Security Level:

Capacity Building to Strengthen Cyber Security

—Strategy & Approach

Sept. 2013

www.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Contents

- Cyber Security Challenges and Strategy
- Capacity building to strengthen cyber security
  -Cyber Security Assurance Approach
- Closing Thoughts

Increasing Global Threat in Cyber Space

Government

Secretary Napolitano Unveils National Strategy for Global Supply Chain Security

Dept. of Homeland Security

January 25, 2012

DAVOS, Switzerland– Secretary of Homeland Security Janet Napolitano today unveiled the Obama administrations National Strategy for Global Supply Chain Security [DOWNLOAD PDF] at the World Economic Forum in Davos, Switzerland. The Department of Homeland Security is committed to facilitating legitimate trade and travel, while preventing terrorists from exploiting supply chains, protecting transportation systems from attacks and disruptions, and increasing the resilience of global supply chains.

White House Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure

The President directed a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity. Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities,

Operator

AutomationWorld

NEWS | December 14, 2011

Balancing Security, Compliance and Operational Management

Print Email

Disappearing air gaps and growing network connectivity increase the burden of managing security, compliance and operations, according to Industrial Defender's global survey of critical infrastructure operators regarding cyber security.

Sprint

10 August 2011

Sprint and McAfee Offer Customers Mobile Security Applications to Help Protect Information on Their Wireless Devices

McAfee Mobile Security Technology Provides Malware Protection, Device Recovery and Backup

Application Readily Available to Customers in Sprint Zone

OVERLAND PARK, Kan. & SANTA CLARA, Calif. (BUSINESS WIRE), August 10, 2011 - Sprint (NYSE: S) and McAfee announced today that they are providing Sprint customers easy access to McAfee® Mobile Security and McAfee® Family Protection Android™ Edition software, which will better help them protect the important information stored on their mobile devices.

As the use of smartphones and tablets continues to grow, Sprint is actively working with developers,

TELECOMPAPER

NTT, Mitsubishi Electric develop cloud computing encryption

Thursday 29 July 2010 | 01:07 CET

Nippon Telegraph and Telephone (NTT) and Mitsubishi Electric have developed a new encryption scheme as a potential solution to the security risks in cloud computing. This new encryption scheme enables sophisticated and fine-grained data transmission/access control for cloud computing environments. The two companies now plan to study how to efficiently implement and utilise this scheme for various applications.

End User

Malware Goes Mobile

The more entry points to your organization's network, the greater the risks. And as more connections and data get shared, the risks only escalate. For example, "the source code for the Stuxnet worm has been leaked onto the Internet," Henry says. "Those sorts of malicious technologies become available, and they get used and reused."

Add to that the exploding popularity of social-media sites such as Facebook, which have become

Software's Soft Underbelly

Software applications enable this mobile extension of the workforce. And a significant quantity of malware exploits vulnerabilities in these apps. In fact, there was a 71 percent increase in application vulnerabilities in software "typically found on endpoint PCs"[2].

> "Attackers exploit 60 percent of application vulnerabilities and 50 percent of all 'critical' vulnerabilities."
>
> – Dark Reading, February 2011

eWEEK

FCC: ISPs Need to Protect Users From Botnets, DNS Fraud, Cyber-Threats

ISPs, experts, academics and other Internet stakeholders need to do more to protect users from botnets, IP hijacking, domain name fraud and other security threats, according to the FCC.

The chairman of the Federal Communications Commission is calling on ISPs and other experts to protect users from the ongoing online security threats.

darkREADING

Protect The Business Enable Access

Most Enterprises Face Increased Malware Risk From Social Media

Fifty-two percent of companies say use of sites such as Facebook has caused more infections

Oct 06, 2011 | 12:42 AM | 0 Comments

As ICT industry development, Security in cyber space is becoming an imperative concern for governments, operators and end-users.

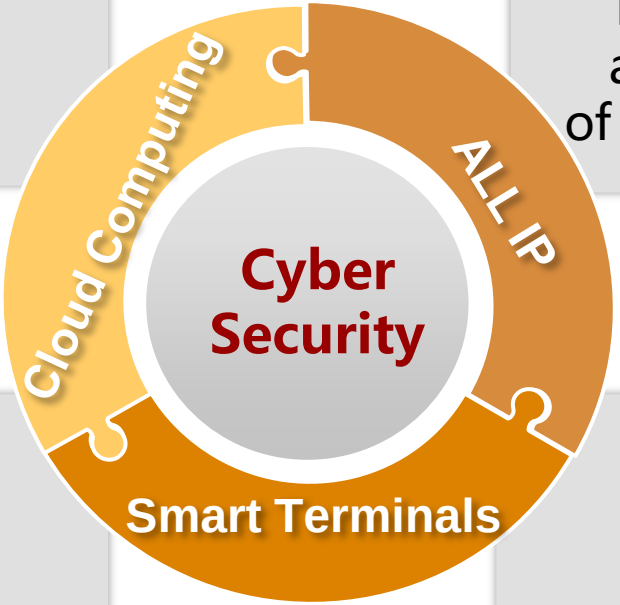
Concerns of All Stakeholder about Cyber Security

Government

Highly-efficient, timely and low cost security system in order to protect strategic interests

Operator

Balance between reputation, security assurance and cost of business operation



End User

High functionality with low security impact, More risk awareness and end user choice

Vendor

Designed to be Secure and trusted for the delivery of services with enhanced security assurance

ICT Vendor shall Take Cyber Security as its Crucial Strategy

Mr. Ren
Huawei CEO

"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."

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

Vision

Facilitating smooth and secure communications among people.

Mission

Working internationally to develop the most effective approach to cyber security, establish and implement an E2E customer-oriented cyber security assurance system within Huawei, which is transparent and mutually-trusted, so that we ensure customer's long-term security trust.

And Specify Security Objectives Accordingly – Both Internally & Externally Focused

Openness, Transparency and Cooperation: actively work with stakeholders in an open and transparent manner to meet and resolve the security challenges and concerns of our customers and Governments.

Proactive Communication: proactively communicating the global nature of ICT and cyber security, encouraging mutual debate with a recognition that we must all positively work together and champion international fair, reasonable and non discriminatory standards, policies and regulation.

Compliance with Laws and Regulations： Huawei aims to comply with security and privacy protection regulation, law and standard of relevant countries and regions, ensure the delivered products and services can withstand legal investigations .

Verified by Independent Parties: We will establish and develop our capability to support worldwide independent test, verification and certification,so that our customers receive internationally recognized security assurance

Security Incident Response： Huawei will keep monitoring threats on our technology and product, so as to be in a position to report or pre-warn our customers, to respond quickly and apply appropriate security measures to resolve issues.

For example,
- Internally Focused Objectives

Employees' Awareness and Responsibilities:

- To raise employees' cyber security awareness based on law, to make them understand they need to bear the liability for their behaviors even without malicious intention;
- For all critical positions, appropriate security qualifications must be obtained;
- Taking measures to deter employees from malicious intention and prevent the occurrence of malicious acts.

Secure by Design, Development and Delivery:

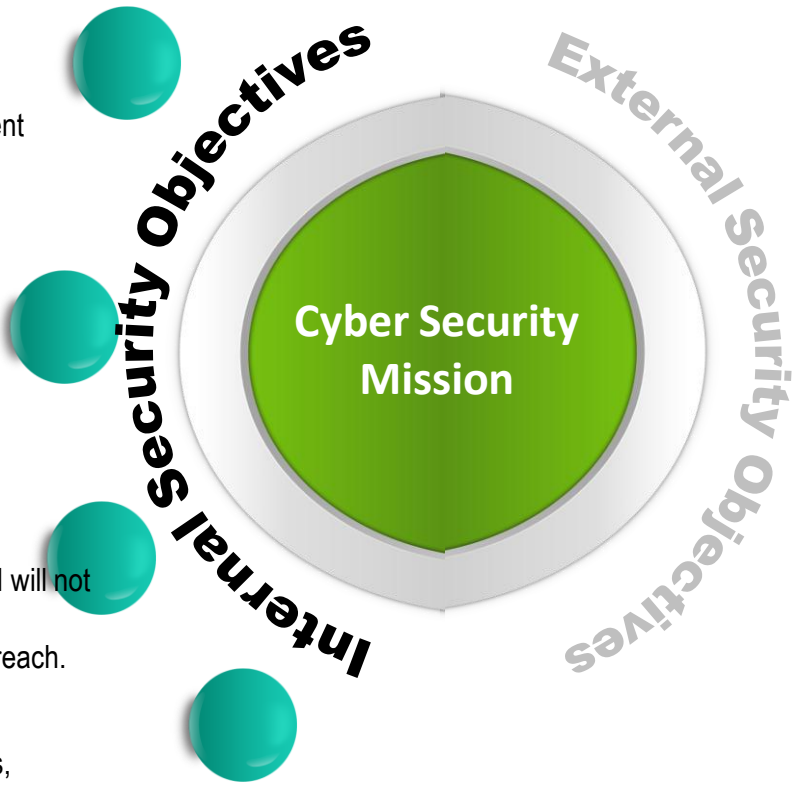
- To embed security assurance into our IPD processes, product design, development and delivery.

No "Back Door" and Tamper Proof:

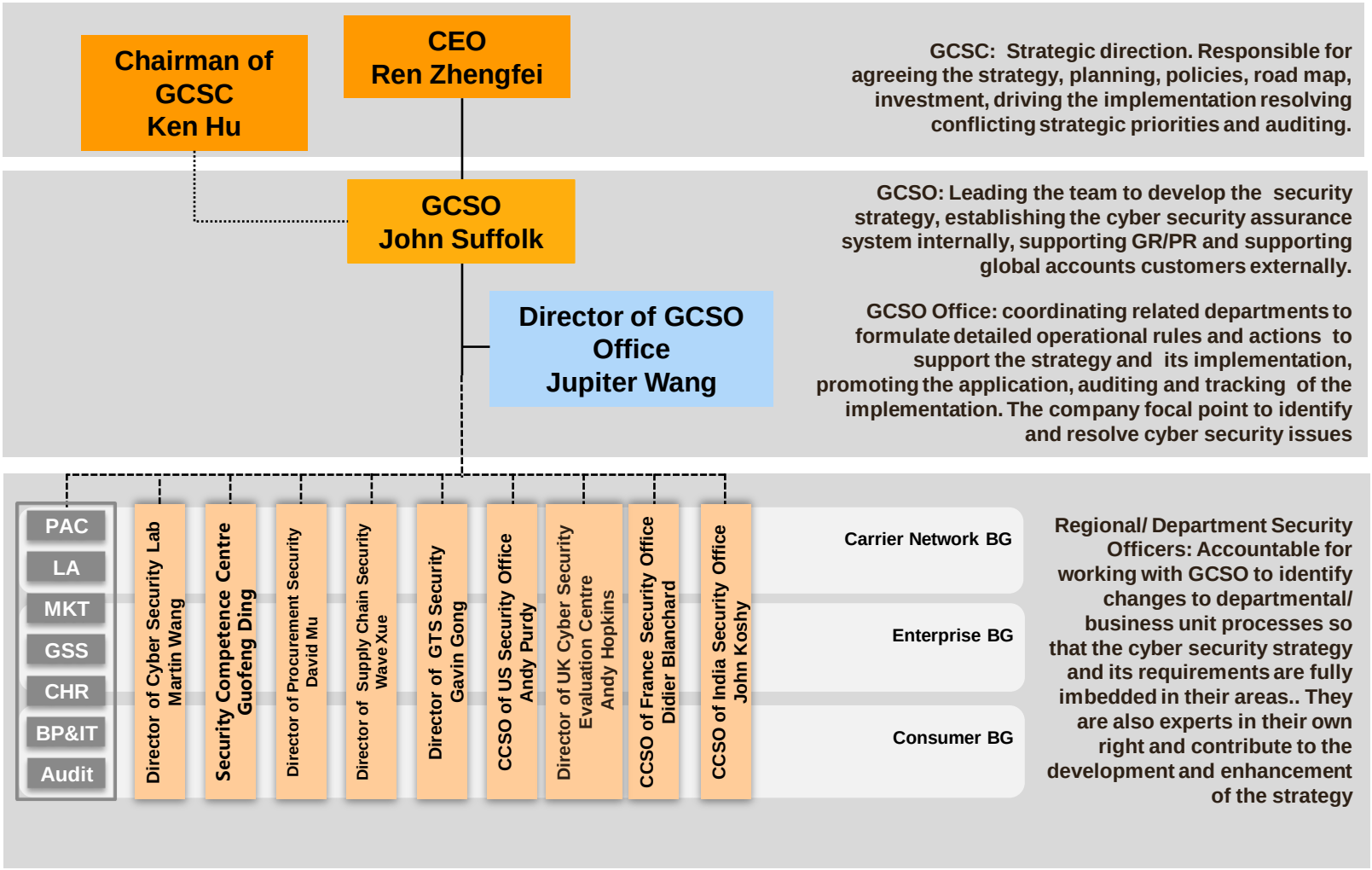
- To prohibit "back door" in product implementation;
- Strictly manage the remote access from China to sensitive countries and will not transfer data from customers' network;
- To protect software integrity and prevent software from tampering and breach.

Traceability:

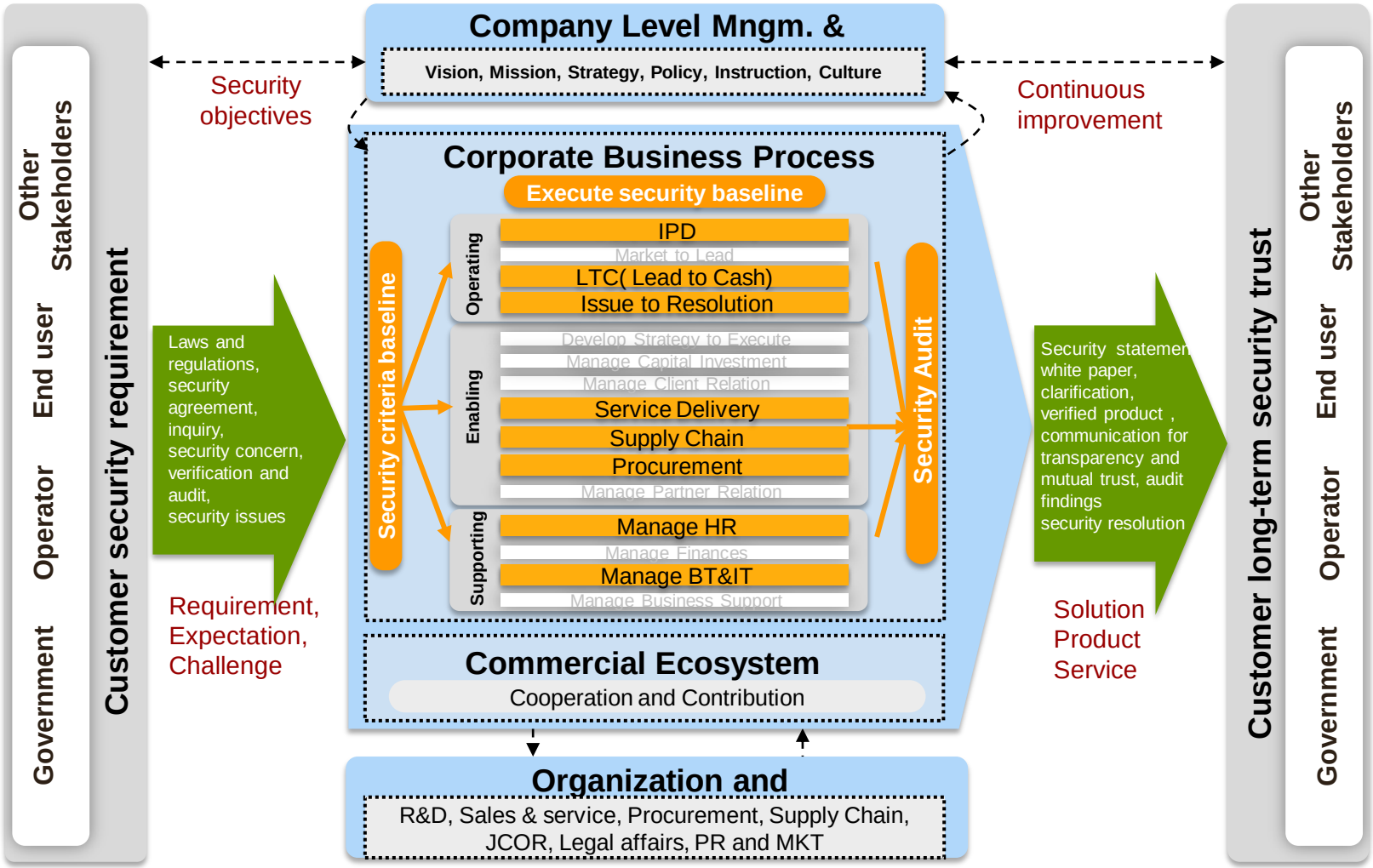
- Through professional integrity management tools, to make our products, solutions, services and components traceable throughout the complete product lifecycle.



Define Cyber Security Governance, Roles and Responsibilities Clearly



Cyber Security Assurance System shall be Integrated into the Core Business Processes



Contents

- Cyber Security Challenges and Strategy
- Capacity building to strengthen cyber security
  -Cyber Security Assurance Approach
- Closing Thoughts

First, you must comply with all of the applicable laws and regulations in every jurisdiction

Huawei hereby undertakes that as a crucial company strategy, **based on compliance with the applicable laws, regulations, standards of relevant countries and regions, and by reference to the industry best practice**, it has established and will constantly optimize an end-to-end cyber security assurance system. Such a system will incorporate aspects from corporate policies, organizational structure, business processes, technology and standard practice. Huawei has been actively tackling the challenges of cyber security through partnerships with governments, customers, and partners in an open and transparent manner.

Core Interests protected by the Cyber Security Strategy

Ren Zhengfei

- **Citizen:** Communication Privacy and Freedom shall be respected and protected
- **Enterprise:** Cyber Space shall operate securely; Protect the Intellectual Property and Business Secrets from theft and disclosure
- **Nation:** focus on security of critical infrastructure; ensure National Security and promote Economic Prosperity

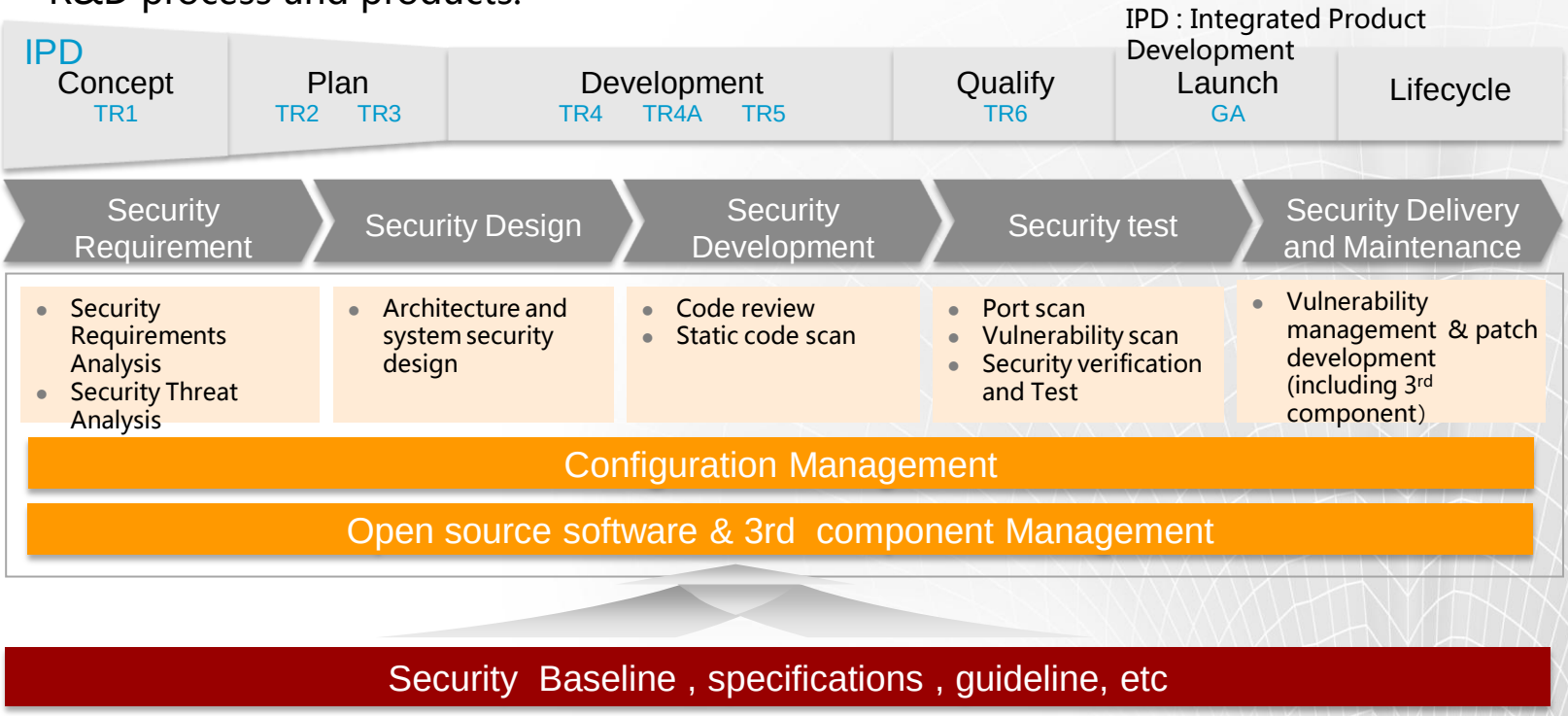
Personal Data and Privacy | **Communication Privacy and Freedom** | **Customer Telecommunication Network and information**

Cyber Security Compliance Strategy and Requirement

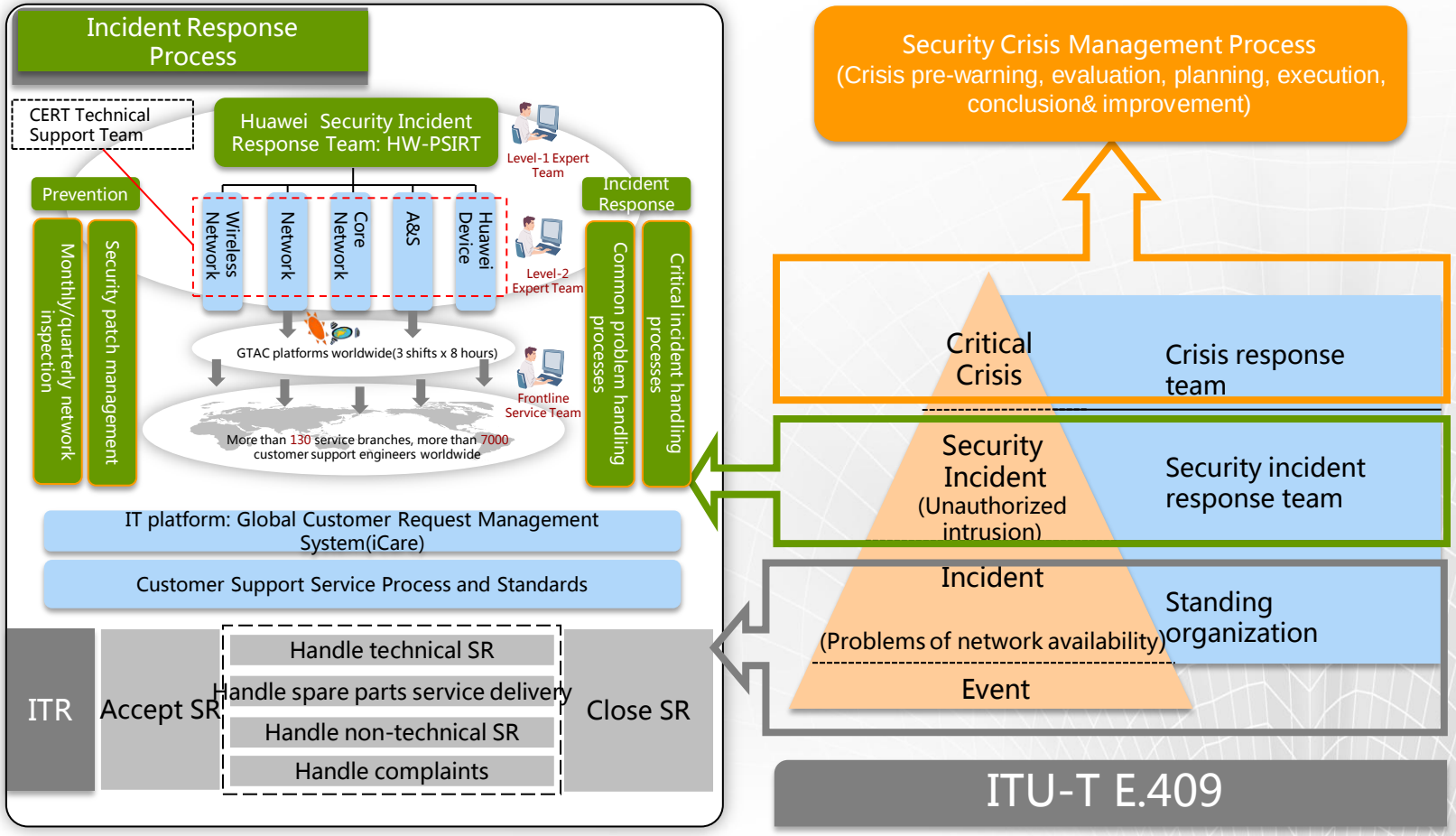
Sales & Marketing | **R&D** | **GTS** | **Procurement** | **Supply Chain** | **HR**

In R&D, you've to reference and optimize excellent practices to build security of products and solutions in the processes

- IPD was introduced in 1997 from IBM which had been implemented and optimized in Huawei in past over 10 years.
- Since 2010, referred industry security practices (OpenSAMM, SSE_CMM ,etc), integrate security activities into IPD process to improve products security.
- Use configuration management to ensure the integrity, consistency and traceability of R&D process and products.

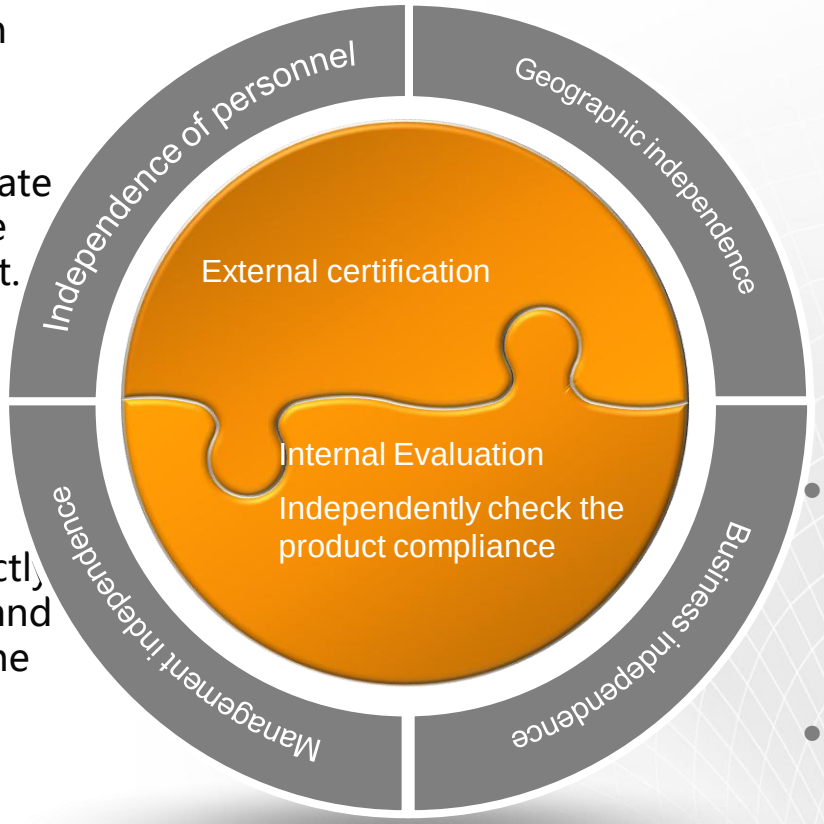


Should there be a security incident you must have a clear process to communicate and resolve the issue



Cyber Security Labs shall be independent from business departments to produce independent and objective reports

- security experts outside of the BGs in the lab.
- Experts can independently evaluate products and release the evaluation report.



- Products can be verified and evaluated by a local 3rd party recognized by the industry.

- Organizational independence: directly managed by GCSO and independent from the BGs.

- Independent from product development; review the quality of the output of main processes;
- Not impacted by businesses; independently carry out testing , Evaluate , verification.

In manufacturing, you shall ensure products and component security and traceability from the processing of incoming materials, production, testing to shipment delivery

Incoming Material

- Appearance check
- Configuration list check
- Performance check
- SW & memory device check

Material setup

- SW server manage
- Set material and check setup Correctness by Task Order
- Record material info.

PCBA Mfg..

- PCBA hardware ver. Confirm
- Manufacture line and process info. Record
- Barcode record

PCBA FT

- SW server daily integrity verifies and virus check
- Separate test network
- SW auto loading
- Digital certificate loading & check
- Barcode record

Maintenance

- Record fault info.& instead material info.
- Standard PCBA test process again
- Test result record
- Barcode record

IQC

IPQC/PQC

Incoming Material

- Base on contract produce
- Separate test network
- SW auto loading and Version control
- Product Virus scan
- Test result record
- Digital certificate check
- Barcode record

Material setup

- Follow C-TPAT
- Trusted staff
- Customer info. protect
- Barcode record

PCBA Mfg..

- Follow C-TPAT
- Trusted staff
- 7*24 security guard & CCTV
- Access control

FQC

OQC

FT: Function Test

ST: System Test;

IQC: incoming quality control;

IPQC: in-process quality control

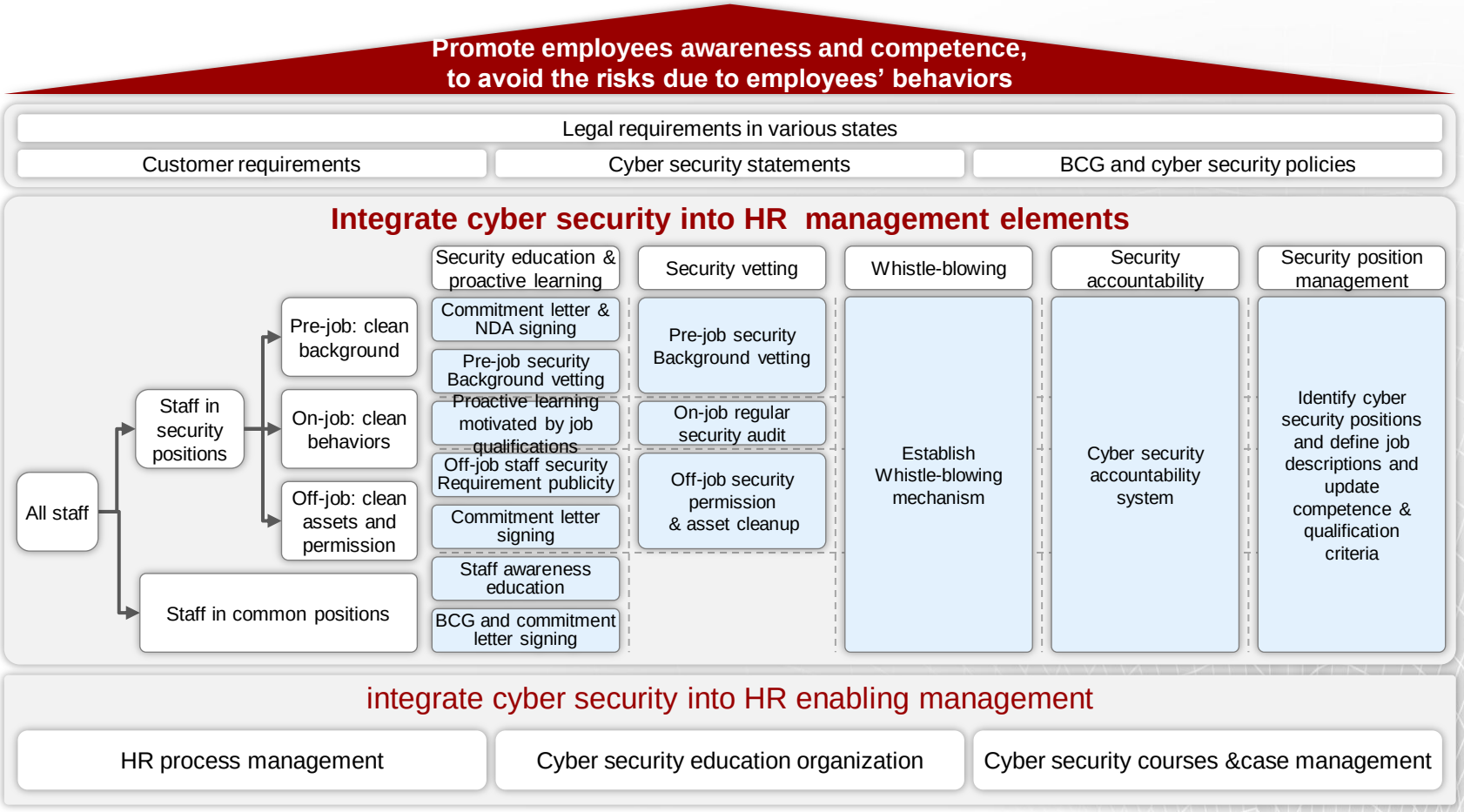
PQC: product quality control

FQC: final quality control

OQC: outgoing quality control

PCBA: Printed Circuit Board Assembly

Finally, employee management is also very important. You shall implement cyber security requirement through establishing accountability and supervision mechanism.



Contents

- Cyber Security Challenges and Strategy
- Capacity building to strengthen cyber security
  -Cyber Security Assurance Approach
- Closing Thoughts

Closing Thoughts： Threat will never stop, we never stop

ICT and Society

The development of networks has contributed to social progress.

Huawei Practice

advocating openness, transparency, and cooperation; building and implementing an end-to-end and reliable global cyber security assurance system

Leverage the social benefits brought by cyberspace and manage the challenges of cyberspace

Cyber security is a common challenge that all of society and the entire world have to confront together.

Common

Governments, the industry, and users need to open up and work together to take their fair share of cyber security responsibilities.

Cooperation

Cooperate to Improve Cyber Security Capacity

Cooperation

•**Governments** should create an environment of trust, transparency, cooperation, and openness conducive to cyber security assurance.

•All parties of the **ICT industry** should be committed to building an end-to-end cyber security assurance system to improve network robustness and resilience.

•**Network users** should abide by laws and regulations, increase risk awareness, and properly protect their personal assets and privacy.

Huawei’ s Practice

•Huawei is a global commercial company. Protecting the cyber security of its world-wide customers is crucial to its fundamental **interests**.

•Huawei has established an auditable, sustainable, and reliable **cyber security assurance system** by integrating security requirements into internal business processes. This system is supported by policies, organizational structures, designated personnel, governance, technologies, and regulations.

•To provide secure, easy, and equal access to information services, Huawei ensures **network robustness and security** through **continuous innovation** and **open cooperation** and has engaged in formulating relevant international standards.

Thank you

www.huawei.com

Copyright©2011 Huawei Technologies Co., Ltd. All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.