# Telecom Outlook: Rising cyber threats a cause for concern, as well as a source of success

Cybercrime is a double-edged sword for the telecoms industry, which benefits from the rising demand for cybersecurity services, but also faces pressure to secure client data

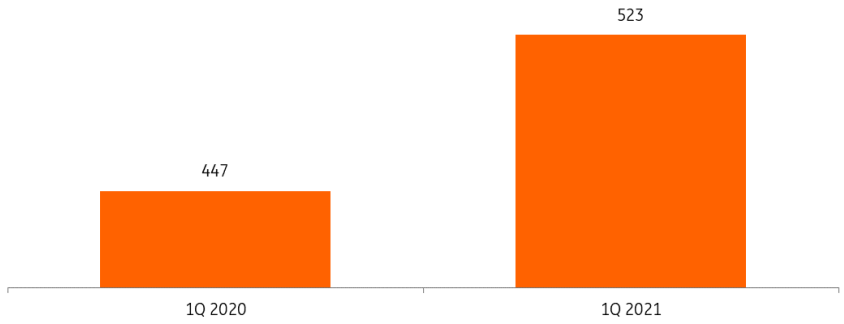
Over the past few years we have seen a rise in both the number and sophistication of cyber attacks

## Cybercrime on the rise

The past few years have shown an almost continuous rise in both the number and sophistication of cyber attacks. The digitisation of business means a larger part of the economy is a potential target. This was accelerated by more people working from home during the Covid-19 pandemic. We're also seeing that the attack surface is on the increase as the number of connected devices grows and the cloud expands. The number of attacks, and the impact they're having, has grown because of the cybercriminals' increased professionalisation, automation, and the limited risk of being caught. As these trends are not at an end, we can expect the cyber threat to continue to rise in 2022.

## Publicly disclosed cybersecurity incidents rise in 2021

Number of reported breaches worldwide, per quarter

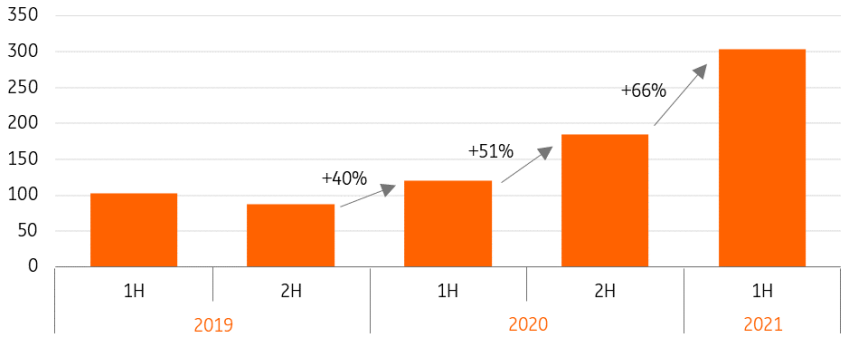



Source: McAfee Labs

## Ransomware a major threat

From the second half of 2019 onwards, ransomware attacks have grown in number. It is mainly the professionalisation of the cybercriminals that drives this growth. Cybercriminals also benefit from the anonymity that cryptocurrencies offer, for example, and many now have the financial means to buy zero-day exploits (weak spots in software unknown to the software developer) increasing the chances of a successful attack. There is a whole chain of criminals with special expertise in every link, generating billions globally. For the victims, the damage is a lot bigger than the ransom that is paid.

## Large rise in ransomware attacks




Source: SonicWall, ING Research

## Growing reliance on mobile encourages attacks

Mobile devices and networks continue to be a target of cybercriminals as well. The number of mobile malware attacks is likely to increase as the use of mobile productivity apps, banking and payment platforms, and data storage solutions continue to grow. During 2020 and 2021, new security threats emerged trying to exploit the growing reliance on mobile devices. Mobile malware, and specifically banking Trojans, for instance, are targeted at intercepting text messages on devices, compromising the two-factor authentication security protocols.

## Cyberthreat especially relevant for telecoms industry

Telecommunication companies are a major target for cybercriminals and nation-state actors because they build, control and operate critical infrastructure that is used to transmit and store large amounts of sensitive data. Securing client data is therefore a key component in protecting the operator brand. The surging complexity of networks increases the complexity of cybersecurity. Virtualisation means networks become more vulnerable to software-based attacks.

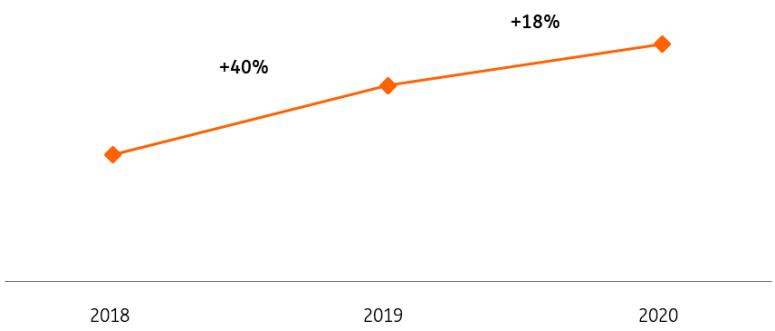
The integration of more and more technologies potentially creates further vulnerabilities, while increased network connectivity (e.g. to the cloud) also complicates security efforts. A recent cybersecurity incident shows that the threat is very much real. In August 2021, a hacker accessed 50 million customer records of US operator T-Mobile. Operators will therefore have to increase investments in cybersecurity while also keeping in mind the additional security efforts required by the Internet of Things (IoT) and the roll-out of 5G, and the increase in connected devices with it. Note that 5G technologies are said to be safer than older technologies.

## Leveraging on cybersecurity capabilities

While the threat of cyberattacks poses a challenge for the sector, it is simultaneously a business opportunity. Besides being an integral part of network services, several telco's such as KPN, Telefonica, Orange and BT offer stand-alone security services. In defending against cyberattacks, telco's have developed capabilities they can sell, while they have the possibility to leverage on an existing customer base. Through acquisitions and organic growth, operators expand their security services. Recently, BT acquired Safe Security, while Orange bolstered its security business back in 2019 by adding SecureLink and Secure Data Group. Scale is an important factor in security services. Most small and medium-sized enterprises do not have in-house cybersecurity expertise and therefore rely on managed services. These services could also help increase customer retention rates.

## Strong growth of telco global security services revenue

Revenue in EUR billions and percentage increase




Source: TM Forum

## Small but growing revenues

Currently, security revenues make up a small part of overall telco revenues, with Telefonica and Orange, for example, generating 1-2% of total revenues in cybersecurity. Growth, however, is high;

for Orange, cybersecurity revenue grew by 14% in the first half of 2021.

Demand for managed security services in general is driven by the increasing value of digital services, a shortage of skilled cybersecurity personnel, and the growing complexity and risks due to the diversified IT landscape combining cloud, edge and operational technology. With many telcos viewing cybersecurity as a significant opportunity for services growth, we can expect the deployment of services such as 5G, cloud, IoT and edge to contribute to further growth in their cybersecurity business.

The cybersecurity market is very fragmented. Customer demand is driving offerings towards integrated security software and services, with companies offering security platforms, not single solutions. We can therefore also expect more mergers and acquisitions in the security area and partnerships with vendors.

## Author

**Jan Frederik Slijkerman**
Senior Sector Strategist, TMT
jan.frederik.slijkerman@ing.com