irdeto

Building a Secure Future.™

Our children, our homes, ourselves:

CYBERSECURITY THREATS, AND A SOLUTION FOR A 'NEW NORMAL'

COVID-19 has transformed the way we live and work. Our homes were once a retreat from the office and school, but for many this space has now been transformed into the office and school. Our homes are also serving as an alternative to cinemas, theaters, gyms, restaurants (the list goes on), while at the same time remaining the primary location for game playing, TV watching, video calling, social media updating and more.

This has all been possible thanks to ever-improving cellular and broadband connectivity. According to Cable.co.uk's annual broadband speed league table, the average broadband speed for 2018/19 was 11.03Mbps, a rise of 20.65% over the previous year. With the advent of 5G, ultra-reliable low-latency connectivity will become the new norm, connecting billions of devices, people and industries. However, with more of us accessing more bandwidth-intensive services for more hours of the day, networks and service providers are under pressure. COVID-19 has resulted in a huge shift in the way we access and use the internet at home. Vodafone's internet usage surged by up to 50% in some European countries according to reports in March; the US saw an average traffic increase of approximately 25% during the same month; while VPN provider NordVPN revealed that global use of its technology had increased by 165% since 11th March.

Many businesses and service providers have successfully transitioned to a digital-first model, while consumer-friendly unified communication and collaboration apps have seen strong pick-up. As such, many of us have been able to enjoy a range of services from home, as well as staying on top of work and studying. Some of these societal changes will remain for the long-term. A Gartner survey of CFOs and finance leaders, for instance, found that 74% plan to move at least 5% of their previously on-site workforce to permanently remote positions post-COVID-19. As such, much of the internet usage behaviors we've seen will remain even after lockdown restrictions are fully lifted.

Our ability to adapt – as employees, business owners, communities – is a sign of humanity's resilience, yet this has created two major challenges in terms of our internet technology. First, network congestion. Members of a household using bandwidth-intense applications at the same time every day (and at the same time as their neighbors) can impact quality of service.

During lockdown, some content service providers even reduced the quality of their streaming services to ease the strain on broadband networks. These include Netflix, Amazon and Apple.

The second challenge is more severe. Greater numbers of people are connecting to their home networks, on a greater number of devices, and for longer time periods, widening the cybersecurity threat landscape. Furthermore, while businesses, public services, education establishments and the like will have cybersecurity policies, CISOs, IT teams, anti-virus and threat detection software, these things are not typically part of the home internet set-up.

The lockdown has been a difficult period for most of us, but it's been exploited as an opportunity by hackers. These criminals have been taking advantage of the current situation by sending phishing emails relating to COVID-19 and attempting to solicit personal information from recipients, or directing them to scam websites. Between 23rd March and the beginning of May, the UK's HMRC, for instance, asked ISPs to remove 292 such site addresses. Hackers have also been taking advantage of the increased use of VPNs to identify vulnerabilities and infiltrate networks, something the NCSC has released guidance on.

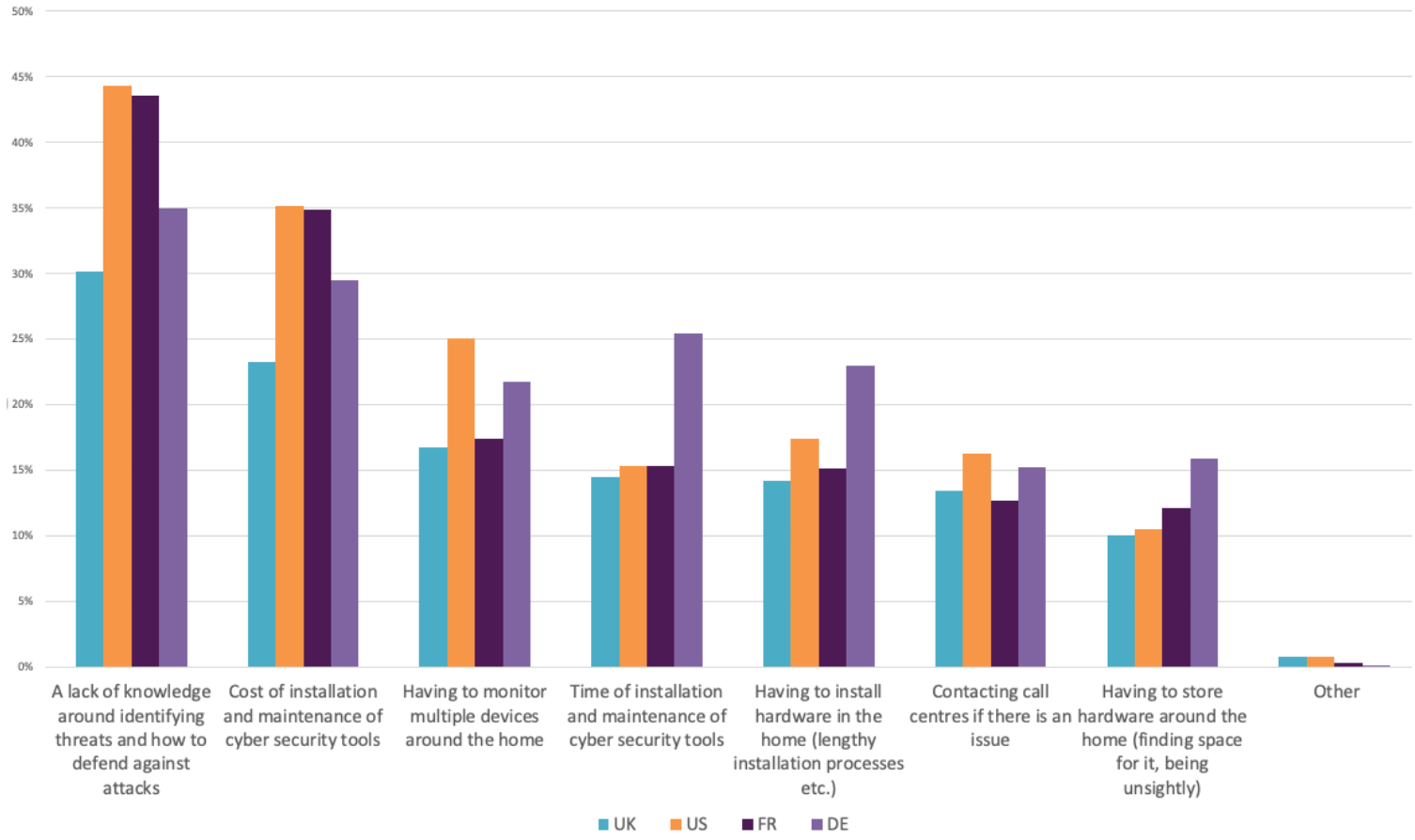
The greater number of connected devices being added to a network has also been a cause for concern, as this increases the threat surface, especially as many are low-cost consumer devices with little or no built-in security. Consumers can take measures to boost cybersecurity themselves, and device manufacturers have a part to play by ensuring more robust built-in security protocols. Yet it's ISPs that are best placed to address the cybersecurity challenge and optimize network security in the home.

ISPs already benefit from existing relationships with customers (providing subscribers with connectivity services), many of whom trust ISPs as gatekeepers of their home networks. ISPs are therefore perfectly positioned to take these relationships one step further, by becoming trusted providers of cybersecurity solutions. To ensure customers adopt these solutions (and that they add the value needed for ISPs to realize ROI), these solutions must allow consumers to view all devices connected to their home network, check Wi-Fi performance at the device level, and offer automated help to improve connectivity. They must boost security by blocking unknown devices, sending alerts about threats, and offering advice for tackling these. Consumers must be able to take control of family browsing, and have the ability to block malicious ads and websites, and apply content filters at user and device level. Parental controls are also essential for consumers seeking to manage how long children spend online and which sites they visit, and must therefore include granular control of device usage times, and connectivity.

Finally, cybersecurity solutions must offer ISPs an advantage, and allow them to monetize and benefit from security features and controls. This means offering a level of functionality and ease of use that serve as competitive differentiators. This can then either prompt new customers to sign up for their service (defecting from an ISP which is unable to provide such a solution), or to opt for the solution as a premium-priced, pay as you go add-on, thus boosting ARPU for the ISP.

The current COVID-19 and lockdown situation has raised some major questions around the quality of service and security of the internet services we're accessing at home – and which we've all become so reliant on. To better understand the perception of these cybersecurity threats, in April 2020, Irdeto conducted a survey of more than 4,000 consumers in the UK, USA, France and Germany. In addition to revealing concerns, the results of this survey have highlighted how we can overcome common cybersecurity challenges, boost general knowledge of online security, and ensure our homes and those within them remain safe throughout these changing and unprecedented times.

What are your main pain points with regards to cybersecurity at home?



CYBERSECURITY AND OUR CHILDREN

The online safety of children and young people has long been a cause for concern for parents, governments and regulators the world over. With time outside having been restricted (and with social distancing likely to continue), many children will be accessing the internet at home, unsupervised, for longer periods of time. And without visibility into the type of content children are accessing (and when, where and how), many parents and carers will be feeling even more concerned.

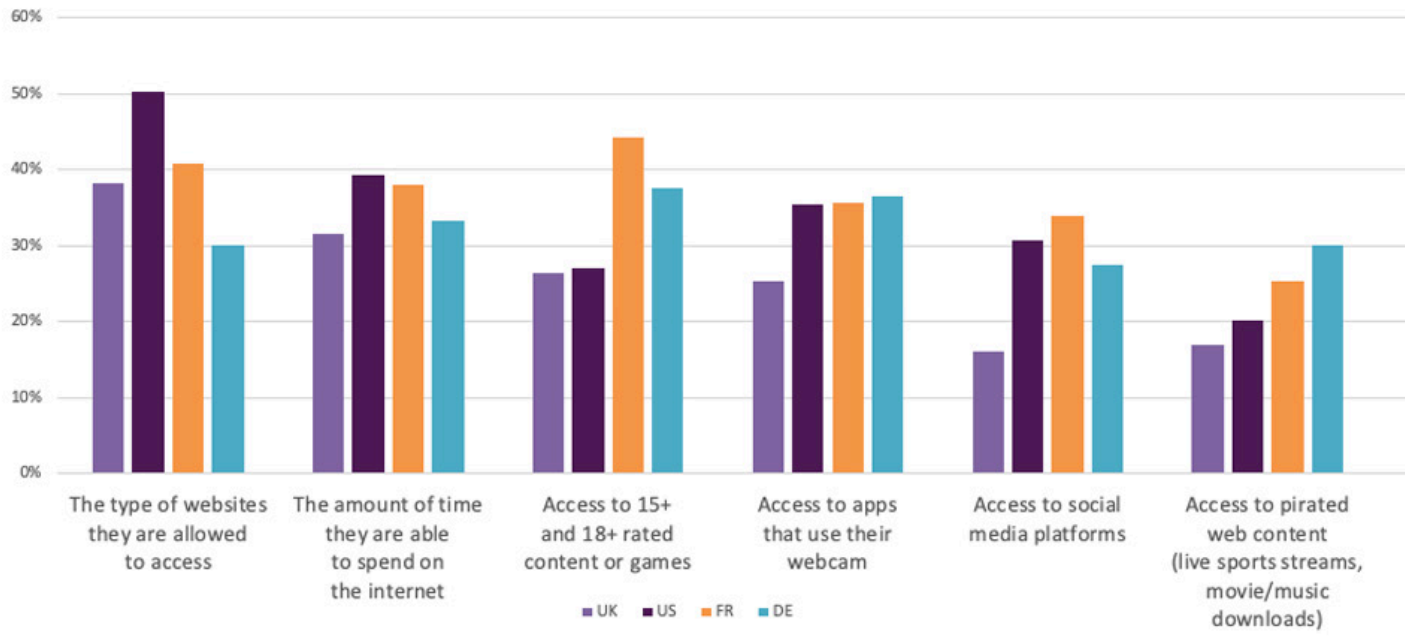
Interestingly, it is their children being exposed to adult material as opposed to illegal material, that respondents were more concerned about in regards to their children and their cyber security.

Though the difference is small (roughly a third of respondents cited both of these things), this could suggest that concern is driven by ease of access and the (perceived) greater prevalence of gambling and pornography sites, versus cult recruitment and grooming. This is a sensible concern given that Europol recently said that it has information that 'strongly indicates increased online activity [during the pandemic] by those seeking child abuse material.'

Platforms such as Facebook and YouTube have faced criticism for not doing enough to protect users – especially children – and for failing to adequately police content on their sites. While there's still a long way to go in this regard, other sites have implemented stricter parental controls. Spotify is one of the latest to join this list with its addition in May of stricter parental controls to its Spotify Kids service. However, the efficacy of these controls is open to debate.

Many children who have been brought up using technology may find it relatively easy to circumvent such controls. In April, for instance, a story emerged of an eight year-old who found a bug in Apple's parental controls that allowed her to circumvent the device's Screen Time control and view YouTube videos. This is supported by findings, in which children aged 12 to 13 (or younger if they had older siblings), said they knew how to access and overcome parental controls.

When thinking about your children's use of the home network, what are the most important things you have control over?



As such, while adding such controls to devices and content services is a good first step, cybersecurity needs to go beyond this level and encompass the entire ecosystem of the home network.

Cybersecurity concerns center not only on what children are accessing, though, but how they're accessing it and how long for. 69% of global respondents said they are concerned about the number of access points used by under 16s to get online.

This is not surprising given that just over half of children in the United States now own a smartphone by the age of 11, while in the UK, the majority of children own a mobile phone by the age of seven, according to a study by Childwise.

In the current pandemic situation, many parents will likely be concerned not only by the devices that their children own, but by the number of devices owned by other members of the household that are lying around and easily accessible in the home environment.

The average UK home now has 10.3 internet-enabled devices, equating to more than 286 million nationally, according to a new study from Aviva.

When it comes to controlling children's use of home networks, the top two concerns cited by parents surveyed in our survey were access to different types of websites (40%) and the amount of time they are able to spend on the internet (36%). Again, these worries are grounded in reality: the aforementioned Childwise report found that overall, UK children spend about three hours and 20 minutes each day messaging, playing games and being online. This is very likely to have increased during lockdown, and set a precedent that may well continue after.

Cited by just over a fifth (21%) of parents and carers, children spending money without realizing by making in-app purchases was their main concern in regards to their children and their cybersecurity. This rises to almost a third (31%) in Germany.

Clearly, greater control by parents and carers over home networks is needed to allay worries, to protect children from accessing unsuitable/illegal content, and to protect them from exploitation and abuse.

CYBERSECURITY AND OUR HOMES

People are, quite rightly, concerned about their personal data and the cyberthreats to them as individuals. However, this has perhaps come at the expense of sufficient awareness of the danger and prevalence of cyberattacks on the wider home network.

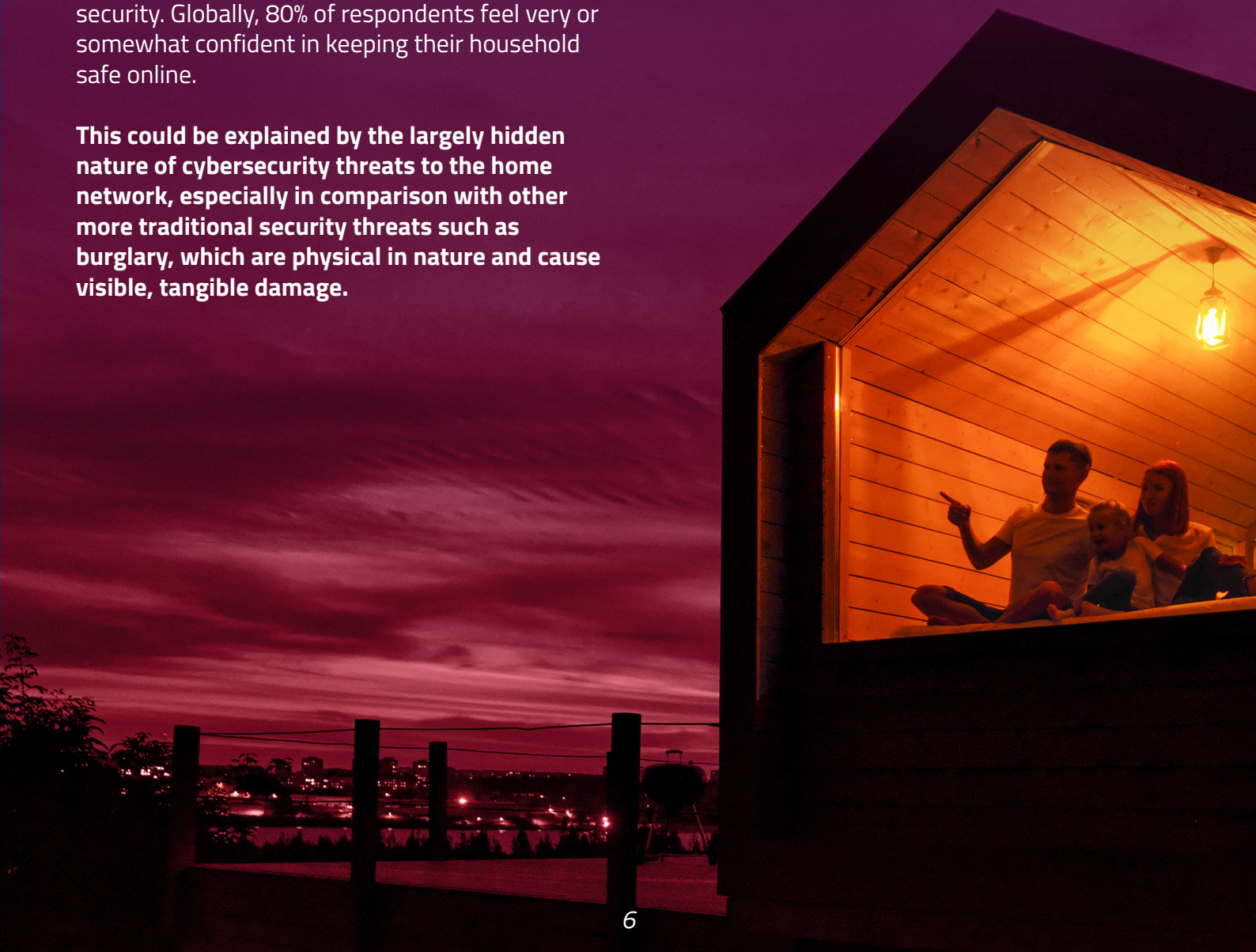
70% of global respondents believe that their households have not been subjected to a cyberattack. UK respondents were the most confident with their ability to keep attackers at bay, with 79% believing their home devices and networks have not been targeted by cyber criminals. This, despite findings by Consumer Reports indicating that many home routers lack basic security tools, and/or do not encourage good cybersecurity practice by users – accepting weak passwords or not requiring users to adjust weak default settings, for instance.

There appears to be a widely-felt false sense of security. Globally, 80% of respondents feel very or somewhat confident in keeping their household safe online.

This could be explained by the largely hidden nature of cybersecurity threats to the home network, especially in comparison with other more traditional security threats such as burglary, which are physical in nature and cause visible, tangible damage.

Indeed, globally, a total of 45% agreed with the statement, 'I am far more concerned about my physical home security than I am my cybersecurity.' Again, lack of knowledge of the dangers and repercussions of cybercrime are apparent, because despite the concern around physical security versus cybersecurity, respondents are actually aware that the likelihood of them falling victim to the latter is far higher.

Respondents picked a cybersecurity attack as the most likely out of several crimes for them to fall victim to, including a home burglary. Many seem to be living by the mantra that what you don't know – and can't see – can't hurt you.



CYBERSECURITY AND OURSELVES

People aren't just worried about their children accessing and using the internet safely, they're also worried about their own personal cybersecurity. Most respondents cited fraud as their main concern in terms of cyberattacks, followed by personal data loss (49%; 45%). Interestingly, the younger the respondents are in age, the more concern they felt around having personal videos/photos stolen. 28% of those aged 16 to 24 said this was their main cybersecurity concern, with the percentage reducing in increments as age groups matured. Only 7% of those aged 55 and over admitted their main cybersecurity concern was having their personal videos/photos stolen.

This highlights a stark generational difference in the way we use digital services and rely on devices and applications to 'look after' our data. Younger people may be taking, storing, editing and sharing personal photos and videos more than older age groups, but it's important that this goes hand in-hand-with an awareness of the dangers of doing so, and an increase in good cybersecurity practices. The iCloud leak of 2014 – during which hundreds of private photos of celebrities were leaked on websites and social network sites – was a high-profile example of the dangers of entrusting applications with personal information. It's not only anonymous hackers that internet users have to worry about, though. Sharing any sensitive information online, even with those you trust, can resurface unintentionally, especially at a time when stresses and emotions are high. Traffic to the UK's Revenge Porn Helpline website nearly doubled in the week beginning 23rd March, and more cases were opened in the following four weeks than in any previous four-week period.

Fortunately, the lockdown does seem to have pushed cybersecurity up the agenda for many people, as internet usage has greatly increased – especially due to the fact that many people's homes are now also their places of work. 47% of global respondents now working from home believe they are more susceptible to cyberattacks as a result of being online more. However, people's fear of personal data and devices being hacked at home does not extend to the company data that they're also accessing at home. Globally, 80% of respondents who are working from home due to Covid-19 are confident that the company data they are accessing on their home network is protected.

Workplace breaches are well-documented in the media, and the ICO has issued millions of pounds worth of fines to those in breach of GDPR. Data breaches in the US get a similar level of media attention. In 2019, Yahoo agreed to pay US$117.5 million over a series of data breaches that affected users between 2012 and 2016. An even bigger payment was made by Equifax in 2019, when the credit firm agreed to pay US$575 million for failing to take reasonable steps to secure its network.

Despite these well-publicized events, just 15% of global respondents believe they've been the victim of a cyberattack at work. This drops to 11% in the UK. Our report identified a gender divide in awareness of the risk of cyberattacks: more men than women think they've been victims of cyberattacks at work (19% vs 11%) and home (34% vs 26%).

This could be attributed to two things: either women are more confident in their cybersecurity practices, or men are more aware of the dangers.

In many instances, the confidence (felt by both men and women) that company data is better protected than personal data when working from home, is misplaced. Many businesses not accustomed to employees working outside of the office do not have specific security measures in place for remote working. According to the UK government's Cyber Security Breaches Survey 2020, only a quarter of businesses and less than a third of charities in the UK have cybersecurity policies that cover home or mobile working – although both of these figures show a rise on previous years.

So, many employees will still be accessing work emails, talking to colleagues via apps, downloading and uploading documents etc. via their home network which, unless properly protected, is vulnerable to attack.

WHAT'S HOLDING US BACK?

Despite general confidence in keeping households safe online, there seems to be a widespread acknowledgement that more should – and could – be done to better manage internet usage.

62% of global respondents said they wanted much more control over their home network.

There also seems to be recognition of the heightened threat level to home networks than new remote working patterns have brought about.

Supporting the consensus that individuals are at greater cybersecurity risk now that they're working from home, 67% of respondents agreed that having control over their home network is more important than ever. And for many, the tools they have in place at present are inadequate. Over half of respondents (54%) believe that manufacturer-level security on home devices is not enough.

The awareness of the risk of cyberthreats – to children, to themselves and to some extent, their households – exists among consumers, as does the desire to improve cybersecurity in the home: so, what's holding people back?

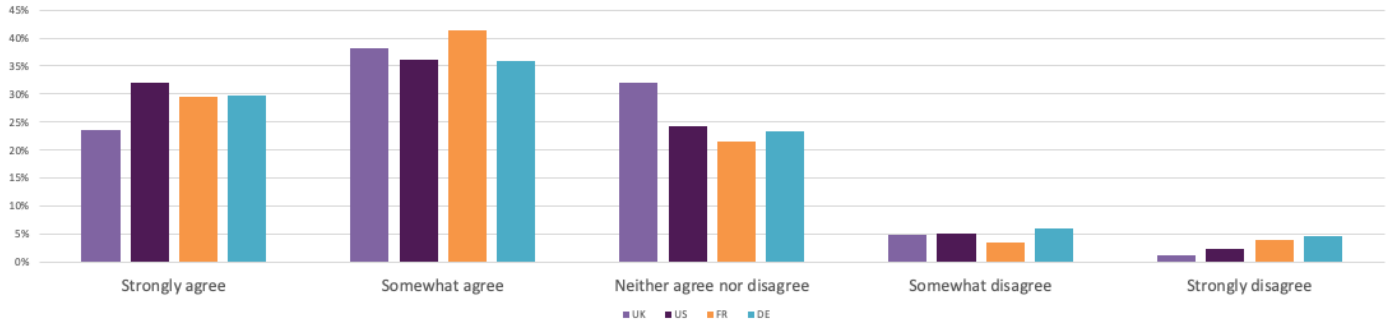
In all regions surveyed, the main pain point was lack of knowledge, around both identifying threats and knowing how to defend against attacks – something 38% of respondents experience.

This varied slightly depending on region, with less than a third (30%) of UK respondents identifying lack of knowledge as a challenge, rising to 44% in the US. Government-backed bodies such as the UK's NCSC, the US's National Cyber Security Division (NCSD), and the European Union Agency for Cybersecurity (ENISA) exist to educate and inform consumers and businesses, but it's clear that more must be done.

Even if consumers understand the threats, there are other factors preventing many from making the leap from seeing cybersecurity tools as a 'nice to have' to adopting such technologies as a 'must-have.' Chief among these is every marketer, retailer and consumer-facing business' nightmare: time and money. If something is expensive and complex to implement, chances are many of us will simply not bother and learn to live without.

The cost of installation and maintainence of cybersecurity tools was identified as pain point by almost a third (31%) of all respondents. Interestingly, this rises to 37% of those aged between 25 and 34; an age group that has grown up around technology but has also become accustomed to an 'on-demand' lifestyle. Individuals in this age group are also less likely to be homeowners than those aged 55 and over (only 28% of whom identified cost of installation and maintainence as an issue), and more likely to be living in shared, rented accommodation where there is less collective responsibility for cybersecurity.

Having control over my network is more important than ever



This latter scenario – where those using home broadband do not own the property – may also influence concerns around having to install hardware in the home, and the lengthy and complex processes associated with this. This was a pain point for 17% of global respondents, and which again was more of an issue for the 25-34 age group (19%) than it was for those aged 55-plus (12%).

Many consumers may also feel overwhelmed by the prospect of securing so many devices within their home – which could range from laptops, desktop PCs and TVs, to connected toys, lighting systems, CCTV cameras and kettles.

A fifth of respondents globally (20%) said that monitoring multiple devices around the home was a challenge.

Complicating this is the idea that different cybersecurity solutions may be required to manage different aspects of different devices. A connected toy or a tablet used by a child for watching TV, for instance, will need tight parental controls, while parents may also want to be able to manage the performance of their Wi-Fi on a more general, all-device level. There is also a widely held belief that solutions are designed to secure one main device, with additional charges applying for securing each additional device – a very expensive prospect for a family whose members all have multiple connected 'things'!

A final challenge identified by consumers relates to possibly the most sensitive issue concerning cybersecurity: protecting children and young people.

Parents want strict controls over devices and services, but managing these can be tedious.

For example, some devices are shared across children of different ages, so controls can often be too restrictive for the older kids. Personalizing these settings would require the consumer to sign in when they use the device – for instance to a service like Netflix – but this is time-consuming, and even once they have signed in, there's nothing stopping a child from signing out and accessing a different profile.

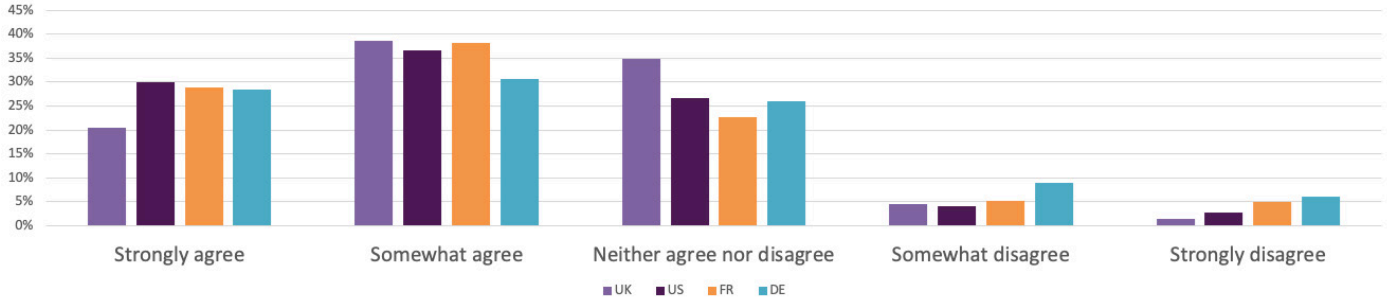
We've looked at the pain points in terms of implementing cybersecurity and the factors holding consumers back. Despite these things, there is a strong desire from consumers to boost the security of their home networks, and they are willing to spend.

A global total of 62% of consumers we surveyed said they wanted much more control over their home network.

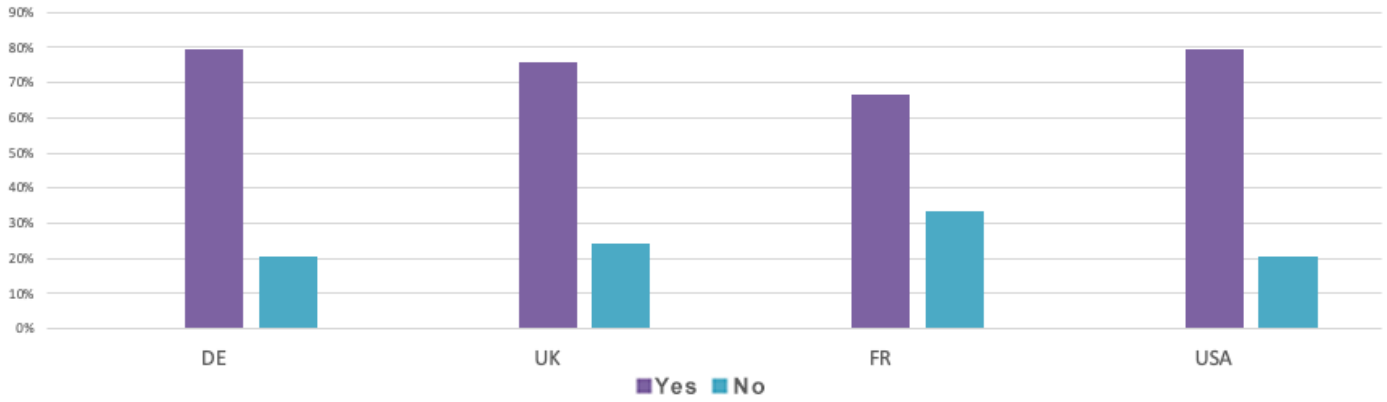
As for the 3% who strongly disagreed with this statement – the majority were under 25 years of age and many no doubt students or living in households in which they are neither the primary bill payer nor the decision maker when it comes to their internet services. Ease of use is important to consumers:

63% of global respondents want software that would allow them to better monitor their home network.

I would like a software that would allow me to better monitor my home network



Are you willing to pay for cybersecurity?



The financial damage which can result from data breaches and hacks to personal accounts has been well conveyed by the media, which no doubt has some influence over the willingness of consumers to invest in a robust, user-friendly, multi-featured cybersecurity solution for their home. The amount of cash consumers would happily part with varied from region to region, but in all geographies surveyed, significantly more respondents preferred a mid-priced solution than one at the bottom end (i.e. cheaper) end of the scale.

In the UK, for instance, only 3% would spend under £17 on a solution, whereas 44% would spend up to £41. It was the £17 to £29 price range that seemed most appealing in most regions surveyed, though.

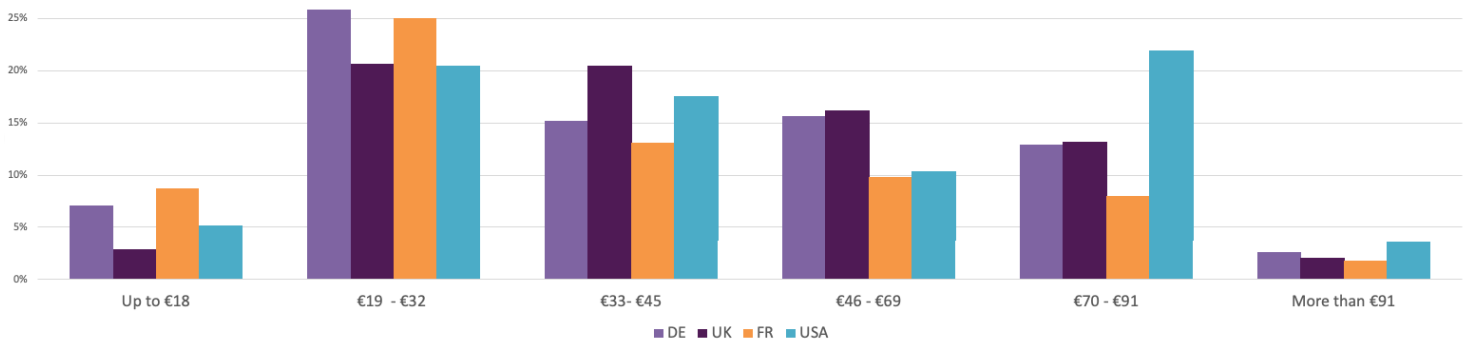
Furthermore, cheap definitely isn't cheerful for many consumers, with a notable number willing to spend between £62 and £81 to ensure the safety of their household against cybersecurity threats.

In the US, for instance, 22% of respondents would be happy to shell out for a solution in this price range, more than those who'd spend US$21 to US$35.

There's a clear opportunity here for ISPs to capitalize on consumers' willingness to spend on the right solution. In addition to providing a value-add service for the consumer (thus increasing ARPU), ISPs can also reduce spend which would have traditionally gone to supporting large customer care teams, by giving more power to the consumer, making troubleshooting problems easier and reducing the time taken to resolve issues.

Whether real or perceived, there are clearly a number of factors holding people back from adequately protecting their home networks and internet users from cybercriminals. Whether practical – space for hardware or cost of installation – or behavioral – 'too difficult to manage' – these problems are underscored by a lack of knowledge of threats and solutions. Thankfully, lack of knowledge of solutions does not mean that solutions do not exist! The question may therefore be: what's holding the ISPs back? Just as consumers would benefit from a greater awareness of solutions available to them, so too, perhaps would ISPs.

How much would you be willing to pay for cybersecurity?



WHAT'S THE SOLUTION?

Government organizations can help educate consumers; employers can set out guidelines; and traditional home insurance providers can branch out into cyberinsurance. However, ISPs also have a responsibility to implement security and Wi-Fi management solutions that give subscribers a premium, connected home experience. This should be part and parcel of an ISP's offering, as many subscribers lack the skills to identify or troubleshoot issues themselves. According to a survey by Which? 20% of people view the broadband ISP market as complex (more than any other sector) and 48% view switching packages as risky (again, more than any other sector). Concerns about Wi-Fi quality can seriously impact sales and customer retention for operator IPTV and OTT services, where a vital differentiator from unmanaged OTT services is the high-quality, seamless user experience.

When selecting a solution to address consumer needs, ISPs should look for those that not only provide the required security and parental control, but also assist consumers with managing the overall Wi-Fi experience and enable their service agents to 'see' what their customers are experiencing.

Fortunately, solutions are now available to ISPs that can solve these challenges. They can automatically fingerprint and identify all devices connected to the home network, and monitor devices and internet usage to detect and block threats, make recommendations and auto-tune router and device settings for improved security. In addition to boosting security, such solutions ease network congestion, and help to improve Wi-Fi performance by identifying and advising on how to troubleshoot issues, subsequently reducing customer churn.

Consumers need to be able to manage all of their devices easily, keeping themselves, their children and their homes safe.

Self-management is key here: 14% of global respondents admitted that having to contact a call center if there's an issue was a pain point in regards to cybersecurity at home.

We've all been there – waiting on hold for a representative to take your call is a frustrating experience. As such, a cybersecurity solution must be user-centric, offering a straightforward UX and empowering individuals by providing granular management controls. This can be achieved via an iOS and Android app, which allows consumers to manage devices, see network activity usage by day, view device performance and run diagnostics, run network speed tests, and manage parental controls. A smartphone app also allows users to receive instant updates and notifcations of new devices joining the network, and inbound, outbound and device-to-device security threats and recommendations for remediation.

Easy to implement, to configure and to manage, such solutions place control and visibility into the hands of subscribers, which will also help to promote greater awareness and understanding of their home network and threats to it.

There are also significant benefits for the ISP. A successful self-care product for connected homes won't just keep subscribers satisfied and loyal, it can also deliver valuable new revenue just as competition is stifling subscriber growth and ARPU. It can consolidate the operator's role at the heart of the connected home at a time when products like Amazon Alexa and Google Home are extending their reach into many households.

User empowerment is perhaps most important when it comes to the issue of protecting children from online threats and better managing kids' usage of the internet and their devices. In addition to being able to check and improve connectivity for each individual device connected to network, a solution must allow users to block adverts and malicious websites to each device, and to apply content filters for certain users and certain devices.

Easy to use management tools must allow parents and guardians to see how long their children spend online, which sites they visit, and how this differs across profiles and devices.

Bedtime and homework times can be set and adapted, and users should have the power to pause connectivity per user or device.

Cumbersome hardware shouldn't be an issue, and subscribers shouldn't need to be tech experts to set up their security. Gone are the days of tech jargon laden interfaces! Instead, home cybersecurity solutions are now available with a smartphone app, giving subscribers everything they need to administer their own home network in a user-friendly, comprehensible interface. Features include parental control, device performance monitoring, device management, admission control and network activity usage stats.

CONCLUSION

Gender, age, and other demographics shouldn't be barriers to understanding and adopting robust, comprehensive cybersecurity in the home. There needs to a collective responsibility and action needs to be taken. However, ISPs occupy a position of power – they have the tools, the insight and the solutions available to take top-down action. It's up to ISPs to secure the home network, the devices attached to it, and these devices' users. This is even more important when it comes to children, many of whom will be learning, socializing and getting entertainment primarily from the digital environment.

ISPs too stand to gain from offering such solutions. The fact that consumers are willing to spend on cybersecurity solutions – especially during a time of financial uncertainty and instability – unlocks a significant opportunity. In the face of industry competition, convenience, a premium user experience and peace of mind are valuable differentiators for high-ARPU premium subscription packages. ISPs can also benefit from gaining enhanced visibility of the devices in their customers' homes, enabling them to exceed expectations with fast, proactive customer care that can lead to tailored offerings and increased ARPU.

ISPs have the power to make robust, user-friendly, all-in-one solutions available directly to subscribers. And, with the right solution, subscribers can protect their homes both virtually and physically.

Using our homes as places of work, schools and entertainment hubs is looking to be our new normal, and the perfect opportunity to set a new benchmark in terms of cybersecurity. With employees working from home – and this being a trend for the foreseeable future – now is the time to put in place solutions that will protect individuals, companies and home networks.

www.irdeto.com

*Consumer survey conducted and data supported by Censuswide. **