจุบัน มีอะไรบ้างที่เราต้องรู้...?

ในการบริหารจัดการความมั่นคงปลอดภัยข้อมูล

สัมมนา การบริหารจัดการความปลอดภัยข้อมูล
เพื่อรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์

สมาคมประกันชีวิตไทย

Version 2.0 / 24.02.2017

ACINFOTEC

ACinfotec is Thailand's leading expert provider of services, solutions and consultation for IT governance, risk and compliance management based on various well-known international standards, best practices and regulations.

Our expertise and client base spans all major industries. We regularly provide services to leading organization across the financial, technology, telecommunication, healthcare, insurance, energy, and manufacturing sectors.

"Driving Business Excellence"

Agenda

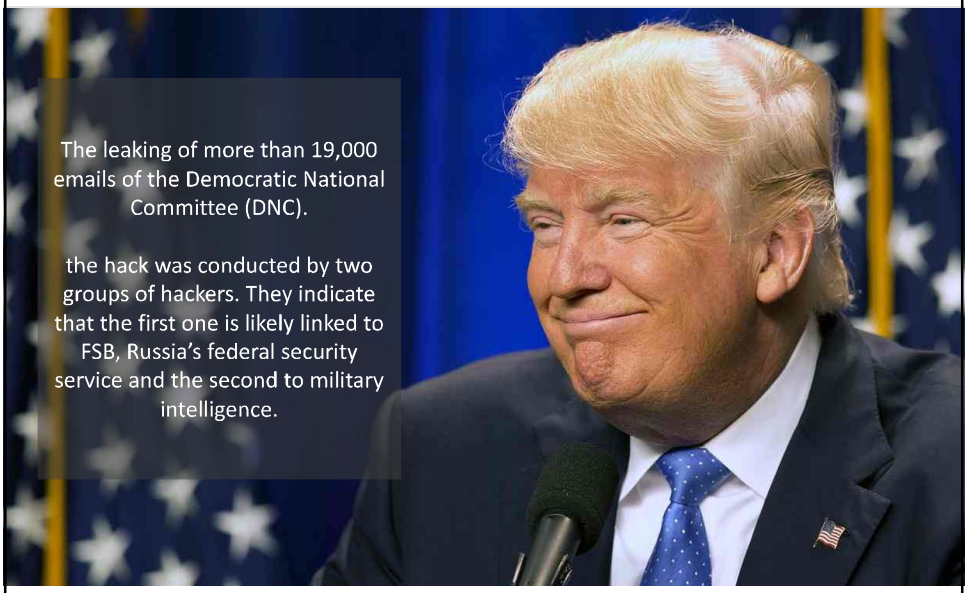
- ภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต (Security Landscape of 2017 and Beyond)
- กฎหมายและข้อบังคับที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- มาตรฐานและแนวปฏิบัติที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

2016 is the Year of Security Breaches

Yahoo!

500 Million + 1 Billion accounts compromised!!!

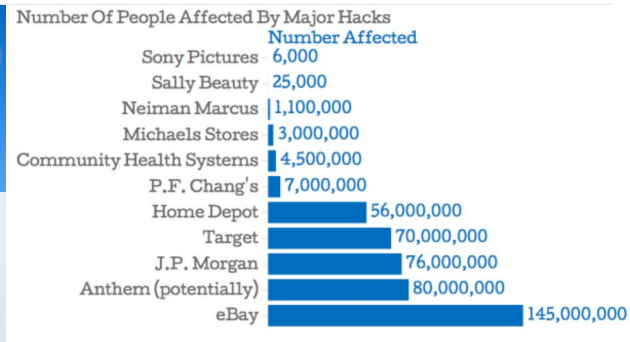
Hacking of The Democrat & Hilary's Presidential Campaign



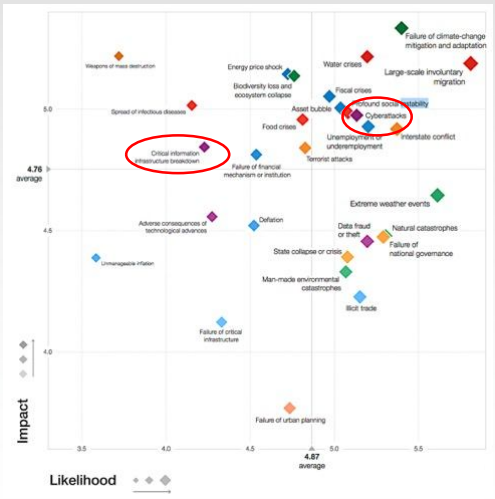
Health Insurance Companies are Prime Targets for Hackers

Anthem
DATA BREACH

Excellus
Health Insurer
HACKED



WEFORUM: Global Risk Landscape 2016



Cyber attacks are among Top 10 Risks

- Adverse consequences of technological advances
- Breakdown of critical information infrastructure and networks
- Large-scale cyberattacks
- Massive incident of data fraud/theft

Source: The Global Risk Landscape 2016, World Economic Forum

Security Landscape – The Changing Perspective!

- **1995 – 2010:** Focus on Firewalls & Anti-virus – based on defense-in-depth security models (castles & moats)
  …….Protection @ *"Speed of Sound" (Space)*
- **2010 – 2025:** Focus on Adaptive and Self-Organizing "Cyber" Tools – based on Temporal Models (AI & Machine Learning)
  …….Defending @ *"Speed of Light" (Time)*

Current Cyber Security Landscape

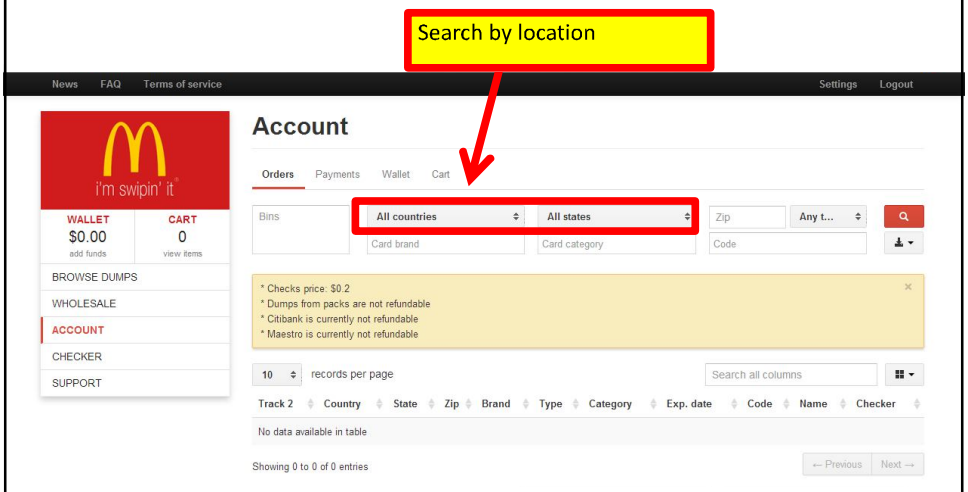
- Convergence of Physical & Cyber Security Operations
- "Cyber" migrates from IT Dept to the Board: C-Suite
- Global Real-Time Targeted Cyber Attacks – 24/7
- Transition from 20thC Tools (Firewalls & Anti-virus) to "Smart" 21stC Tools (AI & Machine Learning)
- Emergence of Enterprise "Internet of Things"
- Evolution of Smart Devices, Cities, Economy & Society
- Dramatic increase in Cyber Crime & Cyber Terrorism

Cyber-Physical Threat Scenarios

- **Physical "Penetration":** Operations Perimeter penetrated to allow theft or corruption of Cyber Information / IT Databases and Confidential Plans
- **Cyber "Hack":** Malicious changes to Cyber Access Controls & IT Databases to allow Criminals/Terrorists to enter Target Facilities (such as Military Bases, Banking HQ, Telco/Mobile Network Operations)
- **Convergent Threats** – Criminals/Terrorists will attack at the weakest links which in the 21stC will be BOTH Cyber Network and Physical Premise

.....Cyber Attacks are now fully industrialized with Malicious Code "Kits" & Botnets for sale "by the hour" on the **DARKNET**

Sneak Peek of "What's" under the DARKNET



WIRED.CO.UK

Hackers cause electricity 'blackout' in Ukraine

MALWARE / 05 JANUARY 16 / by MATT BURGESS

240 shares
0 comments

This Ransomware Malware Could Poison Your Water Supply If Not Paid

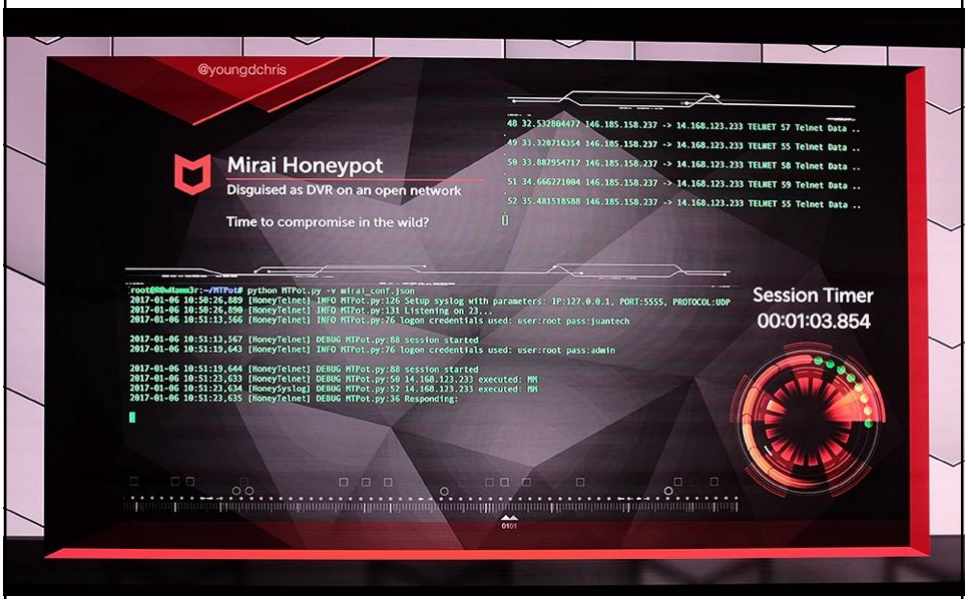
Thursday, February 16, 2017 Swati Khandelwal

G+1 69 Like 2.5K Share 5820 Tweet 1549 Share 624 Share 8365

Special Report from RSA 2017

Photo: Mathew Schwartz

1. Mirai Botnet Pwns in 60 Seconds



Demonstration of Mirai honeypot via Intel Security's Chris Young. (All photos: Mathew Schwartz)

2. Governments Should Hack First

Adi Shamir speaking on the Cryptographers' Panel

3. Segment Your Backup Environment

Left to right: Mandiant's Robert Wallace and Charles Carmakal.

4. Watch For Fakers

Empty Extortion Attempts *Fake Lizard Squad*

From: LZ Security <sec@lzqsec.com>
Subject: DDoS Attack Imminent - Important information

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Lizard Squad and we have chosen your website/network as target for our next DDoS attack.

Please perform a google search for "Lizard Squad DDoS" to have a look at some of our previous "work". All of your servers will be attacked on Tuesday June 3.

How do I stop this? We are willing to refrain from attacking your servers for a small fee. The current fee is 5 Bitcoins (BTC). The fee will increase by 5 Bitcoins for each day that has passed without payment.

Please send the bitcoin to the following Bitcoin address: [REDACTED]. Once you have paid we will automatically get informed that it was your payment.

How do I get Bitcoins? You can easily buy bitcoins via several websites or even offline from a Bitcoin-ATM. We suggest you to start with localbitcoins.com or do a google search.

This is not a hoax, do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again!

MANDIANT A FireEye Company

RSAConference2017

Sample of extortion note received by a Mandiant client

DDoS Simulation / Cyber Drill Testing

Evaluate Security Incident Response Plan

Evaluate the capability of people to respond and recover from cyber security incidents

Evaluate effectiveness of cyber security solutions / tools

Improve plan, process and control

Detect

Response

Recover

Prevent

NOVICE

AVERAGE

SKILL

SPECIALIST

EXPERT

Prevent Breach	Assume Breach
Threat model	War game exercises
Code review	Centralized security monitors
Security testing	Live site penetration testing
Security development lifecycle	

5. DIY Ransomware

6. IoT Regulation Required

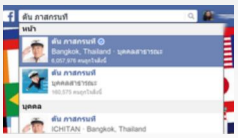
Bruce Schneier talks internet of things regulation

Summary of 2017 Cyber Threat Landscape

- Advanced Threats Targeting the Cloud
- Evolution of Ransomware: Changing Data and Destroying Backups
- GDPR Compliance Approaching
- Increased Demand for Cyber Insurance
- Shadow IT
- Cyber Espionage and Warfare
- Dronejacking
- IoT Malware
- Hacktivists exposing privacy issues

2017 Cyber Security Trends in Thailand

- Cyber security regulations improvement
- More demand for cyber security skills
- Attackers will target consumers



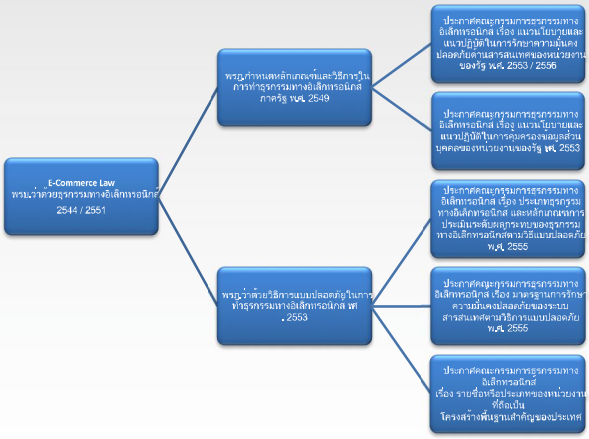
- Attackers will become more bolder, more commercial and less traceable
- Breaches will get more complicated and harder to beat

Agenda

- ภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต (Security Landscape of 2017 and Beyond)
- กฎหมายและข้อบังคับที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- มาตรฐานและแนวปฏิบัติที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

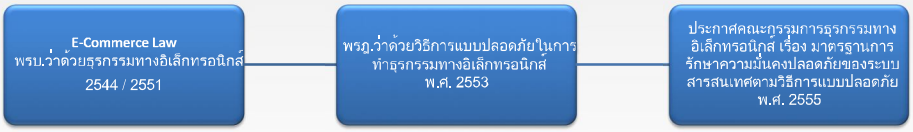
กฎหมายที่เกี่ยวข้องกับ “ธุรกรรมทางอิเล็กทรอนิกส์”

เฉพาะที่เกี่ยวข้องกับ Cyber Security



กฎหมายที่เกี่ยวข้องกับ “ธุรกรรมทางอิเล็กทรอนิกส์”

เฉพาะที่เกี่ยวข้องกับ Cyber Security และธุรกิจประกันภัย



Main Law | Supporting Laws | Regulations

พรฎ.ว่าด้วยวิธีการแบบปลอดภัยฯ พ.ศ. 2553

- กฎหมายฉบับแรกที่เริ่มระบุข้อกำหนดในการรักษาความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนคือ พรฎ.ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 ซึ่งมีใจความสำคัญ ดังนี้

มาตรา 4	ระบุว่าวิธีการแบบปลอดภัยมี 3 ระดับ ได้แก่ (1) ระดับเคร่งครัด (2) ระดับกลาง (3) ระดับพื้นฐาน โดยยังมิได้ระบุรายละเอียดของการรักษาความมั่นคงปลอดภัยในแต่ละระดับ แต่จะมีการประกาศหลักเกณฑ์เพิ่มเติมต่อไป
มาตรา 5	เป็นมาตราสำคัญที่กำหนดขอบข่ายของกฎหมาย โดยระบุว่าธุรกรรมทางอิเล็กทรอนิกส์ที่ต้องได้รับการรักษาความมั่นคงปลอดภัยตามกฎหมายฉบับนี้ คือ (1) ธุรกรรมทางอิเล็กทรอนิกส์ ที่มีผลกระทบต่อความมั่นคง หรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน (2) ธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร ที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

พรฎ.ว่าด้วยวิธีการแบบปลอดภัยฯ พ.ศ. 2553

มาตรา 6	ให้คณะกรรมการประกาศกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์ หลักเกณฑ์การประเมินผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ ตาม 5(1) และ 5(2) ซึ่งต้องได้รับการรักษาความมั่นคงปลอดภัยในระดับเคร่งครัด ระดับกลาง และระดับพื้นฐาน ต่อไป
มาตรา 7	ระบุให้มีการประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับมาตรา 4 ในแต่ละระดับตามความเหมาะสม แต่อย่างน้อยต้องเกี่ยวข้องกับหลักเกณฑ์ซึ่งอ้างอิงมาจากมาตรฐาน ISO 27001 ดังต่อไปนี้ (1) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ (2) การจัดการโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อบริหารจัดการความมั่นคงปลอดภัยทั้งภายในและภายนอกองค์กร (3) การบริหารจัดการทรัพย์สินสารสนเทศ (4) การสร้างความมั่นคงปลอดภัยด้านบุคลากร (5) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบสารสนเทศ (7) การควบคุมการเข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศ (8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (9) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ (10) การบริหารจัดการการดำเนินงานขององค์กรเพื่อให้มีความต่อเนื่อง (11) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ

6 กลุ่มประเภทธุรกรรมที่ต้องใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด

กลุ่มที่ 1
ธุรกรรมทางอิเล็กทรอนิกส์ด้านการชำระเงินทางอิเล็กทรอนิกส์ตามพรฎ.ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551

กลุ่มที่ 2
ธุรกรรมทางอิเล็กทรอนิกส์ด้านการเงินของธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

กลุ่มที่ 3
ธุรกรรมทางอิเล็กทรอนิกส์ด้านประกันภัยตามกฎหมายว่าด้วยประกันชีวิตและประกันวินาศภัย

กลุ่มที่ 4
ธุรกรรมทางอิเล็กทรอนิกส์ด้านหลักทรัพย์ของผู้ประกอบธุรกิจหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

กลุ่มที่ 5
ธุรกรรมทางอิเล็กทรอนิกส์ที่จัดเก็บ รวบรวม และให้บริการข้อมูลของบุคคลหรือทรัพย์สินหรือทะเบียนต่างๆ ที่เป็นเอกสารมหาชนหรือที่เป็นข้อมูลสาธารณะ

กลุ่มที่ 6
ธุรกรรมทางอิเล็กทรอนิกส์ในการให้บริการด้านสาธารณูปโภคและบริการสาธารณะที่ต้องดำเนินการอย่างต่อเนื่องตลอดเวลา

ธุรกรรมอื่นๆ ต้องประเมินระดับผลกระทบตามเกณฑ์ดังต่อไปนี้

Methodology วิธีการประเมินระดับผลกระทบ ให้ยึดหลักการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเชื่อถือได้ และต้องประเมินระดับผลกระทบในด้านต่อไปนี้

การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ประกอบด้วย
(๑) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน
(๒) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย
(๓) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจาก (๒)
(๔) ผลกระทบด้านความมั่นคงหรือความสงบเรียบร้อยของสังคม

ผลประเมินที่เป็นผลกระทบในระดับ**สูง**ด้านหนึ่งด้านใดให้ธุรกรรมทางอิเล็กทรอนิกส์นั้นต้องใช้วิธีการแบบปลอดภัยระดับ**เคร่งครัด**

ผลกระทบในระดับ**กลาง**อย่างน้อย**สองด้าน**ขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับ**กลาง**

ในกรณีที่ไม่เป็นไปตามข้างต้น ให้ธุรกรรมทางอิเล็กทรอนิกส์ใช้วิธีการแบบปลอดภัยในระดับไม่ต่ำกว่าระดับ**พื้นฐาน**

ประเด็นพิจารณา

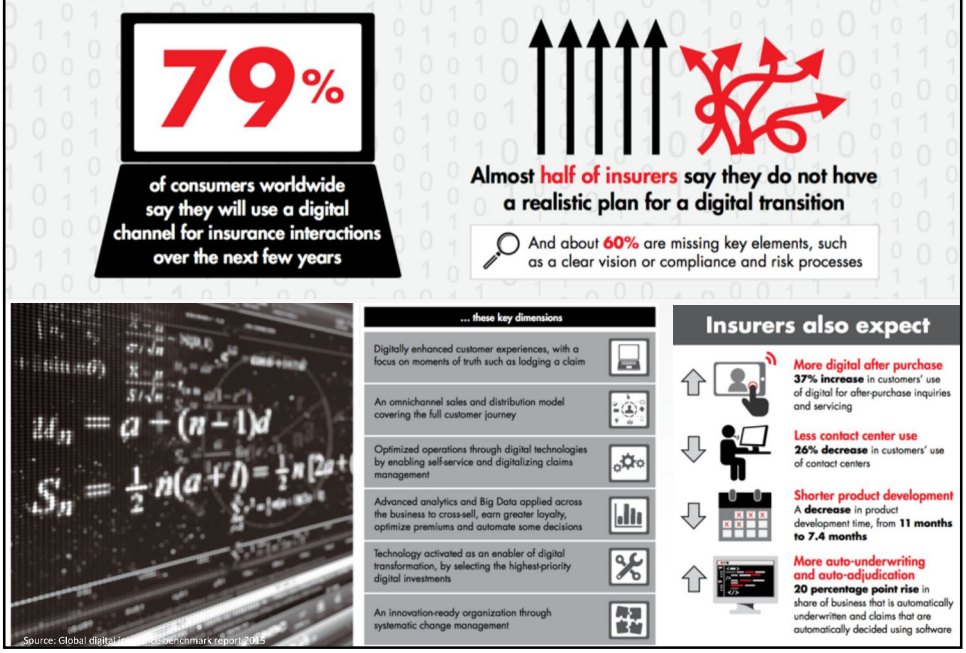
"**ธุรกรรม**" หมายความว่า การกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔

"**ธุรกรรมทางอิเล็กทรอนิกส์**" หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

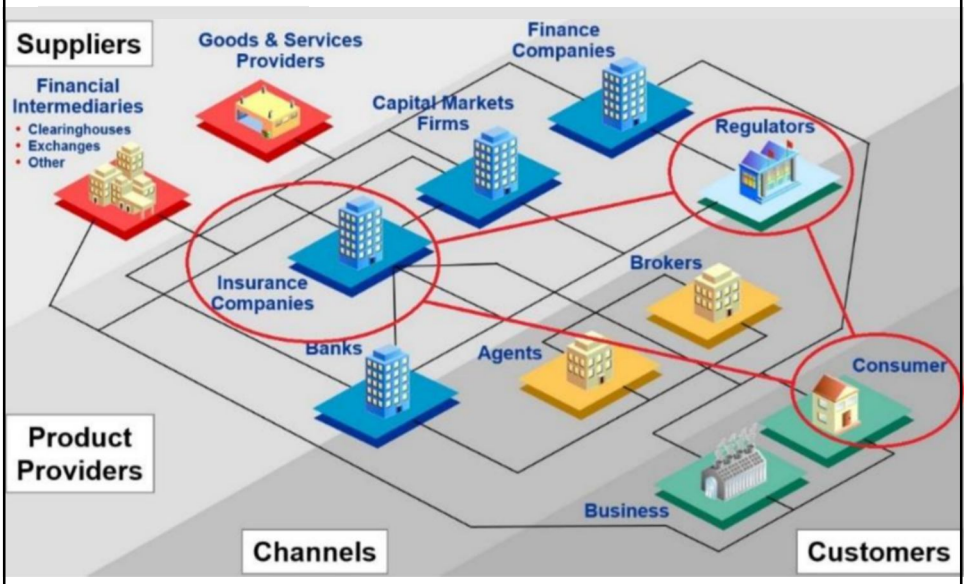
แปลความได้ว่า ทุกกิจกรรมการดำเนินงานขององค์กร หากกระทำผ่านระบบเทคโนโลยีสารสนเทศทั้งหมดหรือบางส่วน ล้วนจัดเป็นธุรกรรมอิเล็กทรอนิกส์ และเข้าข่ายที่ต้องปฏิบัติตามกฎหมาย เช่น E-mail ก็จัดเป็นธุรกรรมอิเล็กทรอนิกส์

ความตั้งใจของภาครัฐคือต้องการให้หน่วยงานจัดทำกระบวนการรักษาความมั่นคงแบบปลอดภัยขั้น**พื้นฐาน**หรือ**ปานกลาง**ทั้งองค์กร และรักษาความปลอดภัยให้แก่ธุรกรรมสำคัญอย่าง**เคร่งครัด**

Digital Insurance



Related Entities



Cyber Threats for Digital Insurance – Sample Cases

Case 1 - Hackers steal personal data about customers

- Cyber-criminals breached the company database and stole information of more than one million customers and sales prospects, including national IDs, house registration, driving license, etc.

Case 2 - Even small breaches can have a meaningful impact and require corrective action

- The attack targeted company employees with e-mails containing malware that could capture confidential data such as bank account numbers, national IDs, user accounts/logins, passwords and credit card numbers. Hackers used this information to compromise several servers, including servers used by employees to remotely access the company's IT systems.

Case 3 - Targeted insurer accused for failing to comply with PCI DSS

- Attackers exploited vulnerable software on the company's servers and stole payment card information for more than 93,000 customers, including names, addresses and unencrypted card security codes.

Cyber Security Regulations for Insurance Industry Around the World

OIC Regulations for Digital Insurance

พรบ. ประกันชีวิต	▪ อาศัยอำนาจตาม พรบ. ประกันชีวิต มาตรา 38 และมาตรา 70/2
ประกาศ	▪ ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่อง หลักเกณฑ์ วิธีการออกกรมธรรม์ประกันภัย การเสนอขายกรมธรรม์ประกันภัย และการชดใช้เงินตามสัญญาประกันชีวิต โดยใช้วิธีการทางอิเล็กทรอนิกส์ พ.ศ....
แนวปฏิบัติ	▪ แนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด
อ้างอิง	▪ กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ▪ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
บังคับใช้	▪ 180 วัน นับจากวันที่ประกาศในราชกิจจานุเบกษา ▪ ต้องมีการขึ้นทะเบียนบริษัท นายหน้าประกันชีวิต ธนาคาร และขอความเห็นชอบสำหรับการใช้บริการบุคคลภายนอก ▪ ต้องมีการตรวจสอบโดยผู้ตรวจสอบอิสระที่ได้รับใบอนุญาต CISA, CISM, CISSP, ISO 27001 หรือโดย CB

การเสนอขาย การใช้วิธีทางอิเล็กทรอนิกส์ประกอบการเสนอขาย การออกกรมธรรม์ หรือการชดใช้เงินตามสัญญา หากส่วนหนึ่งส่วนใดกระทำโดยใช้วิธีการทางอิเล็กทรอนิกส์ ต้องกระทำตามวิธีการแบบปลอดภัยในระดับที่กำหนดไว้ในกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ หรือตามหลักเกณฑ์ที่ คปภ. กำหนด ทั้งนี้ครอบคลุมทั้ง บริษัท นายหน้าประกันชีวิต ธนาคาร และผู้ให้บริการซึ่งเป็นบุคคลภายนอก

OIC Regulations for Digital Insurance – More Points to Concern

+ Digital Signature

- หมวด 2 ข้อ 13 การส่งข้อมูลให้ผู้มุ่งหวัง ต้องลงลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- หมวด 4 การออกกรมธรรม์ประกันภัยโดยใช้วิธีทางอิเล็กทรอนิกส์ ต้องกระทำตามวิธีการแบบปลอดภัยในระดับที่กำหนดไว้ในกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และต้องลงลายมือชื่อทางอิเล็กทรอนิกส์
- ฯลฯ

+ Privacy

- หมวด 6 ข้อ 18 (1)จัดให้มีแนวนโยบายและแนวปฏิบัติด้านการบริหารจัดการความเป็นส่วนตัวและข้อมูลส่วนบุคคล
- ข้อ 11.4 (แนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด) จัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

OIC Regulations for Digital Insurance – Challenges

Scope of Compliance

Many cover huge number of applications

Time

180 days may be too short in the case of updating applications (e.g. for digital signature or heighten security)

Third Party Service Provider

Manage third party compliance also very difficult. In this case, selecting ISO 27001 certified service provider will help ensure compliance

Independent Auditors

Do they have required skills and experience?
Are they reliable?
How much liability?

OIC Regulations for Digital Insurance – Recommended Steps

01 Define Scope

Evaluate yourself and see what will be the scope of compliance

Information, Hardware, Software, Personnel, Location, 3rd Party Service Provider, Partner

02 Assess Current State

Conduct gap analysis to assess current security controls and processes against the requirements

03 Develop Plan

Develop plan for compliance and define required resources and budget

04 Implement Controls

Implement required security controls and processes. This includes: security & privacy policies, digital signatures, technical controls, physical controls, training & awareness, etc.

05 Perform Audit

Engage independent auditor to perform audit. Better to hire auditor from trusted sources rather than freelance auditor

06 Stay Compliance

Managing changes and updating related processes and controls. Maintain awareness of employees and perform audit annually

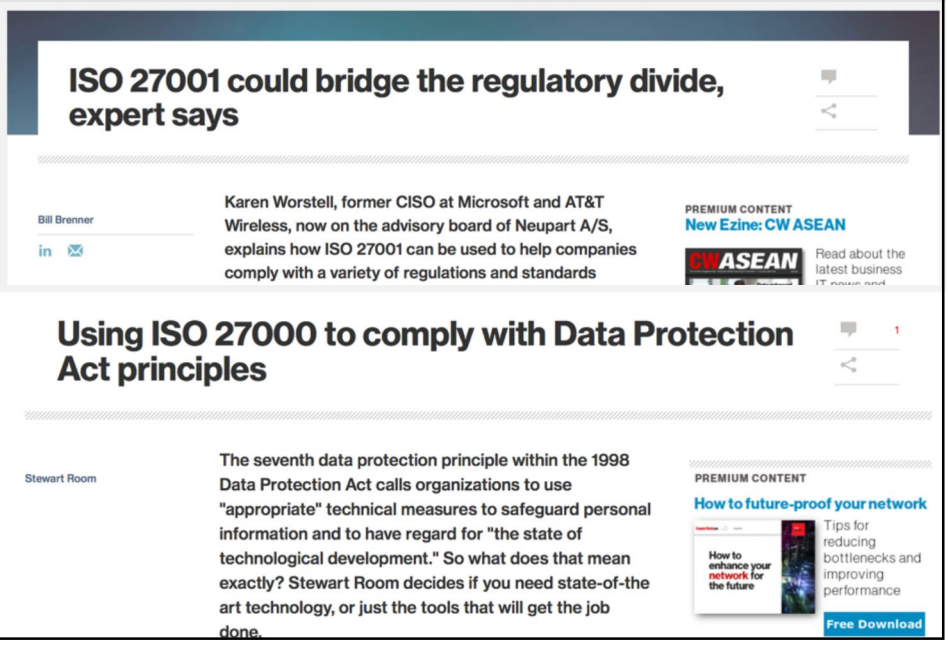
Agenda

- ภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต (Security Landscape of 2017 and Beyond)
- กฎหมายและข้อบังคับที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- มาตรฐานและแนวปฏิบัติที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

Recommended Cyber Security Related Standards

- ISO 27001 & ISO 27002 –> information security
- ISO 27015 –> information security for financial & insurance sectors
- ISO 27032 –> cyber security
- ISO 27017 –> cloud security
- ISO 27018 –> cloud privacy
- CSA STAR –> cloud security
- NIST CSF –> cyber security
- UK Cyber Resilient –> cyber security
- มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 (MICT) –> information security
- แนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศตามวิธีการแบบปลอดภัยในระดับเครงครัด (OIC) –> information security

ISO 27001 is Commonly Used as a Basis for Laws & Regulations



ประกาศ มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศฯ

- ประกาศเมื่อ 13 พฤศจิกายน 2555 บังคับใช้ใน 360 วัน นับจากวันประกาศ
- เน้นที่การขยายความรายละเอียดของวิธีการแบบปลอดภัยตามมาตรา 7 ของพรฎ.ว่าด้วยวิธีการแบบปลอดภัยฯ พ.ศ. 2553
- สามารถใช้อ้างอิงในการสร้างมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

ตัวอย่างมาตรการระดับพื้นฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานต้องปฏิบัติดังนี้

ข้อ ๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการหน่วยงานต้องกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

๒.๒ สำหรับระบบสารสนเทศใหม่ มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงานร่วมกันได้ระหว่างระบบเดิมและระบบใหม่

๒.๓ มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ Non-Disclosure agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูลสารสนเทศ

ตัวอย่างมาตรการระดับปานกลาง

๒. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ ๑. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ หน่วยงานต้องวางแผนการติดตามและประเมินผลการใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้ เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิผลอยู่เสมอ

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ มีการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

๒.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

๒.๓ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าวควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน

ตัวอย่างมาตรการระดับเคร่งครัด

๓. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานและระดับกลาง และต้องปฏิบัติเพิ่มเติม ดังนี้

ข้อ ๑. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๑.๑ มีการสร้างความร่วมมือระหว่างผู้ที่มีบทบาทเกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ในงานหรือกิจกรรมใด ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีหน้าที่ในการกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมาย รวมทั้งหน่วยงานที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

๑.๓ ก่อนที่จะอนุญาตให้หน่วยงานหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของหน่วยงาน ให้มีการระบุความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกันเพื่อลดความเสี่ยงนั้นก่อนการอนุญาต

ข้อ ๒. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

๒.๑ ในการพิจารณารับพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน

๒.๒ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา

ข้อ ๓. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

Common Concepts Across All Standards & Best Practices

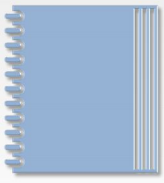
They are all based on risks & controls

Assess Risk

Select Controls

Common Concepts Across All Standards & Best Practices

Manage compliance using policy & audit

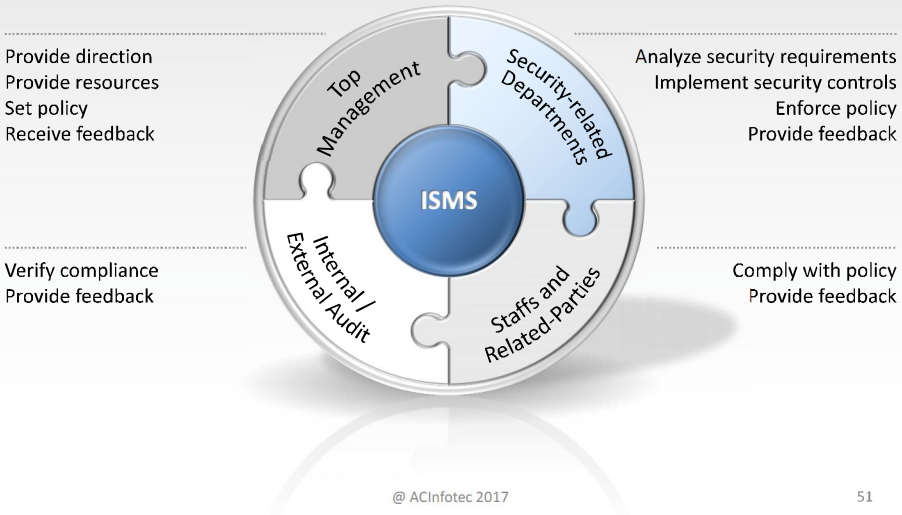


Information Security
Policies and Procedures

Internal Audit
External Audit
Continuous Monitoring

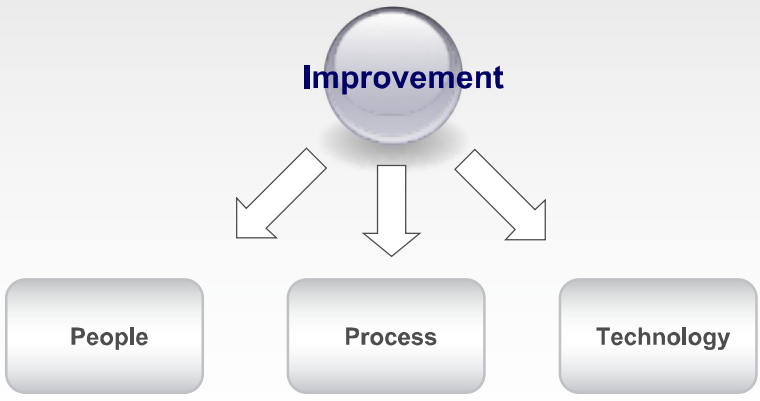
Common Concepts Across All Standards & Best Practices

Top Management Oversees and Manages Security Risks



Common Concepts Across All Standards & Best Practices

Continual improvement




THANK YOU
For more information, contact: ACinfotec Consulting Services
02-670-8980-3 | services@acinfotec.com | www.acinfotec.com
Consulting
Training
Assessment
Solutions
ACINFOTEC > DRIVING BUSINESS EXCELLENCE
@ ACInfotec 2017
53