Better information is crucial

Cyber-attacks occur are **known** to occur in businesses, households and government bodies

It is **unknown** how often disruptions occur, by who and what the consequences are

Users might therefore **overinvest or underinvest** in cybersecurity

Cyber Security Risk Assessment for the Economy 2019

Risks of disruption

Threats are complex and constantly evolving

Critical processes have become more vulnerable to ICT-disruptions. This could lead to disruptions of society

Non-critical processes are entwined with critical processes which makes the chain more vulnerable

New risks

Artificial intelligence makes personalized attacks possible and can find system vulnerabilities more easily

5G facilitates new Internet-of-Things applications. This makes cybercrimes more visible outside of the digital world

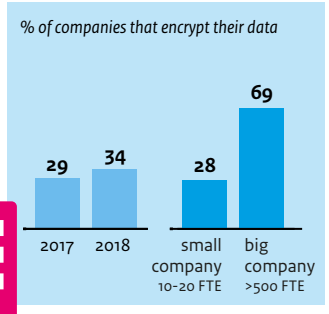
Challenges for businesses and citizens

- How much do we invest in cybersecurity? Effects of investments are hard to quantify
- How can we keep up to date if threats and security measures develop so fast?
- How to guarantee security in a chain of ICT-applications?

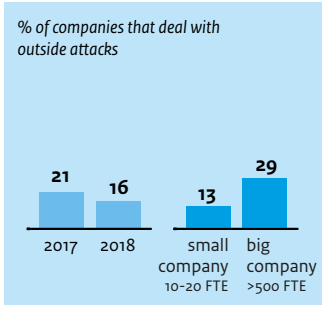
Challenges for government

- How to inform millions of users and hunderds of thousands of businesses?
- Leave measures against disinformation to social media or regulate?
- How effective is stimulating cooperation between organizations?

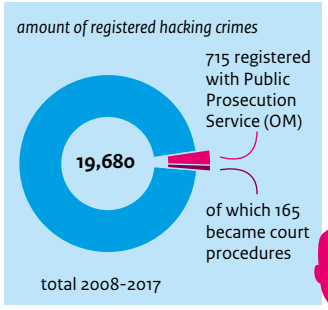
Small companies take less measures compared to big companies



Companies report **fewer ICT-incidents**



Most cybercrimes **never reach a judge**



source: CBS