
Safety
and Security

Digital literacy encounters the challenge of moving from searching, finding and understanding digital information to managing digital footprints, being aware of copyright issues and behaving ethically in crediting ownership, cognisant of the lasting imprint of information online and managing issues of privacy and constructive presence.
Safety and security have become critical issues. In adopting cloud services, robust and efficient identity management is a key business necessity for both cloud service providers and cloud consumers.
In the energy domain Europe is transforming a current traditional electricity network into an advanced, digitised and more efficient Smart Grid. However, both here and in the ever more connected automotive domain, massive data collection also creates new security challenges that have to be tackled. The digital transition is reshaping all of society, exercising control through data flows. Anything arising from these data flows (attacks, bugs) may generate significant damage to our society in the physical sense, too. For all the benefits the digital world brings, there are always threats, and there lies the challenge for Safety and Security.

Some facts and figures

- In 2014, CSIS & McAfee estimated that the likely annual cost to the global economy from cybercrime is more than USD 400 billion. A conservative estimate would be USD 375 billion in losses, while the maximum could be as much as USD 575 billion. [26]

- Businesses suffered nearly 43 million known security incidents in 2014. This increased by 48% compared with 2013 and equals some 117,000 attacks daily. [27]

- In 2016, email posed a dangerous and efficient threat to users: one in 131 emails contained malware, the highest rate in five years. And Business Email Compromise (BEC) scams, relying on spear-phishing emails, targeted over 400 businesses every day, draining USD 3 billion over the last three years. [28]

- Ransomware has escalated across the globe as a profit centre for criminals. In 2016, Symantec identified 100 new malware families released into the wild, more than triple the amount seen previously, and a 36% increase in ransomware attacks worldwide. [28]

- It's only a matter of time until we see major industrial control system (ICS) attacks. Attacks on ecommerce stores, social media platforms and others have become so commonplace that we've almost grown cold to them. Bad guys will move onto bigger targets: dams, water treatment facilities and other critical systems to gain recognition. [29]

Imagine ...

Imagine investing a huge amount of effort in the digital transition of society, a transformation that will generate huge quantities of data flows that contain everything you are doing and all the command & control signals of society worldwide. These data flows will be susceptible to thieves, terrorists and uninhibited businessman to spy on you, blackmail or intimidate you, or even to command & control the different systems such that they destroy the quality of lives or even lives themselves. The dream of developing some new engineering tools to reduce the number of breaches in the software, to protect access to the data flows for those who need to know and exclusively for them. To have dynamic agents continuously analysing how the data are used and detecting any misuse or bugs so that they can react in real time and adapt the software to protect the end users. Imagine keeping all your data digitally without having the worry of it being misused, stolen or monitored.

Imagine what is possible when we dare to dream, when we reach for the stars in a galaxy full of opportunities ...