Telekom CR-facts

Emerging Risks

Emerging risks are difficult to predict as their development is highly uncertain. They are external risks occurring beyond our influence or control such as natural factors, geopolitical tensions, new technologies, or macroeconomic factors. These risks are newly identified risks expected to have long-term impact on our business (at least three to five years). Although they may have already affected our business today, their importance is expected to significantly increase and they can potentially and significantly be harmful to a large part of our operations.

In order to protect our company and our customers against such risks, we need to act early and effectively to identify and assess such risks and if necessary, adapt our strategy and/or business models to reduce their effects. The tasks of our risk management system, which systematically identifies these emerging risks, evaluates their potential impact on our company and derives mitigation measures to respond to such emerging risks for Deutsche Telekom (DTAG) in a comprehensive way.

The following most significant emerging risks are expected to have long term impact on DTAG:

Technological Risk - Cyberattacks

Cyberattacks are an external and rapidly growing risk. As the speed of digital transformation, machine learning and computing power will grow exponentially, the methods of attack are becoming more specialized and efficient and are outpacing improvements in security. Thus, this development eventually leaves more available points of vulnerability in our business that can be impacted by such

attacks. Therefore, the importance of the risk of cyberattacks is significantly increasing to us.
The impact is significant and specific to our company:

- the need for more sophisticated infrastructure in order to prevent autonomous and artificial intelligence supported cyberattacks requires shifts in business strategy and further investments
- compliance of any increasing legal requirements for data storage and protection may impact our business strategy and investments
- the gap between existing and expected employee skills in cybersecurity may affect business progress
- new extortion techniques becoming more common in attacks, such as cryptocurrency payouts, leading to financial losses
- reputation effects: our customer bases decreases because they may lose trust in the quality of our communication services.

Our mitigation measures include:

- upgrading to more-robust IT-control environments
- enhancing protection against common attack types
- using machine-learning techniques (artificial intelligence) for the detection of network penetration
- response improvement for warding off detected attacks
- raising customer awareness about cyberattacks
- providing better malware detection and improving user authentication techniques.

Environmental Risk - Extreme Weather

The ongoing climate change is expected to accelerate the intensity and frequency of extreme weather conditions, such as flooding and droughts that negatively affect our operations. The climate change impact is difficult to predict as its mitigation requires global efforts.
The impact is significant and specific to our company:

- disruption of network and infrastructure due to
  - damage to our base station sites, network nodes or other infrastructure
  - damage to data centers, radio towers, office buildings and our sales stores
  - reduction of stability of our power supplies
- longer network outages
  - eventually affect management of restoring operations, which may fall back to Deutsche Telekom and damage our reputation
  - lead to customer complaints and in long-term decreasing customer satisfaction and reduced revenues
- additional investments will be necessary to modify our processes, harden our infrastructure and repair damages
- the cost for insurance coverage for such events is expected to steadily increase over time and could also result in substantial property and liability losses.

Our mitigation measures include:

- improving methods of predicting when and where possible future disasters could occur including scenario analyses and physical risk assessment
- identifying weaknesses in our radio towers and other infrastructure
- implementation of a business continuity management including improving business-continuity and disaster-recovery plans for scenarios where such failure events could occur
- installing backup power to all critical network elements in order to avoid network outages or reduce downtime
- modernization of network to be better protected from storm conditions, changes in temperature, and high winds.
- regular assessments to ensure sophistication and resilience of infrastructure facilities.

Economic Risk - Infectious Diseases
We cannot predict the outbreak of a pandemic. However, historical data shows that over the past few decades regional and global pandemics occur more frequently over time. A new disease or virus can quickly spread, become a pandemic, and drastically hamper global economic growth. It can affect multiple industries and global supply chains, and it can have a major impact on the ways in which we live and work.

The impact is significant and specific to our company by:

- increasing delays from our suppliers, payment delays and defaults from our business customers and consumers; thereby increasing our level of bad debt
- related restrictions on public life could force our stores to close and affect or sales and services to customers. customer growth could be dampened as it becomes difficult to acquire new customers
- related travel restrictions could reduce our roaming-traffic volume and revenues
- social contact restrictions leading to home-schooling and working from home could overload our networks and reduce its efficiency; at the same time our employees face higher stress levels; due to working from home companies could see a need to reduce their orders of IT services and equipment
- in the case of a severe pandemic restrictions could temporarily or permanently reduce our workforce.

Our mitigation measures include:

- monitoring relevant developments by our Group Situation Center enabling crisis management and task forces
- issuing pandemic guidelines
- provides suitable hygiene and health & safety equipment for sales stores, offices and our network infrastructure locations
- ramping up and stabilizing our networks to accompany additional peak loads of voice and data traffic
- protecting our customers and employees by allowing remote working
- focus on online sales and customer service.