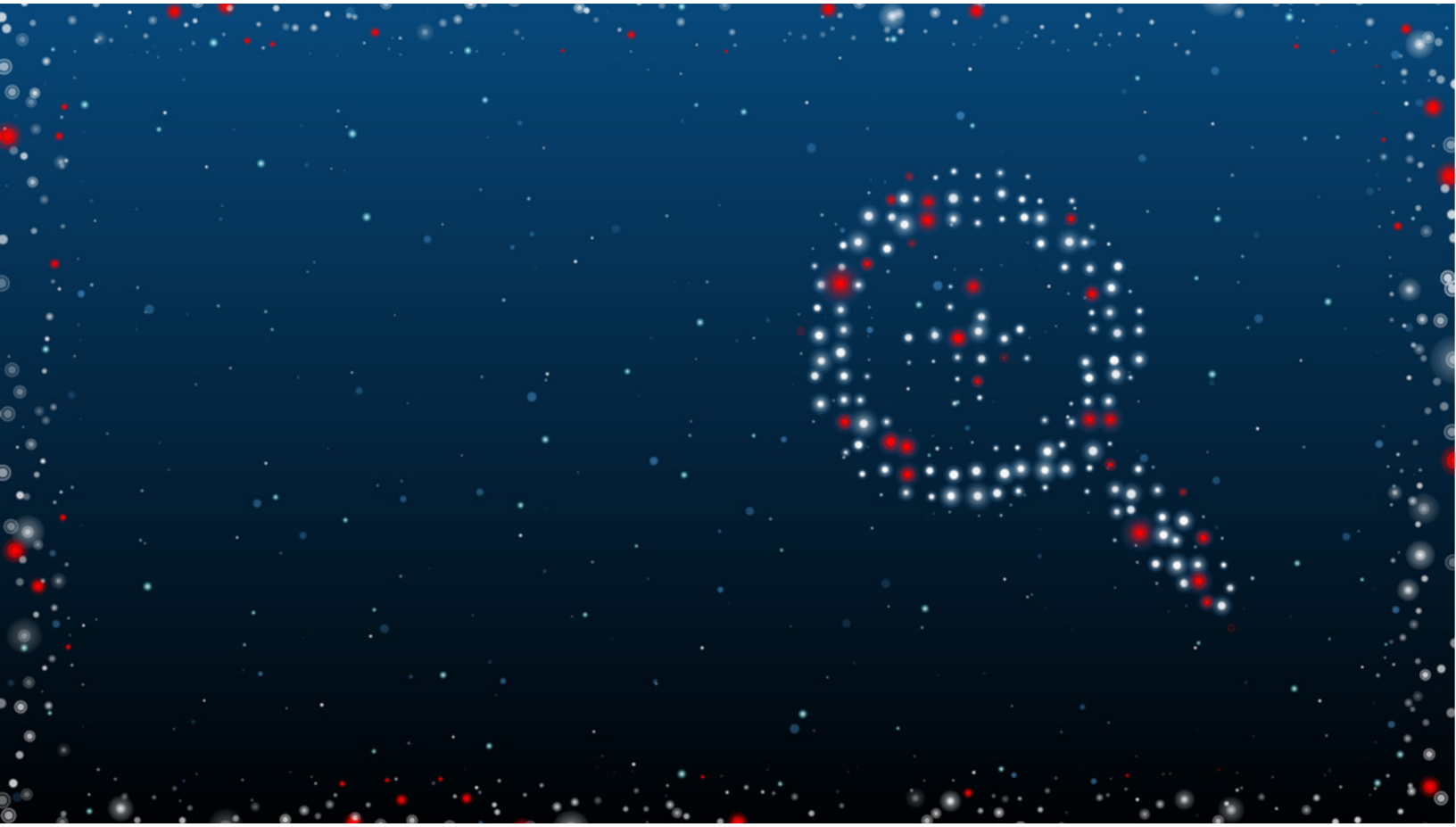

Magnifying glass illustration formed from white and red dots on a dark blue background. Royalty-free stock illustration ID: 1967381209

Jun 29, 2021 15:56 BST

“Knock, knock! It’s the Covid inspectors!”

Jan Hutchins, Senior Security Consultant at NCC Group

Although the idea of taking cyber security seriously is now thankfully fairly ubiquitous, there are other elements of security that still have a way to go to – particularly amongst SME businesses.

Where the usual mantras of patching, decreasing attack surfaces, educating users and managing use of credentials are excellent pillars to build our defences on, a lot of elements in the physical realm can be neglected. What use are the best firewalls, endpoints, switches, staff to maintain them, and

tens of thousands spent on pentests to test their effectiveness, if someone can tailgate into a building and bypass a door to the server room?

While this question is gaining traction amongst decision makers, physical security needs particular attention right now.

A new way of working – and attacking

Covid-19 has changed the way we work irrevocably (see our previous blog "A Whole New World"). Within a matter of weeks, businesses needed to scale up their remote working options and the offices emptied. As well as the increase in attack surface that came with administrators having to deal with entire organisations working remotely, opportunities for attack have also opened in the physical realm.

Sure, the chance of the swift tailgate over a busy lunch hour is not there anymore – but what new vulnerabilities exist as a result?

The safety of being lost in a crowd for a would-be attacker is probably gone. However, once an entry is made by other means, any nefarious party backed by the appropriate props would likely have the run of an entire building and stay unchallenged for as long as they need.

Service staff like lift engineers, builders, cleaners or even surveyors are a go-to for many. And with a convincing work order and a security guard that has likely been sitting there for months on their own, this is likely to be a favourite.

Or maybe you could go covertly, bypassing doors and locks while no one is around to cast suspicious eyes…

New government regulation has however now given us something that fits perfectly into the former category.

As some directors or health and safety executives will no doubt be aware, government guidance and legislation regarding safe working practices has spawned a litany of measures that must be followed to ensure that risk to staff and pubic is minimised from Covid-related threats.

As part of this, an interesting letter from the UK's Health and Safety Executive (HSE) now appears to be doing the rounds. To paraphrase:

"The Health and Safety Executive is carrying out spot checks and inspections on all types of businesses in all areas to ensure they are COVID-secure.

We are making calls so we can give expert advice on how to manage the risks and protect workers, customers and visitors. We are also working closely with local authorities, assisting them in the sectors they regulate such as hospitality and retail.

By calling and visiting premises and speaking directly to employers, we can check the measures they've put in place are in line with government guidance.

To ensure we reach as many workplaces as possible nationally and support the core work of our inspectors, we are working with trained and approved partners to deliver the spot check calls and visits".

While this practice is borne out of necessity for everyone's safety, potential abuse of this system is ripe for companies that do not follow the correct verification procedures. The letter does include a link to further guidance mentioning that visiting officers will be carrying identification and letters of authorisation from the HSE, as well as a number to call to verify a particular visiting officer.

Officiously targeting the unassuming front desk or security staff with this in a combined over-the-phone and follow up visit (with the requisite forged documents) has the potential to be a physical attacker's golden ticket. An excellent reason to be roaming practically anywhere, dropping in subtle references to the visit being a 'legal requirement' and to "keep everyone safe". After all, who wouldn't want to do that?

Consider where in your building you would need to have Covid-safe measures. It's not just the office space, but also the trading floors, maintenance areas, machine rooms, security rooms and reception desks. Not only that, but there are also grounds to reduce the amount of people in such areas, giving rise to the possibility that access to business areas by genuine staff could also be requested to be restricted by a visiting party.

It's common practice now to provide cordoned off areas purely for consultants to use whilst working. This is fine in the case of a trusted and vetted party, but what assurances do you really have regarding your visitors? It doesn't take long to install a network tap, keylogger or rogue access point, let alone more sophisticated attacks these days.

Mitigating measures

While the government information gives business executives some tools to verify the authenticity of the Covid measures inspector at their door, this information is no good unless it is circulated clearly, concisely and with correct emphasis to those members of staff who will be at the forefront of these interactions. These staff will then need to ensure they calling the number provided on the HSE website to verify the individual, NOT a number on the letter provided by the individual that arrives at your office.

User training should already include measures on how to deal with unfamiliar or suspicious people in the building, but it is imperative that what might appear to be an unlikely time for physical attacks, this is taken particularly seriously right now.

It should be remembered that while it might be an organisation's staff that are in the firing line, they are only as good as the support they receive. A security breach – physical or cyber – is rarely one person's fault. Proper procedures and processes need to be in place for everyone to follow if we are to curb the success of attacks.

This is just one example of how Covid-19 has changed the physical attack landscape. For further details about how the pandemic has changed the risk to your business, read our previous blog "A Whole New World".

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 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan 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