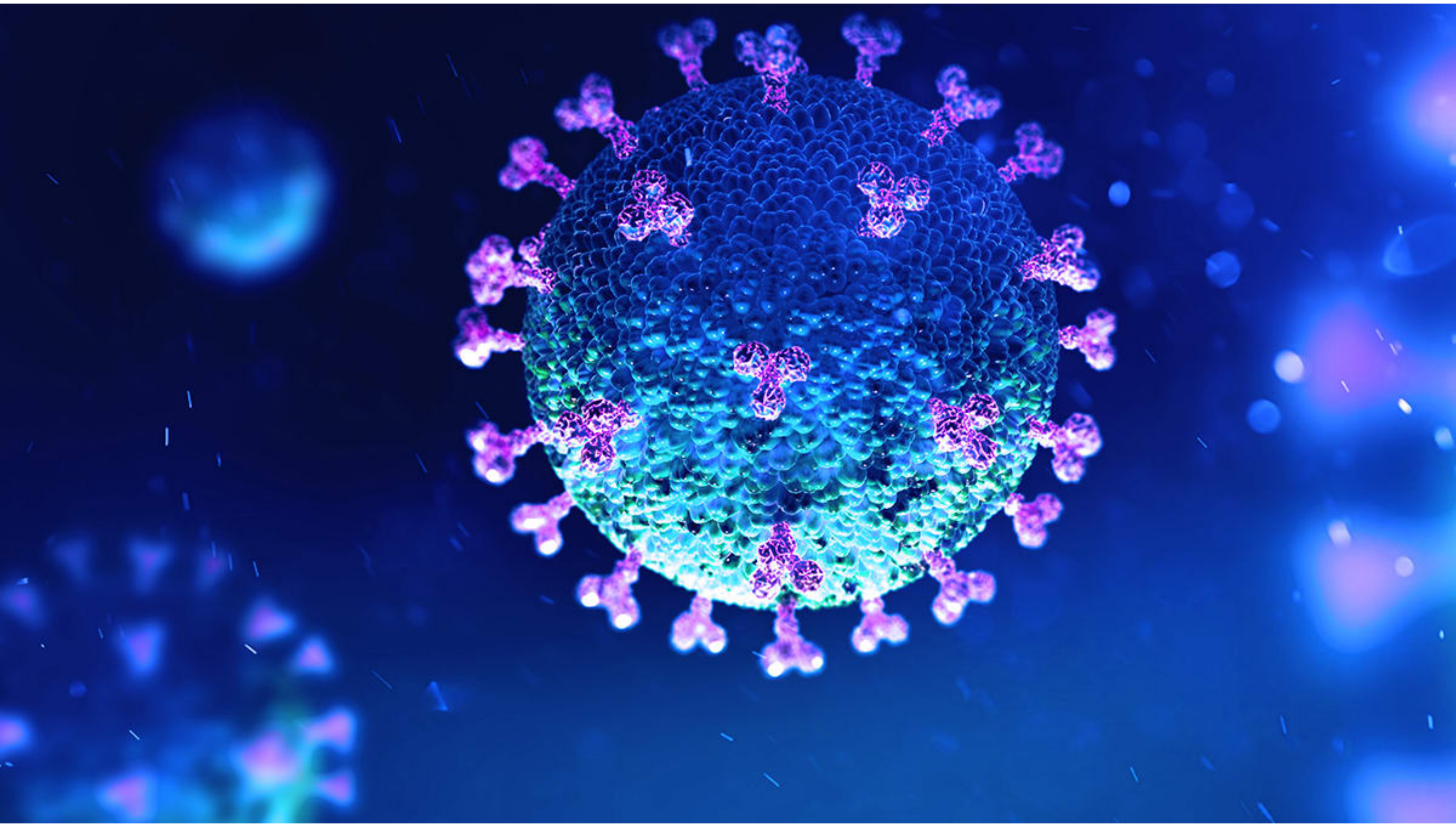

Feb 28, 2020 18:14 GMT

Updating your business resilience plan: advice for those concerned about COVID-19

Updating your business resilience plan: advice for those concerned about COVID-19

Since its outbreak in January, COVID-19 – more widely known as coronavirus – has spread widely and is impacting thousands of individuals.

This article from one of our senior advisers and directors, Tim Rawlins, explores what businesses should be doing to ensure business cyber resilience and continuity, as coronavirus continues to impact on individuals and organisations across the globe.

If you haven't already started planning to deal with the problems that you might face should the coronavirus situation get worse, now is the time to start thinking about how your business operations could be affected by the virus.

Given that cyber resilience always relies on **people, process** and **technology,** you really need to consider these three elements when making or reviewing your resilience plan. And, of course, your plan will need to be adaptable, as the situation can change very quickly and this means that you'll need to reflect and respond promptly.

Updating your colleagues

Given what we have seen so far, your colleagues are likely to be concerned for their health and that of their loved ones, so a first step would be to base your planning on them. Look at refreshing your 'absence and sickness' policies to allow for the closure of nurseries, schools, colleges and care homes which may see your staff are unable to come in to the office for an extended period, far longer than if it is just them off sick, as they have to care for others.

Be ready to answer their questions by either providing your own fact based frequently asked questions (FAQs), or directing them to a reputable source, such as the World Health Organisation or their own national authority. Remind them that random social media posts and gossip is not a reliable source for health advice or updates on the virus.

It's also important to consider that self-isolation and enforced quarantine might have an impact on both your office staff and business travellers, and that the situation can change rapidly as the virus spreads. Reducing fear and maintaining operational activity for the organisation is going to be key if it does.

If you are going to ask employees to work from home for any reason, then you'll need to provide both suitable equipment and advice on how to do it safely and securely. Your organisation's duty of care also extends to them working at home, so provide advice on setting up their equipment and fire safety guidelines. Also advise them to be cautious about being overseen or overheard when working on sensitive matters and the physical security of the laptop or other equipment you provide. It's also important to look at how material is going to be backed up if it's not connected to the office network while working offline. They won't have access to their laptops if they usually leave them in the office, so ask them to take them home as a matter of caution.

You may be sending your staff home if your office is caught within a government declared cordon. Your first thoughts should be your business continuity plan (BCP) and your disaster recovery site. However, your disaster recovery (DR) site may be in a cordoned area as well, so might not be available. if you haven't paid for dedicated desks, the DR site will probably have oversold its shared space which could mean that the first organisation to invoke its DR plan may take all the available space.

It might be possible to relocate your staff to another location; but again you'll need to consider the impact on staff as it will require them to change their work patterns and journeys. Flexibility is key from both sides, so get your senior managers talking to staff and let them know that it will be both required from them and given by the organisation.

Now would also be a good time to test your internal contact plan or call tree, to ensure that your message gets through to everyone at the right time. Remember that new joiners may not yet have their details in the system and people move and change numbers, so the contact plan will need to be constantly updated; many systems can be tied to an active directory to help keep it up to date.

If you are looking at messaging staff by phone, remember that regulated industries may require you to be able to audit business messages, so WhatsApp wouldn't be suitable. Have a look at one of the established mass messaging platforms instead as they come with a management console so that you can send massages, see who has received them and replied, and organise conference calls, and so on.

Accessing your systems

With your office unavailable, consider if there is equipment inside that needs to be turned on and left on. For example, Citrix systems may need the local desktop computer to remain on to allow for remote access. And to support the remote access, it’s important to check how many people can connect at the same time, of your virtual private network, and the bandwidth available. With departments that wouldn’t normally work from home, such as Finance and HR, relying on working at home for a longer period, one of them pulling down a large spreadsheet may take a much larger chunk of your bandwidth than you are used to.

Obviously, the move to cloud-based applications, such as Azure Active Directory and Office 365, will reduce your reliance on your office VPN, but if your office-based staff haven’t had to use them remotely, then check that they have the authenticator application for the two factor authentication on their phone. And then test the systems before you have to rely on them in earnest.

Your internal systems may also rely on back-ups being taken on tape or other media. While you should have your key software in escrow (safely stored off site), you may need to change the process for the back-ups, so that they are taken off site every day to ensure you have access to a safe copy should you not have access for an extended period of time.

There may also be some critical activities that can only be carried out from your normal location, so do engage with your clients and suppliers as soon as possible. You might have to declare ‘force majeure’ if you cannot deliver your contractual obligations, but explaining the situation early and working with them can alleviate a lot of the reputational and damage that might otherwise occur.

Communicating with your stakeholders

Talking of reputational damage, there are several things that you should have in place.

Firstly, plot out a stakeholder map to ensure that you have access to the names, telephone numbers and email addresses of your stakeholders. Think staff, clients, suppliers, professional colleagues, industry experts, and anyone else that you might need to contact.

Then prepare statements so that if something happens you are not thinking on your feet but relying on a considered and thoughtful statement. Have something that deals with sickness of staff, senior managers and families; a response should offices, town and countries where you operate be restricted; and how you would respond to staff stuck in a quarantined hotel or town while travelling and ultimately tragic deaths. Don't forget to remind your staff that any media contact should be directed to your senior management or communications team.

With all these preparations in place, your organisation will be better prepared to respond to a difficult situation. Of course, it doesn't cover every eventuality and I'd be keen to hear what additional measures you are taking.

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

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750