HUAWEI

DIGITALL

INSIGHTS

Huawei's ABC principle in cybersecurity

Over the past 30 years, Huawei has served more than three billion people around the world. We support the stable operations of more than 1500 carrier networks in over 170 countries and regions. In this time, we have always maintained a solid track record in cybersecurity.

Cybersecurity is a global issue. No single government or company can tackle this challenge alone.

ICT products are the result of a global supply chain. A single piece of equipment typically includes components sourced from all over the world. To deal with threats effectively, we need global standards and internationally-agreed processes and best practices. A holistic and comprehensive approach is needed in which everyone takes their fair share of responsibility.

Collaboration with European partners to create a safer online environment is at the heart of our strategy.

Our approach to cybersecurity is that everything needs to be **built-in** rather than bolted on, and so we build security into every single aspect of our company, from strategy, governance and standards, to processes, manufacturing, third-party management, delivery, human resources and audit, as well as demanding the strictest compliance from our global supply chain.

Looking to the future, we want to do more. We will keep investing substantially in our cybersecurity and technical capabilities.

The **Huawei Cybersecurity Transparency Centre** at 9 Rue Guimard in Brussels is an important milestone in this commitment. It offers government agencies, technical experts, industry associations and standards organisations a platform where they can communicate and collaborate to balance out security and development in the digital era.

The centre has three major functions:

1. It showcases Huawei's end-to-end cybersecurity practices, from strategies and supply chain to R&D and products and solutions. This will allow visitors to experience cybersecurity with Huawei's products and solutions, in areas including 5G, IoT and Cloud.

2. The centre facilitates communication between Huawei and key stakeholders on cybersecurity strategies and end-to-end cybersecurity and privacy protection practices.

3. It provides a product security testing and verification platform, and related services, for Huawei customers.

Common challenges

Right now, there are four main challenges to building trust:

1. Fast-developing digital technology has brought new security challenges. As more digital content and services are migrating to cloud data centres and more devices go online, networks have greater attack surfaces than ever before.

2. The global community lacks a common and unified understanding of cybersecurity. Both the public and private sectors lack a basic common understanding of this issue. As a result, different stakeholders have different expectations, and there is no alignment of responsibilities.

3. The industry lacks a unified set of technical standards for security. This is complicated by globalisation of the value chain. There is an urgent need to invest in security standards and verification systems, as well as in professional resources and skills.

4. Governance is key. In some countries, cybersecurity management lacks legislative support, and cybersecurity enforcement is not mature.

Cybersecurity is a challenge we all share. To address these challenges, mutual understanding is the starting point. To build a trustworthy environment, we need to work together.

ABC principle

At Huawei, we use the ABC principle for security:

- Assume nothing.
- Believe nobody.
- Check everything.

Trust needs to be based on facts. Facts must be verifiable, and verification must be based on common standards. Huawei believes that this is an important model for building trust in the digital era.

Huawei EU press contacts:

Jakub Hera-Adamowicz | **Yingying Li**

+32 499 641 839 | **+32 470 779 011**

Find out more: www.huawei.eu

Published May 2019