BESTPATH

The Increasingly Vulnerable Network

What’s changed, and what you can do about it

Introduction

Secure and stable networks are essential to business. But networks have increased in complexity, not least because of pandemic-hastened digital transformations which normalised hybrid working. The latest cybersecurity statistics reveal an increase in frequency of malicious cyberattacks such as zero-day exploits and ransomware[3].

Secure and stable networks are essential to business.

Network security is vital to protect data in transit

Understanding which areas of your network are particularly vulnerable will enable you to strengthen your network

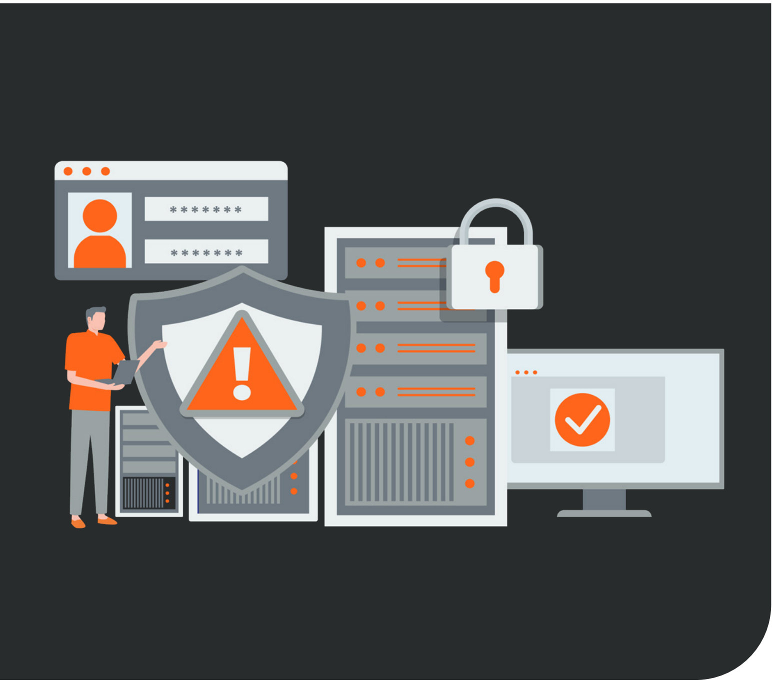
Network security is vital to protect data in transit throughout your network, with authentication to restrict access to sensitive data, and measures to minimise risk from threats such as ransomware.

Understanding which areas of your network are particularly vulnerable will enable you to strengthen your network security, minimise outages, and protect your business.

Here, we explain where your business network could be exposed to security risks. We also outline some practical steps you can take to address the vulnerabilities in your technology and minimise the risk of unwelcome network problems and outages.

Network security is vital to protect data in transit throughout your network

Contents



The need to avoid complacency

Cybersecurity is like any other disaster preparation: when pre-emptive measures are effective, the majority of people will be completely unaware of the danger they were facing.

This unfortunately means that IT security teams who are successful in averting disaster can be victims of their own success—the catastrophic events did not materialise, so the scale of the threat to a business may be underestimated by those not directly involved.

It is unsurprising then that underinvestment in cybersecurity can be a costly mistake.

On fining a construction company £4.4 million for failing to keep data secure, the UK Information Commissioner noted the biggest cyber risk is complacency, including failure to update software, monitor systems adequately, and train staff. That company's complacency gave hackers access to >100,000 employees' personal data via a phishing email[2].

> *"The biggest cyber risk businesses face is not from hackers outside of their company, but from complacency within their company.[2]"*
>
> *John Edwards, UK Information Commissioner*

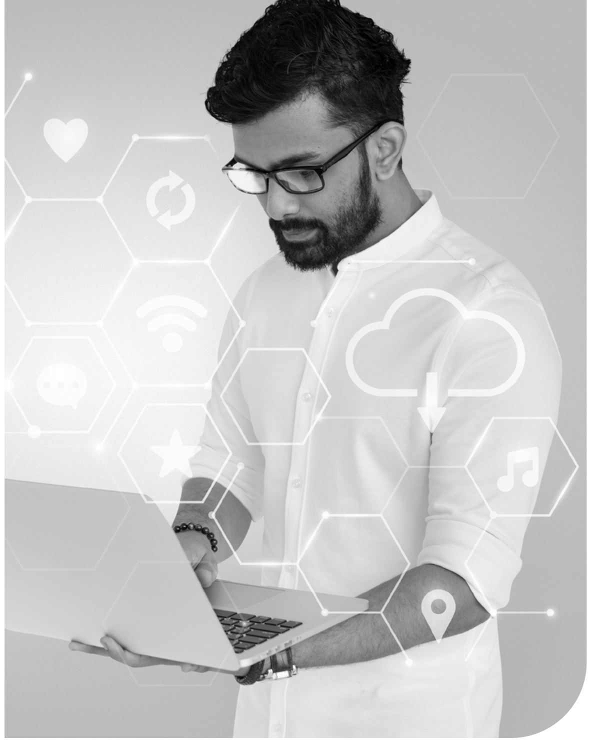
Case study:

Failure to train staff

Failure to update software

Results:

£4.4	>100,000
million fine	employee data breach



Attack surface vulnerabilities

Historically, simple on-prem technology—and on-prem employees—meant that the attack surface for a business was relatively straightforward and contained. But times change. The attack surface area has become significantly larger and more complex for many businesses through two otherwise positive technological and social developments, cloud technologies and workplace changes.

Historically the attack surface for a business was relatively straightforward and contained.

But times change.

Cloud technologies

The ever-increasing array of IT options 'as a service' offers businesses a huge amount of flexibility to customise the way they work, with exciting opportunities to create competitive advantage, often via hybrid and multi-cloud solutions. But if this landscape is not managed properly, end-to-end monitoring capability is likely to be compromised—which means unnecessary network vulnerabilities become almost inevitable.

The challenge of protecting a company's tech stack is not helped by the lack of standardisation between vendors—even the top three cloud infrastructure service providers (Amazon Web Services, Microsoft Azure, and Google Cloud), who shared two-thirds of the worldwide market in Q3 2022[6], differ in their structures and set-up[5].

Finding a professional support team with the knowledge base to secure all possible touchpoints is vital.

> *If you've got so many disparate systems, you're also exposed, because you've got so many different touchpoints within your organisation.*[1]
>
> *James Williamson, Managing Director, BestPath*

Workplace changes

Accelerating rapidly due to the COVID-19 pandemic, technological solutions have enabled employees and contractors to work from home (WFH) either fully or partially, or from decentralised offices, and to use multiple devices in office and field-based applications.

This naturally increases the attack surface through the number and variety of access points workers have to an organisation's infrastructure, increasing the risk to the network.

> *If you're not consolidating your access, if you're not getting visibility into everything it is that you're doing, how do you secure it?* [1]
>
> *James Williamson, Managing Director, BestPath*

Part of the solution is to protect users at the edge - ensuring seamless connections without impacting the users productivity. Without this approach, employees who are unaware of the ways in which an organsiations network might be compromised, may ignore protocols and even bypass security measures that have been put in place.

> *In a year, 58% of businesses delivered cybersecurity awareness or training sessions to those not directly involved in cybersecurity*[7].
>
> *UK Government: Cyber security longitudinal study*

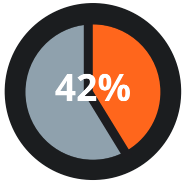
In summer 2022, 36% of businesses allowed staff to access their network or files through their own personal devices. Of the 72% of businesses with a VPN, around four-fifths made staff use it to access their network or files remotely[7].

Ensuring all individuals understand their role in keeping networks secure should help reduce the risk of network outages.

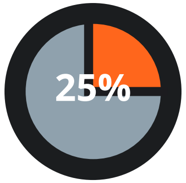
The risk from suppliers

In a recent UK Government survey, only 42% of very large businesses and just 25% of medium-sized businesses had assessed or managed cybersecurity risks related to their suppliers. Among businesses certified to ISO 2700[1], the proportion was higher, but still only 52%[7].

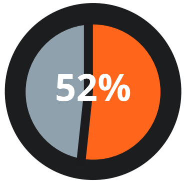
Security risks from suppliers include the touchpoints with your business—some suppliers may have third-party access to parts of your network and could introduce cyberthreats from their own systems. And is your network configured correctly for third-party access—for example, could your network configuration for suppliers also facilitate unauthorised access to, and export of, your intellectual property or data?



of very large businesses



of medium sized businesses



of businesses certified to ISO 27001

Infrastructure integration and configuration

Because systems and applications have evolved so quickly, many businesses have technology stacks that are not fully integrated. The resulting lack of real-time data-driven observability can limit performance improvements and efficient fault tracking[8].

Configuration issues are also a major challenge. According to Microsoft, 80% of ransomware attacks can be traced to common configuration errors in software and devices." [9] Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws.[10]

Technology stacks that are not fully integrated

80% of ransomware attacks traced to configuration errors

99% of firewall breaches caused by firewall misconfigurations

3 ways to reduce your network vulnerabilities:

1. Review and minimise your attack surface

Pay particular attention to recent configuration changes to ensure you are conformant with your configurations, software and hardware strategies.

2. Consolidate access points with a secure single sign-on

Make sure unauthorised access is prohibited, and that you get the relevant insights and logs when those who shouldn’t attempt to gain access. Using a centralised identity provider helps reduce the number of different accounts used.

3. Check that all tech is configured correctly for maximum security of your valuable data and assets

Where different platforms and technologies are used to host different applications, check the correct security procedures are followed to limit exposure.

To learn how BestPath can help you tackle your network vulnerabilities and improve your network security, contact us today.

linkedin.com/company/bestpath/

info@bestpath.io

+44 (0)203 879 4826

We’re BestPath. The unsung heroes, working quietly and competently behind the scenes to inspire and empower our clients. Combining curiosity with innovation we deliver agile, secure and trusted network infrastructures that enable organisations to deliver exceptional services and outstanding customer experiences.

Let’s chat about how we can do just that, for you. info@bestpath.io

References

1. **Switching It Up with Jimbo and Nick! Episode 6: Happy New Year's Trends. Season 1 Episode 6, January 06, 2023.**

https://www.buzzsprout.com/2045427/11991834

2. **ICO (2022). 'Biggest cyber risk is complacency, not hackers' - UK Information Commissioner issues warning as construction company fined £4.4 million. ICO News, 24 October 2022.**

https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/biggest-cyber-risk-is-complacency-not-hackers/

3. **Fox, Jacob (2022). Cybersecurity Statistics for 2023. Cobalt, 27 December 2022.**

https://www.cobalt.io/blog/cybersecurity-statistics-2023

4. **Paz, Jay (2022). The State of Pentesting 2022: How Labor Shortages are Impacting Cybersecurity & Developer Professionals. Cobalt, 06 April 2022.**

https://www.cobalt.io/blog/the-state-of-pentesting-2022-how-labor-shortages-are-impacting-cybersecurity-and-developer-professionals

5. **Morag, Shai (2023). How the Cloud Is Shifting CISO Priorities. DARKReading, 03 February 2023.**

https://www.darkreading.com/cloud/how-the-cloud-is-shifting-ciso-priorities

6. **Richter, Felix (2022). Amazon, Microsoft & Google Dominate Cloud Market. Statista, 23 December 2022.**

https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

7. **UK Government (2022). Cyber security longitudinal study - wave two. DCMS, Reseach and analysis, updated 19 December 2022.**

https://www.gov.uk/government/publications/cyber-security-longitudinal-survey-wave-two-results/cyber-security-longitudinal-study-wave-two

8. **NTT (2022). What you can't see can hurt you: the importance of full-stack observability. CIO sponsored post, 16 November 2022.**

https://www.cio.com/article/411871/what-you-cant-see-can-hurt-you-the-importance-of-full-stack-observability.html

9. https://news.microsoft.com/apac/2022/08/23/microsoft-releases-its-second-edition-of-cyber-signals-tracking-ransomwares-new-business-model/

10. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure