TRUST IN A HYPER-CONNECTED WORLD

Ericsson has a vision of the Networked Society and when everything gets connected, society, industries and people will be immensely affected. The recent Ericsson Mobility Report[1] estimates that the global number of connected Internet of Things (IoT) devices will surpass the number of mobile phones by 2018. This means that digital opportunities and risks will expand beyond human connectivity.

5G is opening for even more IoT use cases with vastly diverse requirements. Some 5G use cases support machine-type of communication with ultra-reliable connectivity. Other use cases are optimized to enable long battery life and very low cost. These requirements call for a new generation of services with a new set of security demands.

ICT infrastructure is becoming increasingly mission-critical for large industry as well as society, for example in cases of remote control and monitoring of industrial systems, self-driving vehicles and more. The availability and functionality of these services depends on the underlying ICT infrastructure. Cyber-attacks with safety implications are unfortunately becoming realities.

With more data residing in the cloud, traditional perimeter protection will no longer be enough. When data flows across organizational boundaries and nations, it must be protected at all stages; when it is generated, stored, transmitted, and used. This must be done over both trusted and untrusted infrastructures.

5G opens even more IoT use cases with vastly diverse requirements and trust models

ICT infrastructure is becoming increasingly mission-critical for large industry as well as society

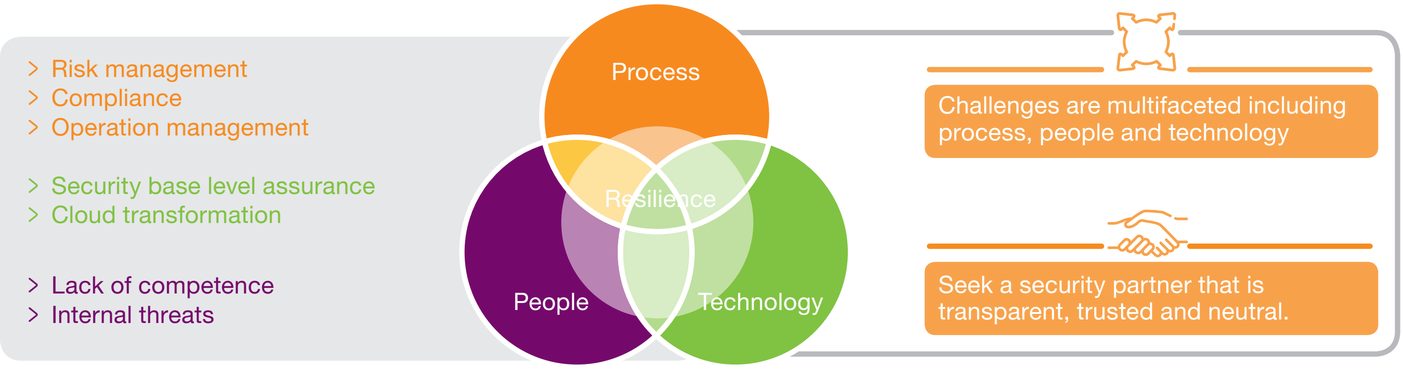
Data must be protected at all stages; when it is generated, stored, transmitted, and used.

Challenges

Every new connected device represents an additional security risk which requires holistic security thinking spanning new business models, technologies, standards and regulations. The traditional principles of risk and security management, such as check-box compliance and access control are being challenged. Security in the digital economy is a balance between the risk of cyber threats and the resilience citizens, business and society demand.

Today's challenges are multifaceted; true cyber readiness comes from process, people and technology. It is important to have an agile and responsive process that is integrated into existing policies of organizations and authorities. Security responsibility cannot reside only within the security department; it should be integrated across all organizations. The lack of security expertise and the risk for internal threats create additional challenges for companies. Existing security solutions are often cumbersome and complex, and legacy networks may have to adapt to new security demands. Stricter security regulations and global variances across regions will magnify operational complexity. In order to cope with these challenges, business and organizations should seek a security partner that is transparent, trusted and neutral.

[1] https://www.ericsson.com/mobility-report



- Risk management
- Compliance
- Operation management

- Security base level assurance
- Cloud transformation

- Lack of competence
- Internal threats

Challenges are multifaceted including process, people and technology

Seek a security partner that is transparent, trusted and neutral.

Important security areas

A secure communication infrastructure for 5G and IoT is the foundation for the networked society. All services for society and business will share the same infrastructure but with different security requirements. Cloud security is one of the top concerns for operators, enterprises, governments and regulators. With increasing data volumes and access to data by many parties for many purposes, it becomes key to prevent unauthorized access as well as ensure the integrity of data in real-time.

There is an extensive demand for digital identity across industries. Solid identity validation, consent and trust management are fundamental elements to build secure services. Trusted computing technologies are becoming vital to ensure end-to-end security, from device and through the whole network.

As the threat landscape evolves, products, services, processes and technologies need to be equipped with capabilities to detect, respond and stop attacks both from outside and inside before causing damage.

All services for society and business may share the same infrastructure but have different security requirements

Products, services, processes and technologies need to be equipped with capabilities to detect, respond and stop attacks from outside and inside before causing damage.

Ericsson and security

Ericsson celebrated 140 years in 2016 and does business with customers in 180 countries. We are a software-dominant company with 39,000 patents and to protect our own vital digital assets we have implemented rigorous information security processes to mitigate an ever-increasing threat landscape.

Ericsson has built the world's largest infrastructure, serving 2.5 billion mobile users.

Security technologies and controls need to be an integrated part of all products, solutions, deployments, integrations and managed operations.

We run telecom systems on behalf on telecom operators and operate telecom infrastructures serving one billion subscribers. We have built the world's largest infrastructure, serving 2.5 billion mobile users. Significant for communications networks is the large scale, in terms of users, services and systems - and high level of complexity.

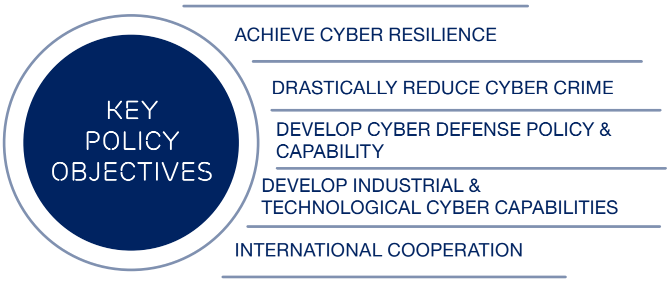
To achieve the required security in a network with these characteristics, security technologies and controls need to be an integrated part of all products, solutions, deployments, integrations and managed operations. In addition to securing that all products fulfill security requirements, Ericsson has a complete portfolio of both security solutions and security consulting services. Ericsson also manages security for customers within various industry segments. Standardization within security is important, and Ericsson is an active driver in relevant security forums and working groups.[2]

Ericsson and public cyber security policy

Cyber security policy needs are a complex and comprehensive topic. Given the context, some key high-level recommendations to governments are as follows:

- Respect human rights and rule of law requirements when pursuing cyber security objectives
- Enforcement powers must be subject to safeguards to ensure that rule of law and human rights
- Policy must be technology neutral and non-prescriptive to cater for the constant evolution of technology and crime as it otherwise risks becoming obsolete very quickly
- Policy must be sufficiently harmonized or at least compatible with the laws of other countries to permit international cooperation.

An effective response can be built on a national cyber security strategy pursuing the following key objectives:



ACHIEVE CYBER RESILIENCE
DRASTICALLY REDUCE CYBER CRIME
DEVELOP CYBER DEFENSE POLICY & CAPABILITY
DEVELOP INDUSTRIAL & TECHNOLOGICAL CYBER CAPABILITIES
INTERNATIONAL COOPERATION

A resilient national cyber security strategy aims at protecting and defending, including the capability to comprehensively mitigate cyber-attacks. It also aims at deterring cyberattacks with resources to detect, understand, investigate, and disrupt cyber actions. Fostering collaboration with universities, public authorities, governments and the private sector will further develop and enhance cyber security capabilities across industries and technologies. Since cyber-attacks know no borders, international cooperation is necessary to achieving the secure Networked Society of tomorrow.

[2] 3GPP Security, ENISA, ETSI Cyber Digital, ETIS Information Security, Cloud Security Alliance, FIRST, TF-CIRT, IETF Security and more.

Ericsson
SE-164 80 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com