What is the Future for Cyber Security?

As the COVID-19 crisis continues, organisations are having to rethink their approach to digital security. **David Hobbs** finds out what options lie ahead

COVID-19 has brought huge disruption and change, with the effects of the pandemic expected to be felt both in the short and long term. While some organisations transitioned to remote working seamlessly, many have struggled to adapt. What the crisis has done has given businesses the opportunity to rethink ways of working – and a major part of that involves technology and cyber security. With that transformation comes new risks through changes in threats and vulnerabilities that will force organisations to think differently.

Criticaleye asked three experts for their thoughts on the technological landscape and what businesses should be thinking about as they move forward in a secure and sustainable way.

Mark Roberts
Partner, Defence & Cyber
Capita Consulting

The move to home working has raised many issues for organisations, and from a business perspective a lot of controls have been loosened to keep the lights on and the business going. That has been manna from heaven for the bad guys. The stats bear this out with phishing attacks up by 4,000 percent, malware incidents by 14,000 percent as well as increases in spoof domains – think covid.com. COVID-19 has presented huge opportunities for attackers because people's attention is elsewhere.

Attacks have been tailored to meet the needs of this situation and any attacker works on what we call escalation of privilege. So, once they get access to an organisation's systems, they look for ways to escalate that privilege to reach the higher levels - systems administrators or chief execs, for example. What can seem like a low-level attack can actually be a precursor to getting deeper into the organisation.

> *"Increase your monitoring, be extra vigilant and recognise that things have changed"*

Train Your People

One of the simplest but effective responses for organisations is talking to and training users. Remote working is new to many people – do they understand policies and what they can and can't do? What is best practice when working from home? People will inherently want to do the right thing but if they don't know a process is in place to protect them, there's every chance they'll circumvent it, accidentally probably, but still circumvent it.

A lot of people will be using their own devices to access corporate systems, so you have a big challenge from a security perspective about managing those devices. How do you assure what's on a device before you allow it to connect to your network?

Do the business as usual but recognise that the situation is different so increase your monitoring. Be extra vigilant and recognise that things have changed and that you need to look out for different things.

Continuity Planning

What this crisis has taught us is that continuity isn't something you have on the shelf somewhere. Your business continuity plan is key and needs regular review and practice. The companies that have invested the time in that properly are the ones who have responded most quickly, such as by moving to the Cloud. A Cloud-based infrastructure is heaven-sent now and companies with that on their roadmap will be reviewing and accelerating it.

From a security perspective, most CEOS will look back over the past few months and see that continuous operations were most important to them, so they have to invest in more agile ways of working.

I would recommend to a CEO to go back and do a risk assessment. How many organisations have real understanding of the level of risk they are carrying and how does that compare to their Board's risk appetite and tolerance? Fundamentally, that is where security budgets, investments and plans all stem from. I suspect that because of the many changes that have been introduced a lot of organisations might not have a good handle on where they sit in terms of risk.

Joe Baguley
VP & CTO
VMWare

From a security point of view, this crisis has mostly been about how a business manages end point security. Taking a device that was designed to be logged onto a corporate network and putting it on someone's wi-fi at home on a public internet – is it as secure as we think it's going to be? >

We're in a world where employees are taking devices into potentially very insecure environments full of IOT [Internet of Things] devices that have much less of a security stance than user devices, so the attack threat vectors are much higher when you're out in what is a 'dirty' environment.

This is about zero trust, the concept that a device has zero trust of anything that it comes near and assumes that anything it does come near – whether it's a wi-fi network or any other device on the network – is trying to destroy or attack it. At the same time the IT department doesn't automatically trust any device trying to use their services either.

Zero trust should be the starting point and the basis for any end-user computing strategy. It's then down to IT departments to manage devices by giving people applications and data on devices that the IT department doesn't even trust. How the users consume those two things is down to them but the IT department needs to make sure it is going to be secure and safe for them to do so. That's a fundamental mindset switch from IT departments owning and managing everything to them actually delivering applications and services to an "assumed compromised" world.

Micro-segmentation

What businesses should also be looking at is micro-segmentation. If an individual's device is compromised, what's the blast radius of that? With micro-segmentation we can break down your network into layers of self-contained areas making the entire system protected by your organisation's access points secure.

> *"The 'real world' is not the 'ideal world' anymore"*

Organisations like GCHQ and National Cyber Security Centre are now actively advocating for micro-segmentation in software over hardware basic security methods because they see it as more flexible, faster and scalable.

Most organisations have just gone through an incredibly large proof of concept, and CEOs and senior execs have realised just how important technology is to them. It's the enabler of how they've managed to continue functioning as a business. What would have happened 20 years ago in this situation? We'd have all gone home and been on dial-up. It's unthinkable.

Steve Johnson
Security Lead
Surevine

A lot of businesses have clearly been impacted commercially by the situation, so naturally profit line is the number one focus and will influence many things in terms of investment, time, and potential real estate – there may be downsizing of properties and assets from a capex point of view. I imagine there will be a trade-off, partly influenced by regulators and their expectations of what a secure organisation looks like – whether it's a corporate presence in an office under close scrutiny or an adjustment that accounts for other workplace scenarios.

The Bottom Line

Those conversations are going to shape a strategy in terms of what functions return to an office and what might remain out of an office on a semi-permanent or even a permanent basis. The biggest pain points will get the focus of investment, but bear in mind profitability in the face of this downturn means there's going to be a lot of scrutiny from commercial parts of the business as to what is really necessary to hold onto to keep the lights on in a safe way.

With the scramble in March for many organisations to fully set up remote working environments, I'm sure there were a lot of workarounds and short cuts made in haste around access controls, connectivity protocols, workflows and so forth, just to keep the companies running. That's to be expected in what was a worldwide business continuity test.

What that means from a technology point of view now is a long tail of putting things right again in a period of uncertain investment. It's very difficult to commit to a particular strategy other than perhaps fixing how you're currently working in a more remote way as best you can. That has implications for things like Payment Card Industry Data Security Standard (PCI DSS) compliance, for example, which is very location based.

Regulatory requirements still have to catch up, and I think regulators are going to have a hard time coming to terms with the fact that the 'real world' is not the 'ideal world' anymore. Regulatory compliance is going to be heavily influenced by the majority of companies trying to do business and justifying their practices as, 'this is the best we can do'. ■