




สถานการณ์โลกในปัจจุบัน มีอะไรบ้างที่เราต้องรู้...?

ในการบริหารจัดการความมั่นคงปลอดภัยข้อมูล

สัมมนา การบริหารจัดการความปลอดภัยข้อมูล
เพื่อรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์

สมาคมประกันชีวิตไทย

E-Commerce Law 2544

E-Transaction Law 2553

Security Standard & Regulations 2556

Version 2.0 / 24.02.2017
© ACinfotec 2017



ACinfotec กับ 10 ปี
แห่งความมุ่งมั่นสร้างมาตรฐานด้านไอที
 พร้อมเดินทางไปกับบริษัทไทยสู่แนวหน้าของการไอทีมาตรฐานสากล



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.





Consulting
Provide expert advice to help client implementing ISO 27001, ISO 20000, ISO 22301, CMMI and various international standards and best practices.



Assessment
Provide assessment services to help client understand risks and regulatory compliance issues as well as actionable items for improvement.



Solutions
Provide IT standard driven, world-class solutions that can help client to optimize their IT operations and processes.



Training
Deliver international recognized IT training courses to meet and exceed organizational training requirements

"Driving Business Excellence"

@ ACinfotec 2017

Agenda



- 🔒 ภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต (Security Landscape of 2017 and Beyond)
- 🔒 กฎหมายและข้อบังคับที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- 🔒 มาตรฐานและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

@ ACInfotec 2017

3

2016 is the Year of Security Breaches



Yahoo!

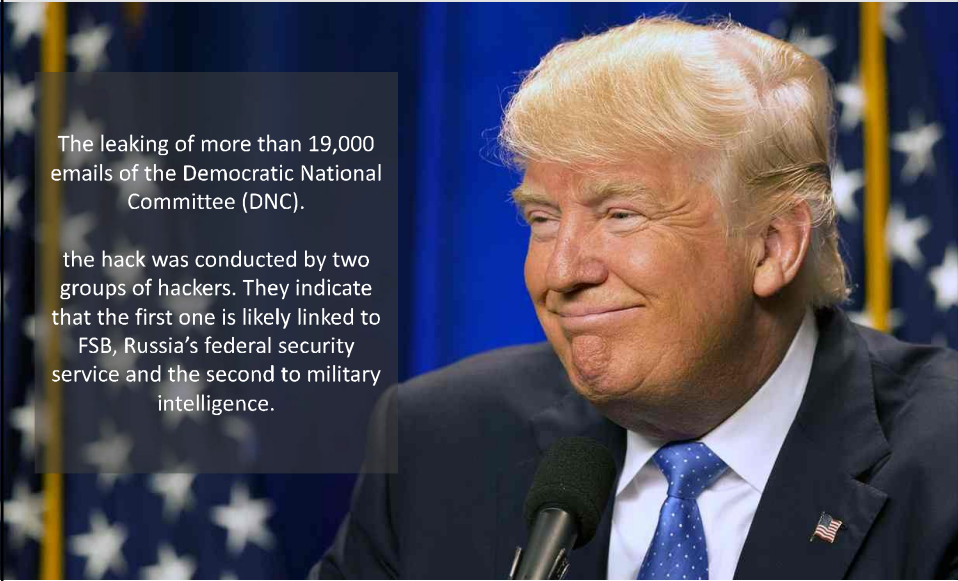
A graphic with a purple background. The word "Yahoo!" is written in white. A magnifying glass is positioned over the '@' symbol in the word "Mail!". The '@' symbol is inside a white envelope icon. Below the magnifying glass, the text "Yahoo! Mail! Hack!" is written in white inside a purple rectangular box.

Yahoo! Mail! Hack!

500 Million + 1 Billion accounts compromised!!!

@ ACInfotec 2017 5

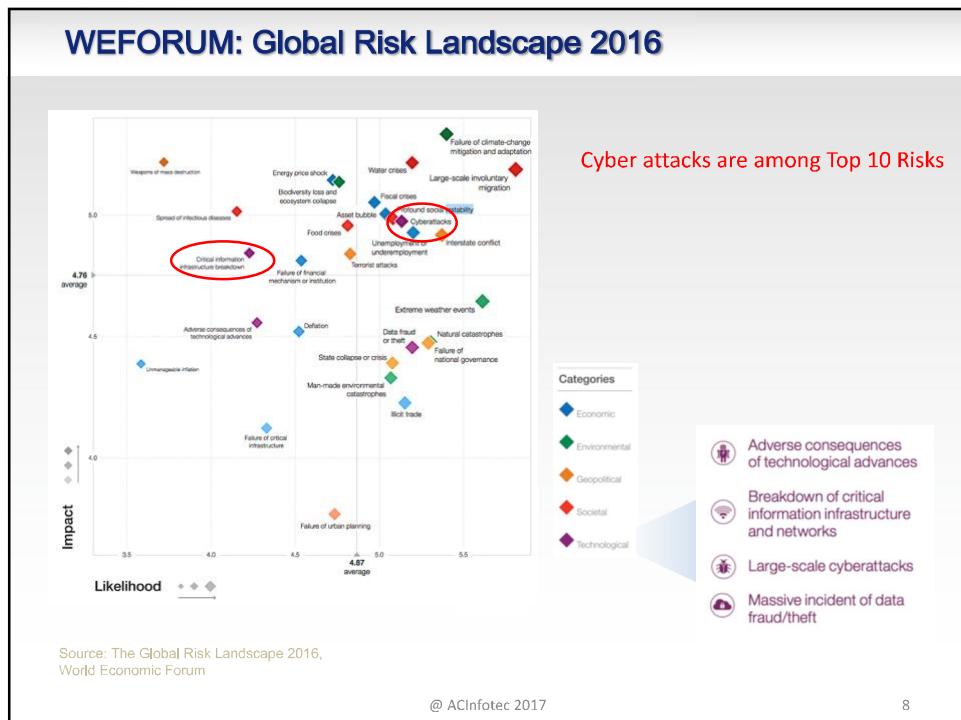
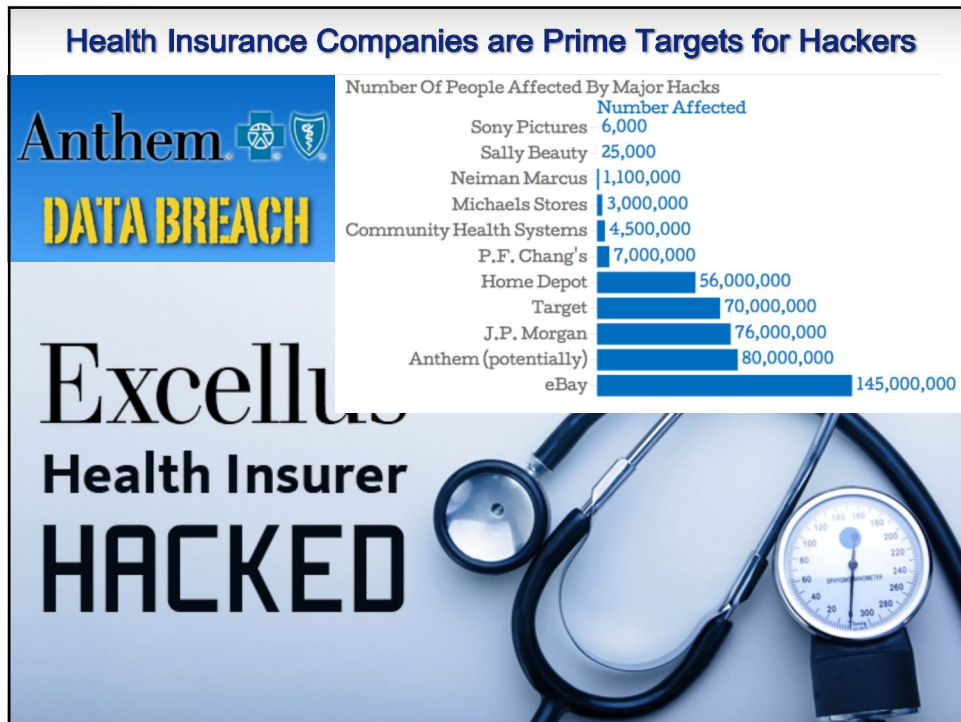
Hacking of The Democrat & Hillary's Presidential Campaign

A photograph of Donald Trump speaking at a podium. He is wearing a dark suit, a white shirt, and a blue tie with white polka dots. He is looking down and to his left. The background is a blue curtain with white stars.

The leaking of more than 19,000 emails of the Democratic National Committee (DNC).

the hack was conducted by two groups of hackers. They indicate that the first one is likely linked to FSB, Russia's federal security service and the second to military intelligence.

@ ACInfotec 2017 6



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)*

@ ACInfotec 2017

9

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

@ ACInfotec 2017

10

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**

@ ACInfotec 2017

11

Sneak Peek of "What's" under the **DARKNET**

Search by location

The screenshot shows a darknet marketplace interface. At the top, there's a navigation bar with links: News, FAQ, Terms of service, Settings, and Logout. Below this is a header for the 'Account' section, which includes tabs for Orders, Payments, Wallet, and Cart. A red box highlights the 'Search by location' text, with a red arrow pointing to the 'All countries' dropdown menu in the search filters. The search filters also include 'All states', 'Zip', 'Any t...', 'Card brand', 'Card category', and 'Code'. A yellow warning box displays the following text:

- * Checks price: \$0.2
- * Dumps from packs are not refundable
- * Citibank is currently not refundable
- * Maestro is currently not refundable

 Below the warning box, there's a table with columns: Track 2, Country, State, Zip, Brand, Type, Category, Exp. date, Code, Name, and Checker. The table is currently empty, showing 'No data available in table'. At the bottom, it says 'Showing 0 to 0 of 0 entries' with 'Previous' and 'Next' navigation buttons.

@ ACInfotec 2017

12



Special Report from RSA 2017

RSA®Conference 2017 AGENDA AT A GLANCE

#RSAC

TUESDAY, February 14

ROOM CHANGES

PM: 150-151: Trust, Privacy & Compliance with Google, Microsoft and Cisco
3:30 PM - 5:00 PM
New Room: Room 1202

SDV-7509 | Changing Face/View on Identity
6:30 PM - 8:00 PM
New Room: Room 1202

PM: 150-151: Global Approaches to Protecting Critical National Infrastructure
5:45 PM - 8:30 PM
New Room: Room 1202

WEDNESDAY, February 15

AM: 150-151: The Future of Security
8:00 AM - 9:30 AM
New Room: Room 1202

AM: 150-151: The Future of Security
9:30 AM - 11:00 AM
New Room: Room 1202

AM: 150-151: The Future of Security
11:00 AM - 12:30 PM
New Room: Room 1202

PM: 150-151: The Future of Security
2:00 PM - 3:30 PM
New Room: Room 1202

PM: 150-151: The Future of Security
3:30 PM - 5:00 PM
New Room: Room 1202

THURSDAY, February 16

AM: 150-151: The Future of Security
8:00 AM - 9:30 AM
New Room: Room 1202

AM: 150-151: The Future of Security
9:30 AM - 11:00 AM
New Room: Room 1202

AM: 150-151: The Future of Security
11:00 AM - 12:30 PM
New Room: Room 1202

PM: 150-151: The Future of Security
2:00 PM - 3:30 PM
New Room: Room 1202

PM: 150-151: The Future of Security
3:30 PM - 5:00 PM
New Room: Room 1202

FRIDAY, February 17

AM: 150-151: The Future of Security
8:00 AM - 9:30 AM
New Room: Room 1202

AM: 150-151: The Future of Security
9:30 AM - 11:00 AM
New Room: Room 1202

AM: 150-151: The Future of Security
11:00 AM - 12:30 PM
New Room: Room 1202

PM: 150-151: The Future of Security
2:00 PM - 3:30 PM
New Room: Room 1202

PM: 150-151: The Future of Security
3:30 PM - 5:00 PM
New Room: Room 1202

Photo: Matthew Schwartz

@ ACInfotec 2017

15

1. Mirai Botnet Pwns in 60 Seconds

@youngdchris

Mirai Honeygot
Disguised as DVR on an open network
Time to compromise in the wild?

```

root@kali:~# python MITP.py -v mirai.conf.json
2017-01-06 10:50:26,889 [MoneyTelnet] INFO MITP.py:126 Setup syslog with parameters: IP:127.0.0.1, PORT:5555, PROTOCOL:UDP
2017-01-06 10:50:26,898 [MoneyTelnet] INFO MITP.py:131 Listening on 23...
2017-01-06 10:51:13,566 [MoneyTelnet] INFO MITP.py:76 login credentials used: user:root pass:juantech
2017-01-06 10:51:13,567 [MoneyTelnet] DEBUG MITP.py:88 session started
2017-01-06 10:51:19,643 [MoneyTelnet] INFO MITP.py:76 login credentials used: user:root pass:admin
2017-01-06 10:51:19,644 [MoneyTelnet] DEBUG MITP.py:88 session started
2017-01-06 10:51:23,633 [MoneyTelnet] DEBUG MITP.py:50 14.168.123.233 executed: RM
2017-01-06 10:51:23,634 [MoneyTelnet] DEBUG MITP.py:52 14.168.123.233 executed: RM
2017-01-06 10:51:23,635 [MoneyTelnet] DEBUG MITP.py:36 Responding

```

Session Timer
00:01:03.854

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

@ ACInfotec 2017

16

2. Governments Should Hack First



Adi Shamir speaking on the Cryptographers' Panel

@ ACInfotec 2017

17

3. Segment Your Backup Environment



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

@ ACInfotec 2017

18

4. Watch For Fakers

Empty Extortion Attempts *Fake Lizard Squad*

From: LZ Security <sec@lqsec.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

@ ACInfotec 2017

19

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



Prevent Breach

Threat model
Code review
Security testing
Security development lifecycle



Assume Breach

War game exercises
Centralized security monitors
Live site penetration testing

@ ACInfotec 2017

20

5. DIY Ransomware



@ ACInfotec 2017

21

6. IoT Regulation Required



Bruce Schneier talks internet of things regulation

@ ACInfotec 2017

22

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



What the new EU GDPR means in 1 minute

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

Tough penalties:
fines of up to
4% of annual global revenue
or
€20 million, whichever is greater.

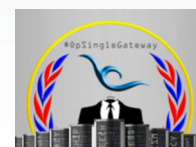
The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

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

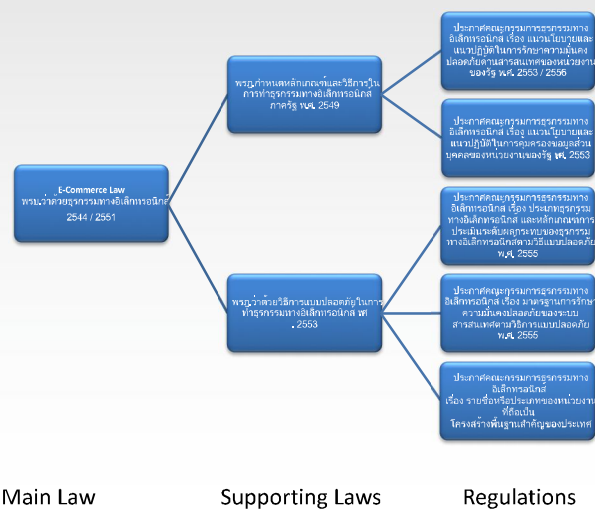
- 🔒 ภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต (Security Landscape of 2017 and Beyond)
- 🔒 กฎหมายและข้อบังคับที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- 🔒 มาตรฐานและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

@ ACInfotec 2017

25

กฎหมายที่เกี่ยวข้องกับ “ธุรกรรมทางอิเล็กทรอนิกส์”

เฉพาะที่เกี่ยวข้องกับ Cyber Security



© ACInfotec 2017 | www.acinfotec.com

Page 26

กฎหมายที่เกี่ยวข้องกับ “ธุรกรรมทางอิเล็กทรอนิกส์”

เฉพาะที่เกี่ยวข้องกับ Cyber Security และธุรกิจประกันภัย



พ.ร.ก.ว่าด้วยวิธีการแบบปลอดภัยฯ พ.ศ. 2553

- กฎหมายฉบับแรกๆที่เริ่มระบุข้อกำหนดในการรักษาความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจนคือ พ.ร.ก.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) ซึ่งต้องได้รับการรักษาความมั่นคงปลอดภัยในระดับเครื่องคิด ระดับกลาง และระดับพื้นฐาน ต่อไป
มาตรา 7	ระบุให้มีการประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับมาตรา 4 ในแต่ละระดับตามความเหมาะสม แต่อย่างน้อยต้องเกี่ยวข้องกับหลักเกณฑ์ซึ่งอ้างอิงมาจากมาตรฐาน ISO 27001 ดังต่อไปนี้ (1) การสร้างความมั่นคงปลอดภัยด้านการบริหารจัดการ (2) การจัดการโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อบริหารจัดการความมั่นคงปลอดภัยทั้งภายในและภายนอกองค์กร (3) การบริหารจัดการทรัพยากรสารสนเทศ (4) การสร้างความมั่นคงปลอดภัยด้านบุคลากร (5) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบสารสนเทศ (7) การควบคุมการเข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศ (8) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (9) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ (10) การบริหารจัดการการดำเนินงานขององค์กรเพื่อให้มีความต่อเนื่อง (11) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

@ ACInfotec 2017

29

หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ



@ ACInfotec 2017

30

6 กลุ่มประเภทธุรกรรมที่ต้องใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด

กลุ่มที่ 1

ธุรกรรมทางอิเล็กทรอนิกส์ด้านการชำระเงินทางอิเล็กทรอนิกส์ตามพรก.ว่าด้วยการควบคุมและธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551

กลุ่มที่ 2

ธุรกรรมทางอิเล็กทรอนิกส์ด้านการเงินของธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

กลุ่มที่ 3

ธุรกรรมทางอิเล็กทรอนิกส์ด้านการประกันภัยตามกฎหมายว่าด้วยประกันชีวิตและประกันวินาศภัย

กลุ่มที่ 4

ธุรกรรมทางอิเล็กทรอนิกส์ด้านหลักทรัพย์ของผู้ประกอบธุรกิจหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

กลุ่มที่ 5

ธุรกรรมทางอิเล็กทรอนิกส์ที่จัดเก็บ รวบรวม และให้บริการข้อมูลของบุคคลหรือทรัพย์สินหรือทะเบียนต่างๆ ที่เป็นเอกสารมหาชนหรือที่เป็นข้อมูลสาธารณะ

กลุ่มที่ 6

ธุรกรรมทางอิเล็กทรอนิกส์ในการให้บริการด้านสาธารณูปโภคและบริการสาธารณะที่ต้องดำเนินการอย่างต่อเนื่องตลอดเวลา

@ ACInfotec 2017

31

ธุรกรรมอื่นๆ ต้องประเมินระดับผลกระทบตามเกณฑ์ดังต่อไปนี้

Methodology

วิธีการประเมินระดับผลกระทบ ให้ยึดหลักการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นที่ยอมรับเป็นการทั่วไปว่าเชื่อถือได้ และต้องประเมินระดับผลกระทบในด้านต่อไปนี้

การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ประกอบด้วย

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

ผลกระทบที่เป็นผลกระทบในระดับสูงด้านหนึ่งด้านใดให้ธุรกรรมทางอิเล็กทรอนิกส์นั้นต้องใช้วิธีการแบบปลอดภัยระดับเคร่งครัด

ผลกระทบในระดับกลางอย่างน้อยสองด้านขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับกลาง

ในกรณีที่ไม่มีไปตามข้างต้น ให้ธุรกรรมทางอิเล็กทรอนิกส์ใช้วิธีการแบบปลอดภัยในระดับไม่ต่ำกว่าระดับพื้นฐาน

32

ประเด็นพิจารณา

“ธุรกรรม” หมายความว่า การกระทำใดๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔

“ธุรกรรมทางอิเล็กทรอนิกส์” หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน

แปลความได้ว่า ทุกกิจกรรมการดำเนินงานขององค์กร หากกระทำผ่านระบบเทคโนโลยีสารสนเทศทั้งหมดหรือบางส่วน ล้วนจัดเป็นธุรกรรมอิเล็กทรอนิกส์ และเขายายที่ต้องปฏิบัติตามกฎหมาย เช่น E-mail ก็จัดเป็นธุรกรรมอิเล็กทรอนิกส์

ความตั้งใจของภาครัฐคือต้องการให้หน่วยงานจัดทำกระบวนการรักษาความมั่นคงแบบปลอดภัยขั้นพื้นฐานหรือปานกลางทั้งองค์กร และรักษาความปลอดภัยให้แก่ธุรกรรมสำคัญอย่าง เคร่งครัด

@ ACInfotec 2017

33

Digital Insurance

79%

of consumers worldwide say they will use a digital channel for insurance interactions over the next few years

Almost **half** of insurers say they do not have a realistic plan for a digital transition

And about **60%** are missing key elements, such as a clear vision or compliance and risk processes

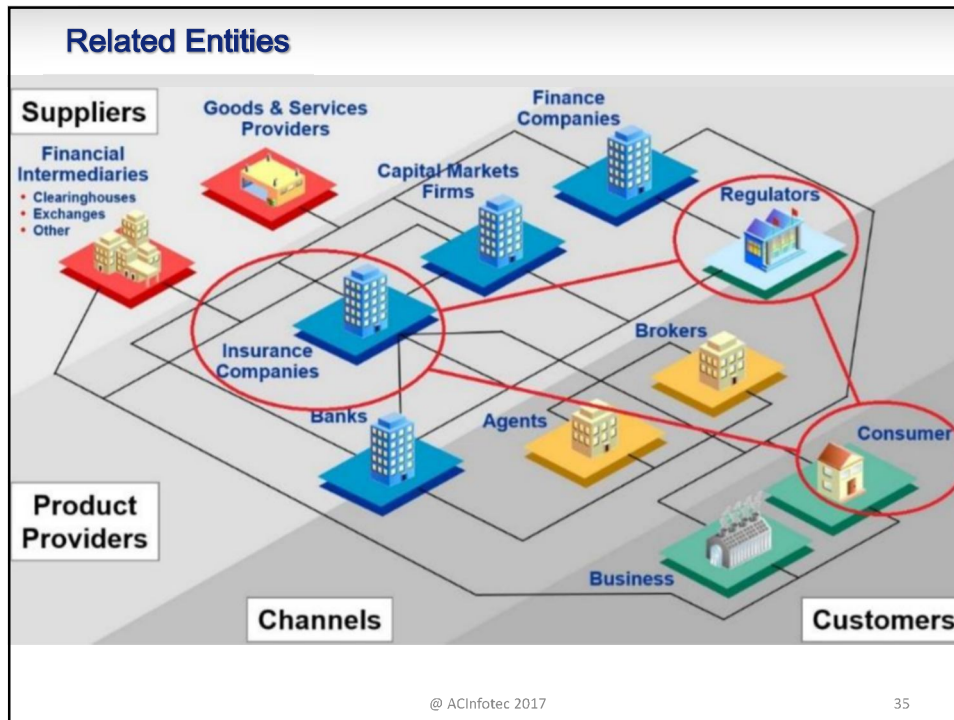


Source: Global digital insurance benchmark report 2015

... these key dimensions	
Digitally enhanced customer experiences, with a focus on moments of truth such as lodging a claim	
An omnichannel sales and distribution model covering the full customer journey	
Optimized operations through digital technologies by enabling self-service and digitalizing claims management	
Advanced analytics and Big Data applied across the business to cross-sell, earn greater loyalty, optimize premiums and automate some decisions	
Technology activated as an enabler of digital transformation, by selecting the highest-priority digital investments	
An innovation-ready organization through systematic change management	

Insurers also expect

- More digital after purchase**
37% increase in customers' use of digital for after-purchase inquiries and servicing
- Less contact center use**
26% decrease in customers' use of contact centers
- Shorter product development**
A decrease in product development time, from 11 months to 7.4 months
- More auto-underwriting and auto-adjudication**
20 percentage point rise in share of business that is automatically underwritten and claims that are automatically decided using software



Cyber Threats for Digital Insurance – Sample Cases

Case 1 - Hackers steal personal data about customers

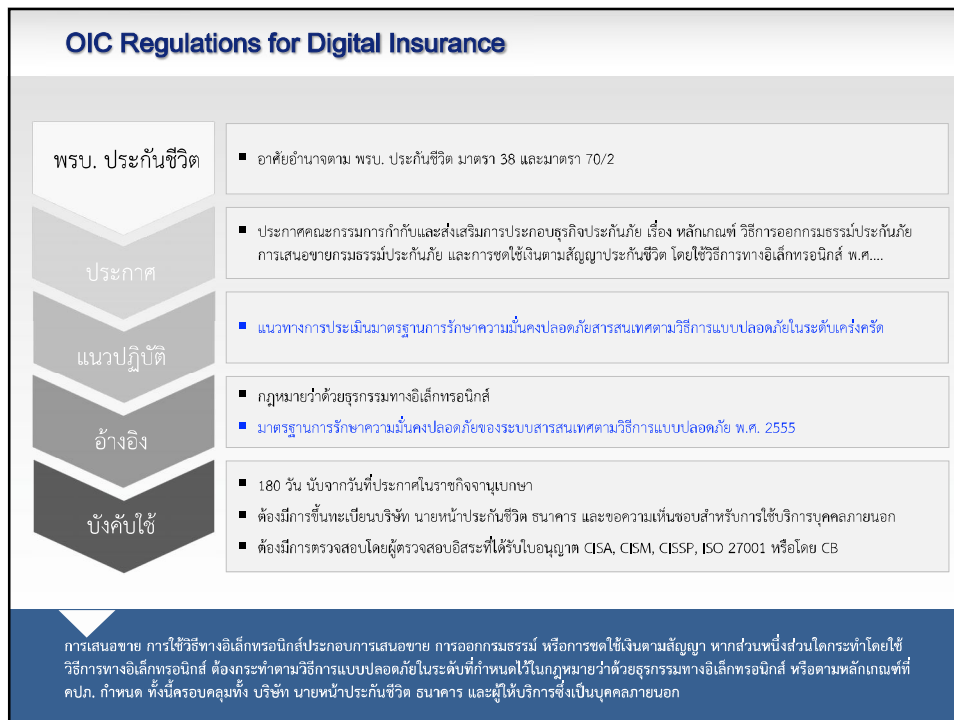
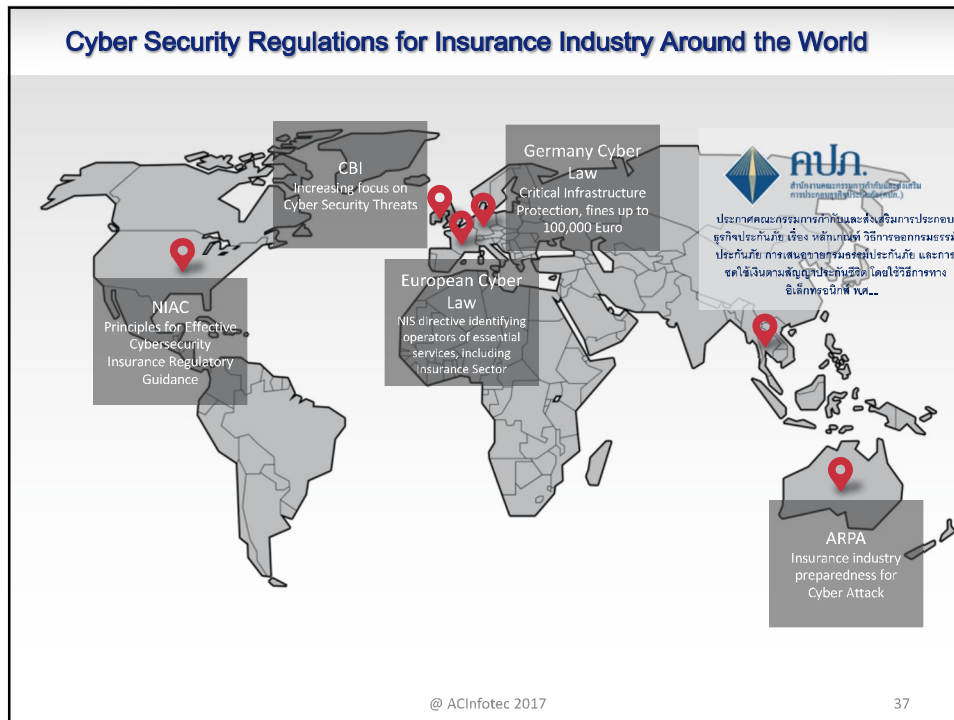
- Cyber-criminals breached the company database and stole information of more than one million customers and sales prospects, including national IDs, house registration, driving license, etc.

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.



OIC Regulations for Digital Insurance – More Points to Concern

+

Digital Signature

- หมวด 2 ข้อ 13 การส่งข้อมูลให้ผู้มุ่งหวัง ต้องลงลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- หมวด 4 การออกกรรมธรรม์ประกันภัยโดยใช้วิธีทางอิเล็กทรอนิกส์ ต้องกระทำการตามวิธีการแบบปลอดภัยในระดับที่กำหนดไว้ในกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และต้องลงลายมือชื่อทางอิเล็กทรอนิกส์
- ฯลฯ

+

Privacy

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

@ ACInfotec 2017

39

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 heightened 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?

@ ACInfotec 2017

40



Agenda



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

@ ACInfotec 2017

42

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
- แนวทางการประเมินมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศตามวิธีการแบบปลอดภัยในระดับองค์กร (OIC) → information security

@ ACInfotec 2017

43

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

ISO 27001 could bridge the regulatory divide, expert says

Bill Brenner



Karen Worstell, former CISO at Microsoft and AT&T Wireless, now on the advisory board of Neupart A/S, explains how ISO 27001 can be used to help companies comply with a variety of regulations and standards

PREMIUM CONTENT
New Ezine: CW ASEAN



Read about the latest business IT news and

Using ISO 27000 to comply with Data Protection Act principles

Stewart Room

The seventh data protection principle within the 1998 Data Protection Act calls organizations to use "appropriate" technical measures to safeguard personal information and to have regard for "the state of technological development." So what does that mean exactly? Stewart Room decides if you need state-of-the-art technology, or just the tools that will get the job done.

PREMIUM CONTENT
How to future-proof your network



Tips for reducing bottlenecks and improving performance

Free Download

ประกาศ มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศฯ

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

สอดคล้องกับ
11 Domains ของ
ISO 27001

มาตรฐานการรักษาความ
มั่นคงปลอดภัยของระบบ
สารสนเทศ

วิธีการแบบปลอดภัยระดับ
เคร่งครัด

พื้นฐาน + ปานกลาง
+ 42 ข้อ
รวม = 132 ข้อ

วิธีการแบบปลอดภัยระดับ
กลาง

พื้นฐาน + 38 ข้อ
รวม = 90 ข้อ

วิธีการแบบปลอดภัยระดับ
พื้นฐาน

52 ข้อ

@ ACInfotec 2017

45

ตัวอย่างมาตรการระดับพื้นฐาน



๑. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานต้องปฏิบัติ

ดังนี้

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

@ ACInfotec 2017

46

ตัวอย่างมาตรการระดับปานกลาง



๒. มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติม ดังนี้

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

ข้อ ๒. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

๒.๑ มีการกำหนดเงื่อนไขหรือหน้าที่ความรับผิดชอบต่าง ๆ เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศไว้อย่างชัดเจน

๒.๒ มีการกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศภายใต้สถานการณ์ต่าง ๆ ไว้อย่างชัดเจน

๒.๓ จัดให้มีการพิจารณาทบทวนแนวทางในการบริหารจัดการงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ ในการดำเนินงาน ทั้งนี้ การพิจารณาทบทวนดังกล่าวควรดำเนินการโดยผู้ไม่มีส่วนได้เสียกับงานที่มีการพิจารณาทบทวน

@ ACInfotec 2017

47

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 ในการพิจารณาจ้างพนักงานเข้าทำงาน หรือการว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้มีการตรวจสอบประวัติหรือคุณสมบัติเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบและจริยธรรมที่เกี่ยวข้อง โดยให้คำนึงถึงระดับชั้นความลับของข้อมูลสารสนเทศที่จะให้เข้าถึง และระดับความเสี่ยงที่ได้ประเมิน

๒.๒ ในสัญญาจ้างหรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก ให้ระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้ในสัญญา

ข้อ ๓. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

@ ACInfotec 2017

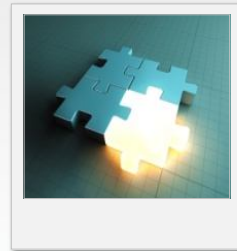
48

Common Concepts Across All Standards & Best Practices

They are all based on risks & controls



Assess Risk



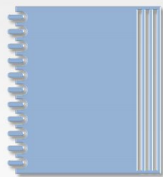
Select Controls

@ ACInfotec 2017

49

Common Concepts Across All Standards & Best Practices

Manage compliance using policy & audit



Information Security
Policies and Procedures



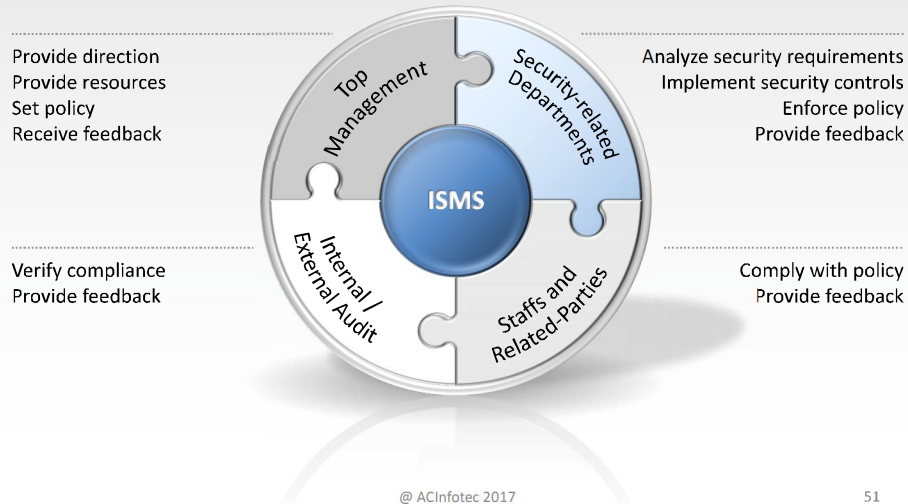
Internal Audit
External Audit
Continuous Monitoring

@ ACInfotec 2017

50

Common Concepts Across All Standards & Best Practices

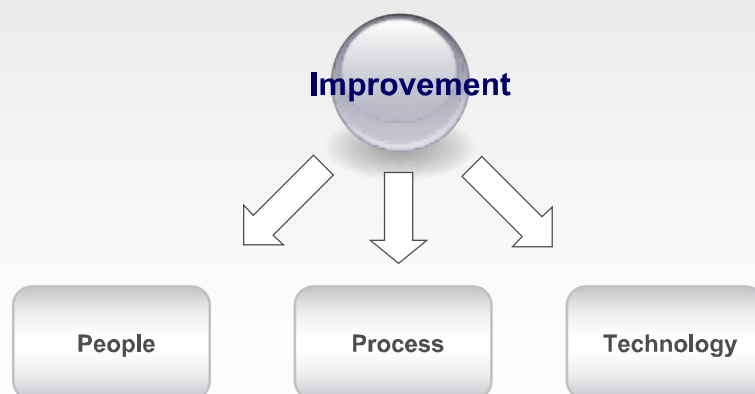
Top Management Oversees and Manages Security Risks



51

Common Concepts Across All Standards & Best Practices

Continual improvement



© ACInfotec 2017

52

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