Stratia Cyber
CERTIFIED CYBER SECURITY CONSULTANCY

SC Insights Dispersed by design

Six things to consider before adopting a hybrid working model

1. Seize board-level buy-in to secure budget

There's a fine line between tactics and strategy. "Right now, boards are switched on to the issue of cyber security and finally seeing it as a business imperative. If you've got the drive from the top, you get the budget that goes with it and you also get the orders to do it. Those who have faced budget-related issues with reasonable success are the ones who have spotted the opportunity to seize Board-level interest and closed decisions quickly.

"Another route is to focus on tactical improvements that actually contribute towards strategic play. As for smaller companies, it's easier to manage change. And when you've always had a distributed workforce, like ours is, you definitely have to own responsibility for it for yourself. "Ultimately, investment in cyber security has to go up in line with the price points of all the technologies coming down."

43% of workers will stay remote after the pandemic ends, and two-thirds of IT professionals are very concerned with endpoint misuse and security breaches.

https://www.eweek.com/mobile/what-next-gen-networking-brings-to-the-home-table/

2. Out with the fear factor, in with the endpoints

"We've reached a broad level of understanding across the whole business now that while previously you may have had 4000 people working for you in one environment, now you've got 4000 separate endpoints, plus access to devices outside of the office that double or triple that number." Lou urges companies not to neglect the significantly more distributed supply chain they're now dealing with in the employee population alone. One tiny element of any supply chain lacking the type of protection you'd expect from larger organisations could introduce potentially huge vulnerabilities. Hybrid working model or none, attackers only need one way in.

3. What worked in the past may no longer be good enough

According to Lou, bridging this gap is key. “Some organisations can expect to accelerate very quickly, and many may perceive that transforming the way you work in a small company is easier. However, some do really struggle because of the size of the leaps that they have to take to remain competitive.”

4. Take a more holistic view of risk

In the context of the hybrid working model, people and process have probably never been more critical to ensuring cyber security. Adoption of a holistic outlook is essential to achieving each and every aspect of the ideal work-life balance hybrid working promises to enable; and when it comes to taking a more holistic view of risk, this is an advancement that’s been long overdue. Lou Mahanty comments: “It’s not just about technical kit, individual employees have a right to know and understand why various measures are in place (indeed, we see people taking a more proactive interest than ever), and thus what they need to factor into their day to day routines and interactions. Training and awareness levels have undoubtedly been pushed up the priority list in recent times.” Any organisation hoping to enable a smooth and rapid transition to hybrid working should take note.

Dr Bansal adds: “It’s a matter of time until insurers start to mandate cyber security for any organisation seeking indemnity; and if you’re a startup in the technology space, you’ll be in the high risk category. What measures will you take to get indemnified?

"We’ve been through this process with Stratia Cyber’s support to prove that our technology has been penetration tested, and that the necessary firewalls are in place. So you’re either investing in the security of your business, or you’re paying the price anyway with higher insurance premiums.”

5. Calculate the cost of downtime

"If you're wondering where to begin with cyber security, simply imagine you're running the business. One of the first things you'd consider is how you can reduce your vulnerabilities." Lou explains why downsizing office real estate on a permanent basis is a change that's also encouraging senior management and leaders to ask themselves why certain things need to be done in a certain way; in his mind, another positive shift away from perfunctory activity that is likely riddled with inefficiency.

> **"If you don't have access to your systems and two days go by in trying to manage an attack or a breach, what does that mean for your business in terms of revenue loss? High profile breaches that first hit the headlines years back still have a running total of costs incurred."**
>
> **Dr Bansal, CEO and founder, Medic Bleep**

Budgets for cyber security must equate to a sensible reflection of total impact, overall value, and potential loss.

6. Don't wait until it's too late

Human health is not a new analogy in cyber security, and yet it's true; in the same way it's very easy to neglect our health until a real problem surfaces, many organisations struggle to fully embed a culture in which prevention is considered better than the cure. When momentum is high, taking steps to protect ourselves in the long-term fall way down the list – living in the moment is much more exciting. And throughout the isolated circumstances many have found themselves in due to the pandemic, a large majority of the population has, largely unconsciously, opted for the fasttrack to burnout. The same applies to any business that hasn't seriously considered its cyber security risks and responsibilities; carrying on until you start to fall apart can often mean it's too late to reverse the damage.

Dr Bansal explains: "Cyber security is just so abstract, and that is half of the problem. In healthcare the iceberg phenomenon is commonly used, for example, let's say 10% of people have diabetes - figures and calculations are reported based on what we can actually see - but that doesn't mean to say that beneath the surface, there's not another 90% that aren't visible who are about to become diabetic. The same goes for cyber attacks, which in many cases go unnoticed for weeks and months until some server bill comes in at 10x what you were expecting. In both scenarios, spotting the signs too late will seriously minimise your ability to recover to full health."

This bitesize download forms part of SC Insights | Dispersed by design. The full report compiles a rich compilation of firsthand insights, generously contributed by Stratia Cyber and client organisation, Medic Bleep (Medic Creations). It has been designed to facilitate cyber security decision making as your organisation progresses with the implementation of the hybrid working model.

Lou Mahanty, Managing Director at Stratia Cyber explains that long before the pandemic, their company culture continued to grow and strengthen very organically despite having always operated as a remote team.

Dr Sandeep Bansal, CEO and founder of Medic Creations, shares his firsthand experience of living and working through the shifts driven by the global events of the last year.

About Stratia Cyber

Stratia Cyber is a founding National Cyber Security Centre (NCSC) Certified Cyber Security Consultancy (read press release here) and has some of the most experienced and respected security consultants in the United Kingdom. Stratia Cyber remains certified under the scheme to provide Risk Management, Risk Assessment and Security Architecture.

Stratia Cyber is an independent cyber security consultancy with a track record in providing Cyber Security services for Commerce and Government, including Defence. Founded in 2011 as Stratia Consulting, Stratia Cyber boasts a management team of senior security consultants with collective cyber security experience of more than 90 years, gained in the public and critical national infrastructure sectors. For a complete view of Stratia Cyber's Accreditations and Frameworks, visit https://stratiacyber.com/Accreditations

SUBSCRIBE SC INSIGHTS

FOLLOW STRATIA CYBER

TALK TO A CONSULTANT

Stratia Cyber
CERTIFIED CYBER SECURITY CONSULTANCY

ten years
of creating safe environments for our customers

2011 | 2021