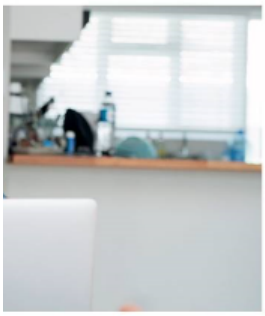

ackers out there,' Connory says, despite ightened emotion around coronavirus. t if things get worse in the next six to nths, who knows what's going to occur?'

angers of working from home

ecurity practitioner who isn't asking elves similar questions is doing elves and their companies a disservice cially as they come face to face with the ations of near-ubiquitous remote working. h companies like Twitter, Square, , Google and Microsoft were quick to rage employees to work from home to nt or limit the outbreak – but companies overnment agencies rapidly followed y forcing employees to stop travelling eetings, and eventually to stay home ther for self-imposed home isolation. ntries like China and Singapore ed working from home early to ain economic momentum, with alia and other countries rapidly ring suit. A recent Gartner survey found 8 per cent of Australian companies had mployees home to work – a sharp rise he 24 per cent of workers normally so.

rking from home is nothing new – alian-born unicorn Atlassian, for one, l off a formal remote-working initiative ar after internal surveys suggested cent of staff would like to work from more often – but blanket coronavirus-ed bans have been a baptism by fire for nies that haven't previously pursued from-home capabilities with such ardour.

Without the luxury of time and resources to plan such a significant change in workplace logistics, many companies have been caught flat-footed by the security implications of a model of that was completely online.

Working from home, for one thing, exposes corporate infrastructure to whatever security infrastructure exists on employees' computers, Internet of Things (IoT) and smart-home equipment, and personal mobile devices, which are often shared by less-than-security-conscious children and spouses.

Mobile devices' smaller screens make it harder for even careful users to spot the deceptions that cybercriminals use, such as malicious copycat domains that swap a capital 'I' for a lower-case 'l.'

This, according to Verizon APJ Managing Principal and Head Ashish Thapar, means that mobile users are six times more likely to click on malicious emails – as reported in the firm's latest Data Breach Investigations Report and expanded upon in its recent Mobile Security Index (MSI) 2020.

'The risk becomes amplified because of lack of visibility,' he explains. 'Mobile devices are becoming a much bigger contributor regarding attacks that are social-engineering-oriented – so protection will be done from both an enterprise standpoint and a consumer standpoint.'

Of the organisations surveyed in the MSI 2020, 39 per cent said that they had suffered a security compromise involving mobile or IoT devices over the past year – up from 27 per cent in 2018. Despite this, 43 per cent of respondents admitted that their companies had cut corners, ignoring security considerations of mobile and IoT devices to 'get the job done'.

No security in isolation

Work-from-home orders would expose the weaknesses created by past security compromises – surfacing vulnerabilities in company systems that were predominantly designed for in-office use, and the networks that support them.

Extending this access to remote workers and sites might mean, for example, relaxing firewall rules or introducing remote-access tools to let workers access their own desktops. As a recent Australian Cyber Security Centre warning highlighted, you must also manage the security implications of videoconferencing apps that have quickly become go-to tools for routine meetings and training.

There has never been a better time for robust identity- and access-management (IAM) tools like multi-factor authentication (MFA). Yet, without careful top-level planning – and coordination with disaster preparedness and risk-management specialists, and data-protection specialists – companies' coronavirus response plans could become their Achilles heel.

Unfortunately, the MSI also found that many companies have only increased their security spending after being compromised – and by then it was too late, with two-thirds of respondents saying that they had suffered a major impact from a mobile-related compromise.

Forty-three per cent of companies that had been compromised had increased their security spend in the past 12 months – a big increase from the 15 per cent that had done so without being compromised.

A similar percentage expected to do so in the coming year – well up from the 17 per cent that were expecting to increase security spending in the next year des not having been breached.

'Once bitten, twice shy' hardly seems a legitimate enterprise risk-management approach, but companies are finding the way as disaster preparedness plans push Australian businesses into remote work whether they're ready or not.

It shouldn't have needed the unprecedented disruption of a global pandemic for companies to address the issues – but now that the threat is real, make sure you're prepared.

Remind employees to remain scepti Update your filtering and access cont systems to protect remote workers, a work with operational business units to figure out how your organisation will safely support 50 per cent or eve 100 per cent mobile workers for the n 12 months.

'Security has to move the way that business moves,' Thapar says. 'It has to b agile; it has to be coherent in terms of y overall risk-management approach; and has to be non-intrusive to the extent tha can mitigate risk to an acceptable level.'

Are you ready for a remote-working mandate?

Tighter restrictions around COVID-19 have forced you to enable your workforce fo overnight. Are you ready?

West Monroe Partners offers five key tips to facilitate your remote lockdown:

- *Do employees have the hardware they need to be successful?* Ensure that there are enough laptops, headsets and related hardware for all of your employees, and that employees have access to 'good enough' broadband services to support their needs. Consider reimbursement policies, distribution of mobile hotspots, and even issues like virtual private network (VPN) licensing and capacity.
- *Do you have the right tools and technologies for virtual collaboration?* Ensure you have access to tools for online collaboration, intelligent workplace tools, and the like. Train staff to use them now so that they're not trying to figure things out under pressure later.
- *Do you have the right company culture to support virtual collaboration?* Increasingly common travel bans will require extensive reliance on virtual meet your culture supports vi includes ongoing metri communication tools to remote teams.
- *What is the best path fo mobility?* Fast-track MFA security frameworks to locked down. Ensure th secure tools allowing re access, server administr
- *Can your support desk of requests?* Do you ha and knowledge bases access to support whe troubleshoot security remotely? Have you de guides and automation everyday administratio