Delivering a collaborative cybersecurity services model for telcos and systems integrators

Rewriting the relationship between DIY and outsourcing for secure digital transformation

The pandemic has generated a threat landscape that continues to become more intense and complex. Three quarters of business leaders say there are more and more security threats every year and we know that email scams, ransomware and brute force attacks have rocketed. Email scams have increased by 600%, ransomware has increased by 100% and there's been a 400% increase in brute force attacks.

In a survey we ran last year, cybersecurity was ranked as the main priority for organisations after managing the consequences of the pandemic. 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 18 months. Along with others in the industry, we've 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.

Five main insights from our 'CISOs under the spotlight' research

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's 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.

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

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.

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.

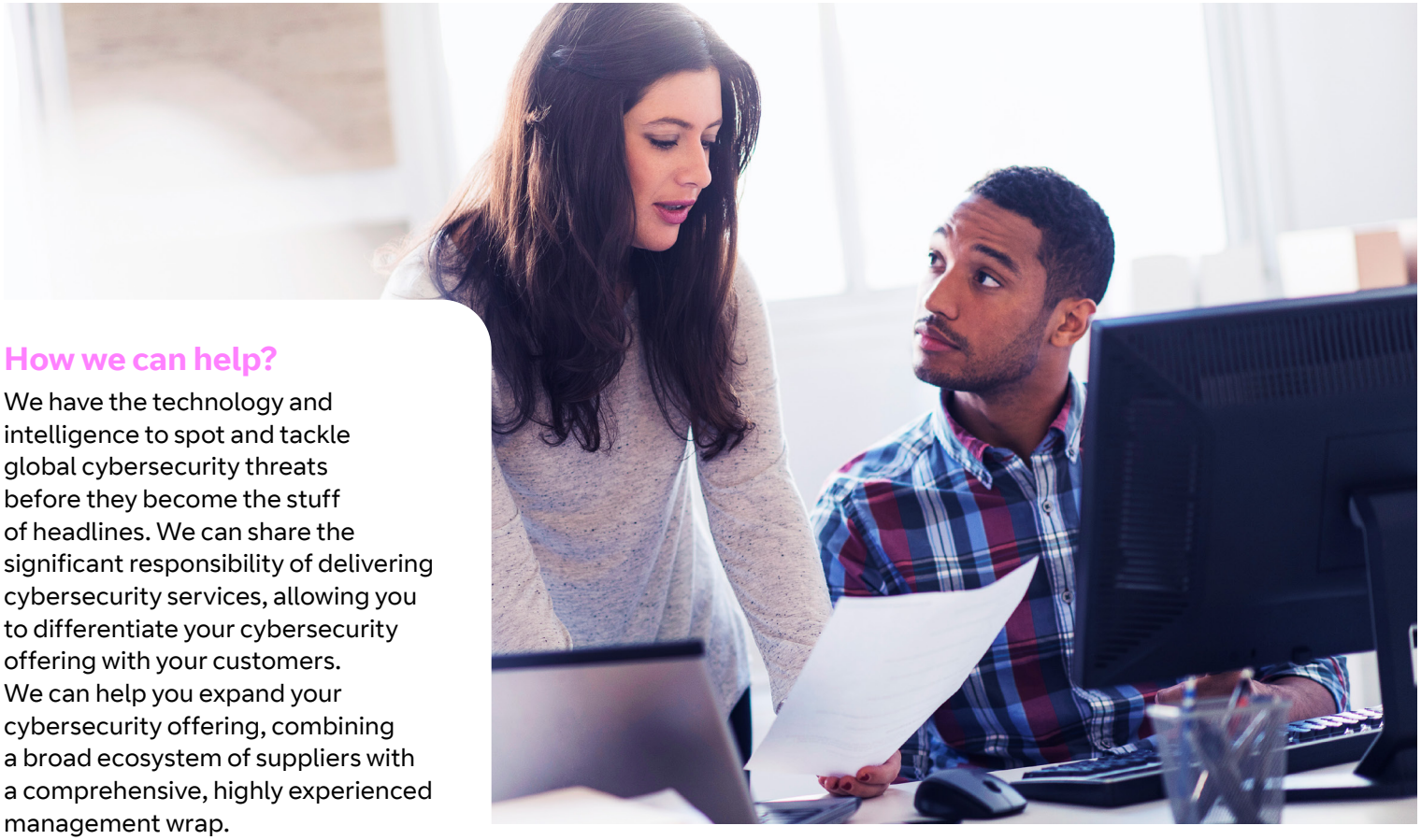
Managing risk is clearly another key consideration, and one that has many moving parts. As we've already discussed, some of the more tactical technology decisions taken during the pandemic, such as engaging new vendors to address a particular need, led to an increase in risk that security teams now need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

Are you ready to help your customers with cybersecurity solutions?

As telecoms resellers or systems integrators your customers are looking to you to provide innovative cybersecurity approaches to futureproof their digital infrastructure across the globe. Delivering on this can be a big ask, as you're likely to be suffering from a cybersecurity skills shortage and finding your in-house expertise is challenged by the sheer range and scope of the cybersecurity landscape. You're also facing lengthy development times to get a product to market. Add to this the complexity of the regulatory environment and, potentially, limited technological capabilities, and keeping your customers secure is a daunting prospect.

Many telecoms resellers and systems integrators are identifying areas where external partners can add value and share the significant responsibility of delivering cybersecurity services. A solid partnership is key because the pace and complexity of cyber threats can't be addressed singlehandedly.



How we can help?

We have the technology and intelligence to spot and tackle global cybersecurity threats before they become the stuff of headlines. We can share the significant responsibility of delivering cybersecurity services, allowing you to differentiate your cybersecurity offering with your customers. We can help you expand your cybersecurity offering, combining a broad ecosystem of suppliers with a comprehensive, highly experienced management wrap.

Why BT for security?

- Over **3,000 global security experts**
- **350 global consultants** supporting customers throughout their cybersecurity journey
- **70 years of expertise** of dealing with major incidents and managing the threat environment
- Operations in more than **180 countries** supporting some of the world's largest companies, nation-states, and critical national infrastructures - giving a unique perspective on cybercrime
- **Two million events** processed per second
- **6,500 potential attacks** identified and analysed every day.

Conclusion

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 can help telecoms resellers and systems integrators achieve an acceptable return on their investment while securing their customers and helping them meet their future needs.

Visit our website for more information or talk to your account manager.

November 2021