



Cyber Security – Strategy and Approach

Making Cyber Security part of your company DNA

David.Francis@Huawei.com

Cyber Security Officer, UK

HUAWEI TECHNOLOGIES CO., LTD.



Today, Huawei is a world-class company

Who is Huawei



- A leading global **ICT** solutions provider
- A **Fortune Global 500** company, ranking 315 in 2013

Employees



- **150,000+** employees worldwide
- **70,000+** engaged in R&D

Market Progress



- **\$39.5B** revenue in 2013
- Serving **45** of the world's top 50 carriers, which account for **77%** of Huawei's revenue generated from the carrier network business
- Serving **1/3** of the world's population

Business Areas



- Carrier
- Enterprise
- Consumer

Huawei in Malaysia



1,900 employees
75 % locally recruited
USD \$80 million annual local procurement



Partnership with all major telecom operators including TM, Maxis, Celcom, DiGi
150 local partners



Southern Pacific Regional HQ is based in Kuala Lumpur
6 offices and **11** sharing centres across the country
1 data hosting and **1** logistic centres in Iskandar



Member of Multimedia Super Corridor in Malaysia, contributing to digital development in Malaysia

Technology has fundamentally helped enhance mankind – better education, better health, better economic output, better lifestyle choices. This is set to continue...



Future = Ubiquitous + Omnipotent

Open networks connect the world, facilitate economic exchanges across regions, and promote global trade. 5G telecommunications technology will increase today's fastest wireless speeds by 100 times – new opportunities and new threats

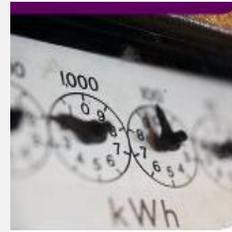
7 Billion People  **50** Billion Machine

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 management

Remote monitoring & Health



Remote home-caring, health, safety management

Vending



Vending, cargos management, E-wallet management

Electronic Consumer



Info sharing, on-line game, media download, communication, etc.

Technology and its use is advancing at an amazing rate and brings substantial benefits to all, but so are the threats to the users of technology advancing

darkREADING
Protect The Business | Enable Access

CISO GUIDE: FISMA Compliance
Do more than just cursory scans. Develop a holistic approach to app security. [Find out how!](#)

Welcome Guest | [Log In](#) | [Register](#) | [Membership Benefits](#)

ATTACKS / BREACHES | VULNERABILITIES | APPLICATION SECURITY
SECURITY MANAGEMENT | STORAGE SECURITY | ENCRYPTION

Panasonic
Ideas for life

INTRODUCING THE NEW TOUGHBOOK H2

- 2nd gen Intel® Core™ i5 vPro™ Processor*
- Hot-swappable twin batteries
- 3G Gobi™ or 4G LTE mobile broadband

E-mail this page | Print this page | BOOKMARK

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](#)

ZDNet
15th Anniversary

News & Blogs | Reviews | Downloads | White Papers

Companies | Hardware | Software | Mobile | Security | Research

iGeneration
Zack Whittaker

Mobile | RSS | Email Alerts

Home / News & Blogs / iGeneration

Microsoft admits Patriot Act can access EU-based cloud data

By Zack Whittaker | June 28, 2011, 8:10am PDT

Summary: Microsoft's UK head admitted today that no cloud data is safe from the Patriot Act — and Microsoft will hand it over to U.S. authorities.

LONDON — At the Office 365 launch, Gordon Frazer, managing director of Microsoft UK, gave the first admission that cloud data — regardless of where it is in the world — is not protected against the USA PATRIOT Act.

Tech Center: Advanced Threats

Topics: Security Views : Advanced Threats Tech Center

E-mail this page | Print this page | BOOKMARK

Advanced Exploitation Of Flash Vulnerability In The Wild

New Flash exploit is extremely effective against the security technologies that many depend on for shelter -- is this a sign of things to come?

Jun 19, 2011 | 05:00 PM | [0 Comments](#)

By Tom Parker
Dark Reading

Not a day goes by lately without a new piece of malware making the rounds, with many anti-virus firms touting collection figures in excess of ten thousand new samples per day. It seems that it is becoming more and more common to see malware leveraging unpatched flaws in client side software: the most common targets, of course, being Web browsers and plugin interfaces that they access. In many cases, while such malware may function as unpatched

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

WIRED | SUBSCRIBE | SECTIONS | BLOGS | REVIEWS | VIDEO | HOW-TO

DANGER ROOM

WHAT'S NEXT IN NATIONAL SECURITY

PREVIOUS POST | NEXT POST

Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video)

By Noah Shapiro | December 17, 2009 | 10:15 am | Categories: Drones

Follow @dangerroom - 25.1K followers

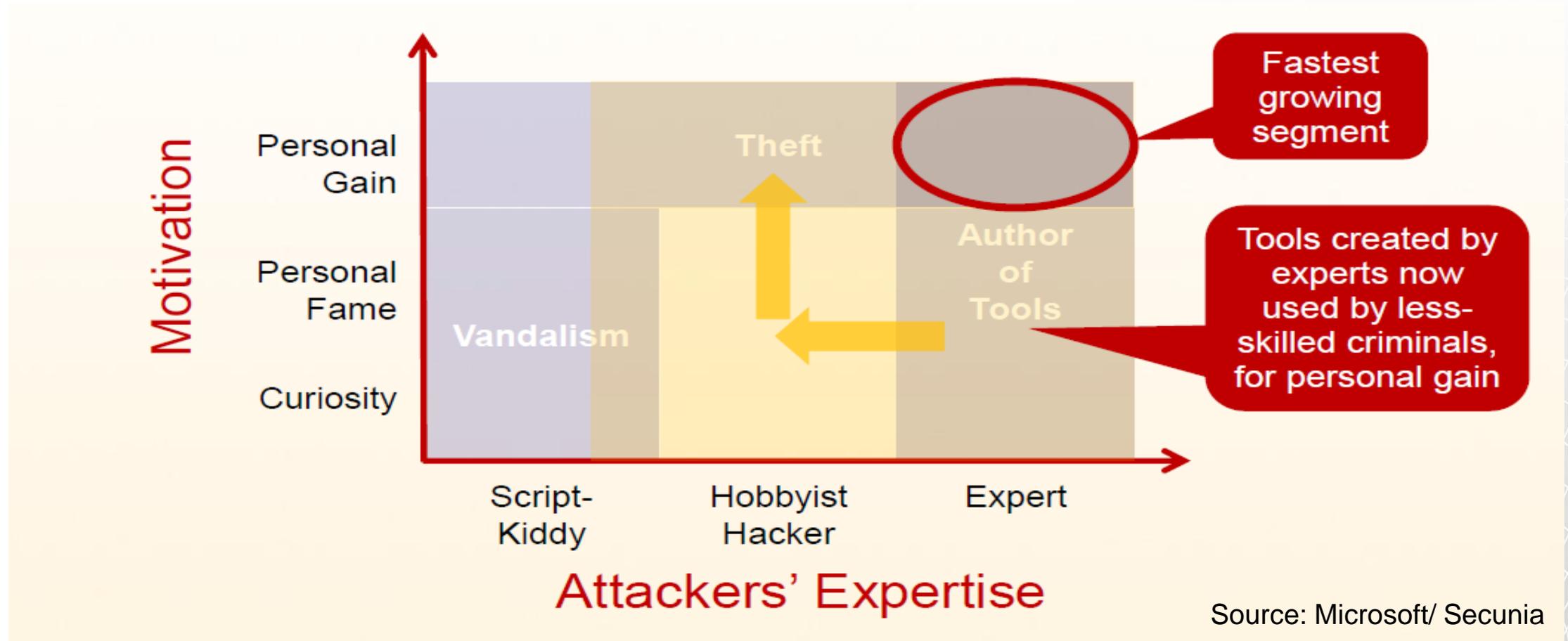
Software's Soft Underbelly

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".

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

- It is hard to stop the tide of progress and technology innovation. Threats are increasing every day.
- The bad guys are getting significantly more sophisticated.
- And international law provides its own security twists and turns.
- And finally it is impacting on almost all hardware and software – even systems not connected to the internet are being breached.

Cyber Security – The threat is changing, roles are changing and the purpose of the attack is changing – politics, protectionism, money and hacktivism

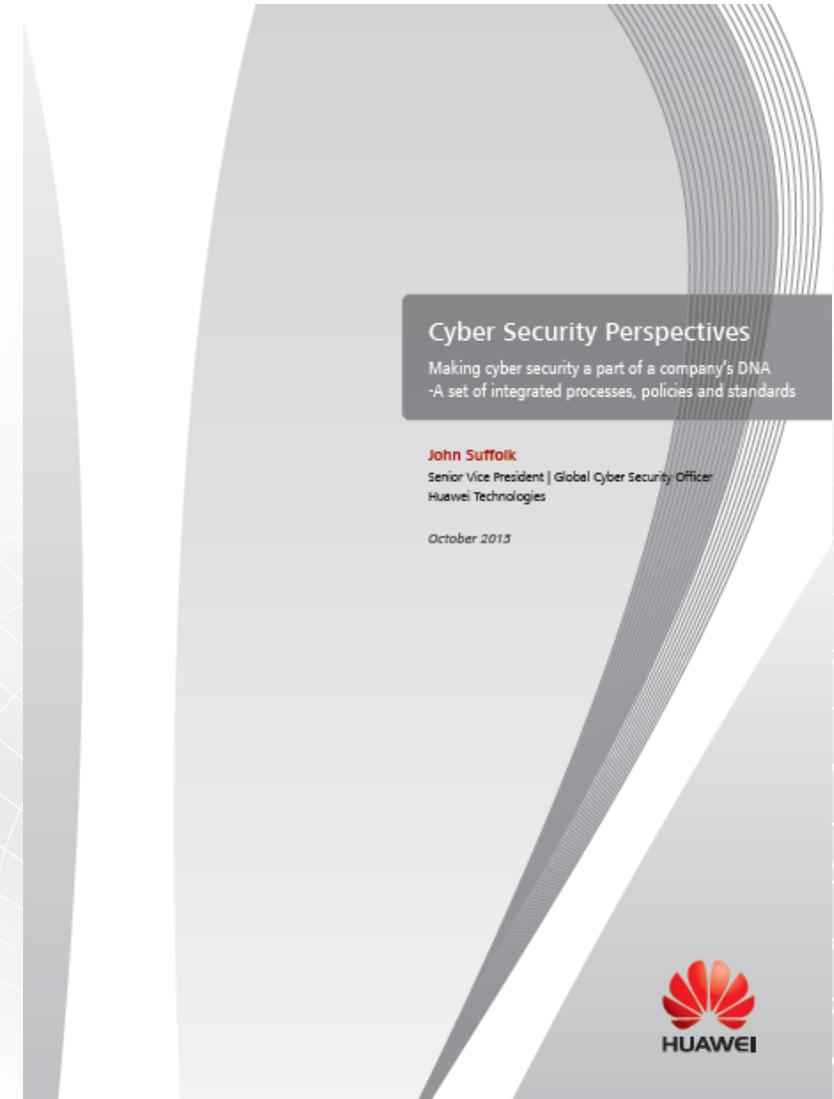


Huawei's Second Cyber Security White Paper

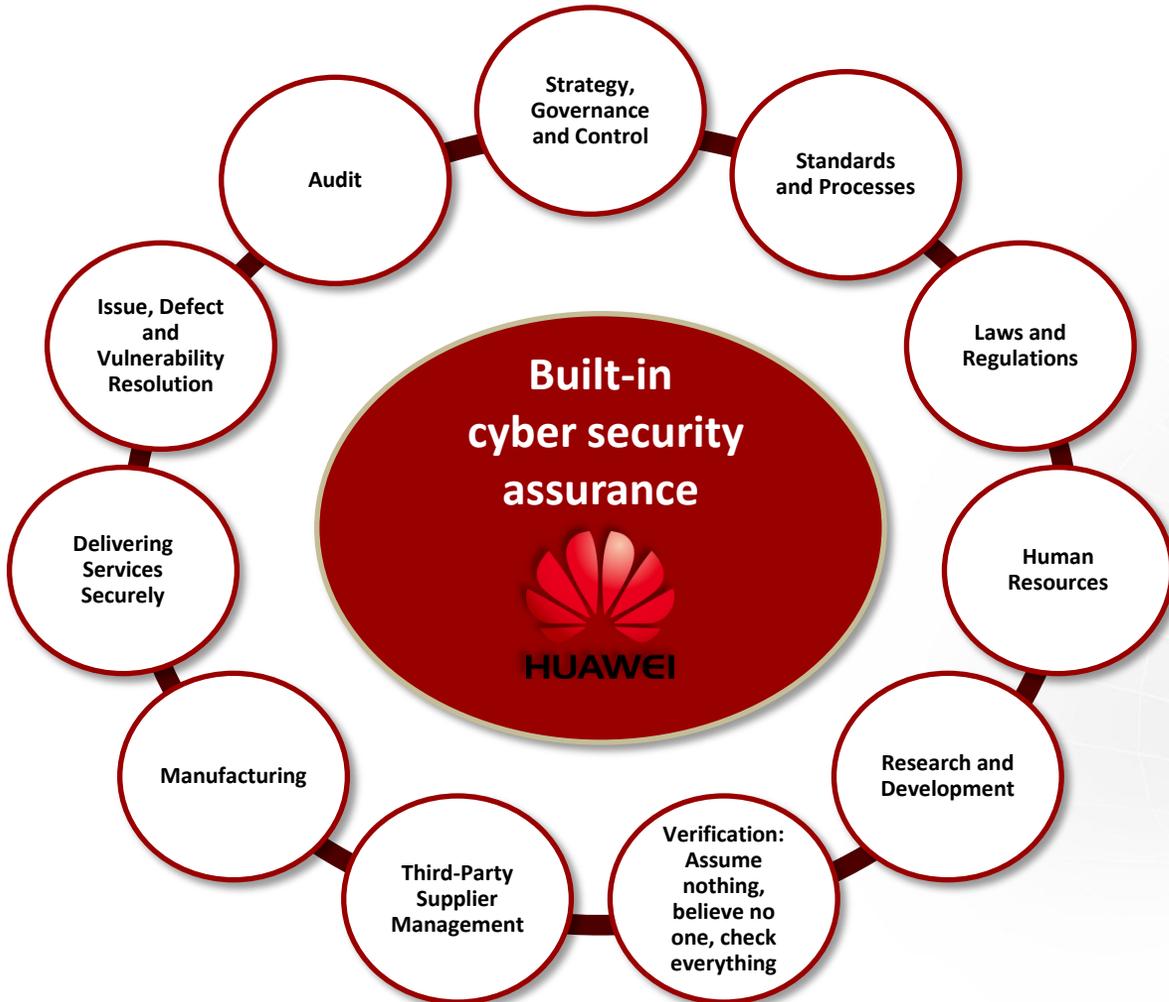
Cyber Security Perspectives

Making cyber security a part of a company's DNA – A set of integrated processes, policies and standards

October 2013

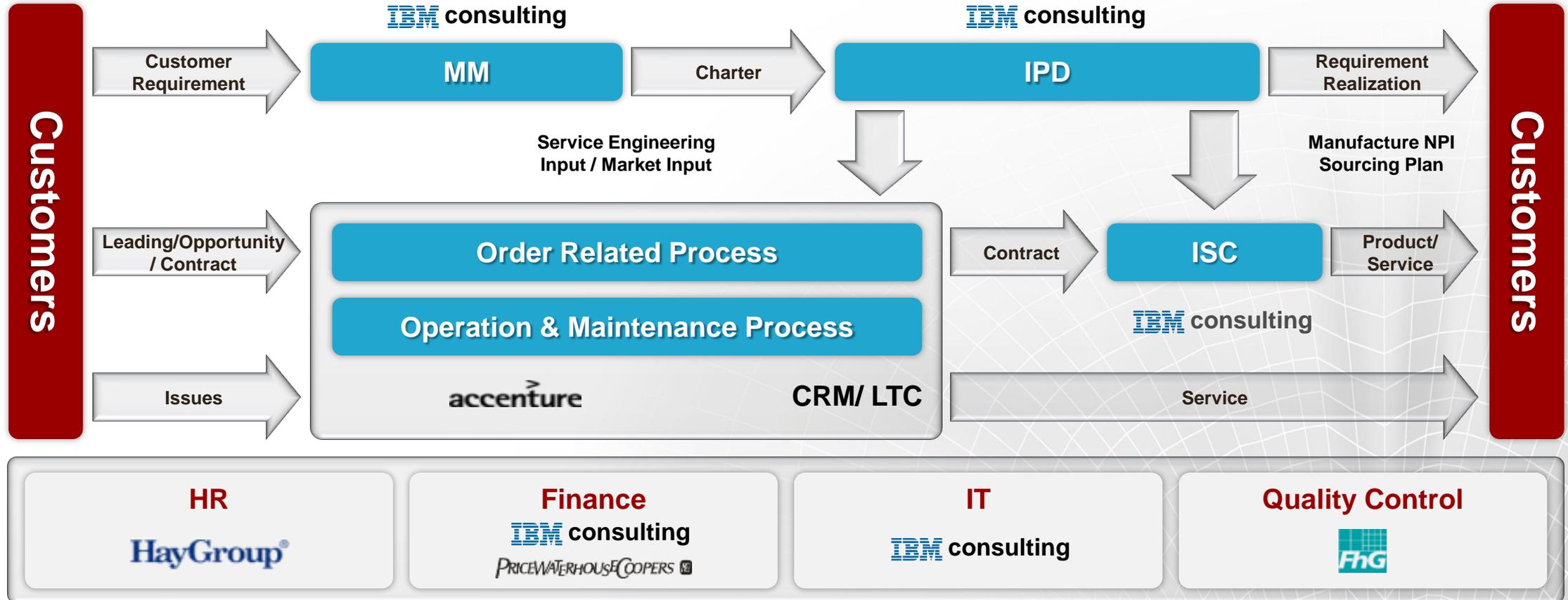


Every part of Huawei, and every person, is included in our “built-in” strategy.



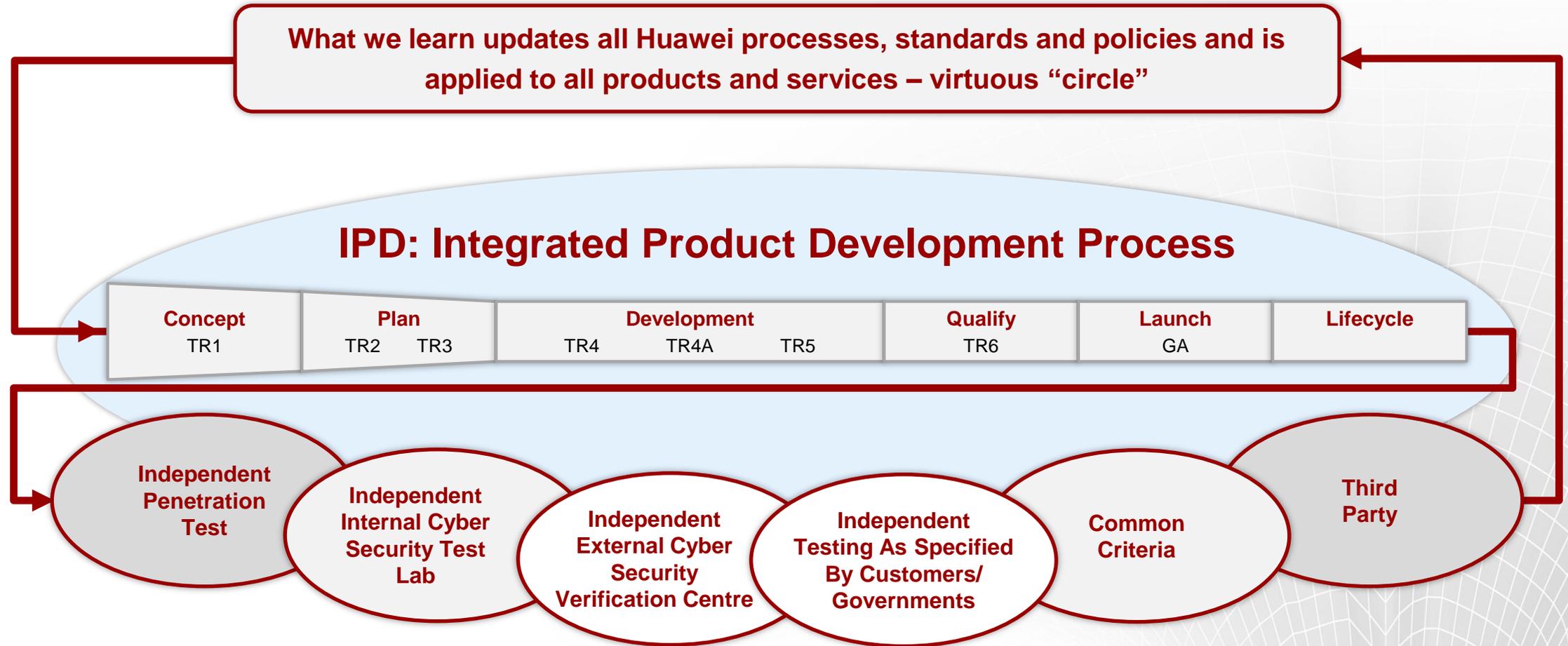
Area	Focus
Strategy, Governance and Control	Having an overall strategy and the accountability to make it happen
Standards and Processes	Using the best standards and approaches to protect against threats and risks
Laws and Regulations	Making your products and operations legally compliant in every country you operate in
Human Resources	Getting the right people, in the right roles with the right behaviour to limit insider issues
Research and Development	Designing, building, testing products in a secure way that builds on the above building blocks
Verification: Assume nothing, believe no one, check everything	Many eyes, many hands many checks. Tiered independent approach to security verification
Third-Party Supplier Management	Getting your suppliers to take security seriously – 70% in the box is not Huawei’s
Manufacturing	Manufacturing products that secure each step along the way – right through to delivery
Delivering Services Securely	Ensuring installation, service and support is secured. No tampering, fully auditable
Issue, Defect and Vulnerability Resolution	As issues arise, solving them quickly and ensuring customers technology is secured
Audit	Using rigorous audit mechanisms to ensure every part of Huawei conform to the strategy

The white paper details our approach to implementing consistently understood, globally rolled-out repeatable processes on which to embed the change – a “built-in” strategy – our corporate processes are the foundation stones

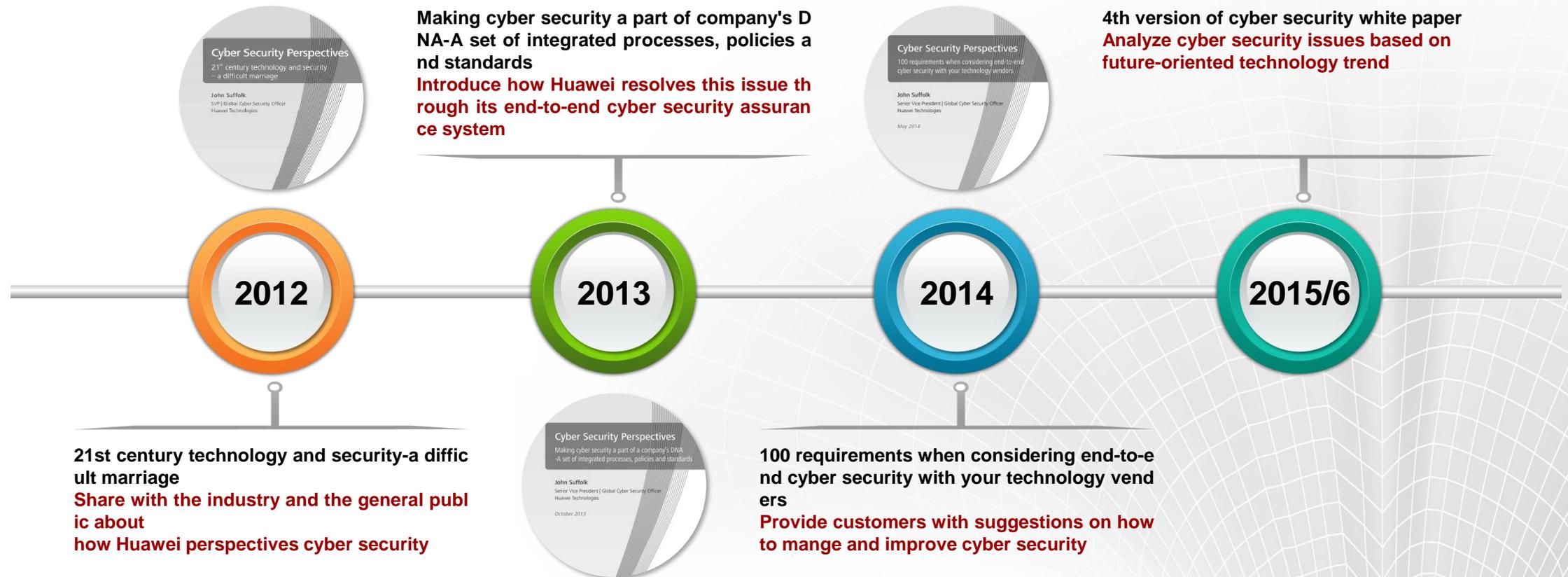


MM: Market Management | IPD: Integrated Product Development | ISC: Integrated Supply Chain | LTC: Lead To Cash

We have created a virtuous circle of “many eyes and many hands” ensuring we continuously improve our knowledge our technology, our people and our processes, this creates a win-win-win process – customers, Government, Huawei

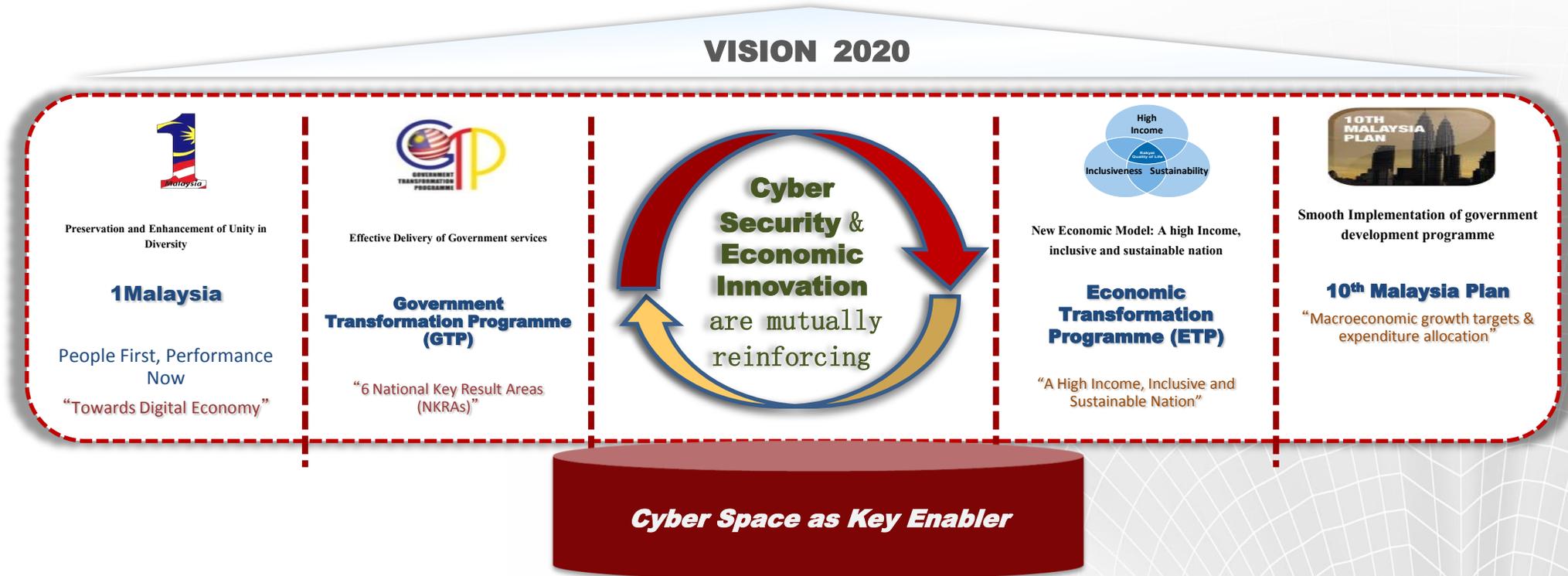


A series of cyber security white papers--Cyber Security Perspectives Remain open and transparent; demonstrate Huawei's policies, challenges, and solutions in terms of cyber security.



Malaysia has developed clear cyber security policies and comprehensive approaches based on the well developed ICT infrastructure

1 HSBB project, **67.3%** broadband household penetration rate, **19.2** million digital citizen



- ❑ The national cyber security policy has been designed to facilitate Malaysia's move towards a knowledge based economy.
- ❑ Cyber Security Malaysia was set up to implement national cyber security policy

Collaborations with Malaysian government

To establish a collaborative relationship on the issue of cyber security between Malaysian Government and Huawei to communicate and implement activities to increase cyber security awareness and improve competence

- **Communication Mechanism:** establish a Steering Committee to respond to the changing external environment on cyber security including technical standards of cyber security, the innovation of ICT technology, the approach to identify and manage potential risks. Meeting twice a year and visit to Huawei.
- **Knowledge transfer:** Cooperate on cyber security knowledge-sharing and training based on Huawei's end-to-end cyber security best practice. Organize cyber security research discussions and meetings routinely.
- **Increase Awareness:** leverage international/regional are to jointly promote cyber security cooperation and dialogue. Jointly develop training courses to increase cyber security awareness across industries.

Closing Thoughts: Threat 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.
- 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.
- 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.

Thank you

www.huawei.com

Copyright©2012 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.