O2 business

Mind the gap

O2 Digital Defence closes four security gaps that could put your organisation at risk

Closing the security gaps in your organisation

As commuters we're often told to 'mind the gap'. But what happens when the gap is something you can't see?

When it comes to cybersecurity, that's the situation many large organisations are in today. The threat landscape, network and IT infrastructure, and the way people work are all changing fast.

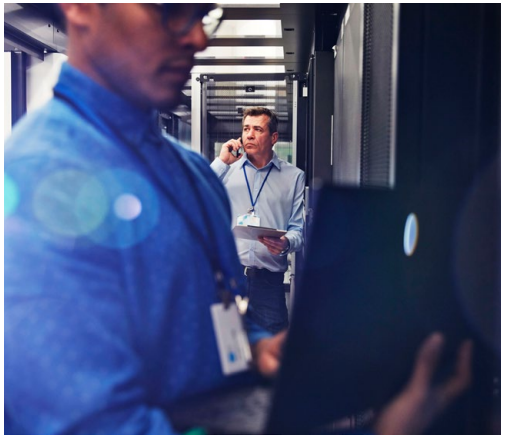
The result: an IT security setup that, even with the best will in the world, could have invisible gaps that could compromise your business, your customers and your people.

We get that in a fast-changing world, protecting everything you have can seem an impossible task. That's why we partner with the industry leading names in the industry to create a comprehensive suite of solutions and services to keep your whole organisation safe.

You may not have the time or the resource to address all of these gaps. If that's the case, we can help. We draw on 16+ years' global security expertise and a comprehensive suite of security solutions and services to help you address all four critical gaps.

"More than three out of four firms (**61%**) reported an attack in the last year - up from **45%** the previous year."

Hiscox Cyber Readiness Report 2019[1]



1 - Hiscox Cyber Readiness Report 2019


#1
The **coverage** gap
#2
The **workstyle** gap
#3
The **skills** gap
#4
The **awareness** gap

#1 The **coverage** gap

Most enterprise IT infrastructures have grown over time to become extremely complex.

Even organisations that have gone through a modernisation exercise, like a cloud or digital transformation, are still managing thousands of endpoints, network connections, databases and applications.

More than likely, those elements are protected by different security solutions at different layers, and perhaps by different teams of internal and external professionals.

Your business systems and applications may combine to expose a wider platform for attack. As new vulnerabilities to software and systems continue to emerge, it makes it difficult to keep up to date with the latest protection. And how to identify and prioritise the order in which vulnerabilities should be tackled to minimise your exposure and risk levels. It's a continually moving set of goal posts to understand and manage.

Every one of those gaps is a vulnerability – and while it's unrealistic to think the organisation will ever be 100% safe, it makes sense to know where the gaps are and try to close them.

A Minerva Labs survey of 600 security professionals found that two-thirds don't believe their controls could prevent a significant malware attack on their endpoints

Minerva Labs, April 2018[2]

How we can help

Our comprehensive Cyber Security Assessment is a detailed evaluation of your current security posture. Our enterprise security team will conduct a thorough assessment, highlight any coverage gaps and make recommendations for the best ways to close them – and keep them closed.

Uncover gaps in your defences with a Vulnerability Management service from O$_2$

Our Vulnerability Management service delivers a continuous review of your IT systems to find any security gaps and alert you to any issues, so you can swiftly close the door on potential weaknesses. Dashboards and 24/7 alerts keep you up to date with your current security posture across your business. You can also choose to add manual penetration tests, where our ethical hackers supplement automated tools with human intelligence to mimic a real-life attack.

2 - Minerva Labs press release, April 2018

#2 The **workstyle** gap

There's a new adage doing the rounds: 'work is something you do, not somewhere you go'.

We are seeing today in some organisations a shift to more flexible workspaces in corporate environments. Lifestyle changes, technology advances and digital workplace policies have ushered in a range of new workstyles: from remote and flexible working to virtual teams, job-sharing, field working, the gig economy and many flavours in between.

The shift has had a profound effect on the technology your people use to get work done. They're working from cafés using free wifi, and using their smartphones to create mobile hotspots on the train. They're switching between company laptops, personal laptops and personal smartphones. They're installing their own apps on company devices, and using their own devices to access company apps and data.

If your security solutions were installed before this workstyle revolution got underway in your organisation, you may be poorly protected against a whole swathe of threats: from lost or stolen devices to malware or data theft introduced through unsecured wifi.

During the second half of 2018 there was a rapid growth in threats against mobile devices and other connected things. The number one threat category was hidden apps which accounted for almost one third of all mobile attacks.

McAfee Mobile Threat Report 2019[3]

How we can help

We can help keep your people, customers and data safe, no matter where they are. We can route calls over a secure network, and protect internet and cloud connections from malicious attacks, and more. With us, you can give your people security that follows them anywhere – enabling smarter communication, collaboration, and productivity.

Protect your mobile workforce with O$_2$

We can maintain continuous security across your business, including mobile, laptop, servers and IoT. Our solutions can detect cyber threats, through a combination of cloud- and device-based services. We can provide always-on, up-to-date protection for you and your business – by blocking malicious activity that may help stop attacks before they cause any brand, reputational or financial damage.

3 - McAfee Mobile Threat Report 2019

#3 The **skills** gap

In 2018, the UK Parliament's Joint Committee on National Security Strategy[4] found that even some of the most security-conscious companies in the UK were struggling to fill internal cybersecurity positions. And the problem isn't limited to the UK. An October 2018 report by (ISC)[2] revealed that 63% of businesses worldwide have a cybersecurity skills gap.

When external candidates are in short supply, the options for addressing the skills gap include upskilling internal staff and partnering with an expert security provider. Working with an external partner can ensure vital competencies are available in the short term while you upskill your team.

63% of businesses worldwide say they have a cybersecurity skills gap.

(ISC)[2], Global Cybersecurity Workforce Study, 2018[5]

How we can help

When you work with someone you trust, you lose the day-to-day worry of finding the skills you need or the headache of juggling all the solutions that ensure your security. We work with best-of-breed providers to get you a comprehensive security package that's shaped around the way your business and your people work.

Bridge the skills gap with O$_2$ Security

Our global reach extends to 10 SOCs (Security Operation Centres) located in the UK, Spain, Brazil, Peru, USA, Argentina, Colombia, Mexico and Chile. Every year, we track over 100 million security events worldwide – giving us detailed, up-to-the-minute insight into what's going on in the world of enterprise security. This is combined with an established cyber security practice with over 16 years of global experience with Telefónica's ElevenPaths.

4 - UK Parliament's Joint Committee on National Security Strategy
5 - (ISC)[2], Global Cybersecurity Workforce Study 2018

#4 The **awareness** gap

Often, even the best-structured technological defences are no match for skilled cybercriminals.

Often, even the best-structured technological defences are no match for skilled cybercriminals. Many of the most successful attacks work by social engineering: persuading employees to part with passwords or other confidential data, and even convincing them to transfer large sums of money into criminals' bank accounts.

If they're not aware of what an attack looks like, employees can unwittingly put your organisation at risk from malware, phishing, CEO fraud, ransomware and other types of attack that exploit people's trusting and helpful nature.

Before an attack happens, cybercriminals need to understand more about your company and what is valuable to target. This data can then be directly sold on or traded on the dark web.

Cybercriminals may also replicate your brand with online sites pretending to be you. Potentially extracting payment for goods and services not only scamming you but also your customers.

With social engineering attacks growing daily in sophistication, staying alert to the latest techniques – and understanding your digital exposure enables you to better protect your brand, your income, your intellectual property, your customers, and your reputation.

The frequency of attacks has also increased markedly. Among firms that experience cyber attacks, the proportion reporting four or more incidents is up from 20% to 30%.

Hiscox Cyber Readiness Report 2019[6]

How we can help

We fortify your defences; working with you to spot and eliminate threats inside and outside the network. With our people managing your one-stop security infrastructure, we'll help to create a stronger network, increased performance, and less downtime.

Stay alert with CyberThreats Digital Surveillance from O$_2$

CyberThreats Digital Surveillance monitors illegal activity across thousands of sources on the open Web as well as the Deep Web and the Dark Web. It gives you insights into the typical attacks in your industry. It checks the information on your selected executives and builds a risk profile about how these people could be targeted. It detects if you've had credentials to your systems stolen. And finds malicious apps that are stealing data. And we find sensitive data that has leaked out. Most important, it gives you ways to help prevent these threats from undermining your business.

6 - Hiscox Cyber Readiness Report 2019

Why choose O_2?

We have a long experience of working with organisations of all sizes to connect and empower their people, customers and suppliers.

With us you'll have access to the benefits of the first UK CAS(T) certified Mobile and WAN network, and reap the rewards of our powerful security partnerships with best-of-breed providers such as Radware, Fortinet, Forescout, Zscaler, Cisco and Palo Alto Networks.

In addition to the extensive portfolio of products we can offer, our global reach extends to 10 SOCs (Security Operation Centres) located in the UK, Spain, Brazil, Peru, USA, Argentina, Colombia, Mexico and Chile. Every year, we track over 100 million security events worldwide – giving us detailed, up-to-the-minute insight into what's going on in the world of enterprise security. And all this knowledge – combined with an established cyber security practice with over 16 years of global experience with Telefónica's ElevenPaths – is channelled into the services we offer you.

We are part of the Cyber Security Alliance[7] and Cloud Security Alliance. And we're at the forefront of assisting GCHQ and NCSC[8] develop a cyber security economy with Wayra – the security accelerator program designed to protect the UK digital borders.

Leave the security to us, and you can focus on your core business priorities – your people and your performance – safe in the knowledge that you have the security infrastructure to back it all up.

7 - Cyber Security Alliance
8 - GCHQ and NCSC

Telefónica

Find out more about O_2 Digital Defence

The first step towards closing the security gaps in your enterprise is to discover where they are. We can help, with a comprehensive portfolio of solutions that range from an upfront assessment to ongoing threat detection and prevention across your whole IT estate.

To learn more about O_2 Digital Defence solutions:

Call us on 01235 433 507
or visit: o2.co.uk/business/solutions/security

O_2 business

Published in August 2019. All information is correct at time of going to print.

Telefónica UK Limited. Registered in England no. 1743099. Registered Office: 260 Bath Road, Slough, SL1 4DX