
Managed Security Service Forum 2019
nccgroup
Staying Ahead of the Hype-Cycle &
Effectively Harness MSS Security Technology
Making the world safer and more secure
v1.0

About NCC Group – Global Cyber Security Presence

NCC Group operates globally, with offices spread across the world. The group has particular presence in Northern America, UK & Europe and Asia Pacific. The Map below indicates where the NCC Group office locations are around the world.

United Kingdom
- Manchester (HQ)
- London
- Cambridge
- Cheltenham
- Edinburgh
- Glasgow
- Leatherhead
- Leeds
- Milton Keynes
- Reading
- Slough

35,000+
Clients Globally

2,000+
Colleagues Globally

United States & Canada
- Atlanta, GA
- Austin, TX
- Boston, MA
- Campbell, CA
- Chicago, IL
- New York, NY
- San Francisco, CA
- Seattle, WA
- Sunnyvale, CA
- Toronto, ON
- Kitchener, ON

Europe
- Denmark
- Germany
- Lithuania
- Spain
- Switzerland
- Netherlands (Amsterdam)
- Netherlands (Delft)
- Netherlands (The Hague)

Asia Pacific
- Sydney
- Singapore
- UAE (Dubai)

35
Offices across North America, Europe Asia-Pac & Middle East

nccgroup

To deliver and be recognised as world class for 24/7 managed security solutions that prevent, detect and respond to cyber-attacks and form part of a wider Cyber Security capability that NCC Group has to offer in the cyber market space.

NCC Group MSS Highlights

Devices Monitored Across 80 Countries
The NCC Group UK SOC monitors over 5,000 security devices across more than 80 countries on 5 continents.

Over 130 Million Events Processed
The NCC Group UK SOC processes over 130 million events per day correlating to approximately 200 actionable events per day.

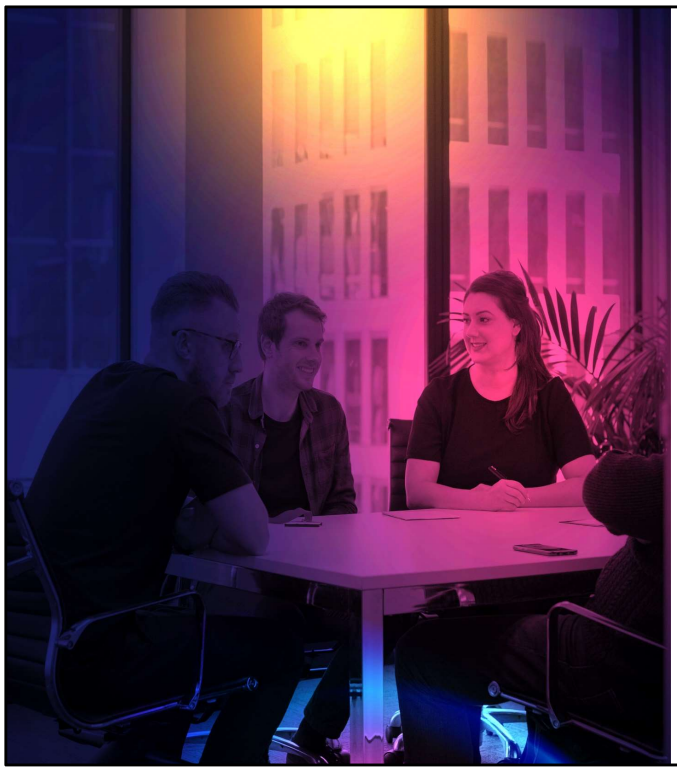
ISO 27001:2013 Certification
The NCC Group UK SOC operates under the ISO 27001 standard for Information Security with our service management aligned to ITIL.
Certificate Number LRQ 0963077/B

45+ Experienced Security Analysts
The NCC Group UK SOC has over 45 experienced Security Analysts all whom are Security Cleared, with over 100 Security Analysts within the group.

Crest Certified SOC
The NCC Group UK SOC was the second SOC in the world to be accredited by CREST

24x7x365 GLOBAL Operation
The NCC Group UK SOC Operates - UK, Netherlands and Australia
24/7 365 days a year.

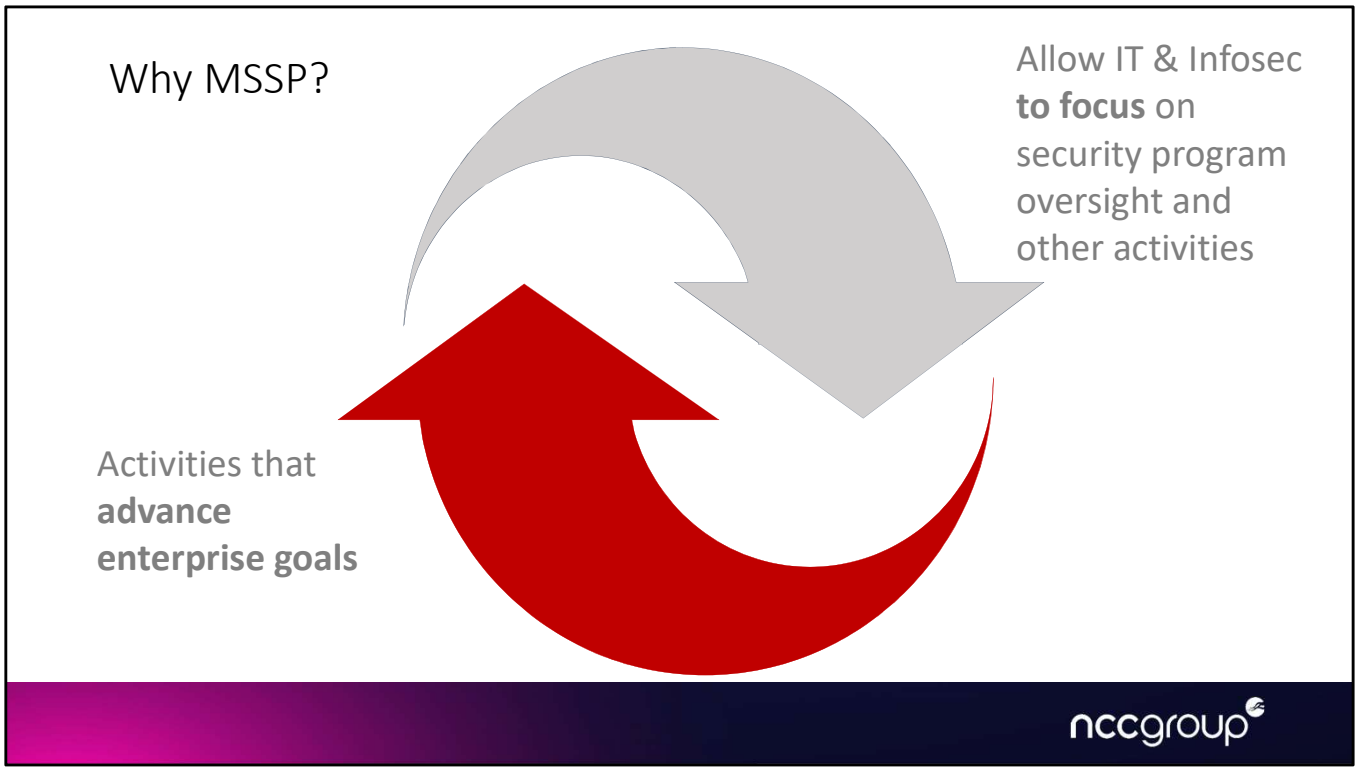
nccgroup



Agenda

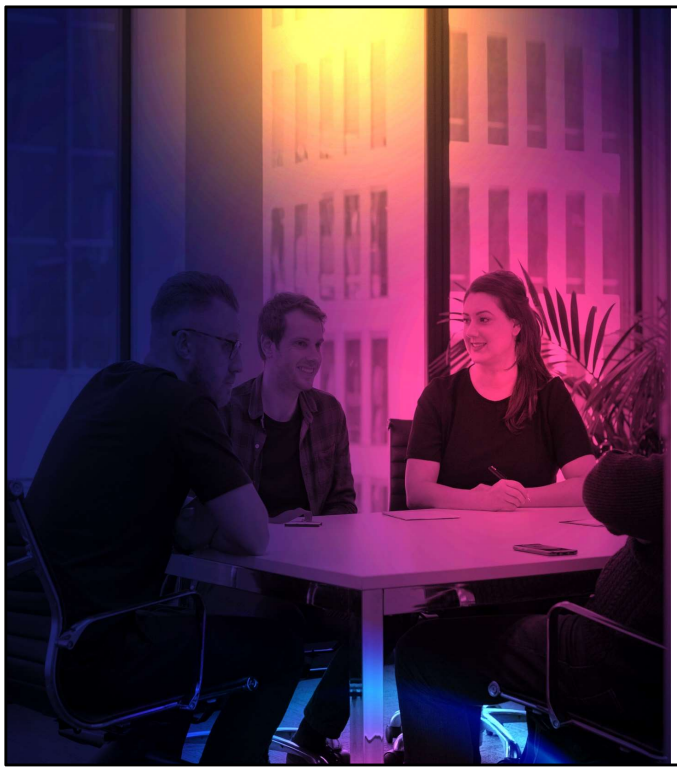
- Context – It's a new World
- Peel back the marketing hype
  - What to look for
  - MSSP & MSP's
- New Operating Models
- Q&A

nccgroup



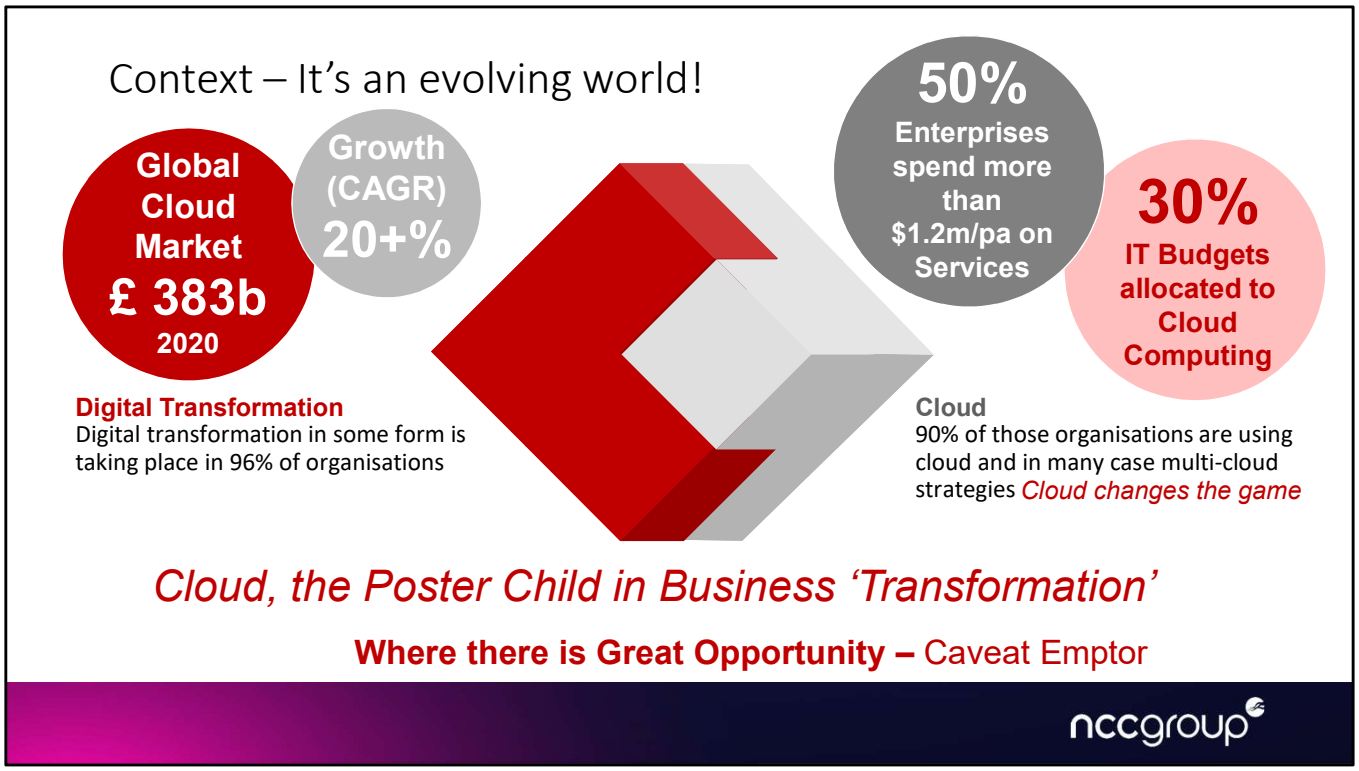
The primary benefit of managed security services is the security expertise and additional resources they provide, to reduce an organisations risk and exposure.

There are a wide range of security services being offered by MSSPs today, the focus of this presentation are the more integrated full stack service providers who deliver Security Operations Centre capabilities and complementary response and specialist warp around services rather than the point solution end of the market.



Context – It's a new World

nccgroup



Stats Ref (Note: Dollar conversion rate used 1.3):

- Cloud Security an annual growth rate of 28% over the next five years (Forrester 2018)
- The global cloud security market is expected to garner $8.9 billion by 2020 (Allied Market Research)
- Private Cloud Market $262b (£202) CAGR 29.2%(Wikibon 2018)
- Public Cloud Market $278b (£213) (Gartner September 2018)
- IDC's figures show growth CAGR 21.5% in 2020. https://www.cloudpro.co.uk/saas/6646/gartner-and-idc-think-saas-and-iaas-will-be-growth-leaders-up-to-2020
- CISCO 2019 - Worldwide SMBs are projected to grow their spending on remote managed security to an estimated $21.2 billion by 2021, making it the highest growth area in the managed services market.

With digital transformation in some form taking place in 96% of organisations and 90% of those using cloud, the inevitable complexity of those environments become a barrier to implementing proper data security measures.

Now multiply up digital transformation complexity with an increased number and sophistication of attacks, organisations are heading for a perfect storm without an NCC in their corner.

Security organizations fail to evolve their structure and how they operate to support corporate goals need MSS in their corner.

The times have changed, with 66% of organisations bypassing IT when buying new technologies for digital transformation, yet still holding IT accountable when programmes fail!

Why are organizations failing to meet their digital transformation security goals?

- They are NOT all executing properly or optimizing the allocation and use of resources in managing digital economy cyber-related risks.
- Action – Achieve a greater level of integration between security functions and the business (Investment in better internal and external partnerships)
- Goal – To realise their business outcomes faster and more securely, in real-time

Cloud Re-sets security *(& trust)*

- **Threat Profile / Evolution** – Do you know what yours is in the Cloud? Cyber attacks evolve at an incredibly fast pace
- **Skill Deficit** – Do you have the internal expertise
- **Discipline** – Cloud = change, its evergreen
- **Economics** – Viability of proportionality & currency (future proofing)
- **Vendor Capability/Credibility** – Trust challenged by complacency, supply chain depth.

Cybersecurity is the new business operating model

nccgroup

With today's attacks becoming more sophisticated, the days of securing ourselves and our customers through a tools-based model (endpoint and firewall protection, email security/backup, and DNS) are not enough.

We need to recalibrate our customer's mindset, we need to be able to speak a common language about how the threat landscape has changed, and what has worked for years, won't work in the future.

Leading Managed Service Providers (MSPs) must use the best technologies and equipment on the market to deliver services. IT services are constantly upgraded with no additional cost or financial risk to customers. No worry that your Managed IT Services will become obsolete.

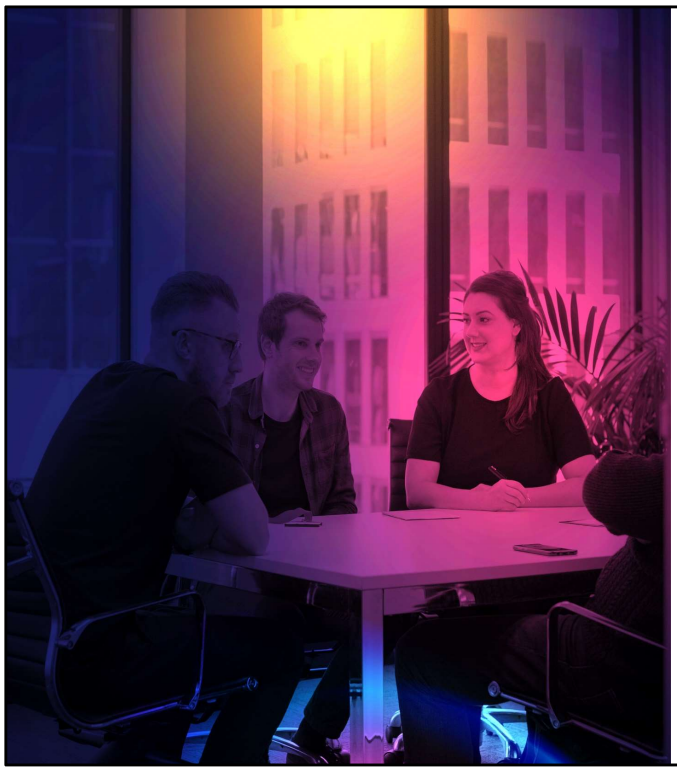
MSSP have challenges themselves which are good to have some insights into as this helps guide questioning and awareness of what is being offered:

- Due to the pace of change and dynamism of the threat landscape mixed with business end user agility, amongst other things, MSSP's find it difficult to provide the right services at the right time and for the right cost.
- Scalability, automation, internal processes and professional expertise are often cited as the most significant technical issues. Cloud has helped but is not a

panacea as many solutions and IP investments require significant re-engineering to fully leverage Cloud.

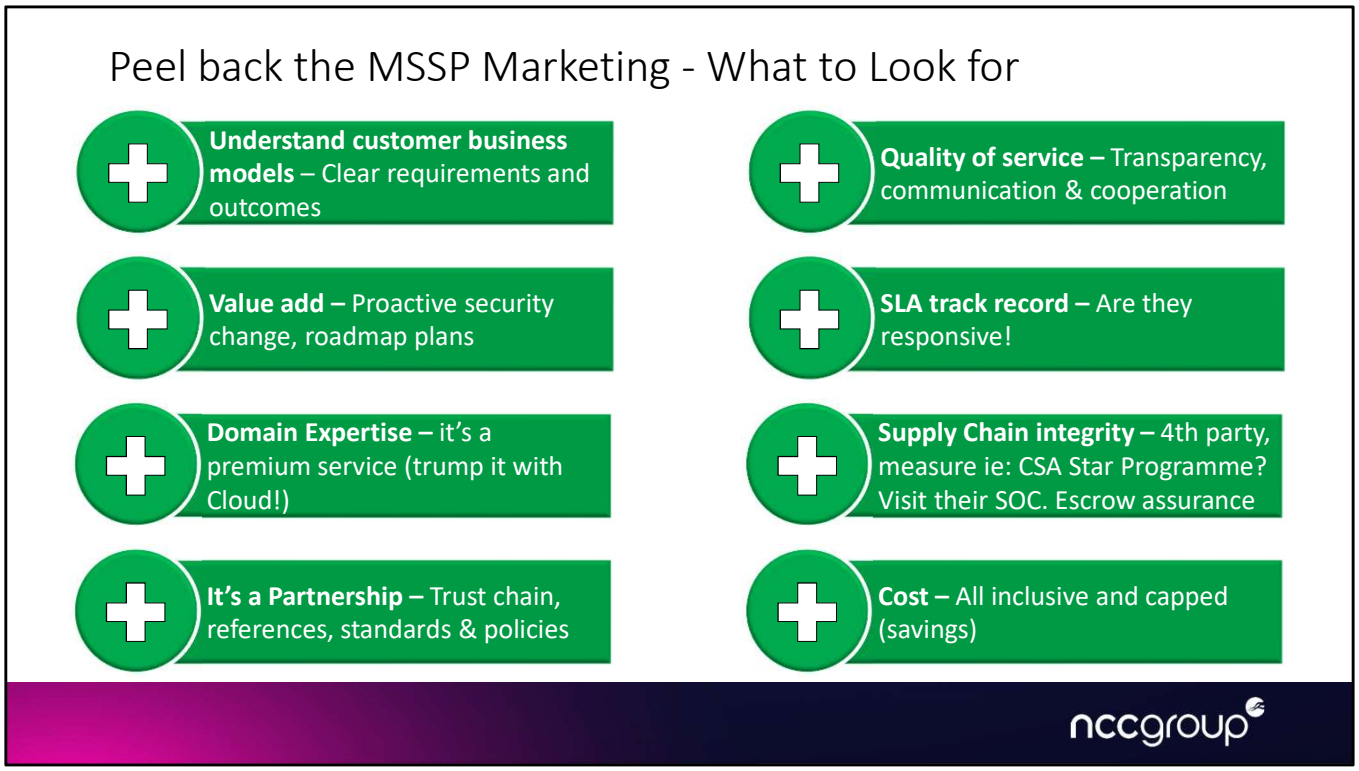
Quote -“You cannot run a successful managed services business by trying to leverage off-the-shelf, prepackaged security technologies," said Jason Hilling, manager of platform solutions for IBM's Global Technology Services division in Atlanta.

- Security tools are often custom software products, relying on experienced security professionals to develop meaningful rules and analytical behaviours for the software. Skills demand is creating disruption and quality consistency.
- New regulations are emerging and existing regulations are changing is a double edged sword. Compliance offers opportunity but also challenges.
- Cloud has exacerbated the constant margin and pricing pressure. With pressure on a provider to maintain a competitive menu of services and offer additional security features without a significant price increase.
- On boarding clients requires flawless execution on a very complicated list of tasks that do represent risk to network uptime and availability.



Peeling back the Hype

nccgroup



Not all MSSP's are born equal and the perceived attraction of Security and Compliance market demand is seeing VARs entering the managed service business thinking it will increase their margins, without realizing the level of resources and skill levels required to efficiently manage more than a handful of clients, due to an unrealistic perspective on investment required.

CompTIA's annual Trends in Managed Services report suggests that MSP adoption is surprisingly low among IT professionals and business users. According to the study, roughly only 30% of organizations use any form of managed IT services.

Justification - IT and security is regarded as important a core function as sales, marketing and accounting. This is keeping many from reaching out to MSP's, yet many fail to realize they're in desperate need of a managed solution in the face of the rapid pace of change and threat landscape dynamics.

Cost - Today's enterprise is digitally aware and rightfully cost conscious. Managed services represent yet another chunk out of the budget. BUT the CompTIA report found that cost savings/ROI has declined in priority in the face of service quality demand.

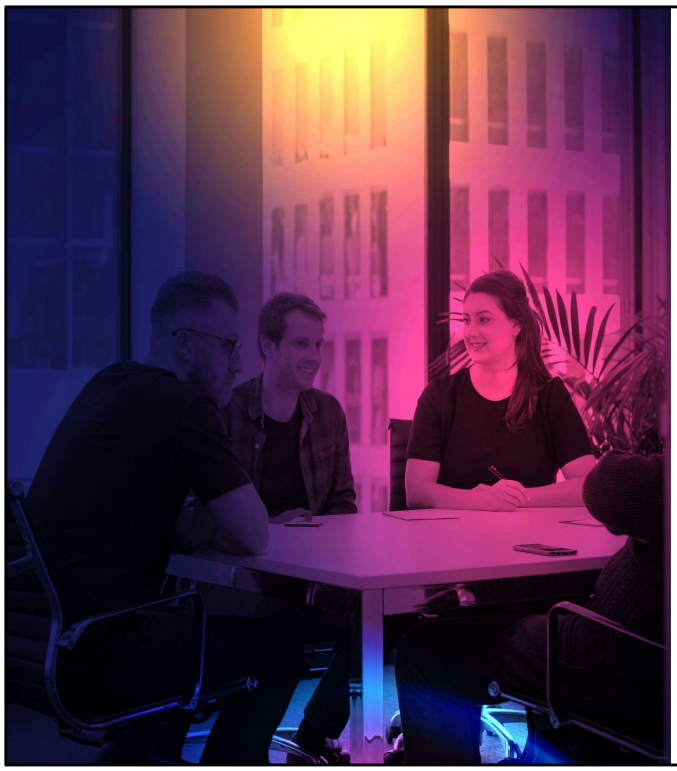
Security Concerns - CIOs remain reticent at the mere thought of handing over the keys to a multi-million dollar infrastructure. With some remaining in the most imperfect of situations just to avoid change and the lack of direct control of the functions outsourced, despite the fact that they actually gain a greater degree of control over their infrastructure in total.

The outlook though looks good, 50% of organisations say they would consider using a third-party IT service provider within the next two years.

MSSP & MSP's!

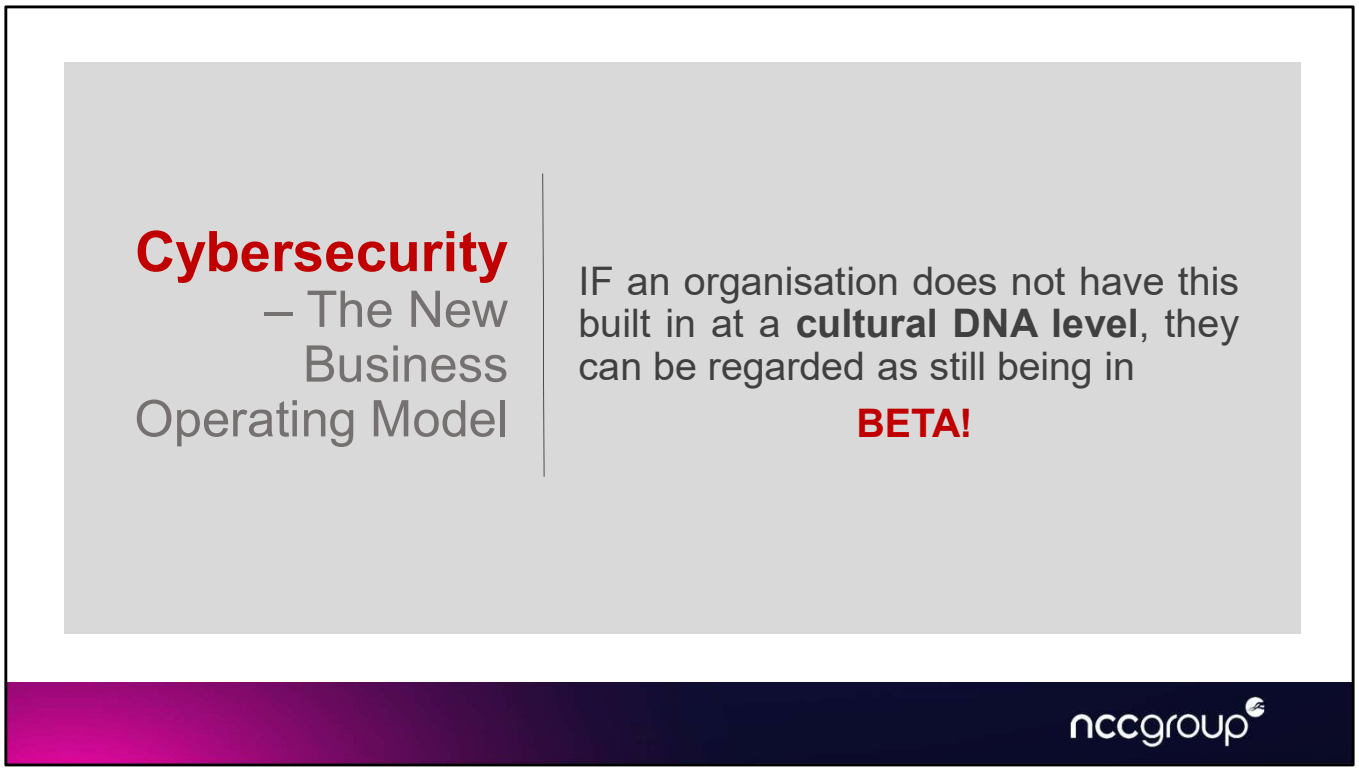
Not all MSP = MSSP

- **MSS Pure play** – Harmony with incumbent suppliers
- **MSP Vendor Benders** – Vendor centric gateway services
- **Boundaries** – who is accountable for what?
- **Advisory** – Domain Expertise keeps services honest
- Visibility – Trust mark maturity, CSA, NCSC, NIST not just ISO27001



New Operating Models

nccgroup



CyberSecurity has moved from a niche into a must have mainstream and is now the default expectation across the operational spectrum and at board level. This means a business centric, fully integrated Security attitude for todays hyper connected world.

The role of InfoSec and a Board level relationship is subtle but fundamental as an enabler to the digital success of organisations and core to the success of modern business strategies. It is what will make the business models operational in the information economy. InfoSec will be delivering the assurance so that the Business can take its IT tools and safely forge new ways of working with customers, open new markets and return greater shareholder value. Without this 'cybersecurity' posture an organisation can regard itself as still in beta. The need is for that mandatory operational layer that's no longer defensive and controlling and to recognise it as an enabling and facilitating part of core business DNA.

Cybersecurity IS the New Business Operating Model. A key principle of this strategy is the nature of minimum levels of baseline tolerance (risk) extending into optimal states (adaptive) as the various elements mature over time. The Baseline itself should not be misinterpreted as a static state, it is drawn against

the organisations Threat Profile which is subject to a rapidly evolving threat landscape. The organisations threat profile must similarly be adaptive to the demands of rapidly change business outcomes. One of the approaches is to harness the magnification effect of integrated and adaptive solutions to solve diverse problems in response to these demands, including but by no means exclusive:

- Unify access, device and security management.
- Respond to threat sophistication with tooling that is maintained for fit, form and functionality in real time with MINIMUM intervention or customisation.
- No dark endpoints – A single control plain that can help close the gaps in the kill chain through which threats penetrate.
- Tap the CTI (Cyber Threat Intelligence) of core technology ecosystems.
- Get ahead of the threats – This is only achievable by reducing the reaction time to respond, a policy based approach to risk management that allows integrated tooling to respond AND adapt in real time.
- Strong protection for identity and data both on-premises and integrate technologies such as cloud and 3rd party services such as ServiceNow.
- Last but NOT least – its about People and relationships (Supply Chain). Your security team IS your workforce, your weakest link is your Supply Chain so check each link.

Back to the Future with Escrow

EaaS enables organisations to embrace the adoption of cloud technology and gain confidence in its resilience

- Provides reassurance, protection and the freedom to innovate with new and exciting cloud technology
- Offers organisations the option to either access or replicate their unique cloud environment
- Additional verification testing options available for further assurance
- Developed in collaboration with leading cloud service providers Microsoft Azure and AWS

nccgroup

In brief outline, with Escrow as a Service, or EaaS for short, NCC Group provides the solution to simple cloud resilience that our customers require.

We give ISV's and their customers the freedom to innovate with new and exciting technology.

We offer a flexible solution which enables the customer to either access or replicate their unique cloud environment.

We provide a range of complimentary verification services to strengthen the contractual escrow solution.

And we developed our products in collaboration with the world's leading cloud service providers, AWS and Microsoft Azure.

Remember

Security remains YOUR responsibility

nccgroup

nccgroup

People led knowledge and capability is at our core

nccgroup

www.nccgroup.com

Twitter: @NCCGroupplc @NCCGroupInfoSec