Huawei Cyber Security -- Strategy and Approach

Jaap Meijer
CSO Huawei Technologies
Email: jaap.meijer@huawei.com
Mobile: +31 6 2612 0985

HUAWEI TECHNOLOGIES CO., LTD.

Open networks connect the world, facilitate economic exchanges across regions, and promote global trade
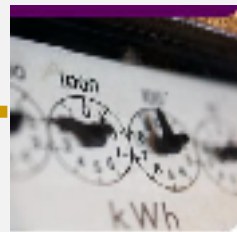
By **2025** ➡ Add **4 Billion** internet users

Produce **100 Billion** connections

In-vehicle Communication & Smart Traffic

Vehicle communication, navigation, tracing, security and maintenance
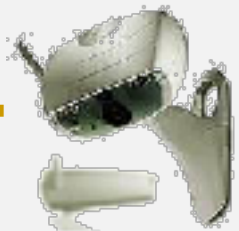
Auto Meter Reading

Remote meter reading is safer and easier. Benefit for Green City construction

Merchandise Distribution

RFID is used for merchandise trade and garbage sorting mgmt

Remote monitoring & Healthy

Remote Home-caring, Healthy, Safety mgmt

Vending

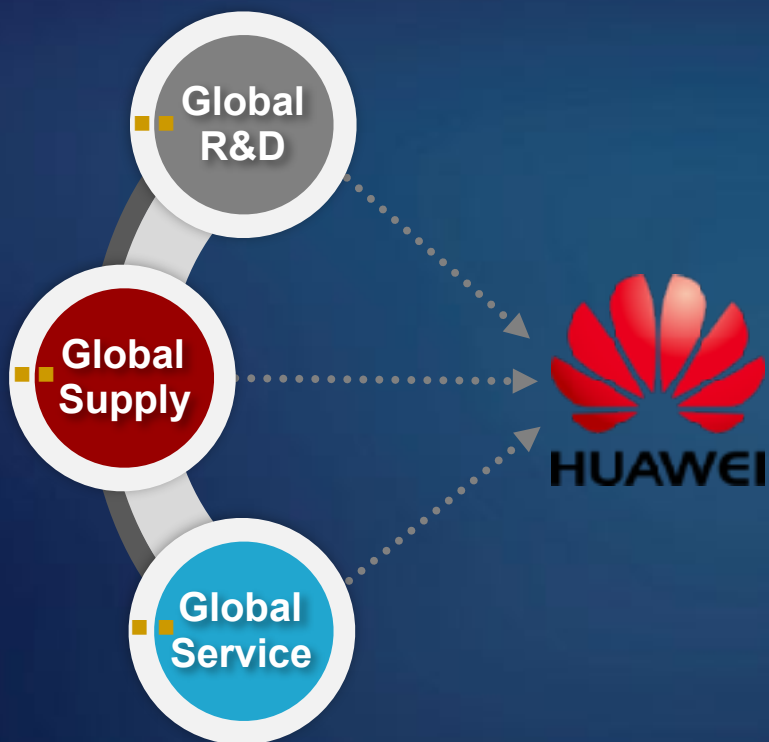Vending, cargos magt, E-wallet mgmt

Electronic Consumer

Info Sharing, on-line game, media download, communication and etc.

We are global – We are facing challenges of global supply chain, cyber security is not a single country or specific company issue

Global R&D

Global Supply

Global Service

HUAWEI

secure products, solutions and services

The Chinese city of Chengdu has 16,000 companies registered and 820 of them are foreign-invested companies. Of these, 189 are Fortune 500 companies. Household brand names such as Intel, Microsoft, SAP, Cisco, Oracle, BAE, Ericsson, Nokia, SAP, Boeing, IBM and Alcatel-Lucent are all located there to name but a few.

Every major telecommunications equipment provider has a substantial base in China：

- Nokia has its biggest manufacturing base globally in China and has 14 wholly owned or joint ventures in China, and its factory in Suzhou manufactures a third of its global production of wireless network products;
- Ericsson's joint-venture Nanjing Ericsson Panda Communications Co. has become the biggest supply centre of Ericsson in the world;
- Cisco also has a huge presence in China, with R&D centres in six major cities, Over 25% of all Cisco products are produced by Chinese partners.

NOKIA

ERICSSON

CISCO

HUAWEI TECHNOLOGIES CO., LTD.

Cyber security is a Huawei crucial company strategy

HUAWEI

■

As a leading global ICT solutions provider, we provide information network products and services. The global network needs to be stable at all times. It is our primary social responsibility to support stable and secure networks for customers in any time.

"Huawei hereby undertakes that as a **crucial company strategy**... Taking on an **open, transparent and sincere** attitude, Huawei is willing to work with all governments, customers and partners to jointly cope with cyber security threats and challenges ... Our **commitment to cyber security** will never be outweighed by the consideration of commercial interests."

Mr. Ren
Huawei CEO

■ **Our Cyber security vision and mission focusing on the needs of our customers**

Vision   **To provide secure, easy and equal access to information services.**

Mission   **Working internationally to develop the most effective approach to cyber security, establishing and implement an end-to-end customer-oriented cyber security assurance system within Huawei, which is transparent and mutually-trusted, so that we ensure customer's long-term security trust.**

Our current focus is on designing and implementing activities to achieve **9 strategic objectives** imbedded within our processes.
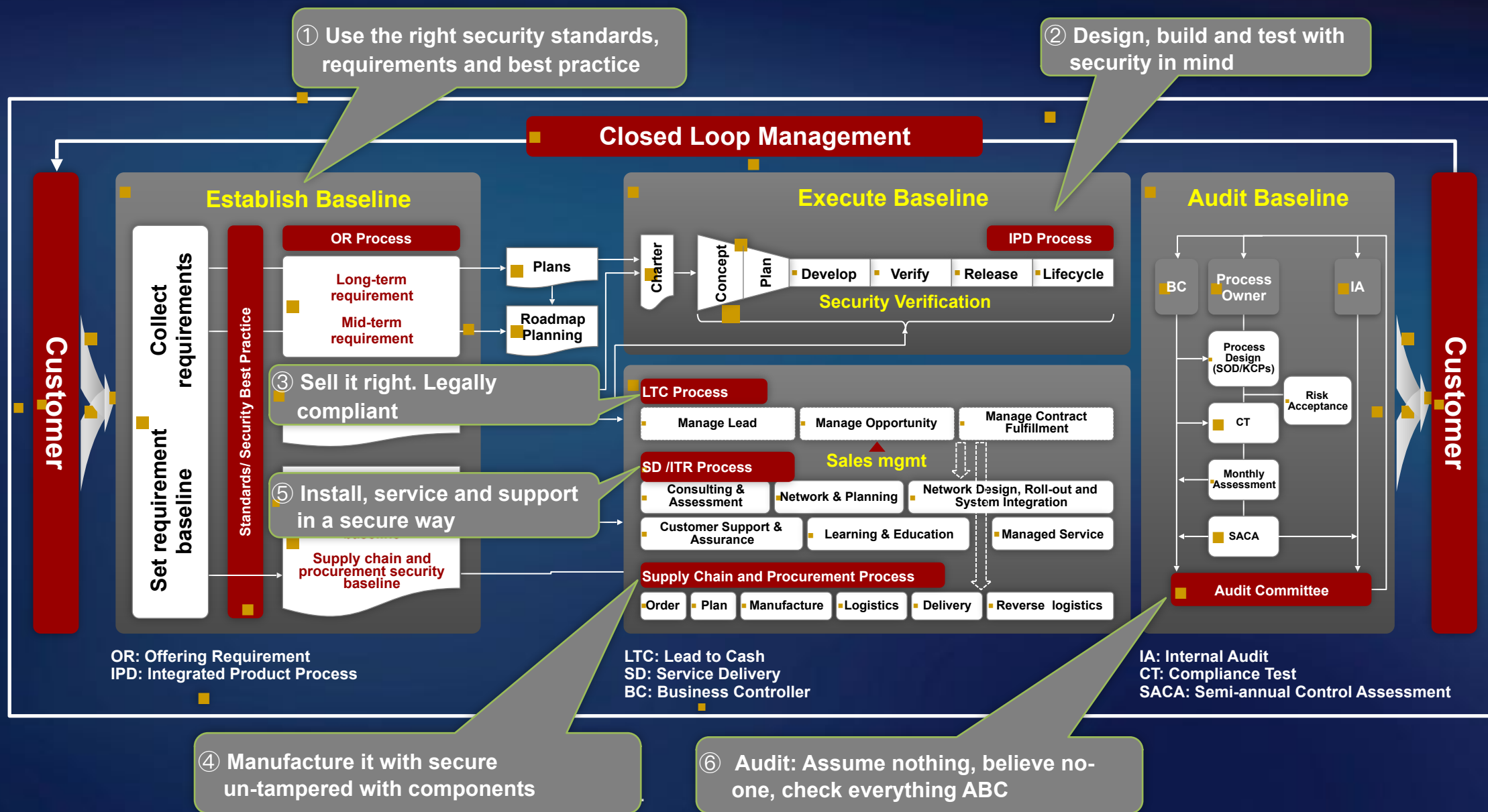
EXTERNALLY FOCUSSED

- OPENESS, TRANSPARENCY AND COOPERATION
- PROACTIVE COMMUNICATIONS
- COMPLIANCE WITH LAWS AND REGULATIONS
- VERIFIED BY INDEPENDENT THIRD-PARTIES
- EMERGENCY RESPONSE

INTERNALLY FOCUSSED

- EMPLOYEE AWARENESS AND RESPONSIBILITIES
- SECURE BY DESIGN, DEVELOPMENT AND DELIVERY
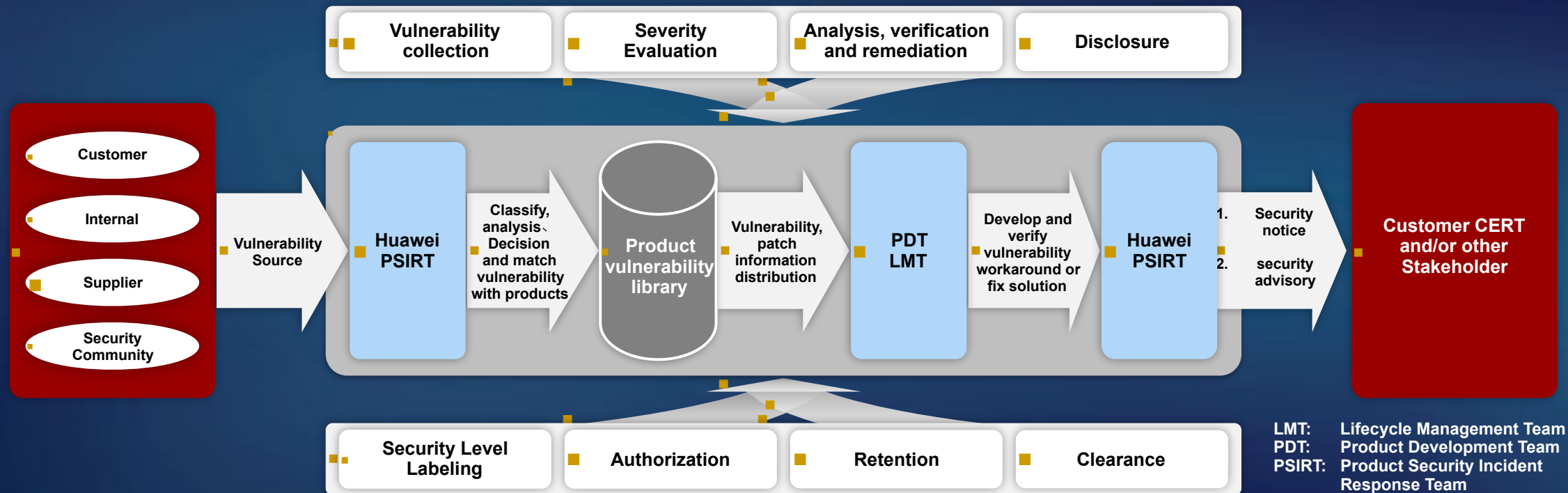- NO "BACK DOOR" AND TAMPER PROOF
- TRACEABILITY

End to End Cyber Security Management covers every process and every part of Huawei's product and services, thus making cyber security a part of Huawei's DNA.

HUAWEI

① Use the right security standards, requirements and best practice

② Design, build and test with security in mind

Closed Loop Management

Establish Baseline

Customer

Collect requirements

Standards/ Security Best Practice

OR Process

Long-term requirement

Mid-term requirement

Plans

Roadmap Planning

Set requirement baseline

③ Sell it right. Legally compliant

⑤ Install, service and support in a secure way

Supply chain and procurement security baseline

Execute Baseline

IPD Process

Charter — Concept — Plan — Develop — Verify — Release — Lifecycle

Security Verification

LTC Process

| Manage Lead | Manage Opportunity | Manage Contract Fulfillment |

Sales mgmt

SD /ITR Process

| Consulting & Assessment | Network & Planning | Network Design, Roll-out and System Integration |
| Customer Support & Assurance | Learning & Education | Managed Service |

Supply Chain and Procurement Process

| Order | Plan | Manufacture | Logistics | Delivery | Reverse logistics |

Audit Baseline

BC — Process Owner — IA

Process Design (SOD/KCPs)

Risk Acceptance

CT

Monthly Assessment

SACA

Audit Committee

Customer

OR: Offering Requirement
IPD: Integrated Product Process

LTC: Lead to Cash
SD: Service Delivery
BC: Business Controller

IA: Internal Audit
CT: Compliance Test
SACA: Semi-annual Control Assessment

④ Manufacture it with secure un-tampered with components

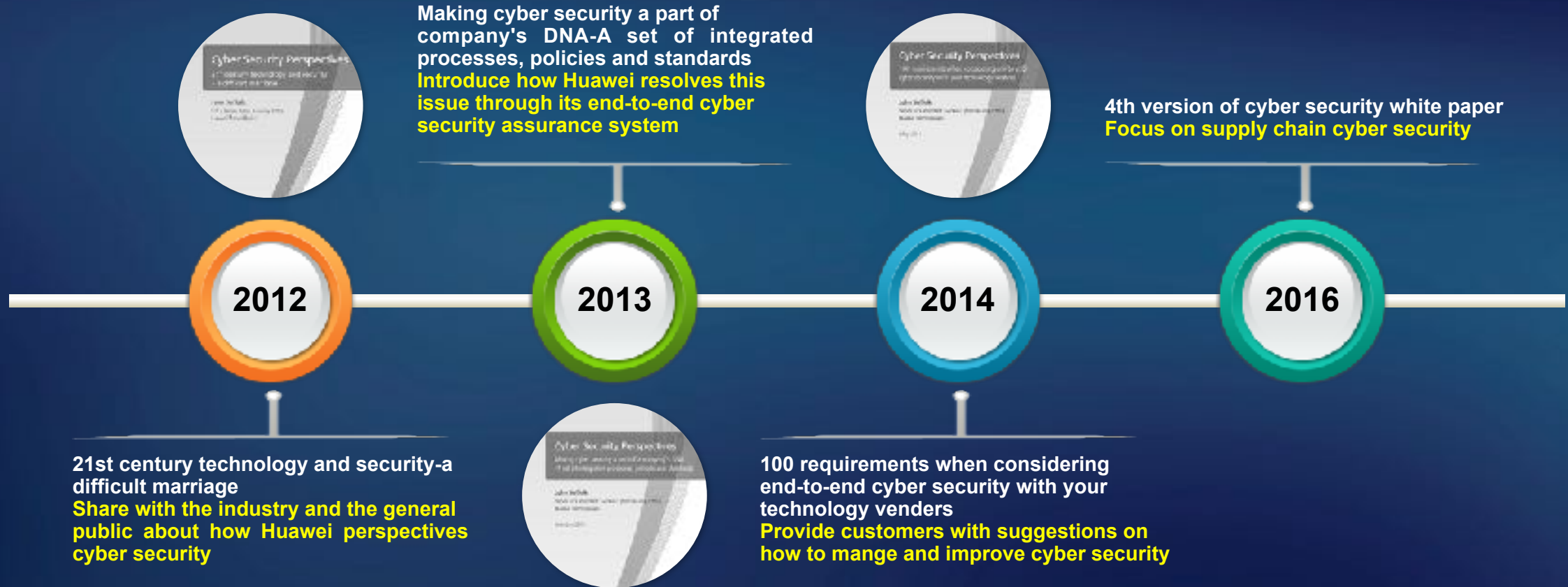⑥ Audit: Assume nothing, believe no-one, check everything ABC

We are enhancing our vulnerability management. We adopt responsible disclosure processes with vendors, CERT organizations and security researchers. We coordinate the resolution of the product vulnerability

- Vulnerability collection
- Severity Evaluation
- Analysis, verification and remediation
- Disclosure

Customer
Internal
Supplier
Security Community

Vulnerability Source → Huawei PSIRT → Classify, analysis, Decision and match vulnerability with products → Product vulnerability library → Vulnerability, patch information distribution → PDT LMT → Develop and verify vulnerability workaround or fix solution → Huawei PSIRT → 1. Security notice 2. security advisory → Customer CERT and/or other Stakeholder

- Security Level Labeling
- Authorization
- Retention
- Clearance

LMT: Lifecycle Management Team
PDT: Product Development Team
PSIRT: Product Security Incident Response Team

- For different BG customers use responsible disclosure: Carrier Network BG, Enterprise Business BG, Consumer Business BG
- Learn from the industry's vulnerability management best practices: CVSS, CPE, CVRF etc.
- PSIRT response to the vulnerability of the self-development, open source and third-party components, speed up response to the vulnerabilities which are already in the wild

A series of cyber security white papers--Cyber Security Perspectives
Remain open and transparent; demonstrate Huawei's policies, challenges, and solutions in terms of cyber security.

Making cyber security a part of company's DNA-A set of integrated processes, policies and standards
Introduce how Huawei resolves this issue through its end-to-end cyber security assurance system

4th version of cyber security white paper
Focus on supply chain cyber security

2012　　　　**2013**　　　　**2014**　　　　**2016**

21st century technology and security-a difficult marriage
Share with the industry and the general public about how Huawei perspectives cyber security

100 requirements when considering end-to-end cyber security with your technology venders
Provide customers with suggestions on how to mange and improve cyber security

Active Engagement with Cyber Security Organizations and Forums

Join in the security groups of standards organizations

Cyber security forums

lists.grok.org.uk

Contributions to cyber security standards

EMUKarp   Lead 4 proposals

SG17   7 Independent proposals
4 WG drafts

SA3   Over 180 suggestions have been adopted

HUAWEI TECHNOLOGIES CO., LTD.

Closing Thoughts： Threats will never stop, we never stop

- The development of networks has helped to advance social progress. Open networks have encouraged information flow and sharing, provided more opportunities for innovations, lowered the costs of innovation, and has helped improve the world's health, wealth and prosperity.

- As a crucial company strategy, Huawei has established and will constantly optimize an end-to-end cyber security assurance system.

- This is a continual effort, and Huawei is committed to providing best-in-class products and services to meet the needs of our customers. We take cyber security seriously and have invested substantial resources into our efforts to promote and improve the ability of our company, our peers and others to provide the best-possible security assurance and ensure a safer and more secure cyber world for all.

- Cyber security is not a single country or specific company issue. All stakeholders – governments and industry alike – need to recognize that cyber security is a shared global problem requiring risk-based approaches, best practices and international cooperation to address the challenge.

Thank you