EXHIBIT K

Cyber Security Perspectives

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

John Suffolk

Senior Vice President | Global Cyber Security Officer
Huawei Technologies

October 2013

HUAWEI

Authors

This document has been co-authored by numerous excellent colleagues from around the world. My role has been simple: to edit their fine work into a white paper that clearly and consistently communicates Huawei's position and perspectives on cyber security; I hope I have done their work justice.

I would like to express my gratitude to those who have given me valuable suggestions and made a significant contribution to this document: Jeff Nan (Jianfeng), Jupiter Wang (Weijian), Penny Peng (Liwei), David Francis, Huang Shasha, Andy Purdy, Eric Zhang (Bo), Debu Nayak, March Ma (Hongwei), Peter Rossi, Jerry Liu (Chenxi), Michael Moore, Harry Liu (Haijun), Andy Hopkins, Liang Yonggang, Xue Yongbo, Mu Dejun, Wout van Wijk, William Plummer, Brent Hooley, Olaf Reus, Scott Sykes, Scott Bradley, Ruri Tomioka, Daisy Li (Lidong) Sam Liu (liusong), Brian Liu (Liubin), Ludovic Petit, Ulf Feger and others who contributed to this paper directly or indirectly. Please accept my apologies if I have neglected to name you, and thank you for your contribution.

John Suffolk

TABLE OF CONTENTS

October 2013

1. Foreword 1
2. Executive Summary 2
3. Introduction 4
4. What we said 12 months ago 5
5. Securing the future – security for tomorrow's world 6
6. The problem with standards is that they are not standard 7
   - 6.1 The top 100 things customers ask us about relating to security 8
7. The Huawei end-to-end cyber security approach 9
   - 7.1 Strategy, governance and control 10
   - 7.2 Building the basics: Processes and standards 14
   - 7.3 Laws and regulations 15
   - 7.4 People matter 17
   - 7.5 Research and development 20
     - 7.5.1 Configuration management and the Build Centre 22
     - 7.5.2 Tools and third-party component management 24
   - 7.6 Verification: Assume nothing, believe no one, check everything 24
   - 7.7 Third-party supplier management 27
     - 7.7.1 Supply chain 27
     - 7.7.2 Procurement security 30
   - 7.8 Manufacturing 32
   - 7.9 Delivering services securely 34
   - 7.10 When things go wrong: Issue, defect and vulnerability identification and resolution 37
   - 7.11 Traceability: finding the needle in the haystack 40
   - 7.12 Audit 42
8. Going forward together – pressing the reset button on security 43
9. About Huawei 45

TABLE OF FIGURES

Figure 1, Simplified cyber security governance structure 12

Figure 2, Overall process architecture 14

Figure 3, Imbedding cyber security into Human Resource processes 17

Figure 4, Market Management to Integrated Product Development..... 20

Figure 5, Security imbedded into the IPD process 22

Figure 6, Multi-tiered independent verification approach 25

Figure 7, Supplier management model 30

Figure 8, Bar-code traceability approach..... 34

Figure 9, Service delivery overview 35

Figure 10, PSIRT integration with other processes..... 37

Figure 11, PSIRT/CERT process..... 39

Figure 12, Software forward and reverse traceability diagram..... 41

Figure 13, Hardware forward and reverse traceability diagram..... 41

1 Foreword

Cyber security continues to be an issue of intense interest to our customers and governments, and vendors alike; it is a focus of Huawei and cyber security assurance is one of our core company strategies.

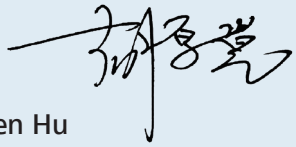
We believe it is only by working together internationally, as vendors, customers and policy and law makers will we make a substantial difference in addressing the global cyber security challenge. We also believe that we must share knowledge and understanding of what works and what doesn't work to reduce the risk of people using technology for purposes never intended.

If there was a simple answer or a solution to the cyber security challenge it would have been found by now, and it would have been adopted. However, the sheer fact that the world continues to debate standards, laws, codes and norms tells you we are all at the early stage – we must share what works, so others can adapt and improve.

This white paper is a small contribution to our collective knowledge and we have written it to help people understand some of the policies, procedures and transformations that vendors such as Huawei are considering in relation to cyber security. We hope you find it useful and welcome your feedback and constructive ideas on what else you believe we, and the industry in general, should be doing to improve our approach to designing, building and deploying more secure technology.

> Particularly, as the Deputy Chairman of the Board of Huawei and the Chairman of the Global Cyber Security Committee of Huawei, I would like to make our company's position clear. We can confirm that we have never received any instructions or requests from any Government or their agencies to change our positions, policies, procedures, hardware, software or employment practices or anything else, other than suggestions to improve our end-to-end cyber security capability. We can confirm that we have never been asked to provide access to our technology, or provide any data or information on any citizen or organization to any Government, or their agencies.
>
> We confirm our company's unswerving commitment to continuing to work with all stakeholders to enhance our capability and effectiveness in designing, developing and deploying secure technology.

We firmly believe that the world is a better place when the innovations brought about by the use of technology are maximised, they improve people's lives, and they improve economies. Huawei will continue our open and transparent approach and responsible position to its operations and everything we do.



Ken Hu

Deputy Chairman of the Board of Huawei and
Chairman of the Huawei Global Cyber Security Committee

2 Executive Summary

We live in a globally-connected world, which faces globally-distributed cyber threats. These threats are not restricted by geographical boundaries, and are targeted at all technologies, hardware/software/service providers and users – consumers, the private and the public sector alike. The threats are at an all-time high, in terms of sophistication and volume, and continue to trend upwards.

Our mantra for cyber security has always been: "Assume nothing, Believe no-one and Check everything"

One year ago, Huawei published our first Cyber Security White Paper, confirming our intention and commitment to work with public and private sector stakeholders to jointly capitalise on the benefits of technology and globalisation while rationally and pragmatically addressing related challenges.

We described an environment in which personal and business lives are linked by global interconnected telecommunications infrastructures built on technologies provided by a wide range of information and communications technology (ICT) vendors sourcing inputs from a vast global component and service-provider ecosystem.

We detailed how we have all become reliant on technology, and how digital innovation has made the world a smaller, more inclusive place, enabling social growth, improved education, better and more ubiquitous healthcare, and an enhanced human experience in general.

And, we acknowledged that the globalisation, interdependence and digitalisation of our lives also presents challenges in terms of those who wish to use technologies for purposes they were never intended - to steal, corrupt or damage.

Securing the future – security for tomorrow's world

We return to these core themes in this second Cyber Security White Paper, going into additional detail in terms of providing an overview of the approach we take to the design, build and deployment of technology that has cyber security considerations built into them. We discuss our overarching strategy and governance structure, our day-to-day processes and standards, our understanding of local and global laws and regulations, our approach to human resources and research and development, and our commitment to verification procedures and disciplines built around "assume nothing, believe no-one and check everything."

Further, we devote significant detail to our approach to managing third parties and supply chain and procurement practices, as well as how we govern and secure our manufacturing process and service delivery, while further describing our processes related to audit, traceability and defect and vulnerability identification and resolution.

The white paper highlights key digital trends ranging from the indispensable nature of the Internet in everything we do, to the liberation this brings to our anywhere-everywhere connected lifestyles and borderless business prospects, to the prospect of the Cloud as a new, powerful and dynamic source of collective wisdom. We discuss how broader and smarter information pipes will approach 'zero distance' between consumers and networks, connecting all new possibilities in the next wave of digital society, and how the convergence of our digital and physical worlds and the Internet of Things will bring groundbreaking changes to all of humanity.

In presenting current and future technology benefits, we remain mindful of the parallel challenges in terms of network and data security and integrity and, we want to stress that at Huawei, when we consider security, we do not just

consider addressing yesterday's problems, or even the problems we experience today, rather, we focus equally on laying down the foundations for securing tomorrow's world, a world that is dramatically different to what it is today.

The problem with standards is that they are not standard

It is with this eye to the future that we recognise and embrace the need for international industry standards for cyber security. The more that governments, enterprises and technology vendors can detail common standards, understand their purpose and positive contributions and commit to their effective adoption, the more the world will agree on "what good looks like". This is not about solving every problem, but it is about having a common agreement about what problems we are trying to solve and how they should be solved.

The reality is that the problem with standards is that they are not standard. We stress that this is a universal and industry-wide challenge. Just as the ICT industry has exploded around global technical standards and disciplines, so too must the industry work together to ensure the benefits of digital society through common and standardised approaches to security. We believe that one of the biggest challenges that vendors and buyers of technology share is a plethora of standards and best practices.

We are encouraged by the work in Europe and the United States on this agenda and we ourselves have taken the opportunity to document the top 100 things our customers ask us about security. They do not purport to be a standard but they do focus on some of the key attributes of success in relation to cyber security as seen through the eyes of our customers.

The Huawei end-to-end cyber security approach

Huawei does not claim to have the best or most comprehensive approach to addressing cyber and related challenges. We know we have much more work to do on this constantly evolving issue. This white paper details our end-to-end approach, responding to the biggest single piece of feedback that we received related to last year's white paper, as echoed in the many conversations we have had with customers, governments and other stakeholders: "Please provide more detail on your end-to-end cyber security approach".

We actively encourage input on our processes, and, more broadly, on ways to address the overarching challenges we face as an industry. Our most modest hope is that this white paper serves as a catalyst for broader, collaborative and rationally-informed public-private dialogue to meet common cyber security goals and objectives.

3 Introduction

If cyber security was easily addressed we wouldn't be writing this white paper. The reality is that there are no easy or perfect answers to this challenge. Cyber security as an issue is too broad, there are too many devices being connected to the internet that have variable security, too many vulnerabilities in hardware and software, the rate of change in technology is too great, and actors with ill intent only need to be successful once while defenders of cyber security have to be successful all of the time.

In our first White Paper on Cyber Security entitled "21st century technology and security – a difficult marriage" which was published in September 2012, we contributed to a wide-ranging international debate on the need for collaboration to reduce the risk from cyber security attacks.

Since our last publication the debate has continued to rage on, the challenges have continued to be articulated, and governments and customers alike, have continued to define, refine, and execute their respective strategies.

In this white paper we focus our attention on the governance, strategy, policies and procedures of Huawei relating to cyber security. We set out to detail at a more practical, more detailed level than our last white paper how we go about making cyber security a part of our company's DNA. In doing so, we are trying to strike an appropriate balance between brevity, on the one hand, and an adequate level of detail to contribute to the cyber security dialogue, on the other. We hope the document increases your understanding of our approach, to continuously improve the safety, security and quality of our products and services.

However, no document can adequately cover in full detail every policy, procedure, process template and work instruction for an organisation with the size and complexity of Huawei. In this context, this document only sets out to give a good indication of our end-to-end cyber security strategy so as to contribute to a public dialogue about these important issues.

4 What we said 12 months ago

Our first white paper on Cyber Security, "21st century technology and security – a difficult marriage" was widely-published with the media commenting on:

- The fact that cyber security can be bad for business
- That the world's ICT supply chain is intertwined and it is not possible to label any ICT equipment as "foreign"
- That we must all step back from the internet becoming a lawless "wild west"
- Solving, or reducing the risk of, cyber security challenges requires all international players to collaborate

The first white paper set out how reliant we have all become on technology and the fundamental benefits technology brings to mankind. Technology has made the world a smaller, more inclusive and more interconnected place. It has enabled social growth, improved education and healthcare and generated a shift in the capability of countries and companies to compete on the world stage.

We discussed in detail the exponential growth in connected devices, the use of applications on these devices and the rise in cloud computing. An environment where you are inherently using a global supply chain whilst being connected by global interconnected telecommunications infrastructures with technology being provided by a wide range of ICT vendors in your daily personal and business lives. Within this complex, intertwined ecosystem lays the potential for those that wish to use the technology for purposes it was never intended, to steal, corrupt and damage technology and infrastructure.

We detailed Huawei's supplier ecosystem and explained that having Huawei's name on a box does not mean that all of the components are from Huawei. Indeed up to 70% of the components that are in Huawei's technology portfolio are not from Huawei, but from a global supply chain with America being the biggest provider of components at 32%. We provided statistics and information to show that many Western ICT vendors have large R&D centres in China and that one city alone, Chengdu, had 189 of the Fortune 500 companies based in the city – today that number has risen to 250. This is mirrored around the world as companies place their research and development as well as support services in the best countries for these activities.

We were candid about the role of government in using technology to further their aims and we questioned the inconsistency of message that saw some governments criticising those that they did not agree with or those who were competing with their own companies, whilst at the same time buying zero-day exploits[1] and using technology to further their own economic and political ends at the expense of others. Indeed, we were critical of governments and politicians who were using cyber security as a trade barrier without providing any evidence of any facts to support their efforts to lock companies out of their market.

We also described Huawei's approach to cyber security and detailed at a very high level how we are building cyber security into everything that we do, and we gave an overview on how we went about this.

Finally, we called for a focus on harmonising and making laws transparent and in the light of recent revelations concerning some government agencies and the role of some companies we think this is now even more urgent.

[1] A zero-day (or zero-hour or day zero) attack or threat is an attack that exploits a previously unknown vulnerability in a computer system, meaning that the attack occurs on "day zero" of awareness of the vulnerability. This means that the developers have had zero days to address and patch the vulnerability.

5 Securing the future – security for tomorrow's world

In a speech titled, "The Next Wave of Digital Society"[2] ,our company's Deputy Chairman Mr. Ken Hu shared his insights on four trends of the digital society.

- **First,** the Internet will become a fundamental element of our business mindset.
- **Second,** flexible working practices facilitated by mobility will become a basic lifestyle option, with borderless enterprises becoming an essential form of business operations.
- **Third,** through effective use of the Internet, cloud computing, and big data, mankind can leverage the wisdom of people and machines worldwide to create a new, connected and shared wisdom.
- **Finally,** as the Internet and social media continue to gain popularity, the behaviours and preferences of consumers and individuals are converging, and intelligent analytics can be harnessed for business benefits. As the boundary between niche and domestic markets is increasingly vague as a result, enterprises must evolve to do business globally.

As we look forward, 5G technology is expected to achieve a speed which is 100 times that of today's fastest wireless bandwidth. As a pioneer of global 5G standardisation and research, Huawei is committed to providing broader and smarter information pipes to achieve 'zero distance' between consumers and networks, ultimately connecting possibilities in the next wave of digital society.

In a report entitled, "Beyond ICT, embracing the next digital revolution,"[3] we said that we believe that the past century has witnessed several waves of progress made possible by information technologies, including those used for communications (telegraphy, telephony, and broadcasting), home entertainment (radio, TV), computing, and the Internet. Information technologies drive economic growth worldwide and reshape the way people live and work. At present, we are evolving from a "society on wheels" to a "society on the network." However, information systems are still regarded as aid tools and support systems, keeping the digital and physical worlds somewhat parallel and compartmentalised. Now, as the digital and physical worlds begin to merge, the development of the Internet of Things has proven to be an effective catalyst of information-based developments and is sure to bring groundbreaking changes to all of humanity.

Beyond information and communications, the increasing integration of the digital and physical worlds will lead to a new digital revolution.

Heavy reliance on networks will usher in an age of digital citizenry with the age of digital business drawing near, as seen by our commercial dependence on networks for production and operations. This borderless Internet will give rise to a digital society.

From big data to "big wisdom", the IT systems of carriers and enterprises are evolving from post-processing support systems to real-time business systems. As traditional IT enterprise architecture is no longer capable of processing the huge volumes of data being encountered, an Internet-oriented cloud computing architecture will emerge. The

[2] http://pr.huawei.com/en/news/hw-266216-kenhu-digitalsociety-nikkei.htm

[3] http://www.huawei.com/ilink/en/special-release/HW_200943

rebuilding of data centres will provide the basis for supporting big data.

Low-bandwidth networks will hinder information-based development and user-experience improvement, and because of this, a ubiquitous Gigabit networks will be a prerequisite for any digital society.

An evolution from a "hard" pipe to a "soft" pipe will see the development of programmable, scalable, application-agile, automatic, and open intelligent networks. Software-defined networking (SDN) will lead to the development of next-gen network architectures.

Intelligent terminals will not just be tools for communications; they will also become extensions of our own senses. Terminals of the future will be context-aware and have intelligent sensory capabilities.

At Huawei when we consider security we do not just consider securing yesterday's problems or even the problems we experience today. We actively focus on laying down the foundations for securing tomorrow's world, a world that will be dramatically different from what it is today. Information technology plays a profound role in securing the freedom and prosperity of future generations as well as social and economic interaction, and that is why it's so important that we ensure that we take the right approach to addressing cyber security challenges.

6 The problem with standards is that they are not standard

One of the challenges that vendors and buyers of technology share in common is a plethora of standards and best practices. It is not an understatement to say that the "problem with standards is that they are not standard". It is not always clear that we even have the same terminology in discussing standards, guidelines and best practices. There is frequently overlap or duplication of standards or large parts of standards, as well as regional variations and industry variations. However, John Donaldson the Chairman of ISO / CASCO rightly said, *"Without standards, conformity assessment will be pointless and meaningless; without conformity assessment, the value of standards will be restricted; therefore, these two are indispensable in promoting international trade."*

If we had a magic wand we would certainly use it to rationalise, simplify, normalise and standardise what "good looks like" when it comes to cyber security. However, every high-technology company must deal with the situation as they find it today, including Huawei.

The Huawei approach to dealing with this challenge is to utilise a wide range of quality management techniques such as Kano[4] and Six Sigma, amongst others, and our broad approach is as follows:

Step 1: We assess the laws, standards, best practices, customer requirements, case studies and emerging new knowledge to assess how these can and should be applied to Huawei's solutions, policies, and procedures;

Step 2: We prepare / update our vision, strategic objectives, and organisational design etc. We create / update security baselines in every area of Huawei that should apply this "knowledge / requirement";

Step 3: We update our solutions, processes, policies and procedures in line with that required in the updated security baselines;

[4] http://www.kanomodel.com/

Step 4: From this we may produce technical standards, regulations, templates, guidelines, audit Key Control Points and when appropriate we also provide appropriate training and awareness;

Step 5: Forcontinuous improvement, we repeat the loop applying closed-loop management techniques to resolve issues as they are found; and finally;

Step 6: We start again at Step 1.

We do this for every part of Huawei's operations in relation to garnering knowledge on standards and best practice and then continuously implementing improvement activities.

6.1 The top 100 things customers ask us about relating to security

In dealing with the challenges we identified in the previous section we have taken the opportunity to document the Top 100 things our customers talk to us about in relation to security. In essence, that list includes some of the questions anyone may wish to ask their technology vendors when it comes to their approach to cyber security.

We have termed this list a "Reverse Request for Information (RFI)". In essence it is a potential list of cyber security requirements that buyers should consider asking their vendors if they can meet – i.e., we have reversed the process, we are asking customers to ask us, as vendors, how we deal with cyber security.

This list by its very nature cannot be comprehensive for every industry, covering every law and every technical standard; this is not the purpose. The purpose is to provide a suggestion based on questions posed to Huawei so that buyers can systematically analyse vendor cyber security capability when responding to tenders and can use this information to strengthen the quality of their RFIs and Requests for Proposals (RFPs) when seeking the best vendor(s) to meet their immediate and longer-term technology needs.

We will publish the Top 100 list shortly and we welcome comments, views, additions and modifications to that publication, with the intention of publishing an updated list in 2014.

7 The Huawei end-to-end cyber security approach

The biggest single piece of feedback that we have received since the publication of our last white paper, and a key element of the many conversations we have had with customers, governments and other stakeholders, has been a request to: "please provide more detail on your end-to-end cyber security approach". In this section we do just that; we provide a more detailed overview of the approach we take to the design, build and deployment of technology that involve cyber security considerations.

In detailing our approach, just as we did with our first white paper, we make no claims as to the robustness or completeness of our approach – this is not for us to assess but for our customers. We recognise we still have much to do to continuously improve our approach. However, our commitment to openness and transparency drives everything we do and we believe the more people who review, consider, assess and question our policies and procedures, the greater the promotion and impact on our ability to deliver better quality products and services. It is in that spirit that we welcome your feedback and the opportunity to engage in an open discussion about these issues.

The White Paper is organised into twelve sections which broadly follow Huawei core processes:

Process Area	Why is this process/ capability important
1. Strategy, Governance and Control	If cyber security doesn't matter to the Board and senior officials, it doesn't matter to the staff. Ensuring that cyber security is imbedded into the organisational design, governance risk management strategy and internal control framework is the starting point for the design, development and delivery of good cyber security.
2. Building the basics: Processes and standards	To get a repeatable quality product demands repeatable quality processes, standards and a similar approach by your employees and suppliers. Cyber security is the same: if your processes are random or your approach to standards is random, so will the quality, safety and security of the end product be – random.
3. Laws and Regulations	The law is complex, variable and ever-changing. Even if there is a law in a country, the ways of enforcement might differ greatly or there might be different interpretations of the same law or code. Laws, codes, standards and international controls add complexity and risk to a supplier and a business. Your processes must cater and deal with this variability and confusion and work to the highest level of law not the lowest level.
4. People matter	Many companies say that their people are their most important asset, which is true. However, from a security perspective they can also be their greatest weakness. The way people are employed, trained, motivated and their performance managed, often determines the difference between success and failure – not just for cyber security but also for the delivery of the overall company strategy.
5. Research and Development	Companies do not want to use their scarce capital to buy high-technology products from companies who do not have rigorous R&D processes that deliver consistent high quality, safe products. Nor do they want to see vendors having to make investment decisions between 'do they invest in a new product' or 'do they invest in making all products safe and secure'. Just as quality cannot be bolted onto a product neither can cyber security; companies need to demonstrate their long-term commitment to enhancing their R&D approach to accommodate appropriate cyber security design, development and deployment, as well as investing in the next generation of products.

Process Area	Why is this process/ capability important
6. Verification: Assume nothing, believe no one, check everything	Whilst a robust R&D process is fundamental to quality and to safe and secure products, R&D can be under pressure to launch new products quickly without the right testing and verification. Having in place a multi-layered "many hands" and "many eyes" approach to independent verification reduces the risk of unsafe products being distributed. A balance of end-to-end checks and balances supplemented with tiered independent security verification ensures a "no shortcuts" approach and protects customers' investment and services.
7. Third-party supplier management	Many large high-technology companies use third-party companies for hardware components, software components, delivery support and installation. If the third-party's technology or processes have security weaknesses, this can significantly increase the weaknesses of the vendor's products and services as they are integrated into the product the customer will receive. End-to-end cyber security means a vendor must work with its suppliers to adopt best practice cyber security approaches.
8. Manufacturing	Manufacturers of products must take in all of the components from whatever their source country of origin and security standard, manufacture an end-product for a customer and ensure that throughout every stage of manufacturing and product shipment, no security risk has inadvertently or intentionally been introduced.
9. Delivering services securely	There is not much point in focusing on designing your products with security in mind if when you come to deploy your technology, or support and maintain the technology, this is not done in a secure way. Customers rightly want to ensure when equipment is supporting their business that its operation and maintenance is safe and secure including upgrades, patches and fault fixing – they expect security throughout the life of the product.
10. When things go wrong: Issue, defect and vulnerability resolution	It goes without saying that no responsible company can give a 100% guarantee when it comes to security. Therefore, a company's ability to respond effectively to issues and learn lessons from what has gone wrong is critical to both the customer and the vendor. Knowing what to do in a "crisis", ensuring senior executives are informed to make speedy decisions and working effectively with customers and stakeholders ensures that normal service is restored quickly and safely.
11. Traceability	When things go wrong being able to quickly identify where it has gone wrong, what hardware or software component caused the issue and identifying where else that component is used is crucial to timely recovery. However, that is not enough; root-cause analysis demands an ability to forward and reverse trace every person, every component from every supplier in every product for every customer.
12. Audit	Rigorous audits play a key role in assuring the Board and senior company officials, and assuring your customers, that the appropriate policies, procedures and standards are being executed to deliver the required business outcomes.

7.1 Strategy, governance and control

If cyber security doesn't matter to the Board and senior officials it doesn't matter to the staff. Ensuring that cyber security is imbedded into the organisational design, governance risk management strategy and internal control framework is the starting point for the design, development and delivery of good cyber security.

We included our corporate policy in our last white paper, and it is as valid today as it was in 2011 when we first published it.

"As a global leading telecom solutions provider, Huawei Technologies Co. Ltd. ("Huawei") is fully aware of

the importance of cyber security and understands the concerns of various governments and customers about security. With the constant evolution and development of the telecom industry and information technology, security threats and challenges are increasing, which intensify our concerns about cyber security. Huawei will therefore pay a great deal more attention to this issue and has long been dedicated to adopting feasible and effective measures to improve the security of its products and services, thus helping customers to reduce and avoid security risks and building trust and confidence in Huawei's business. Huawei believes that the establishment of an open, transparent and visible security assurance framework will be conducive to the sound and sustainable development of industry chains and technological innovation; it will also facilitate smooth and secure communications among people.

In light of the foregoing, 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, organisational 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. In addition, Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests.

From an organisational perspective, the Global Cyber Security Committee (GCSC), as the top-level cyber security management body of Huawei, is responsible for ratifying the strategy of cyber security assurance. The Global Cyber Security Officer (GCSO) is a significantly important member of GCSC, in charge of developing this strategy and managing and supervising its implementation. The system will be adopted globally by all departments within Huawei to ensure consistency of implementation. The GCSO shall also endeavour to facilitate effective communication between Huawei and all stakeholders, including governments, customers, partners and employees. The GCSO reports directly to the CEO of Huawei.

In terms of business processes, security assurance shall be integrated into all business processes relating to R&D, the supply chain, sales and marketing, delivery, and technical services. Such integration, as the fundamental requirement of the quality management system, will be implemented under the guidance of management regulations and technical specifications. In addition, Huawei will reinforce the implementation of the cyber security assurance system by conducting internal auditing and receiving external certification and auditing from security authorities or independent third-party agencies. Furthermore, Huawei has already been certified to BS7799-2/ISO27001 accreditation since 2004.

In connection with personnel management, our employees, partners and consultants are required to comply with cyber security policies and requirements made by Huawei and receive appropriate training so that the concept of security is deeply rooted throughout Huawei. To promote cyber security, Huawei will reward employees who take an active part in cyber security assurance and will take appropriate action against those who violate cyber assurance policies. Employees may also incur personal legal liability for violation of relevant laws and regulations.

Taking on an open, transparent and sincere attitude, Huawei is willing to work with all governments, customers and partners through various channels to jointly cope with cyber security threats and challenges from cyber security. Huawei will set up regional security certification centres if necessary. These certification centres will be made highly transparent to local governments and customers, and Huawei will allow its products to be inspected by people authorised by local governments to ensure the security of Huawei's products and delivery service. Meanwhile, Huawei has been proactively involved in the telecom cyber security standardization activities led by ITU-T, 3GPP, and IETF etc., and has joined security organizations such as FIRST and partnered

with mainstream security companies to ensure the cyber security of its customers and promote the healthy development of industries.

This cyber security assurance system applies to Shenzhen Huawei Investment Holding Co., Ltd., and all subsidiaries and affiliates which are under its direct or indirect control. This statement is made on behalf of all the above entities.

This statement should comply with local laws and regulations. In the event of any conflict between this statement and local laws and regulations, the latter shall prevail. Huawei will review this statement on an annual basis, and shall keep it in line with laws and regulations."

Huawei Technologies Co., Ltd.
CEO Ren Zhengfei

However, turning these words into a consistent strategy and approach where the requirements are built into every role, every process, and every product and service is another matter. Our starting point was to create the governance that will make this happen, but importantly, provide clear accountability for its success or failure. This can only happen at the very top of the organisation – if it doesn't matter to the Board and senior officials it will not matter to the employees. The governance at Huawei is as follows:

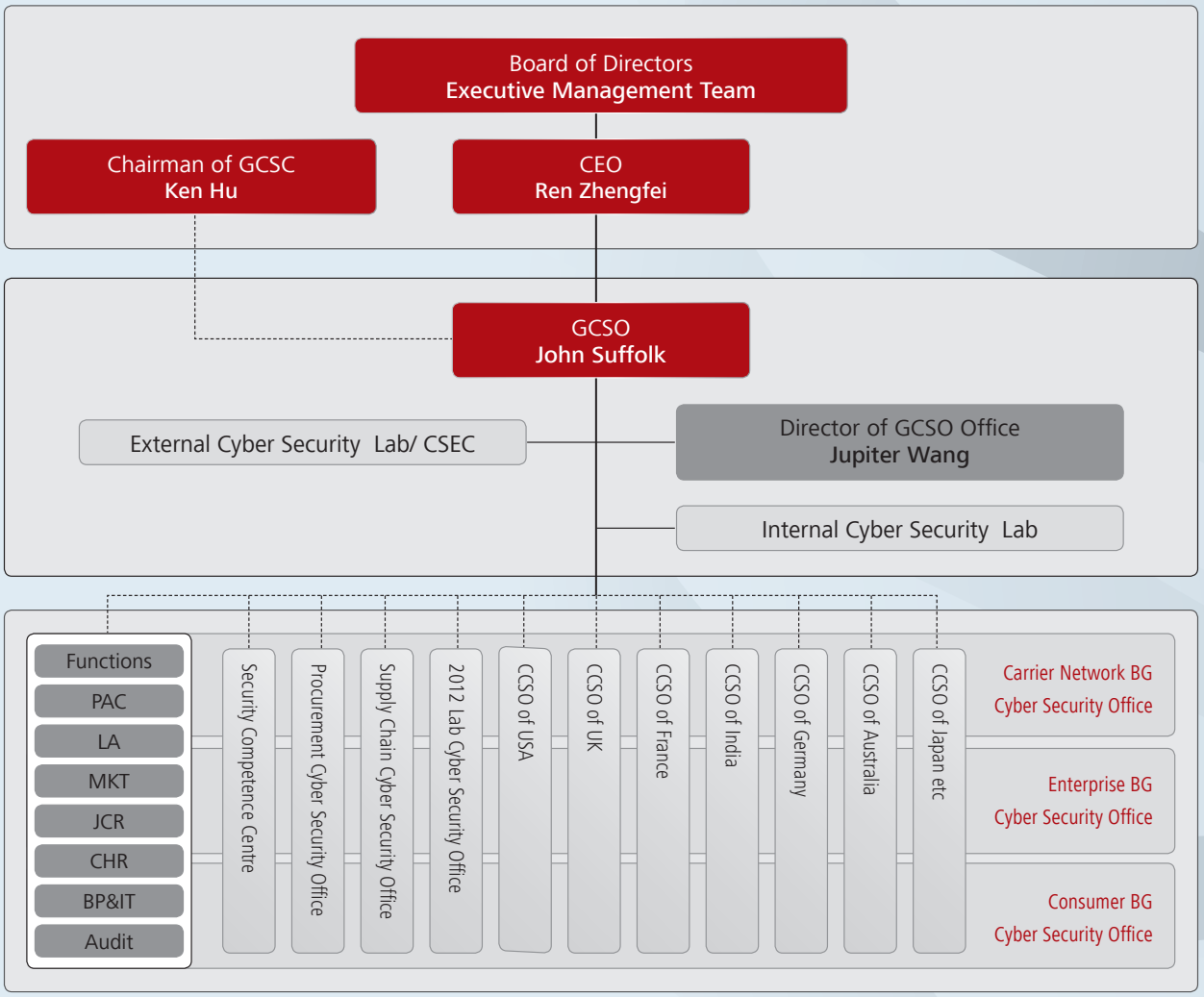


Figure 1, Simplified cyber security governance structure

It starts with Huawei's founder and CEO, Mr Ren Zhengfei, who has issued his public policy statement on cyber security and it clearly demonstrates that the issue matters to him. The Global Cyber Security Officer reports directly to Mr Ren. Core cyber security-related roles include:

Global Cyber Security Committee:

GCSC: Strategic direction; responsible for agreeing on the strategy, planning, policies, roadmap, and investment, and for driving the implementation and resolving conflicting strategic priorities and auditing.

The development of the cyber security strategy, policies procedures and the standards, and the assignment of resources are all governed by this standing Committee dedicated to cyber security which is chaired by a Deputy Chairman and one of our company's rotating CEOs. On this Board sits the main Board Members and the Global Process Owners each of whom has a role in ensuring that cyber security requirements are imbedded in all processes, policies and standards and that they are executed effectively. If there is any conflict, or resource issue in cyber security, this committee has the authority to make decisions and any necessary changes to the business.

Global Cyber Security Officer:

GCSO: Leads the team in developing the security strategy, establishing the cyber security assurance system internally, supporting government relations and public relations (GR/PR) and supporting global customer accounts.

Global Cyber Security Office:

GCSO Office: Coordinates related departments to formulate detailed operational rules and actions to support the strategy and its implementation, promoting the application, auditing and tracking of the implementation. The role is the company focal point for identifying and resolving cyber security issues.

Regional and Departmental Cyber Security Officers:

Regional / Department Security Officers: Accountable for working with the GCSO to identify changes to, and monitor implementation of, departmental / business unit processes so that the cyber security strategy and its requirements are fully imbedded in their areas and updated as necessary. They are also experts in their own right and contribute to the development and enhancement of the overall strategy. Each department has dedicated cyber security experts.

Huawei Auditors, both internal and external, use the Key Control Points (a point within a process where it can be evidenced that the process is working effectively and delivering its desired outcomes and outputs) and the Global Process Control manual to ensure that processes are executed and that they are effective. Audits, external inspections and third-party reviews all validate what is happening against what should happen. Individual personal accountability and liability (the rules and regulations) are built into Huawei's Business Conduct Guidelines and business processes that specify how we must behave in our daily operations. Knowledge is updated through online exams every year to keep knowledge current and this forms part of our Internal Compliance Programme.

7.2 Building the basics: Processes and standards

To get a repeatable, quality product demands repeatable quality processes, standards and a similar approach with your employees and suppliers. Cyber security is the same; if your processes are random or your approach to standards is random, so will the quality, safety and security of the end product be – random.

Huawei is governed by a set of integrated processes that encompass everything that we do. From our initial interaction with a customer to when we have successfully completed the project; or from the inkling of an idea that is put through the complete R&D process and through to the end of a product's lifecycle.

Each person in the process knows that their activities directly or indirectly create value for customers or reduce value due to poor quality, poor service or poor security considerations. Board Members are appointed as Global Process Owners; they own the quality, completeness and health of this process. From a security perspective it is their job to ensure that their process satisfies all of the cyber security needs.

Global Process Owners identify business key control points for each process and the matrix of segregation of duties that will be applied to all regions, subsidiaries and business units. This segregation of duties ensures that one person (or team) does not create so much control for themselves that they have the opportunity to put at risk the safety, security and quality of the outcomes and outputs of that process. Global Process Owners organise and implement monthly compliance tests at the key control points to continuously monitor the effectiveness of internal control and from this they will issue a test report. Focused on the "pain points" of the operation, Global Process Owners optimise the process and internal controls to improve operational efficiency, safety, security, customer satisfaction and benefits and help the achievement of business objectives. Global Process Owners conduct semi-annual control assessments each half-year to comprehensively evaluate the effectiveness of process design and implementation in business units.

The results are reported to the Audit Committee and other standing committees.

In our last white paper we detailed a simple process architecture that operates within Huawei. A more detailed representation is presented below:

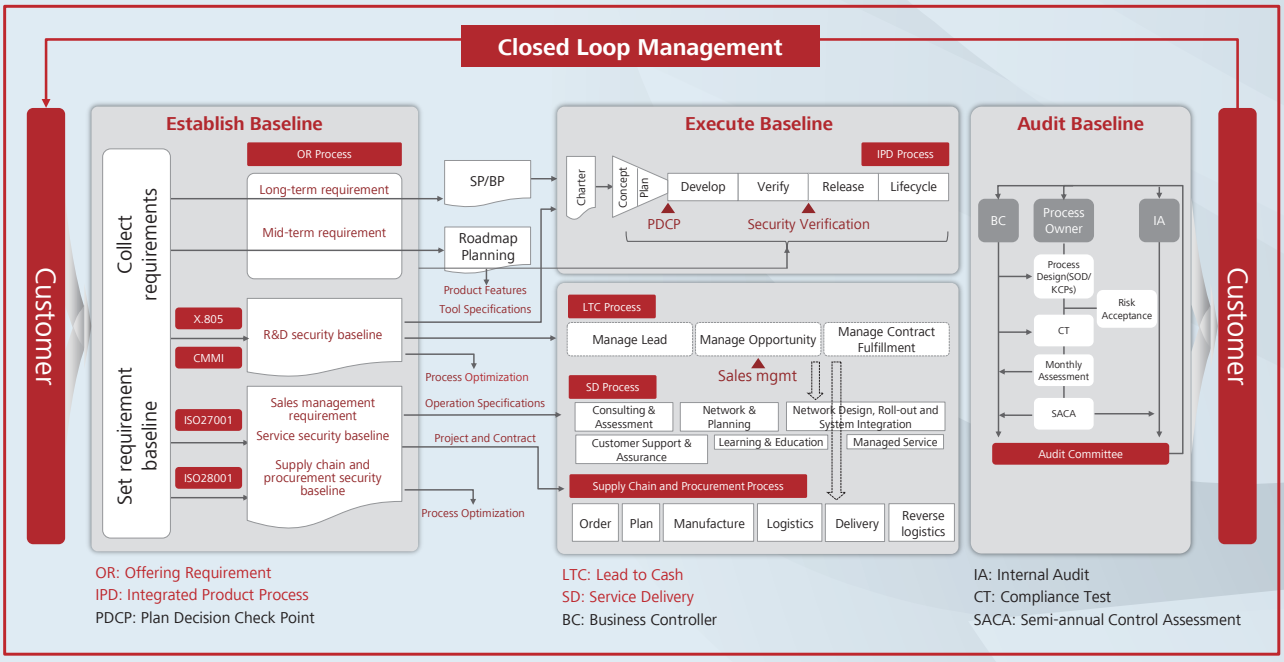


Figure 2, Overall process architecture

The above figure shows a closed-loop end-to-end process for cyber security and the overall policy framework at Huawei. On the left you see the gathering of all requirements, whether they are law, standards, customer requirements or Huawei requirements. This knowledge is turned into strategic and business plans and which is turned into policies and procedures and baselines. The baseline defines a minimum set of requirements. The middle set of processes executes the defined strategies, policies and procedures according to the agreed plans. Finally on the right there are a set of auditing mechanisms that validate whether the execution fulfils the requirements defined at the start of this process. Newly-learned knowledge and any identified weaknesses and gaps are then fed back to the beginning of the process to be considered and factored in the next iteration.

7.3 Laws and regulations

The law is complex, variable and ever-changing. Even if there is a law in a country, the ways of enforcement might differ greatly or there might be different interpretations of the same law or code. Laws, codes, standards and international controls add complexity and risk to a supplier and a business. Your processes must cater and deal with this variability and confusion and work to the highest level not the lowest level.

Huawei, like other ICT equipment vendors and their customers, face a range of complex legal and regulatory environments. However, just as we outlined in the Statement on Establishing a Global Cyber Security Assurance System, Huawei complies with all of the applicable laws and regulations in every jurisdiction in which it operates. To make cyber security an integral part of Huawei business, we investigate, identify, trace, map and classify all the applicable law and regulatory requirements from the countries in which we operate. We ensure that our products, services, personnel and operational controls address the relevant cyber security regulatory compliance requirements throughout our end-to-end business/transaction processes. The way we do this is as follows:

Tracking and identification of applicable legal requirements:

Huawei tracks and identifies the applicable legal requirements Huawei employs over 500 qualified legal experts all over the world with many in-house cyber security legal counsels and over 140 local lawyers who on an ongoing basis survey applicable laws and regulations[5] . We engage law firms with recognised reputations and experience in cyber security law. We continuously receive information from our Government Relations professionals and legal counsels who maintain appropriate relationships with relevant national or local regulatory government bodies. We also identify applicable laws and regulations through contracts which we enter into with our customers. In this context one of the challenges that all customers and vendors face is that not all countries have relevant laws on cyber security or personal privacy protection. If they do have laws they are not always fully implemented, or may not be clear. Just because a law does not exist it does not mean there are no codes and standards. Customers themselves also apply their own requirements and interpretations.

However, looking at the totality of all of the relevant applicable regulatory requirements, they do appear to be consistent in principle, which is to protect end-users' communication secrets and freedom, to protect end-users' personal data and privacy and to support stable and secure networks for customers.

[5] We subscribe to relevant information services; attend industry forums and seminars; monitor regulators' websites

Control of regulatory compliance:

Based on the legal requirements noted above, Huawei develops its cyber security strategy and compliance requirements policy, which also serves as a strategic framework and baseline to ensure that cyber security compliance requirements are integrated into our end-to-end business practices, product life-cycle and management from product development through to service delivery, and support service.

For example, in the Integrated Product Development (IPD) process (the main process that operates with Research and Development), our legal team provides advice to individual business units on applicable laws and regulations in addition to providing compliance support. Furthermore, the legal team has the power of veto in reviewing the development of any product if any non-compliance issue is identified. In Human Resources, we address the requirements of supporting the secure operation of customer networks and business and protecting end-users' privacy and communication freedom in our Business Conduct Guidelines, which serve as the principle code of conduct that should be followed by all employees and contractors. We also continuously train personnel on compliance requirements to raise their compliance awareness and support them in conducting their jobs in accordance with the laws and regulations and our cyber security compliance requirements policy. We provide new employee entrance training, management team training, and even specific training to key cyber security relevant positions. We also enforce an award-discipline policy to ensure all personnel take their compliance responsibilities seriously. In regards to suppliers, we require our vendors to sign a cyber security contract to ensure cyber security-related requirements can also be complied with by them (more details can be found in section 7.7, Third-party supplier management).

Huawei has also established and maintains a procedure for periodically evaluating compliance with our cyber security strategy and compliance requirements policy. The oversight responsibility for the legal compliance rests with the Legal Affairs Department and GCSO Office. The Legal Affairs Department and GCSO Office will report suspected non-compliance activities and potential risks to the GCSC, following the individual Business Group Executive Team's review, for further review and follow-up action.

The Huawei compliance model is imbedded into each person's role and each function's role, which in itself is independently checked and audited. Accountability for adhering to the controls, policies and standards rests with the individual and his/her supervisor and manager. In terms of incentives and disincentives this includes the management hierarchy, not just the individual who generated the breach or issue.

Take part in legislative activities:

Over the past year, we have seen many notable changes to cyber security laws and regulations in a number of countries. In the United States, President Obama issued a cyber security Executive Order to develop voluntary cyber security standards for critical infrastructure and assurance-related requirements for governmental ICT procurement. The European Commission published a proposal for a Directive on Network and Information Security to establish a secure and trustworthy digital environment. Australia publicly discussed potential reforms of national security legislation and New Zealand released its new Telecommunications Bill to encourage partnership between network operators and the Government. Huawei was invited to submit its comments and suggestions in Australia and New Zealand on cyber security-related legislation activities and in the United States we provided formal comments in response to the NIST Cyber security Framework Request for Information (RFI) and are contributing our thoughts on the USA security standards that will be referenced in the Framework. To avoid further conflicting or ambiguous legal obligations, and to hopefully encourage simplification of requirements for the global supply chain, Huawei welcomes the development of a globally-consistent cyber security framework. We also believe security outcomes are best delivered by a competitive, well-informed marketplace - so we strongly support the risk-based, technology-neutral and outcomes-based approach.

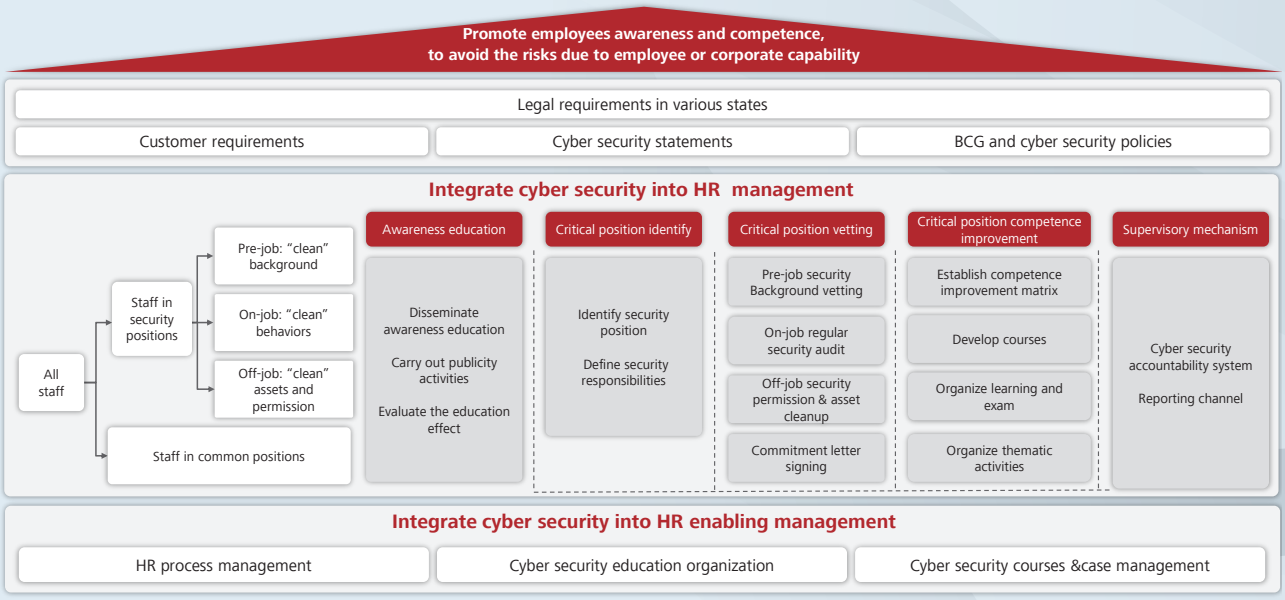
In addition to cyber security areas such as export control, IPR protection, fair competition and anti-corruption, we have established relevant compliance management systems to ensure compliance with the law. For example, in export control, we provide equipment all over the world and we ensure that equipment meets communication standards for civilian use and all applicable laws and regulations and implement and enforce an internal compliance policy (ICP) of export control that meets the industry standard.

In IPR protection, we pay more than $300 million for patent licenses each year and are one of the global top three patents applicants (with more than 30,000 patents granted worldwide). In fair competition, Huawei has established a series of policies to ensure that employees are required to abide by the rules of fair competition, including product pricing, management of cooperating partners, business contacts with competitors and commercialised banking relationship. In anti-corruption, we believe that an efficient and transparent anti-bribery system helps in building trust with partners and customers, and that promotes the consistent development of Huawei. Our Business Conduct Guidelines describe Huawei's anti-corruption and anti-commercial bribery policies and must be signed annually by our global employees.

7.4 People matter

> *Many companies say that their people are their most important asset, which is true. However, from a security perspective they can also be their greatest weakness. The way people are employed, trained, motivated and their performance managed, often determines the difference between success and failure – not just for cyber security but also for the delivery of the overall company strategy.*

The Human Resources management framework of cyber security is based on the foundations of a country's legal system and regulations. Cyber security requirements on Human Resources are to ensure that the background of our employees is appropriate, that the behaviour of employees is in line with all laws, policies, and procedures and Huawei's Business Conduct requirements, and that our employees have the knowledge, skills and experience to undertake their duties. The overall model is detailed below:



BCG = Business Conduct Guidelines

Figure 3, Imbedding cyber security into Human Resource processes

In terms of cyber security awareness education for all employees, Huawei is building a cyber security education and culture atmosphere across the company that recognises the importance of cyber security. To do so, Huawei organises ongoing cyber security awareness activities to improve and enhance employees' cyber security understanding.

In 2012, Huawei organised managers' workshops involving over 6,000 managers in discussions on cyber security issues. The purpose was to nurture an environment across the organisation for cyber security awareness education and learning within the company. Huawei also carried out a round of cyber security awareness training for all employees and organised all employees to learn cyber security requirements, take part in and pass an exam and sign a commitment letter indicating their understanding of their cyber security responsibilities. This work covered over 150,000 employees all over the company globally and achieved the objective of having cyber security awareness-education cover every employee. Moreover, business departments also carried out cyber security knowledge and skills training and other awareness education activities for employees based on their own business requirements, and they also studied cyber security cases specific to their business area.

We also distribute cyber security periodicals regularly through the internal publicity platform. In addition, we use other methods, such as posters and cards to publicise the content of cyber security education. Business departments carry out customised cyber security publicity activities according to their own business requirements and features, such as soliciting articles of cyber security and recognising these articles with an award, the selection of cyber security slogans, case studies etc. All the activities help cyber security awareness education to be inculcated into the daily work of employees.

Huawei regards cyber security training as a long-term campaign. On the one hand, we have embedded cyber security requirements into the Business Conduct Guidelines (BCG) of Huawei employees to pass on cyber security requirements to all employees through the annual BCG learning, testing and commitment-signing activities to help them improve cyber security awareness. On the other hand, we will continue to carry out the study of cyber security training and case studies, the publicity of cyber security requirements on behaviours and knowledge, so as to keep enhancing the cyber security awareness of all employees.

From a risk perspective, some roles pose a greater insider threat in relation to security than others. Huawei has identified the cyber security-critical positions in each business area and clearly defined positions that could provide opportunities to embed tamper or undertake malicious activity throughout the design, build, deployment and support of products we provide to our customers.

For employees undertaking cyber security critical positions, Huawei has established the following requirements:

- Before an employee joins the company, we will conduct background vetting to ensure the potential employee has an appropriate background and history that matches the requirements of our customers' requirements for that position.

  We use a detailed and consistent template with cyber security requirements built into the "qualifications review" process of searching and selecting candidates. This pre-job vetting covers both external recruitment and internal allocation of existing employees.

- When the employees are in their positions, we use the criteria of job qualification and certification to direct them to raise their awareness and improve relevant skills, and we also conduct regular security audits.

For the behaviours of employees in cyber security-critical positions, we review their cyber security-related conduct to check whether there are any violations and thus ensure the behaviours of employees are appropriate.

- When the employee leaves the position, or when an employee leaves a critical position, we use check-points in the off-job vetting process to guide Human Resources and cyber security personnel in removing or modifying privileges and remove assets of the employees, where appropriate. The off-job vetting covers internal re-allocation and resignations.

Growing the skills and knowledge of our employees so that they can adequately fulfil their roles efficiently and effectively forms a core part of Huawei's performance-based culture. We develop specific security competence improvement plans and baseline courses to improve the cyber security competence of employees through our systematic learning schemes. Huawei aims to improve the cyber security knowledge and skills of employees in critical positions to reduce the occurrence of non-compliant behaviours. Meanwhile, we also direct employees to learn proactively to supplement passive training with proactive learning. In addition, for the competence required in cyber security-critical positions in different business departments, we have developed customised courses and test papers. We organise annual learning and exams for employees to push them to learn proactively and hold them accountable for doing so. Various practice-oriented competence improvement activities are carried out to improve the knowledge and skills of employees in critical positions. For example, we have cyber security lecture series, cyber security forums and a database of cyber security cases. To evaluate competence improvement, we adopt the Kirkpatrick model[6] and use methods such as the surveying of training satisfaction and exams to evaluate the effectiveness of competence improvement.

Huawei has adopted a strict cyber security responsibility system that implements formal accountability mechanisms. We require that every employee should be accountable for what they do and for the consequences of their actions, not only in terms of technology, but also laws. Our employees know that in the case of any occurrence of a cyber security issue, there may be significant impact to the customer, the company and the individual. Therefore, no matter whether the behaviour is intentional or unintentional, we execute a formal procedure based on the event and the consequences. We have determined seven categories of violations and five business scenarios according to cyber security statutes in various countries and regions, including Europe and the US. Based on this, we have published the Accountability System of Cyber Security Violations in which we clarify the consequences to the individual in the event of any cyber security violations.

Our starting position is that our employees, and the employees of most companies, come to work to do a great job. However on occasion, employees may see other colleagues doing things that make them feel uncomfortable, either because it is just plain wrong, they morally think it should be wrong, or they are not sure, but want someone knowledgeable to know about the conduct. Like all good organisations we recognise such situations and offer a whistle-blowing channel to report any suspected wrong-doing through our Business Conduct Guideline (BCG) process.

[6] http://www.kirkpatrickpartners.com/OurPhilosophy/TheKirkpatrickModel/tabid/302/Default.aspx

7.5 Research and development

Companies do not want to use their scarce capital to buy high-technology products from companies who do not have rigorous R&D processes that deliver consistent high quality, safe products. Nor do they want to see vendors having to make investment decisions between 'do they invest in a new product' or 'do they invest in making all products safe and secure'. Just as quality cannot be bolted onto a product neither can cyber security; companies need to demonstrate their long-term commitment to enhancing their R&D approach to accommodate appropriate cyber security design, development and deployment, as well as investing in the next generation of products.

The Research and Development Organisation consists of over 75,000 engineers and follows a formal set of processes and methodologies as depicted in the following figure. It builds on the MM (Market Management) process and IPD (Integrated Product Development) processes that are detailed in Figure 2, Overall process architecture.

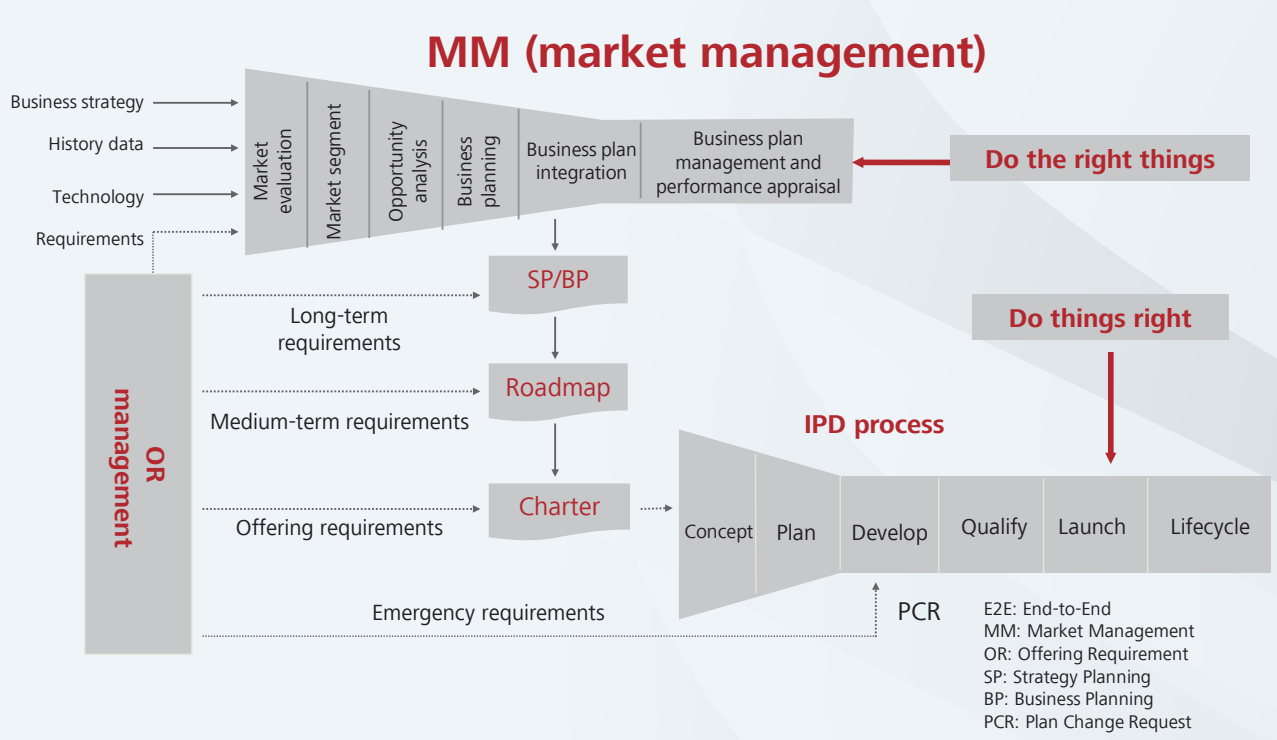


Figure 4, Market Management to Integrated Product Development

The core process within our Research and Development (R&D) area is the Integrated Product Development Process, or IPD. We introduced the IPD process in 1999. The process is an integration of the PACE methodology of PRTM, advice from IBM and Huawei's long-term extensive practices and experience.

Based on the breadth of Huawei's R&D activities and with reference to industry security practices such as OpenSAMM[7] and SSE_CMM[8] , and customer and Government feedback, we have embedded in the IPD process

[7] http://www.opensamm.org/

[8] http://en.wikipedia.org/wiki/ISO/IEC_21827

security activities such as security design, security development and security testing. This ensures the effective execution of those security activities so as to improve product robustness, enhance privacy protection and provide products and solutions to customers that are more secure. A more granular level of detail of the IPD process shows how cyber security is being built into everyone's daily operations; in this way security becomes everyone's job and something that is done naturally.

We take a built-in approach to embed into our end-to-end business processes cyber security requirements such as security threat analysis and security scanning of source code, etc. To support this approach we have established the Security Technical Competence Centre that works across Research and Development and all of Huawei's business to build security into design, respond to security attacks, and improve security defence.

- In the **concept phase**, the security requirement analysis mainly focuses on two aspects. First, the product security baseline should be included in the list of requirements and should be executed without fail – these are the mandatory requirements. Second, a threat analysis of the scenarios regarding where the product will be installed in the customer's site should be undertaken to identify any additional, or customer-specific, security requirements.

  Product security baseline consists of security requirements to ensure the achievement of security assurance or the containment of risks to an acceptable level. The baseline is derived from international and local laws and regulations, government requirements, a customer's threshold and live network issues, etc. The objective is to ensure security legal compliance, protect users' communication and privacy, enhance the system's access control / protection of sensitive data and improve the defence capability of the system.

  Threat analysis is used to find the potential source and types of threats and attack points according to specific scenarios where the product is used so that we can assess the risks and ensure that counter-measures are included in the list of product requirements.

- In the **plan phase**, we further specify the security threats identified in the concept phase as the product design goes into more detail. At this point we design the product security architecture and security design features. We always refer to industry best practices such as X.805 and OWASP security specifications and develop our cyber security design standards based on a wide range of standards and best practices.

- In th**e development phase**, product developers follow the secure coding specifications when writing software and then conduct cross reviews. Automatic code scanning tools are used to conduct security scanning and analysis of the code to reduce security defects in the code and to identify areas of further investigation.

- In the **qualifying phase**, testers conduct testing based on the specifications of security requirements. The density of product defects is an important index for decision making at ADCP (Availability Decision Check-Points). The internal Cyber Security Lab checks products of all Business Groups (Carrier Network, Enterprise, Consumer) including OEM products independent from business departments to verify whether they comply with the product security baseline.

In addition, we ensure full segregation of duties throughout the complete R&D process. Software developers cannot approve the final test results or the final release. Nor can software developers authorise the release of their own software. There is an independent and rigid review and release process---once the software is released, it will be

digitally signed and then automatically uploaded to the support website for download in manufacturing or at a customer's site.

A summary of the imbedded IPD process can be seen in the following figure.

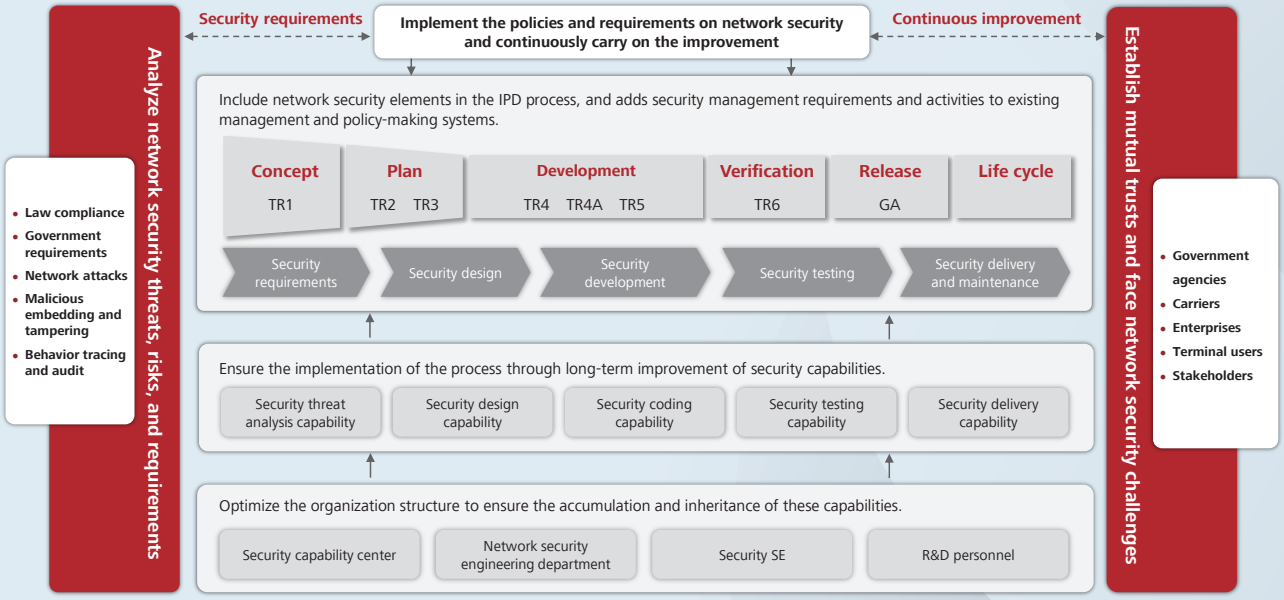


Figure 5, Security imbedded into the IPD process

7.5.1 Configuration management and the Build Centre

Configuration management includes the processes by which Huawei ensures integrity, consistency and traceability of their products. Configuration management not only ensures the integrity of Huawei self-designed and developed software, but also ensures the integrity, of third-party and open-source components.

Huawei's configuration management process is an integral part of the Integrated Product Development (IPD) process. Configuration management activities are carried out at different stages of the IPD process. These include configuration management strategy and planning, configuration item identification, configuration item change control, release management, configuration library management, configuration status accounting, and a configuration audit. This environment creates full traceability, which is a key cyber security outcome. To access Huawei's configuration management library, developers need to apply for the proper authority, thus ensuring the code in the configuration library is secure and that only authorised developers assigned to the project can gain access.

An important role in configuration management is the segregation of duties, which isolates the activities, roles and responsibilities that are involved in the building process, and ensures that roles are clearly defined, from the iteration preparation, planning, and development, to system acceptance.

At the integration preparation stage, a Continuous Integration Engineer (CIE) develops a list of compilation and building tools required for the development of the products, and establishes the continuous integration environment according to the relevant tool list. Once a product reaches the iteration development stage and the R&D engineers have completed coding, the CIE develops the building scripts and compilation guide, and implements a one-click automatic building process. Automating the build process ensures that there is no potential to input additional non-

authorised code or items. The build process also uses appropriate tools such as Fortify[9] as well as numerous other commercial and self-built analysis tools, which check for coding errors. These errors are then logged into our Defect Tracking System (DTS) and re-assigned to the engineer responsible for the development of the code. Once all the defects have been addressed, the CIE initiates the single-build process again.

At the system acceptance stage, the integration and verification team will confirm that the building process was completed based on the compilation guide, and at the same time ensure that the compilation guide is correct and workable. The Quality Assurance team will perform audits for the tools that are actually used in the build process to avoid the use of tools without application or approval. Upon completion of all these tasks the software is then released into Huawei's distribution portal for customer download.

To ensure the build process is repeatable, Huawei has established a build centre where all hardware, compilation tools, third-party software, database source and operating systems meet a rigorous set of standards and support requirements. The Build Centre is a solution to product building and compilation and it provides a cloud service to support the software-building activities during the IPD process. It has three major features: standardised management of resources, building process standardisation and service acceleration.

Standardised management of resources: conducts centralised management of standard hardware, standard operating systems, virtual technology, cloud technology and the hardware and operating systems involved in the product building environment. It significantly increases the stability of software building and improves the success rate. It ensures that any product contains legitimate components, from legitimate sources at the correct service, patch and version number. It ensures that only approved components necessary for the product are included in the software build process.

Building process standardisation: automates the complete building process from environment building, to code download, to one-click compilation, packing, static code review, automated low-level test to high-level test through a centralised management of tools, standardisation of building scripts, one-click building and automatic installation of the building environment etc. In doing so, we ensure the product-building process can be reproduced / restored and traced.

Service acceleration: leverages the building efficiency. In essence this is a cloud-based service available 24 hours a day.

Two additional functions have been implemented into the build centre, these are: a virus scan centre that runs four anti-virus software products concurrently has been integrated into the testing process and, secondly, a digital signature centre to digitally sign the compiled code with the key being stored in a key database for safety.

Huawei has introduced Application Lifecycle Management (ALM), which is a mature industry solution, to establish an integrated software collaborative development platform to support end-to-end traceability. Huawei has grouped its business objectives for using ALM into three areas:

- During requirement analysis, raw requirements (RRs) are broken down into initial requirements (IRs) and system requirements (SRs).
- In system design, test cases and functions are designed based on the system requirements. The development engineers write and build code to implement the functions during the coding and building activity.
- After coding and building, a test version is produced. After it passes the testing and verification process, it will be delivered to customers as a release version.

Traceability relationships between these business objectives have been implemented to ensure that all customer requirements are correctly developed and verified. In particular, linkages between the various stages of development enable forward and backward traceability of requirements and identification of individuals associated with the development of the product during each stage.

[9] http://www8.hp.com/uk/en/software-solutions/software.html?compURI=1338812

7.5.2 Tools and third-party component management

Huawei sources many third-party and open source software components from around the world. Sourcing software from third-parties provides challenges to all companies and it is important to consider the following:

- Is the source code or component you are using from a reliable source?
- How do you track its usage for fault rectification and licence management?
- How will you deal with security vulnerabilities?
- How do you intend to reuse the component?
- How does the overall lifecycle management of the third-party component fit into your product's own lifecycle?

Not only do we need to consider the third-party component, we also need to ensure that the component and the selection of all of the associated components required to compile the source code or third-party component are also controlled. Huawei has implemented the full lifecycle management of the sourcing of third-party software, from the sourcing of these components to how they are incorporated into our products.

Huawei strictly controls the use of open source and third-party components and ensures that the components are only acquired from authenticated sources. We have created a library in which we store all our third-party and open source components and our developers can only obtain access to the components after receiving appropriate approvals. This ensures that Huawei can centrally keep the open source or third-party components up to date and properly maintain the tools required to build the code.

Using a centralised repository for our third-party and open source code that is embedded into Huawei's overall IPD process also allows us to ensure that each component has been obtained from a reliable source, is properly licensed and to track where the component has been used and in which product, as well as to ensure that the selection of tools used is appropriate. Importantly, we can manage vulnerabilities and ensure that the developers fully address any issues related to the use of the component.

An extremely important part of the centralised database is to ensure Huawei can trace vulnerabilities that may occur from time to time in the third-party and open source code. Once a vulnerability is detected by the customer, the component supplier or Huawei, it is then evaluated, and either a resolution is provided by the original developer or a workaround is obtained. At this point it is then passed to our PSIRT group to be addressed with our customers.

The use of a centralised repository allows us to manage the lifecycle of the third-party and open source code. This is extremely important as while Huawei's software is produced with its own lifecycle; the third-party or open source component may be updated during this lifecycle and will need to be changed to ensure consistency, especially in the event that the third-party or open source component is declared end-of-life by the original developer.

7.6 Verification: Assume nothing, believe no one, check everything

Whilst a robust R&D process is fundamental to quality and to safe and secure products, R&D can be under pressure to launch new products quickly without the right testing and verification. Having in place a multi-layered "many hands" and "many eyes" approach to independent verification reduces the risk of unsafe products being distributed. A balance of end-to-end checks and balances, supplemented with tiered independent security verification, ensures a "no shortcuts" approach and protects customers' investment and services.

At Huawei we subscribe to the "many eyes and many hands" approach to provide openness and transparency on what we do. We encourage audits, reviews and inspections on all technology vendors, including Huawei, in a fair and non-discriminatory manner, as every audit or review enables companies to challenge their thinking, policies and procedures, in turn enhancing their capability, product quality and product security. We believe that from an efficiency, effectiveness and security perspective, the more people who are looking, touching, testing, and questioning everything we do, the better it is for Huawei and the better it is for our customers. It is something we positively encourage for all vendors.

In recent years, Huawei has implemented many initiatives to proactively address the serious and complex cyber security challenges faced by governments and telecommunications network providers globally. One such challenge is helping all stakeholders gain a significantly greater understanding of what all technology vendors should be doing to mitigate security concerns. We believe that most of our stakeholders agree that there should be a standard or set of standards for cyber security in the telecommunications context. However, it is difficult for stakeholders to come to an agreement on what those standards should be, or if new standards need to be developed. Huawei believes that we must collectively (vendor, carrier, and government) address these common challenges in a broad, rational manner that addresses the most commonly held concerns.

While there is no global consensus about cyber security evaluation standards, Huawei believes that by building a fair and objective cyber security assurance environment, many of the common cyber security challenges can be overcome. At Huawei we review our products from initial concept through to deployment and ongoing management and patching / upgrades to ensure that security of the product is reviewed at every stage. The creation of a global conformity assessment program for ICT products would contribute greatly to the ability of purchasers of ICT products to make more informed decisions about ICT products and provide additional incentives for manufacturers and vendors to make products with fewer vulnerabilities and higher assurance characteristics.

Tiered evaluations

Huawei has built a multi-tiered cyber security evaluation process to ensure that our products are reviewed for potential security issues from product design, development, and right through to deployment and maintenance in our customers' networks around the world.

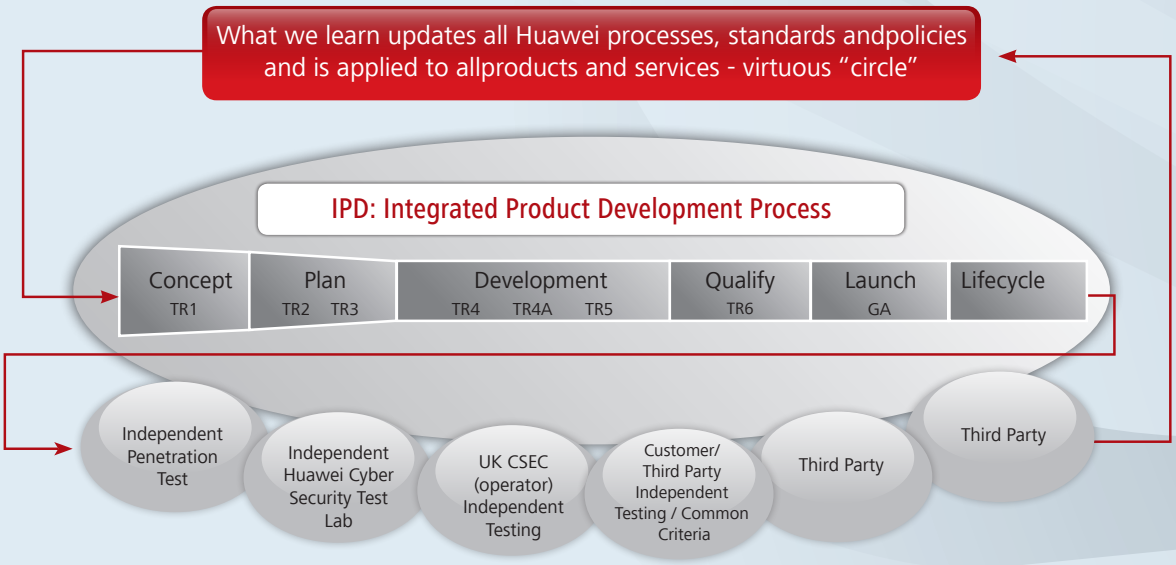


Figure 6, Multi-tiered independent verification approach

We carry out and continuously improve our product development by using "closed-loop management". Closed-loop management aims to ensure customer security concerns and requirements are incorporated into the design phase of our products to improve the quality and security at an international level. Any reports generated from an evaluation of our products are provided to our Research and Development (R&D) organisation to ensure any findings are corrected for future product releases.

We provide customer security assurance through independent testing and evaluation of our products through many different platforms such as Huawei's Internal Cyber Security Lab, the UK Cyber Security Evaluation Centre (CSEC), customer evaluations, and third-party auditors and evaluators.

Due to the different approaches and understanding of security, one customer's security requirements might differ significantly from another's. Security requirements also vary among networks and equipment at different levels. Accordingly, we provide security evaluations to satisfy the security requirements of individual customers. Huawei currently operates three different evaluation models to continuously improve the security of our products:

1. The Huawei Internal Cyber Security Lab is responsible for security self-verification. Security self-verification involves reviews against known vulnerabilities and the product's security baseline. This involves internal checks and controls of Huawei products from initial concept through to deployment.

2. The Huawei External Cyber Security Lab model is responsible for security evaluation at regional and national levels. This kind of evaluation aims to meet the security certification requirements proposed by local governments and customers. Currently, the UK Cyber Security Evaluation Centre (CSEC) provides such evaluations. In these centres, code quality and security is analysed using commercial and self-designed tools to search for potential code weaknesses. The software is also tested using a range of tools and techniques to assess its ability to withstand being hacked and finally additional reviews are provided on security design characteristics.

3. Huawei also works with independent third-party evaluation agencies and evaluators who provide unbiased security evaluation of our products, and in some cases, certification. This type of evaluation is commonly carried out by customers and third-party auditors, including the Common Criteria (CC) security certification model. Huawei has gained CC certificates for multiple products. Some carriers conduct their own internal security testing on products as they continue to develop more secure environments, while other customers invite a third-party to test products independently such as customers in North America and Europe.

Many eyes, many hands, many checks

Another benefit from the multi-tiered approach is the "many eyes, many hands and many checks" approach to ensure that one lab's review receives additional verification with a different review approach thus providing another perspective through which products are evaluated.

Our Internal Cyber Security Lab is also set up to allow customers or third-parties to perform their own testing from within the facility itself. Within our current internal lab, we have implemented private, secure environments that can support simultaneous evaluations from customers or third-party subject matter experts. Customers and third-parties can leverage this platform to carry out independent security evaluations in a fast and effective manner. This provides them with a private testing environment with access to resources, test tools, and equipment to satisfy their own evaluation needs. Customers are already leveraging this facility to directly evaluate and assure the security of their products.

Customers may also use a third-party lab that is independent of Huawei, and whose tools, technologies and approaches are not known to Huawei. In such cases once an evaluation has been completed, a confidential audit

report is issued to customers, key stakeholders such as relevant government bodies, and Huawei's R&D team. These reports are statements of fact, providing details of any issues discovered and their potential severity assessed, as well as any details of mitigating measures that the customer may wish to implement until a permanent solution is available. Any findings are also provided to the product development teams to ensure a consistent improvement in overall product security and quality.

Following the publication of the report, any changes to software made because of upgrades or problem solutions can be tested by customers and governments, providing continuous assurance of the solutions over their lifecycle.

In some cases, product certifications such as a Common Criteria (CC) certification may be required, and Huawei works with our stakeholders to achieve this.

Huawei believes that cyber security evaluations work best when stakeholders collaborate. We work with the security departments of customers, third-party security vendors and security groups to learn from their experience and to improve our evaluation capabilities, practices and requirements. In addition, we leverage the independent and objective results presented by third-party security vendors, security agencies and customers to verify whether our reviews are accurate and objective.

Importantly, the approach to independent testing and verification takes, not surprisingly, an independent approach. Each lab or third-party model adopts different tools, techniques, approaches and methods. The objective is to test and verify the product from as many different dimensions and approaches as possible to enhance its security.

In summary, we at Huawei are acutely aware of the risks that companies face in today's world and we will continue to proactively participate in product evaluations and work to achieve fair and objective reviews of our products. While the industry deliberates on a global consensus of what a standard cyber security review might look like, Huawei will continue to work with our customers and stakeholders to meet their security needs.

7.7 Third-party supplier management

Many large high-technology companies use third-party companies for hardware components, software components, delivery support and installation. If the third-party's technology or processes have security weaknesses this can significantly increase the weaknesses of the vendor's products and services as they are integrated into the product the customer will receive. End-to-end cyber security means a vendor must work with its suppliers to adopt best practice cyber security approaches.

7.7.1 Supply chain

Huawei has established a comprehensive supplier management system through which Huawei selects and qualifies suppliers based on the supplier's systems, processes and products, continuously monitors and regularly evaluates the delivery performance of qualified suppliers, and selects suppliers who can contribute to the quality and security of the products and services procured by Huawei.

The Huawei supply chain management (SCM) program regards the quality of products as a core strategy and continuously improves product quality and process efficiency through a number of continuous improvement activities, such as Six Sigma, optimisation projects, quality control circles (QCCs), the traditional suggestion box, and the Huawei

Production System (HPS). For example, since the launch of Six Sigma in 2002, Huawei has extended its quality efforts from internal product quality to external customer satisfaction and from production to the end-to-end supply chain process, such as plan and order management.

Through Huawei's global logistics management process and regional and country logistics processes, Huawei manages the global logistics businesses in a hierarchical (global-region-country) manner that supports the supply chain security management system. Huawei has deployed an IT system, HTM (Huawei Transportation Management), which enables visualisation and monitoring of the transportation process.

Huawei has established processes for supply chain return performance. Huawei sets requirements for the applicable return, or reverse-goods handling methods, based on the local laws and regulations to meet all local requirements for obsolete goods and returned goods. To ensure the customer's data security, such as the risk that sensitive data might exist in the returned equipment, Huawei requires the customer to properly erase any data before the equipment is returned. Huawei's global supply chain strategy emphasises the following foundational, security-related characteristics:

- Effectiveness –promote the timely and efficient flow of Huawei products and services in the supply chain in order to protect the supply chain from being violated or exploited, and to reduce the vulnerability of exploitation or disruption.
- Security – ensure the integrity of the products and services throughout the global supply chain; identifying and addressing threats at the earliest stage of the process, and establishing and maintaining a supply chain security management system that operates uninterrupted and is improved continuously.
- Resilience – identify and manage supply chain risks and developing response, recovery and improvement plans to ensure the quick response, recovery and continuous improvement of Huawei's supply chain. Huawei has established an accurate and efficient traceability system to identify and mark issues, and relate them to vulnerabilities or defects in components or processes that need to be improved to enhance the resilience of the supply chain.

Huawei believes that malicious damage may occur in all activities of the supply chain, so it is important to focus not only on a certain activity, but the entire supply chain.

Supply chain threats fall into two major categories: tainted products and counterfeit products. Threats that can cause tainted and counterfeit products include malware, unauthorised parts, unauthorised configuration, scrap sub-part parts, unauthorised production, and intentional damage.

Huawei has established a supply chain security management system based on Huawei's requirements and processes for quality assurance, information security, environmental protection, and IT assurance, as well as the requirements of ISO28000 (supply chain security management), C-TPAT[10] (Customs-Trade Partnership Against Terrorism), and TAPA[11] (Transport Asset Protection Association). The supply chain security management system has passed third-party certification requirements for ISO28000 and has been awarded the corresponding certificate.

Huawei develops supply chain cyber security baselines to ensure the integrity, traceability, and authenticity of the products in the supply chain. The baselines include requirements on physical security (entity delivery security), software

[10] http://www.c-tpat.com/

[11] http://www.tapaonline.org/

delivery security, as well as organisational, processes, and personnel security awareness. Physical security baselines are designed to prevent physical access that might permit tampering or implementation of unauthorised code.

Software delivery security ensures the end-to-end integrity of software by preventing unauthorised physical access to software and enabling technical verification. To manage risks related to incoming materials Huawei inspects incoming materials based on the technical specifications for the materials and relevant quality standards and materials guidelines, and follows unique processes in each of the following phases of the product lifecycle: procurement, development, and supply chain.

For the supply chain phase, Huawei has established an ISO28000-compliant supply chain security management system, which can identify and control the security risks during the end-to-end process from incoming materials to deliveries to customers. Huawei checks the integrity of the third-party components during each of the incoming material, production and delivery processes, records the performance, and establishes a visualised traceability system throughout the process.

Software management is a significant activity of security management. Huawei uses key software security management methods for the supply chain, including strict access control and physical security. We apply a unique Part Number for each software version (VRC) which will be delivered to customers, and this Part Number goes all the way through the software delivery process. In the software delivery process the system generates the related authorisation and license automatically according to contract information; meanwhile, the system sends a software pre-loading request to the manufacturing (ATE) server automatically. All these data transfers among systems are conducted automatically, without manual intervention, to avoid the risk of tampering. We keep detailed records for software loading and testing, and when we need to track something such as a software version in the equipment of a certain site, it can be quickly located.

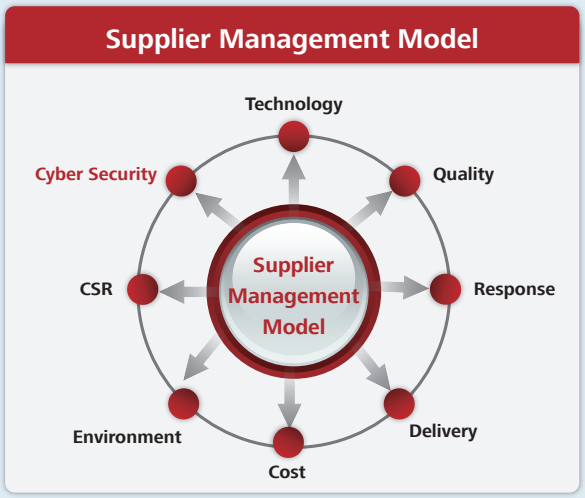
Huawei continuously improves its support systems and software distribution platform to support service engineers and to provide upgrading services to customers and to support customer self-upgrading programs. We adopt a hierarchical authorisation management approach where only authorised employees can apply and download software or license from the support system and the software distribution platform according to the contract or the equipment requirements, otherwise, the system will deny the login or download. All requests and the individuals who accepted the requests are fully logged for auditing purposes.

As a key part of the supply chain security management system, Huawei has built in traceability of components and products from first contact to delivery, based on the Advanced Planning and Scheduling System (APS) and Cooperation-Manufacturing Execution System (C-MES).

7.7.2 Procurement security

Huawei's supplier management system is comprised of the following elements: technology, quality, response, delivery, cost, environment, social responsibility, and security.

Huawei has developed and implemented procurement cyber security baselines applicable to suppliers, which clearly define product and service security criteria that must be satisfied by suppliers.



Descriptions

1. **Technology:** Technological edge, open resources, and capabilities of early involvement R&D, innovation, and technical service capabilities.
2. **Quality:** Quality system, quality performance, response speed in problem handling, and capabilities of continuous quality improvement.
3. **Response:** Lead time, supply flexibility, market information sharing, promptness in capacity preparation, and response to push in orders.
4. **Delivery:** timely, accurate and completeness of delivery
5. **Cost:** Price competitiveness, capabilities of continuous price reduction, contribution to the TCO, Total Loss, and favorable commercial payment terms and conditions.
6. **Environment:** Establishment of environmental system, including removing harmful substances, controlling and reducing pollution and greenhouse gases
7. **Social Responsibility:** Establishment of Integrity of the social responsibility and occupational health and safety management system (OHSMS). Including Labor standards, health and safety and business ethics
8. **Cyber Security:** Policy, Baseline, Process, Agreement, Training, Test, Emergency Response

Figure 7, Supplier management model

In the absence of applicable cyber security procurement standards, Huawei developed 46 procurement cyber security baselines built on the security characteristics of products and services from global suppliers, an analysis of suppliers' potential security risks and hazards, and an assessment of customers' cyber security needs.

The procurement cyber security processes were established in coordination with – rather than independent of – the procurement business to ensure both parties understand what is required and recognise that cyber security is a joint effort. Huawei implements procurement management security through these processes, which include supplier security qualification, material security testing, supplier security inspection / audit, performance management, risk evaluation, vulnerability management and emergency response and traceability. Huawei also requires suppliers to sign security agreements that clearly define joint responsibilities.

At a high level, procurement cyber security requires managing the supplier and managing the supplier's security. Managing the supplier involves managing procurement requirements, strategy, qualification fulfilment and acceptance. Managing supplier security involves:

- supplier and material security certification
- security agreement and execution
- supplier security audit and emergency response
- security test and acceptance
- supplier security and phase-out

Procurement security is not only incorporated into the production material procurement and engineering service procurement processes, but is also integrated into two supporting processes: supplier management and material management. Procurement security has also been integrated into Huawei's processes for R&D Integrated Product Development (IPD), Lead to Cash (LTC), supply chain, and Service Delivery (SD), and links to R&D, production, service,

and marketing processes. Because of this integration, security management initiatives at Huawei are linked from end to end to become an effective and indispensable part of Huawei's cyber security assurance system.

In the supplier qualification stage, Huawei integrates cyber security requirements into four key procedures: the supplier Request for Information (RFI), self-check on supplier systems, the qualification of the supplier system, and the terms of the mandatory security agreement that must be executed. Each stage is conditioned upon the preceding stage; and only suppliers who meet Huawei's security requirements can become a supplier to Huawei.

Huawei has developed a security system qualification mechanism that targets material suppliers, engineering service suppliers, logistics suppliers, EMS suppliers, device service suppliers, and software outsourcers. After obtaining the supplier's system qualification, all prospective suppliers must sign the cyber security agreement before becoming formal suppliers to Huawei.

The security agreement Huawei executes with suppliers covers a range of related areas, including: product security requirements, service security requirements, system security requirements, and obligations in the event of future violations.

Huawei has also developed an engineering service security agreement targeted specifically at engineering subcontractors, and that has been signed by all of Huawei's cyber security-related engineering subcontractors. This agreement includes service security requirements, system security requirements, and obligations in the event of violations. In addition, Huawei has developed security agreements for logistics suppliers, EMS suppliers, software outsourcers, and device service suppliers. All these suppliers have signed agreements with Huawei and are committed to working collaboratively to reduce cyber security risks.

Huawei places equal importance on supplier materials security qualification and on supplier security qualification. Given this, Huawei has integrated cyber security requirements into three critical procedures: material specifications, cyber security risk evaluation in technical quality risk evaluation, and integrating cyber security testing into the material testing and verification process. Doing so helps ensure that Huawei only procures materials that have minimal security risks and pass security testing and verification.

To manage the security of existing suppliers, Huawei uses a hierarchal management mechanism based on security risk evaluations, which involves assessment of supplier security risk levels, and inspection and improvement of any supplier security issues. Huawei uses a scorecard to evaluate supplier security performance, supplier vulnerability notification, and emergency response. The scorecard contains six elements and 11 evaluation items. Every year, Huawei evaluates and rates suppliers' security performance. Huawei reduces cooperation, or even ceases cooperation, with suppliers with poor security performance.

Huawei uses the supplier cyber security risk evaluation tool to evaluate suppliers' security risk levels, and then places suppliers in lists based on their risk level: low, medium, and high. Based on these lists, Huawei manages suppliers hierarchically, requiring high-risk suppliers to conduct self-checks and conducting a two-day onsite audit at the supplier's facilities; medium-risk suppliers to conduct self-checks and conducting a half-day inspection; and low-risk suppliers to implement self-checks.

At Huawei, supplier security vulnerability notification and emergency response are an extension of supplier management initiatives by Huawei Product Security Incident Response Team (PSIRT). By requiring suppliers to release warnings on vulnerabilities and responding to them quickly, Huawei helps to ensure that vulnerabilities in third-party software are effectively managed.

When security vulnerabilities are found in products, suppliers must send the information in writing to Huawei PSIRT

based on requirements stipulated in Huawei's vulnerability notification service level agreement. Suppliers must fix the vulnerabilities in a timely manner by developing new product versions or patches, and must notify Huawei through formal version-release channels.

7.8 Manufacturing

> *Manufacturers of products must take in all of the components from whatever their source country of origin and security standard, manufacture an end-product for a customer, and ensure that throughout every stage of manufacturing and product shipment, no security risk has inadvertently or intentionally been introduced.*

Manufacturing security is a key component of Huawei's global assurance program. Huawei has established a standards-based, efficient, high-quality, and secure end-to-end manufacturing / production system that encompasses incoming material across the entire process through to packing and shipment of end-products. The system has been integrated into all activities of the production process based on the required process documents, standard operations, and other work instructions.

Huawei's manufacturing / production process is divided into the following core steps: incoming quality control, tin printing, surface mounting, reflow soldering, plug-in, wave soldering, board commissioning, assembly and aging, functional (system) test, and packaging and shipping.

In addition, based on the processing characteristics of the specific products at each stage, Huawei has inspection stations at each of the five levels, with 1,188 inspectors who conduct inspections on raw materials through to finished goods. Huawei applies advanced instruments and equipment for automatic inspection and testing, such as automated optical inspection (AOI) and automatic X-ray inspection (AXI) equipment, as well as in-circuit test (ICT) and functional test (FT) equipment.

Huawei continuously improves product quality and process efficiency through a number of activities, such as Six Sigma, optimisation projects, quality control circles (QCCs), suggestion box, and the Huawei Production System (HPS). For example, since the launch of Six Sigma in 2002, Huawei has enhanced its quality assurance efforts from internal product quality to external customer satisfaction and from production to the end-to-end supply chain process, such as plan and order management.

Huawei has adopted a series of measures to ensure the production process conforms to legal requirements and industry standards, including, carrying out environmental protection testing on incoming materials, and effectively transferring relevant requirements to the suppliers where this is appropriate.

To address manufacturing security risk and ensure the integrity of hardware and software, Huawei implements end-to-end processes to prevent tampering, including such risks as unauthorised hardware replacement, software implantation or tampering, and virus infection. Huawei records, and inspectors check, every operating step in the manufacturing process.

Software management is a significant activity of security management. Huawei uses key software security management

methods and software is treated as confidential data within Huawei:

1. R&D personnel release software only via a secure internal system and all software information is managed as confidential data within the company, with only designated personnel being allowed to receive software update information.
2. Designated authorised personnel download the software from the R&D software library Product Data Management System (PDM) to the Cooperation-Manufacturing Execution System (C-MES), a secure manufacturing distribution system and the software is verified by other authorised personnel. The C-MES server automatically verifies and records changes to the server on a daily basis and releases corresponding reports.
3. Robust physical security processes are implemented for the equipment room and production preparation management.

Huawei uses automatic loading and testing of 95% of its products. Products without automatic testing are covered under strict software download management processes through the software application approval process and the loading and testing of such products are inspected by inspectors.

Through automatic testing, Huawei has reduced risks and security threats caused by man-made errors. In addition, Huawei can readily locate the links or points where the errors and threats occur through the records generated and traceability enabled in the end-to-end processes and supporting technology.

Huawei has implemented a secure and strict maintenance process to ensure the integrity of the products in the process. Huawei records the whole process in the manufacturing and bar code systems and this record includes points of failure, maintenance materials, maintenance personnel, software reloading, test information, goods-product warehousing, and replaced faulty components. The records and audit trails enable Huawei to query the bar code of the faulty board, the fault phenomenon, the maintenance personnel involved, the loaded software version, and the testing results, among others.

In the area of Electronic Manufacturing Services (EMS) security management, Huawei has a dedicated EMS management team to manage EMS partners. Huawei has different management modes for supply centres in and outside China. In China, Huawei has factory directors and inspectors working within the factories; supply centres outside China are managed according to Huawei's factory mode requirements which include having a production management team working within the factories that is responsible for the technical support, quality monitoring, and security management of the EMS partners Huawei cooperates with. For software management, Huawei ensures software is directly synchronised from the Huawei HQ software distribution server to ensure accuracy and to prevent any alteration to the software prior to it being loaded onto the equipment.

The internal logistics of the manufacturing process – materials selection and verification, product packaging, weighing and labelling, and packing – are also important from a security perspective. Huawei manages the facilities in strict accordance with C-TPAT[12] (Customs-Trade Partnership Against Terrorism) requirements. In the area of personnel management, Huawei conducts strict background checks on the personnel in the packaging area before, and carries out security awareness training after, their enrolment. Access to the packaging area is closely controlled to ensure that unauthorised personnel are not allowed to enter the area, and authorisation is cancelled after the personnel resigns.

[12] http://www.c-tpat.com/what-is-ctpat/

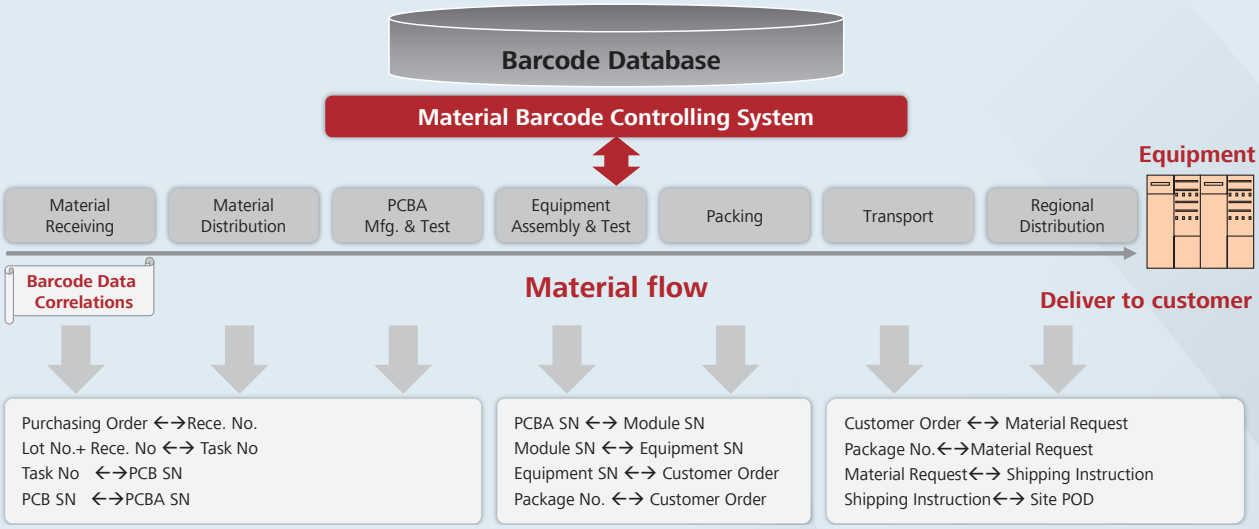


Figure 8, Bar-code traceability approach

End-to-end traceability is a high priority for Huawei and, as stated previously, Huawei uses a product traceability system based on bar codes. The bar code application IT system is the core of Huawei's product traceability system. All the bar code systems share the same bar code database. The bar code system undertakes part of the functions of the ERP system and handles part of the administrative services and a few data collection tasks. Through the data transfer and interconnectivity of all systems, Huawei assures complete traceability from incoming materials to delivery of end-products.

Huawei's manufacturing processes contribute to the global assurance program by enhancing understanding of risks, setting and enforcing requirements, and emphasising continuous improvement.

7.9 Delivering services securely

> *There is not much point in focusing on designing your products with security in mind if when you come to deploy your technology, or support and maintain the technology, this is not done in a secure way. Customers rightly want to ensure when equipment is supporting their business that its operation and maintenance is safe and secure including upgrades, patches and fault fixing – they expect security throughout the life of the product.*

Huawei recognises that service delivery touches every part of our company's core processes, from our core operating business processes through to enabling and support processes.

The starting point for any service operation is clarity on the needs of the customer. Core elements include: control and access to networks; the access and control of data, both business and personal; requirements for the use of local employees; and the approach to be taken to trouble-shooting must all be addressed.

The customer's network and information are a customer's assets. Therefore, any access to and operations performed on them must be explicitly approved by approved customer's personnel, and be in line with relevant laws and regulations. Huawei has implemented a set of specific processes and procedures in the early stages of network design

that encompass obtaining approval for the collection, storage, usage and processing of customer network data.

There are four key business processes in Huawei's Network Integration Service, these are: network planning and design, network roll-out, acceptance and cutover, skill transfer and handover.

Each of these business processes requires a level of risk and security assessment. Huawei has incorporated the key cyber security management requirements into each of these service delivery activities. The following key security management requirements have been incorporated into the Network Integration Service:

- Skill transfer and handover
- Project solution review
- Personnel management
- Security hardening
- Project transfer-to-maintenance
- Customer data management
- Software management
- Network cutover management
- Skill transfer to customer

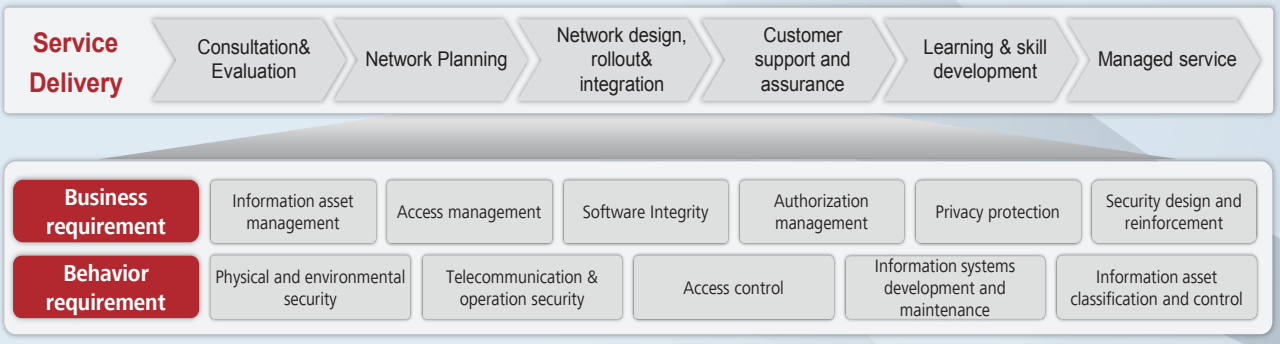


Figure 9, Service delivery overview

By implementing end-to-end cyber security assurance processes, we enhance our capabilities in addressing and resolving cyber security issues, including improving product techniques, process and regulations, and personnel management. By doing so, we can ensure that products and services delivered by us are as secure as they can be.

As telecommunications operators move to reduce their capital expenditure by outsourcing the management and day-to-day operations of their networks, a new set of security risks have to be considered and these will need repeatable and auditable processes and procedures. Areas to be considered include:

- Information security
- Personnel management
- Local laws and regulations compliance
- Core business strategy
- Physical security
- Transition management

However, unlike a network integration service, these risks are now shared by both the managed service provider and the network owner.

Prior to any work on a network, express permission must be granted by the network owner. When software is being loaded onto our customer's networks it is scanned before implementation to eliminate viruses, and to ensure that the tools and software used are acquired through legitimate channels (such as official support websites), and have the correct digital signature when leaving the R&D process.

All operations on a network are recorded in audit logs to ensure the customer can validate their prior authorisation for the work, and that the work that was undertaken matches the work that had been authorised.

However, things can go wrong on a customer's network, be it a hardware or software fault, or performance issues with the technology. What matters to customers is that the problems can be quickly identified and resolved. Huawei identifies cyber security incidents based on their definitions as logged with support centres and cyber security issues are tagged with the "Cyber Security" label in the iCare system to escalate such issues to the TAC/GTAC team, and submitted to PSIRT, ensuring that progress on problem-handling is reported in a timely manner.

In addition, four major control points are in place in the spare parts repair and return services process to ensure data security, these are:

1. After a repair and return service application is submitted, the system automatically reminds the customer to delete data stored in the parts to be repaired.
2. Before spare parts are returned to Huawei, the repair card template is used to remind the customer to delete data or remove storage media.
3. In the case where the parts cannot be repaired locally and have to be returned to Huawei's headquarters, the fault tag is checked item by item. Products for which stored data has not been forensically cleaned or the storage media have not been removed are prohibited to be returned to headquarters. The customer can also authorise Huawei to delete data if permitted by the local laws.
4. In the case where the faulty parts are to be repaired locally, the test equipment will automatically cleanse the data from the faulty parts.

Service delivery employees are the front-line of any company as they have access to potentially sensitive information, and as such, it is essential that they are trained to assist in protecting the network against identity concerns, access control issues, communication security issues and data protection concerns among others. In the area of employee management, Huawei has developed, based on ISO27001 and other standards, a Code of Conduct for employees comprising five key aspects, such as physical and environmental requirements. Network management must also take into consideration multi-vendor domains and protection against unlawful removal of personal or private information.

Huawei strictly manages employees who have access to customer networks. These employees sign letters of commitment that detail roles, accountabilities and potential legal liabilities, and are required to study and take relevant tests on cyber security topics.

Representative offices and project teams must manage cyber security on a regular basis and follow up on the progress of team members and employees in regard to compliance with cyber security requirements. Management of outsourced employees is an important part in onsite project management. Outsourced employees may have a different understanding about cyber security; therefore, they must participate in training sessions organised by project teams and they can undertake tasks only after they pass the evaluation of the project team. Huawei has developed standards for accepting projects completed by outsourced employees and evaluates the quality of their projects based on these standards.

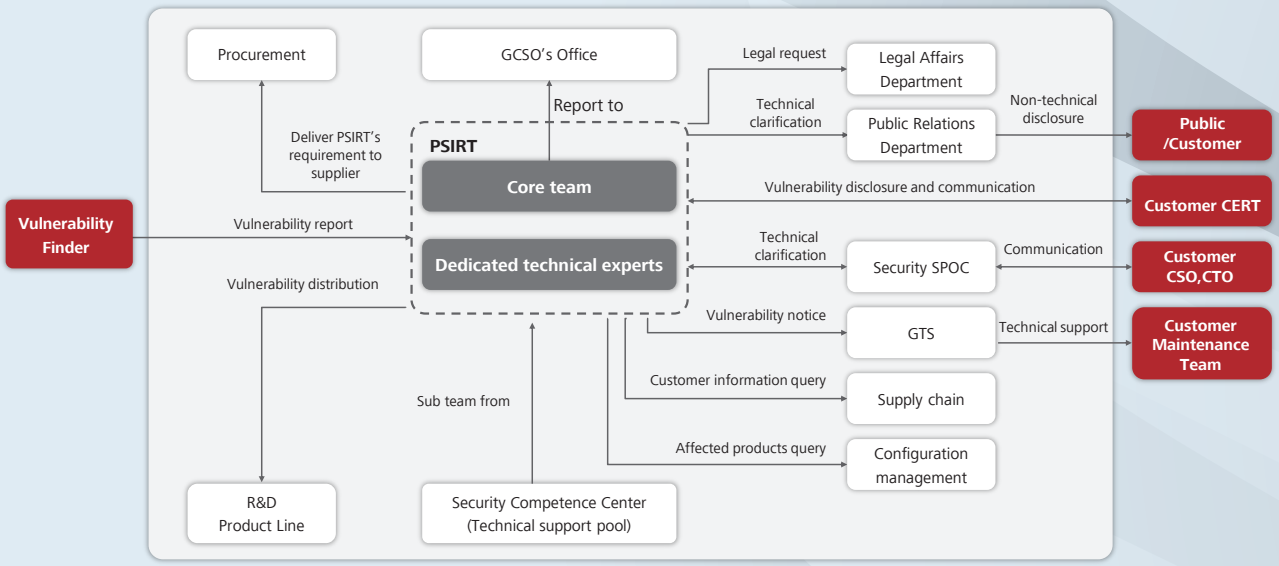
7.10 When things go wrong: Issue, defect and vulnerability identification and resolution

It goes without saying that no responsible company can give a 100% guarantee when it comes to security. Therefore, a company's ability to respond effectively to issues and learn lessons from what has gone wrong is critical to both the customer and the vendor. Knowing what to do in a "crisis", ensuring senior executives are informed to make speedy decisions and working effectively with customers and stakeholders ensures that normal service is restored quickly and safely.

We live in a globally-connected world, which faces-globally distributed cyber threats. These threats are not restricted by geographical boundaries of nations, and are targeted at all technologies and hardware / software / service providers. The threats are at an all-time high, in terms of sophistication and volume, and continue to trend upwards.

The Issue to Resolution (ITR) process provides an end-to-end framework for receiving, analysing and resolving any problems encountered by our customers, security-related or not.

Potentially, customer issues can affect any part of our business whether it is a technical service request, an operational service request and a spare part issue, a reported security issue or a customer complaint. Hence, the ITR process is tightly integrated with the R&D lifecycle (IPD), PSIRT, Defect Tracking System (DTS) and other processes. This helps to ensure a timely response to resolving customer issues.



GCSO: Global Cyber Security Officer SPOC: Single Point of Contact

Figure 10, PSIRT integration with other processes

Any issue being experienced by our customers with our products, solutions, or services has the potential to have an impact on our customers in terms of the availability, integrity, confidentiality, traceability, robustness and resilience of their operations. It is therefore important that we are able to identify any security impact as early in the process as possible.

In responding to an issue, no matter how trivial, it is important that any solution proposed and implemented does not inadvertently introduce security issues or risk behaviours.

We need to continually improve and learn from any issues that arise. The diversity of issues raised is significant given that Huawei serves over a third of the planet's population, but we need to be sure that we as an organisation grow and learn from the experience – the same issue should not keep recurring; if it does, it means that the root cause of the problem or issue has not been addressed and effectively.

Huawei has developed a virtuous closed-loop system to create a holistic and integrated ITR process that connects other critical processes. This ensures all issues are resolved appropriately and effectively.

To support the ITR process, and vice-versa, a Computer Emergency Response Team (CERT) is a fundamental component of a holistic cyber security system as it enables technology users to reduce or eliminate potential risks resulting from vulnerabilities to live networks and technology through the confidential sharing of vulnerability information, practical mitigation actions and management of vulnerability resolution. At Huawei this function is owned and delivered by the Product Security Incident Response Team (PSIRT).

Without the timely sharing of vulnerability information, technology may be exposed to exploitation and abuse. If product vulnerability information was to get into the hands of the wrong people then all technology built using the hardware and/or software that contains that vulnerability is potentially at risk.

Huawei takes this threat extremely seriously and applies the strongest controls around vulnerability information. In addition, Huawei actively participates in international standards bodies and forums to advocate education around these issues and share best practice with the cyber community. However, in the absence of strong international standards[13] and auditing systems, it is left to individual vendors to make judgment decisions on how and with whom to share such vulnerability information.

Cyber security is an arms race between those who wish to break into technology for illegal or the wrong reasons, and vendors and customers who are working hard to stop them from succeeding. In response, the role of PSIRT is to ensure that network operators are briefed on any potential vulnerability, along with either mitigation techniques or permanent solutions to risks associated with Huawei products. The timely and accurate communication of this information allows network operators to maintain the security of the network by ensuring their protection measures comply with the latest product advice.

The PSIRT vulnerability-handling process is divided into four stages:

1. Vulnerability research and collection - This has to do with the identification and/or reception of incoming vulnerability notifications. Incoming notifications are accepted from any sender, including customers, external CERTs, researchers or staff searching website and analysing risks factors. At Huawei we encourage responsible disclosure which means external vulnerability finders should give the vendor reasonable time to handle and fix any issues before public disclosure. The vulnerability collection stage also covers the communication of security requirements to upstream supply chain vendors through procurement staff, and ensures the effective fulfilment of these requirements through contracts. These contractual commitments ensure suppliers report security vulnerabilities related to Huawei products in a timely manner.
2. Security vulnerability assessment, analysis, and verification - Once a vulnerability is either suspected or verified, the PSIRT team works with the product owners to quickly complete an assessment of the vulnerability's authenticity and associated risks. During the analysis and verification process the PSIRT team employs industry-leading commercial and open source tools and standards to enhance the accuracy and timeliness of vulnerability analysis.
3. Tracking and fixing - Once a vulnerability has been confirmed, PSIRT promptly conveys the information to the teams responsible for the affected products, and then actively tracks the progress to resolution. The vulnerabilities

[13] ISO 29147 vulnerability disclosure and ISO 30111 vulnerability handling processes are both under development

are checked to confirm whether they exist in common components or platforms, or in unique parts of products (customised parts based on common platforms), thus ensuring that the issue is addressed in all product families, product versions and product models. The PSIRT process is tightly integrated with the R&D core process to ensure a timely response to vulnerabilities. The R&D and IPD process includes the product development, documentation, configuration management, and testing and release management. The integration of the PSIRT and IPD has the additional benefit of improving staff security awareness and product security through timely reporting, case sharing, and training. These actions deliver a closed-loop, virtuous environment for continuous improvement.

4. Disclosure - The communication of concise, accurate information to the network operators is an important requirement to maintain a secure environment. Throughout the process the PSIRT team manages the communication to both the entity that reported the suspected vulnerability and to customers. The communication to customers includes mitigation strategies along with information on permanent solutions. The list of customers with the affected products is generated from the supply chain database to ensure the accuracy of the point-to-point communication (PSIRT to CERT). Before releasing a Security Advisory externally, the company streamlines and aligns information across its frontline support engineers (GTS), field account departments, public relations departments, and legal affairs departments, to ensure the accuracy and consistency of vulnerability information when communicating with different stakeholders. Information is shared on a strict "need to know" basis to protect confidentiality. In some situations Huawei may find vulnerabilities in integrated third-party software and Huawei PSIRT immediately reports the vulnerability to the corresponding supplier and encourages them to take necessary remediation action and to disclose the vulnerability.

The process flow is summarized in the following diagram.

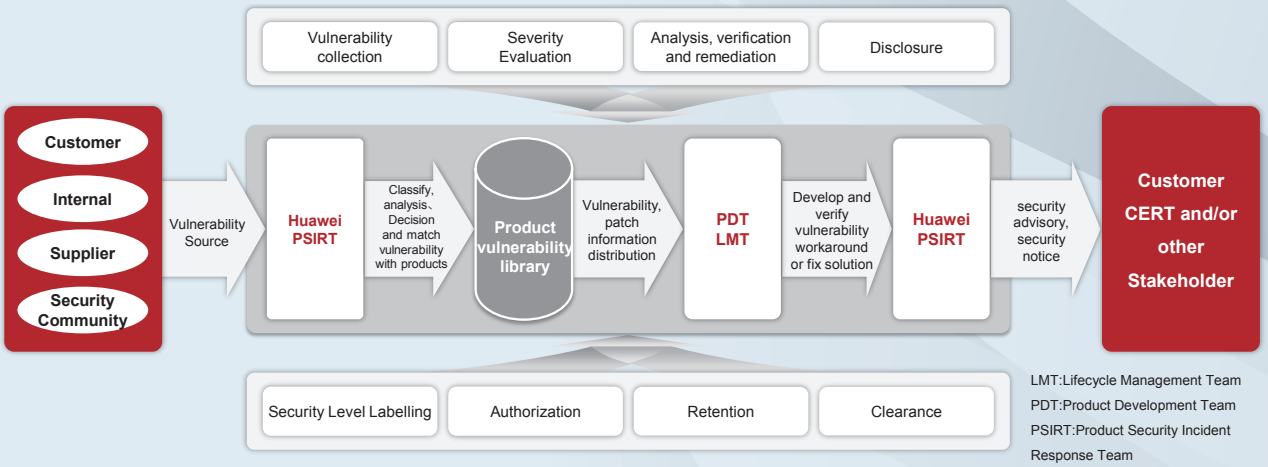


Figure 11, PSIRT/CERT process

In all stages of this process, protecting the confidentially of the customer and the vulnerability information is of paramount importance to Huawei.

In working with customers to address vulnerabilities, we have to recognise that not every vulnerability that exists can be exploited by hackers, as this is determined by the exact configuration and architecture of the network. For instance, if a vulnerability exists in a feature that is disabled by a particular network operator, or applies to an interface that is guarded by other security features, then exploitation may not be a practical concern.

As noted, the vulnerability information that is shared could have far-reaching consequences if it was to fall into the wrong hands. Confidentiality must be safeguarded by all parties. Therefore, the bi-directional relationship and trust between the vendor and the network operator is central to network security.

The Huawei PSIRT team is actively engaged at an industry and general public level in driving proactive change to enhance best practice and raise general cyber security awareness among regulators, legislators and business leaders. This includes, but is not limited to, membership in the Forum of Incident Response and Security Teams (FIRST), established connections with government CERTs, customer CERTs, other vendors, researchers, and third-party coordination bodies.

In order to contribute to enhancing understanding of this important issue among the cyber security community and to drive the alignment of international standards, Huawei actively participates in organisations such as the European Commission Network Information Security Forum.

Huawei believes that to counter the threat posed by cyber criminal activity it is essential that the industry adopt open and transparent methodologies to foster international cooperation and standards. The PSIRT is an example of this cooperation in action.

7.11 Traceability: finding the needle in the haystack

When things go wrong being able to quickly identify where it has gone wrong, what hardware or software component caused the issue and identifying where else that component is used is crucial to timely recovery. However, that is not enough; root-cause analysis demands an ability to forward and reverse trace every person, every component from every supplier in every product for every customer.

Imagine these news headlines in your country: "widely-used open source component contains critical weakness that allows hackers full access to computer systems", or "a supply of computer parts widely-used by tech vendors may have been compromised and installed into local networks".

The first question that a CEO might ask his IT security staff is "are we impacted by this threat" triggering security officers to immediately contact their ICT vendors asking a series of questions:

"Do you use this component?"

"If so, is it included in our equipment?"

"If so, which specific equipment contains the component and where was the equipment sent to?"

And, "when will a solution be available"

Huawei's handling of incidents is detailed in the discussion on our PSIRT process in section 7.10, "When things go wrong: Issue, defect and vulnerability resolution". When things do go wrong both PSIRT and the customer will need information in advance of the full review to assess the scale and scope of the potential risk. An ability to trace any software request from the customer throughout every stage of your process, from design, software coding, testing, QA, authorisation, live deployment and all the way back to the original source speeds up problem resolution. Vendors also need to be able to trace every hardware component from every supplier, route, factory, logistics method, R&D centre, and end-customer product and back to the original supplier.

The process for software traceability is detailed in the diagram below. Huawei traces forward from the original customer requirement through to the final product, and reverse, from the final product all the way through to the original requirement to cover all steps, all processes, all "who touched it", all components, all versions of the software and so on.

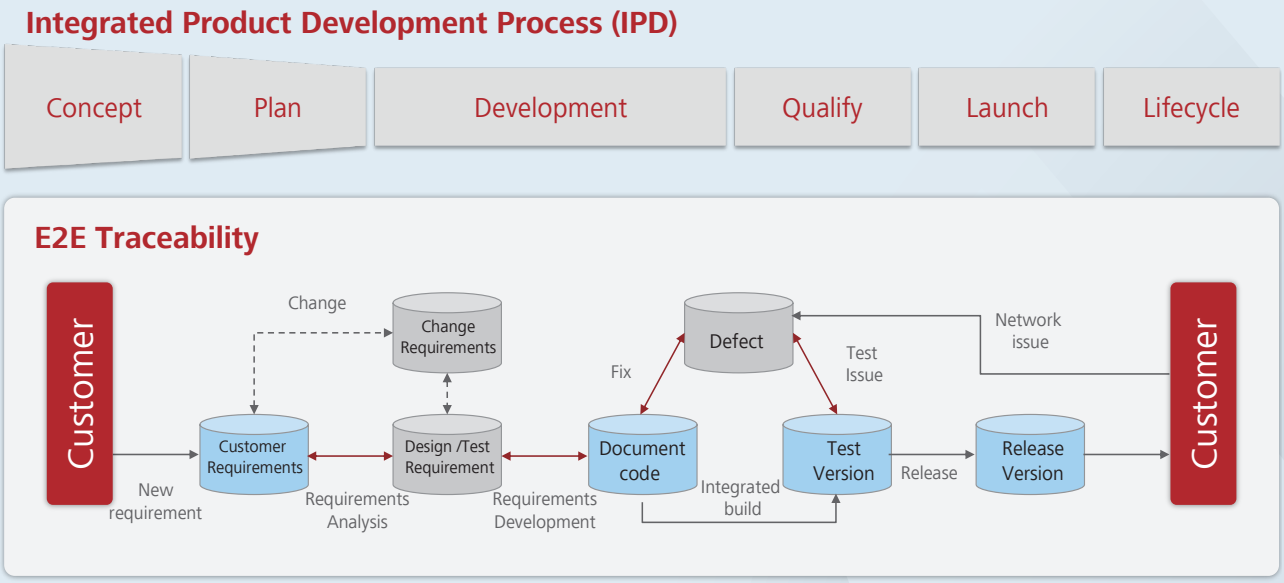


Figure 12, Software forward and reverse traceability diagram

We do the same for hardware. Huawei's bar-coding systems and Electronic Manufacturing Systems (EMS) allow us to forward and reverse trace 98% of all components used. The only items that are not traced are "non-technology" items such as fixtures, labels, packing materials, housing, instructions and documentation.

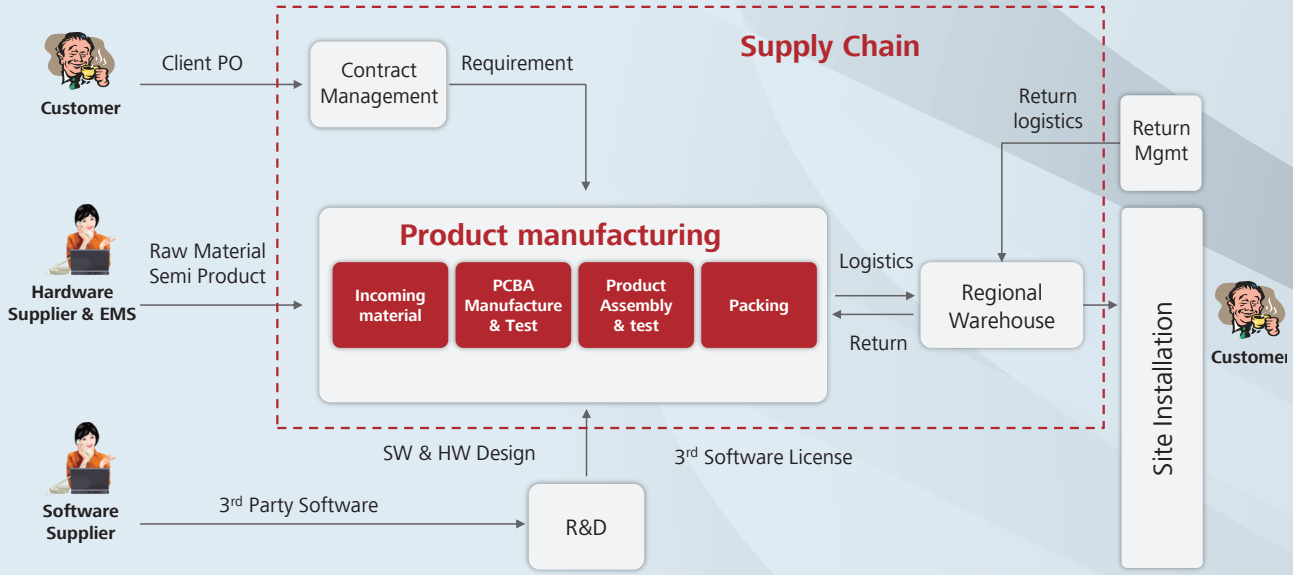


Figure 13, Hardware forward and reverse traceability diagram

In summary, forward and reverse traceability enables the identification of which employees have been involved with what product; who approved what product for implementation; which suppliers provided the components that went into what products; and collectively all of this enables issues to be found quickly and an assessment of the consequences of these issues to be made effectively.

7.12 Audit

Rigorous audits play a key role in assuring the Board and senior company officials, and assuring your customers, that the appropriate policies, procedures and standards are being executed to deliver the required business outcomes.

The Huawei audit process is risk-based and begins with the understanding of the business objective(s) associated with the environment under review. Audit focuses on the controls related to: compliance with laws and procedures, accomplishment of business objectives, reliable information for decision-making, efficient operations, and the safeguarding of assets.

This risk-based approach is established through detailed meetings and interviews with business owners and those involved operationally. When the objectives are clearly understood, an audit assesses and identifies the potential risks associated with the business area and those that would impact the achievement of the business objectives. As detailed in section 7.1, "Strategy, governance and control", process controls and key control points are embedded in each process to manage and mitigate these potential risks. An extensive testing strategy is designed and executed that seeks to identify any gaps, failure, strengths and weaknesses, and importantly, how best to assess if these controls have been implemented and executed as designed. The results of this testing are then used to focus on specific mechanisms that are in place (monitoring, measurement, and reporting), to understand how assurance is achieved on a day-to-day basis.

This same robust audit approach is used for Cyber Security Assurance, which from an audit perspective within Huawei focuses not only on the processes but also on the link between core business units that are essential in ensuring an end-to-end cyber security approach. This begins with a review of existing mechanisms to see how requirements from customers (Government, customers, end-users etc.) are managed through to major business processes, such as Integrated Product Development (IPD), where these requirements are analysed, solutions are designed developed and tested. Additional validation is undertaken to ensure the relevant business areas, such as Marketing and Sales, have received the necessary communication to be in a position to understand and advise on the appropriate product features for different markets based on local laws and regulations.

In between these steps supporting processes such as Procurement and Supply Chain are also reviewed to ensure qualified suppliers are used to provide products (hardware and software) that are in line with Huawei's cyber security requirements, and that the products delivered to clients are in fact the same as what were developed and tested prior to shipment (i.e. there is traceability and integrity).

The delivery mechanisms are also audited to ensure engineers and project managers are aware of cyber security elements that need to be included in processes such as Service Delivery for product maintenance and remote services, and Issue to Resolution (ITR) when customer goods are returned and privacy becomes a priority. The latter of which comes into play in closed-loop mechanisms that ensure we are responsive to any cyber security related incidents in a timely and efficient manner.

The audit approach is evolutionary; therefore changes in the market and within Huawei's business and operations will continue to drive the need for an on-going review of this strategy and approach.

8 Going forward together – pressing the reset button on security

It was Francis Bacon the English philosopher and scientist who said, "He that will not apply new remedies must expect new evils; for time is the greatest innovator".[14]

2013 will go down in history as a year where the sharp reality of the extent of digitisation and the way that technology has permeated all of our lives became real as we obtained a better understanding of the critical need to protect the privacy, integrity, and availability of personal and organisational data.

Building cyber security into a vendor's product goes hand-in-hand with the protection of citizen data. However, national security and personal privacy often appear to be on opposing ends and we must work collectively to optimise this balance.

The time has come to up the ante and concretely address the security challenge of global information infrastructure. While in the past we have looked at cyber security as an issue that could be dealt with locally, this hasn't yielded any significant results. On the contrary, the cyber challenge is more pressing now than ever. Governments, the industry and end-users worldwide need to collectively come to an understanding on how we will work together to define and agree on new, specific norms of behaviour, standards, and laws, and how we promote privacy and security in global networks.

In section 5, "Securing the future – security for tomorrow's world", we detail the way the world will change as the next wave of the digital society descends upon us, the way 5G technology will provide 100 times more speed than today and the way the world, economies and businesses will be redesigned, reconfigured and rebuilt.

Just as the pace of technological innovation continues to race ahead we must also accelerate our pace when considering the security needs of the future – we cannot drive the car by looking in the rear view mirror. For too long we have been discussing the same issues and challenges, still talking about cooperation, new norms, new standards and new behaviours, but without any concrete outcomes. The technological pace of change we will inevitably experience will jeopardise our success over the next ten years if we do not address these security challenges.

In our view, it is paramount that the entire ecosystem of governments, industry and end-users step up to collectively work on the problems and challenges we will face in the future. In doing so we should consider:

- The challenge of privacy in a digitised world: Given that much of our lives and business are online, with our data being globally distributed and processed in many countries by many technology vendors and governed under many different laws, we need strong and compatible legal frameworks, and globally-agreed rules of engagement and technology that support the protection of personal and business data.
- Thorough risk assessment practices: With the increasing rate and speed at which devices and users connect to the internet, combined with the continuous development of technology, society exposes itself to ever-evolving threats as well. Technology cannot be secured to the point of satisfying everyone's needs in every scenario. Strategic focus on a risk management approach that references the critical elements as described in this document, and

[14] http://en.wikiquote.org/wiki/Francis_Bacon

recognition of the fact that global networks rely on the global supply chain, are essential to enhancing cyber security.

- Customer is king: Buyers of technology - be it governments, enterprises or consumers - should use their economic buying power to demand more from their technology vendors and service providers. The top 100 questions we've collected from our customers can help buyers formulate their requirements and incentivise vendors to raise the bar on the assurance characteristics of their products. Because many major enterprises operate across national borders, these companies and vendors need to ensure compliance with regulatory frameworks while maintaining the benefits of economies of scale. The reality is that localised approaches to personal and organisational data hinder economic gains (and profit) and stifle innovation.

From Huawei's perspective we will continue to be passionate about working with governments, customers, standards bodies and other interested stakeholders to drive forward the quality and completeness of Huawei's end-to-end cyber security approach and ensure our technology complies with all of the applicable laws, regulations and codes. We will continue to champion the need for independent verification of products that enables many different stakeholders to satisfy themselves that a vendor's product is as safe as it can be. We will also work tirelessly with the ICT industry to ensure that all vendors are treated in a fair non-discriminatory way and collectively we use our talents to drive forward innovation to better the lives of citizens around the world – we will continue to do this in an open, transparent and collaborative way.

In our last white paper we proposed a set of principles:

Guiding Principles

1. IT'S GLOBAL: Efforts to improve cyber security must properly reflect the borderless, interconnected and global nature of today's cyber environment
2. IT'S THE LAW: We must harmonise and align international laws, standards, definitions and norms
3. IT'S COLLABORATIVE: Efforts to improve cyber security must leverage public-private partnerships. It cannot be a club of "some"; it must be a club for "all"
4. IT'S STANDARDS-BASED: We must agree on and implement international standards and benchmarks of ICT security
5. IT'S VERIFICATION-BASED: We must develop and implement global independent verification methodologies that ensure products conform to these agreed standards
6. IT'S EVIDENCE-BASED: Efforts to improve cyber security must be based on evidence of risk, evidence of the attacker, evidence of loss or impact and evidence of what works
7. IT'S DOING THE BASICS: All of us must implement basic cyber security "hygiene" so that we drive up the entry cost of attack

We believe that these principles are still valid today.

Huawei will continue to play our part as a leading global information and communications technology (ICT) solutions provider working with governments, customers and other stakeholders to live up to those principles and meeting their cyber security assurance requirements in an open, collaborative and transparent way.

9 About Huawei

Huawei operates in over 140 countries and our products and solutions serve more than one-third of the world's population. We employ 150,000 people and the average age of our employees is 31. On average, 73% of our people are locally-employed in countries in which we operate. As of 2012, we have deployed over 130 LTE commercial networks and more than 70 EPC commercial networks, ranking first in the world.

Huawei has a leading role in the industry through continuous innovation and has one of the most significant IPR portfolios in the telecommunications industry. Huawei respects and protects the IPR of others. Huawei invests 10% of its annual revenues into R&D and 45% of our employees are engaged in R&D. In 2012, Huawei invested USD4.8 billion in R&D, accounting for 13.7% of the total annual revenue. The total investment in R&D in the last decade is over USD19 billion.

As of the end of 2012, Huawei had filed 41,948 patent applications in China, 12,453 under the Patent Cooperation Treaty (PCT), and 14,494 patent applications overseas. We have been awarded 30,240 patent licenses, 90% of which are patents for invention. Compared to the quantity, Huawei attaches more importance to the commercial value and quality of IPR. Huawei holds over 15% of the basic patents in the new generation wireless telecommunication technology LTE and is in a leading position in terms of patents in FTTP (Fibre To The Premises), OTN (Optical Transport Network), G.711.1 (fixed broadband audio) etc. The protection of IPR is therefore critical to the ongoing success of Huawei, and because of this, Huawei is a champion of IPR protection.

We have 16 R&D centres around the world, 28 joint innovation centres, and 45 training centres. Overall, 68% of our revenue is generated outside of Mainland China, and we source 70% of our materials from non-Chinese companies. The United States is the largest provider of components at 32% -- some USD5.72 billion of Huawei's purchases were from American companies in 2012.

We provide managed services for more than 120 operators in over 70 countries to help customers achieve operational excellence and we have acquired an accumulated total of over 330 managed services contracts. Huawei has built cloud-based IT solutions and collaborated with over 400 partners to accelerate the commercial application of cloud computing technologies across various industries. By August 2013, we had helped customers around the world set up 330 data centres, including 70 cloud computing data centres.

In 2012, Huawei's consumer business shipped 32 million smart phones all over the world, an increase of 60% of that in 2011. The device shipments totalled nearly 127 million units, including 52 million mobile phones, 50 million mobile broadband terminals and 25 million home terminals.

Huawei is passionate about supporting mainstream international standards and actively contributes to the formulation of such standards. By the end of 2012, Huawei had joined over 150 industry standards organizations, such as the 3GPP, IETF, ITU (International Telecommunication Union), OMA, ETSI (European Telecommunications Standards Institute), TMF (Tele Management Forum), ATIS, and the Open Group, among others. In total, Huawei submitted more than 5,000 proposals to these standards bodies and we hold more than 180 positions in organisations supporting the drive for consensus and agreement on international standards.

By December 31, 2012, 74,253 employees had purchased an equity stake in the company. The Employee Stock Ownership Plan closely links Huawei's long-term corporate development with our employees' personal contribution and forms a long-standing mechanism for dedication and reward-sharing. This gives us the ability to take a long-term view; it also ensures we balance risk with reward and strategy. Employees know if we do not excel at serving our customers, or if we undertake inappropriate activities, their equity and pensions may be destroyed.

Copyright © 2013 Huawei Technology Co., Ltd. All rights reserved.

You may copy and use this document solely for your internal reference purposes. No other license of any kind granted herein.

This document is provided "as-is" without warranty of any kind, express or implied. All warranties are expressly disclaimed. Without limitation, there is no warranty of non-infringement, no warranty of merchantability, and no warranty of fitness for a particular purpose. Huawei assumes no responsibility for the accuracy of the information presented. Any information provided in this document is subject to correction, revision and change without notice. Your use of, or reliance on, the information provided in this document is at your sole risk. All information provided in this document on third parties is provided from public sources or through their published reports and accounts.

HUAWEI, and are trademarks or registered trademarks of Huawei Technologies Co., Ltd.

All other company names, trademarks mentioned in this document are the property of their respective owners.