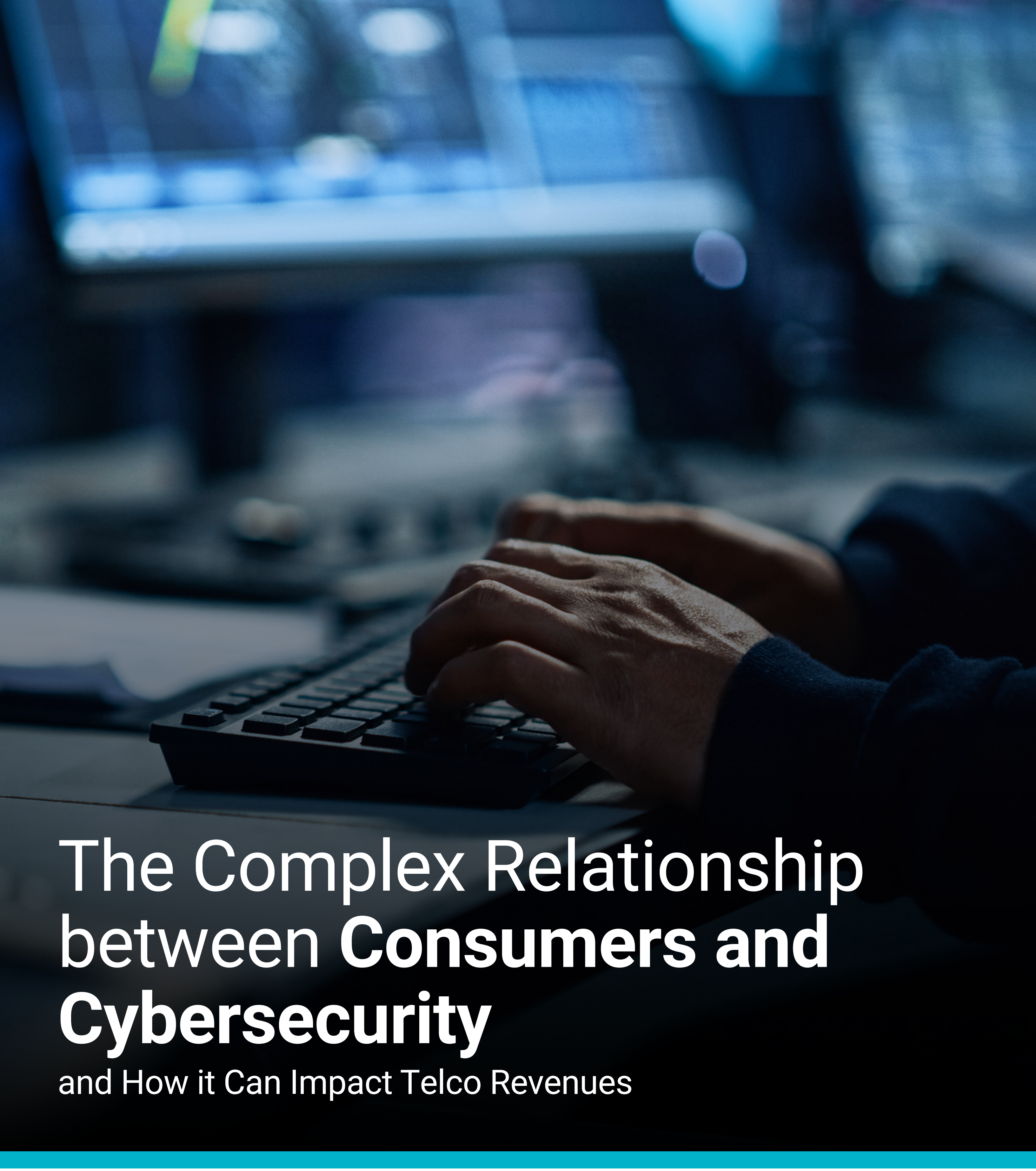


The Complex Relationship between **Consumers and Cybersecurity**

and How it Can Impact Telco Revenues

Sponsored by

Bitdefender

telecoms.com

Executive Summary

The need for constant connectivity – further accelerated by the pandemic – has increasingly opened opportunities for cybercriminals to infiltrate and exploit vulnerabilities in devices and in consumer habits. As the industry continues to undergo a digital transformation based on cloudification and virtualisation of services, there are also greater risks of misconfiguration of data storage and security breaches. These have set the stage for some of the most unprecedented growth rates in cyberattacks globally in recent years. According to the Verizon Mobile Security Index Report 2022, based on companies' self-admission of suffering a security compromise, cyberattacks have increased at a 14% compound annual growth rate over the past five years.

In this paper, we will explore consumers' attitudes and behaviours towards threats and vulnerabilities as well as the routes to solutions and how service provider bottom-lines can benefit from improved solution provision.

Attitudes and Behaviours Towards Cybersecurity Threats and Vulnerabilities

The accelerated shift to working from home, as well as the increased consumption of social media, online shopping, and streaming services, have all contributed to the changing behaviours of consumers both at home and in their professional world. Consumers are continuously switching between online platforms and accounts. In fact, a recent study which investigated cybersecurity and internet users' online behaviour[1] has found that on average consumers use eight different platforms.

The same piece of research also discovered internet users' typical accounts include Amazon, Facebook, WhatsApp, Gmail, and YouTube. Internet users adopt varying methods for managing these account details with half relying on reusing memorised passwords, a third on autofill options and a further quarter writing their passwords down or making use of a password manager. However, for some accounts, such as car services/rentals (60%) or video streaming (49%) many users share account details.

Adding to that, connected devices play a key role in the modern home, especially with the merging boundaries of private and professional life. Most consumers often use at least three devices to access their online platforms and accounts with mobile phones as the most frequently used device for half of those users, yet with use highest among younger generations (up to the age of 44).

These increases in number and type of devices, combined with the rise in number of platforms and accounts used, have meant a 22% rise in major cyberattacks in the last year which involved a mobile or Internet of Things (IoT) device in the US alone.[2] But cybercriminals have taken further steps, feeding off the nations' fears around a global pandemic, criminals upped their threats with healthcare related spams which alone accounted for an average of 19% of the global spam volume in 2021.[3]

With both digital activity at such an all-time high and unparalleled increases in threats, it is prudent to understand consumer attitudes towards threats and vulnerabilities better and to uncover the opportunities it creates for awareness raising and consumer engagement.

While many internet users confirm they are familiar with changing privacy settings and reviewing privacy aspects when signing up for a new account, many also admit that creating new passwords and the use of multi factor authentication are disliked chores. As such, there is no surprise that over 60% of these users have experienced some sort of threat in the past year.[4] Meanwhile the largest area of concern for consumers is falling victim to a potential financial fraud scheme at 41%, followed by a data breach (35%) and ransomware (35%).

Yet, despite experienced threats and vast concerns over cyberthreats, on average a third of consumers still lack the right security measures on their main devices, with 15% not using any type of protection for online data security and privacy on their most used devices at all.

To some extent, the behaviours are explained by personal beliefs, such as deeming their habits to be safe enough that security solution are not needed (14%). But many also have the misconception that smartphones are sufficiently safe devices in aspects related to malware or privacy or that they have embedded security already (a combined 31%).

Yet another 30% of internet users also believe that they don't need security solutions on their phones. Combine these findings with other vulnerabilities, such as using repeated or few passwords, and it quickly becomes clear how cybercriminals have been dealt an easy hand and a call for action becomes imminent. Raising awareness and educating internet users over threats and available protection, however, could drive the usage of security products and services on devices, including mobiles.

A greater emphasis on protection for mobile phones is needed as these not only are more exposed but also more users lack security products on their mobile devices compared to other devices. Additionally, mobile phones are used more by younger consumers who have fewer concerns over threats and vulnerabilities.

ISPs Can Improve Bottom-Lines By Raising Awareness, Educating Consumers, and Providing Solutions

Internet service providers (ISPs) and the telecommunications industry are facing an ever-growing demand for tighter security measures by governments and industry alike. A recent data breach in Australia compromising personal data from 9.8 million telecom customers has led the government to contemplate tougher cybersecurity laws. Meanwhile the UK government has initiated plans of its own for tighter security measures as its communications regulator Ofcom seemingly does not trust the network operators' security measures.

Often cited as one of the biggest collectors of data, increased pressure on telcos has meant that there is a greater need to evaluate existing security measures for both their own infrastructure and their consumers. The need to shift consumer behaviours, in particular at times of such high cyberthreat levels, becomes pertinent to the root cause. Telcos are in the best position to fulfil this need and also to enable their customers, enterprises or consumers, to manage risks and to provide efficient processes in relation to cybersecurity. But what's in it for the telco of today? Incentives are a key driver on both fronts, in that, for the telco to ensure consumers are protected sufficiently and for the consumer to pay extra for more security.

As the primary provider of critical services into nearly all homes, ISPs have first stab at addressing the gap and play the role of educators as well as solution providers. ISPs can increase their customers' understanding of the threats posed in our hyper-connected and digital world. In turn this can increase consumers' willingness to pay for that extra protection. In fact, a 2020 study on the value of device security to consumers found out that people's willingness to pay for

enhanced security and for specific devices can be increased by exposing them to relevant information about threats and security measures available.[5] This creates a clear pathway for service providers to intervene and raise awareness around the threats of hyperconnectivity and more importantly also raise the profile of available solutions.

Communicating about security risks associated with account management and educating users on security best practices can also attract more usage and help build a positive brand image. In doing so, ISPs can be the hero by acting as both the educator and solution provider to the issue. They can achieve a great adoption of security services, increase existing revenue, and generate new revenue streams.

What We Offer

A Single App Ecosystem For Connected Consumers

✓ Increase ARPU

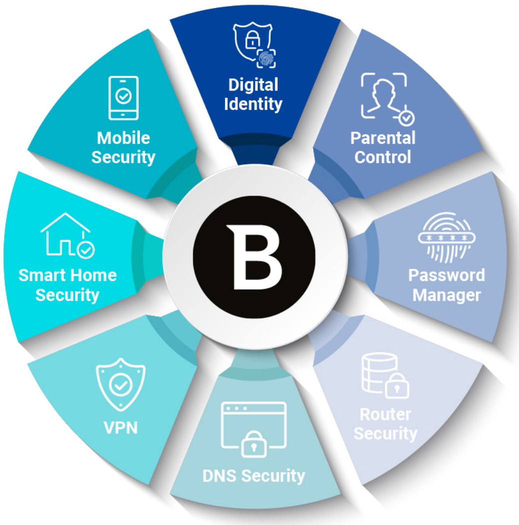
Our partners consistently report ARPU increases when selling cybersecurity as the top value-added service.

✓ Reduce Churn

Our solution ecosystem increases stickiness, so subscribers are less likely to cancel or switch vendors.

✓ Improve Customer Satisfaction

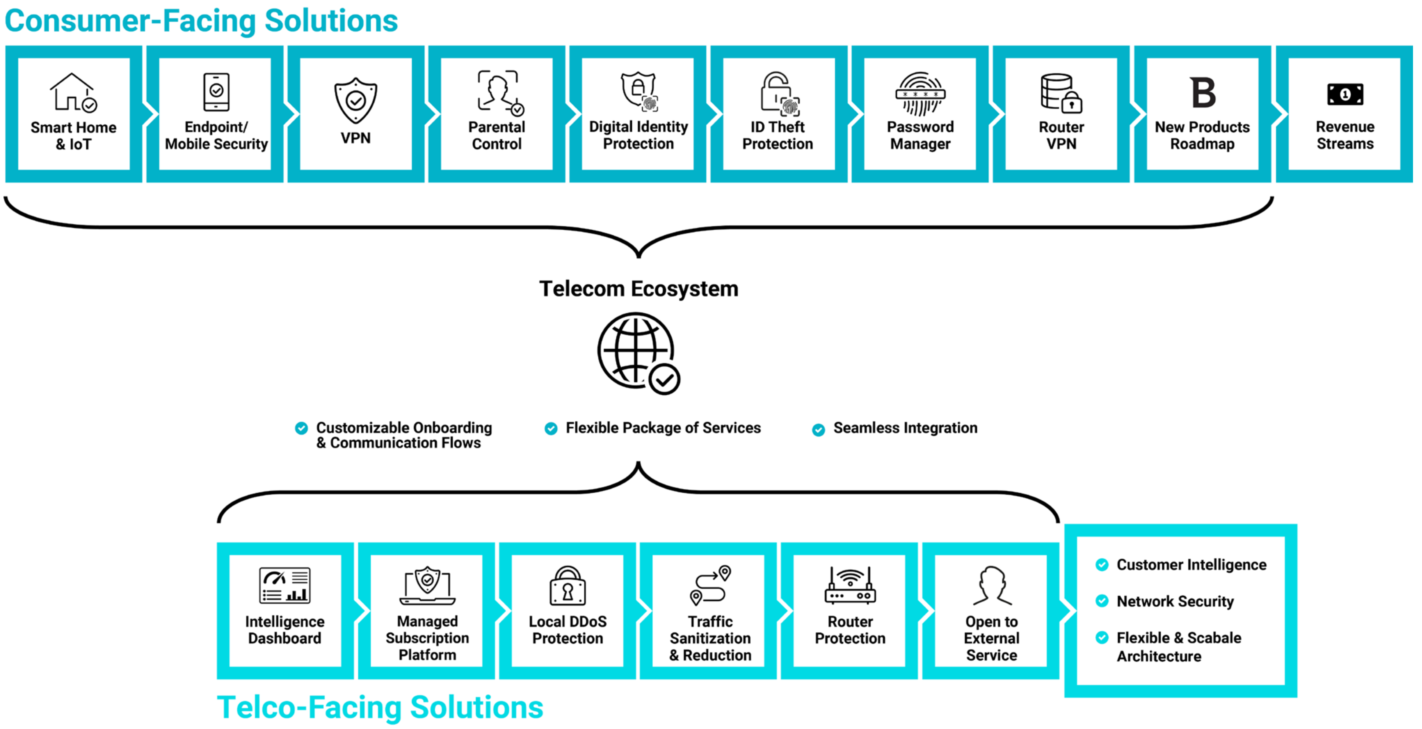
Our high-NPS services are easy to use from a single central console.



Source: Bitdefender

For example, the US-based networking hardware manufacturer Netgear, collaborated with Bitdefender on the integration of Bitdefender IoT Security Platform into their consumer-grade routers. This in turn increased the ISP's touch points with their end customers and added a significant cyber security differentiator to their products. This way, Netgear has secured all connected devices at home or on-the-go, reduced the threat of attacks, and protected sensitive user data at once. Offered only as a security subscription service, Armor allows ongoing revenue share benefit between Bitdefender and Netgear. This means, Netgear has been able to stay ahead of the competition with significant next-generation security capabilities while improving the bottom-line.

By adopting a multi-pronged strategy formed around structure, provision of digestible data, improved threat responsiveness, proactive and future proved services, solutions such as those offered by Bitdefender can support service providers to enhance the overall consumer protection and prevent their customers from ongoing cyber threats. Solutions that provide a seamless integration into the existing telco offering are more likely to engage and unlock revenue streams undiscovered before.



Source: Bitdefender

Conclusion

There has been an unparalleled increase in the number of cyberthreats and attacks in recent years. While some were driven by the perfect storm of circumstances (pandemic and working from home), and others by geopolitical motivations (Ukraine-Russia war is a frequently cited driver), many are simply due to the proliferation of connected devices in our homes and professional lives, while a disregard for protection is compounded by lack of understanding of issues related to our devices and their security.

More specifically, cybersecurity creates an opportunity for the telco of today to tap into the world of managed services even further, to reinvent themselves as the go-to digital service providers of their customers, and unlock new revenue streams. Many have understood the value it can offer and are already generating significant revenues; those include incumbents such as Deutsche Telekom, Orange, AT&T and Verizon. Several of these, such as Orange, have taken the route to acquire whole security companies. However, such an investment intensive route is not necessary for the commercial opportunity that is within reach. Revenue sharing business models, such as those examples presented in this paper, sufficiently offer telcos access to services and products, while maintaining a low investment approach yet increase touch points and engagement with consumers.

To commence their journey towards becoming the chosen digital service provider, ISPs need to ask themselves some difficult questions and investigate whether their consumers are covered sufficiently. Are they driving adequate usage, learning and engagement and do they have a full understanding of the specific needs of their customers? Service providers must ask themselves if they can do more in offering solutions to safeguard their subscribers while also boosting bottom-lines.

Educating users on the importance of cyber threats and the need for security is a starting point, but this needs to be closely followed by the next step, namely, providing consumers with the solutions needed to meet their security requirements. Combining education, awareness and solution availability will then lead to greater adoption.

Sponsor’s Comment

Scams, malware, and identity theft are three of the biggest online dangers people face today. Given that the number of connected devices is at the highest level that it’s ever been while cyberthreats continues to evolve, efforts also need to be elevated in driving cybersecurity awareness and adoption.

Trends in consumer behavior and recent cyberattacks all point to the same conclusion – that now is the ideal time for telcos provide their subscribers with what they need and want with simple, effective security and privacy solutions.

Not only will this increase long-term customer satisfaction, but it will also allow telcos to diversify their portfolio with value-added services and distance themselves from the competition.

Bitdefender's mission is to assist telecoms in providing the best possible cybersecurity to their subscribers while also easing their understanding of the actual threat landscape. We aim to provide the most advanced, powerful solutions for protecting connected devices and making cybersecurity available to everyone.

About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide to small and medium businesses, mid-market enterprises and consumers. Guided by a vision to be the world's most trusted cybersecurity solutions provider, Bitdefender is committed to defending organizations and individuals around the globe against cyberattacks to transform and improve their digital experience. Founded in 2001, in Romania, it currently has 1600+ employees, over 20,000 qualified partners and resellers, headquarters in Bucharest Romania and Santa Clara, California, and worldwide offices in the US, Canada, United Kingdom, France, Germany, Spain, Denmark, Italy, Sweden, Netherlands, UAE and Australia.

About Telecoms.com Intelligence

Telecoms.com Intelligence, the industry analysis arm of Telecoms.com, works closely with its partners to provide deep research and create educational services on the key topics shaping the industry today. A consultative and collaborative approach with our intelligence team ensures the creation of truly unique content, highly regarded by the industry. Our services combine statistical analysis and broad industry knowledge to effectively deliver insight and analysis through webinars, survey reports, white papers and more. Learn more about our services at telecoms.com/about-intelligence.

1. 2021 Bitdefender Global Report: Cybersecurity and online behaviors (2021). Bitdefender.
2. Mobile Security Index 2022 (2022). Verizon.
3. 2021 Bitdefender Consumer Threat Landscape Report (2022). Bitdefender.
4. 2021 Bitdefender Global Report: Cybersecurity and online behaviors (2021). Bitdefender.
5. Blythe et al. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices.