Cybersecurity and Personal Data Protection:

THAILAND 4.0 AND STRATEGIES FOR THE THAI GOVERNMENT

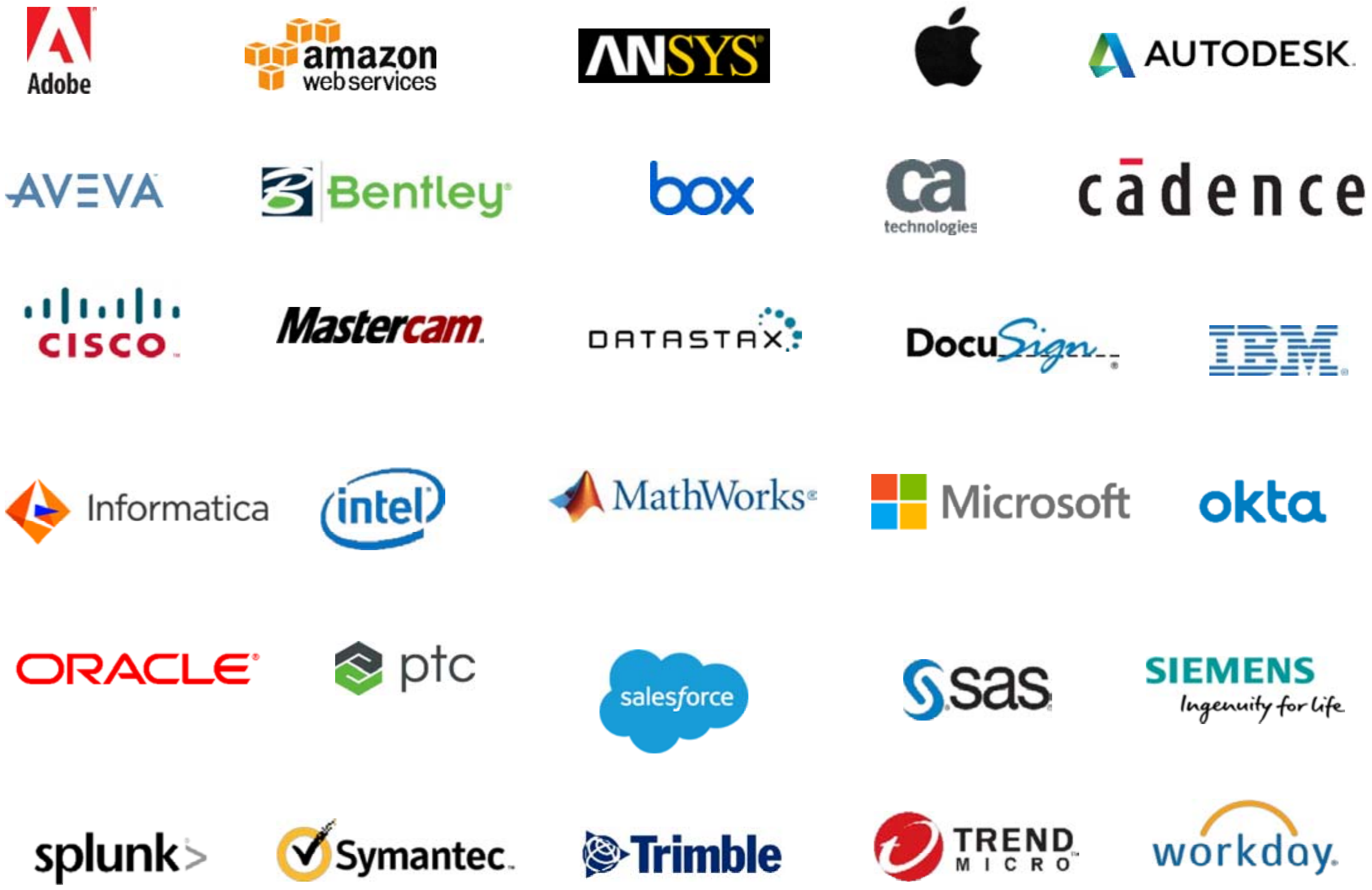
AUGUST 14, 2018

Jared Ragland, Ph.D., Senior Director, Policy – APAC
JaredR@bsa.org

Outline

- Tomorrow’s Technology and the Digital Economy
- BSA 2018 Global Cloud Computing Scorecard
- Cybersecurity
  - Threats, Trends, and Lessons for Cybersecurity
  - BSA International Cyber Security Framework
- Personal Data Protection
  - Laws and Systems
  - APEC CBPR
  - EUGDPR
- Links and Resources

Introduction to BSA



Tomorrow's Technology and the Digital Economy

Technology and the Digital Economy

- Emerging Technology is the key driver for achieving Thailand 4.0 goals:
  - **Data Analytics**
  - **Artificial Intelligence**
  - **Blockchain**
  - **Internet-of-Things**
- **Clear** and **effective cybersecurity** and **personal data protection** policies/legislation will enable these technologies.

2018 BSA Global Cloud Computing Scorecard

2018 Global Cloud Computing Scorecard

The Software Alliance

BSA

2018 BSA GLOBAL CLOUD COMPUTING SCORECARD

Powering a Bright Future

galexia

Introduction

Ranks 24 Countries for cloud readiness – representing 80% of global IT market

- 10 Asia-Pacific countries surveyed: Australia, China, India, Indonesia, Japan, Korea, Malaysia, Singapore, Thailand, and Vietnam

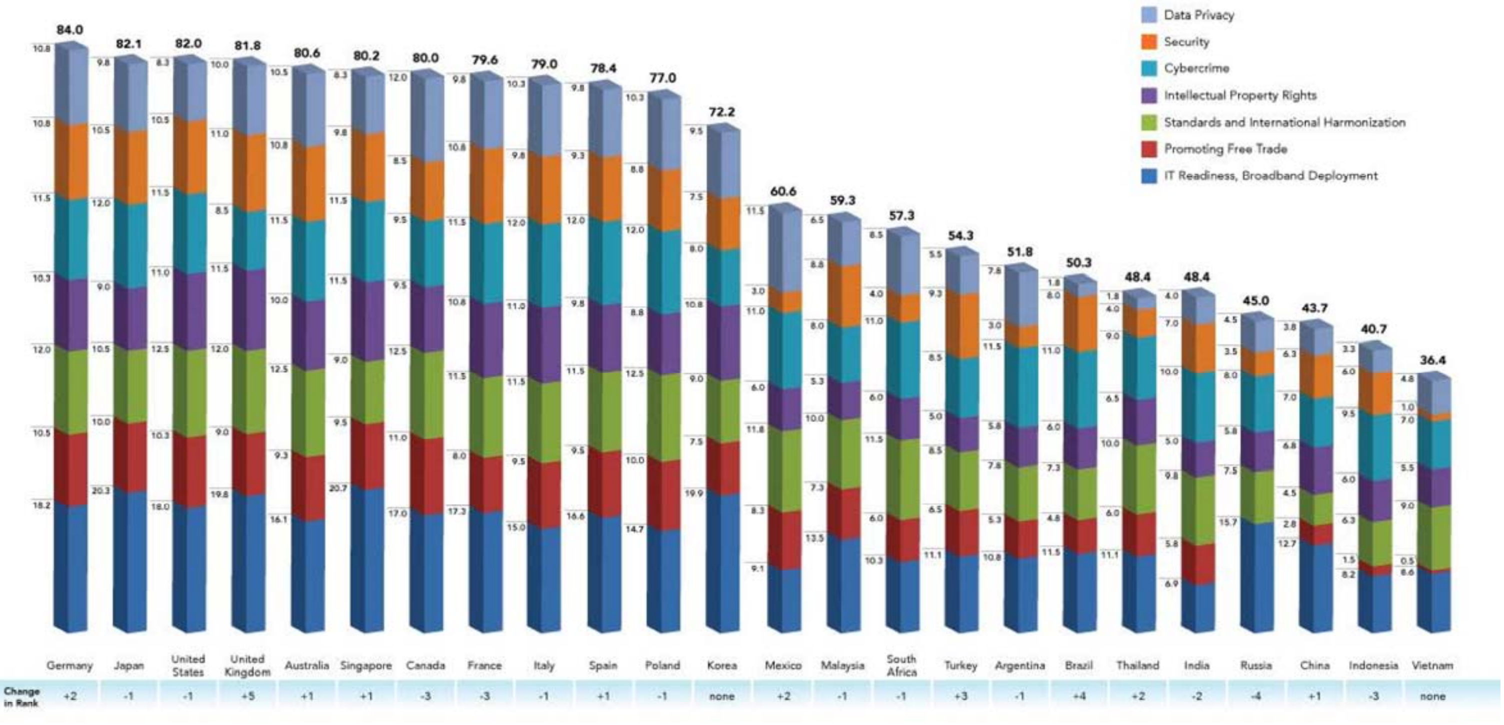
Updated methodology focused on 7 themes:

- Privacy and Data protection
- Security
- Cybercrime
- Intellectual Property Rights
- Support for Industry-Led Standards & International Harmonization of Rules
- Promoting Free Trade
- IT Readiness, Broadband Deployment

2018 Global Cloud Computing Scorecard

2018 BSA Global Cloud Computing Scorecard

By focusing new attention on the policy areas that matter most to cloud computing, the 2018 Scorecard shows continuing improvements in the policy environment for cloud computing in key global economies.



Observations - Thailand

- Thailand ranked 19 out of 24, gaining 2 places since 2016

- Comprehensive cybercrime legislation helps enhance confidence in information technology

- The lack of a comprehensive personal data protection law is a weakness

Observations - General

- Advanced privacy and security policies set leading countries apart from lagging markets

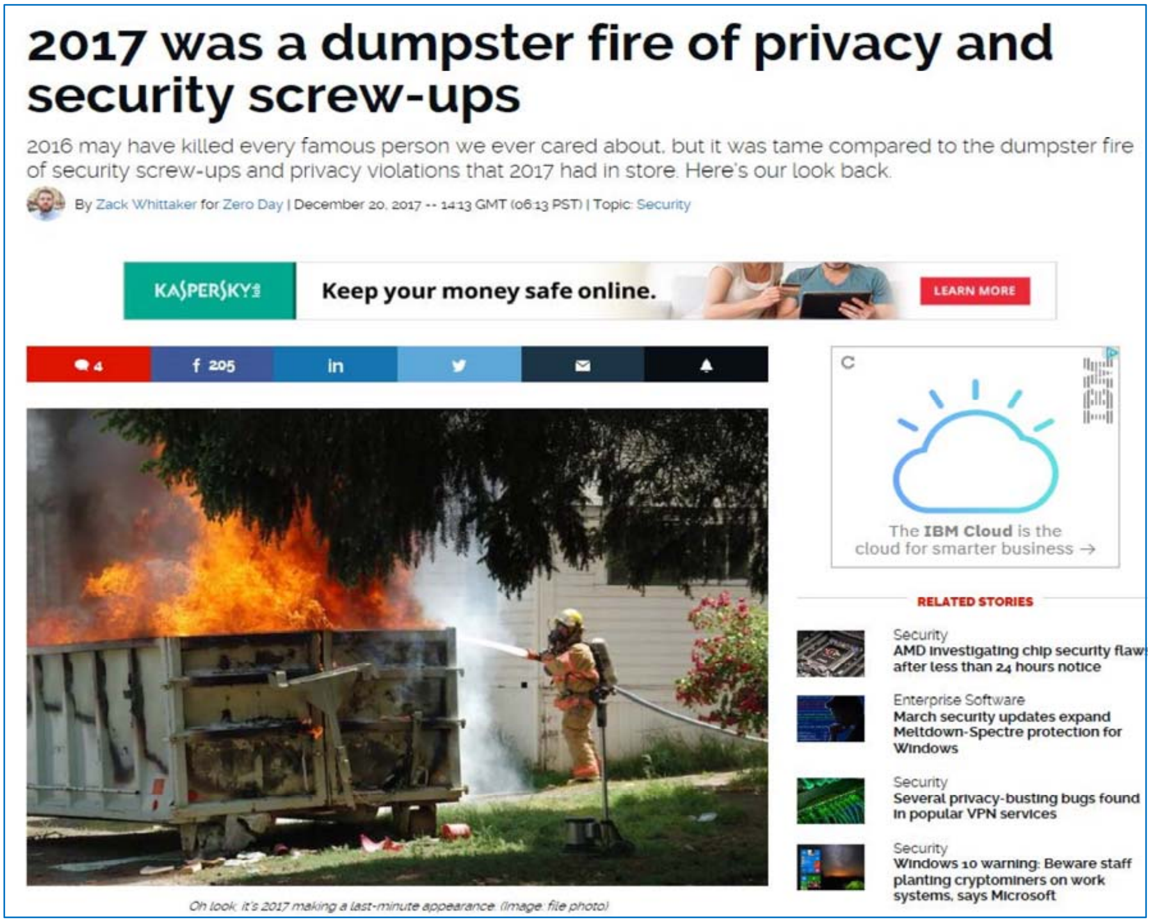
- Policies that inhibit international data transfers make it harder to take full advantage of cloud computing and other emerging technologies, and hinder growth

- Policies should adhere to widely adopted best practices and international agreements

- Globally accepted standards, certifications, and testing help improve the security environment for cloud computing

Cybersecurity

The Year in Cyber



2017 was a dumpster fire of privacy and security screw-ups

2016 may have killed every famous person we ever cared about, but it was tame compared to the dumpster fire of security screw-ups and privacy violations that 2017 had in store. Here's our look back.

By Zack Whittaker for Zero Day | December 20, 2017 -- 14:13 GMT (06:13 PST) | Topic: Security

Oh look, it's 2017 making a last-minute appearance. (Image: file photo)

RELATED STORIES

Security
AMD investigating chip security flaw after less than 24 hours notice

Enterprise Software
March security updates expand Meltdown-Spectre protection for Windows

Security
Several privacy-busting bugs found in popular VPN services

Security
Windows 10 warning: Beware staff planting cryptominers on work systems, says Microsoft

Threats, Trends and Lessons

- **Recent Significant Events**
  - WannaCry
  - NotPetya
  - Equifax
  - Spectre + Meltdown

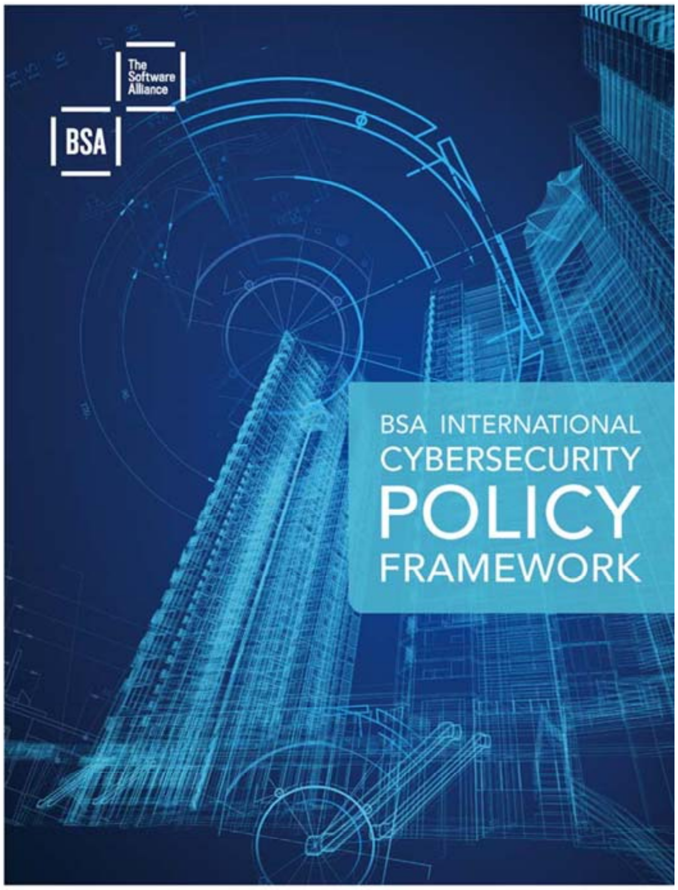
… and some regional data breaches

- Telecommunications service provider in Thailand (Apr ’18)
- Healthcare group in Singapore (Jul ’18)
- Financial Institutions/Banks in Thailand (Aug ’18)

- **Policy Lessons**
  - Blurred Lines – Criminal Tactics + Nation State Capabilities
  - Cyber Threats, Real World Impacts
  - An Ounce of Prevention is Worth a Pound of Cure
  - Global Threats Require Global Solutions

Introduction to BSA International Cybersecurity Policy Framework

BSA International Cybersecurity Policy Framework

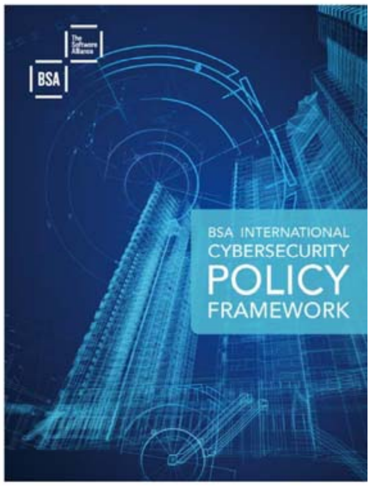


BSA International Cybersecurity Policy Framework

Principles for Effective Cybersecurity Policy

Cybersecurity policies are most effective when:

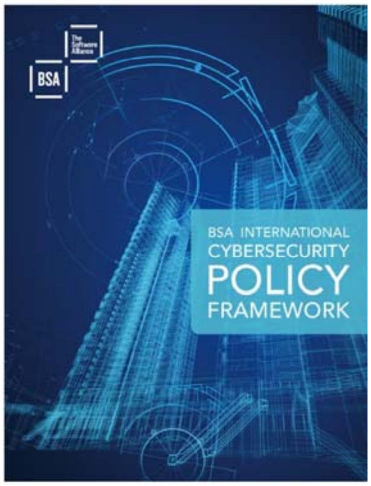
- Aligned with internationally-recognized technical standards
- Risk-based, outcome-focused, technology-neutral
- Market-driven where possible
- Flexible and adaptable to encourage innovation
- Rooted in public-private collaboration
- Oriented to protect privacy



BSA International Cybersecurity Policy Framework

Key Elements

- Government Organization and Strategy
- Cybersecurity and the Government
- Cybersecurity and the Private Sector
- Cybersecurity and the Citizen
- Civil and Criminal Codes
- International Engagement



BSA International Cybersecurity Policy Framework

Key Elements: Highlights

Government Organization and Strategy

- ✓ Single National Body Responsible for Cybersecurity
- ✓ Issue a National Cybersecurity Strategy and Critical Infrastructure Cybersecurity Strategy

Cybersecurity and the Private Sector

- ✓ Enable Cross-Border Data Flows for Business Purposes
- ✗ Avoid Data Localization Requirements
- ✗ Avoid Overbroad Definition of Critical (Information) Infrastructure
- ✗ Avoid Indigenous Security Standards
- ✗ Avoid Requirements to Disclose Source Code and Other Intellectual Property

Cybersecurity and the Government

- ✓ Leverage the Security Benefits of Cloud Services
- ✗ Avoid Domestic Preference Requirements

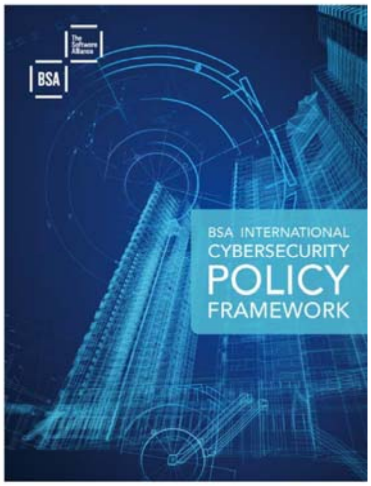
International Engagement

- ✗ Avoid Export Control Policies That Impede Legitimate Cybersecurity Activity
- ✗ Avoid Mandates That IT Systems Manufacturers Support State-Sponsored Hacking

Policy Lessons

ASEAN Regional Policy Trends

- Enhanced Transparency, Private Sector Engagement
- Potentially Broad Incident Reporting Requirements
- Cybersecurity Licensing Requirements
- Potentially Opaque Certification Requirements
- Use of Cyber Policy to Advance Non-Security Objectives



Personal Data Protection

International Trends in Personal Data Protection

- **More Personal Data Protection Laws**:
  - In the Asia-Pacific, **10** comprehensive data protection laws are in operation, **3** in ASEAN:
    - Australia, Hong Kong, Japan, Macao, **Malaysia,** New Zealand, Taiwan, **the Philippines, Singapore**, South Korea
- **Emergence of Data Localization Requirements for Personal Data**:
  - **Cybersecurity laws** with **personal data localization** requirements.
    - In jurisdictions with otherwise no comprehensive personal data protection laws (e.g. China, **Vietnam, Indonesia**)
- **Acceleration of cross-border data flows language in regulations/ systems/ trade agreements**
  - APEC CBPR: 6 economies (Canada, Japan, Mexico, **Singapore,** South Korea, the United States) + 3 more in the process (Australia, **the Philippines,** Taiwan);
  - Bilateral recognition (**Malaysia's** draft whitelist, Russia's whitelist, EU-Japan Mutual Adequacy);
  - The Comprehensive and Progressive Trans-Pacific Partnership (CP-TTP) contains binding language to support data flows and prevent localization.

Laws and Systems

Creating a Personal Data Protection Regime

BSA Data Protection Principles – 5 Pillars:

1. Scope and Definition of Personal Data
2. Collection, Use, and Disclosure of Personal Data
3. Allocation of Obligations and Liability
4. International Data Transfers
5. Personal Data Breach Notifications

- Good examples of effective and business-friendly personal data protection laws map to these principles
  - *e.g. Singapore's PDPA and Japan's PIPA*

Creating a Personal Data Protection Regime

International Examples:

Principles for Personal Data Protection

- High-level multi-lateral principles based on transparency, accountability, and data quality principles
- Sometimes includes implementation rules or processes

(e.g. OECD Privacy Principles, APEC Privacy Framework, ASEAN framework on Personal Data Protection)

Frameworks for Cross-border Data Flows

May include implementation rules or processes

(e.g. APEC CBPR System, Bilateral Adequacy Recognition, Jurisdiction White-Lists)

Comprehensive Data Protection Legislation

- Provides a clear legal framework for cross-sectoral data protection;

(e.g. EUGDPR, Japan's PIPA, Singapore's PDPA, Malaysia's PDPA, Philippines Data Privacy Act)

Sector-specific Data Protection Legislation

In-lieu of or in addition to comprehensive PDP legislation

(e.g. US Health Insurance Portability and Accountability Act, Singapore's Banking Secrecy Act)

Certification to Domestic Laws or Standards

Usually voluntary, to demonstrate accountability

(e.g. Japan's P-Mark, Singapore's Trustmark, France's Privacy Seal)

APEC CBPR

What is the APEC CBPR?

Voluntary, accountability-based system that facilitates data flows among participating APEC member economies

Summary of process:

- APEC member economy submits a letter of intent to:
  a. Participate in the Cross-border Privacy Enforcement Arrangement;
  b. Commit to appoint an accountability agent (AA); and
  c. Complete enforcement mapping between “CBPR System Program Requirements” to domestic personal data protection or privacy law.
- Joint-Oversight Panel (JOP) + Electronic Commerce Steering Group (ECSG) Chair + Data Privacy Sub-Group (DPSG) Chair approves application
- AA is nominated/notified, application submitted for approval to APEC JOP.
- Whole process takes roughly 1.5 – 2 years (including preparation of enforcement map, letter of intent, AA’s application and approval)
- Certification and program requirements are operationally prescriptive – intended for certification.

Benefits of APEC CBPR

Enhanced Privacy Protection for Consumers

- Supports establishing a digital ecosystem of trust

Facilitates Legal Compliance and Provides Access to Regional and Global Markets

- Organizations can be certified to comply with the CBPR Program Requirements
- Depending on member economies' laws, CBPR certified organizations can transfer to or receive from other CBPR certified organizations in compliance with domestic cross-border transfer requirements

APEC Privacy Rules for Processors (PRP)

- Additional mechanism allowing personal data processors to demonstrate that they can help personal data controllers meet their privacy and security obligations
- Assists personal data controllers, including SMEs, to identify trustworthy personal data processors and more easily engage in global data processing operations

EUGDPR

EUGDPR – What’s different?

- The EU General Data Protection Regulation is the ***domestic*** personal data protection legislation for European Union Member States.
- It is similar to many other consent-based data protection laws, with some additional rights and prescriptions, notably:

New and Enhanced Rights of Data Subjects
Data Portability
Right to be Forgotten
Right to Object to Automated Decision-Making

New Procedural Elements
Data Protection Impact Assessments
Data Breach Reporting Requirements
Significant penalties: up to 4% Annual Gross Turn-Over (AGTO)

Policy Lessons

Policy Lessons

- Differentiating between Principles and Frameworks, Laws, and Certification
- Data Protection ≠ Data Localization
- Balancing Flexibility and Prescriptiveness
- Digital Trade and Data Flows language being included in trade agreements (e.g. CP-TPP and RCEP)

Summary

Trends, Challenges, and Recommendations

- Global trend towards more comprehensive personal data protection and cybersecurity laws.
  - Some cybersecurity laws also contain elements of personal data protection.
  - Emerging concerning trend of cybersecurity laws containing broad data localization provisions.
- Challenges of differing laws, data localization provisions, domestic standards and certifications leading to **fragmentation** and **inconsistencies**.

Recommendations for Thailand:

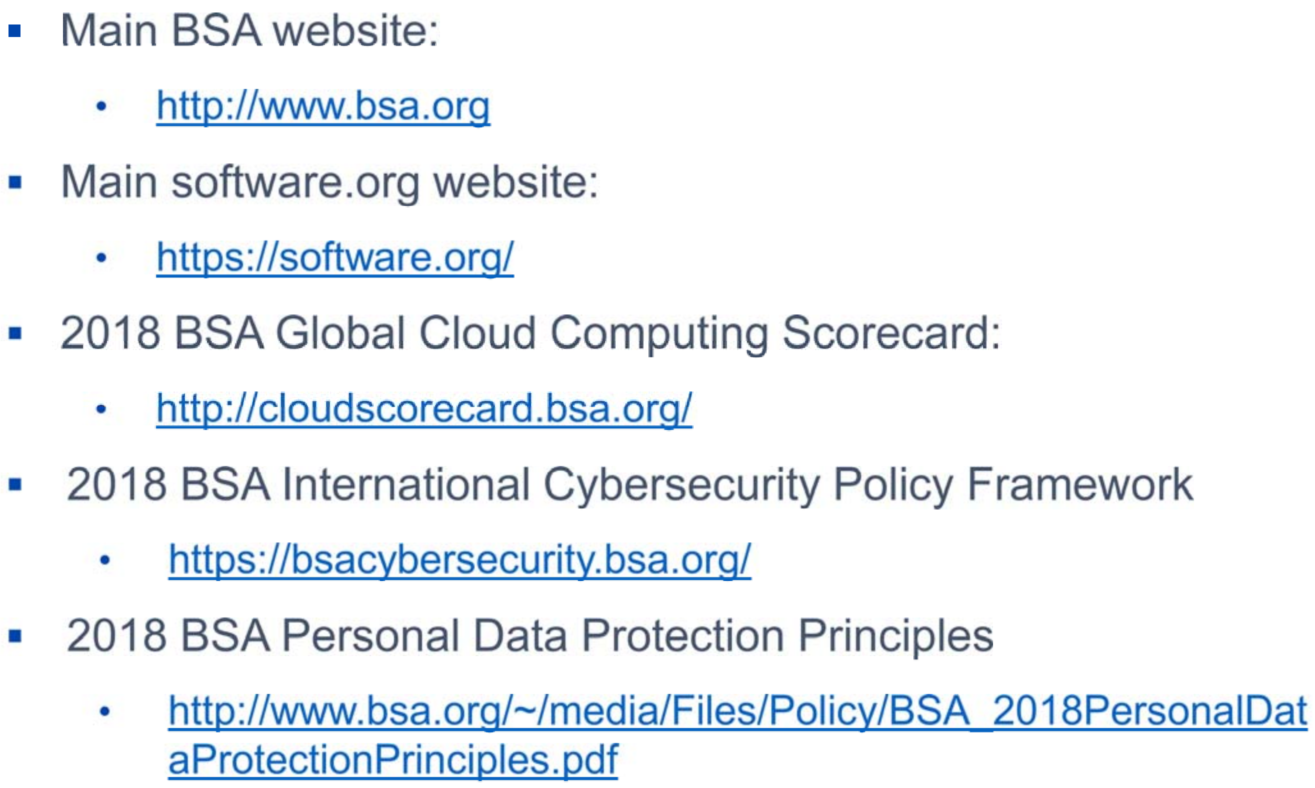
✓ Clear personal data protection law in line with international best practices – consider enforceability and avoid overt prescription.

✓ Well-scoped cybersecurity legislation with clear requirements

X Avoid data localization or requirements that will prevent data transfers

Links and Resources

Links and Resources



- Main BSA website:
  - http://www.bsa.org
- Main software.org website:
  - https://software.org/
- 2018 BSA Global Cloud Computing Scorecard:
  - http://cloudscorecard.bsa.org/
- 2018 BSA International Cybersecurity Policy Framework
  - https://bsacybersecurity.bsa.org/
- 2018 BSA Personal Data Protection Principles
  - http://www.bsa.org/~/media/Files/Policy/BSA_2018PersonalDataProtectionPrinciples.pdf

- bsa.org

BSA

Thank you – Q&A

- **Jared Ragland, Ph.D.**
  Senior Director, Policy – APAC
  JaredR@bsa.org