

3 Feb 2016

Chief Information Officer : CIO 27

INFORMATION SECURITY MANAGEMENT

การบริหารงานด้านความมั่นคง

ปลอดภัยสารสนเทศ

Outline

- ◎ ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศเป็นศาสตร์และศิลป์ที่จำเป็นต้องเน้นให้ความสำคัญด้านการบริหารจัดการที่ต่อเนื่อง โดยจะต้องมีองค์ประกอบที่ครบถ้วน ไม่ว่าจะเป็นปัจจัยด้านเทคโนโลยี ปัจจัยด้านบุคลากร ปัจจัยด้านธรรมาภิบาล รวมทั้งปัจจัยภายนอกอื่นๆ ที่จำเป็นต้องมีความร่วมมืออย่างมีประสิทธิภาพ การบริหารจัดการที่ดีจะส่งผลกระทบต่อโอกาสทางธุรกิจ ความร่วมมือทางธุรกิจ ความเชื่อมั่นของผู้ใช้บริการอย่างมีนัยสำคัญ

Instructors

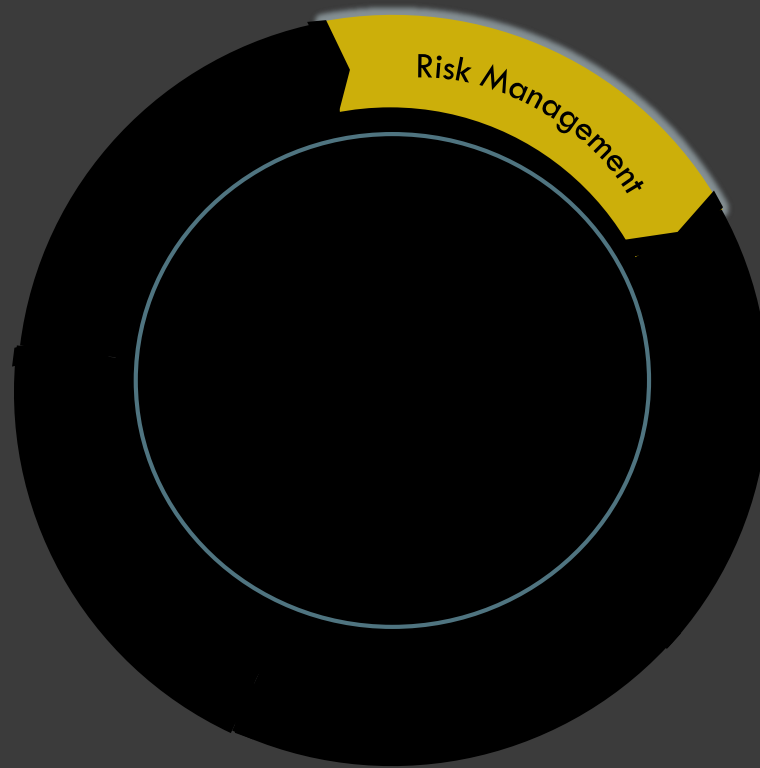


◎ ดร. กิตติ โฆษะวิสุทธิ์

- **Vice President** ธนาคารกรุงเทพ จำกัด (มหาชน)
- อนุกรรมการกำกับดูแลธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
- กรรมการวิชาการมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็กทรอนิกส์ (ISO27001)
- กรรมการสมาคมไทยแลนด์พีเคไอ (Thailand PKI Association)
- กรรมการสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ Thailand Information Security Association (TISA)

Information Security Framework

Information Security Framework





What is the RISK?



Various types of Risk



Determine Risk



What if you jump from the top of Taipei 101 building (508m.)?

What if you jump from the 2nd floor?

Who has RISK?



VIDEO #1: How to Outrun a Cheetah



Risk when you come to work

- ⦿ Police
- ⦿ Car Accident
- ⦿ Falling object
- ⦿ Theft
- ⦿ Car engine failure/overheat
- ⦿ Etc.

Risk Scenarios



Definition

“A risk scenario is a description of a possible event that, when occurring, will have an uncertain impact on the achievement of the enterprise’s objectives. The impact can be positive or negative.”



Four Types of Risk Mitigation

- ◎ **Risk reduction** – It is the most common risk management strategy. It reduces the negative effect or probability of the threat.
- ◎ **Risk avoidance** – Avoid any exposure to the risk. Usually it is the most expensive of all risk mitigation options
- ◎ **Risk transference** – Handing risk off to a willing third party
- ◎ **Risk acceptance** – it does not reduce any effects while the cost of other risk management options such as avoidance or reduction may outweigh the cost of the risk itself. A company that doesn't want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.



Threat : *A potential cause of an incident, that may result in harm of systems and organization*

--- ISO27005

Vulnerability: *A weakness of an asset or group of assets that can be exploited by one or more threats*

--- ISO27005

Vulnerability vs. Threat



= Risk ?



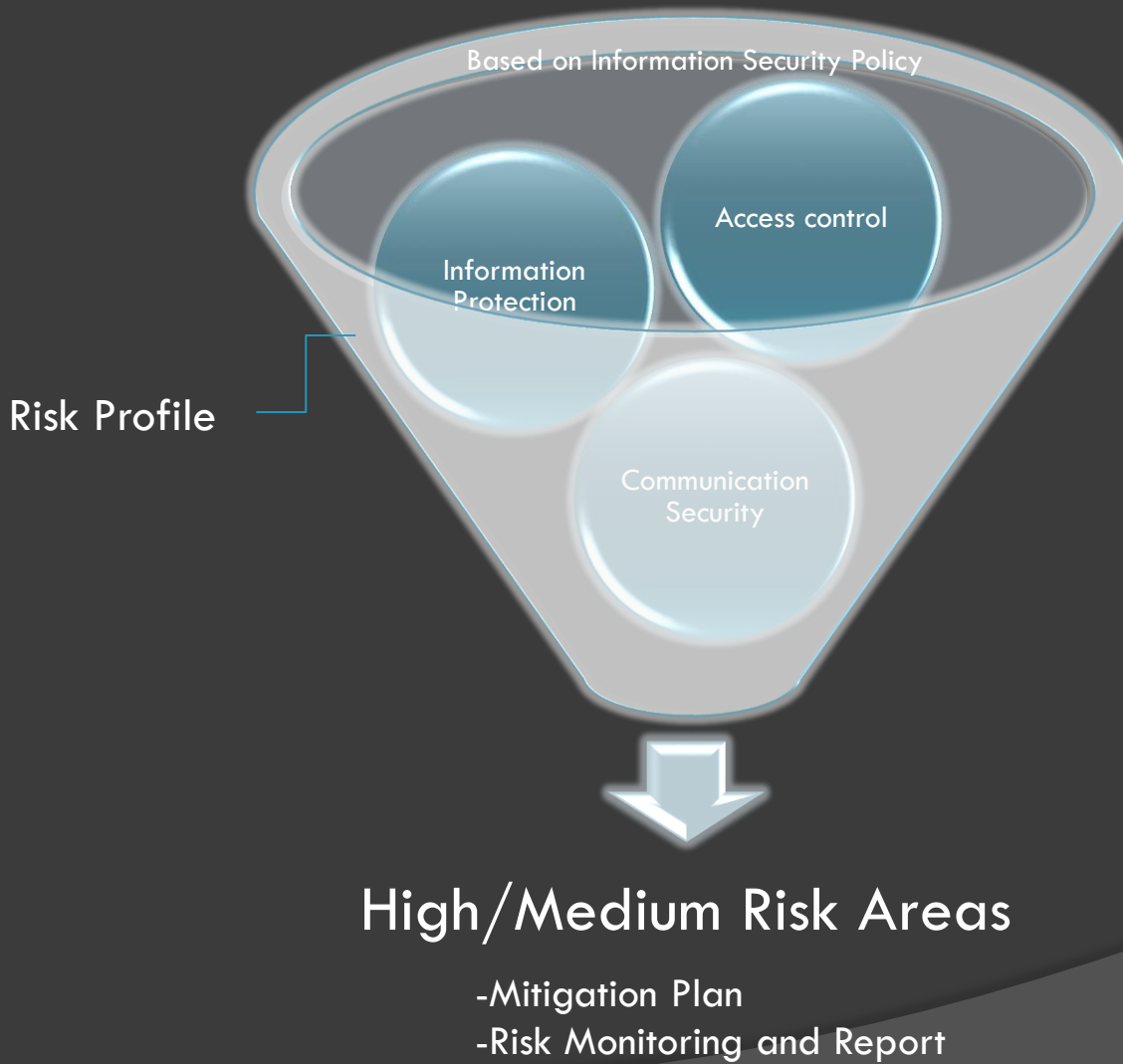
Vulnerability vs. Threat



With countermeasure



Risk management





Digest #1 : Secure Telephones

The organization needs to make phone calls that can't be overheard.



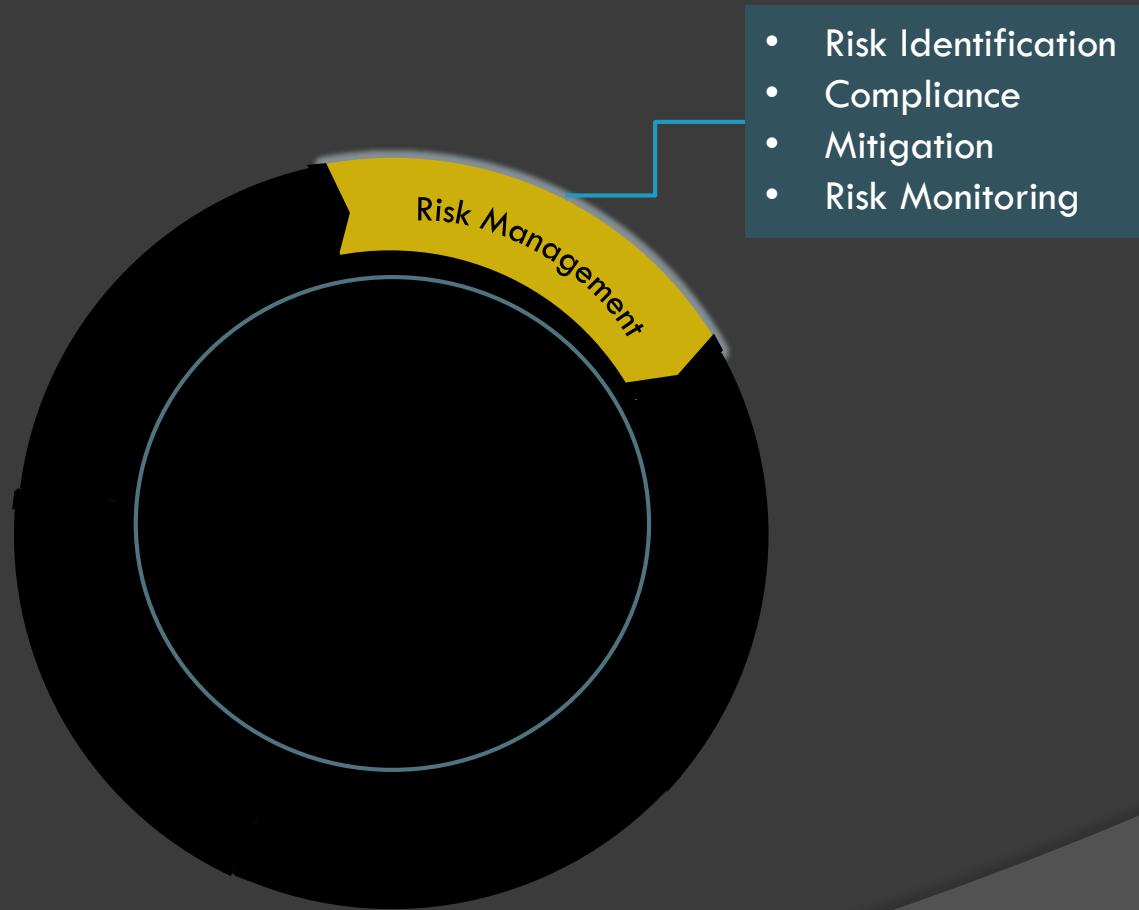
Use encrypted phone ??



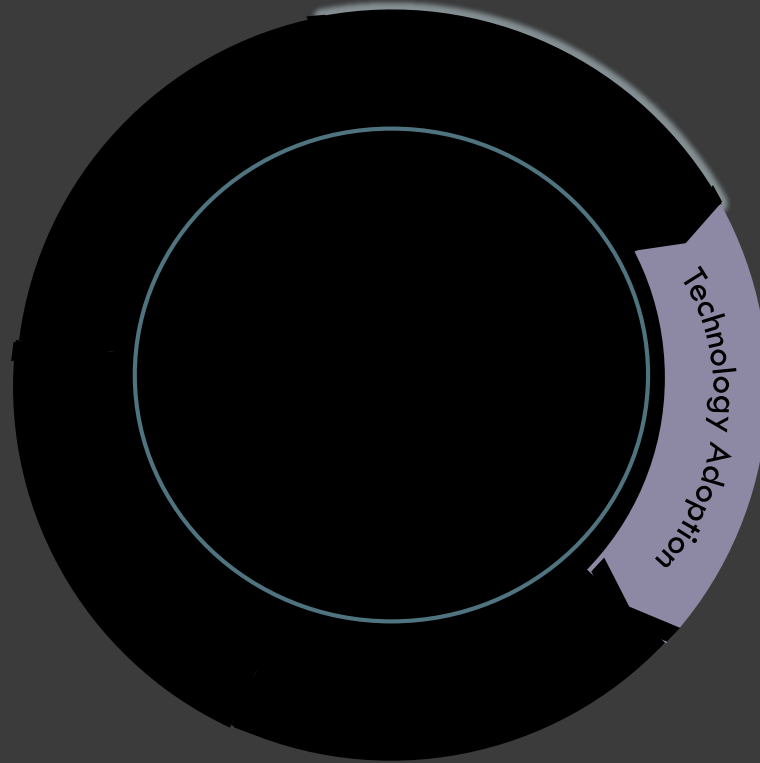
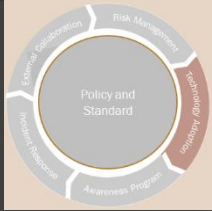
What are the threats?

- ⦿ Weak encryption algorithm
- ⦿ Mess the key generation system
- ⦿ Design & development
- ⦿ System bug or vulnerability
- ⦿ Manufacture process fault or sneaked
- ⦿ Maintenance
- ⦿ Force encrypted phone not to work

Information Security Framework

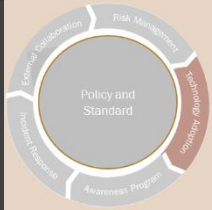


Technology adoption

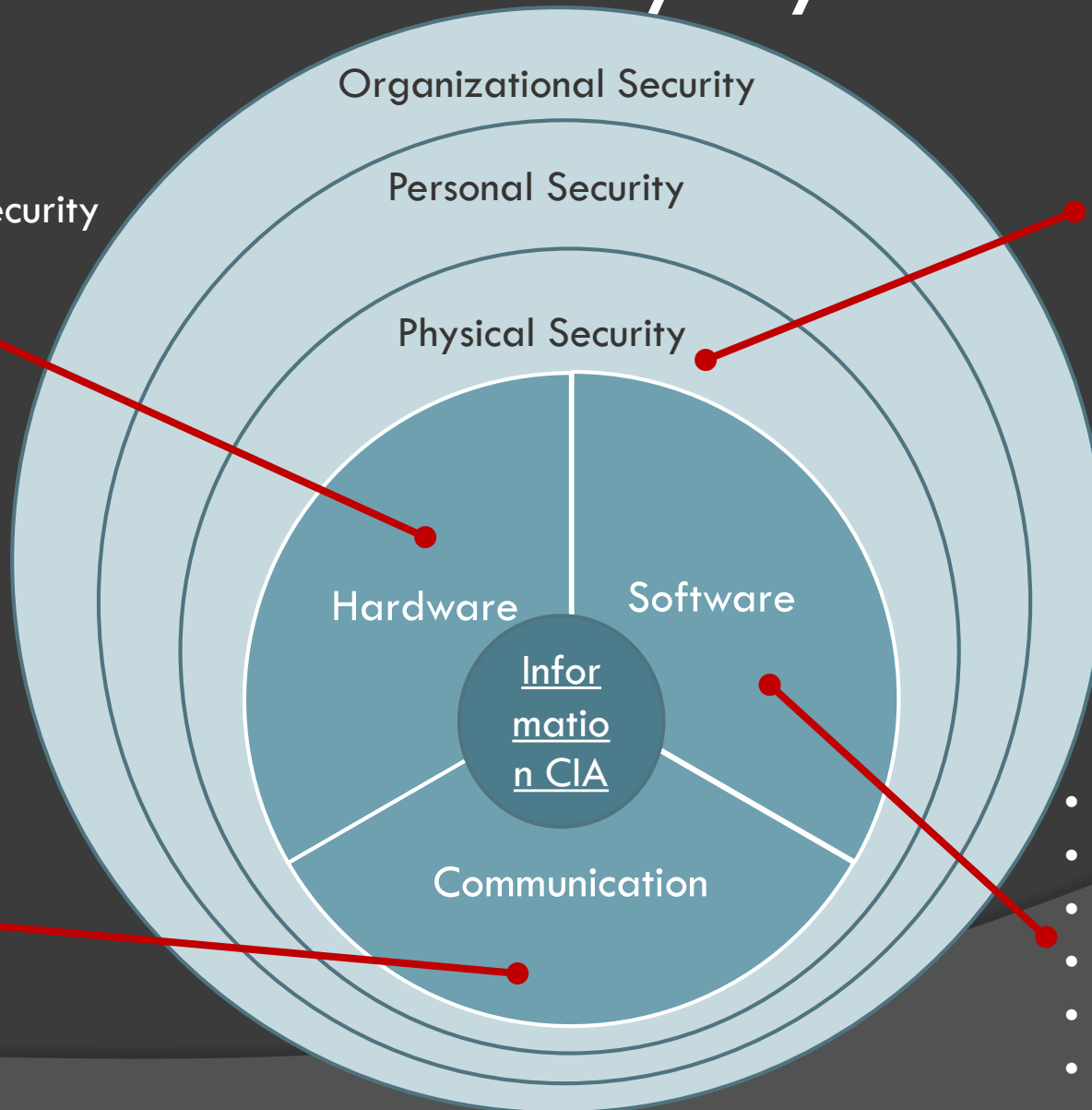
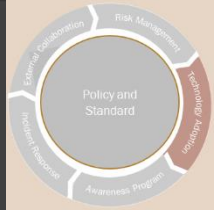




"You know, you can do this just as easily online."



Information Security System



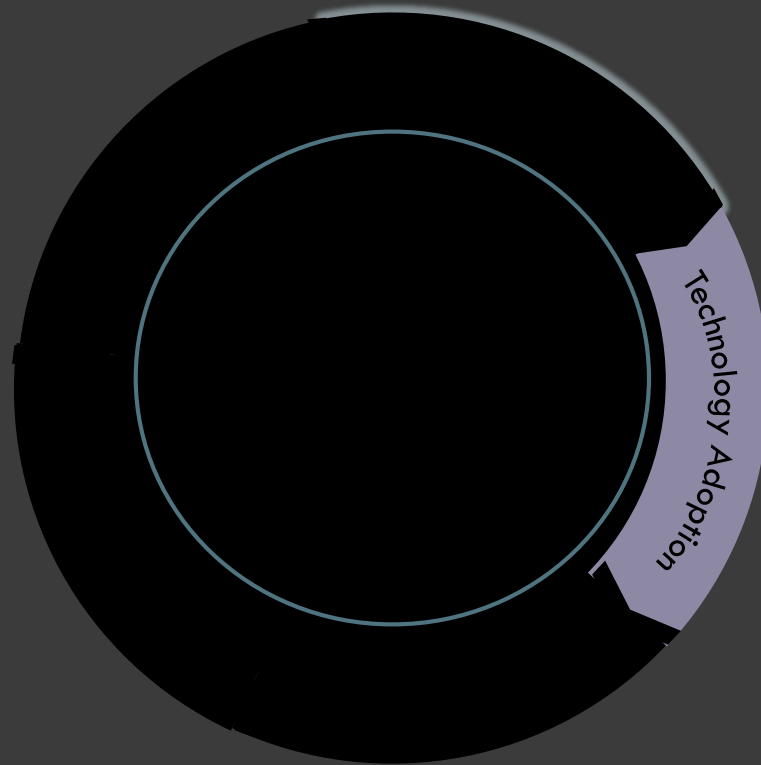
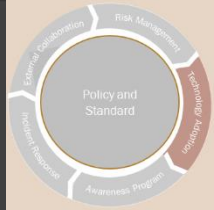
- Access Control
- Guard
- Fire Detection
- etc.

- Soft token
- Anti-virus/malware
- FIM
- Encryption
- Analytics
- etc.

- Hardware security
- Token
- Firewall
- IDS/IPS
- etc

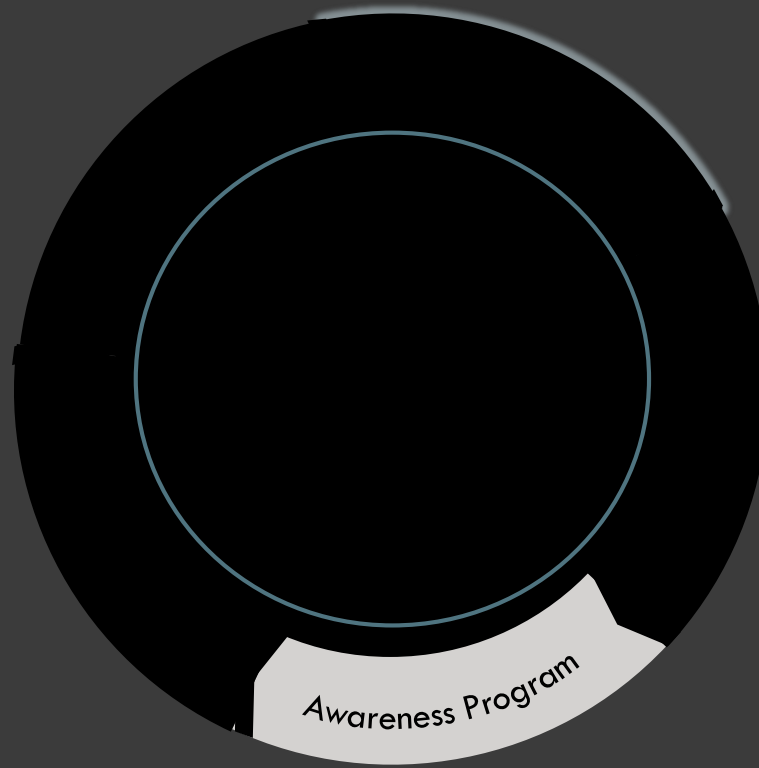
- IPSEC/VPN
- SSL/TLS
- etc

Technology adoption



- Infrastructure Refresh
- Application Security
- Monitoring and correlation Technology
- Analytics

Awareness program



Awareness on various attack methods?



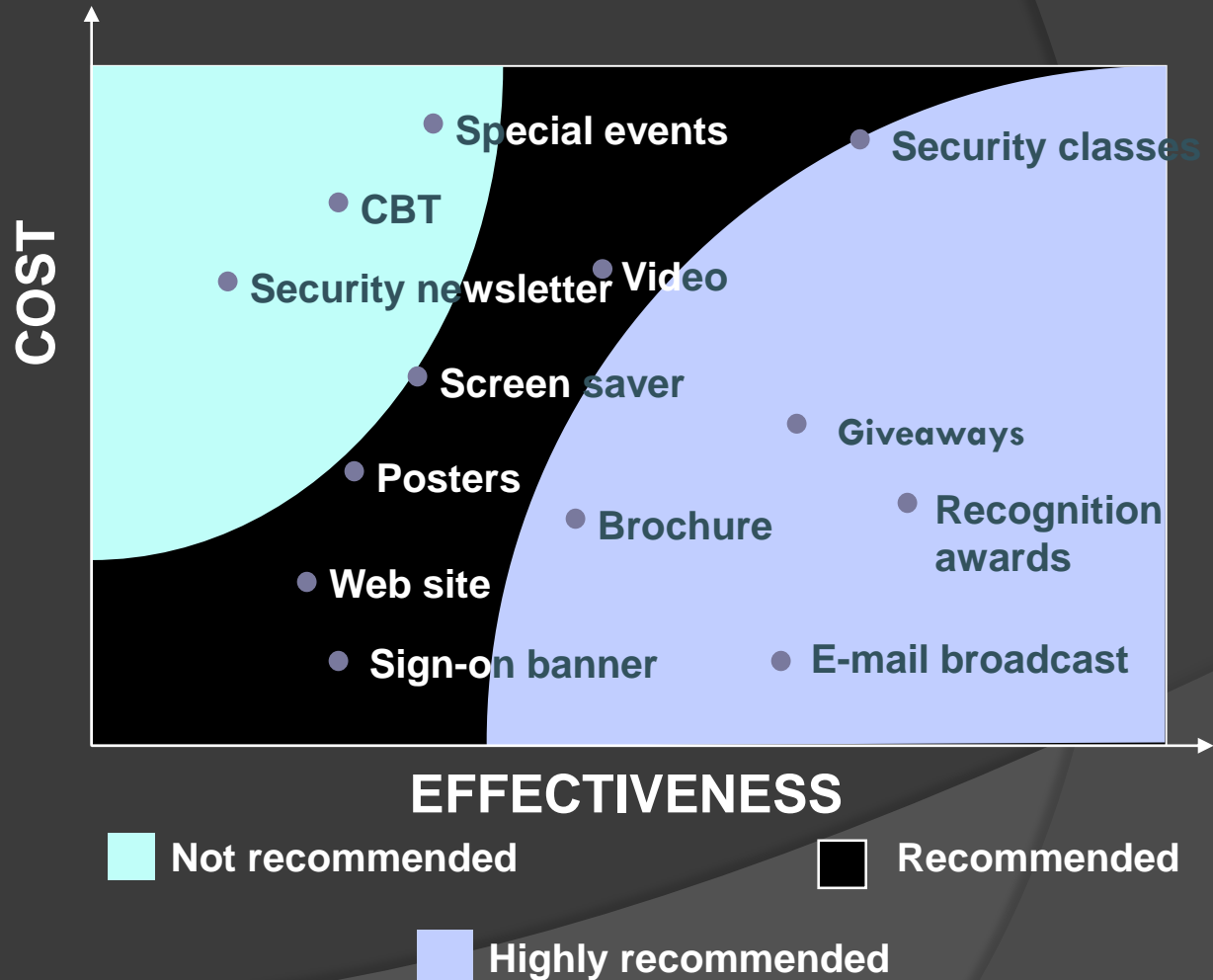
VIDEO #2: Cyber heist The Invisible Enemy



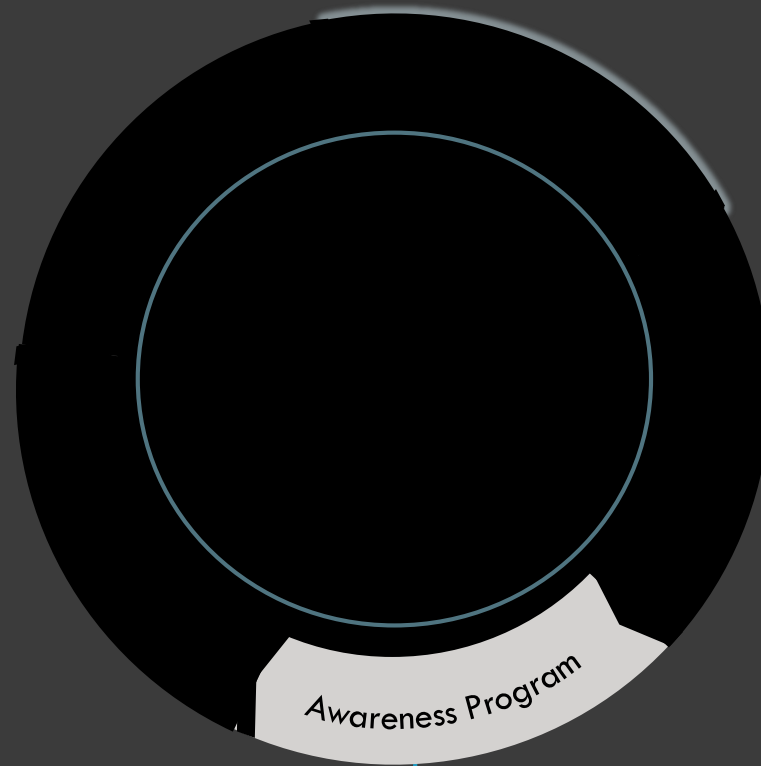
Awareness program

Master Plan and Method

Key Messages
Information Security
Information System Security
Hardware Security
Software Security
Access Control
Communication Security
Physical Security
Personnel Security
Information Asset Security
Business Continuity
Segregation of Duties

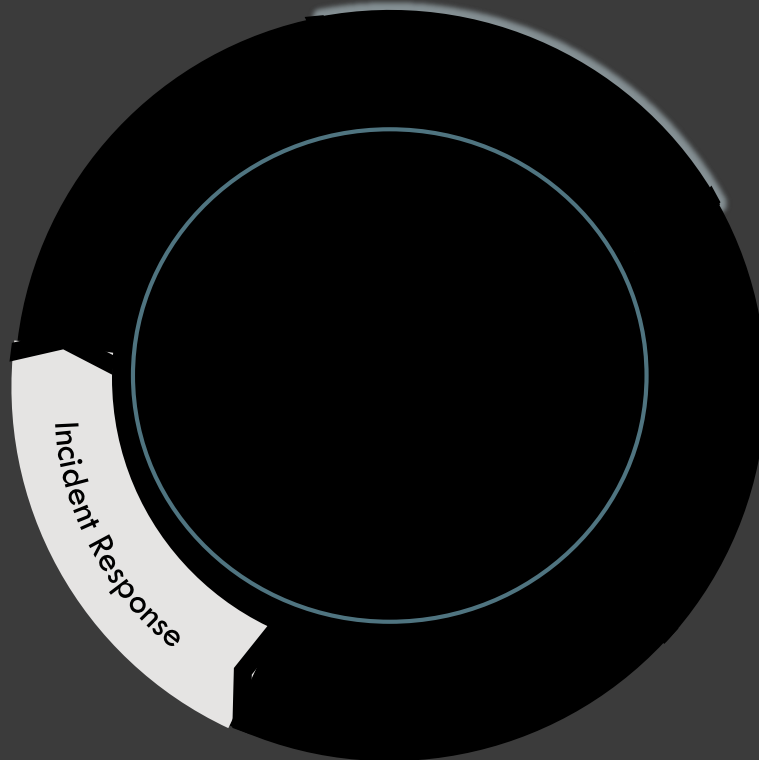


Awareness program



- Employee
- Executive
- Customer
- Vendor/Outsource
- Visitor

Incident response





Incident Response Process

Incident Scenarios

“Web Defacement”
“Phishing”
“DDoS”
etc.

Investigation

-Type of attack
-Source of attack

Analyze and Mitigate

-Target attack
-Technical impact
-Business impact
-Resolution

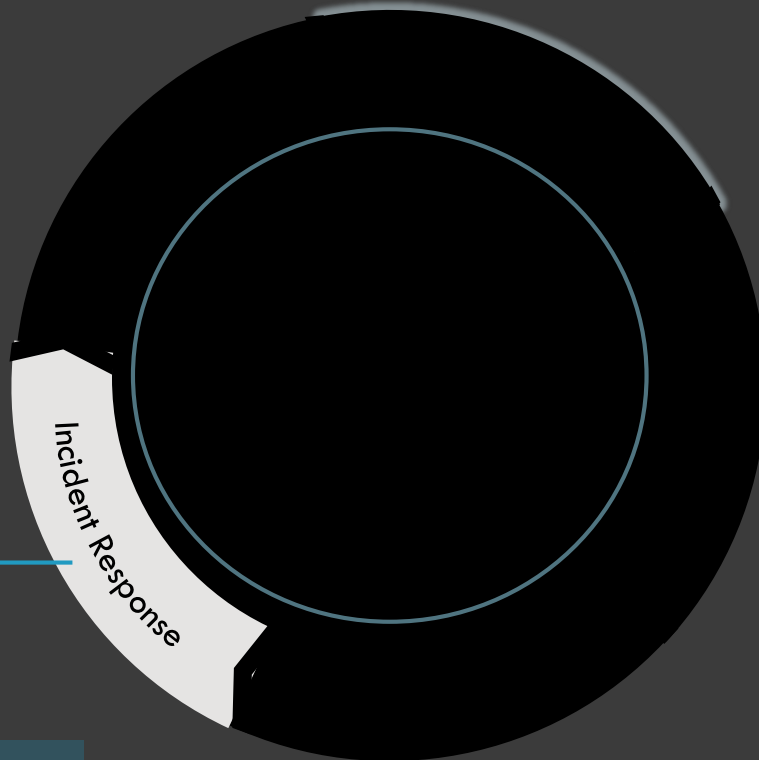
Communication

Related Parties
-Technical Team
-Business owner
-Executives



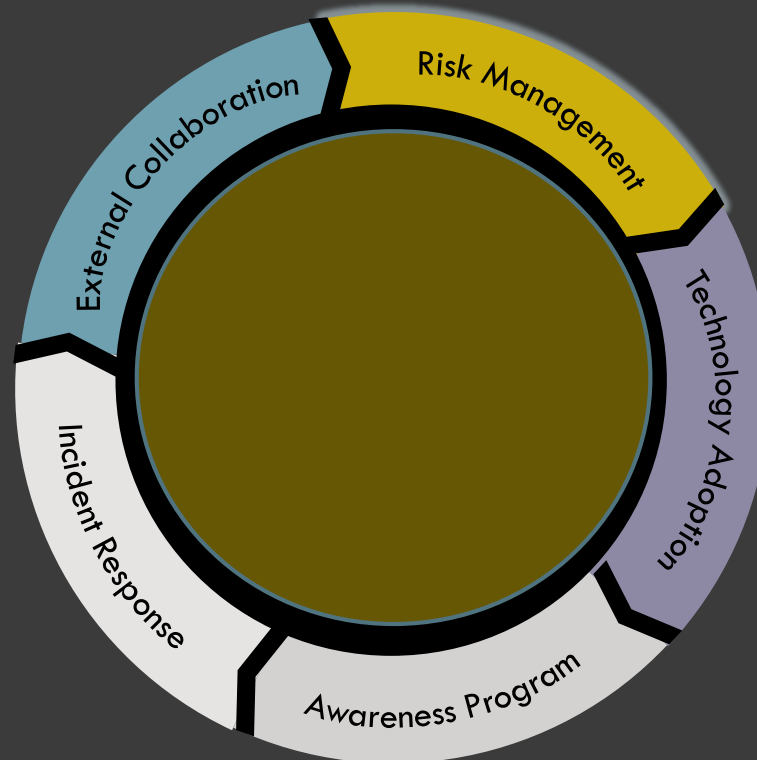
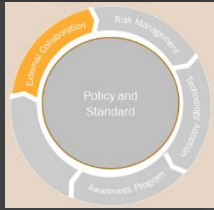
-Security Operator
-Monitoring Tool
-Customer

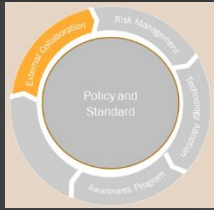
Incident response



- Operation Process
- Escalation Process
- Problem Management
- Analytics and Investigation
- Drill

External collaboration





External collaboration

Incident



Time

Information Sharing and Update

- Thai CERT
- US CERT Mail list
- NIST Mail list
- Key Vendor
- Key Security Consultant
- FS-ISAC

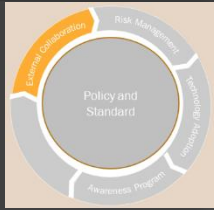
Co-ordinate with Law Enforcement

- DSI
- TCSD
- Thai CERT

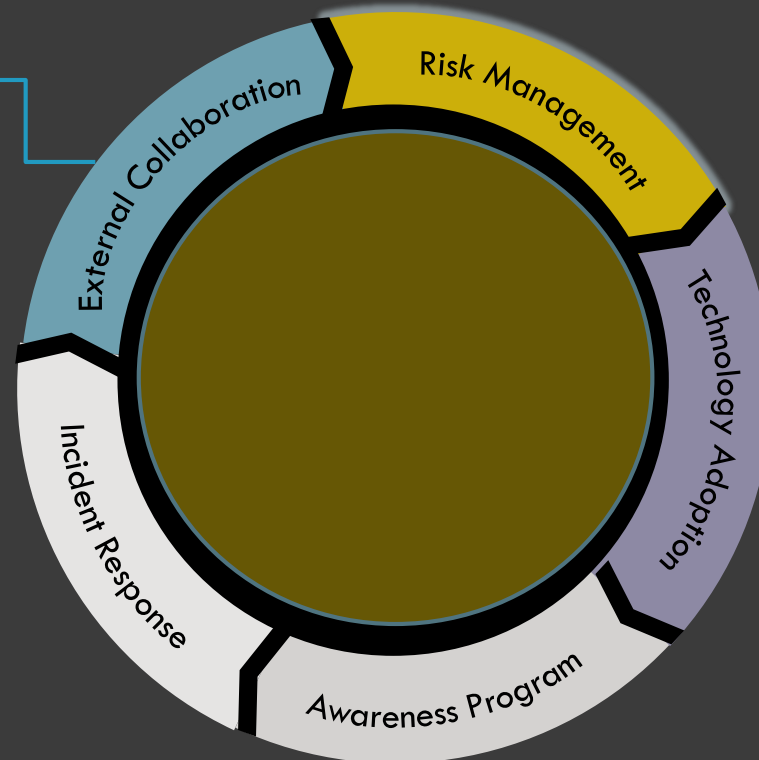
Communication with Media

- Media

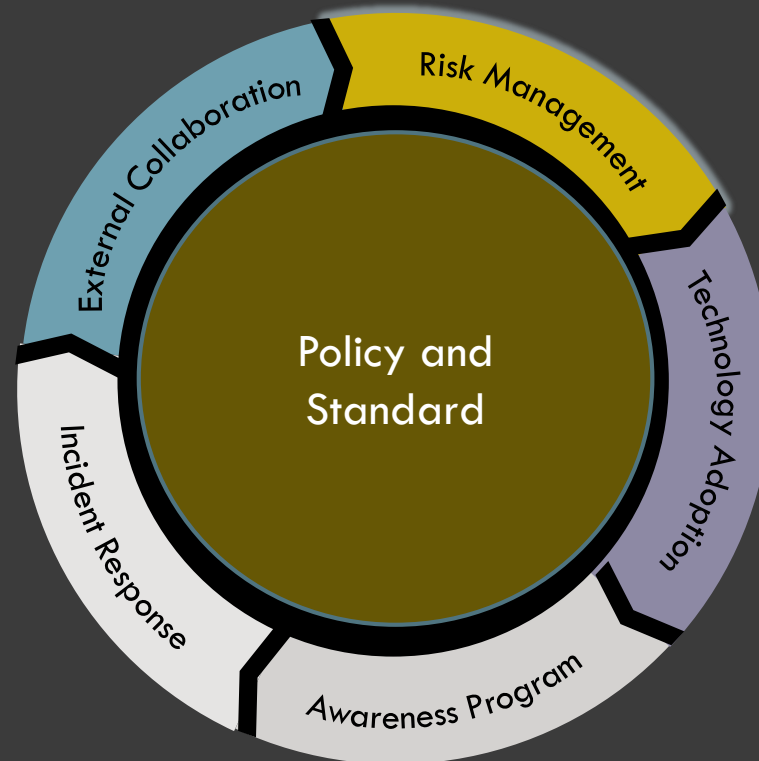
External collaboration



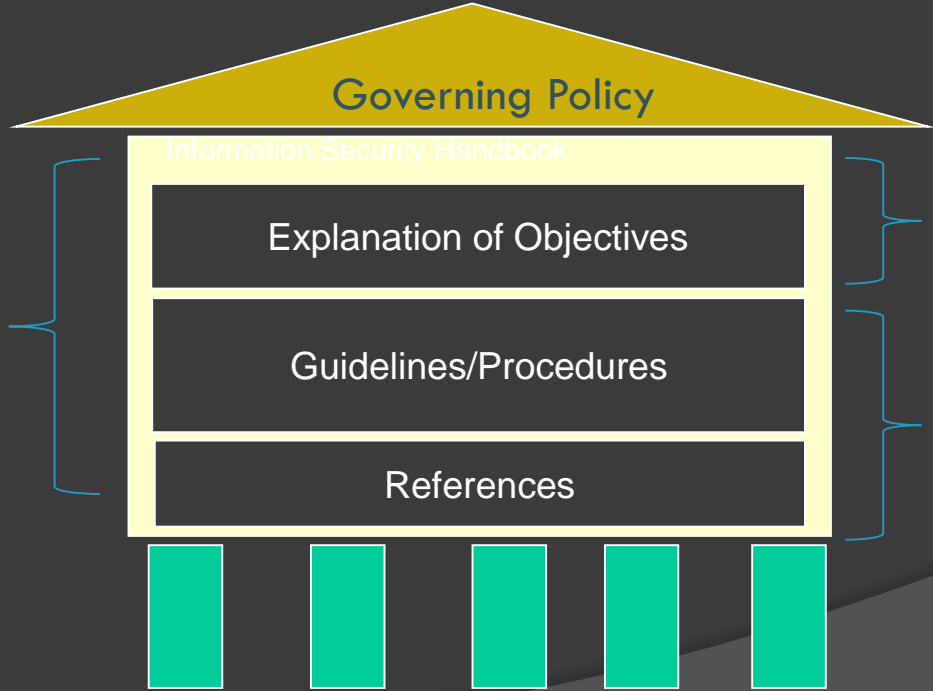
- Law Enforcement Agency
- Media
- CERT
- NIST
- FS-ISAC
- Key Vendor
- Consultant



Information Security Policy

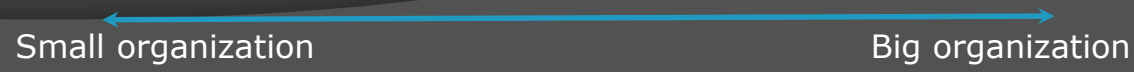


Balance

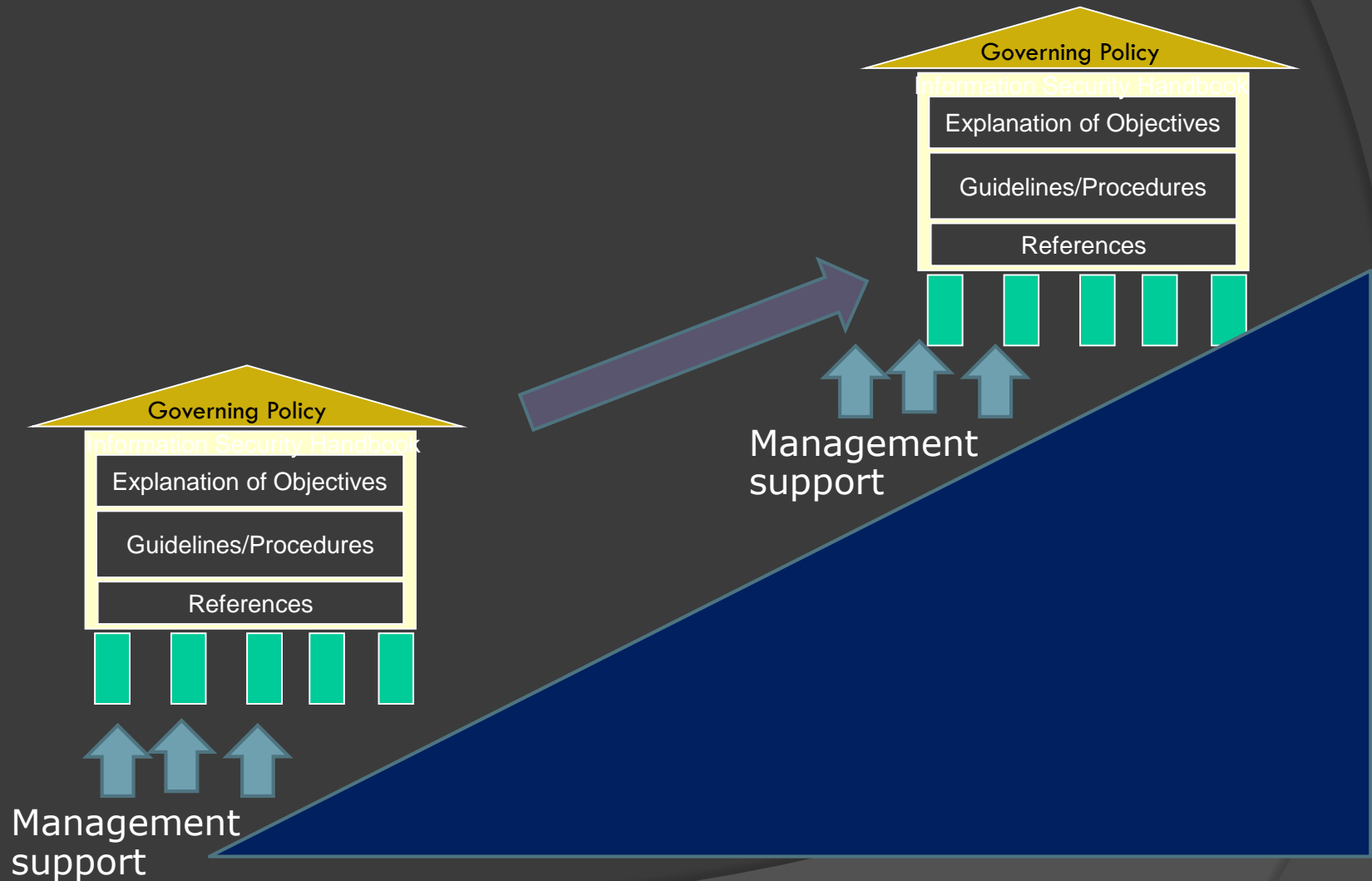


Combine for ease of communication and reference

Separate for ease of understanding, approval and update



Information Security Policy Improvement



Information Security Framework

- Law Enforcement Agency
- Media
- CERT
- NIST
- FS-ISAC
- Key Vendor
- Consultant

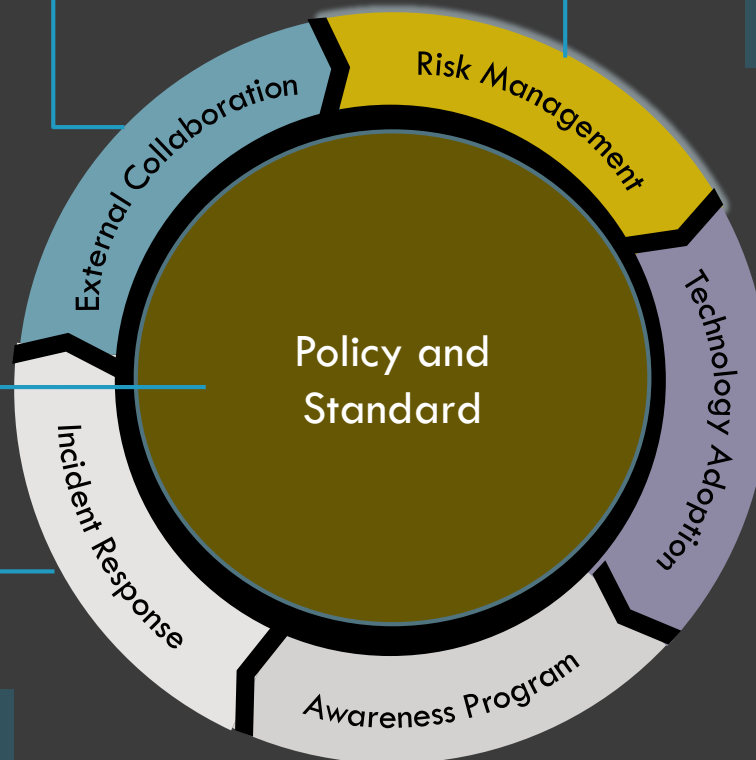
- Risk Identification
- Compliance
- Mitigation
- Risk Monitoring

- Information Security Committee
- Information Security Policy and Standard revising process

- Infrastructure Refresh
- Application Security
- Monitoring and correlation Technology
- Analytics

- Operation Process
- Escalation Process
- Problem Management
- Analytics and Investigation
- Drill

- Employee
- Executive
- Customer
- Vendor/Outsource
- Visitor



Security Incidents

Chase Attackers Exploited Basic Flaws

Hackers Compromised Server that Had Only Basic Authentication

By Tracy Kitten and Mathew J. Schwartz, December 24, 2014.

★ Credit Eligible



Email

Tweet

Like

Share

Get Permission



The **JPMorgan Chase breach** that began this past spring might have been prevented, if the bank's information security team hadn't failed to upgrade a sensitive server to require **two-factor authentication** controls.

SPEAR PHISHING AND CUSTOMER INFORMATION STOLEN (EMAIL, HOME ADDRESS AND PHONE NUMBER) BUT NOT FINANCIAL DATA.

70M CUSTOMER UNDER RISK

ACCORDING TO BLOOMBERG, THERE ARE BELIEVES THAT THE HACKERS WERE SPONSORED BY THE RUSSIAN GOVERNMENT AND IT MAY RELATE TO US-IMPOSED SANCTIONS ON RUSSIA.

North Korea threatens to blow up the White House, the Pentagon and other targets

f Like 30

Next: Nebraska and Oklahoma suing Colorado over marijuana

Use your key for the next article

December 22, 2014
9:17 AM MST



THE MONDAY BEFORE THANKSGIVING (15DEC2014), SONY PICTURES WAS ATTACKED BY NORTH KOREA. SENSITIVE INFORMATION WAS STOLEN AND WIPER MALWARE LAUNCH. THE STUDIO IS STILL HOLDING OFF ON ITS OFFICIAL ANNOUNCEMENT, BUT BY NOW IT SEEMS CLEAR THAT THE ATTACK CAME IN RETALIATION FOR THE UPCOMING FILM THE INTERVIEW, A COMEDY ABOUT AN ATTEMPT TO KILL NORTH KOREAN LEADER KIM JONG-UN.

Ref: <http://www.examiner.com/article/north-korea-threatens-to-blow-up-the-white-house-the-pentagon-and-other-targets>

Cyberattack suspected as North Korea experiences complete Internet outage

6.3k
SHARES



North Korean students in a computer lab at Kim Il Sung University in Pyongyang, North Korea, in 2013.

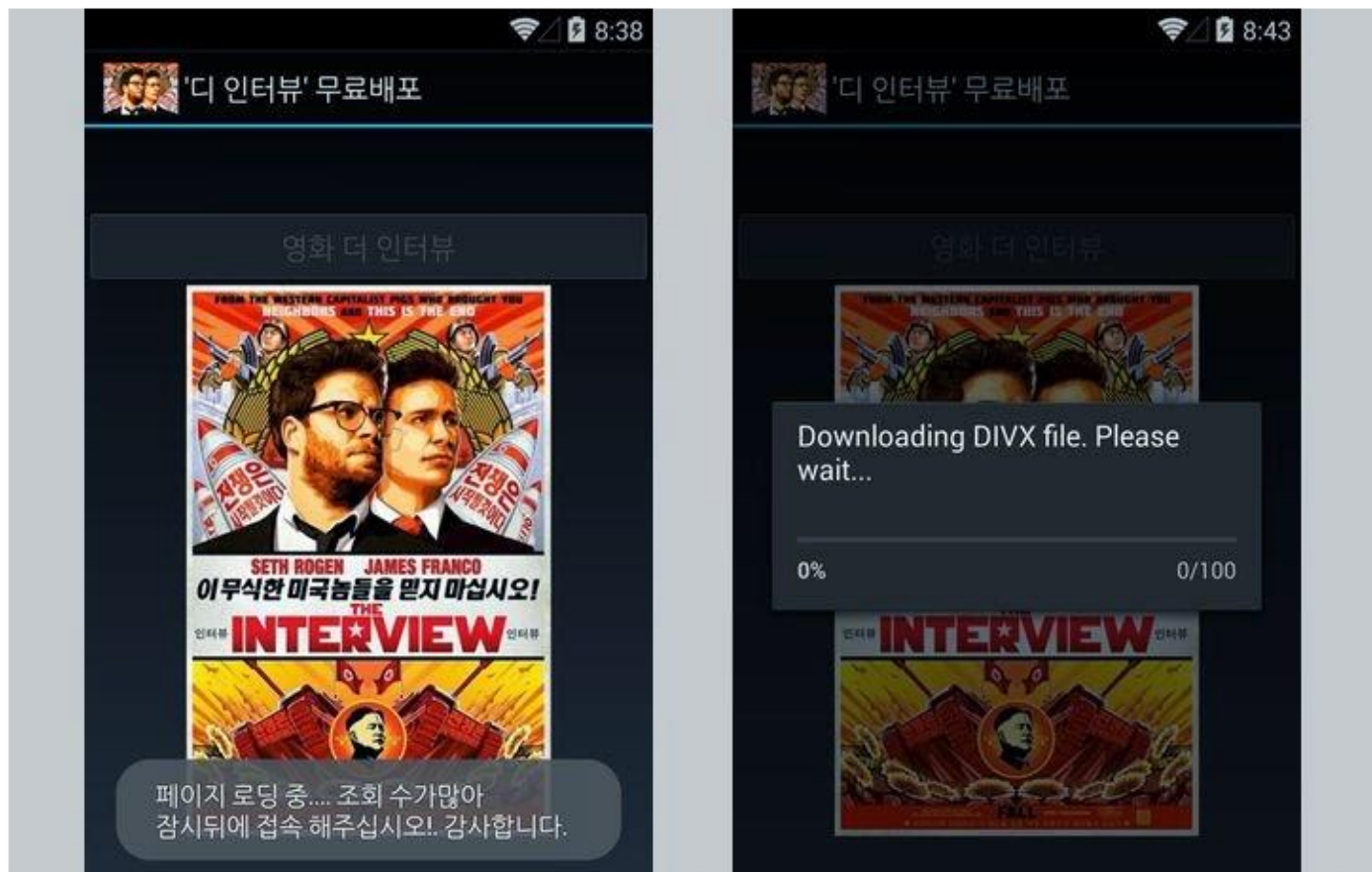
IMAGE: DAVID GUTTENFELDER/ASSOCIATED PRESS

**NORTH KOREA
EXPERIENCES
COMPLETE INTERNET
OUTAGE BY DDoS
FOR 9 HOURS**

Ref: http://mashable.com/2014/12/22/north-korea-internet-outage/?utm_cid=mash-com-Tw-main-link

Beware: Fake 'The Interview' App Affects Android Users

📅 Saturday, December 27, 2014 👤 Swati Khandelwal

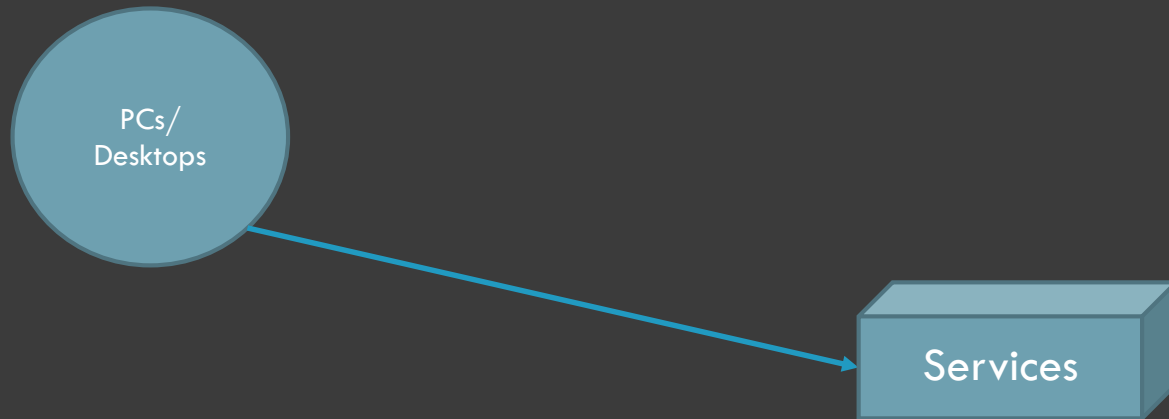


EVERYONE ALSO CAN BE THE TARGET WHERE THERE IS A HIGH LEVEL OF PUBLIC INTEREST.

"[The Interview](#)", the controversial North Korean-baiting film which appeared to be the root cause of the cyber mishap occurred at [Sony Pictures Entertainment](#) that threatened terror attack at theaters showing the movie, now threatens to expose users of Android phones to a malware attack.

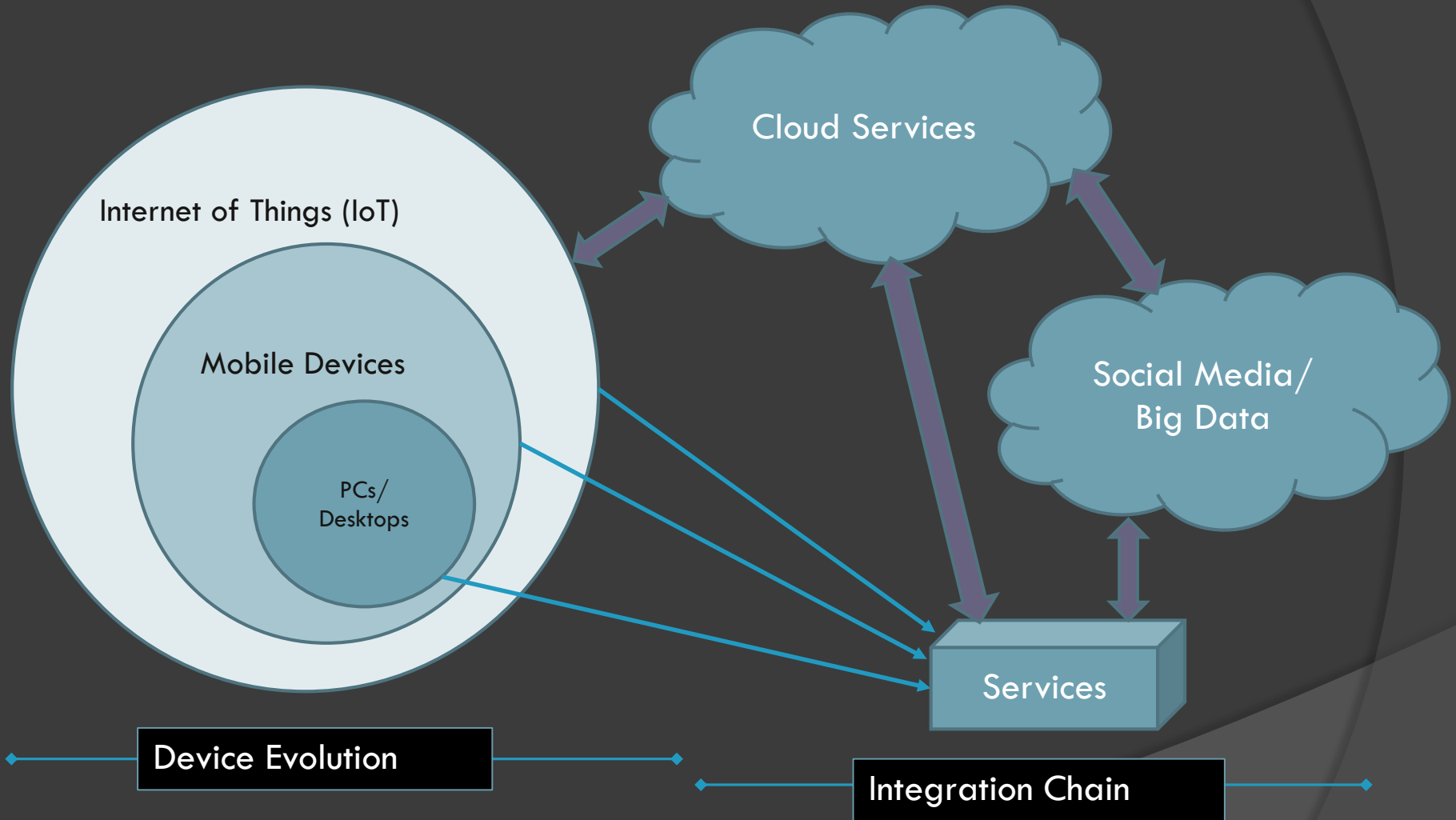
Since its release, everyone is talking about "The Interview" — the Seth Rogen and James Franco-starring comedy centered around a TV host and his producer assassinating North Korean dictator Kim Jong Un. Because cybercriminals are known to take advantage of major events where there is a high level of public interest, The Interview became their target.

Cyber Space - Traditional



Cyber Space Expands

Attack surface
Tremendously
expands



IoT – Internet of Thing

The Internet of Things (IoT) is the interconnection of uniquely identifiable [embedded computing devices](#) within the existing [Internet](#) infrastructure. Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue. According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 26 billion devices on the Internet of Things by 2020

IO – Information Operation

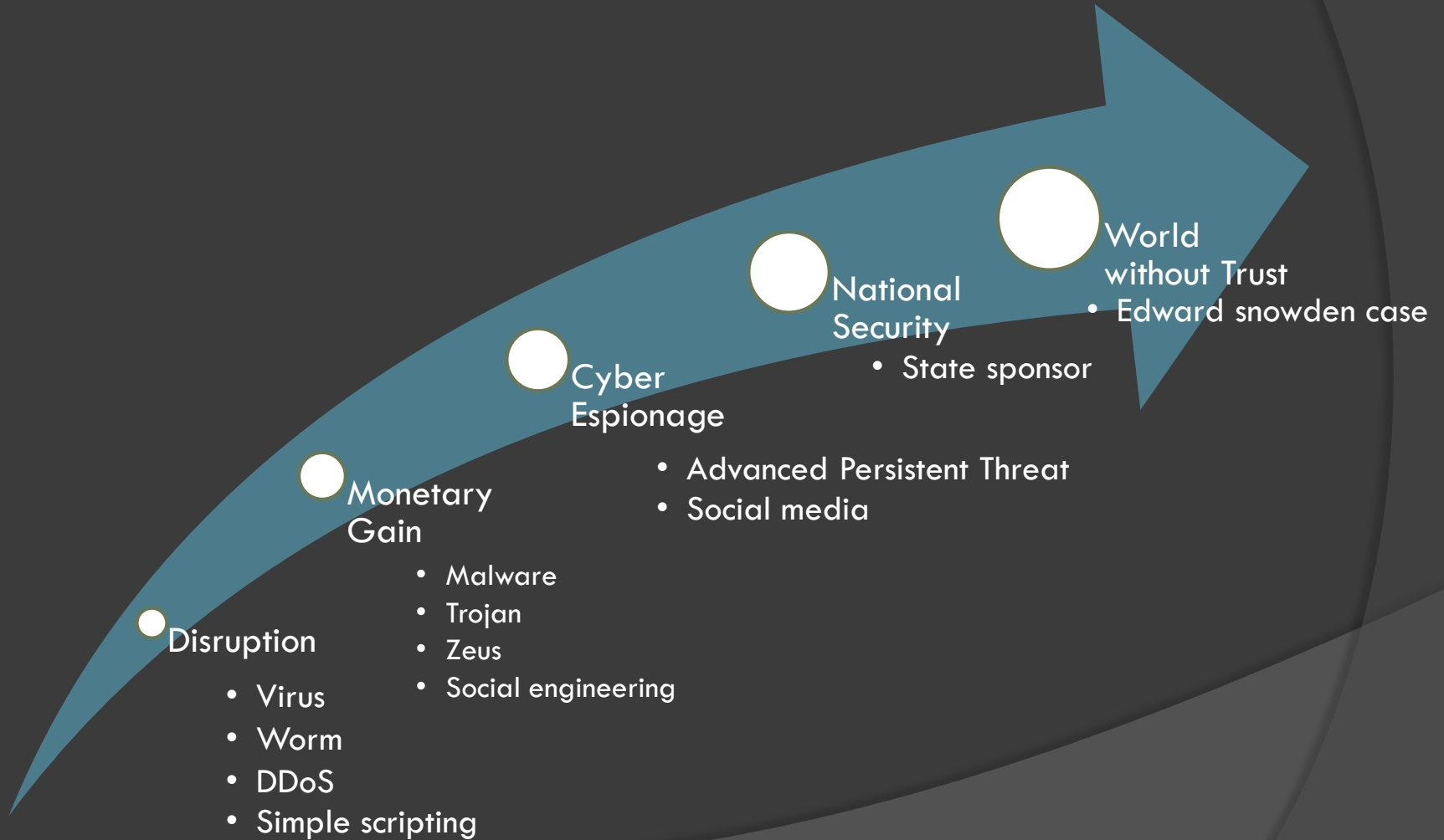
Information Operations (IO) are actions taken to affect adversary information and information systems while defending one's own information and information systems. or rumors deliberately spread widely to influence opinions

Privacy in our Everyday Life



VIDEO #3: Hot on Your Trail Privacy, Your Data, and Who has access to it

Motivation Change



Snowden Phenomenal



VIDEO #4: Watching Snowden's pivotal moments in Citizenfour

Why the data privacy matter?

What is Data Privacy (ข้อมูลส่วนบุคคล) ?



Internet and Our Privacy



VIDEO #5: The Internet and Our Right to Privacy

Why do we need Data Privacy Law?

หลักมาตรฐานสากลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (1)

1. ต้องแจ้งเจ้าของข้อมูลอย่างชัดเจนว่าจะมีการเก็บข้อมูลส่วนบุคคล วัตถุประสงค์การเก็บ ประเภทบุคคลหรือองค์กรที่ข้อมูลส่วนบุคคลอาจได้รับการเปิดเผย ต้องแจ้งสิทธิของเจ้าของข้อมูลและมาตรการที่จะใช้ในการจำกัดการใช้ การเปิดเผย การเข้าถึง และ การแก้ไข ทั้งนี้ต้องแจ้งก่อนหรือในขณะที่ยกเก็บ หรือเร็วที่สุดหลังการจัดเก็บ
2. ต้องมีการจัดเก็บอย่างจำกัดเท่าที่เป็นไปตามวัตถุประสงค์ของการเก็บ การเก็บต้องทำโดยวิธีที่ถูกต้องกฎหมาย และ วิธีที่เป็นธรรมและเหมาะสม โดยได้แจ้งต่อและได้ขอคำยินยอมจากเจ้าของข้อมูลแล้ว
3. ข้อมูลที่เก็บไว้จะเอาไปใช้ได้เฉพาะตามวัตถุประสงค์ของการเก็บเท่านั้น เว้นแต่ได้รับคำยินยอมจากเจ้าของข้อมูล

หลักมาตรฐานสากลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (2)

4. เจ้าของข้อมูลมีสิทธิเลือกว่าจะยินยอมให้มีการเก็บ ใช้และเปิดเผยข้อมูลส่วนบุคคลของตน
5. ข้อมูลที่จัดเก็บต้องมีความถูกต้อง สมบูรณ์ เป็นปัจจุบันตามความจำเป็นและตามวัตถุประสงค์การเก็บ
6. ต้องมีมาตรการคุ้มครองข้อมูลอย่างเหมาะสมเพื่อป้องกันอันตรายที่อาจเกิดไม่ว่าจะเป็นการสูญหาย เสียหาย การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การทำลายโดยไม่ได้รับอนุญาต การใช้ ปรับเปลี่ยน แก้ไข เปิดเผยโดยมิชอบ

หลักมาตรฐานสากลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (3)

7. เจ้าของข้อมูลที่มีสิทธิรับรู้ว่ามี การเก็บข้อมูลส่วนบุคคลของตนหรือไม่ และมีสิทธิเข้าถึงข้อมูลของตนเอง และมีสิทธิขอให้ตรวจสอบความถูกต้องและขอให้ปรับปรุงแก้ไข เพิ่มเติมหรือทำลาย ข้อมูลของตน
8. ผู้เก็บข้อมูลจะต้องรับผิดชอบจัดมาตรการต่างๆ ให้เป็นไปตามหลักเกณฑ์ดังกล่าว การส่งข้อมูลส่วนบุคคลไปยังบุคคลหรือองค์กรอื่นๆ ไม่ว่าจะภายในประเทศหรือส่งไปยังต่างประเทศ จะต้องได้รับความยินยอมจากเจ้าของข้อมูล และจะต้องมีมาตรการที่เหมาะสมที่ประกันได้ว่า บุคคลหรือองค์กรที่ได้รับข้อมูลไปแล้วจะเก็บรักษาข้อมูลให้เป็นไปตามหลักเกณฑ์นี้

หลักมาตรฐานสากลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (4)

9. ในกรณีที่เป็นการค้าขายที่เกี่ยวกับข้อมูลของเด็กเยาวชน หรือผู้ที่ยังไม่บรรลุนิติภาวะ จะต้องคำนึงถึงการให้คำยินยอมที่เหมาะสม ไม่ว่าจะเป็นการดำเนินการโดยตัวผู้เยาว์เอง หรือโดยผู้ปกครองที่ชอบด้วยกฎหมายรวมทั้งการใช้ดุลยพินิจของผู้ปกครองโดยพหุติฝ่าย และสถาบันด้านการศึกษา
10. ในกรณีที่จะต้องมีการว่าจ้างหรือมอบหมายให้บุคคลหรือหน่วยงานอื่น (**third party**) ในลักษณะหน่วยให้บริการ (**service provider**) ให้ทำหน้าที่หรือจัดการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล บุคคลหรือหน่วยงานดังกล่าวจะต้องมีระบบการคุ้มครองข้อมูลที่มีมาตรฐาน และจะต้องมีการจัดทำข้อตกลงที่ชัดเจนว่าบุคคลหรือองค์กรดังกล่าวเมื่อได้รับและครอบครองข้อมูลไปแล้วจะเก็บรักษาข้อมูลให้เป็นไปตามหลักเกณฑ์นี้

Digest #2 : Privacy in Practice

ในสถานการณ์ที่มีเหตุ ฆาตกรรม เกิดขึ้นบ่อยครั้งในห้องน้ำสาธารณะ การดำเนินการป้องปรามเหตุดังกล่าว มีข้อเสนอให้ติดตั้ง **CCTV** ในทุกห้องน้ำสาธารณะ ท่านเห็นด้วยหรือไม่และหากต้องดำเนินการควรจะดำเนินการอย่างไร

Information Security Framework

- Law Enforcement Agency
- Media
- CERT
- NIST
- FS-ISAC
- Key Vendor
- Consultant

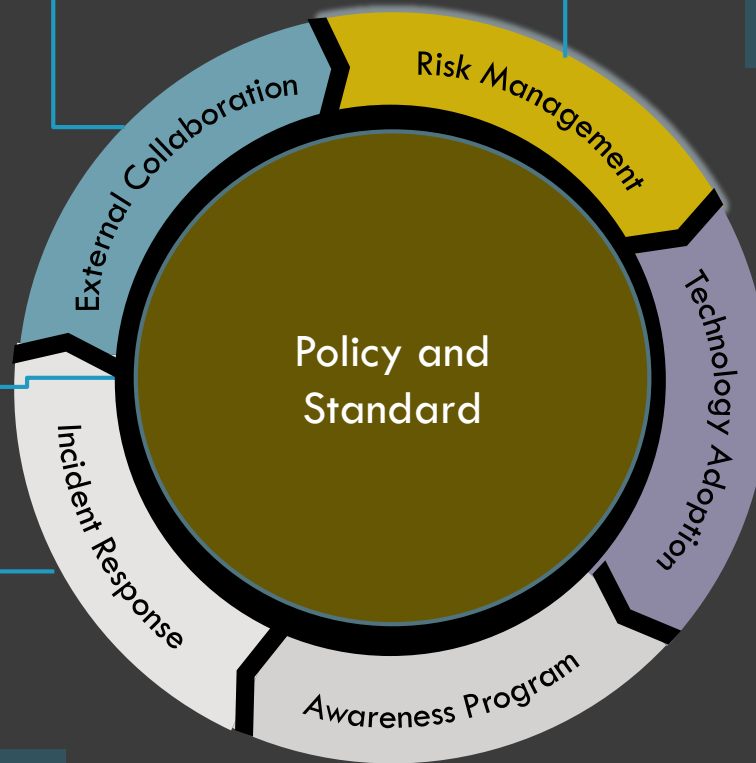
- Risk Identification
- Compliance
- Mitigation
- Risk Monitoring

- Information Security Committee
- Information Security Policy and Standard revising process

- Infrastructure Refresh
- Application Security
- Monitoring and correlation Technology
- Analytics

- Operation Process
- Escalation Process
- Problem Management
- Analytics and Investigation

- Employee
- Executive
- Customer
- Vendor/Outsource
- Visitor



Thank you