Stratia Cyber
CERTIFIED CYBER SECURITY CONSULTANCY

SC Insights Dispersed by design

Accelerated adoption of hybrid working models post-pandemic and the opportunity for cyber security functions

Cyber security functions everywhere found their worlds turned upside down overnight when in spring 2020, Covid-19 forced organisations to migrate to a dispersed way of working without warning. More than a year on from when disaster first hit, we find ourselves in a time when planning for the long-term feels a long way off, and yet change is surely the only constant. Many feel ready to return to the office, at least part of the time. So what does this mean for the team who has only just kept its head above water until now?

This 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.

STRATIA CYBER is assured by the National Cyber Security Centre to deliver cyber security services. This year the consultancy celebrates 10 years in business, and has assured mission critical systems for Government bodies and commercial businesses across the UK and internationally.

Ten years of growth as a dispersed team

Perception of cyber risk indeed varies across sectors when asked to reflect on the pre-coronavirus era versus the times we now find ourselves in. One thing is clear that growth for new businesses in particular in the cyber security industry is not just high, it's also relatively stable.

This year Stratia Cyber celebrates 10 years in business as a dispersed team. While many cyber security vendors and consultancies launch on an opportunistic basis, Stratia Cyber was established when the team was not only in pursuit of growth, but when they were ready for it.

"Trust is repaid with good performance."
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.

KPMG insights on Redesigning the Future of Work describe our New Reality as an opportunity – offering employees greater flexibility is seen as a positive – but also a challenge – firms have concerns over diminished team building and a dilution of culture due to decentralised working.

Lou says: "Of course we recognise that in-person interactions will always be fundamental to some elements of running a business." But at its core, trust is the key to success for this NCSC-accredited cyber security consultancy. "Trust is part of our mission; trust in what we do to make safe environments in which businesses can thrive, we have no option to fail because our clients are trusting us with their ability to survive. But it's also distinct from our values and in many ways also separate from our mission. And in our experience, trusting our people has been repaid with good performance, and this kind of culture is absolutely responsible for our decade o growth."

Challenge statement

What is the hybrid working model?

A term we've all become familiar with very quickly, hybrid working is a model that aims to create 'a workplace that is a moveable feast for normal and power users alike'. Having had our fill of what it's like to work from home for the past year, organisations and colleagues are now demanding freedom to work from anywhere on a phone or laptop that is safe, reliable and efficient.

Others define the hybrid working model as based on the idea that an employee's physical presence in the office isn't always necessary for work to be carried out, designating certain days for in-office work and other days for remote work that requires individual focus.

> **"Depending on the type and size of the company, this can just be business as usual. However for some, it's transformational."**
>
> **Lou Mahanty, Managing Director, Stratia Cyber**

According to reports, 76% of companies adopted cloud services faster than they had planned in the last 12 months. Unsurprisingly, the sudden change in circumstances for society has resulted in rapid acceleration of digital transformation. Three quarters of organisations were forced to respond to the pandemic in this way. But let's consider what this means for people and processes.

"People are much more effective if they are comfortable in their workspace, wherever that happens to be. We should be much more malleable in our approach. Hybrid working models represent being socially distanced, while remaining connected. Some people can cope with it, some people can't, and those who can't need to know that they can seek support from the mothership – the function that's making sure the workforce remains one whole and maintains productivity. However, this kind of pastoral care has traditionally not been built into the way corporations do business."

The hybrid workforce will only add intricacy to security and IT operations. In many scenarios, workers are moving between secure office environments with enterprise network monitoring, firewalls, event and data analytics, to vulnerable home networks that might have rogue devices, weak passwords or outdated equipment.

An 80% increase in cybercrime in 2020 has made building robust cyber security resilience even more critical

https://www.eweek.com/mobile/what-next-gen-networking-brings-to-the-home-table/
https://www.isc2.org/resource-center/reports/2020-cloud-security-report

i. Remote working policies rise to the challenge

Was it standard to have a remote working policy in the past? As we look ahead, now is the time to capitalise on existing cyber security policies to ensure remote and hybrid working can be sustained long-term without increasing cyber risk.

“This is probably a once only opportunity as businesses are currently thinking about how they change the way they operate to become secure by design.

"Now is the time to leverage appetite to design safe practices so that looking after the health of the business becomes easier. Now is the time to insinuate that if you want to be everlasting, and you want to be easily able to adapt to new security situations, you need to make the decisions now that are right for your specific organisation."

"You’ve got this window, and you can and should use it."

LOU MAHANTY
STRATIA CYBER

ii. Dispersed by design

Dr Sandeep Bansal is CEO and founder of Medic Creations, and began working with Stratia Cyber before Covid-19 became a reality. “We’re a technology-led startup; our company setup included a remote working policy from the get go, allowing us to work from home if we needed or wanted to. We’re a critical system servicing hospitals and healthcare, so our team has always needed to react very fast and to be able to access the servers and the technology from the engineering side, from wherever they happened to be.”

Looking more closely at the healthcare industry, Dr Bansal explains that not only was the NHS never before set up for mobile working, mobile device policies for using personal devices were mostly not in place. “Over the last year this has had to have been thought about very rapidly, and healthcare trusts have been forced to look at MDM (mobile device management) solutions, and of course the cyber security elements associated with that.”

“The cyber threat isn’t going anywhere. Working with healthcare data, we understand its potential value and we simply can’t go down. Stratia Cyber has helped us to understand where our gaps were, and what we can do to build up the existing security measures we do have in place. On the product side, they’ve helped us with penetration testing, and reassessed us once we’ve made some changes. The assessment process is a continual cycle. I anticipate that Medic Creations and Stratia Cyber will be working much, much more closely in the future to meet the need to constantly tighten up our security.”

Opportunity for cyber security functions everywhere

So how should organisations weigh up this enhanced desire for work-life balance with their fundamental necessity to responsibly protect information assets? It wouldn't be unfounded to predict that the gap will widen, in the short term at least. Lou Mahanty reflects on whether the risk that the gap between what the business wants to do, and security enabling it to happen, is really one for concern.

i. Break it down

"For organisations whose main interest is migrating to the cloud, the starting point is to understand what represents their most valuable information. Many haven't already done this, and many have great difficulty because they lack the sort of structure that features data or information owners. And the bigger the organisation, the more political these things become. So partitioning off key bits of data and information is critical; the smaller you break it down, the easier it is to look at security. But it's not a quick process."

> **"The starting point for migrating to the cloud is to understand what represents your most valuable information. Many organisations have great difficulty doing this because they lack the sort of structure that identifies information owners."**
>
> **Lou Mahanty, Managing Director, Stratia Cyber**

ii. Don't provide a poor second

"For individuals, you've got a whole different set of issues, from kids or housemates to no dedicated workspace at home, to living in an area with poor WiFi. Each group of individuals have very specific issues that must be addressed, and there's no simple or fast solution for that. We've also seen distance and remoteness affect the younger generation much more than the more mature workforce, who have already been through the period when you need to be surrounded by people.

"I think the worst case hybrid scenario would be to replace your main place of work where you meet and develop relationships with people, with gravitating to temporary offices that offer little more than a different place to sit. Without the company interaction, a space to get a coffee is enriching to a very limited extent. The worst thing you can do is provide a poor second."

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."

Client lens

Firsthand insights from a health tech startup

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.

Putting policy into practice

Making sure the team understood the policies and processes relating to handling sensitive data that we had in place back when our working patterns first felt the impact of Covid-19 was our number one priority. We worked with Stratia Cyber to implement Cyber Essentials Plus and ISO 27001, as well as pen testing our solution, Medic Bleep.

Communication, really good communication

Surviving the pandemic was one thing; thriving despite it comes down to really good communication. When we got rid of our physical office space, we increased the frequency of team meetings initially to once a week. We only introduced town hall style meetings for the entire team to be present and focus on what we can do better after making the decision to become a fully dispersed team. And day to day, Slack provides a lifeline, especially for the engineering team who is most likely to struggle as a result of poor communication across the business.

Stratia Cyber MD, Lou, echoes Dr Bansal's views on regular team interactions and get-togethers.

"We have a heartbeat of regular meetings as well as all hands calls for everyone to attend and to keep up to date with what others are doing." For them, the advent of Zoom was not revolutionary maintaining dialogue with individuals.

Lou explains that right now the consultancy is introducing data rooms to make it easier for people to liaise on topics, particularly those who need technical support.

No one has complete immunity

We've really tightened our email security; during the pandemic, scams targeting the healthcare sector have spread faster than the virus itself. Global panic and anxiety create the perfect conditions for fraud, and in May 2021 statistical market research estimated the Global Healthcare Fraud Detection Market is expected to reach US$ 6.9 billion by 2027.

In March 2020, I actually got caught out. Since then our focus has been unmoved to ensure that doesn't happen again. Thankfully, the incident was contained and the impact was low, but this kind of threat comes with a huge knock-on effect for our customers, and anyone else we're working with. As more IOT (Internet of Things) devices come into play and the popularity of new technologies like virtual reality and 5G grows, so does the level of risk. We intend to continue to work very closely with Stratia Cyber to make sure that we're adhering to best practices.

In March 2020, I actually got caught out by an email scam. Since then our focus has been unmoved to ensure that doesn't happen again.

Dr Bansal, CEO and founder, Medic Bleep

Protect yourself, not just your product

Since I was targeted with an attack that succeeded in duping me, it's definitely made the entire organisation a lot more aware of the real risk. Until then we'd been focusing so much on our product, and the security of the product, that we'd not fully recognised that there's a whole lot more that applies to the company itself. Your product might not go down or even be affected by a cyber attack, but if you can't get into your emails, you can't function as a business. It's not just the product that needs protection, it's the entire company and end-to-end solution, right from somebody touching our website, all the way through to the delivery of our service.

We have the necessary security protocols in place, but we've definitely seen a rise in attacks on our server, and we know firsthand that people have tried to DDoS (Distributed Denial of Service) Medic Bleep in the last year.

https://healthitsecurity.com/news/report-rise-in-covid-19-vaccine-social-engineering-bec-phishing
https://www.prnewswire.com/in/news-releases/healthcare-fraud-detection-market-to-reach-us-6-9-billion-by-2027-globally-cagr-25-3-univdatos-market-insights-881508062.html

What are the key learnings?

Google 'cyber security and hybrid working models' and its widely documented, or perhaps assumed, that key decision-makers are in the throes of currently upgrading their networks. Meanwhile new technologies dedicated to facilitating a marked change to the way the world has traditionally done business, are, of course, emerging.

But if a cyber security consultancy with 10 years of remote working can teach us anything, it's that the cyber security challenges organisations face now perhaps don't demand the technology that the hype suggests.

Dr Bansal reflects: "In the healthcare world, we obviously understand the pros and cons of drugs before prescribing something. We run clinical trials, and everything has a good side and a bad side to it. It might not make sense for the business to go for these emerging solutions at this point in time, and not unlike an individual patient, this is something that needs to be assessed on a case by case basis."

"The healthcare sector has typically been pretty poor at implementing change, so you can give it all the technology, but if you don't change the processes around it, and understand the technology, there's no point.

"You can't just go ahead and parachute in technology without understanding those fundamentals. And, obviously, you need to get your organisation onside if it makes a material impact on how they might work."

The coming hybrid workplace is just one more development that will test the imaginations of security professionals. It's not too early to address the challenges presented by this complex combination of people, places and devices.

SECURITY IMPLICATIONS OF A HYBRID WORKPLACE, SECURITYMAGAZINE.COM

Lou concludes that this has very little to do with solutions. "Many think no one understands yet because this feels like a totally new way of working. Stratia Cyber has been used to working remotely, but we've never been an organisation in which we've learned about working together in one place, so our start point is very different. For many companies now planning to roll out hybrid working models post-pandemic, business life and their interactions in a pre-Covid19 world were very different to the ones we've had. Even though we've always been moving in the same direction, our points of attack were historically quite different."

People, process, technology

"It will always be a people, process, technology thing. And decision-makers should not feel it compulsory to follow a particular technology route, when what may be needed is in fact just a little process. That could look like training a couple of people up, or looking more closely at the subject matter."

Before the temptation prevails to leap aboard the technology bandwagon to address the shifting cyber security environment in the world of hybrid working, focus first on your essentials. The likelihood is that many of the fundamentals that you'll need to adapt, and to manage this transition are there already. Implementing yet more new technology too soon should come with a caution. The risk? It will only increase.

Introducing new technology that demands new and different behaviours from the people using it only serves to further increase your attack surface, far beyond the technical vulnerabilities that will inevitably arise and be exploited during these early days.

About Stratia Cyber

Stratia Cyber is a founding National Cyber Security Centre (NCSC) Certified Cyber Security Consultancy and has some of the most experienced and respected security consultants in the United Kingdom. Stratia Cyber remains certified under the scheme to provide three areas of service:

- Risk Management
- Risk Assessment
- 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