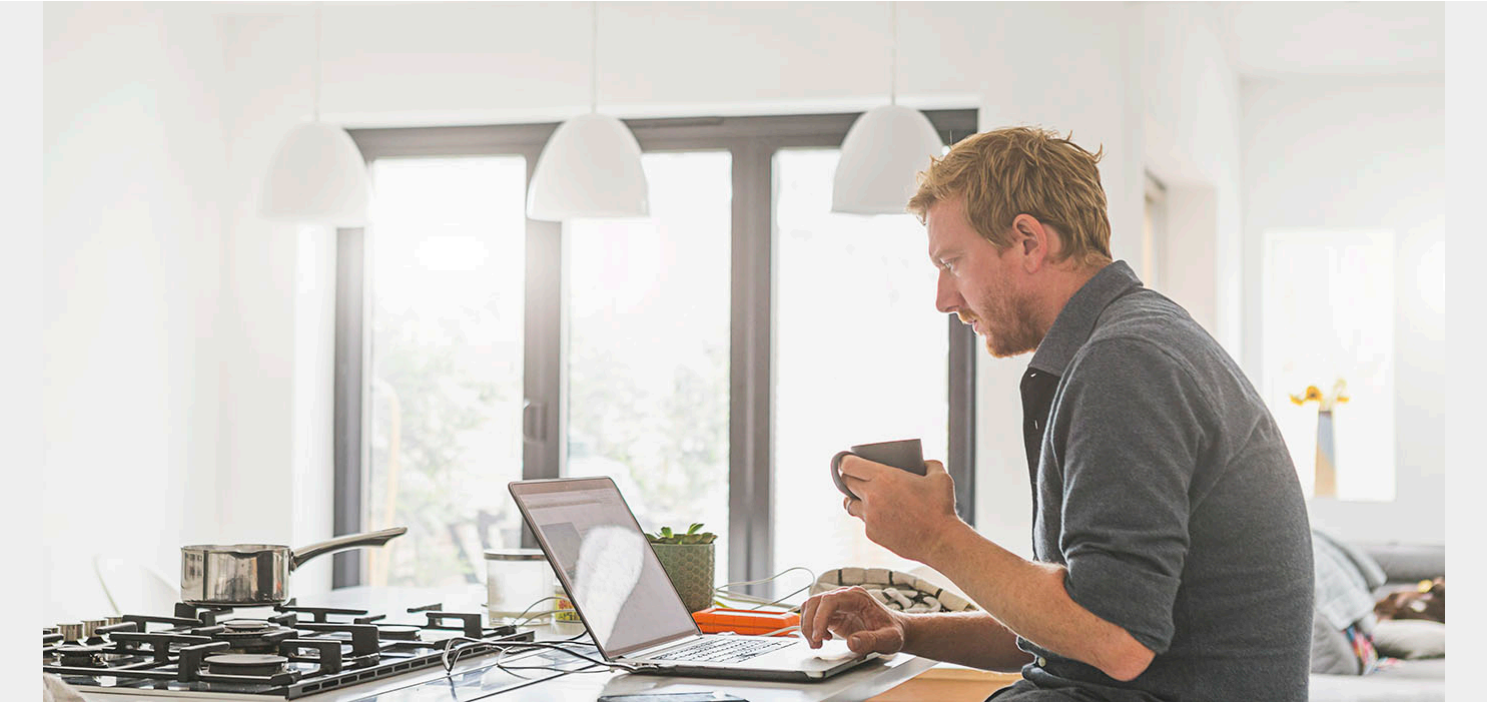
REMOTE WORKING: DELIVERING MAINFRAME SECURITY SERVICES IN THE NEW NORMAL



As countries went into lockdown and social distancing and remote working became the norm, our clients and teams have seen significant and lasting changes in how we work.

It feels like an age ago when my team spent most of the year globe-trotting. At times, we felt as much like a travel agency as a mainframe services provider. But with security policies and rules rewritten overnight, off-site and remote working quickly became standard practice. Quite apart from social distancing requirements, most of our clients' offices remain shut. Our own offices are closed. At the moment, if you want something doing, it has to be done remotely.

Because we've always been able to deliver this way, we moved to a secure all-remote footing immediately and across the full range of mainframe services including security assessments, penetration testing and vulnerability scans. At the height of lockdown we planned and implemented an end-to-end Db2 system security project. So how does it work in practice?

Several options are available to enable our people to access and work remotely. The client can send a physical laptop pre-loaded with their own VPN solution. Or send us a soft or hard RSA token and we use our own laptops to remote desktop or VPN into their systems. The point is, we can work however our clients want – and they know we'll be working as securely as possible.

A couple of weeks ago, I built a secure laptop to send to a client, a major insurance company. They plugged this into their network and we have access. This is the new way of doing things: a faster, more flexible and ultimately lower cost approach. If onsite delivery (when permitted) is required or preferred, it will most likely be priced as a premium service and incur higher expenses. With "COVID-19 secure" requirements clear, if you don't need to address a 48-point risk assessment and

all the logistics and practicalities involved in having people work onsite, then why would you?

Clients new to remote working immediately recognised how agile this approach can be. We can react more quickly, which is particularly important when it comes to security. We don't need to spend time making travel plans. We can be up and running within 24 hours. And that's true of all mainframe services, not only security.

Reduced travel means people can use more of their time more productively. Clients don't need to cover the costs of travel and accommodation, and there are environmental benefits too. Remote working vastly reduces our carbon footprint. I've taken two flights for professional reasons this year. Last year, by the autumn, I'd taken at least 20.

In terms of staffing, if a client's team member is unable to work through quarantine or self-isolation, or becomes unwell, we can respond fast with standby or interim personnel. Someone who knows the technology inside out, and is available for BAU activity or special projects within 24, 48, 72 hours… whatever you need.

We are even more flexible and responsive for cross-border clients. Our consultants and engineers can schedule their working days to match the job at hand and different time zones. We have a security consultant based in Australia right now supporting mainframe operations for a global bank's business unit with facilities in Asia Pacific, South and Central America, and Europe. It's a good fit.

Remote and home working have, of course, brought additional security issues: new ways of working, new vulnerabilities. Lockdown was a boom time for the bad actors. For example, the first month of lockdown saw a 72% surge in financial losses from cybercrime.[1] While the mainframe is the most securable platform on the platform, it does need thought, effort and application to actually secure it. More needs to be done in securing both mainframe and enterprise systems.

Indeed, a Forrester Consulting study[2] published in July 2020 provided evidence of "a false sense of mainframe security" with overconfidence and complacency leaving many companies vulnerable. The study found that only two-fifths of organizations are taking the steps required to actively secure the mainframe. Yet issues including security detection and response, protecting data, and reducing endpoint security risks all increased in priority. The study also reported that many organizations are now looking to managed services to help them fill the gaps in their security stance: services that, as we know, are increasingly easy to access remotely and securely.

When you add up the benefits of remote service delivery, it begs the question: unless you have a specific reason or want to pay a premium, why would you go back to onsite? The future may be uncertain but it always pays to look ahead. Could your own organization be leveraging remote managed services to complete delayed or stalled projects, to augment your own resources, and help develop the next generation of mainframers?

[1] https://eandt.theiet.org/content/articles/2020/09/introduction-of-coronavirus-lockdown-saw-financial-cyber-crime-surge/

[2] Source: A False Sense of Mainframe Security – a commissioned study conducted by Forrester Consulting on behalf of BMC Software, July 2020