White Paper

HardenStance

Home Router Security: The Buck Stops Where?

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

allot
See. Control. Secure.

July 2021

Executive Summary

(*This is an update of a HardenStance White Paper first published in April 2019*)

- Adapting to the impacts of the pandemic has made billions of us much more reliant on our home networks in how we live our lives – and more vulnerable to the impact of cyber threats targeting us and our devices in our homes.
- As Orange states in a current marketing campaign, home routers are "the router of all evil." Responsibility for securing them is shared between consumers, router vendors, Internet Service Providers (ISPs), Internet companies and governments but there is still no consensus on sharing responsibility or where the 'buck' stops.
- ISPs can just comply with bare minimum regulations. Alternatively they can commit and differentiate with home router security features like blocking unauthorized access and restricting the tasks home routers are allowed to perform.

The Pandemic Has Increased Cyber Risk at Home

The Coronavirus pandemic has materially increased the risks we are exposed to from our home networks. That's an arresting statement but it's demonstrably true. An end of 2020 survey of 22,000 consumers in 22 countries conducted for IBM Security by Morning Consult found that individuals created an average of 15 new online accounts during the pandemic. Moreover, 82% of those respondents admitted to re-using the same username and password credentials at least some of the time.

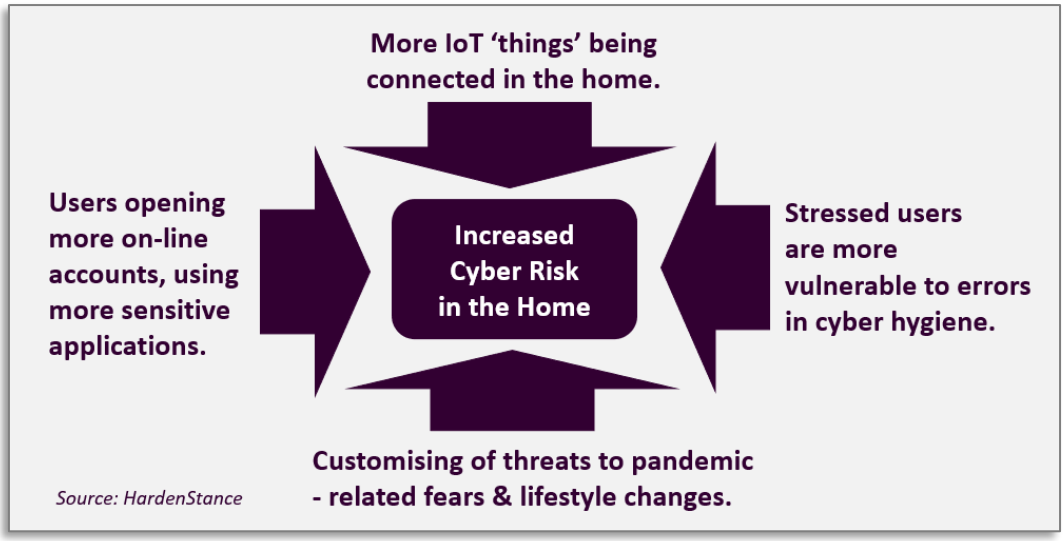
On average, our habits and preferences have shifted decisively to a more hybrid model in which a greater share of critical interactions happen in the home.

We and our children are working and learning from home more than we were. We are engaging in more on-line medical consultations instead of visiting our doctors' office. The risk to us from these kinds of applications being disrupted or the private content shared being leaked is materially greater than a lot of the usage that characterized our consumption of on-line applications prior to the pandemic.

This Shift to Greater Dependence on the Home Network is Permanent

Some amount of this shift to greater reliance on our home networks is permanent. On average, our habits and preferences have shifted decisively to a more hybrid model in which a greater share of critical interactions happen in the home and fewer occur on other premises. We are also increasing the exposure of our homes to risk from 'IoT' things. IPSOS Mori surveyed 2001 UK consumers for the UK government in October – November 2020. It found that in the six months since the start of the pandemic, UK households connected an average of two more smart devices to their home router.

Figure 1: Increased Cyber Risk to the Home Network in the Pandemic Era



The impact of the pandemic on people's mental health has also made us more vulnerable to cyber threats. This is also borne out by data. The U.S. Centre for Disease Control and Prevention (CDC) recently reported that during the period August 19th 2020 - February 1st 2021, the percentage of U.S. adults with symptoms of an anxiety or a depressive disorder during the previous 7 days increased by 5% - from 36.4% to 41.5%. Isolation, as mandated by government lockdowns, is known to cause serious mental health issues as well as lesser ones such as memory loss. This is made worse by ongoing social and political strife within and between countries, as well as extreme weather events driven by climate change. Our frame of mind leaves many of us more distracted nowadays, hence more vulnerable to making basic errors in our cyber security hygiene.

From a cyber threat actor's perspective, the pandemic is an opportunity. There's been a surge in email and SMS-borne phishing attacks using COVID-19 themed lures based on Personal Protective Equipment (PPE), fake 'track and trace' and fake lockdown breach notifications, as well as fake promises of early access to vaccines. There's also been a surge in scams relating to fake home delivery notifications. Attackers will continue tailoring new attack themes to different phases as we emerge from the pandemic.

Home routers that are optimized for lowest cost, maximum convenience and rapid time to market continue to have high market share in many markets.

Vulnerabilities in "The Router of All Evil"

The home router is the central point in the home network through which all traffic flows. As such, Orange is currently using the term "the router of all evil" as part of a campaign to raise cyber security awareness in the home network. An attacker that gains access to a router can potentially see any traffic running across that network and execute any number of different attacks. These include eavesdropping; altering DNS settings to send users to a rogue imitation of a familiar website; downloading malware-infected versions of legitimate software; serving up unwanted ads; and corrupting the integrity of messages between devices in the network.

Hence as industry stakeholders and consumers look to different layers of security to protect against increased risk in the home, home router security needs to be pivotal. The fundamental problem is that home routers that are optimized for lowest cost, maximum convenience and rapid time to market rather than security continue to have high market share in many markets. Such devices are susceptible to vulnerabilities that take very little sophistication to exploit. As shown in **Figure 2**, researchers are still regularly identifying new vulnerabilities in home routers. Look at the installed base of

Figure 2: High Profile Home Router Vulnerabilities 2019 - 2021

Date	Country	Vulnerabilities and Impacts
7-2019	Brazil	Avast identifies 180,000 home users with active DNS hijacking from February to June 2019 (a variant of attack activity dating back to the summer of 2018)
9-2019	W-Wide	Avast finds vulnerabilities in 600,000 GPS trackers used to track children and the elderly spanning 29 different models
6-2020	W-Wide	D-Link releases a patch for its DIR-865L home routers following the discovery of six vulnerabilities by Palo Alto Networks Unit 42 in February 2020.
7-2020	W-Wide	Trend Micro identifies new variant in the MIRAI botnet malware that exploits 9 vulnerabilities, one of which is in the ComTrend VR-3030 home router.
6-2020	W-Wide	D-Link releases a patch for its DIR-865L home routers following the discovery of six vulnerabilities by Palo Alto Networks Unit 42 in February 2020.
12-2020	U.S	FBI warns of "swatting attacks" where email compromise access insecure home 'things' with camera and voice capabilities for hoax calls to emergency services.
5-2021	UK	Research by consumer magazine "Which?" suggests up to 7.5 million UK consumers could be at risk from old home routers.

Source: HardenStance

home routers in even the most advanced countries and you'll find a sizable share suffering from one or more characteristics ranging from inadequate hardening; use of default passwords; use of unencrypted protocols like Telnet; support of unauthenticated services like Structure of Management Information (SMI); and lack of vendor support for security and other software updates.

In the UK, for example, a "Which?" magazine survey of 6,000 households in December 2020 found that millions of users could be using home routers that are more than five years old and no longer supported by firmware updates. And in its July 2020 "Home Router Security Report" the Fraunhofer Institute concludes that "there is no router without flaws" and that "much more effort is needed to make home routers as secure as current desktop and server systems."

An Insecure 'Smart Home' Isn't Just a Risk to That Household

The threat to home networks is also worsening with the momentum behind 'smart homes', whose security posture is often anything but 'smart'. An IPSOS Mori survey of 2001 UK households in October – November 2020 found that in the six months since the start of the pandemic, British households purchased an additional two smart devices for the home. Only 1 in 5 of those surveyed checked to see if they had default passwords.

The threat to home networks is also worsening with the momentum behind 'smart homes', whose security posture is often anything but 'smart'.

In the past, issues around home router security could be viewed as a largely closed one between an end user, their home router and their ISP. But as demonstrated by the massive impact of the MIRAI botnet attack on Dyn in 2016, the rise in the automation of attacks and the proliferation of IoT 'things' has changed the balance of externalities arising from Internet usage. If a home router or other devices in a home network are taken over by a botnet, those infected devices pose a substantial indirect risk to any endpoint on the planet as well as a direct risk to the immediate householder.

Another example of this is the end of 2020 warning by the FBI in the U.S. of "swatting attacks" whereby email compromise allows access to insecure home 'things' with camera and voice capabilities so that attackers can place hoax calls to emergency services. Individuals practising good cyber security hygiene in their own self-interest is certainly a key layer of home network security. However, policy prescriptions that rely largely or entirely on user hygiene take insufficient account of this critical issue of externalities.

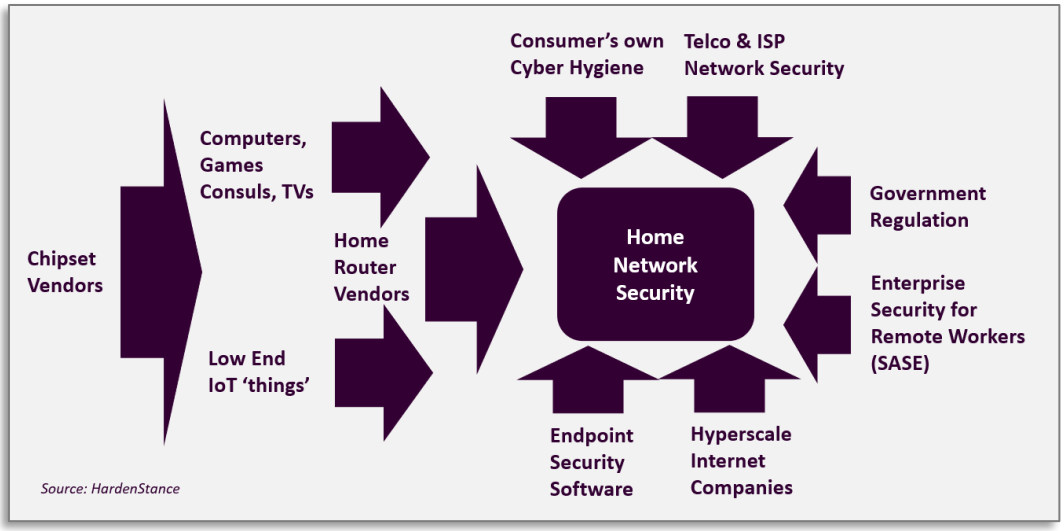
Misalignment in Stakeholder Motivations

Once one understands the risk from vulnerabilities in the home network - both to oneself and to others - it's easy enough to conclude that 'something needs to be done' about it. But defining what that something is – and agreeing on the right market incentives to support it – continues to elude many industry stakeholders and government regulators alike. That often leaves stakeholders having to decide how to respond in isolation or in partnership with one other party rather than in concert with multiple partners.

Some examples of how different stakeholders have different or even irreconcilable perspectives on the best way forward, are shown below:

- Some banks, telcos and other organizations have become more likely to make compensation for consumer fraud conditional upon a user's own behaviour whereas in the past compensation was more likely to go un-questioned.
- Liability for a home router product continues to be very complex, potentially touching on the ISP, the router vendor, and the user themselves.
- Earlier this year, most Canadian telcos and ISPs rejected a proposal by the Canadian Radio Television and Telecommunications Commission (CRTC) for a mandatory network-based malicious botnet-blocking regime. This is fairly typical of the kind of misalignment that often exists between government and the telecom industry as regards home network security policy prescriptions.

Figure 3: There are Multiple Stakeholders in Home Network Security



SASE protects the employer's assets against cyber threats from the employee's home network. It doesn't protect the home network itself.

- A lot of relevant legislation in Europe, including in Germany and the UK, has recently focused on mandating better security requirements for the sale of new 'IoT' things. This is certainly a positive development but it won't have a substantial impact on today's households for a number of years. Moreover it won't prevent people from deploying rogue devices if they're determined to – and it only takes one to create an entry point for an attacker.
- The shift to home working during the pandemic has greatly accelerated the momentum behind the Security Access Services Edge (SASE) product or service category. But while SASE can do a great job of protecting the employer's assets against threats from the employee's home network, it doesn't protect the home network itself or any of the household's own devices.
- There's a fairly common view held by many stakeholders that some Internet hyperscalers should be contributing less to threats to consumers from cyber scams - and doing more to preventing, detecting and mitigating them. In a speech in June 2020, Charles Randell, Chair of the UK's Financial Conduct Authority, stated: "it is frankly absurd that the FCA is paying hundreds of thousands of pounds to Google to warn consumers against investment advertisements from which Google is already receiving millions in revenue."

Obligations and Opportunities for ISPs

Probably more than any other stakeholder, ISPs have wrestled with the question of how far they should commit to home Internet security for many years. Three very different principles present themselves to ISPs, all pointing in conflicting directions:

1 **ISPs are not responsible for cleaning up the Internet**. If there is to be a major clean-up operation, which necessarily requires investment, ISPs tend to believe that those costs should be shared across different stakeholders.

2 **Irrespective of the exact cause, ISPs usually get blamed for home network security breaches because they often supply a large share of the routers.** Incidents impact an ISP's brand, churn rates and Net Promoter Score (NPS).

3 **The worse home Internet security gets, greater awareness will create better opportunities for ISPs to differentiate with security as a trusted provider.** Business cases then turn on whether the ISP can make enough additional revenue and margin from the required investment (and if so, for how long).

Figure 4: What is to be Done? Key Security Measures for Home Routers

Security Measure	Direct Responsibility	Description
Network security	ISP	Blocking of unauthorized access to the home network
Network security	ISP	Restricting the tasks the home router is allowed to perform
Network security	ISP	Two Factor Authentication to limit use of permitted communications
Antivirus software	User, router vendor or ISP	Real time or regular scanning & updates for the home router
Router firmware updates	User, router vendor or ISP	Manual (by the user) or automated (supported by some vendors)
Router Product design	Router vendor or ISP	Product hardening; encrypted protocols; authenticated services.
Cyber hygiene	User / ISP	Strong password policy; enable security features; avoid risky sites

Source: HardenStance

In most countries, the law doesn't clearly tell ISPs where their responsibility for home router security begins and ends. Where they re-badge a router vendor's product with their own brand, the ISP is often liable for that product's performance. Where they don't, they're probably not. The truth is, though, that the detailed legalese is usually too nuanced, and ultimately not relevant enough, for the ISP's strategy to be driven by it. If an ISP decides to pursue a strategy of leadership in home Internet security, then being seen to discriminate between those among its customers that it will stand by and protect, and those it won't, is inconsistent with that market positioning. ISPs need to be binary about this. If they want to lead in consumer Internet security, they must take a universal, all-embracing, stance across all their customers - or not bother at all.

Telcos and ISPs are unique in being able to address every layer of home router security.

As shown in **Figure 4**, telcos and ISPs are unique in being able to address every layer of home router security. Even when it comes to the user's own cyber hygiene, the ISP can be active not just in educating them but in providing on-line tools and mobile apps so users have an option to monitor and improve their home security posture themselves.

Most ISPs already engage very actively in preventing, detecting and remediating network attacks, notably at major peering points where they can protect against the greatest threats to the greatest number of customers. They can also combine their unique network-wide visibility and footprint in the home to protect the home networks of individual consumers. Security is always about layers. In home router security, AV software is very important, but it doesn't protect against unauthorized access. Firmware updates are very important, but they can represent a vulnerability in their own right.

New Tools for ISPs to Differentiate With

Network level white-listing and authentication capabilities provide additional protections that ISPs can bring to bear in addition to those depicted **in Figure 3**. These include:

- **Blocking unauthorized access to the router.** White-listing here can ensure that only specifically authorized servers are able to communicate with the home router. Unauthorized access is automatically blocked.
- **Prescribing only those binaries that are allowed to run on the home router.** This enables ISPs to ensure that unauthorized binaries are unable to run.
- **Two factor authentication (2FA) to limit the use of permitted communications.** While legitimate access to the management interface has to be allowed, another security layer can be added by means of 2FA such as a message to a mobile app to ensure only authorized users are accessing the home router.

The measures described can provide additional protection against many of the most straightforward attack vectors. As has been shown, these continue to cause high levels of harm to Internet users. Moreover these capabilities have the unique advantage that they can be applied across an ISP's entire installed base. It can therefore protect all the different home routers in the ISP's network, including the substantial share of different devices that tend to be highly insecure.

If ISPs Don't Choose to Lead, they May Face New Regulations Anyway

The cyber risk to home networks is greater now than it was just eighteen months ago. Hence there's potentially more commercial risk to an ISP from allowing its security capabilities to fall behind those of competitors. That said, the fundamental decision for the ISP remains essentially the same. It can lead in home router security. Alternatively it can wait for government to impose new regulations (which may or may not be effective) or let competitors get out in front.

About Allot Communications

Allot is a leading provider of innovative network intelligence and security solutions that empower communications service providers (CSPs) and enterprises worldwide to enhance the value they bring to their customers.

Allot Secure network-based security disrupts the security industry. It positions CSPs as leading Security-as-a-Service providers able to capture market penetration exceeding 50% and generate value-added-service revenue of 10-15% on top of connectivity revenue. Allot Secure enables CSPs to deliver security services that protect mobile devices and the broader connected home environment, as well as improving the security posture of the home router itself.

The Allot Smart solution suite, powered by inline DPI technology, generates insightful intelligence that empowers customers to optimize, innovate, and capitalize on every service opportunity. By analyzing every packet of network, user, application and security data, Allot Smart cost-effectively enables the highest Quality of Experience (QoE) for their users. Use of Allot Smart has lowered access bandwidth costs by 10%, deferred capacity expansions by 1-2 years and reduced revenue leakage by 15%.

Allot's multi-service platforms are deployed globally, in the most demanding environments, by over 500 mobile, fixed and cloud service providers and over a thousand enterprises. We support evolving network architectures by offering the most flexible platforms in the market, including COTS hardware, software only and field-proven, fully NFV compliant solutions.

With over 20 years of proven success, Allot solutions make customers' networks smarter and their users more secure. For more information, visit www.allot.com

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, and ETSI. www.hardenstance.com