Rewriting the relationship- a collaborative model for security

April 2021

Rewriting the relationship between DIY and outsourcing for secure digital transformation

Coronavirus has turned the spotlight on cybersecurity as a strategic issue and business enabler

The past year has been a turning point for many reasons, not least of all the role cybersecurity plays for organisations. In businesses all over the world, IT teams raced to support homeworking at an unprecedented scale as the global pandemic forced millions of people out of their offices. But tactical decisions that were taken to keep businesses going have, in some cases, inevitably and understandably led to compromises and increased risk when it comes to security controls. Security teams are now striving to regain visibility and control of their estate and security posture and are shifting their focus to supporting these new hybrid working models over the long-term.

These workplace changes have also coincided with an increase in the threat landscape. Three quarters of business leaders say there are more and more security threats every year. This has been amplified by coronavirus – with a 600% increase in email scams, 100% increase in ransomware, and 400% increase in brute force attacks.

In a recent survey we ran, cybersecurity was ranked as the main priority for organisations after managing the consequences of coronavirus. We're also hearing from analysts that there's been a real change in the perception of the value of security and professionals in this field in the last 12 months. We, and others in the industry, have been saying this for a few years now, so it's encouraging to see a wider recognition of the fact that security is a true business enabler.

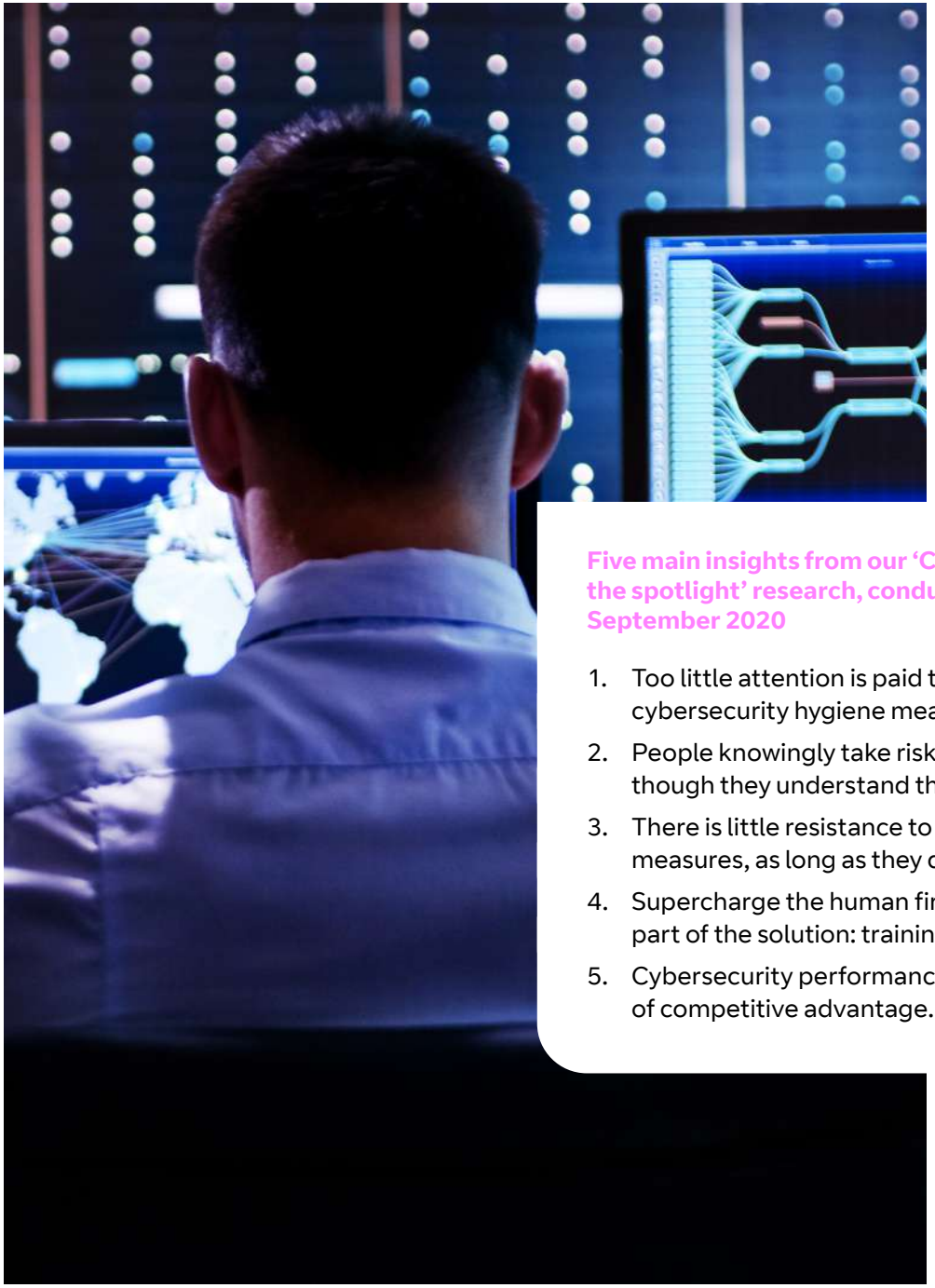
In-house security teams are faced with more threats, more technology choices, and a more important seat at the table

Whilst the above is true, within some organisations there remains a degree of inconsistency and complacency to treating security as a priority – even as it becomes more central to business decisions and the breadth of what needs to be protected widens. In our survey, three quarters of business leaders rated their organisation's IT strategy as excellent or good at protecting against cybersecurity threats. Yet 84% of executives also said that their organisation had suffered from data loss or a security incident in the last two years.

The scale of the problem is only increasing – 75% of executives say there are more security threats to their organisations every year – and a much broader range of solutions will be needed to tackle the rise in cybercrime. Emerging technologies, such as automation and orchestration, will be key to dealing with the volume of attacks.

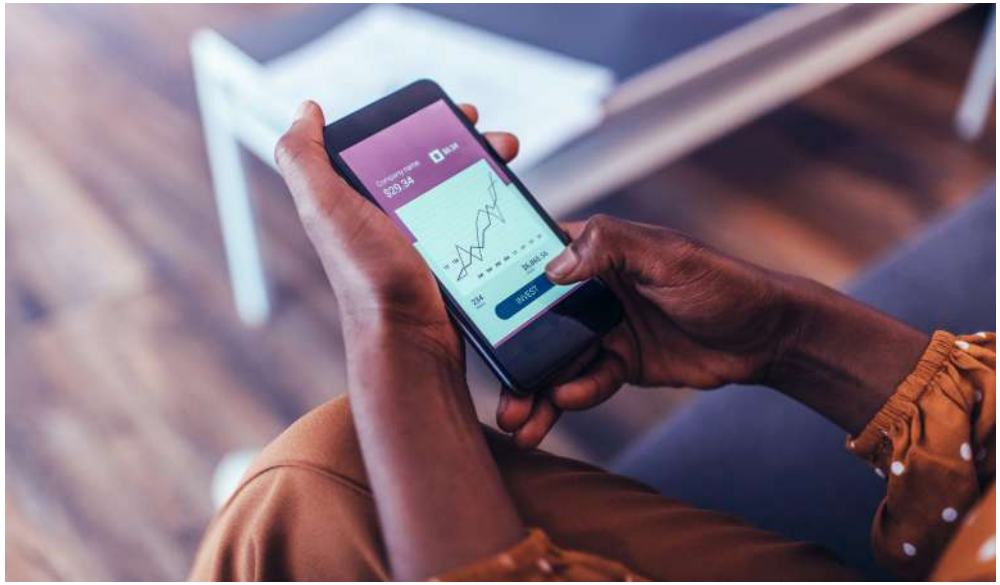
Added to this are critical skills shortages. According to a recent PwC survey, 56% of respondents said their organisation is at risk due to a lack of cybersecurity staff. It was also one of the top cybersecurity challenges called out when we surveyed 200 of our multinational customers at the end of last year.

It's clear that maintaining security in the face of the increasing pace and volume of threats can't be addressed singlehandedly. We believe that organisations need help from external partners to augment and bolster their in-house capabilities. But rather than a traditional outsourcing approach, the future security operations model must become a truly co-managed ecosystem if it's to succeed.



Five main insights from our 'CISOs under the spotlight' research, conducted in September 2020

1. Too little attention is paid to foundational cybersecurity hygiene measures.
2. People knowingly take risks online even though they understand the dangers.
3. There is little resistance to greater security measures, as long as they don't get in the way.
4. Supercharge the human firewall as a critical part of the solution: training is key.
5. Cybersecurity performance can be a source of competitive advantage.



Getting the right support is key as cybersecurity becomes a central strategic pillar to support digital transformation

Organisations should examine their sourcing strategies to identify areas where external partners can add value, such as introducing new technologies or complementary skillsets, as well as identifying which areas should remain under the organisation's direct control. Introducing the concept of 'shared responsibility' between the business and service provider will foster a more holistic approach to cybersecurity, rather than one in silos which can open-up areas of vulnerability.

This is the time to reassess security strategy and policies in line with new boardroom priorities and business objectives. With the right partners on board, cybersecurity can play a central role in how organisations position themselves for digitisation, the move to the cloud, and new ways of working. And as we've found, a business with a clear and visible cybersecurity posture will inspire customer confidence and create itself a competitive advantage.

Driving factors of a sourcing strategy include current investments, past experience, the need for flexibility, and trust and risk management

As we've talked to our customers about their sourcing strategies, a few key themes have stood out:

- the need to maximise existing resources and investments
- the need for clarity on what activities need to be retained in-house, and which can be managed by a trusted partner
- the impact of previous experiences with outsourcing
- the need for flexibility, both operationally and commercially
- trust and shared responsibility – both from their customers being able to trust the organisation, and from them being able to trust their partners and vendors
- taking risk-based decisions – both in terms of maintaining control and ownership and benefiting from outside expertise.

When it comes to existing investment, unsurprisingly, customers want to get the most out of their current assets. Those who've invested in security operation centres (SOCs) want to utilise this resource but may consider outsourcing the volume activities which don't need business context and insight to reduce the load on their analysts. Others who've invested in functions such as firewall management may want to outsource advanced threat detection to get up to speed more quickly in areas such as threat hunting. As they look at their teams, they must balance the need to develop their in-house talent with the need to do more without necessarily being able to increase headcount. And even if they're able to recruit, they may struggle to attract and retain those with the necessary skills.

The need for flexibility – both operationally and commercially – is another key consideration. Operationally, the current threat landscape means that organisations and their vendors and partners need to be a lot more proactive, particularly when dealing with the fallout from high-end attacks, such as SolarWinds. There needs to be clear agreements on who's doing what during times of 'peace' and times of 'war'.

Some businesses say that they can't be as nimble as they need to be while working with third parties and have been scarred by previous negative experiences. It's certainly true that in the past, many outsourcing agreements have stayed static while organisations' needs have changed. But we've seen that this can be addressed by having adequate governance and flexibility within the contracts, as well as by offering different service levels.

An additional factor that we believe is essential to the speed of response in complex, hybrid environments is automation. When we surveyed 200 multinational corporations across all verticals, 69% of them believed that automation was important to the success of their security operations, and 53% were already completely comfortable with the idea of a platform-based security automation and orchestration service.

However, almost 60% of respondents said that they wouldn't want changes made automatically to their security policies. This highlights the need to create trust by proving the safety and efficacy of automation, and that it won't lead to unintended consequences. We're seeing customers increasingly looking to share security responsibility with a trusted partner as a way forward to decrease risk and get the best out of both emerging technologies and existing investments. But trust must be earned.

Managing risk is clearly another key consideration, and one that has many moving parts. As we've already discussed, some of the more tactical technology decisions taken during the pandemic, such as engaging new vendors to address a particular need, led to an increase in risk that security teams now need to address. The more vendors that are introduced into a service model, the more complex it becomes to consistently apply policies.

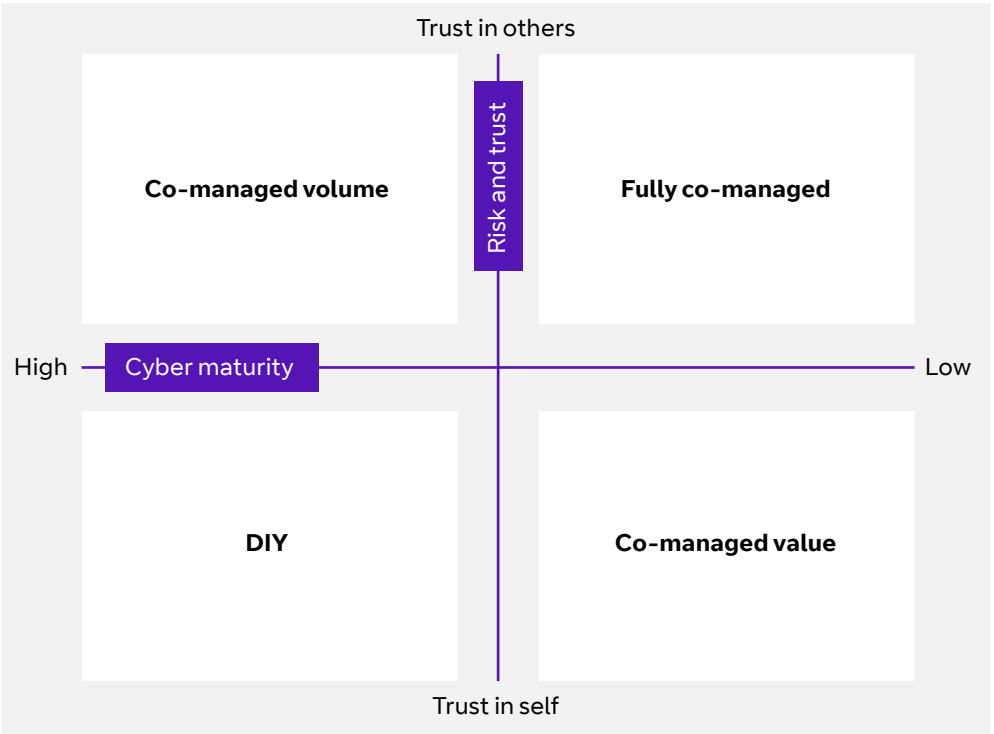
The two key levers in terms of managing risk are, firstly, the need for an organisation to regain or maintain a high degree of control and ownership, and secondly, to identify and get the benefit of outside expertise. For the first point, some organisations feel that outsourcing can result in the loss of control and ownership over their estate. However, on the flip side are the palpable gains brought by partners that can harness the cutting-edge technology and expertise needed to address today's sophisticated threats – particularly when coupled with the right co-management model.

Driven by an organisation's current state and priorities, a hybrid model can provide the level of flexibility necessary to support effective digital transformation

Against this backdrop of an increasing volume of threats, evolving technologies and skills shortages, the conversation becomes about where organisations see themselves today, where they want to get to in the future, and what levers they can use to help them get there.

This is where a hybrid sourcing model comes in. Rather than a binary decision, these models offer a sliding scale from DIY to full co-management, which caters for the fact that each organisation will be subtly different as to where they place themselves when it comes to risk, trust, and cyber maturity. Thanks to our global footprint and customer reach, we can also overlay some general trends by vertical or geography related to areas such as compliance and data privacy.

So, it's not about insourcing versus outsourcing. It's about which elements become co-managed, guided by how an organisation prioritises the levers, the nature of the co-management and where they are in the journey towards digital transformation – how fast, how to manage risk, who to trust, etc. This requires partners that can grow and adapt with the organisation over time, offering the necessary flexibility and agility while sharing the responsibility to maintain security.



Where are you today? Where do you need to be in the future? Where do you want to place your trust?

	DIY		Co-managed volume		Co-managed value		Fully co-managed
Level of existing investment and resources	High						Low
Previous experience of outsourcing	Bad						Good
Requirement for operational agility	High						Low
Requirement for commercial flexibility	Low						High
Need to maintain control / ownership	High						Low
Requirement for additional expertise (security maturity)	Low						High
	Trust in self						Trust in others

Our future strategy is to use the Eagle-i platform as a modular system to power a flexible hybrid service model

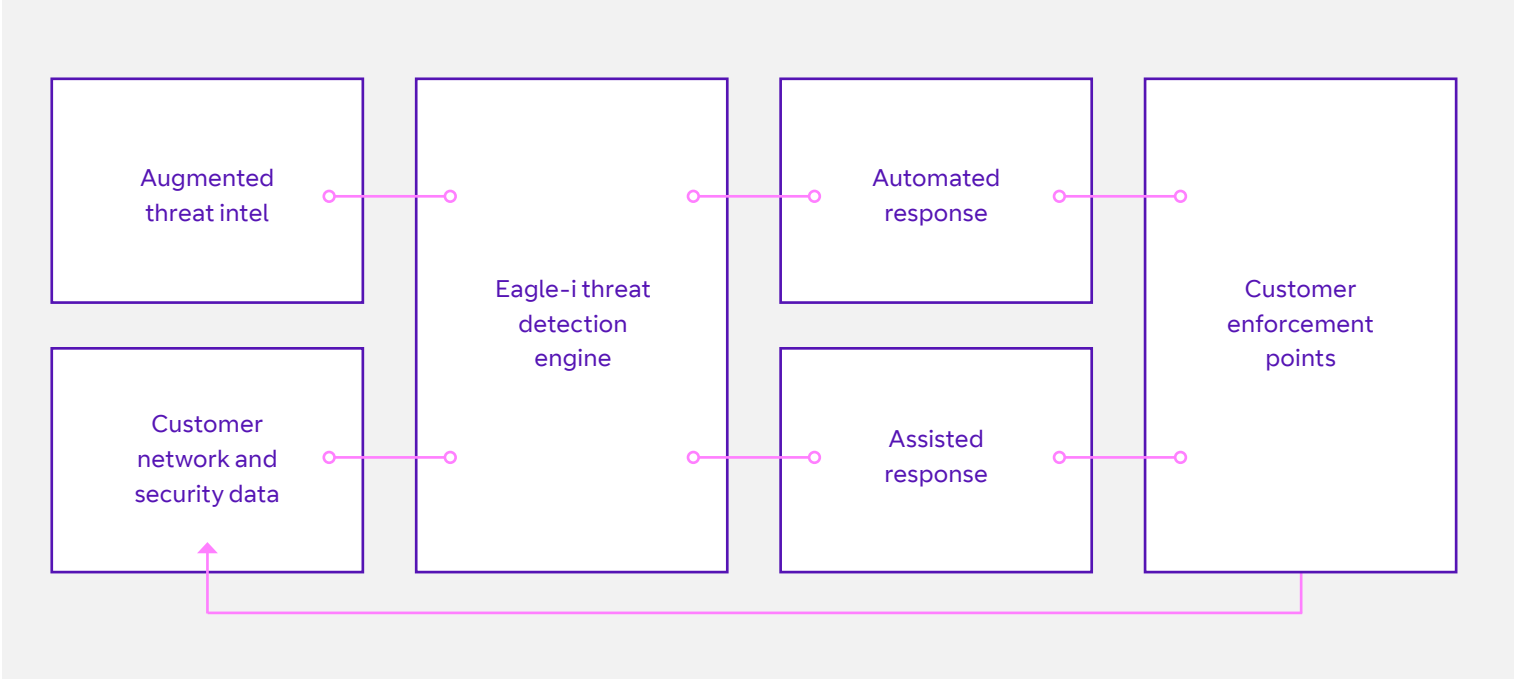
To address the need for a hybrid co-management model, our service levels can be fully or semi-automated via our Eagle-i cybersecurity platform. This platform and wider ecosystem – which includes DigiCo and our other tooling and service capabilities – is made up of best-of-breed partners that we've integrated together into a seamless solution.

Because it's modular and platform-driven by nature, we can design and tune the remediation aspects of our service to a solution that's based on an organisation's priorities, where they are now, their target state and the response state they're in. This can be around specific enforcement points, threat detection and response, or general security of specific parts of the estate.

One specific area that underpins all solutions is our threat intelligence. Our privileged position of carrying a vast amount of the world's network traffic gives us advanced visibility on many threats. We couple this with curated intelligence from hundreds of threat feeds and correlate this information to produce tailored, actionable threat intelligence that's fed into our Eagle-i threat detection engine.

Once threats are identified, how these are managed will depend on the use cases that we identify together as the best starting point to introduce co-management and automation. And our experience of defending our own estate, as well as our customers', is something we'll draw on where appropriate. As trust is built up and the organisation's cyber maturity develops, they can then decide what else to automate, in which context, or to keep a human on the loop for as long as needed.

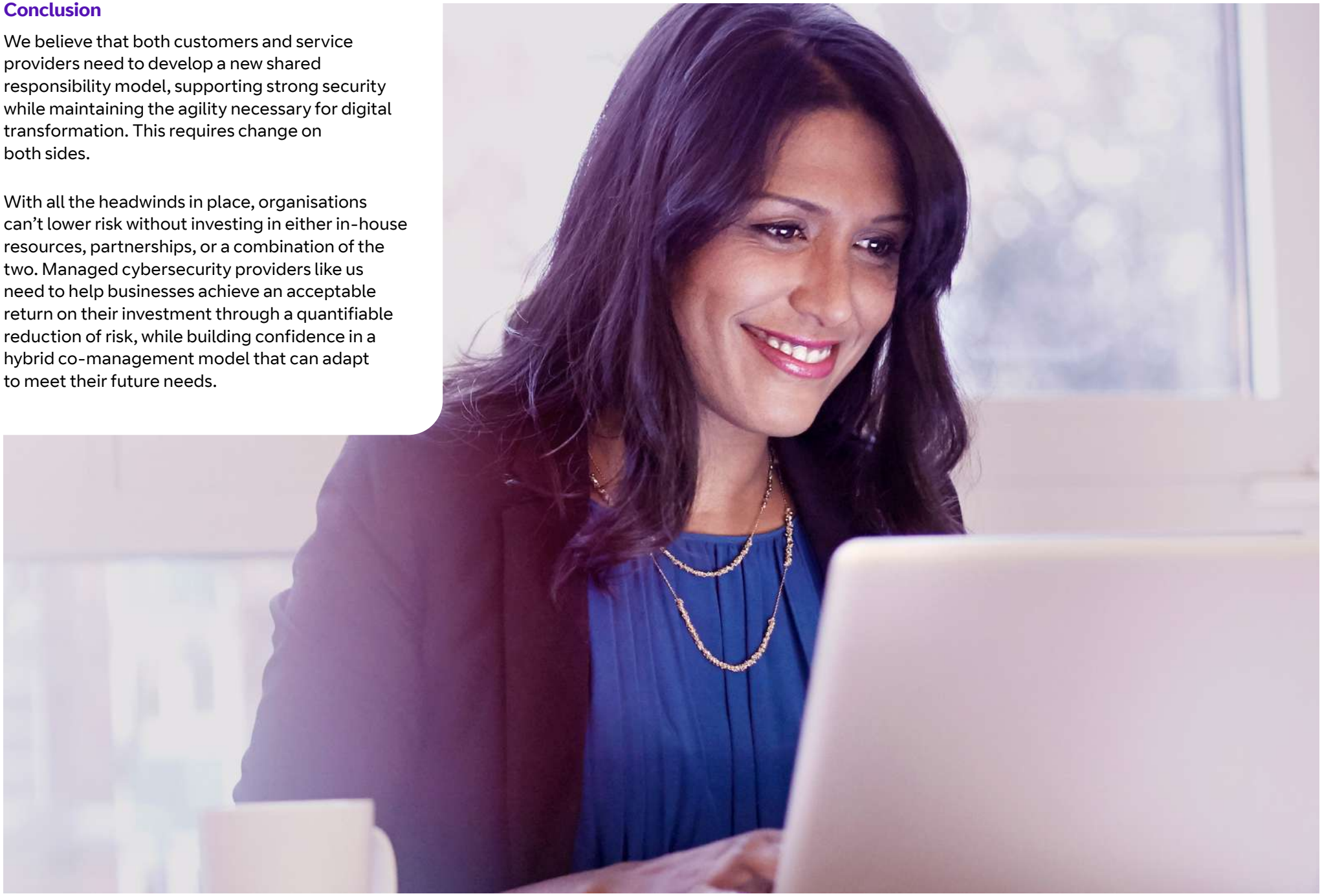
Initial CISO feedback has been positive, particularly around how this provides an opportunity to start small and iterate together as a way to build trust, to work towards a holistic security posture that will reduce vulnerabilities, and to start introducing automation as the only way forward to deal with threat volume.



Conclusion

We believe that both customers and service providers need to develop a new shared responsibility model, supporting strong security while maintaining the agility necessary for digital transformation. This requires change on both sides.

With all the headwinds in place, organisations can't lower risk without investing in either in-house resources, partnerships, or a combination of the two. Managed cybersecurity providers like us need to help businesses achieve an acceptable return on their investment through a quantifiable reduction of risk, while building confidence in a hybrid co-management model that can adapt to meet their future needs.



Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

April 2021