Remote Working

Managing cyber security and data privacy risks

iso systems uk
Concept to Certification

services@isosystems.org
www.isosystems.org.uk

Published 04/01/2021

SECURE YOUR REMOTE WORKING INFRASTRUCTURE

Many organisations that quickly adapted to the COVID-19 lockdown by moving to a remote working model in late March found there was simply not enough time to carry out suitable risk assessments before making such sweeping changes to their working practices.

Their focus was on ensuring their services were able to continue rather than considering the risks associated with the change.

Those that had little to no existing infrastructure to support home working found the situation particularly challenging as they were exposed to cyber security risks, they were unprepared for and often didn't even understand.

Research shows why this was so damaging: a recent survey by Barracuda Networks found that almost half of organisations have experienced a cyber security incident since the lockdown began, and the major cause was their lack of preparation for such a dramatic change in working practices:

51%	**46%**	**49%**
of respondents said their workforce is not proficient or properly trained in the cyber risks associated with long-term remote working.	said they are not confident that their web applications are completely secure.	expect to see a data breach or cyber security incident in the next month due to remote working.

The risks worsened as more people switched to home working, thanks to a combination of unresolved security vulnerabilities, diminished IT support and increased attacks.

The cyber security company Darktrace told the Guardian that the "proportion of attacks targeting home workers increased from 12% of malicious email traffic before the UK's lockdown began in March to more than 60% six weeks later".

Working from home has now become the new normal: many organisations have realised that not only is it a perfectly viable way of working productively, it has numerous advantages too – not least economically.

With a deep recession predicted for the next two to three years, keeping costs under control will be even more important than ever.

Ensuring you and your staff can work from home safely and securely is a key part of that responsibility: data breaches and cyber security incidents – including network outages and loss of service – are expensive.

Fortunately, they're also avoidable.

HOME WORKING: WHAT ARE THE SECURITY RISKS?

Having a remote workforce brings its own security issues, from a reliance on BYOD (bring your own device) and the lack of corporate control over the configuration of employees' devices to issues relating to third-party Cloud services.

Criminals know this and have adjusted their attack methods accordingly.

According to Tripwire and Dimensional Research, 83% of organisations reported a significant increase in employees working from home as a result of the pandemic, and nearly all respondents (94%) said they were more concerned about security now than before the lockdown.

Further questioning reveals why:

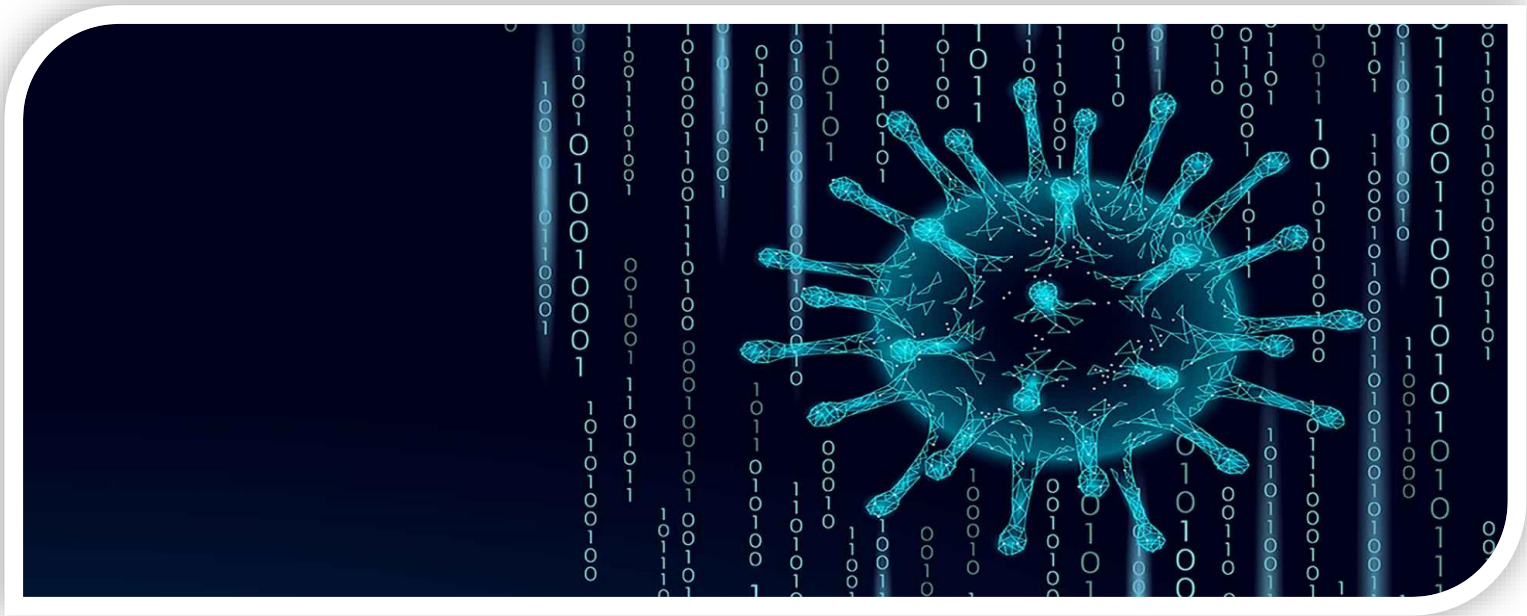
63%	**65%**	**68%**
of organisations have experienced COVID-19-related attacks.	report their security is worse because of COVID-19 (at least temporarily).	experienced security difficulties when dealing with COVID-19.

Other research tells a similar story: attacks on home workers have increased significantly while organisations have struggled to put appropriate security measures, such as remote penetration testing and staff training, in place.

According to Google, 18 million phishing emails about COVID-19 are sent every day, and the virus could be the biggest phishing topic ever.

But what can you do to ensure your organisation stays safe with a remote workforce?

See our Key Actions Infographic on the next page.



Actions to manage cyber risks

Processes	Your Suppliers	Your Employees
• Update remote working policies • Review changes against policies and contracts • Assess the risks to the updated processes • Review the effectiveness of your management reports and controls • Train your staff in final procedures • Review your internal audit plan • Carry out remote access and remote compromise penetration tests.	• Establish what changes have been made • Review the changes against contracts, service level agreements, data sharing agreements, etc. • Assess the risks introduced by the changes • Review the effectiveness of your management Reports and controls • Review your supplier audit plan.	• Review individual working environments • Ensure privacy and information security are appropriate for the tasks assigned • Train staff on new procedures • Train staff on evolving threats, e.g. COVID-19 phishing attacks.

Actions to manage GDPR compliance

Processes	GDPR Activities	Information Security
• Review and update data process maps • Focus on these processes: - Legal compliance, e.g. data subject access requests - Business-critical and high-risk data • Focus on compliance with critical contract terms • Make sure documentation is up to date, especially systems configurations and contact details.	• Carry out data protection impact assessments For COVID-19 processing, e.g. collecting Employee health data • Review data subject rights processes and document any areas where COVID-19 will prevent you from complying – the Information Commissioner's Office (ICO) will take genuine problems into account • Test data subject rights processes.	• Review physical security at empty offices and archive stores – risks of theft, vandalism, etc. • Review processes to maintain and replace hardware in offices • Review processes to maintain and Replace hardware in homes – consider health and safety issues, e.g. social distancing and hygiene.

Actions to support data breach management

Incident response management	Information Security	Your Employees
• Review procedures to ensure they are still relevant and effective • Review documentation to ensure all required information will be easily available when needed • Run a test to identify pain points and challenges.	• Review the threat landscape, including risks of compromised devices being activated once outside the office security perimeter, and COVID- 19-specific attacks • Review processes to secure devices and networks • Review processes to retrieve and replace devices, including risk of reinfection.	• Provide refresher training on recognising and reporting incidents • Test effectiveness, e.g. simulated Phishing attacks • Provide information security 'first aid' training • Support employees to prevent attacks through better home information security practices.

Find more resources at: www.isosystems.org.uk/resources

www.isosystems.org.uk