PERSONAL DATA PROTECTION, DATA SECURITY AND PRIVACY COMPLIANCE

BHUME BHUMIRATANA PH.D.

AGENDA

- Recap of the law & rights granted
- How Organization should adapt
- Data Security framework and compliance with the law

MINI PDPA SUMMARY

PERSONAL DATA PROTECTION ACT

- What?
  - Law governing the proper and lawful processing of personal data in Thailand.
  - Define sets of rights for Thai people in regards to their data and how others can use them.
- When?
  - Effective May 28, 2020
- Who?
  - Every businesses in Thailand that collects/use/distribute personal data of Thai people are regulated under this law.

KEY CONCEPTS

- Personal Data
- Sensitive Data
- Data Subject
- Data Controller
- Data Processor

DATA THAT HAS ALREADY BE COLLECTED

- Section 95: Personal Information collected prior to the law enactment – Data Controller can continue to use them as per original intent and usage.
  - Data Controller must allow for individual to request revocation of consent
  - Data Controller must inform via notification to all individuals so that they know they can revoke their consent.
  - Any new usage requires new consent even on the same data.
  - This exception is only for collecting and using data, not sharing.

LAWFUL DATA PROCESSING

- **Personal Data**
  - **Consent**
  - Research (Historical, Statistical, or other research purpose)
  - Vital Interest (Health and Safety)
  - **Contractual Obligation**
  - Public Task (Public Authority related activities)
  - **Legal Obligation**
  - **Legitimate Interest (Must balance the controller's interest with the data subject rights)**
- Example:
  - Name, Address, Phone, Customer ID
  - Age, Gender, Height
  - Username, Password
  - IP Address, Mac Address

- **Sensitive Data**
  - **Explicit Consent**
  - Vital Interest (Health and Safety)
  - Social Protection & Non-Profit
  - Manifestly made public (with data subject consent)
  - Legal claim
  - Preventive or Occupational Medicine practice
  - Public Health
  - Healthcare and social care system
  - Archiving, Scientific or Historical Research
  - Substantial Public Interest
- Example:
  - Race, Ethnicity
  - Religious believe, Gender orientation
  - Medical History, Criminal History

DATA SUBJECT RIGHTS

1. Right to informed consent
2. Right to withdraw consent
3. Right of Access to Personal data
4. Machine Readability & Data Portability
5. Right to Object
6. Right to Erasure
7. Right to Restrict Processing
8. Right Rectification

DATA PROTECTION OFFICERS

- Data Controller & Processor must appoint Data Protection Officer IF
  - Government organization are DC or DP
  - Organization store and process large amount of personal data (DPB decides)
  - Primary activity of the organization is to collect, use and distribute data.
- Conglomerates can share DPO.
- You may outsource DPO.
- DPO responsibilities:
  - Advise organization on consent, collection, use, distribution, and protection of data in accordance with this law.
  - Audit/control organization including its employees to obey the law
  - Liaison with DP office when there are issues
  - Protect personal data that it may come across as part of working with DP Office

CIVIL PENALTIES AND RENUMERATION

- DC/DP that disobey the law resulting in damages to DO must pay renumeration fees to DO, whether or not that mistake is by error or intended. Except DC/DP can prove that:
  - The problem is unavoidable/beyond reasonable to prevent or if partially caused by mistake on the DO side.
  - Or if the damage result from obeying DPB order or other laws.
- Renumeration must include all cost occur that DO may have to spend to recover from damage or prevent further damages.
- Court may requires that DC/DP pays additional damage fees to DO, but no more than twice the total real damage caused to DO.
  - DO can file to get renumeration within 3 years after DO has been notified of problems, or within 10 years of the breach.

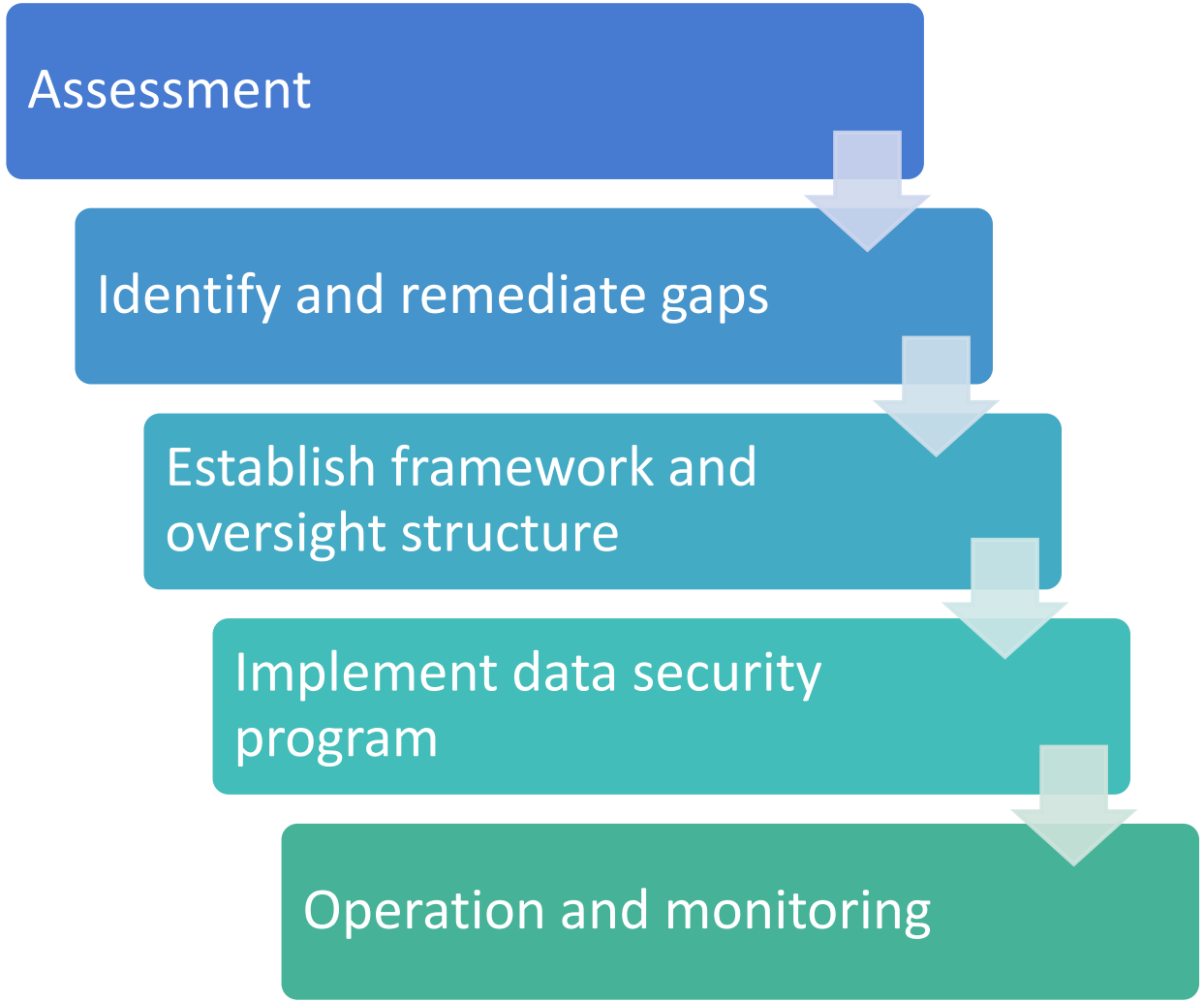
CRIMINAL PENALTIES

- (Section 79) Any DC/DP that collect data without consent (section 27), or send sensitive data (section 26) overseas without complying with data protection standard requirement (section 28) which “may” result in damages/reputation loss/defamatory/shame are subject to 6 months in jail or 500k baht fine.
  - If with intent to cause harm, 1 year jail and 1m baht fine
- (Section 80) Any government officers or DPO comes to access others personal data as part of activities in this law, and release it to others, are subject to 6 months jail or 500k baht fine
- (Section 81) If Organization violate the law, then it’s the fault of whoever order cause the breach/damage or whosever responsibility is omitted.

ADMINISTRATIVE PENALTIES

- DC/DP that
  - collect data without notifying DO of purpose of CUD, rights, etc… (Section 23)
  - Does not provide prompt access to personal data to DO (section 30 clause 4)
  - Does not log all access/processing of personal data as required (Section 39)
  - Does not appoint DPO, or DPO does not do its duty (Section 41,42)
  - Does not ask for explicit consent or does not notify of rights impact for revocation of consent of DO (Section 19 clause 6)
- Punishable by up to 1m baht fine
- All sort of other administrative fine for disobeying various sections for up to 3m or 5m baht fine per violation.

PATH TO WARD DATA PROTECTION COMPLIANCE



PREPARATION ACTIONS: TODO TODAY!

Data Discovery & Gap Analysis	• Identify and classify all personal data in the organization • Which area/activities are already in compliance?
Inventorize and identify how data flows in your organization	• Draw a data flow map • Identify how and where data enters/exit and are used
Create data protection impact assessment (DPIA) framework	• Identify data protection risk framework for your organization future evolution/change to process/products/services
Data Protection related contracts and forms	• Review all consent forms and contracts • Requires dedicated legal services expertise
Create data breach monitoring and response program	• Takes time and investment in People, Process, Technology
Data Protection Officer	• Find and appoint/promote/hire DPO

DATA SECURITY REQUIREMENT IN THE LAW

Data controller must employ security standard/process to protect personal data that it holds or controls

Including controlling distribution and destruction of the data

Data controller must report data breach to the committee in 72 hours (and if severe breach, must offer remediation process/method

Data controller and processor can store and process data overseas

But service provider must have comparable data security and privacy standard as Thailand

The Privacy Committee will define standards

- None yet, so we'll talk about what's likely and what's international today

WHAT DOES THIS MEAN FOR US?

Data security standards, policy, process, and procedures must be in placed by mid 2020

Data Security Framework

Information System Security Framework

Must have capability to detect breach, then respond and report them to the authority

Cybersecurity Framework

Find and appoint Data Protection Officer

Cross border data transfer policy

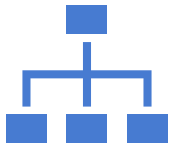
TOPICS TO DISCUSS

- We will discuss data security as element of the following:
  - DPO roles and responsibilities
  - Information Security Framework
  - Personal Information Management Framework
  - Cybersecurity Framework
  - Cloud security Framework
- What to do when breach occur?
  - Because you can’t be sure it won’t happen, you need to be ready.

DATA PROTECTION OFFICERS ROLES

- **Key** person who understand your organization data processing activities and understand key stakeholders related to data
- Informing and advising the organizations and its employees of the data protection law and obligations
- Manage transformation of process toward data privacy framework compliance
- Review/Monitor compliance with the data protection law
- Review and monitor DPIA programs effectiveness and assist in the conduct of DPIA
- Educate and train staff on data security and data protection so that organization remains in compliance
- Serving as contact point for external parties on data protection related activities

DATA PROTECTION OFFICER IN AN ORGANIZATION



He/She should be independent and without pressure from other roles in the organization

Should be able to investigate and find issues and advise effectively

No conflict of interest with the rest of organization management

E.g. don’t appoint CFO, CMO, CPO, COO, CIO, CEO as DPO… they have a type of objective in mind that may contradict with the goal of DPO. So who should DPO report? Directly possibly Chief Compliance Officer, or the board for public companies/organizations

DPO QUALIFICATIONS

- Understand the law, the process, and the technical measures
  - Does not need to be lawyer, but must understand the law
  - Does not need to be IT person, but must have enough technical knowledge and data security knowledge

INFORMATION SECURITY FRAMEWORK

There are two primary framework/systems

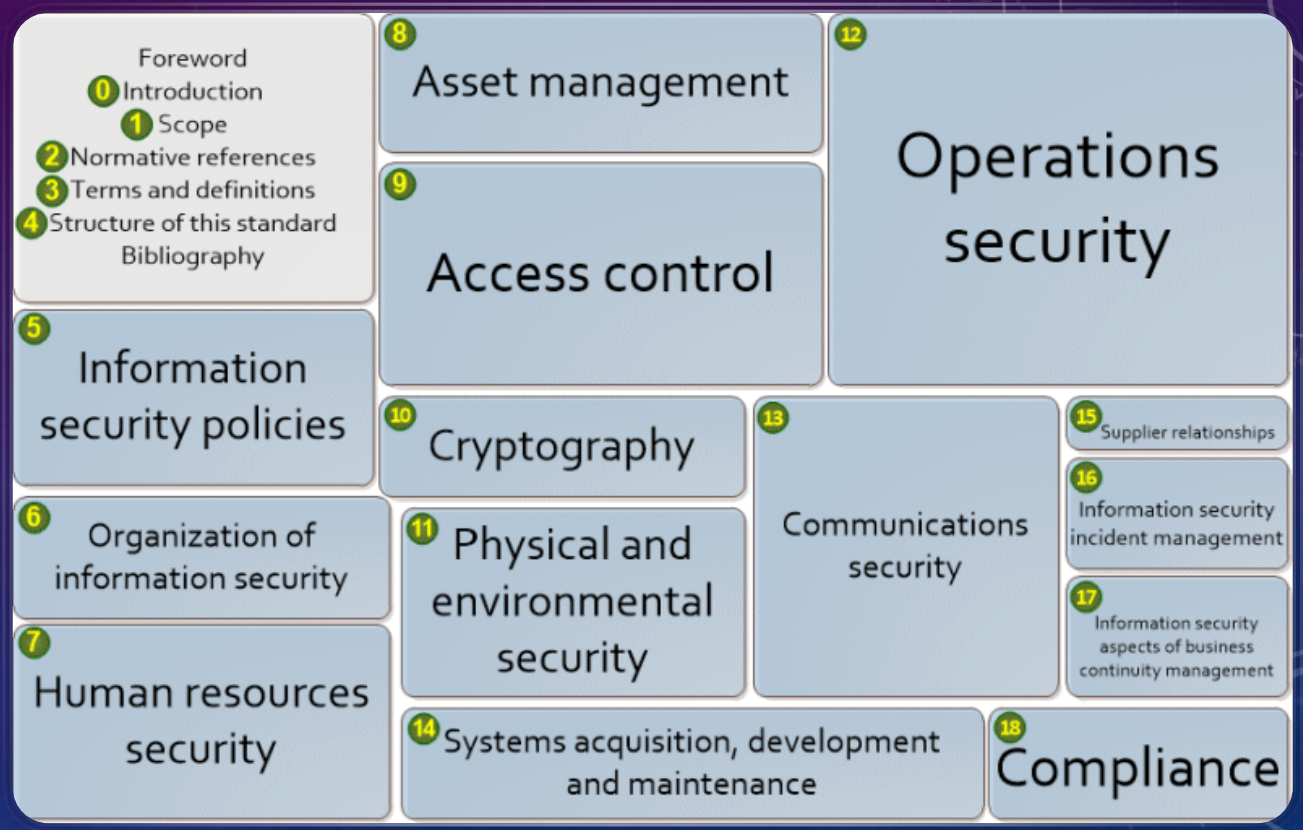
ISO 27001:2013 – Information Security Management System (ISMS)

ISO 27701:2019– Personal Information Management Systems (PIMS)

The law doesn’t require that you are certified, and the later announcement likely won’t. But these framework give us a good guidance on what are the things we need to do

ISO 27K:2013 STANDARD

- 35+ security objectives
- 114+ security controls
- Drawback:
  - Commercial/Proprietary standard (not free)
  - Expensive
  - Too process oriented
  - Does not actually ensure security, just ensure you have thought of all of these things and document them.
- Incomplete, does not cover privacy adequately



https://www.iso27001security.com/html/27002.html

WHERE IN ISO27K THAT IS RELATED

Risk Assessment

Data Protection Impact Assessment fits well within this part of ISO

Asset Management

A.8 – Organization has to identify and document the use of information asset, Personal Data is among them

Compliance

ISO requires legal, regulatory, and contractual risk compliance process, add PDPA as another law/regulation

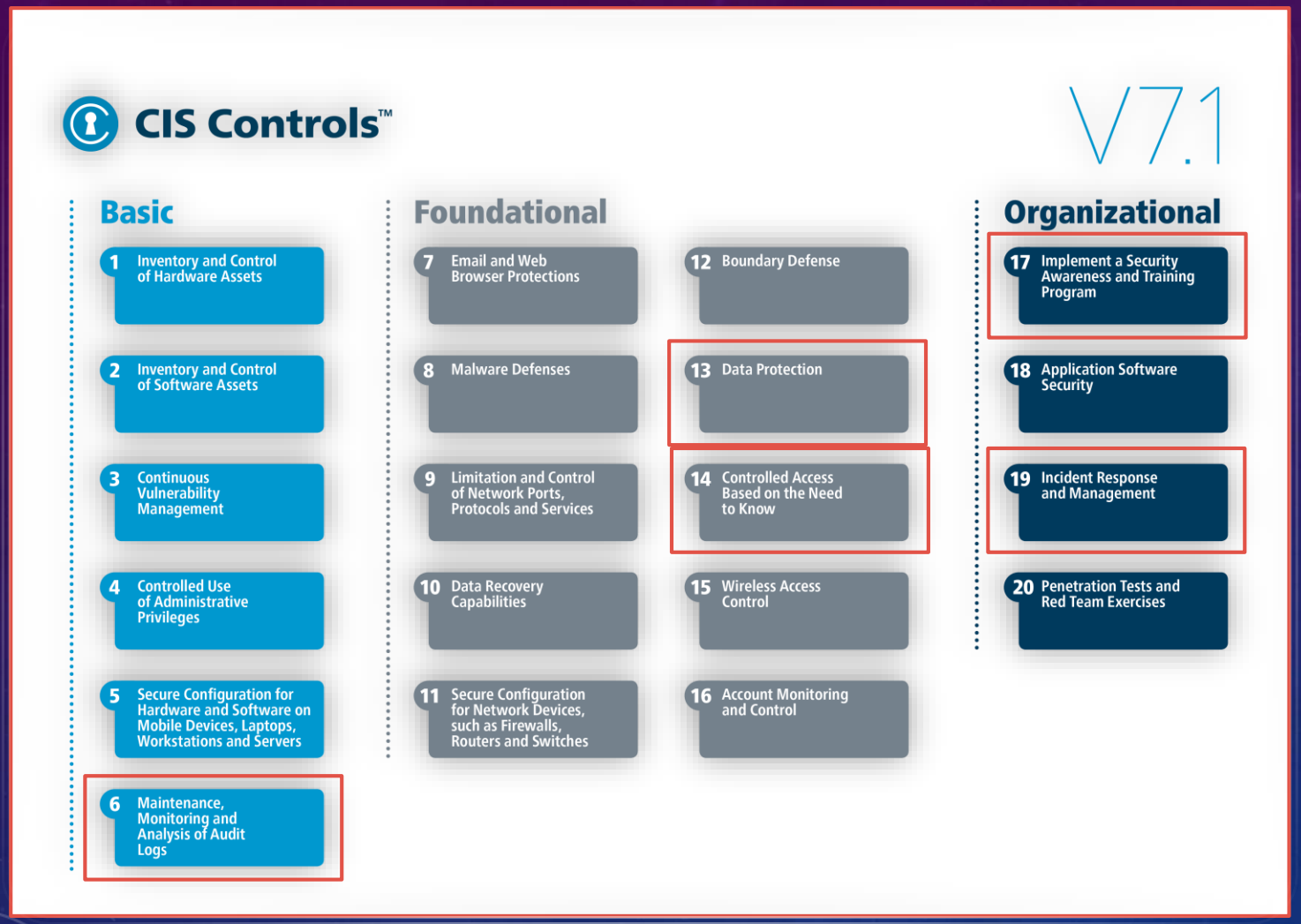
A.18.1.4 -- Privacy and protection of personally identifiable information – already exist in ISO 27k, give it more priority after the law is passed

Supplier Relationship

A.15 – Information security in supplier relationship – Will help ensuring that data transfer to other organization, Controller or Processor, remain compliance

A.16 Information Security Incident Management

ALTERNATIVE: CIS SECURITY CONTROL



- More technical
- We can't go over them all, so lets pick a few samples

https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cis-controls/

CIS 6: MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS

- Utilize Three Synchronized Time Sources
- Activate Audit Logging
- Enable Detailed Logging
- Ensure Adequate Storage for Logs
- Central Log Management
- Deploy SIEM or Log Analytic Tools
- Regularly Review Logs
- Regularly Tune SIEM

CIS 13: DATA PROTECTION

- Maintain an inventory of sensitive information
- Remove sensitive data or systems not regularly accessed by organization
- Monitor and block unauthorized network traffic
- Only allow access to authorized cloud storage or email providers
- Monitor and detect any unauthorized use of encryption
- Encrypt mobile device data
- Manage USB devices
- Manage System’s external removable media’s read/write configurations
- Encrypt data on USB storage device

CIS 14: CONTROLLED ACCESS BASED ON THE NEED TO KNOW

- Segment the Network based on Sensitivity
- Enable Firewall Filtering Between VLANs
- Disable Workstation-to-Workstation Communication
- Encrypt All Sensitive Information in Transit
- Utilize an active Discovery Tool to Identify Sensitive Data
- Protect Information Through Access Control Lists
- Enforce Access Control to Data Through Automated Tools
- Encrypt Sensitive Information at Rest
- Enforce Detail Logging for Access or Changes to Sensitive Data

CIS 17: IMPLEMENT A SECURITY AWARENESS AND TRAINING PROGRAM

- Perform a Skill Gap Analysis
- Deliver Training to Fill the Skills Gap
- Implement a Security Awareness Program
- Update Awareness Content Frequently
- Train Workforce on Secure Authentication
- Train Workforce on Identifying Social Engineering Attacks
- Train Workforce on Sensitive Data Handling
- Train Workforce on Causes of Unintentional Data Exposure
- Train Workforce Members on Identifying and Reporting Incidents

CIS 19: INCIDENT RESPONSE AND MANAGEMENT

- Document Incident Response Procedures
- Assign Job Titles and Duties for Incident Response
- Designate Management Personnel to Support Incident Handling
- Devise Organization-wide Standards for Reporting Incidents
- Maintain Contact Information for Reporting Security Incidents
- Publish Information Regarding Reporting Computer Anomalies and Incidents
- Conduct Periodic Incident Scenario Sessions for Personnel
- Create Incident Scoring and Prioritization Schema

OTHER NOTABLE CIS CONTROLS

CIS 1: INVENTORY & CONTROL OF HARDWARE ASSETS

CIS 2: INVENTORY & CONTROL OF SOFTWARE ASSETS

CIS 7: EMAIL & WEB BROWSER PROTECTION

CIS 8: MALWARE DEFENSES

PERSONAL INFORMATION MANAGEMENT SYSTEMS (PIMS)

- BS 10012 (Recently replaced by ISO 27701)
  - New framework created specifically for GDPR and other Data Protection related issues
- Not complete – focus only on privacy related topics
  - You need ISO or other framework for security aspect
- Advantage:
  - Help identify risk to personal information

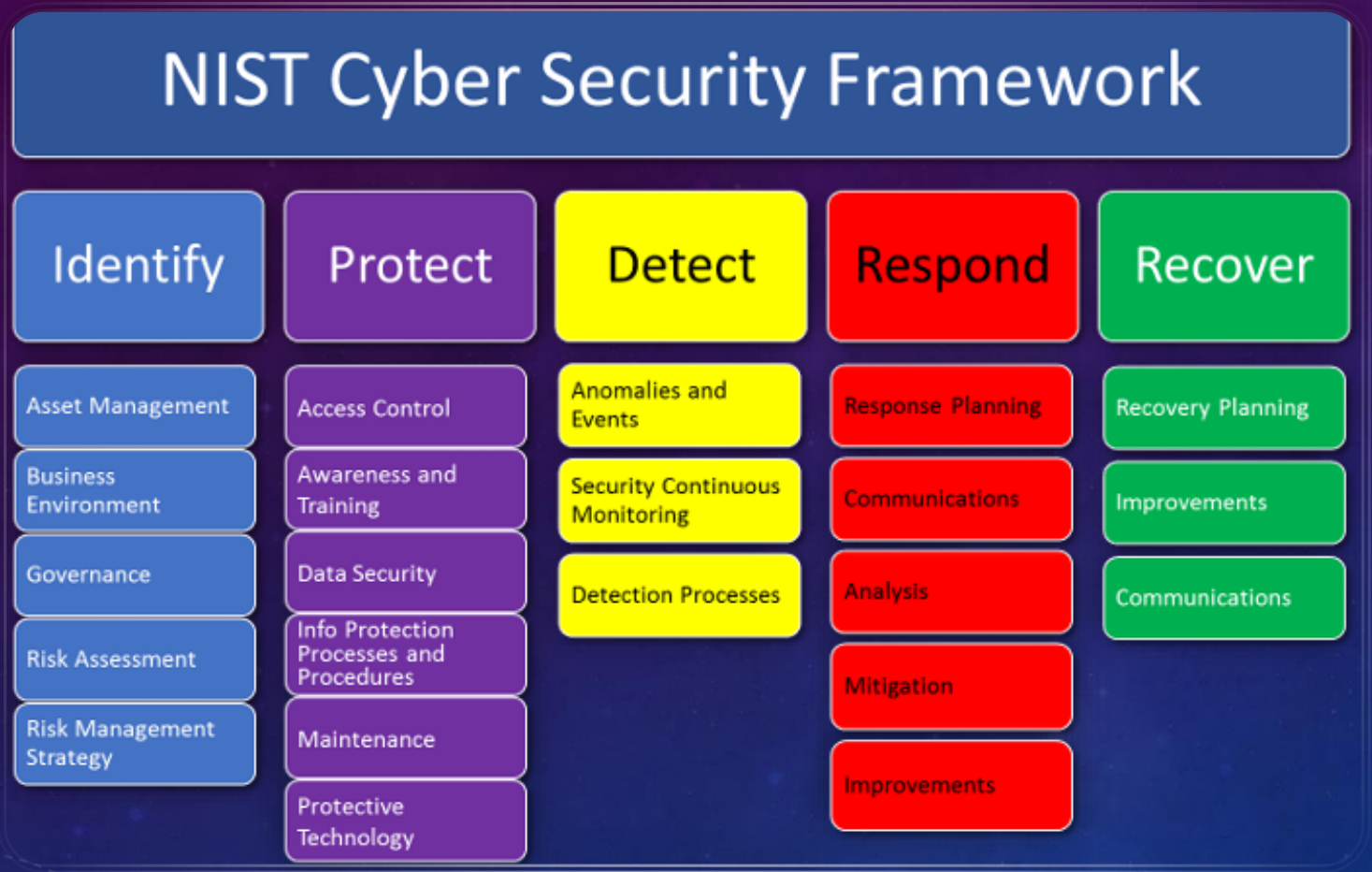
PIMS COVERAGE

- Management roles and responsibility
- DPO responsibility and tasks breakdown
- Framework for personal/sensitive data classification
- Framework for organization policy and process for collection, use, and share of data such as
  - Data collection policy, Privacy notice record and timing, accessibilities, use of third parties, consent to new purpose, grounds for collecting data, adequate and not excessive use of data, rights, security, security assessment, etc…
    - Basically a full list of things an organization has to do to be compliant, you'll have to fill in the detail yourself, but you start with a long list so you don't have to spend time looking.

CYBERSECURITY FRAMEWORK

NIST CYBERSECURITY FRAMEWORK

NIST CYBERSECURITY FRAMEWORK



- Cybersecurity framework that focuses on 5 phases
- Highlight for Data Protection Compliance:
  - Detect
  - Response

NIST SP 800-53 SECURITY CONTROLS

- Open and Freely accessible
- Modern and vendor neutral
- Update frequently (on Rev 5 already)

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

NIST CONTROLS HIGHLIGHT

- Introduce Privacy Control as a dedicated matter
  - The only framework currently that covers both security and privacy control
- Very detailed list of controls
  - Access Control: 23 groups 120+ controls
  - Awareness and Training: 4 groups 12 controls
  - Audit and Accountability: 16 groups 60 controls
  - Assessment, Authorization and Monitoring: 8 groups 27 controls
  - Configuration Management: 12 groups 51 controls
  - Contingency Planning: 12 groups 49 controls
  - Identification and Authentication: 12 groups 53 controls
  - Individual Participation: 6 groups 11 controls
  - Incident Response: 10 groups 36 controls
  - Maintenance: 6 groups 26 controls
  - Media Protection: 8 groups 21 controls
  - Privacy Authorization: 4 groups 6 controls
  - Physical and Environmental Protection: 21 groups 51 controls
  - Planning: 10 groups 12 controls
  - Program Management: 32 groups 38 controls
  - Personnel Security: 8 groups 16 controls
  - Risk Assessment: 8 groups 17 controls
  - System and Service Acquisition: 20 groups 86 controls
  - System and Communication Protection: 40+ groups 110+ controls
  - System and Information Integrity: 19 groups 90+ controls
  - **Total: 270+ groups 860+ controls**

CLOUD SECURITY FRAMEWORK

- Cloud Security Alliance has a GDPR resource page and working group
  - https://gdpr.cloudsecurityalliance.org/
  - Group of Cloud Service Provider joined together to pledge compliance to GDPR
  - Should be applicable to Thai PDPA law with some small caveats
- CSA Code of Conducts for GDPR Compliance
  - If you're cloud service provider or CSP (of any type including SaaS), the document provide a good list of activities you have to do to help your clients be GDPR (and possibly TPDPA) compliance
  - If you're cloud customer, this give you a list of things you need to put in the contract with CSP to be compliant with the laws

BREACH AND RESPONSE

BREACH EXAMPLE

- There are many more
- Equifax
- SingHealth
- Etc…

British Airways faces $230 million fine. It would be a record under Europe's tough data privacy law

By Charles Riley, CNN Business

Updated 1500 GMT (2300 HKT) July 8, 2019

London (CNN Business) – British Airways faces a record $230 million fine after a website failure compromised the personal details of roughly 500,000 customers.

It would be the largest penalty yet under a tough privacy rule known as the General Data Protection Regulation, which came into force last year in the European Union.

The UK Information Commissioner's Office said that weak security allowed user traffic to be diverted from the British Airways website to a fraudulent page starting in June 2018. The regulator said the company will have a chance to contest the proposed fine.

Related Article: Facebook investigated in Ireland over mishandled passwords

Attackers were able to harvest customer details including log ins, payment cards, and travel booking details, according to the regulator. The airline disclose the incident in September 2018.

The £183.4 million ($230 million) fine is roughly 1.5% o British Airways' annual revenue. The carrier, which is owned by IAG (ICAGY), said it would fight the penalty.

"We are surprised and disappointed in this initial finding," British Airways CEO Alex Cruz said in a statement.

"British Airways responded quickly to a criminal act to steal customers' data. We have found no evidence of fraud [or] fraudulent activity on accounts linked to the theft," he added.

TYPICAL CAUSE OF BREACHES

WEAK AND STOLEN CREDENTIALS

APPLICATION AND SYSTEM VULNERABILITY

MALWARE AND RANSOMWARE

EMPLOYEE NEGLIGENCE

INSIDER THREAT

HOW TO PREVENT BREACHES

- Implement strong and comprehensive cybersecurity program
- Train your staff
- Implement and operate security technologies
- And just in case breach start to happen
  - Implement security monitoring and response program

BREACH RESPONSE GUIDELINE

- Distinguish typical cybersecurity breach vs. Personal Data Breach
  - With TPDPA you only need to report personal data breach (cybersecurity breach report to CSA if you're CII)
- Details on how to report is TBD by the PDPA committee
  - But we know everyone must report within 72 hours
  - GDPR does make exception: IF encrypted data is stolen but the key is not, then no Report is needed.
  - GDPR requires reporting for all breach that could impact "risk to rights and freedom"
  - GDPR requires all breach to be recorded (though not all need to be reported)

SUMMARY

- Security is about risk management, not about compliance
  - Compliance is a type of risk
- Don’t let the perfect be the enemy of the good
  - If you are in a hurry with limited resource, but willing to learn start with ISO 27701:2019 it covers GDPR without other fluff
    - Then expand with ISO or CIS or **NIST** for security aspect enhancement
  - If you have the resource and organization is not so rigid with lots of processes, study GDPR and go straight for NIST cybersecurity framework and control
  - For very large organization, ISO27k is the easiest to find consulting to help adopt, if you do not have the resource/manpower to study and do it yourself
    - But consultant only help you get started, you still need to develop your own team

THANK YOU