Telekom CR-facts

Emerging Risks

There is a strong need to predict and prepare for long term risks that could occur in the future. Although these risks are difficult to spot, they can have a significant impact on our company. It is therefore necessary to effectively identify and evaluate such adverse events early and develop mitigation strategies to protect our business and our customers against such risks. Having a comprehensive view of emerging risks for Deutsche Telekom is part of our risk management system, which systematically identifies, assesses, and manages relevant risks.

These emerging risks are categorized into political, economic, social, technological, environmental and regulatory/legal events that could occur. The assessment factors considered include velocity and novelty of the risk and relevance for our industry and business in the years ahead.The following emerging risks are on the rise:

Technological: Cybercrime is exploding. Digital transformation, expanding device adoption, machine learning and other applications of exponential increase in computing power are trying to outpace current security protection. As the number of entry points into organizations grows, and cybercrime becomes ever-more profitable, the number of cyberattacks will continue to rise.
Risks include hackers deploying ransomware that can block access to data and key systems (either by exploiting security holes in companies' networks or using phishing emails to harvest credentials and gain entry), AI-powered cyber-attacks will become more autonomous and self-propagating, learning the target's network environment rather than relying on known or common vulnerabilities.
Ongoing mitigation measures include creating a more robust IT control environment to increase prevention of these common attacks; deploying (Artificial Intelligence) machine learning techniques into network intrusion detection and

strong effective reaction capabilities to defend against detected attacks; improving malware detection and secure user authentication and raising cyber awareness to reduce potential cyber breaches.

Economic: A pandemic crisis is impossible to predict, but historical data shows that in the past decades regional and global pandemics have been occurred more rapidly. A new pandemic can drastically reduce economic growth globally affecting multiple industries, supply chains and how we live and work.
Relating risks could be higher payment delays and defaults of our business and consumer customers increasing our bad debt. Possible lockdowns would force shops to close and travel restrictions would reduce our subscriber growth and the volume of roaming traffic. Additionally, companies could reduce their IT orders. Social distancing and homeschooling could lower overall efficiency or in the case of a severe pandemic temporarily or even permanently reduce our workforce. All of this could in turn, lead to a decline in revenue.
Our Group Situation Center monitors the development of any emerging pandemic. As part of our crisis management, they communicate pandemic guidelines and provide hygiene and safety equipment to all shops, offices and infrastructure sites to protect customers and employees. Other group wide mitigation measures include ramping up and stabilizing our networks to ensure our network can handle additional surges in voice and data traffic. To minimize the spread of a possible outbreak, employees may work from home and our sales and service teams can reallocate to meet changing demands.

Environmental: Natural Disasters such as flooding, severe storms, hail, heat waves, wildfires, hurricanes and earthquakes are occurring more often. The physical effects of our changing climate are leading to ocean warming, heat and humidity increase and increasing average temperatures and humidity levels. Therefore, these extreme weather scenarios are likely to intensify in the future.
As more natural disasters occur, specific areas will become more vulnerable to flooding, storms, or heat and could increase the number of network outages of our network infrastructure (direct damage) or affecting the relevant supply of power or water (indirect damage). This in turn could lead to loss of revenues or lower customer satisfaction.
Mitigation to reduce such network outages include analysis of previous and forecasting of possible future disasters to identify weak spots in areas that are

more prone to stronger and more frequent disasters. Any identified weak spots in our network equipment would be upgraded to increase robustness against such disasters. Furthermore, detailed business continuity and disaster recovery plans are in place in case such events should occur.

Content Owner:
claudia.kurpiers@telekom.de
