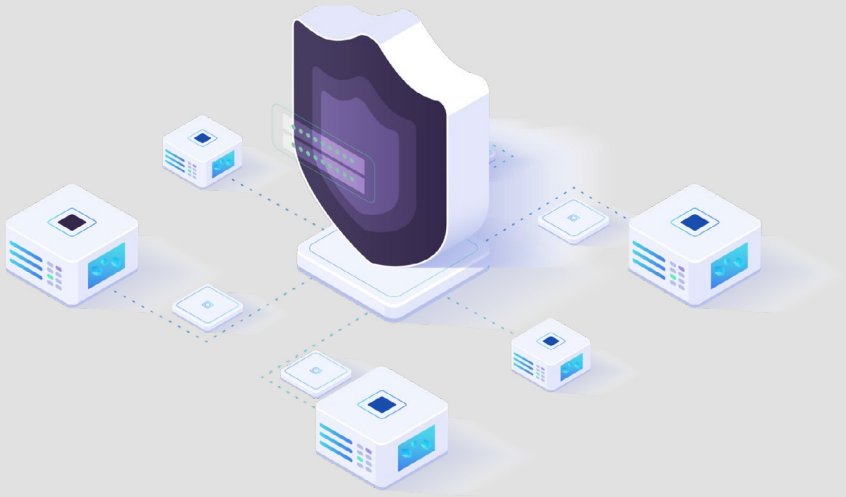
LOXADA™

SAFE, SECURE, REMOTE

WHITE PAPER

The Growing Focus on Network Edge Risk: Why Off-the-Shelf Routers are a Concern for Organizations of All Sizes

By Gwilym Lewis, Co-founder at Loxada



"More than 80% of off-the-shelf routers have known unpatched vulnerabilities. Even when running the latest firmware."

SOURCE https://www.packetlabs.net/posts/work-from-home-increases-risk-of-cyberattacks-via-soho-routers/

Executive Summary

Network edge risk has become a significant concern for organizations as employees increasingly access corporate data from locations beyond direct IT control. While often referred to as Small Office/Home Office (SOHO) routers, employees across businesses of all sizes use these off-the-shelf devices, introducing critical security vulnerabilities.

Government agencies and cybersecurity experts have highlighted the growing number of threats targeting these devices, leading to large-scale incidents like the Mirai and VPNFilter botnet attacks.

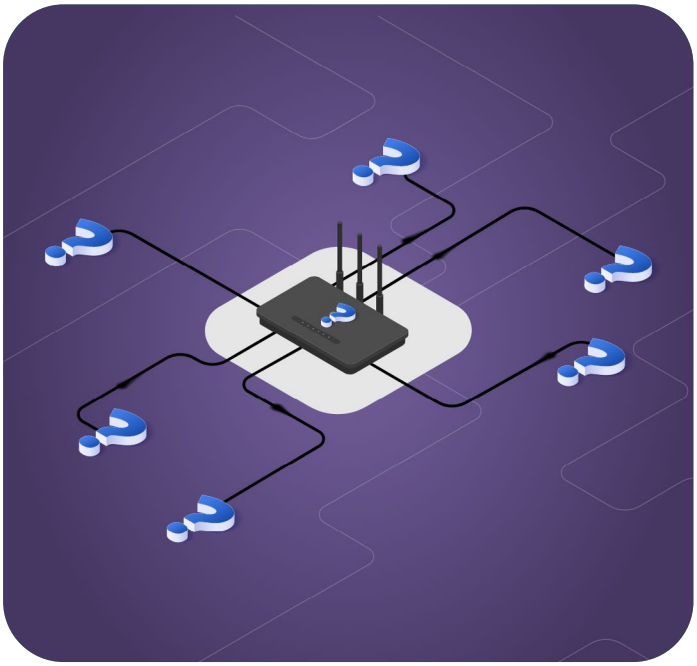
This whitepaper brings together recent developments, real-world examples, and expert perspectives to provide a single point of reference explaining why off-the-shelf routers pose a serious and often overlooked risk.

It explores how vulnerabilities persist even with regular updates, how human factors amplify these risks, and what organizations can do now to reduce their exposure based on current industry best practices. It concludes with a practical checklist for organizations looking to assess their level of risk and take immediate action.

Introduction:
Understanding Network Edge Risk

> **"Malicious actors are increasingly exploiting vulnerabilities in edge devices to infiltrate critical networks and infrastructure."**

SOURCE https://www.bleepingcomputer.com/news/security/cyber-agencies-share-security-guidance-for-network-edge-devices/



Recent headlines have brought renewed focus to the security challenges network edge devices pose. Government agencies, cybersecurity researchers, and industry experts are sounding the alarm on the threats posed by off-the-shelf routers and other network edge devices that are often physically close to users but outside the direct control of IT departments, MSPs, and security teams.

The routers in this category are commonly referred to as Small Office/Home Office (SOHO) routers, but this term is misleading. While it suggests the problem is confined to small businesses, the reality is that these routers are used extensively by employees across companies of all sizes.

SOURCE https://www.cisa.gov/news-events/alerts/2024/01/31/cisa-and-fbi-release-secure-design-alert-urging-manufacturers-eliminate-defects-soho-routers

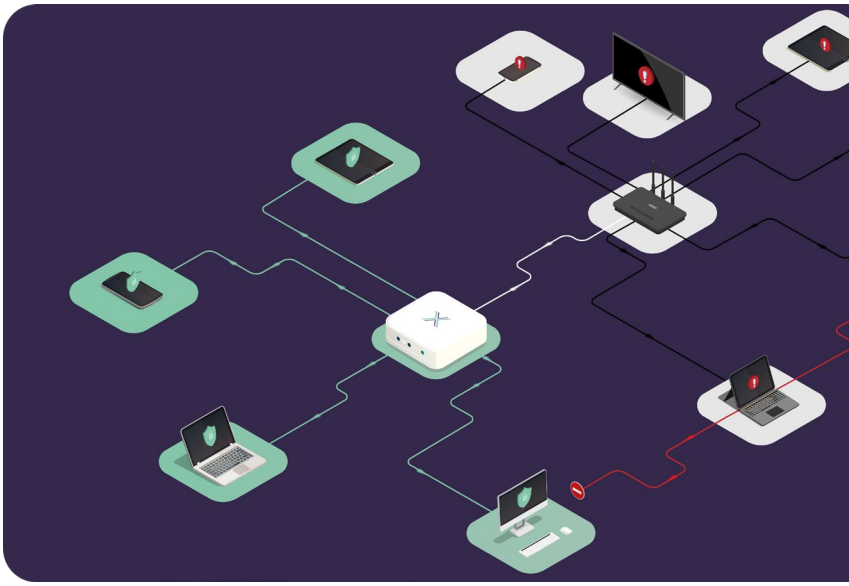
Whether people work from home, in private offices, in coworking spaces, or in serviced offices, the risks multiply as organizations don't have direct control over the networks used to remotely access data, sensitive or otherwise.

In February 2025, the Five Eyes alliance (comprising intelligence agencies from the United States, United Kingdom, Canada, Australia, and New Zealand) released a joint advisory emphasising enhanced security measures for network edge devices.

SOURCE https://www.bleepingcomputer.com/news/security/cyber-agencies-share-security-guidance-for-network-edge-devices/

While this guidance is mainly aimed at manufacturers, encouraging secure logging, forensic readiness, and secure-by-design principles, widespread adoption may take years, if it happens at all. With hundreds of millions of devices already in use, what follows focuses on what organizations can do now to better understand and mitigate the risks highlighted.

Why the Focus on Off-the-Shelf Routers?



Governments and regulators are increasingly concerned about the security of consumer-grade routers. The US Cybersecurity and Infrastructure Security Agency (CISA) and the FBI have warned that many off-the-shelf models lack secure-by-design principles.

SOURCE https://www.cisa.gov/news-events/alerts/2024/01/31/cisa-and-fbi-release-secure-design-alert-urging-manufacturers-eliminate-defects-soho-routers

In March 2025, the US Congressional Committee on China publicly recommended that Americans stop using certain foreign-manufactured routers, specifically naming TP-Link (although they are by no means alone here) due to national security concerns.

SOURCE https://www.reuters.com/world/us/us-congressional-committee-china-urges-americans-ditch-tp-link-routers-2025-03-05/

Similar concerns have been raised in the UK Parliament, where policymakers have warned about remote sabotage risks via imported electronics and even called for increased domestic manufacturing.

SOURCE https://www.ft.com/content/518e6b5d-068a-4375-a625-87d8c5b422a1

Case Study

In one persistent campaign, Chinese threat actors exploited firewall products from a UK security vendor over a five-year period, accessing sensitive targets including military and government agencies. This highlights the difficulty of securing edge devices; even organizations with in-house security expertise can fall victim.

SOURCE https://www.wired.com/story/sophos-chengdu-china-five-year-hacker-war/

The Multiplier Effect of Network Edge Risk

For organizations, the risks associated with off-the-shelf routers grow exponentially with scale. While one insecure router may pose a minor risk, hundreds or potentially thousands of employees connecting via unknown networks, typically outside corporate IT oversight, represent a significant threat.

Unlike corporate networks maintained by IT teams, many personal networks, or those in shared office buildings and coworking spaces, are a patchwork of router models, firmware versions, and configurations.

SOURCE https://avoidthehack.com/soho-routers

Threat actors can exploit these inconsistencies to bypass traditional security controls and gain initial access. Once inside, they may monitor traffic, install malware, or use the compromised network as a pivot point into more sensitive systems. CVE-2024-41335, for example, allowed remote code execution via a common TP-Link model, offering a foothold for deeper compromise.

Case Study

The VPNFilter malware infected over 500,000 routers across 54 countries, intercepting traffic, stealing credentials, and rendering devices unusable. Despite manufacturer patches, many devices remained vulnerable due to a lack of user action.

SOURCE https://avoidthehack.com/soho-routers

Even 'Up-to-Date' Isn't Always Safe

A common misconception is that regularly patching routers eliminates security risks. While patching is undoubtedly essential, it does not guarantee protection. Though many router updates address surface-level issues such as performance or interface enhancements, underlying vulnerabilities may remain unpatched.

SOURCE https://www.cybersecuritydive.com/news/150000-asus-routers-critical-vulnerability/719523/

A study by cybersecurity firm PacketLabs found that over 80% of off-the-shelf routers had unpatched vulnerabilities even when running the latest firmware. Some of these vulnerabilities were due to outdated software libraries embedded in the router's firmware, making them difficult for manufacturers to detect and resolve.

SOURCE https://www.packetlabs.net/posts/work-from-home-increases-risk-of-cyberattacks-via-soho-routers/

A study by the American Consumer Institute analyzed 186 routers and found over 32,000 known vulnerabilities, of which 28% were rated as high or critical risk.

SOURCE https://www.msspalert.com/news/home-wifi-router-vulnerabilities

The median CVSS score for edge-related vulnerabilities now stands at 9.8, compared to 8.8 for non-edge issues. This suggests a significantly higher level of exploitable threat, particularly for devices that have historically not been treated as a major source of risk.

Case Study

The Mirai botnet used insecure routers to launch DDoS attacks that disrupted services like Twitter and Netflix, demonstrating the systemic risk these devices can pose when deployed at scale.

SOURCE https://thehackernews.com/2024/09/quad7-botnet-expands-to-target-soho.html

Human Factors: The Often Overlooked Risk

Technical solutions alone are not enough. Employees themselves play a crucial role in reducing network edge risk. Even a small percentage of individuals making smarter security choices can have a meaningful impact.

Organizations should provide practical training to help employees understand why router security matters. Studies indicate that user awareness programs can significantly reduce incidents of network compromise.

SOURCE https://www.infosecinstitute.com/resources/security-awareness/home-router-security-best-practices/

Simple actions like changing default passwords, disabling unnecessary features like remote management, and updating firmware can drastically reduce risk. When employees understand that their home, serviced office, or coworking space network is an extension of their company's attack surface, they are more likely to follow best practices.

Expert Perspectives

Michael Horowitz, founder of RouterSecurity.org, warns that compromised routers can redirect users to malicious sites without their knowledge and emphasises regular updates and credential changes as basic defence measures.

SOURCE https://www.csmonitor.com/World/Passcode/2015/1202/Your-Internet-router-is-a-security-risk.-Here-s-why

Craig Young of Tripwire notes that many routers are rushed to market with minimal security testing. Whilst this applies to many products, routers are especially risky because users may not know they need to check for updates (or even how). As discussed above, even when updates are applied, there's no guarantee that security has actually improved.

SOURCE https://www.csmonitor.com/World/Passcode/2015/1202/Your-Internet-router-is-a-security-risk.-Here-s-why

Recommendations for Mitigating Network Edge Risk

While we wait for manufacturers to improve the security of their devices, there are immediate steps organizations can take. Many companies are adopting stricter remote access policies in response to these challenges. Some now provide secure, pre-configured routers to remote staff. Others are building policies around trusted hardware lists and patch enforcement. Cybersecurity frameworks like NIST's IoT guidelines offer a helpful reference.

SOURCE https://csrc.nist.gov/pubs/ir/8425/a/final

Case Study

Another example involves older ZyXEL ADSL in use in many countries. Forensic analysts discovered a severe vulnerability enabling full network compromise. Despite this, the manufacturer did not release a fix even though it was still possible to buy the models in question on sites like Amazon. They did suggest replacing the devices, but that's a tough ask, especially when individuals or IT teams don't know the equipment's model they have at home and may never see security advisories for it.

SOURCE https://techcrunch.com/2025/02/05/router-maker-zyxel-tells-customers-to-replace-vulnerable-hardware-exploited-by-hackers/#:~:text=The%20vulnerabilities%20were%20discovered%20by,Amazon%2C%20which%20TechCrunch%20has%20confirmed.

To reduce the threat posed by insecure off-the-shelf routers, organizations should adopt a layered approach:

01 **Promote Secure Router Practices**
Help employees keep devices safe by guiding them on updates, strong passwords, and disabling risky features like remote access.

02 **Account for Third-Party Networks**
Make staff aware of the risks in managed offices and coworking spaces, even when networks feel familiar or professional.

03 **Implement Network Separation**
Require separate networks for corporate and personal devices to limit exposure and reduce the chance of lateral threats.

04 **Leverage Endpoint Security Solutions**
Use endpoint tools like EDR to detect unusual activity from devices connecting through external or unmanaged networks.

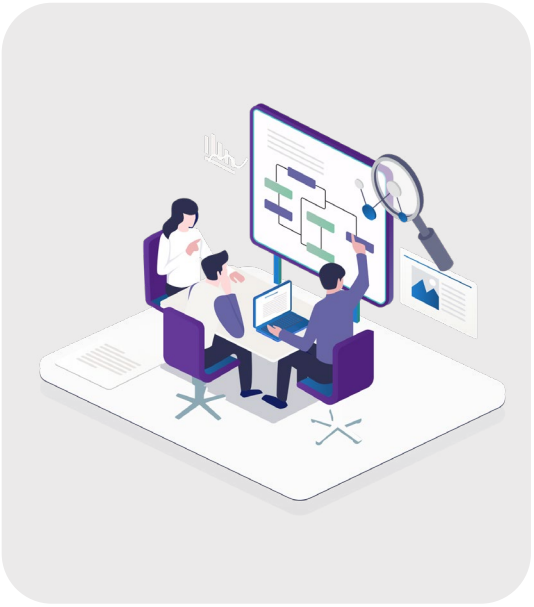
05 **Consider Zero Trust Principles**
Treat all external networks as untrusted and require continuous verification before granting access to company resources.

06 **Educate and Empower Employees**
Offer simple, repeatable training that explains real-world risks and how users can reduce them wherever they connect.

Conclusion

The risks posed by network edge devices outside the control of IT, such as off-the-shelf routers, are not going away anytime soon. Most organizations have people accessing data from networks they don't manage, whether at home, on the move, or in office environments where the IT is controlled by a third party. This isn't just a "remote working" issue; it's a visibility and control issue over how people access data remotely, for any purpose, and from anywhere.

By acknowledging and addressing the real-world risks of edge devices, especially those physically close to users but far outside security oversight, organizations can start to reduce their exposure. It begins with education, practical policies, and a clear understanding of what's at stake.

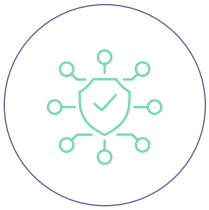


Quick Risk Assessment Checklist for Organizations

Use this checklist to assess your organization's exposure to network edge risk:

Network Awareness and Control

1. Do you have visibility into the types of routers your employees use for remote access?
2. Are employees required to register their home or third-party office networks with IT security teams?
3. Have you established clear guidelines for router selection and secure configuration?



Router Security Practices

1. Do you instruct employees to update router firmware regularly?
2. Do you monitor for routers that are no longer receiving manufacturer updates?
3. Do you provide guidance on disabling unnecessary services like remote management and Universal Plug and Play (UPnP)?

Employee Training and Awareness

1. Do you offer training on identifying router vulnerabilities and applying security updates?
2. Do you encourage employees to use strong, unique router passwords and change default credentials?
3. Do you provide a process for reporting suspected router compromises?

Network Separation and Monitoring

1. Do you require the use of separate networks for corporate and personal devices?
2. Do you implement endpoint detection and response (EDR) tools to monitor external connections?
3. Are corporate devices configured to enforce secure VPN connections?

Third-Party Network Risks

1. Do employees working in managed offices or coworking spaces receive guidance on network security risks?
2. Do you have a policy for evaluating third-party networks used for corporate data access?
3. Do you apply Zero Trust principles to ensure continuous authentication on untrusted networks?

This checklist can serve as a starting point for discussions within your security team. Addressing these areas will help mitigate the risks posed by insecure routers and improve your overall security posture.