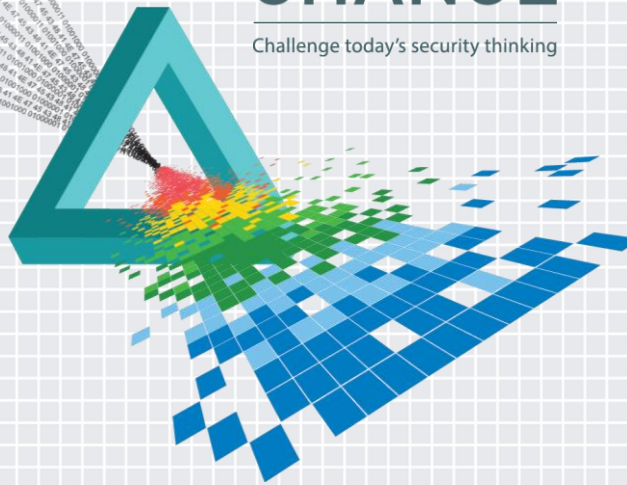
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: ECO-W02

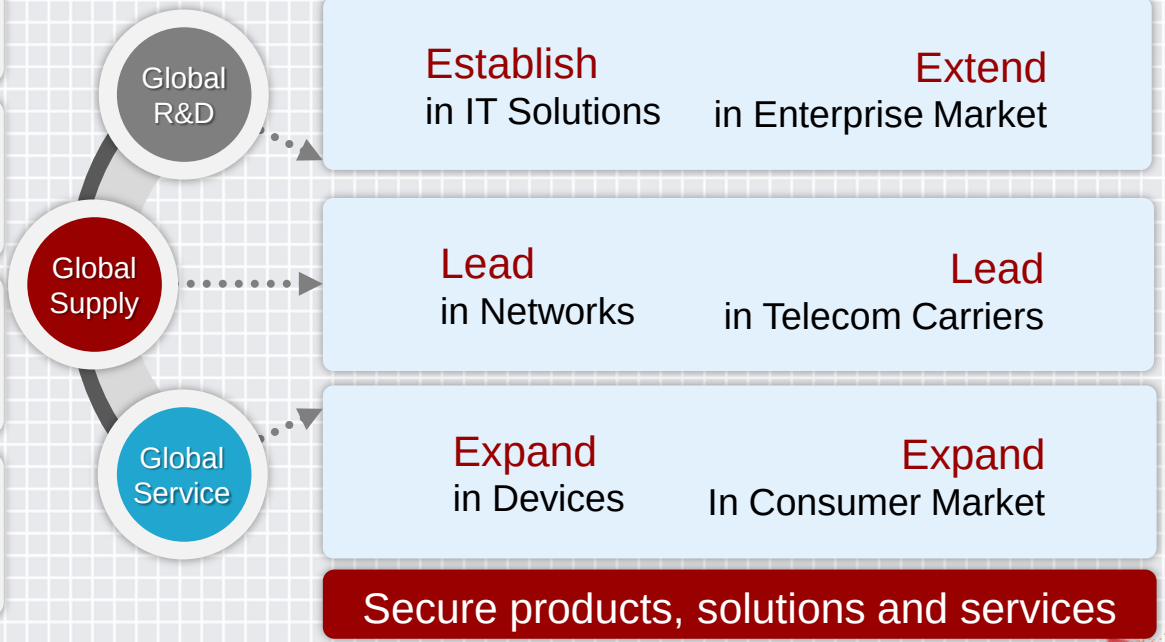
Addressing the Global Supply Chain Threat Challenge – Huawei, a Case Study

Andy Purdy

Chief Security Officer
Huawei Technologies USA

Huawei is a global organization serving over a third of the planet's population.

- A leading global ICT solutions, Fortune Global 500 company
- Operations in 170 countries, 150,000 employees, 73% recruited locally
- 70,000 employees in R&D
- 15 R&D centers; 25 Joint Innovation Centers
- $46 B revenue in 2014
- Serving 45 of the world's top 50 operators



Huawei and Cyber Security

Toward a risk-based, level playing field for ICT

- Supply Chain Risk – Huawei is working with the Open Group Trusted Technology Forum and other major companies and government to gain international support for the Open Group Trusted Technology Provider Standard and accreditation program.

Huawei and Cyber Security

Toward a risk-based, level playing field for ICT (2)

- EastWest Institute Cyber Initiative – EWI is working with key companies (Huawei and Microsoft and others) and governments (US, China, Russia, UK, Germany, India, etc.) to seek agreement on contentious cyber issues, including the global availability of more secure ICT products.

Huawei and Cyber Security
The Open Group Trusted Technology Forum

Huawei and Cyber Security

"Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. …
It（Cyber Security）is for our survival."

- To meet our customers' security and assurance requirements with transparency
- To strengthen – and promote transparency about – Huawei global and US assurance programs among customers and stakeholders.
- To promote adoption of a fact-based, risk informed, transparent, level-playing field for ICT products and services

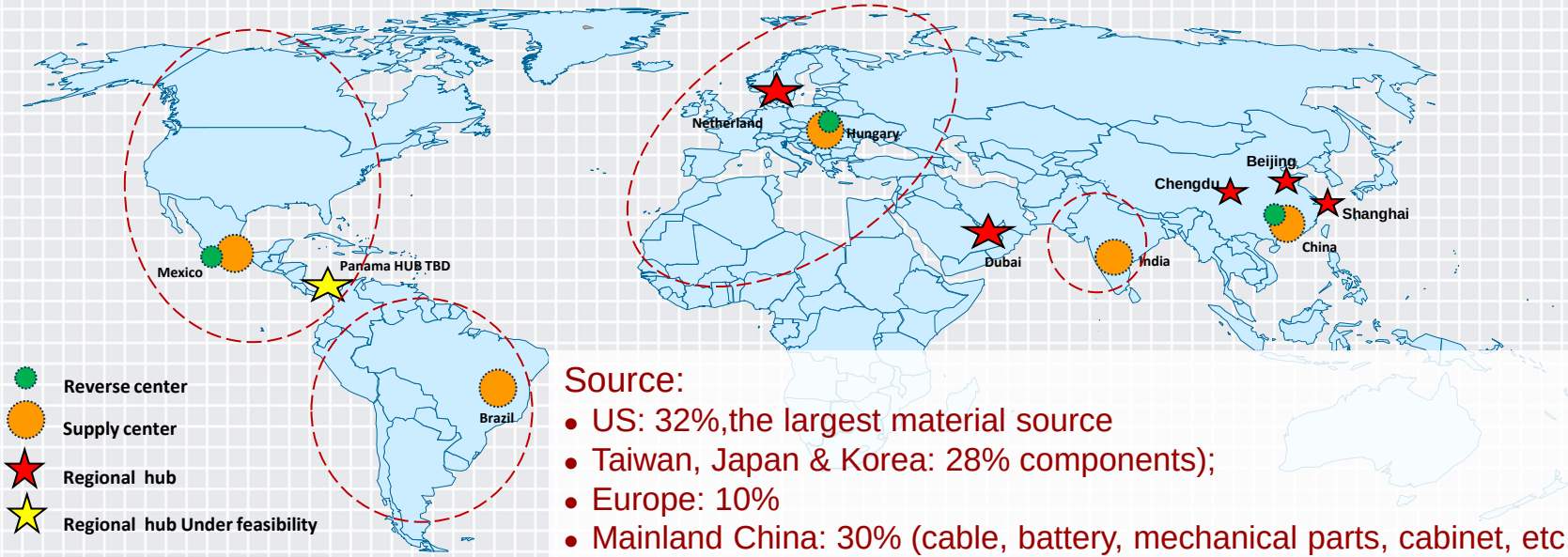
Huawei and Cyber Security
Critical Success Factors for Global Assurance

- Organizational commitment
- Strategy based on addressing future challenges
- Clear governance roles and responsibilities

Huawei and Cyber Security
Critical Success Factors for Global Assurance

- Consistent, repeatable processes
- Robust verification -- “assume nothing, believe no-one and check everything.” Plan, Do, Check, Act.
- Openness and transparency regarding progress, successes, and failures

Huawei Global Supply Network



Source:

- US: 32%,the largest material source
- Taiwan, Japan & Korea: 28% components);
- Europe: 10%
- Mainland China: 30% (cable, battery, mechanical parts, cabinet, etc.)

Supply Center

- China (Delivery for the globe)
- Europe (Delivery for West Europe &North Africa)
- Mexico (Delivery for North America & Latin America)
- Brazil (Delivery for South Latin America)
- India (Delivery for India)

Regional Hub

- Dubai (United Arab Emirates)
- Netherlands

Reverse Center

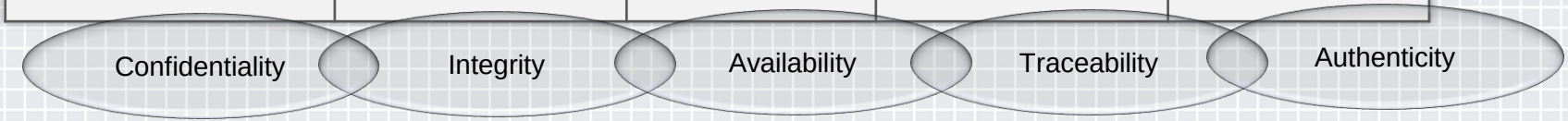
- China
- Mexico
- Europe

Local EMS

- Brazil , Mexico, India and Hungary supply centers work with local partners to do manufacturing and make delivery

Global Supply Chain Threats

Stakeholders / Main Threats	Tainted		Counterfeit	
	Upstream	Downstream	Upstream	Downstream
Malware	√	√	√	
Unauthorized “Parts”	√	√	√	
Unauthorized Configuration		√		
Scrap/Sub-standard Parts			√	
Unauthorized Production			√	√
Intentionally Damage	√	√		



Courtesy of the Open Group

Supply Chain Security Strategy

Objective: E-2-E assurance in all stages of supply chain: trusted material, manufacturing, software, logistics, regional warehousing, and distribution.

Efficiency

- Promote timely and efficient flow of products and services in the supply chain
- Protect the supply chain from exploitation
- Reduce the risks of supply chain interruption.

Supply Chain Security Strategy

Objective: E-2-E assurance in all stages of supply chain: trusted material, manufacturing, software, logistics, regional warehousing, and distribution.

Security

- Ensure products and services integrity in global supply chain.
- Identify and resolve threats early in the process and strengthen the security of supply chain infrastructure, logistics and information assets
- Establish a sustainable supply chain security management system. Identify supply chain risks and work out improvement plans to ensure the supply chain can quickly recover from disruption due to changing threats and risks.
- Establish an accurate and effective traceability system to identify and mark problems at the first time and recover and improve the supply chain quickly and pointedly.

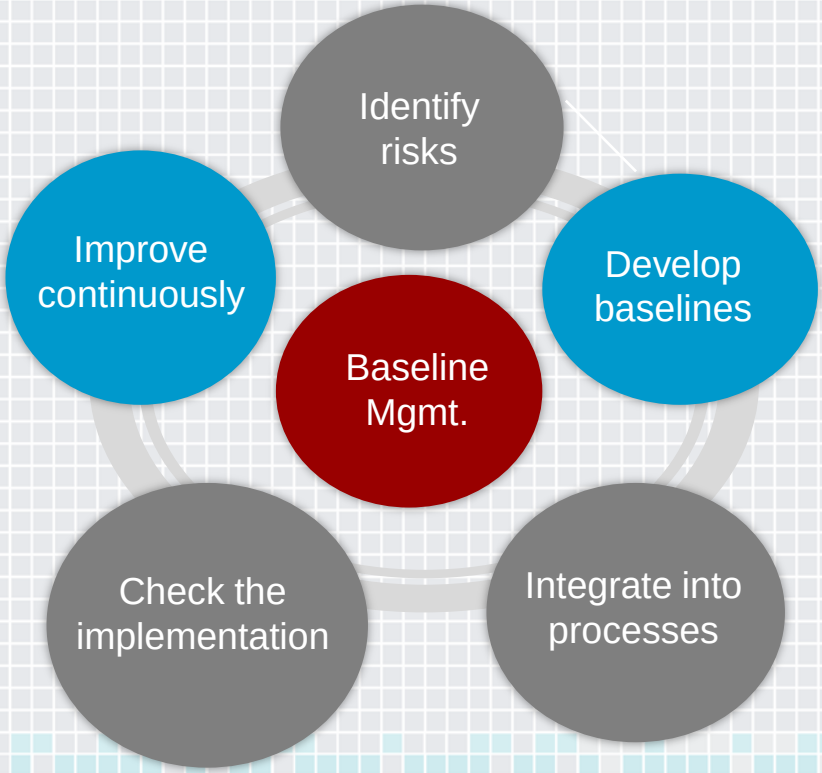
Supply Chain Security Strategy

Objective: E-2-E assurance in all stages of supply chain: trusted material, manufacturing, software, logistics, regional warehousing, and distribution.

Resilience

- Identify supply chain risks and work out improvement plans to ensure the supply chain can quickly recover from disruption due to changing threats and risks.
- Establish an accurate and effective traceability system to identify and mark problems at the first time and recover and improve the supply chain quickly and pointedly.

Supply Chain Cyber Security Baseline Management



Supply Chain Cyber Security Baseline Management

- Based on risks to the supply chain and customer & government requirements:
  - we develop cyber security baselines, aiming to protect product integrity, traceability, and authenticity, and
  - take a built-in approach to integrate the baselines into processes.
- We have developed nearly100 baselines around 10 security elements.

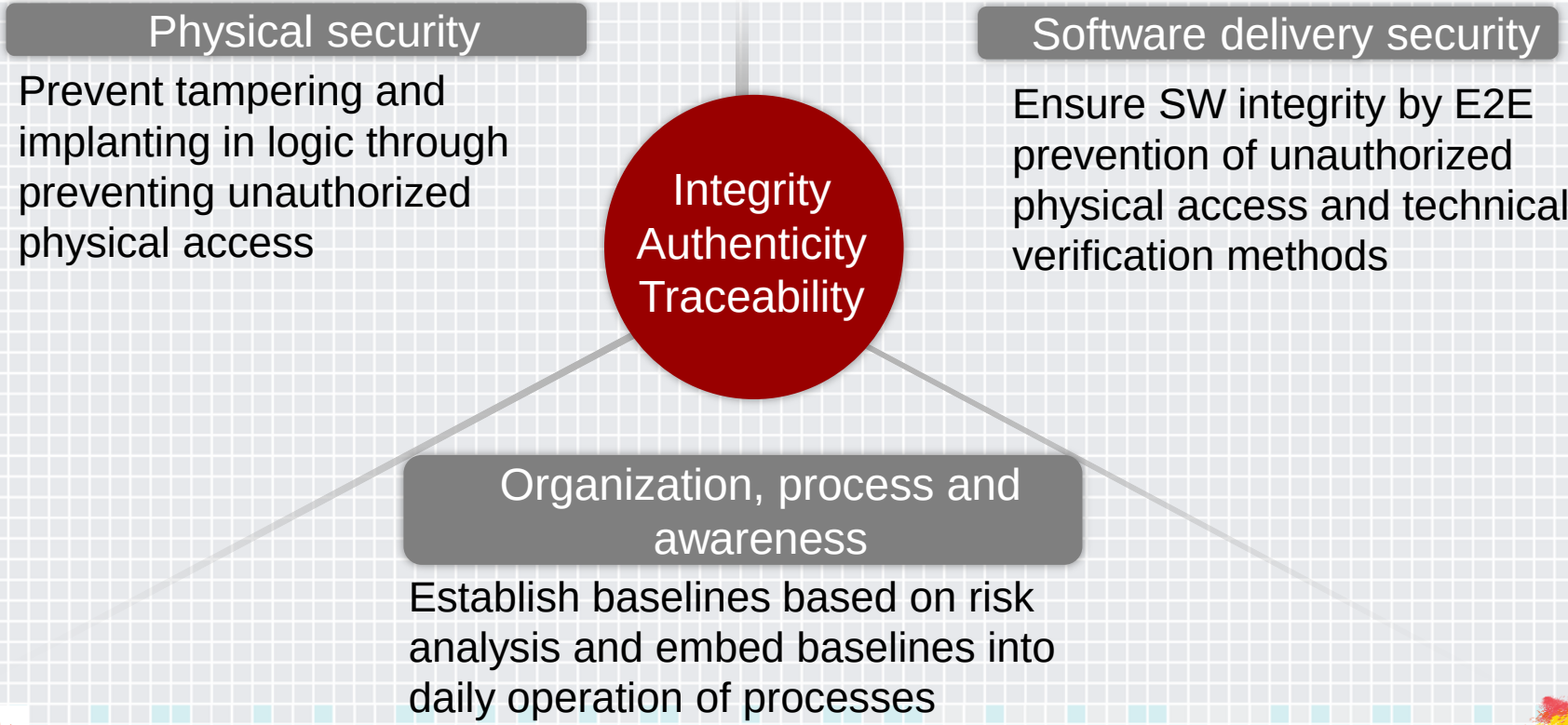
Supply Chain Cyber Security Baseline Management

- Laws and regulations
- Infrastructure security
- Access control
- Incoming material security
- Manufacturing security

Supply Chain Cyber Security Baseline Management

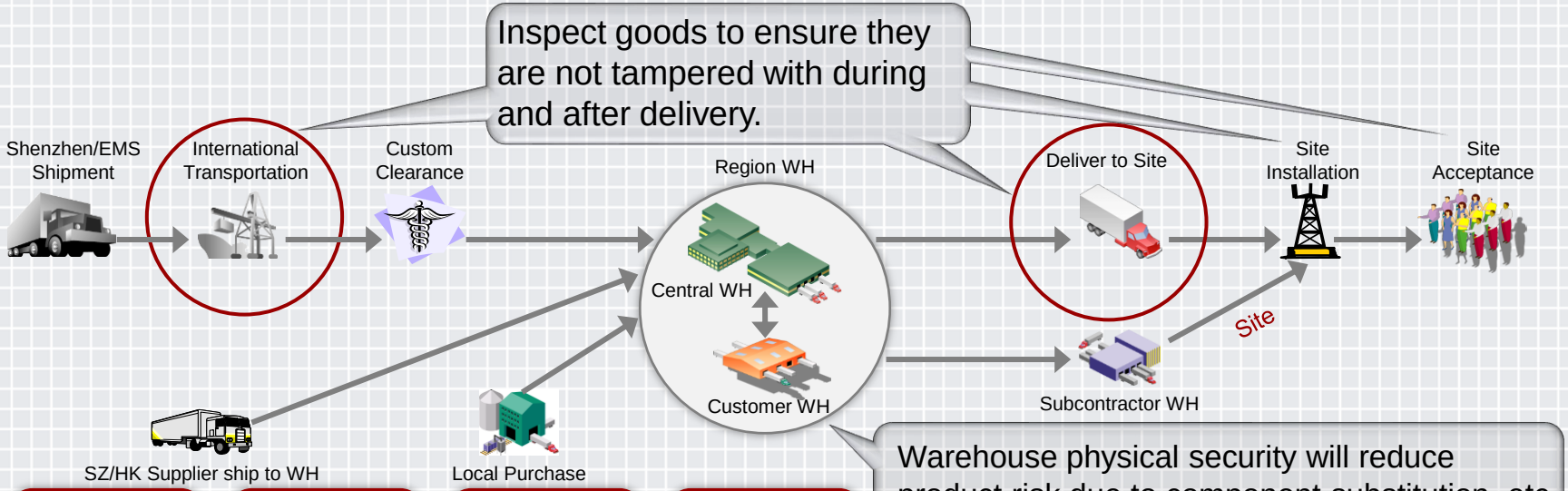
- Software delivery security
- Order fulfillment security
- Traceability system
- Emergency response
- Risk analysis improvement and audit

Framework of SCM Cyber Security Baselines



Supply Chain Management Security

Logistics and return are key areas of security risk.



Integrity and Traceability
Integrated processes/technology in supply chain

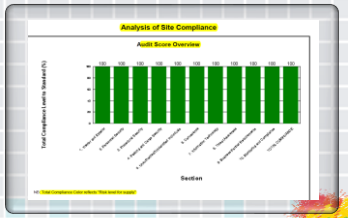
- ISO28000 supply chain security system operating and 3rd certification.
- Global multi-supply centres to provide efficient and resilient supply to customers.
- Barcode system to support tracing

Security of incoming materials	Security of Factory (EMS)	Security of logistics & warehousing

Infrastructure & entry control：7*24 security guard and CCTV monitoring, Electronic entry control & identify identification system

ISO28000 certificate

C-TPAT 3rd party audit report



Manufacturing Security
Ensures product and component security

FT: Function Test
ST: System Test;
IQC: incoming quality control;
IPQC: in-process quality control
PQC: product quality control
FQC: final quality control
OQC: outgoing quality control
PCBA: Printed Circuit Board Assembly

Secure and Efficient Delivery
World-class logistics service providers (LSPs)

Secure logistics solution	• Global-Region-Country logistics solution; • Route security analysis • Business continuity assurance solution
Trusted LSP	• Industry role model, secure main LSP • Sign security agreement
Visualized process	• Visualized transportation process; • IT systems record logistics process details.

Secure and Efficient Delivery
World-class logistics service providers (LSPs) (2)

Standardized Warehouse Mgt.	• Follow C-TPAT • Record barcode when product leaves warehouse • 7*24 security guard & CCTV; Access control
Products reverse Mgmt.	• Return material with customer info. cleared out. • Manage according to government and customer's rules and requirements.

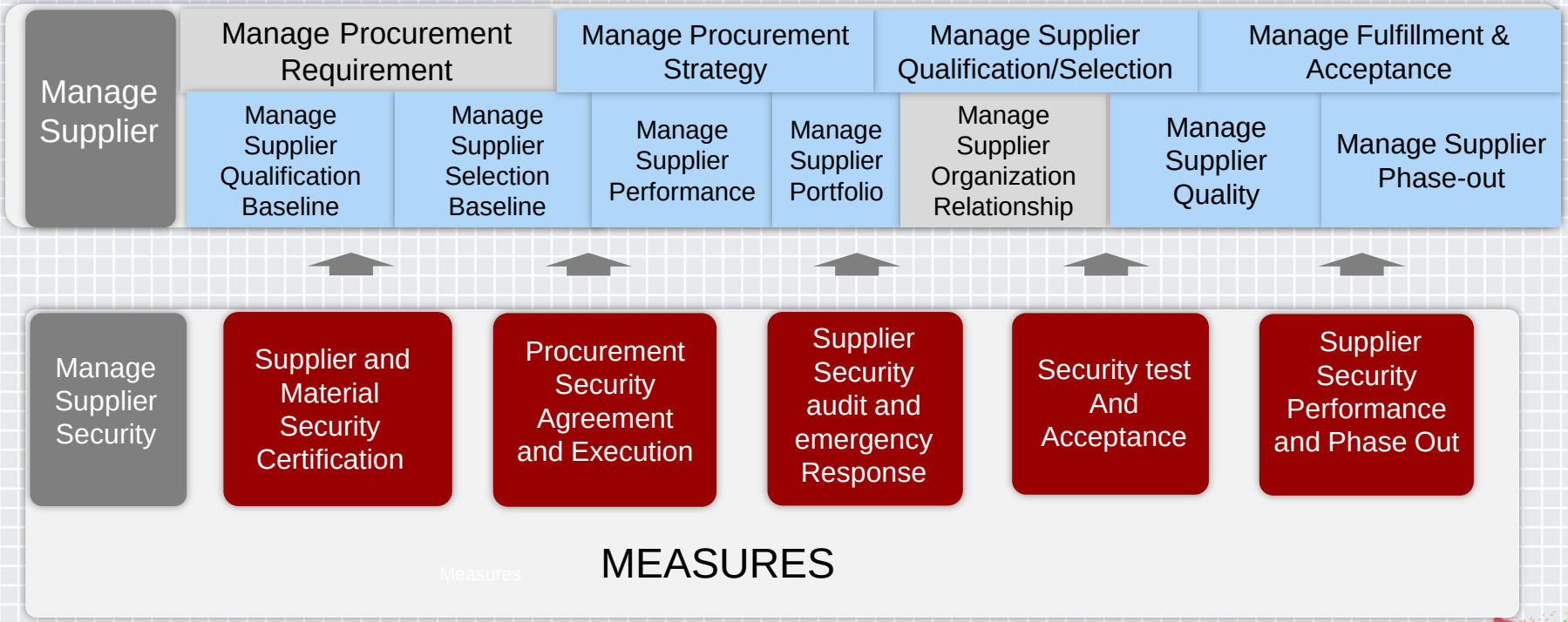
Supplier Management

Reduce potential risks and mitigate security threats

- Security is one of the seven elements of supplier management TQRDCES (Technology, Quality, Response, Delivery, Cost, Environment and CSR, security).
- All Suppliers that are related to cyber security must sign the cyber security agreement, and pass the cyber security system qualification.
- All materials of cyber security must pass the material security test and qualification.

Supplier Management

Reduce potential risks and mitigate security threats



Supplier Management Measures

Manage Supplier Security	Supplier and Material Security Certification	Procurement Security Agreement and Execution	Supplier Security audit and emergency Response	Security test And Acceptance	Supplier Security Performance and Phase Out
Measures	• Procurement security baseline • Material Security Sourcing and Qualification • Supplier Security System Certification	• Sign Supplier Security Agreement • Implement Supplier Security Agreement • Security training	• Supplier • Security Risk and audit • Supplier Security Vulnerabilities improvement • Supplier Emergency Response	• Incoming Material Security Check • Engineering Cyber Security Acceptance • Logistics Security Acceptance	• Supplier Security Performance Evaluation • Supplier Security Performance Application • Supplier Security Phase Out

Supplier Security System Qualification
Cyber Security Evaluation

Supplier cyber security risk evaluation involves a determination of risk, using an audit checklist that includes 10 items, 42 questions, each of which is weighted to contribute to the total score.

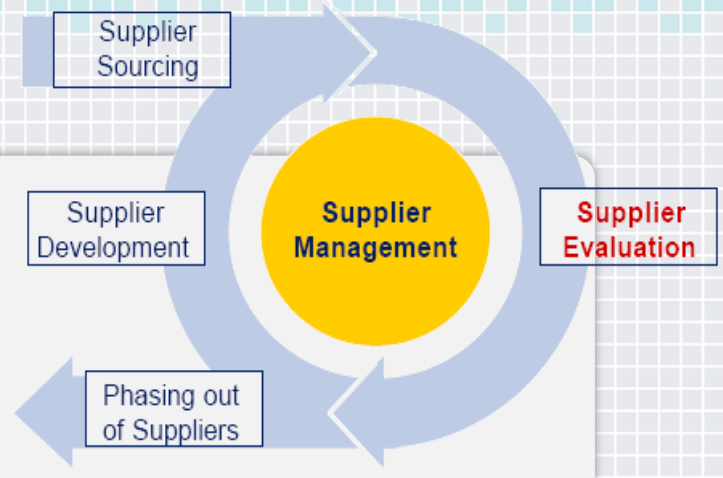
- Security agreement
- Security assurance system
- Product security
- Security testing
- Open source software security
- Delivery security
- Product service security
- Emergency response
- Traceability
- Personnel management

Supplier Security Performance
Scorecard and Product Test

- Appraise the suppliers' performance in security each year and the appraisal result will be applied in the selection and phase-out of suppliers
- Security testing of materials include the testing for selection of new materials, at shipment, and at arrival at Huawei.

Supplier Security Performance
Scorecard and Product Test

- Pass the product security test
- Products do not contain any unknown functions
- Products or services are traceable
- Product security emergency response
- Cyber security training



Sourcing Test

- Material specifications
- Cyber security technical quality risk assessment report
- Cyber security sourcing process

Supplier product test

- Supplier sign security agreement including security test
- Supplier security test

Incoming Materials Test

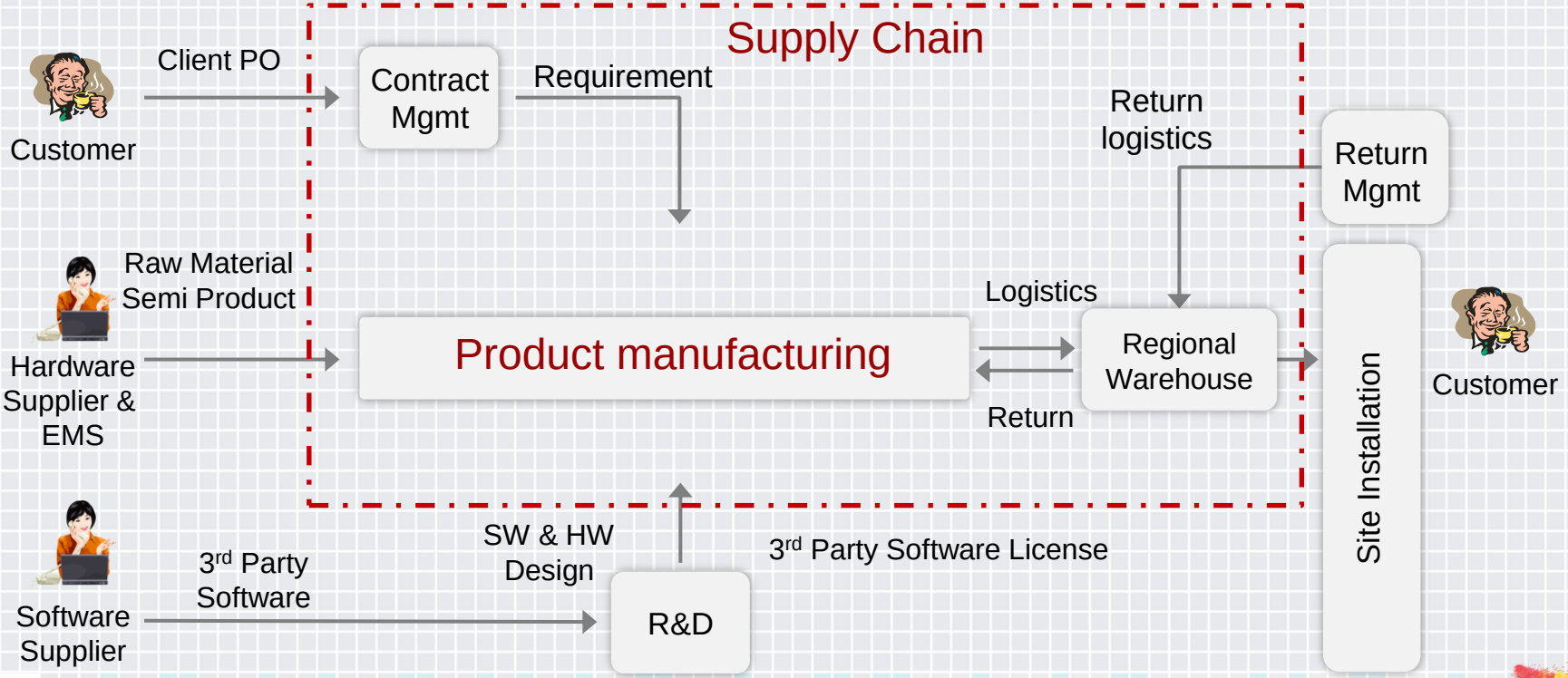
- Perform virus test for cyber security critical materials
- Perform virus inspection and comparison with standard source software for software

End-2-End Traceability System

- Process of product design & contact delivery ensures rapid locating and querying
- We look to:
  - trace every component from every supplier, every route, factory, logistics method, R&D center, and end customer product and back.
  - trace any software request from the customer through every stage in the process, through design, software coding, testing, QA, authorization, live deployment and back to the original source.

Software Development Traceability
From customer requirement to final release.

Product Traceability in Supply Chain
From contract to delivery.



Third Party Supplier Management
Leverage Purchasing Power – *Top 100 Requirements*

End-to-end cyber security means a vendor must work with their own vendors to adopt best practice cyber security approaches.

61. How does the vendor conduct security management with their suppliers? Has the vendor established relevant security criteria and passed them to their suppliers? How frequently does the vendor update their criteria to ensure they keep up-to-date with the latest thinking?
62. What procurement process requirements do the vendor's suppliers take with their suppliers?
63. Does the vendor have contractual clauses or security agreements in place with their core technology suppliers that provide a comprehensive, risk informed set of requirements that they must meet?

Conclusion

- There is no simple, cookie-cutter approach to understanding and managing supply chain risk.
- Managing supply chain risk appropriately requires organizational commitment and a comprehensive end-to-end approach based on standards and best practices with independent verification for each critical component.
- Agreement on a global supply chain standard, such as the Open Group OTTPS, could contribute to reduction in supply chain risk and increased trust.

Apply What You Have Learned Today

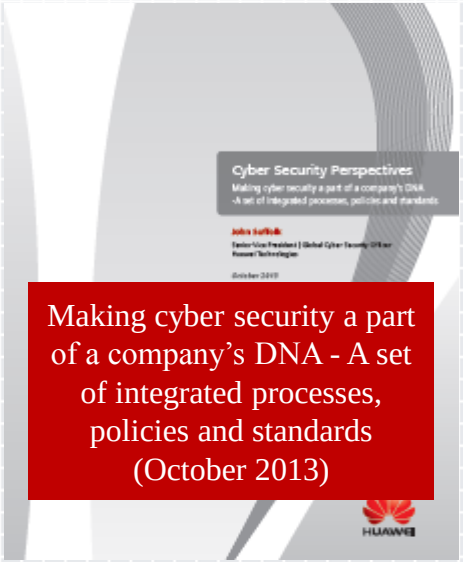
- Next week you should:
  - Determine if/how you address supply chain risk within your organization and the security risk of your suppliers.
- In the first three months following this presentation you should:
  - Assess the adequacy of your supply chain risk controls and your security requirements for your suppliers
  - Review the Open Group Trusted Technology Provider Standard (OTTPS)
  - Review the Huawei security papers, Making cyber security a part of a company's DNA - A set of integrated processes, policies and standards (October 2013), and Top100 cyber security requirements.
  - Implement a supply chain risk mitigation strategy appropriate to your risk, including risk-informed security requirements for your suppliers.

Huawei and Cyber Security

Huawei's cyber security White Paper series

2012

http://www.huawei.com/ilink/en/download/HW_U_202577



2013

http://www.huawei.com/ilink/en/download/HW_310547

2014

http://www.huawei.com/ilink/en/download/HW_401430