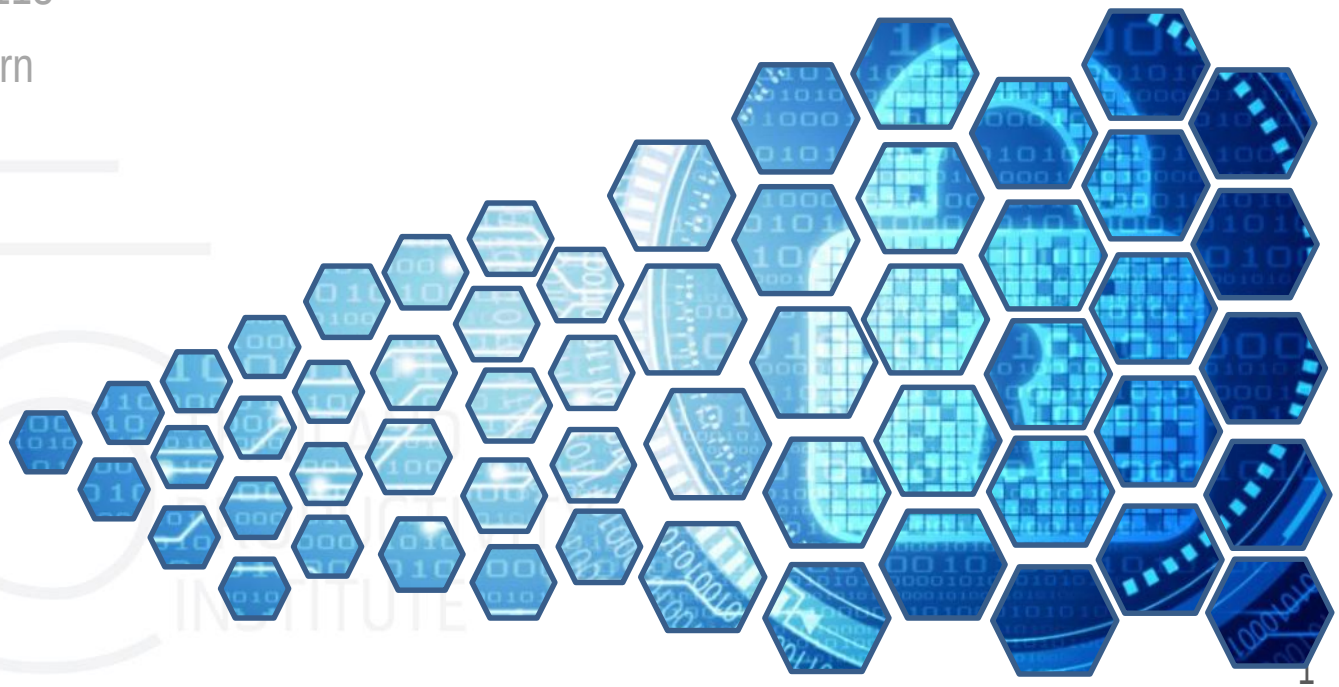
Cyber Security & TQA Criteria

By Athisarn Wayuparb, Ph.D., CISA

January 16, 2020

089-109-7113

Line: athisarn



Transforming Productivity for Tomorrow Success

Changed Criteria

- Overall & Multiple Level

2020

- Information Systems Security
- Information Confidentiality

Cybersecurity

Extended Cybersecurity

2001

2017

2019

Transforming Productivity for Tomorrow Success

BASIC

1

Reacting to the problem (0–5%)

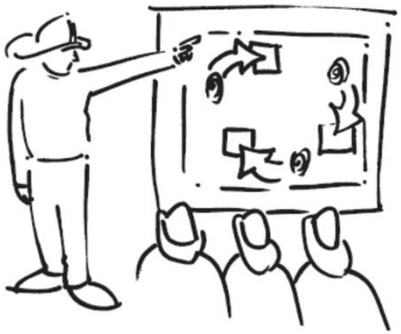
Run with the hose and put out the fire.

2

General improvement orientation (10–25%)

Install more fire hoses to get to the fires quickly and reduce their impact.

3

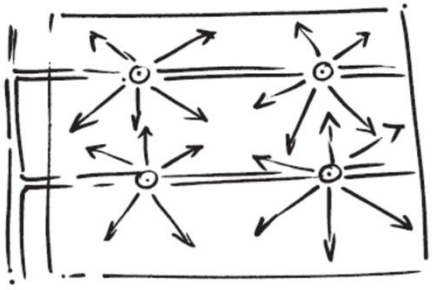


Systematic evaluation and improvement (30–45%)

Evaluate which locations are most susceptible to fire. Install heat sensors and sprinklers in those locations.

OVERALL

4



Learning and strategic improvement (50–65%)

Install systemwide heat sensors and a sprinkler system that is activated by the heat preceding fires.

MULTIPLES

5

Organizational analysis and innovation (70–100%)

Use fireproof and fire-retardant materials. Replace combustible liquids with water-based liquids. Prevention is the primary approach for protection, with sensors and sprinklers as the secondary line of protection. This approach has been shared with all facilities and is practiced in all locations.

THAILAND PRODUCTIVITY INSTITUTE

6.2 Operational Effectiveness

	(Baldrige 2017-2018) Overall Approach 50% and 65%	(Baldrige 2019-2020) Overall Approach 50% and 65%
6.2b(1)	~~Ensure the reliability of information systems~~	Ensure the security and cybersecurity of • Sensitive or privileged data and information, and • Key assets
6.2b(2)	Ensure the security and cybersecurity of sensitive or privileged data and information	

6.2b. Managing cybersecurity includes protecting against the loss of sensitive information about employees, customers, and organizations; protecting assets, including intellectual property; and protecting against the financial, legal, and reputational aspects of breaches. There are many sources for general and industry-specific cybersecurity standards and practices. Many are referenced in the *Framework for Improving Critical Infrastructure Cybersecurity* (https://www.nist.gov/cyberframework). The *Baldrige Cybersecurity Excellence Builder* (https://www.nist.gov/baldrige/products-services) is a self-assessment tool incorporating the concepts of the Cybersecurity Framework and the Baldrige systems perspective.

6.2 Operational Effectiveness

	(Baldrige 2017-2018) Multiple Level 70% and 100%	(Baldrige 2019-2020) Multiple Level 70% and 100%
6.2b(1)		• Manage electronic and physical data and information **and key operational systems** to ensure confidentiality and only appropriate access • Be aware of emerging security and cybersecurity threat • **Ensure that the workforce, customers, partners, and suppliers understand and fulfill security and cybersecurity responsibilities** • Identify and prioritize information technology and **operational systems** to secure • **Protect** these systems from potential cybersecurity attacks and **detect, respond to, and recover** from cybersecurity incidents
6.2b(2)	• Manage electronic and physical data and information to ensure confidentiality and only appropriate access • Be aware of emerging security and cybersecurity threats • Identify and prioritize information technology systems to be secure from cybersecurity attacks and protect the systems from attack • Detect, respond to, and recover from cybersecurity breaches	

- Loss of Sensitive Information
  - Customers
  - Employees
  - Organizations
- Assets
- Intellectual Properties
- Security Breaches aftermath
  - Financial
  - Legal
  - Reputation

Category 1: Leadership Commitment

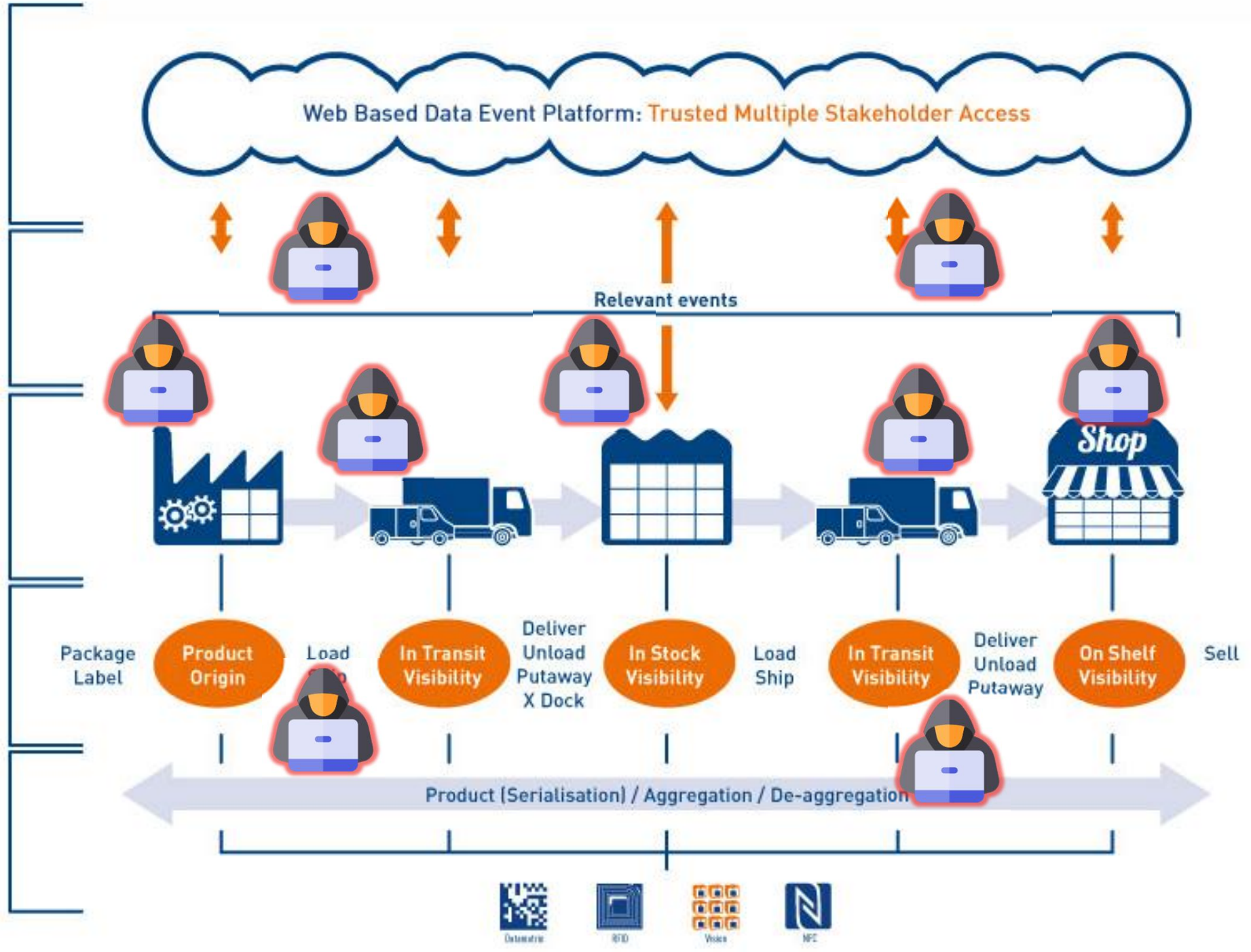
Category 2: Strategic Development & Deployment

Category 3: Customer Data & All Interactions

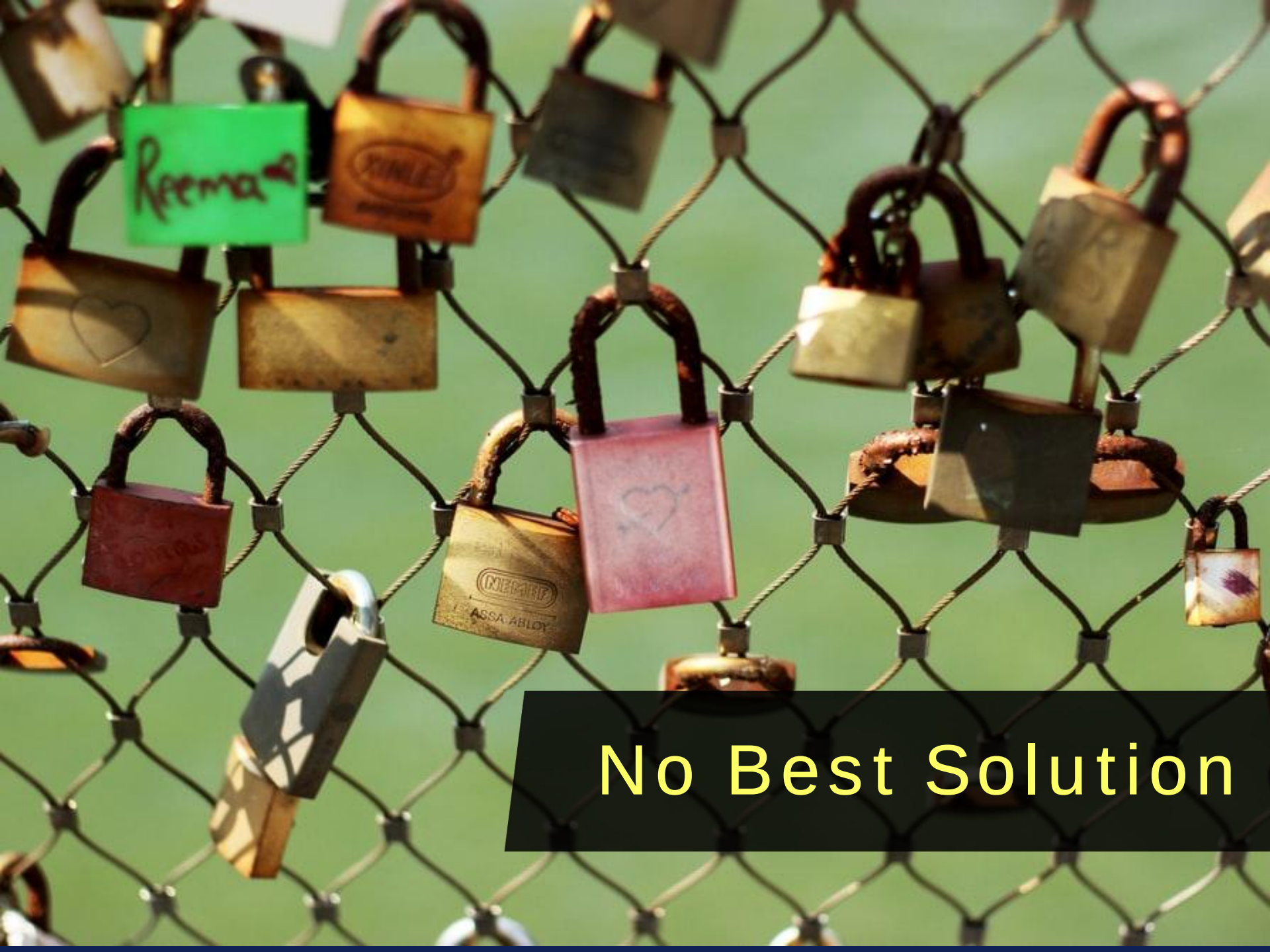
Category 4: Data, IT, and KM

Category 5: Workforce Training

Category 6: Process, Supplier, BCP


Web Based Data Event Platform: Trusted Multiple Stakeholder Access
Relevant events
Shop
Package Label
Product Origin
Load
In Transit Visibility
Deliver Unload Putaway X Dock
In Stock Visibility
Load Ship
In Transit Visibility
Deliver Unload Putaway
On Shelf Visibility
Sell
Product (Serialisation) / Aggregation / De-aggregation

Cyber-security solutions and Investments
How much Loss you can take?


No Best Solution

Examples:

- Name
- Home Address
- Email Address
- ID Card
- Location Data
- IP Address
- Cookie ID
- Data held by a hospital or doctors that uniquely identifies a person

EU Commission

(https://ec.Europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en)

Companies:

- Employee Data
- Customer Data
- Supplier Data
- Intellectual Properties
- All confidential documents

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

FACT & FIGURES

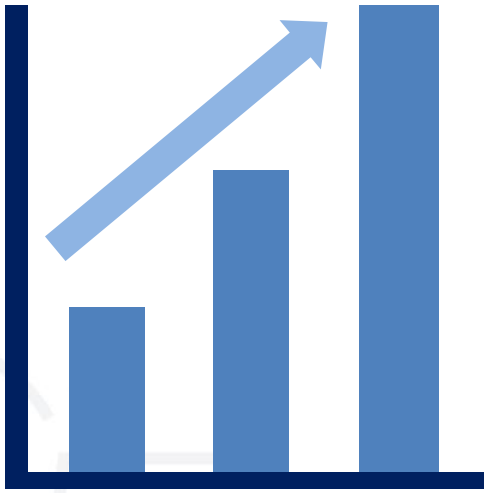
- World Cyber Threat

Terrifying Cybercrime Trend

Ref: www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

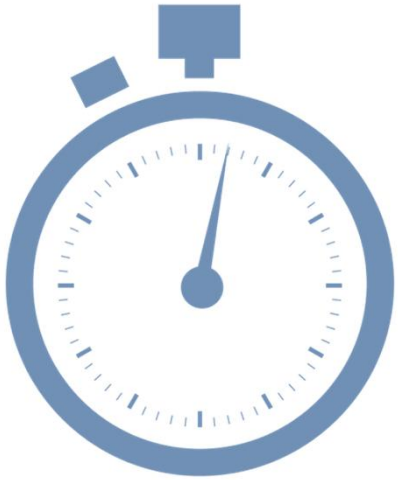
Data Breaches



67% Over 5 Years

Ref: Accenture's global survey

Ransomware



Every 14 seconds

$11.5 Billion by 2019

$20 Billion by 2021

Ref: 2019 Official Annual Cybercrime Report

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

146 Billion Records

Will be exposed in the next 5 Years

>1 million folders don't limit access

www.thesisstore.com

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Cyber Attack

Fastest Growing Crime in US

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

2019

Exposed 885 million Customer Info.

First American

2018

50 billion users compromised
(Largest breach in the History)

2018

Exposed 500 million user accounts

JW MARRIOTT HOTELS & RESORTS

2017

Exposed 3 Billion user accounts

2017

145.5 million customers affected

EQUIFAX

https://www.forbes.com

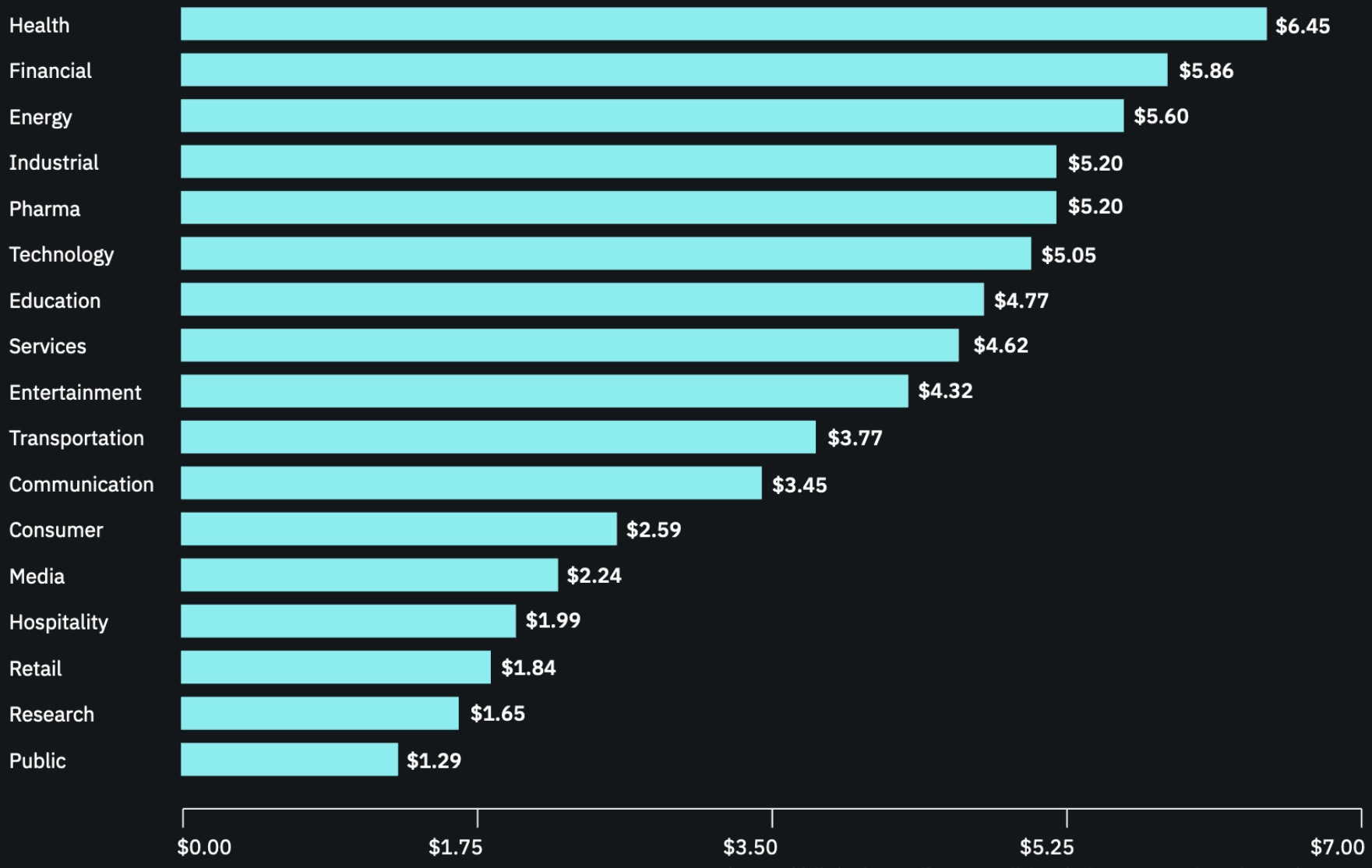
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Figure 10:

Average total cost of a data breach by industry

Measured in US$ millions



https://digitalguardian.com/blog/whats-cost-data-breach-2019

US Govt Says Iran's Cyberattacks Can Disrupt Critical Infrastructure

By Sergiu Gatlan

January 6, 2020 11:34 AM 0

The U.S. Department of Homeland Security (DHS) warned in a terrorism threat alert issued through the National Terrorism Advisory System (NTAS) that potential cyberattacks carried out by Iranian-backed actors against the U.S. have the potential to disrupt critical infrastructure.

The NTAS bulletin was issued to describe the current threat landscape following a lethal strike carried

abc NEWS

Experts urge vigilance for cyber systems amid escalation with Iran

They warn it's vital to sure up defenses when a cyberattack could be imminent.

By **Luke Barr** and **Jack Date**
7 January 2020, 03:36 • 8 min read

Cyber Attack is "Imminent"

CNN BUSINESS Markets Tech Media Success Perspectives Videos Edition

Home › News › Security › US Govt Says Iran's Cyberattacks Can Disrupt Critical Infras

US Govt Says Iran's Cyberattacks Can Di
Infrastructure

By Sergiu Gatlan

The U.S. Department of Homeland Security (DHS) warned in National Terrorism Advisory System (NTAS) that potential cyberattacks carried out by Iranian-backed actors against the U.S. have the potential to disrupt critical infrastructure.

The NTAS bulletin was issued to describe the current threat landscape following a lethal strike carried

One way Iran could retaliate on the United States: Cyber attacks

By Shannon Liao, CNN Business
Updated 1601 GMT (0001 HKT) January 5, 2020

TOP STORIES

Nick Gordon, ex-boyfriend of Bobbi Kristina Brown, dies at 30

Retired Major General James Marks tells senator to 'just be quiet' after...

Recommended by Outbrain

MORE FROM CNN BUSINESS

Zero Risk
Zero Risk Do Not Exist

Information Security Domain

- Information Security
- Baldrige Cybersecurity Framework
- Enterprise Alignment

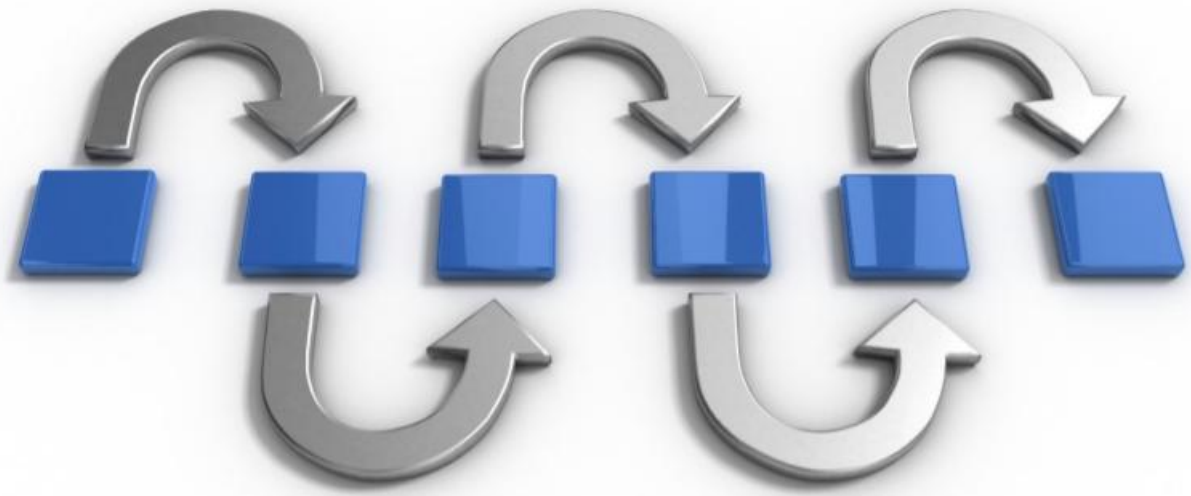
2020

Appropriate Security Levels

> Security is a process, not an end state.

25th THAILAND PRODUCTIVITY INSTITUTE

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA



Security | the process of maintaining an acceptable level of perceived risk

Ref: www.itu.int

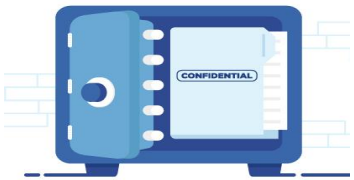
THAILAND PRODUCTIVITY INSTITUTE

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Information Security

3 Key Features

Confidentiality



Integrity

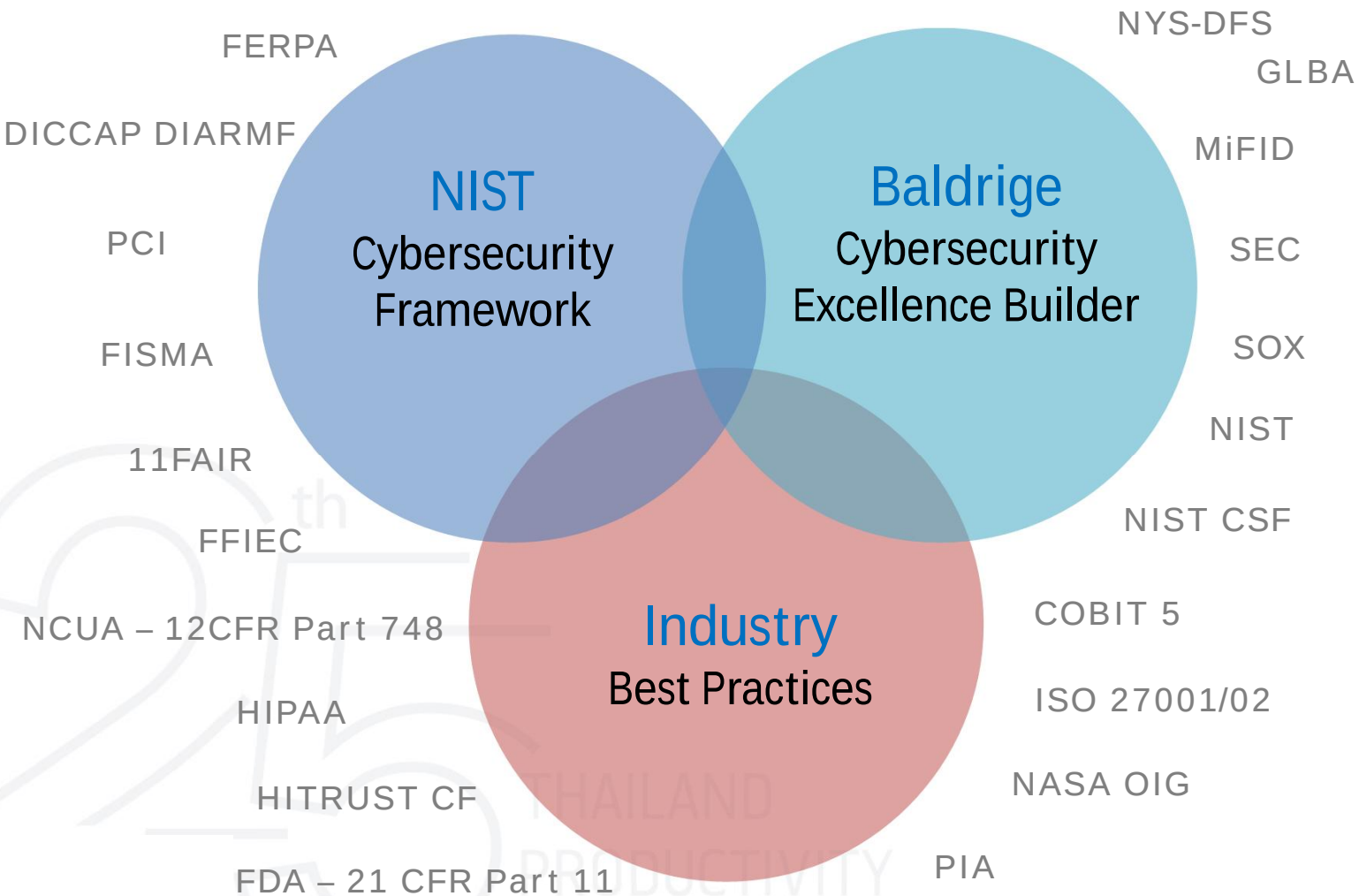
Availability

25th THAILAND PRODUCTIVITY INSTITUTE

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Ref: https://en.wikipedia.org/wiki/Information_security

WADING THROUGH THE CYBERSECURITY CHAOS

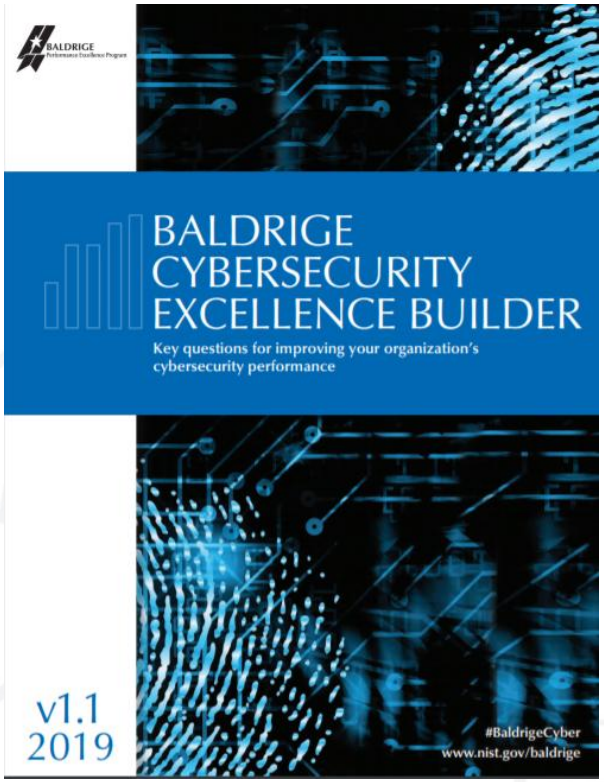


Ref:https://www.assured.enterprises/nist-baldrige-cybersecurity-guidelines/

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Baldrige

Cybersecurity Framework



Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

3 Common Factors

Information Security Risk Management

Assessment

1

Manage

2

Good Practices

3

THAILAND PRODUCTIVITY INSTITUTE

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

RISK Assessment

1

ISO/IEC 27002:2005

- Security policy,
- Organization of information security,
- Asset management,
- Human resources security,
- Physical and environmental security,
- Communications and operations management,
- Access control,
- Information systems acquisition, development and maintenance,
- Information security incident management,
- Business continuity management, and
- Regulatory compliance

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Ref: https://en.wikipedia.org/wiki/Information_security

RISK Assessment

2

ISO/IEC 27002:2005

- Identification of assets and estimating their value e.g., people, buildings, hardware, software, data (electronic, print, other), supplies
- Conduct a Threat assessment
- Conduct a Vulnerability assessment
  - Probability of being attacked
  - Evaluate policies, procedures, standards, training, physical security, quality control, technical security
- Calculate the impact that each threat would have on each asset
- Evaluate the effectiveness of the control measures
  - Cost effective protection without discernible loss of productivity

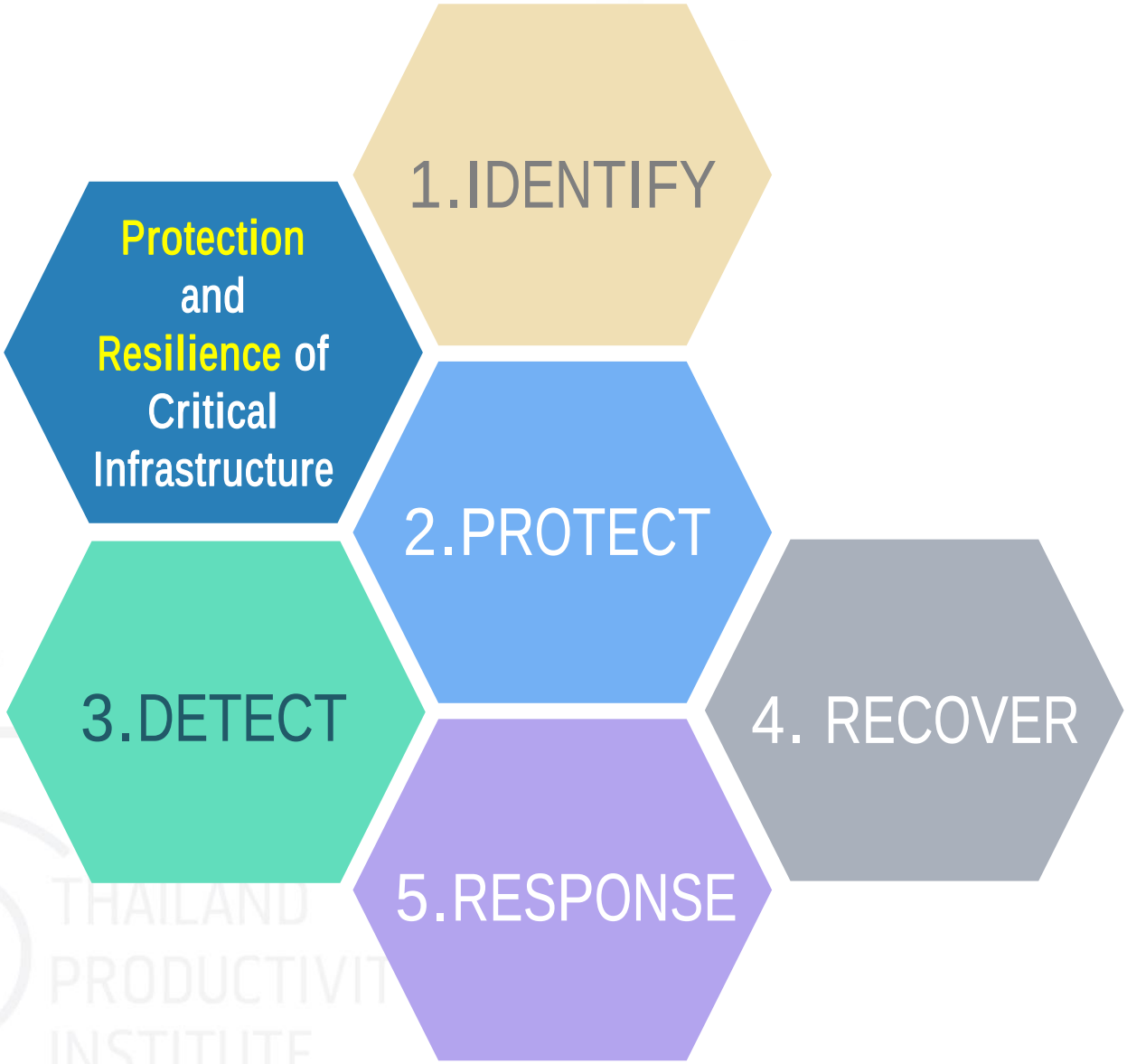
Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Ref: https://en.wikipedia.org/wiki/Information_security

RISK Assessment

2

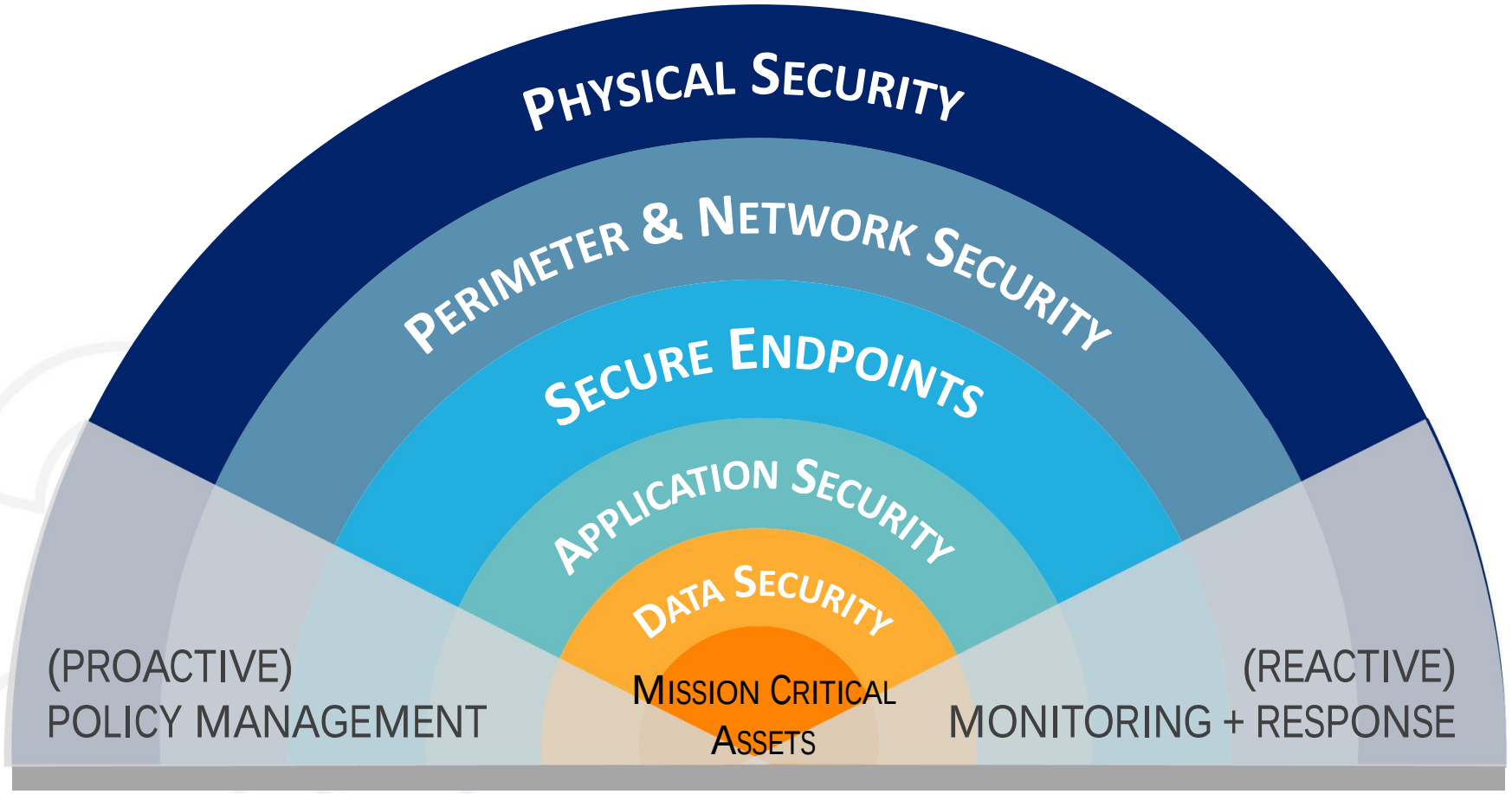
NIST Cyber Security Framework



Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

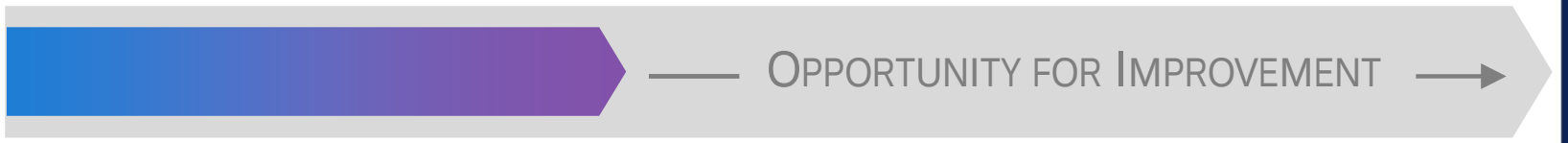
Ref: https://en.wikipedia.org/wiki/Information_security

Protecting Areas



Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

NIST Cybersecurity Framework (800-53)



5 Functions

21 Categories

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security & Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	

103 Sub-Categories

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

	Subcategory	Informativ
sset Management (ID.AM): The data, personnel, ices, systems, and facilities that enable the hieve business purposes are sistent with their relative and the	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-
	ID.AM-3: Organizational communication and data flows mapped	· **CCS CSC** 1 · **COBIT 5** DSS05.02
	ID	

CIS Controls - Center for Internet Security

COBIT: Control Objectives for Information and Related - ISACA

NIST Special Publication 800-53: “Security and Privacy Controls for Federal Information Systems and Organizations."

ISO/IEC 27001:2013 – Information technology –Information security management

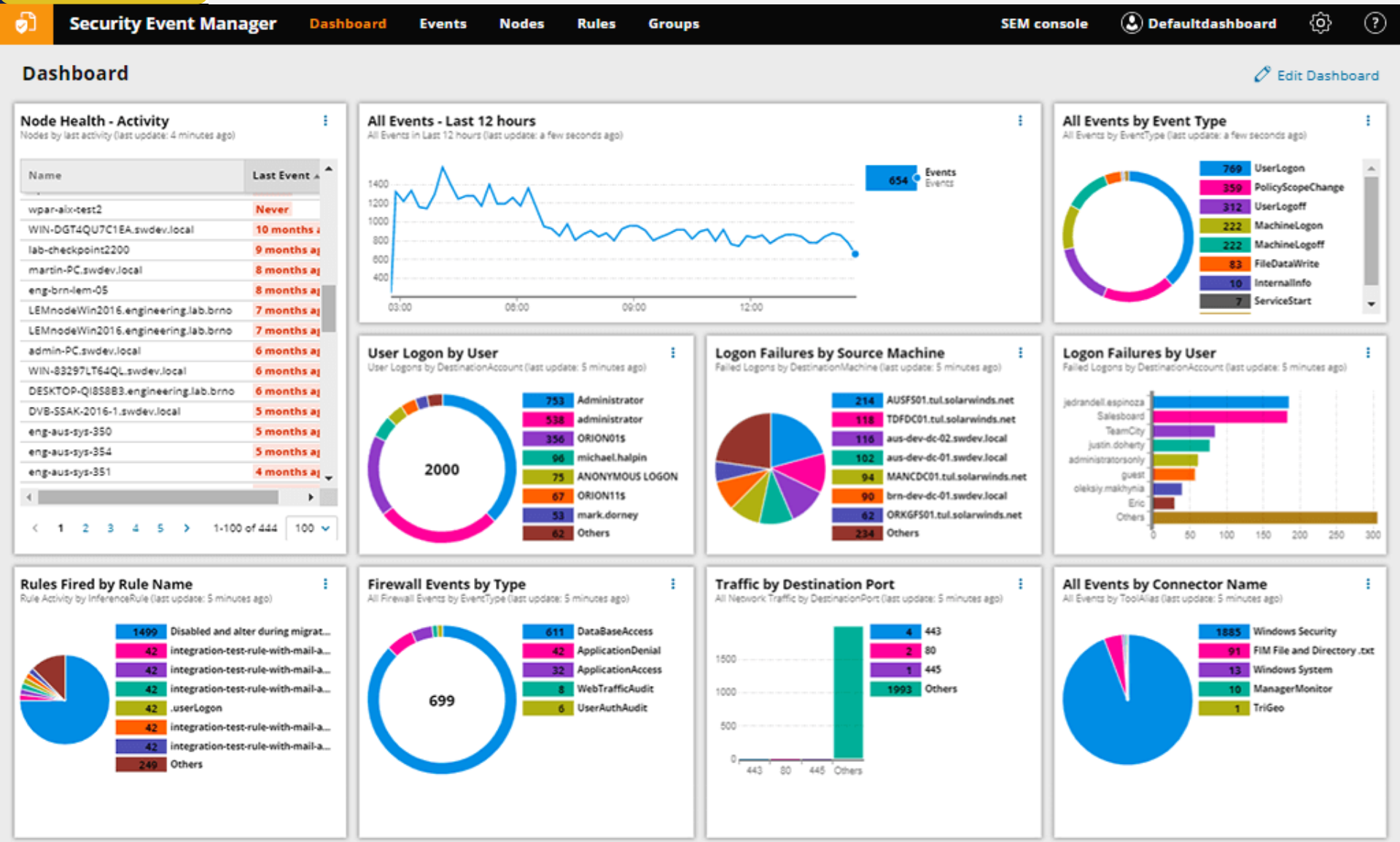
Assessment and Maturity

NIST CSF
PRODUCTIVITY INSTITUTE

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

DETECT

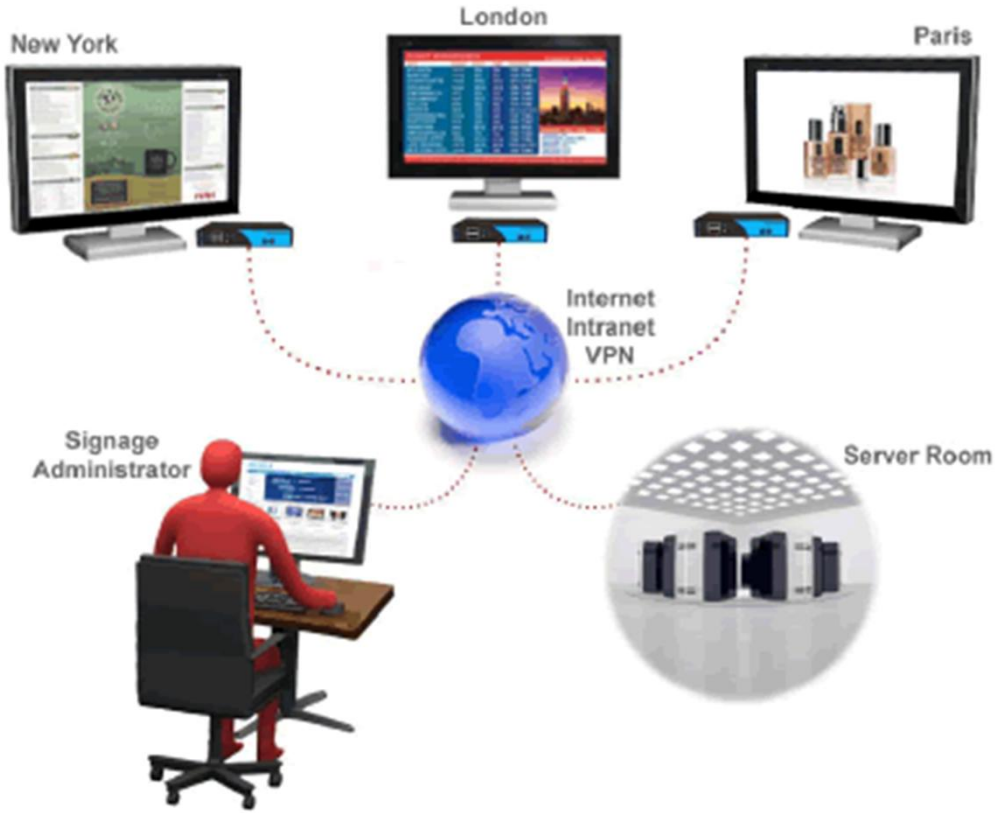
EXAMPLE OF HARDWARE DETECTION SYSTEM



Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

All Assets must be Evaluation & Protected

Enterprise Architecture is Highly Recommended for Mid-Large Enterprise



Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Good Practices

3

Network Security

Firewall, Network Intrusion Detection (IDS), Web Filtering, Virtual Private Networking (VPN), Cloud Security, 24x7 Monitoring

Governance

PCI-DSS 3.2, HIPAA, NACHA, SOC 1 & 2 Type II, National Institute of Standards & Technology (NIST, NIST 800), Computer Security Incident Response Team (CSIRT), Source code Scanning

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Good Practices

3

System Security

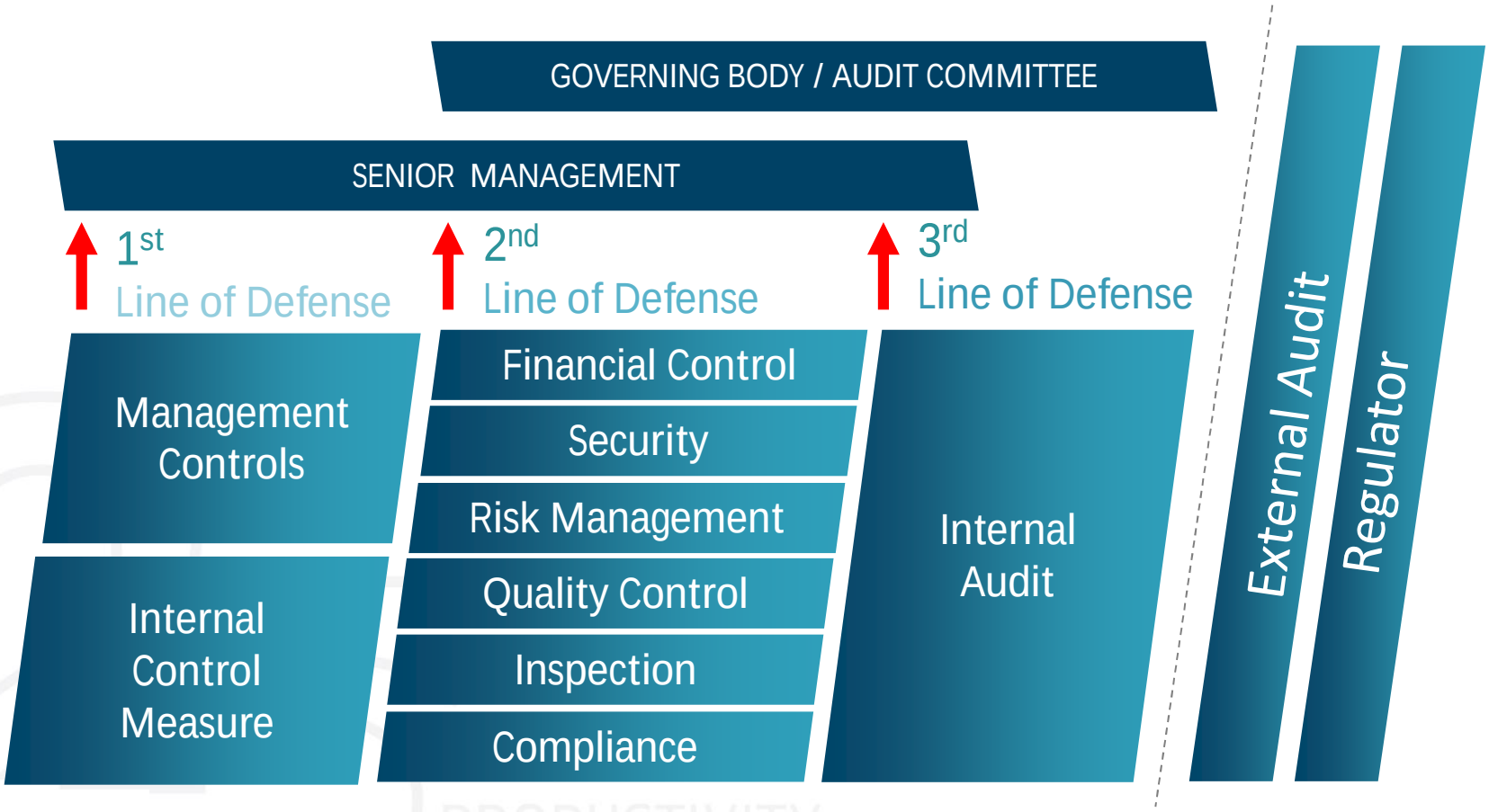
Patches, Anti-Virus, Malware, File Integrity Monitoring, Host based Intrusion Detection, Rogue Applications, Vulnerability Scanning

Data Protection

Data Loss Prevention (Endpoint, Storage & Network), Recovery Point Objective (RPO), Recovery Time Objective (RTO), Encryption, Tokenization,

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

IT GOVERNANCE MUST BE ESTABLISHED

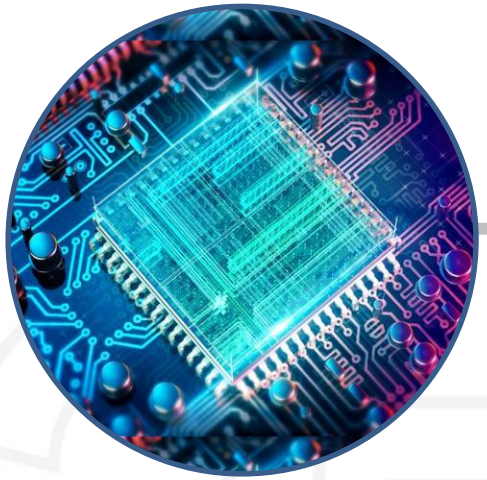


Recommend: ISO 38500 -> COBIT

Ref: https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/

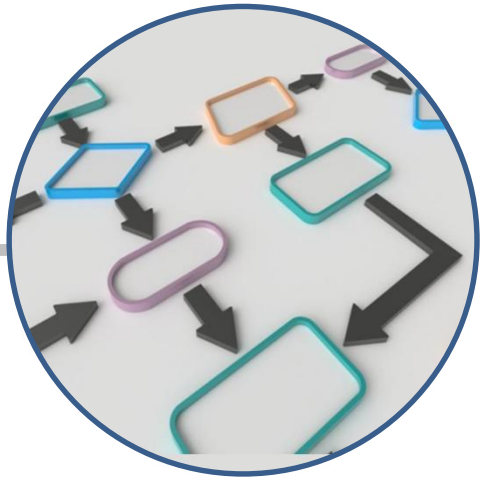
CYBER SECURITY

PEOPLE



TECHNOLOGY

PROCESS



THAILAND PRODUCTIVITY INSTITUTE
CYBER SECURITY

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

60%

attacks that occurred in companies were committed by people from within the organization.

Source: IBM

THAILAND PRODUCTIVITY INSTITUTE

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

IT- Business Strategy Alignment

Business Strategy

- Scope
- Goal
- Capabilities
- Governance

IT Strategy

- Scope
- Policies
- IT Capabilities
- Governance

Business Infrastructure

- Structure
- Process
- People + Skills

IT Infrastructure

- Backbone Communication Technologies
- Equipment Technologies

ENTERPRISE ARCHITECTURE IS HIGHLY RECOMMENDED

Copyright 2020 by Athisarn Wayuparb, Ph.D., CISA

Addendum

25th THAILAND PRODUCTIVITY INSTITUTE

YOUR CUSTOMERS' RIGHTS UNDER GDPR

RIGHT TO BE INFORMED

Be transparent in how you collect and process personal information and the purposes that you intend to use it for. Inform your customer of their rights and how to carry them out.

RIGHT OF ACCESS

Your customer has the right to access their data. You need to enable this either through business process or technical means.

RIGHT TO RECTIFICATION

Your customer has the right to correct information that they believe is inaccurate.

RIGHT TO ERASURE

You must provide your customer with the right to be forgotten, provided that your legitimate interest to hold such information does not override theirs.

RIGHT TO RESTRICTION OF PROCESSING

Your customer has the right to request that you stop processing their data.

RIGHT TO DATA PORTABILITY

You need to enable the machine and human-readable export of your customers' personal information.

RIGHT TO OBJECT

Your customer has the right to object to you using their data.

RIGHTS REGARDING AUTOMATED DECISION MAKING

Your customer has the right not to be subject to a decision based solely on automated processing, including profiling.

Violation Fine: 4% or 20 Million Euros

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

บทลงโทษมีทั้งโทษอาญา ทางแพ่ง และทางปกครอง หากมีการฝ่าฝืนมีโทษจำคุกตั้งแต่ 6 เดือนถึง 1 ปี และโทษปรับทางปกครองตั้งแต่ 5 แสนบาท ถึง 5 ล้านบาท

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

มาตรา ๘๑ ในกรณีที่ผู้กระทาความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล

ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

THAILAND PRODUCTIVITY INSTITUTE

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

มาตรา 23 ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้

(1) วัตถุประสงค์ของการเก็บรวบรวม (Purpose)

(2) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม (What & How long?)

(3) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย (Data Processors)

(4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ ในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

**มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

25th THAILAND PRODUCTIVITY INSTITUTE

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

**มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

THAILAND PRODUCTIVITY INSTITUTE

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

บทลงโทษ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล - มีโทษทางอาญาและทางปกครอง

มาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกิน**ห้าแสนบาท หรือทั้งจำทั้งปรับ**

- โทษปรับทางปกครองไม่เกินห้าล้านบาท

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษ**จำคุกไม่เกินหนึ่งปี** หรือ**ปรับไม่เกินหนึ่งล้านบาท** หรือ**ทั้งจำทั้งปรับ**

THAILAND PRODUCTIVITY INSTITUTE

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

Data Protection by Design

- แต่งตั้ง Working Group ในองค์กร
- แต่งตั้ง DPO
- กำหนดประเภทของข้อมูลและมาตรการในการจัดการข้อมูล
- ทบทวน Data Protection Policy
- ควรทบทวนการบริหารจัดการ Personal Data และหลักเกณฑ์การให้ความยินยอม

–ทบทวนกระบวนการเข้าถึงแก้ไขลบข้อมูลเมื่อได้รับการร้องขอ

THAILAND PRODUCTIVITY INSTITUTE

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
Data Protection by Design

- ทบทวน life-cycleของการเก็บรักษาและทำลายข้อมูล
- จัดเตรียมข้อปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
- ทบทวนมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่มีการโอนย้ายข้อมูลไป
- Documentมาตราการรักษาความมั่นคงปลอดภัยกับข้อมูลส่วนบุคคล
- จัดอบรมให้กับบุคลากรพนักงานและเจ้าหน้าที่
- พัฒนาทักษะและกระบวนการตรวจสอบประเมิน (Audit)
- Privacy by Design และSecurity by Design
- พัฒนากระบวนการแจ้งเตือน(Breach Notification)
- ได้รับงบประมาณและการสนับสนุนจากผู้บริหาร

THANK YOU

By Athisarn Wayuparb, Ph.D., CISA

089-109-7113

Line: athisarn

25th THAILAND PRODUCTIVITY INSTITUTE