RSAConference2017
Singapore | 26–28 July | Marina Bay Sands

POWER OF OPPORTUNITY

SESSION ID: PRG-F01

Governing Without Clear Standards: Lessons Learned from the Trenches

Ronald Raether
Partner
Troutman Sanders LLC
@privacyraether

Standards?

STANDARD + ACTION ‡ COMPLIANCE

- While standard setting organizations work to provide guidance, the variables are too numerous such that a single, universal standard is not possible.
- What is emerging is not a standard, but instead a well developed process.
- *See "Data Security Breaches: Defining Measures Appropriate Under the Circumstances"* (Dec.2007) https://www.troutmansanders.com/files/Uploads/Documents/RIR_DataSecurityBreaches.pdf

What is our goal?

Maximize information security

- without compromising business functionality
- without compromising privacy

How will we find success?

Through proper Data Governance

Data Governance

- Finding a balance between:
  - Technology
  - Operations
  - Data use and needs
  - Security
  - Authority
  - Accountability
  - Privacy

Tensions in Data Governance

Security		Privacy
Obligation to provide security for personal information and other confidential material		Rules for processing Personal Information (and analogs outside the EU)
Quick response to attacks and changing strategies	vs.	Requirements to obtain user consent and register applications/processing
Need to retain log and traffic data for analysis		Restrictions on data retention
Need to consolidate data for analysis		Export limitations on "personal data," banking information and "state secrets"

How to resolve these tensions?

IT Operational Business Needs

Expense concerns
Obligation to keep systems available/operational SLAs
Customer experience Time to market
Technology needs Retain everything
Competitive pressures Internal Deadlines for Project Implementations

How to resolve these tensions – through standards?

- Government
  - Legislative
  - Regulatory
- Industry
- Trade groups/Organizations

Well Known “Standards”

- National Institute of Standards and Technology (NIST)
- Cloud Security Alliance (CSA)
- Payment Card Industry (PCI)
- General Data Protection Regulation (GDPR)

https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

What Standard to Follow?

Argentina PDPA
BIR 2012
Canadian Privacy Laws
CCSL (IRAP)
CDSA
China DJCP
China GB 18030
China TRUCS
CJIS
CS Mark (Gold)
CSA STAR Attestation
CSA STAR Certification
CSA STAR Self-Assessment
DFARS

DoD
EN 301 549
ENISA IAF
EU Model Clauses
EU-U.S. Privacy Shield
FACT
FDA CFR Title 21 Part 11
FedRAMP
FERPA
FIPS 140-2
FISC
GxP

HIPAA/HITECH
HITRUST
IRS 1075
ISO 9001
ISO 22301
ISO 27001
ISO 27017
ISO 27018
IT Grundschutz Compliance Workbook
ITAR
MARS-E

MeitY
MPAA
MTCS
My Number (Japan)
NEN 7510:2011
NHS IG Toolkit
NIST 800-171
NZ CC Framework
PCI DSS
Section 508

SOC 1
SOC 2
SOC 3
Spain ENS
UK G-Cloud
WCAG 2.0

APEC/ US / EU – Guidance on standards?

	APEC	US	EU
Scope of Privacy Legislation	Framework: Advisory	Sectoral	Omnibus and/or Framework: Binding
Main Law/s Cybersecurity and/or Privacy	APEC Privacy Framework 2005		EU Data Protection Directive 95/46/EC (2017)
Potential Sanctions Level	Varies from Severe (China) to Moderate (Japan)	Moderate – no direct enforcement, but FTC can and will bring significant actions	Moderate (2017) – direct MS enforcement, but powers & resources of DPAs differ

APEC Cybersecurity and Privacy Trends, Part I

- Enforcement
  - On the Rise, but Under Development
  - APEC's Cross-border Privacy Enforcement Arrangement (CPEA) creates a framework for regional cooperation in the enforcement of Privacy Laws
  - Philippines created National Cybersecurity Inter-Agency Committee in 2015
  - Singapore restructured regulators to Infocomm Media Development Authority (IMDA) 2016 to be more effective
  - China's new law adds specific "Cybersecurity Administration of China" to roster of regulators

APEC Cybersecurity and Privacy Trends, Part II

- Information Security
  - Tightening across the board
  - Singapore's Computer Misuse and Cybersecurity Act (CMCA) amendments show teeth, inter alia through criminalization of abuse of personal information
  - Philippines' Department of Information and Communications Technology (DICT) is pushing for stronger cybersecurity protections in The Plan
  - China is legislating for a wide application of localization and authorization rules, especially regarding "critical information infrastructure"
- Harmonization
  - Bright lines visible in Cybersecurity and Privacy
  - Telecommunications, Data Storage, and Data Transfer under focus in key APEC countries
  - Standards, certifications, and testing existing (Japan, Korea) or planned
  - Protection of personal data recognized, if weighed against state interest

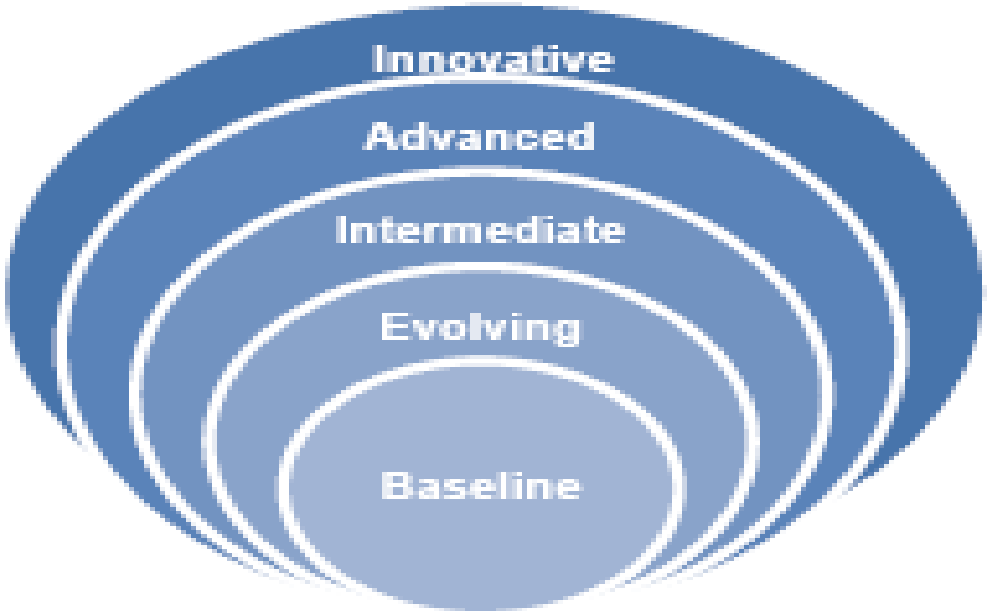
What may work – Frameworks based on maturation

FFIEC Cyber Assessment Tool

- Created to assist FIs identify
  1. Inherent Risk Profile
  2. Cybersecurity Maturity
- Aligns with
  - FFIEC IT Examination Handbook (IT Handbook)
  - NIST CyberSecurity Framework
  - Others

CyberSecurity Maturity Levels

INITIAL LEVEL

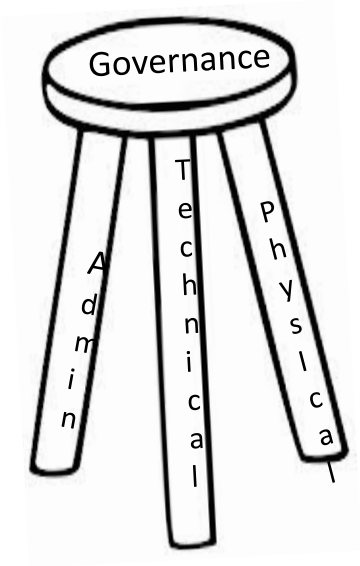


What It Is and What It Isn't

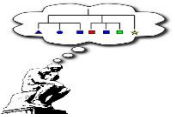
IS	ISN'T
Mgmt tool for Assessing CyberSecurity "maturity	Not a Tool for Assessing Overall CyberSecurity Maturity
Compliments your Existing ISP	Does Not Replace your ISP
Method for Evaluating Cyber Risk	Replacement for Risk Mgmt
Tracking historic progress	Measure of compliance
Focus of regulators	Safe Harbor
Create discoverable materials	Defense against claims made

What is needed?

- **GOVERNANCE** is based on Administrative, Technical & Physical Safeguards
- What Your Company is EXPECTED to understand:
  - Data they collect
  - Where the Data is kept
  - How it is being used, and
  - With Whom is it Shared
  - Keep information secure AND educate employees, third parties, and contractors to do the same
  - Mitigate harms and respond appropriately to all security incidents
- Functions are about MORE than RISK avoidance; its about creating a culture of privacy **COMPLIANCE**



Data Classification & Data Mapping



#1 Step of any GRC Program

- You cannot govern what you do not understand
- Define the data in external terms
  - Personally identifiable information ("PII")
  - Protected health information ("PHI“)
  - Nonpublic personal information ("NPI“)
- Define the data according to internal standard
  - High, medium and low risk
  - Level I, II & III
  - Confidential, public & proprietary
- You cannot safeguard what you cannot locate
- Map existing locations where PII/NPI/PHI is stored
  - Technical locations: databases, servers and systems
  - Physical locations: office, floor and office buildings
  - Don’t forget the "cloud"
- Map of existing data flows
  - Internal: between locations
  - External: from internal locations to external locations
- Map of existing applications
  - Internal: what functions and what data
  - External (including cloud): what functions and what data

Governance and Documentation

- Project Management
  - Initial Risk Assessment
  - Identification of NPI/PII/PHI
  - Identify external access to data onsite
  - Identify encryption utilized
  - Identify remote access requirements
  - CyberSecurity Insurance Assessment
  - Third party contracts
  - Incident Response Plan execution
- Process
  - Timing of decisions
  - Threat timeline
  - Results

Protection

- Understand what you Value
- Understand your Threats
  - What they target
  - What they value
  - Likely attack vectors
- Determine your vulnerabilities
- Prioritize countermeasures based on likely threats and vulnerabilities
- Address Security Culture

Detection

- Understand your Kill Chain
- Detection Deficit Disorder
  - Avoid it
- Human sensors
- Constantly examine the data
- Assume critical assets are being stolen
- Assume networks are compromised and look for indications

Reaction

- Reaction should be anticipated as being a common circumstance
- Reaction built into security program and architecture
- Determine who's attacking you
  - What are their attack methods
- Look for additional attacks
  - Be a hunter
- Feedback into Protection
- Remember, your goal is exit prevention
  - Extrusion prevention is more manageable intrusion prevention

The Role Security Culture/Awareness

- People have a role in Prevention, Detection, and Reaction
- A strong security culture prevents incidents
  - People should behave appropriately
- A strong security culture detects incidents in progress
  - Snowden's coworkers should have noticed suspicious activity
  - Detecting incidents, phishing, etc.
- Reaction
  - Reporting
  - Taking actions to mitigate incidents before they get too damaging

Resolution of Competing Interests

Who Decides?

- Business
- IT
- CISO
- CEO

How is the risk captured?

- Reserve
- Cyber Insurance

Reconsider Skills and Role of CISO

Data Security – Parting Thoughts

- A company's data security procedures must be reasonable and appropriate in light of the circumstances
- A breach does not necessarily show that a company failed to have reasonable security measures – there is no such thing as perfect security
- Attackers are successful not because they are advanced or sophisticated, but because they are adaptive and persistent
- Data security is an ongoing process – show progress - be adaptive and persistent in response
- Need to educate all involved parties, including regulators and judiciary