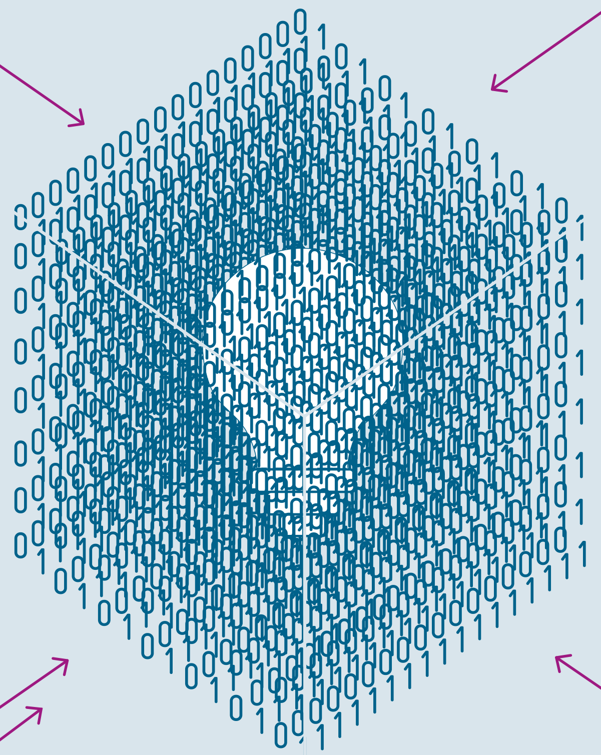
B 2 Cybersecurity

Ongoing digitalization and connectivity make companies more vulnerable to cyberattacks. Corporate innovation activities are directly affected by this threat.



Malware performs unwanted or harmful functions on a computer system.

Ransomware is used by attackers to encrypt the data in an IT system to prevail upon users to pay a ransom.

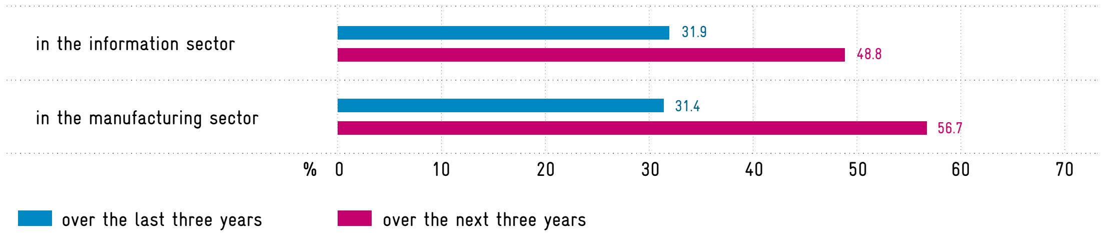
Advanced persistent threats have a high threat potential because the attackers find weaknesses in a targeted and persistent manner in order to exploit them.

Social engineering manipulates people to persuade them to disclose confidential information, open files or links with stored malware, or transfer money to unauthorized recipients.

DDoS attacks cause network services to fail after they have been overloaded and thus blocked by a huge number of requests.

Assessments by companies on the development of the threat from cyberattacks[1]

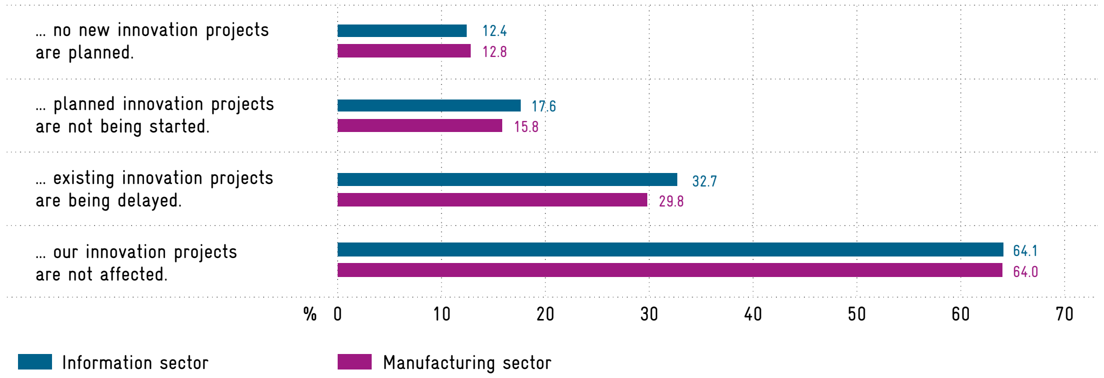
Increase or sharp increase in the threat from cyberattacks ...



Sector-specific extrapolation of results to the question: "How do you assess the change in cyberattack exposure for your company?" Legend: 56.7 percent of manufacturing companies expect the threat of cyberattacks to increase or rise sharply over the next three years.

Impact of cyber threats on innovation activities[2]

Because of the threat of a cyberattack ...



Sector-specific extrapolation of results to the question: "What impact is the threat of a cyberattack having on your company's innovation activities?". Multiple answers possible. Legend: 12.8 percent of manufacturing companies are not planning any new innovation projects because of the threat of a cyberattack.

See chapter D 7 for a list of sources of infocharts.