

# **RSA**®Conference2019 **Asia Pacific & Japan**

Singapore | 16–18 July | Marina Bay Sands



**BETTER.**

SESSION ID: PGR-R01

## **Strengthening Supply Chain Security: A Global Effort**

**Darryn Lim**

Director, Policy – APAC



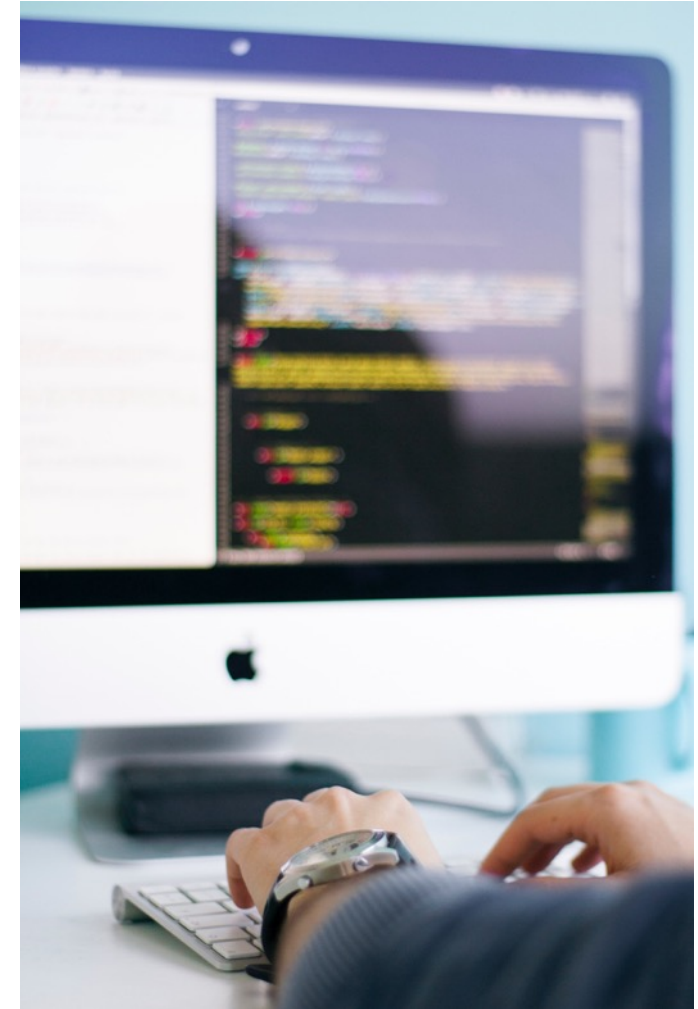
@BSAnews



#RSAC

# Agenda

- Introduction to BSA
- Threat Landscape
- BSA International Cybersecurity Framework
- BSA Software Security Framework
- BSA Supply Chain Security Principles
- Applying the Principles
- Q&As



# Introduction to BSA

- The leading advocate for the global software industry before governments and in the international marketplace
- Headquarters in Washington, DC
- Global operations – APAC regional offices in Singapore, Bangkok, Beijing, New Delhi, Seoul, and Tokyo
- Advocates for public policies that foster technology innovation and drive growth in the digital economy

# BSA APAC Policy Members



# **RSA**®Conference2019 **Asia Pacific & Japan**

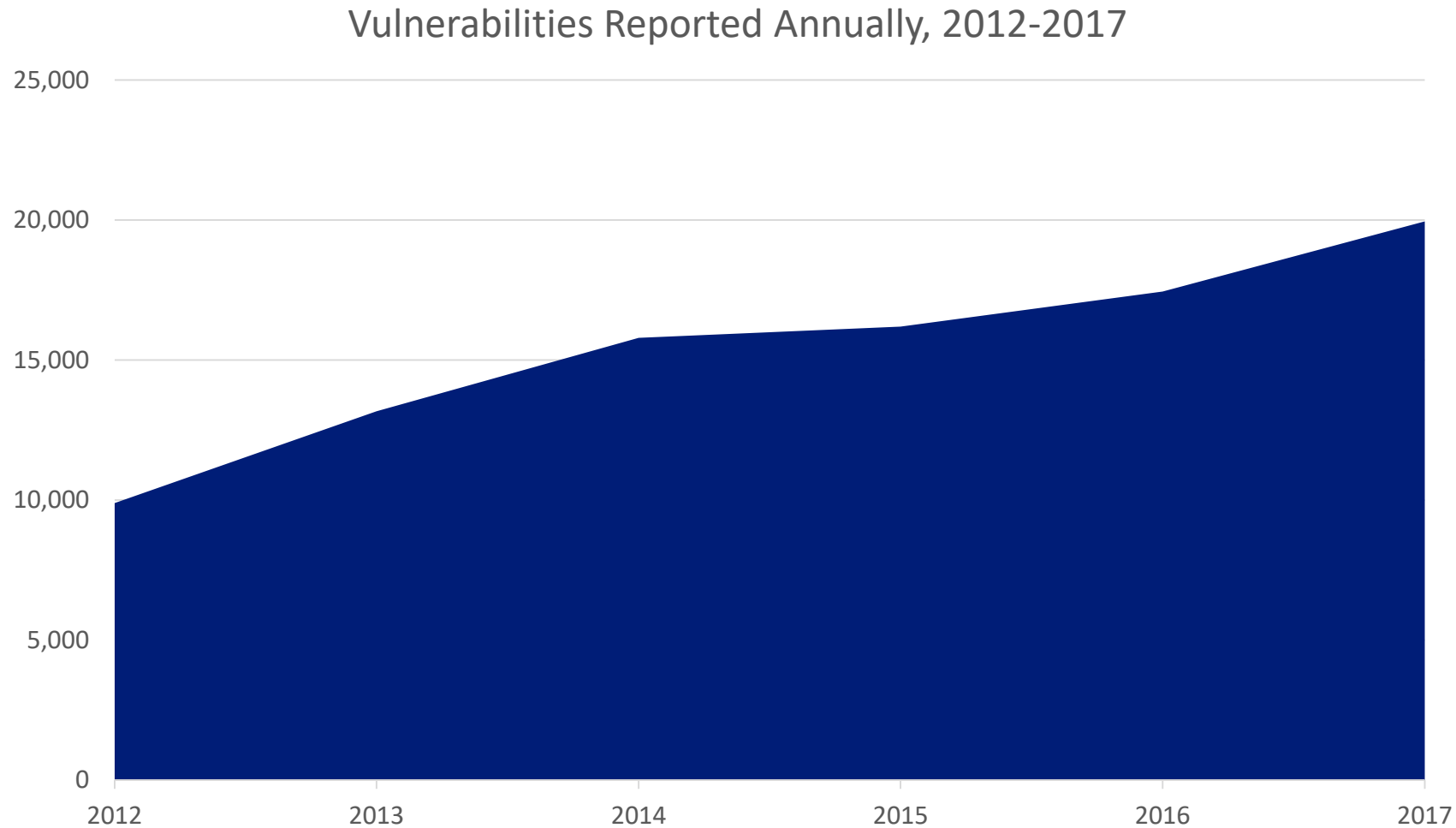
## **Threat Landscape**

An abstract graphic in the bottom right corner of the slide. It consists of numerous thin, curved lines in shades of light blue and purple, flowing from the bottom right towards the center. Small dots of the same colors are scattered along these lines, creating a sense of movement and data flow.



# Software Vulnerabilities Are Increasing\*

#RSAC



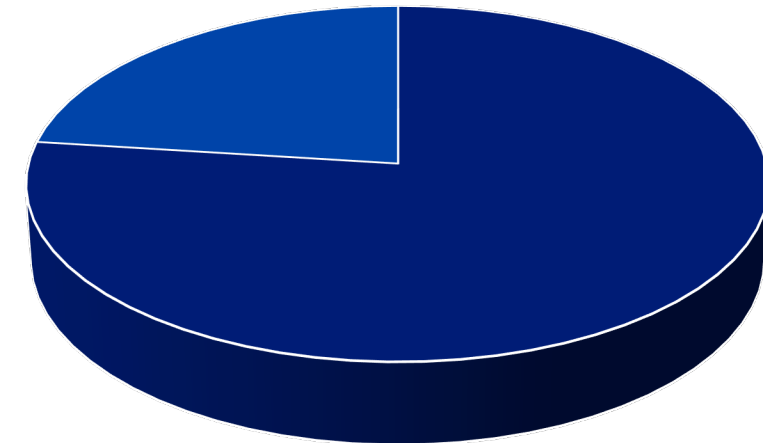
\*Flexera, *Vulnerability Review 2018: Global Trends*

# Malware Increasingly Targets Existing Software Vulnerabilities\*

- 77% of malware attacks in 2017 exploited vulnerabilities in software already installed on the target system
- Fileless malware attacks are 10 times more likely to succeed than file-based attacks
- Cost of attacks ↑ from \$5M (2017) to \$7.1M (2018)

\*The Ponemon Institute, *The State of Endpoint Security Risk in 2017*, *The State of Endpoint Security risk in 2018*

Malware Attacks (%)



■ Fileless ■ File-based payload

# A Growing Target: The Internet of Things

## 600%

- Increase in attacks against IoT Devices from 2016 to 2017\*

\*Symantec, 2018 Internet Security Threat Report

## 125 Billion

- Estimated Number of IoT Devices Deployed By 2030\*\*

\*\*IHS Markit, *The Internet of Things: A movement, not a market*, Oct 2017



# Significant APAC Cybersecurity Events

- **Malaysia, October 2017:** Personal data leak affecting **46.2M** mobile subscribers
- **Singapore, July 2018/January 2019:** Two health data breaches affecting **1.5M** SingHealth patients and **14,200** HIV+ individuals
- **Australia, Japan, Thailand, and Vietnam, March 2019:** Toyota suffers a chain of data breaches affecting **3.1M** Toyota and Lexus customers
- **Indonesia, March 2019:** “Gnosticplayers” hack affecting **26M** user accounts
- **India, April 2019:** Wipro (outsourcing firm) phishing breach

## Case Study: NotPetya Attack

You became victim of the PETYA RANSOMWARE!

The haddisks of your computer have been encrypted with the Petya encryption algorithm. There is no way to recover your data without this key. You can purchase this key on the dark web. Purchase your key and restore your data.

<https://www.petya-ransomware.com/>

# Supply Chain Risk Management Rising in Importance

- Supply chains are increasingly becoming interconnected and automated
- The CSA Singapore recently warned that cyber criminals are target supply chains to
  - Extract information from companies involved
  - Hold them to ransom
- Industries dominated by a few companies are especially vulnerable
- Supply chain risk management is more important than before



# Supply Chain Attacks on the Rise\*

- Attacks on supply chains increased by 78 percent in 2018
- Attacks increasingly through trusted channels:
  - Software update hijacking
  - Malicious code injection into legitimate software

↑ 78%

*\*Symantec, 2019 Internet Security Threat Report*



# Policy Challenges: Supply Chain Security

- While nations are taking steps to address supply chain security, some policies can actually impede collaborative solutions to transnational threats
- Examples include:
  - Country-specific technical standards
  - Domestic sourcing requirements
  - Overly restrictive software provenance policies



# Policy Implications

1. Blurred lines – criminal tactics + nation state capabilities
2. Cyber threats, real world impacts
3. Supply chain risk management increasingly important
4. Global threats require global solutions



# Frameworks for Global Solutions

1. International Cybersecurity Framework
2. Software Security Framework
3. Supply Chain Security Principles

**RSA**®Conference2019  
**Asia Pacific & Japan**

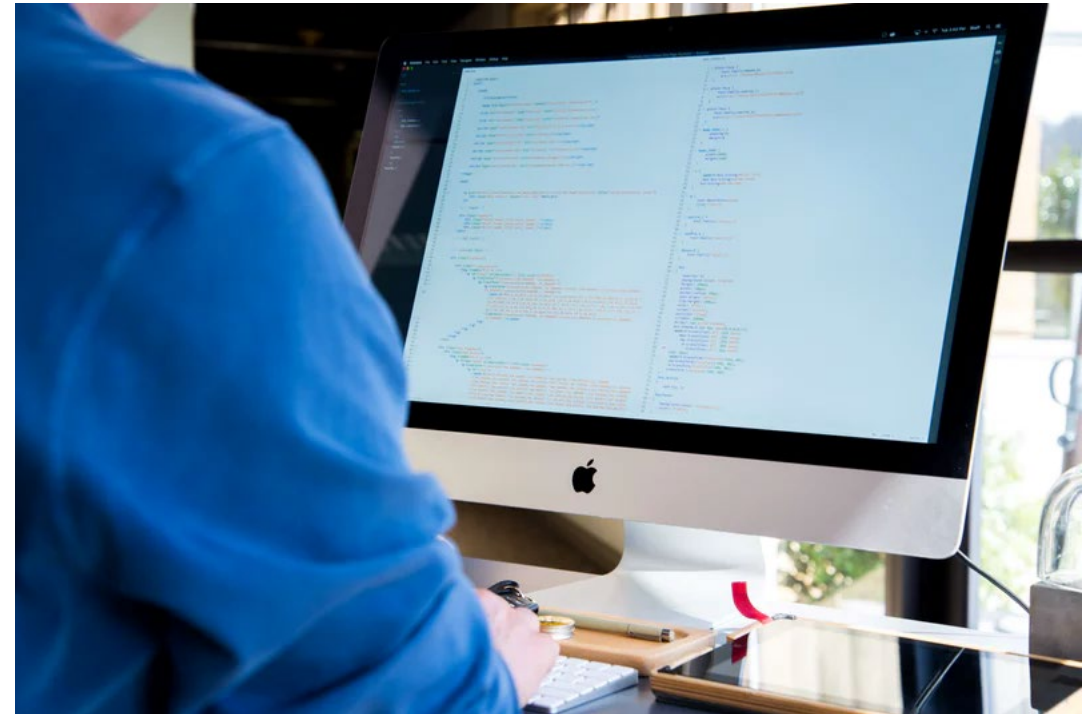
# **BSA International Cybersecurity Policy Framework**

An abstract graphic in the bottom right corner of the slide. It consists of numerous thin, light blue lines that form overlapping circles and arcs. Small dots of varying sizes are scattered along these lines, creating a sense of motion and connectivity, reminiscent of a network or data flow.

# 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



# Key Elements

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



# Government Organization and Strategy

## Structure

- ✓ Establish a Single National Body Responsible for Cybersecurity
- ✓ Clearly Define Stakeholder Roles and Responsibilities
- ✓ Establish a Functional, Timely Interagency Process

## Strategy

- ✓ Issue a National Cybersecurity Strategy
- ✓ Issue a Critical Infrastructure Cybersecurity Strategy
- ✓ Maintain Up-to-Date National Cybersecurity Incident Response Plan for Critical Infrastructure

## Stakeholder Engagement

- ✓ Establish Structure for Facilitating Public-Private Partnerships
- ✓ Create Mechanism for Supporting National and Sub-National Governments

# Cybersecurity and the Government

## Preparedness and Response

- ✓ Establish and Resource National Computer Emergency Response Team
- ✓ Authorize and Encourage Timely Threat Information-Sharing
- ✓ Ensure Calibrated Structure for Incident Reporting
- ✓ Ensure a Consistent, Reasonable Standard for Personal Data Breach Notification
- ✓ Establish a Transparent, Coordinated Process for Government Handling and Disclosure of Vulnerabilities

## Procurement

- ✓ Keep Acquisition Technology Neutral
- ✓ Ensure Use of Licensed, Vendor-Backed Software
- ✓ Leverage the Security Benefits of Cloud Services
- ✓ Build Security Considerations into Acquisition Processes
- ✗ Avoid Domestic Preference Requirements



# Cybersecurity and the Private Sector

## Data Flows

- ✓ Enable Cross-Border Data Flows for Business Purposes
- ✗ Avoid Data Localization Requirements

## Critical Infrastructure

- ✓ Focus on Security Outcomes
- ✓ Use Risk-Based, Flexible Policy Framework
- ✗ Avoid Overbroad Definition of Critical (Information) Infrastructure
- ✓ Align Critical Infrastructure Security with Internationally Recognized Standards
- ✗ Avoid Indigenous Security Standards
- ✓ Ensure Any Certification Regimes Are Balanced, Transparent, and Internationally Based
- ✗ Reject Requirements to Disclose Source Code and Other Intellectual Property

## Consumer Products

- ✓ Promote Market-Driven Solutions
- ✓ Ensure Any Certification Schemes Are Voluntary, Market-Driven, Broad-Based, and Internationally Aligned
- ✓ Encourage Adoption of Internationally Recognized Standards

# Cybersecurity and the Citizen

## Awareness

- ✓ Invest in Public Cybersecurity Awareness
- ✓ Create Tools to Inform Consumer Choices

## Workforce Development

- ✓ Build Cybersecurity Awareness into Every Level of Education
- ✓ Prioritize Diversity in Cybersecurity Education and Training
- ✓ Support Alternative Pathways to Cybersecurity Careers

# Criminal Codes

## Cyber Crime Legislation

- ✓ Establish a Comprehensive Legal Framework Consistent with Budapest Convention on Cyber Crime
- ✓ Apply Criminal Liability Only to Actors with Criminal Intent
- ✓ Provide Technical Training and Support for Law Enforcement

# International Engagement

## Fostering Cooperation

- ✓ Integrate Cybersecurity Cooperation into Foreign Policy
- ✓ Engage in International Cooperative Efforts
- ✗ Ensure Export Control Policies Do Not Impede Legitimate Cybersecurity Activity

## Upholding International Obligations

- ✓ Prevent Territory from Being Used for International Cyber Attacks
- ✗ Avoid Mandates That IT Systems Manufacturers Support State-Sponsored Hacking

**RSA**®Conference2019  
**Asia Pacific & Japan**

## **BSA Software Security Framework**

An abstract graphic in the bottom right corner of the slide. It consists of numerous thin, light blue lines that form overlapping circles and arcs. Small dots of varying sizes are scattered along these lines, creating a sense of motion and connectivity, reminiscent of a network or data flow.

# A Global Uptick in Software Security Policy Initiatives

- **European Union**
  - Cybersecurity Act/EU-wide certification scheme
  - Burgeoning Duty of Care discussion
  - Liability discussions in Netherlands, Germany, France
- **United States**
  - Draft NIST SSDL Guidance Issued
  - *IoT Cybersecurity Improvement Act* Moving Through Congress (S. 734/H.R. 1668)
- **Singapore**
  - IMDA IoT Cyber Security Guide
- **China**
  - Numerous standards and measures under Cybersecurity Law
- **Japan**
  - IoT Certification Scheme discussions
  - Early-stage discussions of software transparency and software liability



# Addressing the Challenge

Governments can collaborate to address the challenge of securing software by encouraging:

- Common security standards and common assessment tools
- Security-by-design principles and secure development lifecycles
- Cyber and supply chain risk management and vulnerability disclosure processes (based on internationally recognized standards)
- Avoiding blanket software provenance policies
- Strategic / long-term policy pathways and security roadmaps

# BSA's Framework for Secure Software

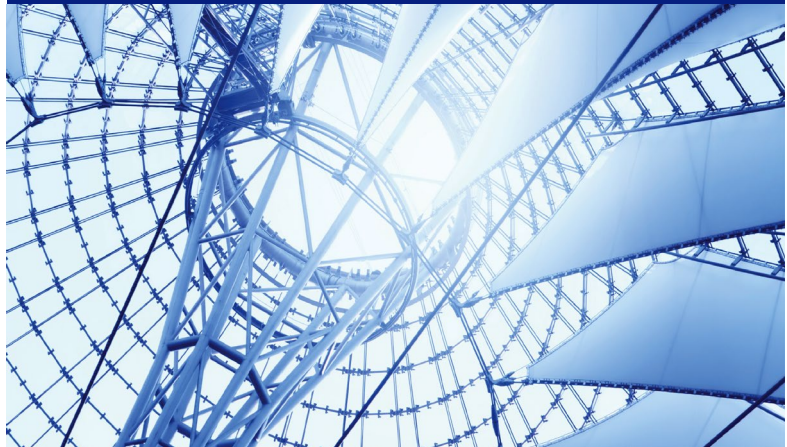
- An approach to software security that is
  - Flexible
  - Outcome-focused
  - Risk-informed
  - Cost-effective
  - Repeatable.
- Provides a common organization and structure to help software developers achieve desired security outcomes



# Guiding Principles

- ❖ Flexible
- ❖ Risk-Based
- ❖ Outcome-Focused
- ❖ Neutral toward *technologies, development processes, and coding languages*
- ❖ Aligned with internationally recognized standards

## Guiding Principles



# Digging Into The Framework

## Digging Into The Framework



### SECURE DEVELOPMENT

Secure development addresses security in the phase of software development when a software project is conceived, initiated, developed, and brought to market



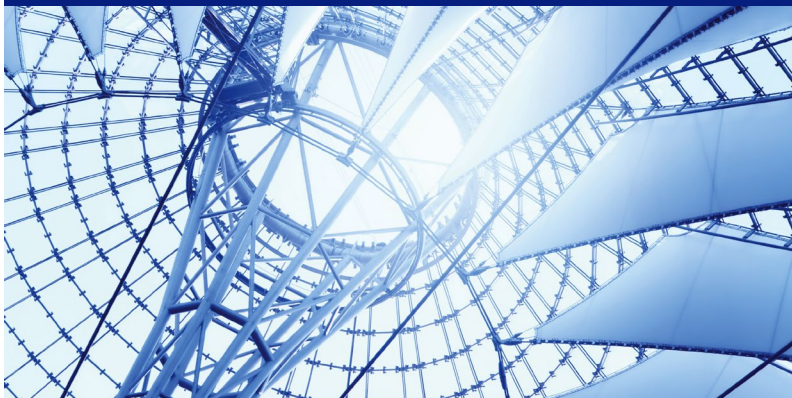
### SECURE CAPABILITIES

Secure capabilities identify key security characteristics recommended for a software product

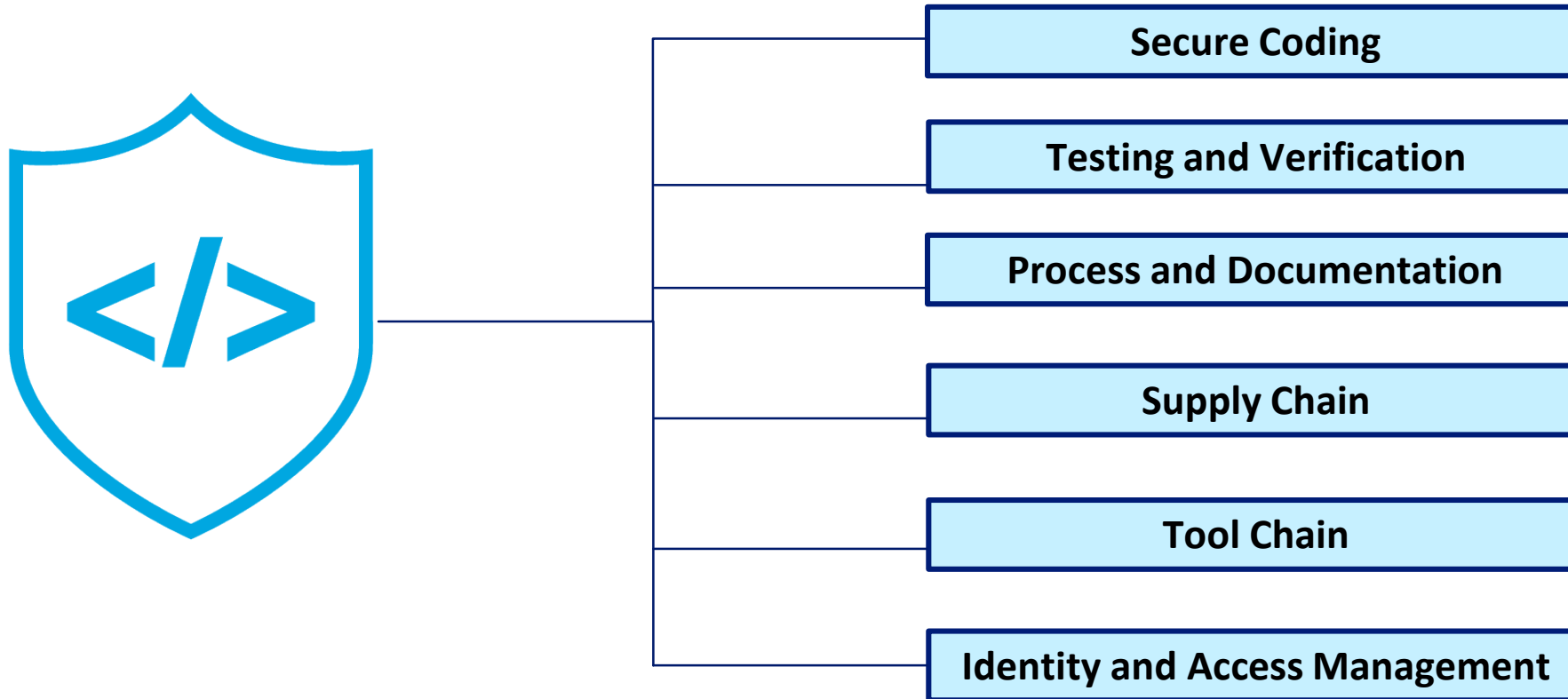


### SECURE LIFECYCLE

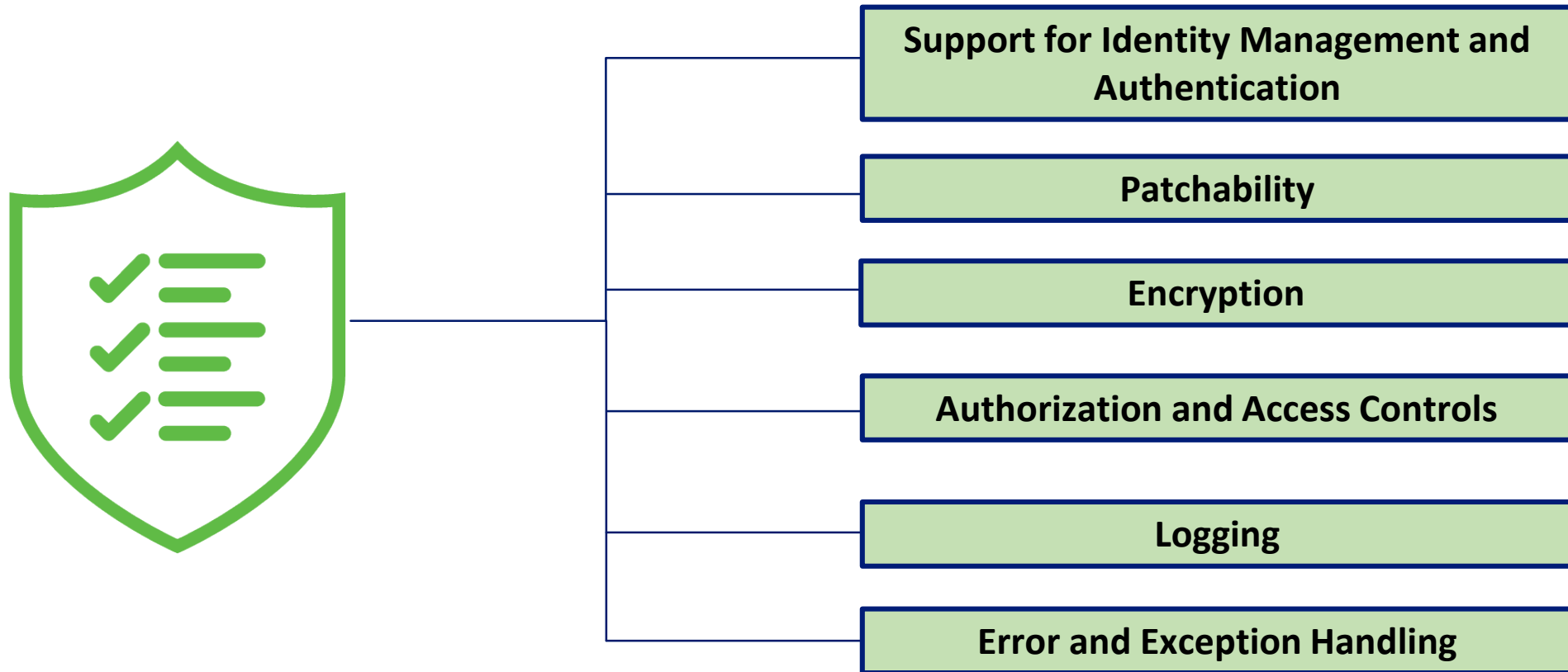
Secure lifecycle addresses considerations for maintaining security in a software product from its development through the end of its life



# Function: Secure Development

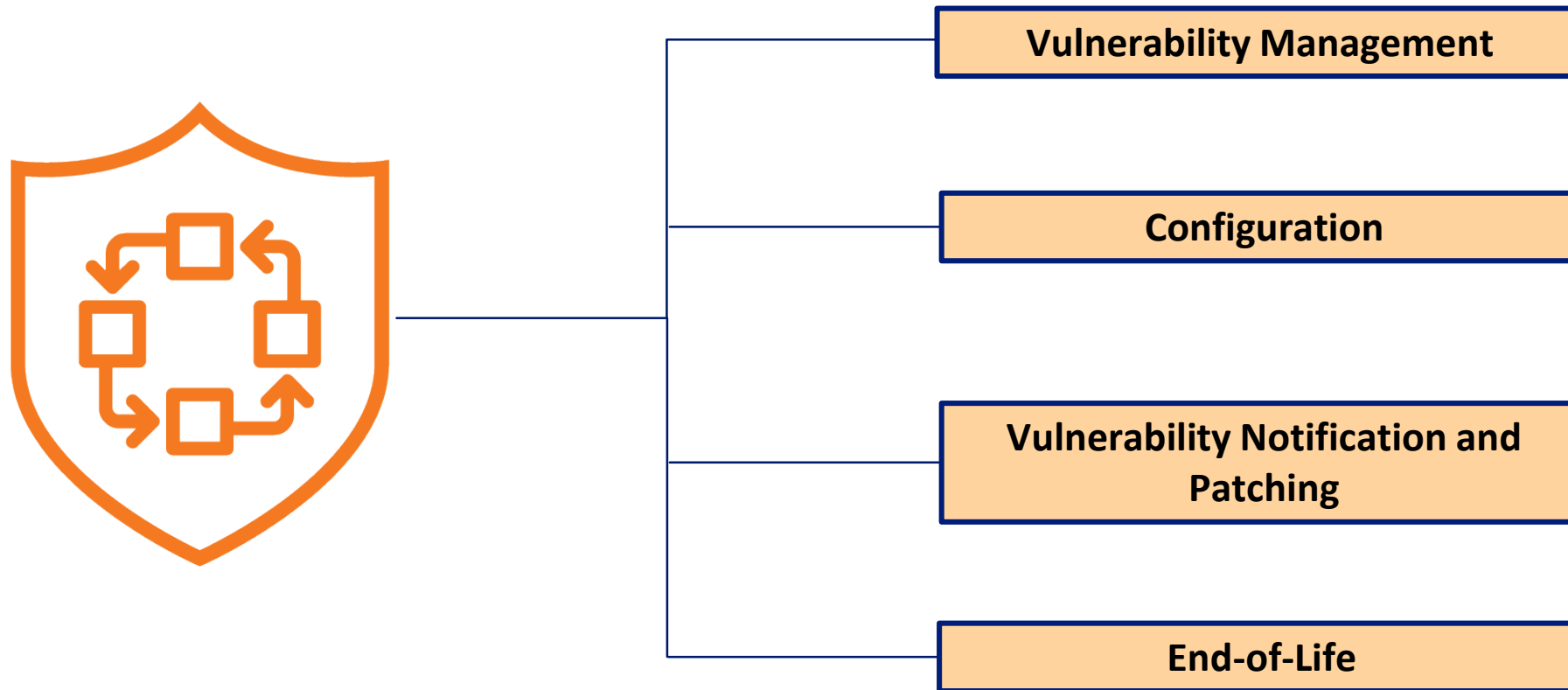


# Function: Secure Capabilities





# Function: Secure Lifecycle



# The BSA Framework for Secure Software

Category	Subcategory	Diagnostic Statement	Comments on Implementation	Relevant Standards and Informative Resources
SECURE DEVELOPMENT				
Secure Coding (SC)	SC.1. Threat modeling and risk analysis are employed during software design to identify threats and potential mitigations.	SC.1-1. Software development organizations document likely threats.	Some software developers work in accordance with “zero trust” principles, which assume a pervasively hostile environment. Yet, even with zero trust approaches, threat modeling is important for identifying sensitive data and prioritizing threats for mitigation.	ISO/IEC 27034; OWASP Application Security Verification Standard; SAFECode “Fundamental Practices”; SAFECode “Tactical Threat Modeling”; SAMM; BSIMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet
		SC.1-2. Threats are rated and prioritized according to risk.		ISO/IEC 27034; SAFECode “Fundamental Practices”; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet
		SC.1-3. Software development organizations apply common threat modeling methodologies.		ISO/IEC 27034; SAFECode “Fundamental Practices”; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet; SAFECode “Tactical Threat Modeling”

# The BSA Framework for Secure Software

Category	Subcategory	Diagnostic Statement	Comments	Standards and Resources
SECURE DEVELOPMENT				
Secure Coding (SC)	SC.1. Threat modeling and risk analysis are employed during software design to identify threats and potential mitigations.	SC.1-1. Software development organizations document likely threats.	Some software work in accordance with "zero trust" principles, but assume a pervasive environment. Zero trust approach modeling is important for identifying sensitive data and prioritizing threat mitigation.	OWASP Application Security Standard; SAFECode "Fundamental Practices"; SAFECode "Tactical Threat Modeling"; SAMM; BSIMM; CWSS; Threat Modeling Cheat Sheet
		SC.1-2. Threats are rated and prioritized according to risk.		ISO/IEC 27034; SAFECode "Fundamental Practices"; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet
		SC.1-3. Software development organizations apply common threat modeling methodologies.		ISO/IEC 27034; SAFECode "Fundamental Practices"; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet; SAFECode "Tactical Threat Modeling"

**Diagnostic Statement:**  
specific,  
measurable  
metric  
applicable to  
policy tools  
(e.g.,  
certification)

# The BSA Framework for Secure Software

Category	Subcategory	Diagnostic Statement	Comments on Implementation	Relevant Information
SECURE DEVELOPMENT				
Secure Coding (SC)	SC.1. Threat modeling and risk analysis are employed during software design to identify threats and potential mitigations.	SC.1-1. Software development organizations document likely threats.	Some software developers work in accordance with “zero trust” principles, which assume a pervasively hostile environment. Yet, even with zero trust approaches, threat modeling is important for identifying sensitive data and prioritizing threats for mitigation.	ISO/IEC 27034 Verification Standard “Fundamental Threat Modeling”; CAPEC; OWASP
		SC.1-2. Threats are rated and prioritized according to risk.		ISO/IEC 27034; SAFECode “Fundamental Practices”; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet
		SC.1-3. Software development organizations apply common threat modeling methodologies.		ISO/IEC 27034; SAFECode “Fundamental Practices”; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet; SAFECode “Tactical Threat Modeling”

**Comments on Implementation:**  
guidance for tailoring subcategory and diagnostic statements to specific software types and processes

# The BSA Framework for Secure Software

Category	Subcategory	Discussion	Comments on Implementation	Relevant Standards and Informative Resources
SECURE DEVELOPMENT				
Secure Coding (SC)	SC.1. Threat modeling and risk analysis are employed during software design to identify threats and potential mitigations.	SC.1.1. Organizations apply threat modeling methodologies.	Some software developers work in accordance with “zero trust” principles, which assume a pervasively hostile environment. Yet, even with zero trust approaches, threat modeling is important for identifying sensitive data and prioritizing threats for mitigation.	ISO/IEC 27034; OWASP Application Security Verification Standard; SAFECode “Fundamental Practices”; SAFECode “Tactical Threat Modeling”; SAMM; BSIMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet
		SC.1.2. Organizations apply common threat modeling methodologies.		ISO/IEC 27034; SAFECode “Fundamental Practices”; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet
		SC.1.3. Organizations apply common threat modeling methodologies.		ISO/IEC 27034; SAFECode “Fundamental Practices”; SAMM; CWSS; CAPEC; OWASP Threat Modeling Cheat Sheet; SAFECode “Tactical Threat Modeling”

**Relevant standards and informative resources:**  
Framework is aligned to relevant international standards, and points to relevant best practice literature.

**RSA**®Conference2019  
**Asia Pacific & Japan**

## **BSA Supply Chain Security Principles**

An abstract graphic in the bottom right corner of the slide, consisting of numerous overlapping circles and dots in shades of light blue and purple, creating a sense of motion and connectivity.



# BSA Supply Chain Security Principles

- Risk Management
- Interoperability
- Transparency
- Fairness
- Research and Development
- Collaboration
- Discretion
- Enforcement

# BSA Supply Chain Security Principles

## Risk Management

- Governments should adopt risk management approaches to supply chain security
- Risk management entails:
  - understanding risk through the identification of likely threats, vulnerabilities, and potential consequences
  - tailoring mitigation strategies to risks
  - prioritizing actions based on the most relevant and potentially impactful risks
- Risk management approaches
  - provide flexibility for stakeholders to adapt to a constantly evolving threat environment
  - help policymakers avoid unintended consequences of mistargeted policies

# BSA Supply Chain Security Principles

## Interoperability

- Modern technology supply chains are often transnational
- Policies should be interoperable across borders
  - Internationally recognized, industry driven standards help facilitate transnational operational collaboration against significant cyber threats

## Transparency

- Opaque government supply chain risk management policies and processes create confusion and can undermine economic competitiveness of businesses
- Supply chain risk management policies should be transparent to the public, with specific actions notified to impacted stakeholders
- Governments should have vulnerability disclosure policies (e.g., in accordance with vulnerability disclosure methodologies described in ISO/IEC 29147).

# BSA Supply Chain Security Principles

## Fairness

- There should be meaningful mechanisms for resolving disputes and for stakeholders to be heard
- Dispute resolution mechanisms create an environment of certainty and predictability without limiting tools for mitigating risk

## Research and Development

- Security techniques must adapt to an ever-changing environment of new technologies and new threats
- R&D of new technological approaches to fostering supply chain integrity helps stakeholders maintain the advantage against bad actors

# BSA Supply Chain Security Principles

## Collaboration

- Supply chain risk management efforts will be most effective when undertaken with all stakeholders concerned
- Governments should embrace public-private partnerships to secure supply chains and develop best practices for supply chain risk management
- G-to-G collaboration also important

## Discretion

- Governments should not intervene in global supply chains

## Enforcement

- Governments should pursue aggressive law enforcement against malicious actors

**RSA**®Conference2019  
**Asia Pacific & Japan**

## **Applying the Frameworks/Principles**

An abstract graphic in the bottom right corner of the slide. It consists of numerous thin, overlapping circles and lines, some of which are dotted, creating a complex, web-like pattern. The colors are light blue and white, contrasting with the dark blue background.



# Applying the Frameworks/Principles

- In the Policy Sphere:
  - How can the frameworks/principles serve as a useful benchmark to inform policy regulations, certification schemes, and similar tools?
- In the Marketplace:
  - How can the frameworks/principles help the industry deliver more secure and trusted software throughout the supply chain?

## Summing It Up

1. The threat landscape is rapidly changing
2. Software is critical to the supply chains of products and services across almost every industry
3. Software security is essential to supply chain security
4. A global approach is required
5. BSA's frameworks/principles provide a foundation for effective policy and market interventions to improve software and supply chain security

# Links to Resources

- **Main BSA site:** [www.bsa.org](http://www.bsa.org)
- **BSA Cybersecurity Microsite:** [bsacybersecurity.bsa.org](http://bsacybersecurity.bsa.org)
- ***BSA International Cybersecurity Policy Framework:*** <https://www.bsa.org/reports/bsa-international-cybersecurity-framework>
- ***BSA Software Security Framework:*** <https://www.bsa.org/reports/bsa-framework-for-secure-software>
- **BSA News Room:** <https://www.bsa.org/news-events/news>
- **Twitter:** [@BSAnews](https://twitter.com/BSAnews)

# RSA<sup>®</sup>Conference2019 Asia Pacific & Japan

Thank You

**Darryn Lim**

Director, Policy – APAC



The Software Alliance

@BSAnews