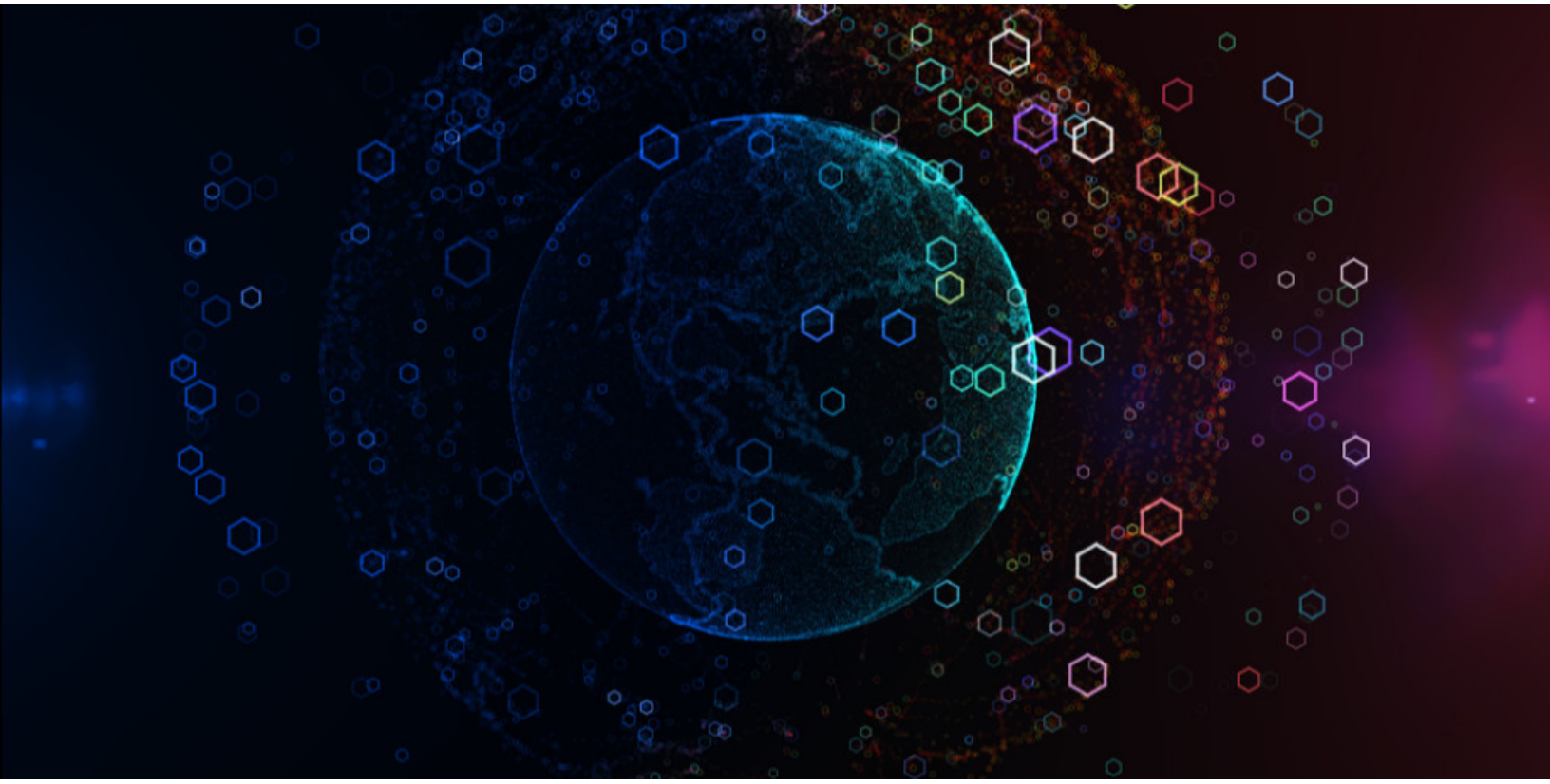

Shutterstock: Royalty-free stock illustration ID: 585942257

Mar 18, 2020 12:26 GMT

#BeRemoteReady: Q&A with NCC Group's CISO, Dominic Beecher

As organisations across the globe find themselves in uncharted territory, we spoke to our own CISO, Dominic Beecher to find out more about what he has been focusing his attention on and what advice he would give to organisations who are finding themselves faced with a whole new set of challenges when it comes to mobilising a remote workforce.

As NCC Group's CISO, what have you been focusing on to ensure that you are remote ready?

I've focused on making sure that our remote access capabilities – VPN and virtual desktop – are sufficient, both in terms of bandwidth and licensed capacity, to support all users who can work remotely. We did this by fast-

tracking some upgrades that were already planned, in order to cope with the increase in day-to-day remote working that we expected.

I've also made sure that users have tested their remote access methods before we need to invoke them, so that any teething problems can be ironed out in advance.

For client services that we have traditionally only ever delivered from our offices, I've worked with colleagues in these lines of business to come up with alternative ways of delivering the services remotely, with a different set of controls. This ensures that our services remain secure, just protected in a different way. It was important to only change the things that we needed to change, and take into account existing plans or desires to improve the services. So it's a case of speeding up future plans rather than a knee jerk reaction that takes us in a different direction.

What are the three things that should be at the top of any CISO's list to ensure their organisation is remote ready?

1. Make sure your colleagues have the necessary equipment and know how to use it securely – a realistic dry run, with a full day working from home for as many colleagues who can do it, will give you a good deal of confidence about your capabilities.
2. Make sure that your IT Help Desk and security incident reporting and investigation processes are set up to operate remotely. Expect an increase in calls to the Help Desk as people who normally work in an office get used to working remotely.
3. Develop key messages that all your colleagues can understand, so that they can talk to clients about your approach to remote working and the measures your company has in place to protect client information and continue delivering a high level of service.

Where do you see the biggest challenges for CISOs when prepping their organisation to be remote ready?

Your employees. If you haven't had a culture of remote working, or established practices for remote working, it is quite a change! Make sure that they have clear and straightforward instructions about how to work securely from a remote location.

There will also be pressure from line-of-business operations to "just keep things working" – and of course this is reasonable, but don't let this compromise security. Speed up your decision-making, but don't make hasty decisions that you regret later.

What are the biggest barriers to remote readiness?

A culture of presenteeism in the office can mean that preparations for remote working are downplayed when crises are not looming. That means

that you have to make decisions quickly when the crisis comes into view – which ties into the above point about not making hasty decisions that you may regret later.

If you could only give one piece of advice to an organisation on remote readiness what would it be?

Knowledge not hope – plan it and test it before you need it.

What technologies should organisations be looking at to support remote working?

Things like VPNs and virtual desktops are well established as the foundations of remote working setups, so I won't go into these. Software-as-a-Service running in the cloud is also tremendously useful. These services should have been designed from the start to scale well, although there have been a few glitches recently as some service providers have struggled to keep up with the hugely increased demand. Make sure you enable two-factor authentication (2FA) on cloud services – this is really important, and I can't emphasise this enough!

A good endpoint detection and response (EDR) solution, coupled with solid monitoring of the alerts that it generates, should give you the visibility of the security state of the computers that your staff use even when they are not directly connected to your corporate network.

Finally, good teleconferencing and collaboration services are really vital. These must be high quality and easy to use, so that remote workers aren't inhibited from taking full advantage of them. It can be isolating and lonely if you aren't used to working remotely, so take the time to build the work and social atmosphere with your team and your colleagues to help maintain team spirit and cohesion.

Do you think that this current situation will change how we work in the future?

It will certainly shine a bright light on ways of working that we might have taken for granted in the past – for example, the merits of paying rent for often inefficiently used office space rather than investing in secure remote working technology.

There are likely to be plenty of cases where contingency plans serendipitously turn out to be more efficient and effective than what they replaced, and they will endure. There is an interesting study The Benefits of Forced Experimentation [1] which showed that, in spite of the short term inconvenience, a Tube strike in London in 2014 produced a net economic benefit in the long term, because people found more efficient ways to get to work.

What's keeping you awake at night right now?

My chief concern is that my colleagues will naturally be more susceptible to the sharp increase in phishing lures that prey on the very understandable concerns about the Coronavirus outbreak. There has been an increase in fake websites, apps and emails with malicious downloads, and businesses should encourage employees to be vigilant. The UK's NCSC have a more detailed page about this [2].

What role can remote readiness play in an organisation's growth aspirations? What may be the long-term strategic benefits from this crisis?

Principally, I would say that having a workforce that is able to work flexibly and not necessarily from a traditional workplace location should make it a lot easier to expand operations in the future. You will now have the infrastructure and practices in place to support staff working wherever they need to.

In addition, organisations that have a solid remote working capability and a willingness & flexibility to use that to its full may also find that they are more attractive to a whole range of people outside their traditional recruitment channels.

Is there a difference in the cyber security mindset of remote workers versus office workers – is this something that needs to be addressed?

That is a great question. I think seasoned remote workers will tend to have the same security mindset that I would expect office workers to have; that is probably not true for those who are hurried into unaccustomed remote working. Sometimes, it is the simple things that catch people out – like leaving valuable laptops visible through a ground floor window – a temptation for thieves – or leaving screens displaying sensitive information visible to shoulder surfers or holding confidential conversations in public places. I'd say that everyone should take a bit more care when working remotely, as the physical security measures we take for granted in an office aren't always there to reduce some of the information security risks. You don't need to go overboard, but just think a little more.

[1] https://www.socsci.ox.ac.uk/the-benefits-of-forced-experimentation-evidence-from-the-london-underground-network

[2] https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus

---

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted

by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

Press Office - Group and UK
Press Contact
nccgroup@thisismc2.com
+44 (0)161 236 1352