Cyber Security Experts From Stratia Cyber Discuss The Future of Remote Working

Submitted by: Stratia Cyber
Friday, 25 June 2021

As businesses begin to re-open offices while retaining a portion of the flexibility that employees have enjoyed, many of us are looking to discuss hybrid working models and how these may work in practice.

Stratia Cyber - an independent cyber security consultancy who provide services for Commerce and Government, including Defence, are celebrating 10 years as a dispersed team and have grown and strengthened their business by working remotely even pre-pandemic. Their team of leading cyber security consultants are available for expert comments and able to offer their expertise via telephone, email or Zoom interview.

- For more information contact Scarlett at Stratia Cyber's press office - stratiacyber@scarlettlondon.com -

The Future of Hybrid Working

How can businesses create a connected, safe & supportive hybrid working model?

Businesses 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 an emerging new ‘hybrid working’ model?

Lou Mahanty, is the managing director of Stratia Cyber and former Director of Intelligence at CSC where he commanded a large supply chain regiment.

“People are much more effective if they are comfortable in their workspace, wherever that happens to be therefore 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.”

“This is probably a once in a lifetime 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. Larger and the most switched-on businesses will be looking at that.”

In addition to a pastoral care re-think, the hybrid workforce will also 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.

“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. 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.”

Case Study: Medic Creations

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 so our set-up included a remote working policy from the get go, allowing us to work from home if we needed or wanted to. 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. 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.”

Notes to editors:
Stratia Cyber is an independent cyber security consultancy with a track record in providing Cyber Security services for Commerce, and Government including Defence. It is one of the first companies to be successfully assessed and accredited under the National Cyber Security Centre (NCSC) Certified Cyber Security Scheme and is a CREST Accredited Company.

Paul Maxwell, Founding Director, Stratia Cyber

Paul is a founding Director of Stratia Cyber and an experienced Risk Management and Security Architect, with excellent technical, communication and leadership skills. He is highly respected by his previous and current clients and enjoys working closely with demanding customers to deliver mutually beneficial outcomes. He has extensive experience working on Government and Commercial systems.

Paul has built up his consultancy experience since leaving his role as a Sensors engineer in the Royal Navy and has carried out roles as diverse as the Operational and Computer Network Defence Manager for MOD DII systems, Lead Security Architect at HM Coastguard, Desktop Accreditor for Top Secret systems to the Security Assurance Manager for GCHQ. His most recent MOD deployment was as Lead Security Architect for the service provider that delivers the MOD’s pay and pension systems for Defence Business Services.

Paul is a CCSC Head Consultant and is a Lead CESG Certified Professional Security and Information Risk Advisor, a Certified IT Professional member of the British Computer Society, a Certified Information Systems Auditor and a member of the Institute of System Engineers. Paul is also a ISC2 Certified Cloud Security Professional CCSP.

Lou Mahanty, Managing Director, Stratia Cyber

Lou Mahanty has been Managing Director of Stratia Cyber, a NCSC accredited cyber resilience business, since April 2017. Previously he was Director for Intelligence UK at CSC where he led a team of 400 specialists providing secure IT infrastructure managed services to Government. Lou is a graduate of Leeds University (BSc Hons Physiology), Kings College London (MSc Physiology), the Open University (MBA) and the Army Staff College.

Lou's experience includes 17 years in the British Army, and 21 years in delivery and leadership roles. In military service, he was a soldier foremost but also at the cutting edge of several change initiatives that were new both to him and the Army; for example: the formation of Agencies as new business vehicles, measurement of defence output and its modelling, Market Testing, and the move to resource based accounting. He commanded a large strong supply chain unit.

With Capgemini he was one of a small team which grew the Aerospace business from £5m to over £50m t/o in the space of 24 months mainly through transformational IT programmes such as the Defence Electronic Commerce Service and a programme to introduce BaaN into a government repair organisation. At Luminova, a 3D virtual reality and visualisation consultancy, he delivered novel changes to decision-making in aerospace and security industries. With Serco he developed the Enterprise Architecture advisory thrust into Government before joining CSC in 2008 where he delivered further IT driven transformation in classified and complex arenas.