STAYING SAFE ONLINE IN THE NEW WORLD OF COVID-19

By Tarquin Folliss

The impact COVID-19 is having on us all is stark. Normal life in the UK came to an abrupt halt in March, no more so than in the workplace. The dramatic explosion of home working has placed extraordinary stress on individuals, networks and systems, forcing organisations to implement rapid changes. Technology is designed to adapt at pace, but in our haste, we may not configure our systems as securely as we would in normal times.

Criminals have always exploited the uncertainty and disruption brought about by crises, and COVID-19 is no exception. They are masters at leveraging the end users' heightened levels of fear, uncertainty and distraction and exploiting the opportunities this exposes.

We have already seen a rise in the levels of cybercrime. Phishing campaigns and ransomware attacks are on the increase. So, how do we protect ourselves, our people and our businesses? Here are a few thoughts.

Know Your Remote Network

Most organisations' infrastructure and systems are currently functioning outside their intended design parameters, with the expected 10-15% of remote workers now supplemented by the remainder of the workforce. This is further compounded by the increased adoption and utilisation of BYOD and direct SaaS platform access as "make it work" business continuity measures.

This creates the potential for a perfect storm: users operating with that heightened sense of anxiety and distraction but lacking the support of their normal layered defensive controls; uncontrolled endpoints that expand the attack surface; and all coinciding with an increase in malicious activity.

Best practise requires the use of corporately issued, managed devices, with corporate networks and systems air-gapped from personal devices and networks. The reality is that does not work at scale for all organisations, especially during the current crisis.

The first step towards managing these risks effectively is to understand what you have – who is accessing your network? From where? And via which devices? While this can seem daunting, working with trusted partners expert in cyber security will help you to establish situational awareness, enabling quick and effective action.

It is vital that security continues to act as an enabler for business, mitigating risks while ensuring continuity. Getting this balance right and supporting your people has never been more critical. Using technical controls where appropriate and effective, but also enabling understanding and encouraging the right behaviours to support the remote workforce, will help address these challenges.

Use a VPN

Most organisations will have invested in a Virtual Private Network. It is more important to have one in place in a remote working environment. VPNs are designed specifically to allow remote users or

branches in organisations to work through the corporate network via a public network while maintaining the same level of security.

Virtually all VPNs come with some form of encryption. It is advisable that your people are logged onto your VPN while operating at home. VPNs are also extremely valuable if you do have an incident, giving investigators data to repudiate actions, investigate movement and see additional breach points.

But be aware that a VPN is not a silver bullet. Creating privacy, security and repudiation is important, however there are a number of challenges with VPNs, including slower internet speeds, less resilience, dependence on VPN manufacturer reputation and, of course, the fact that you have effectively expanded your perimeter, meaning family members or malicious actors who breach devices within your VPN potentially have access to your corporate networks and systems.

In summary, use a VPN, but work with a trusted and respected brand, and deploy, manage and monitor it carefully.

MFA is Essential

Invest in a decent Multi Factor Authentication (MFA) capability. Credential theft, especially from SaaS platforms such as Office 365, is big business for criminals. It is one of the simplest and lowest risk ways to break into a network. Because your users are not behind your normal physical security controls (building ID cards, swipe access systems etc), it is even more important that you have a way to verify the login you are seeing is who you think it is.

Requiring a second factor authentication that is entered separately to verify a username is one of the most effective ways to negate credential theft and stop criminals from compromising your network. Investing in a system that is simple, integrates into your business workflows and your users' lifestyles (e.g. pushbutton approvals integrated with smart phones etc) validates your logins, defends your corporate systems and helps embed security with your people.

MFA can also help avert the unintended breach. A few of us are lucky to work at home in a dedicated space – a study, office or spare room – but many must use a workplace shared with other family members. It is not uncommon for someone leaving their computer for a break to find on return that one of their children has accessed it, having watched the parent enter the password, with embarrassing consequences.

Remember that your users may be using shared or personal devices, and that Mum's iPad might be for the kids' schoolwork as well as work emails. Embedding MFA can partly redress that missing physical perimeter.

Understand the Threat

Making your people aware of the threat and teaching them to be secure online is one of the most effective ways of securing your organisation. Individuals face threats online just like organisations. Improving your people's personal security awareness will not only protect them at home but encourage them to develop a good corporate attitude to security as well. If they have a good attitude to online security at home, they will bring that to work.

Security awareness can become a tick box exercise and, as such, has often grouped remote and traditional users together, rather than considering the specific risks the remote user community face. As the remote community is now the entire community, this is a great opportunity to focus your people on those specific risks.

- Phishing remains the most effective and widely used vehicle for malicious software. Teach your people the techniques of phishing and what to look for in a phishing attack. Encourage them to report suspicious emails to your security team – (if you don't have one, then make a member of the leadership the security point of contact). Emphasise to them that if they aren't sure about an email or link: 1. don't click; 2. contact the sender directly. Criminals bank on people making hasty decisions when under pressure or in an unfamiliar situation – such as now. Help your people to make the right decisions.
- User verification is critical: get them to activate Multi Factor Authentication on their accounts. Make sure they understand the value of strong passwords and are using a different password for each account. There are a number of password management apps which allow you, for free, to test the strength of a password, and use far more complex random passwords without needing to remember them. Test the user community: in a remote working environment, one member of your team may need additional support with cyber security; by identifying them, you will be both help them and strengthen your defences.
- Evidence your testing to ensure your regulatory compliance. Record your training and testing and demonstrate that you have understood the risks and addressed them.
- Don't forget this applies to everyone: your defenders, crisis management teams and key individuals are as exposed. So, train, test and evidence your crisis responders in a crisis.

Look After Your Employees

This period of isolation and uncertainty is stressful for all of us, but particularly for those on their own or with very limited opportunities to socialise. Communicating with your team on a daily basis and giving them the opportunity to sound off about their concerns is good management with benefits for security as well. A motivated team is more likely to take security seriously.

There are a number of excellent collaborative tools on the market to enable this. For corporate communications, stick with the tool provided by your corporate IT team or, if you have yet to adopt one, select a tool as your corporate solution and mandate its usage where possible.

Don't be Afraid to Ask

Finally, don't be afraid to seek advice. The situation we are in is exceptional, bringing new challenges, new experiences and demanding new solutions. We are all learning.

Tarquin Folliss is vice chairman of Reliance acsn, a specialist IT security and digital resilience company based in the UK. A former diplomat, he has more than 30 years of experience working in government, where he focused largely on national and international security policy. Since retiring from government service in 2013, he has worked in the UK's digital technology sector.

Reliance acsn is offering free advice on digital resilience and security during the COVID-19 crisis.