Mark is a Partner in Capita's Consulting business. He joined in January 2020 with specific responsibility for developing business for Capita Consulting in the Defence and Cyber Security markets.

Mark Roberts
Capita Consulting, Partner - Defence and Cyber

Making the world a safer place one click at a time

As of March 2020 over a quarter of the world's population is in lock-down.

That is a lot of people working from home. And even if they aren't working – they're online. The data from Europe's lockdown isn't available yet but in China average weekly downloads of apps during the first two weeks of February jumped 40% compared with the average for the whole of 2019, according to the **Financial Times**.

In the same month, weekly game downloads on Apple devices were up 80% versus 2019. UK Broadband providers have just announced that they will remove data caps on all domestic users in response to the demand for more and more bandwidth.

However, all this leaves us exposed as cybercriminals seek to exploit our increased reliance on screens for their own nefarious means.

Many **cybercriminals** are seeking to exploit our thirst for information as a trojan horse to attack us. Increasingly commonly, they are using the "weakest link" as the route into systems. People. Through increased phishing and social engineering attackers are using our desperation for information on COVID-19 to encourage us to open links that download Remote Administration Tools (RATs) on their devices. There are also numerous cases of criminal COVID-19-related Android applications that give attackers access to smartphone data or encrypt devices for ransom. And the proliferation of tools such as Zoom and HouseParty are beset with reports of hacking and security breaches.

Attackers are also taking advantage of the fact that working from home is rather new for many people. Security systems at home are rarely as sophisticated as those that would be in place in a corporate environment. The rise in people using their own devices also leaves them exposed – with weak passwords, out of date firewalls or relying on unsecured wifi hotspots. Plus by moving out of the office we have left an environment where our technology is protected by physical security systems – key cards, cameras, security on the door. While we can probably trust our family not to hack or steal our laptop – people in house and flat shares, or relying on unsecured remote working spaces are more vulnerable.

Enterprises haven't deployed the right technologies or corporate security policies to ensure that all corporate-owned or corporate-managed devices have the exact same security protections, regardless of whether they're connected to an enterprise network or an open home WiFi network.

The cost of these gaps is potentially huge. Cyber crime costs businesses and government £267 billion per year in the UK alone. According to the World Economic Forum, the average cost of a security breach to a financial institution is $5.3 million. To a media company that average is $4.3 million. They were an average 145 such security breaches PER FTSE 250 company in 2018 alone.

Looking at these figures how is the current environment different? Is this worse than Business as Usual?

The C-19 crisis has forced us indoors and online. The Internet has almost instantly become the channel for effective human interaction and the primary way we work, contact and support one another. Governments are relying on digital communications to provide information but also in many instances to track transmission and to police social controls around movement. And while data remains a target, theft is not always the aim. A new wave of cyberattacks sees data no longer simply being stolen but simply destroyed—or even changed in an attempt to breed distrust and cause chaos.

In this C-19 climate a cyberattack that deprives organizations or families of access to systems could be potentially fatal. In the most extreme scenario, cyberattacks have the potential to cripple infrastructure and take entire communities or cities offline with deadly consequences as emergency services, hospitals and power systems are undermined.

So. What can we do?

There are a variety of responses – from us as individuals and as businesses. Individually a lot of them are the same as the good cyber security practices we should maintain at all times. Use complex, passwords. Use different passwords for different systems. Update security software often. Avoid open wifi hotspots. Keep devices in a safe, ideally locked location.

As organisations we should be focusing on the following actions to keep our data and our infastructure safe.

Knowledge is everything. We need to focus on working with security teams to identify and mitigate for likely attacks and prioritize the protection of their most sensitive information and business-critical applications. Make sure the Board is clear on the level of risk they're exposed to and are prepared to accept.

Keep it simple. Our people are our weakest link. Home-working policies need to be clear and include easy-to-follow steps that let employees make their home-working environment secure. Front and centre of this should be how to reach internal security teams to report an issue, and a no blame culture that rewards flagging up mistakes (opening that phishing email, losing your laptop) rather than punishes them. Cyber training should be made relevant to their non-work life as well.

Invest in the right kit. In times of tightened finances it is still imperative that we invest in providing effective security capabilities, to ensure that we extend the same network security to "own" devices and to all remote environments. Capabilities like endpoint protection on all laptops and mobile devices, including VPN tools with encryption and an ability to enforce multi-factor authentication (MFA) aren't really "nice to haves". They are mission critical. So are automated threat intelligence systems and the capability to thwart common phishing attacks.

Crisis points are always opportunities. Opportunities for the "bad people" to try and take advantage of the chaos and lack of attention that comes from so much change and disruption around us. Cyber attacks are simply sophisticated looters – taking advantage of the high levels of distraction and disarray caused by an air-raid.

But they are also opportunities to get your house in order. Focus on beefing up your systems and procedures around cyber security. Invest in providing your people with the information and software they need to stay safe. Offer a pertinent reminder to us all that the more systems we secure, the safer we all are.