PRISM INFOSEC

# RAPID HOMEWORKING DEPLOYMENTS AND CYBER SECURITY

The essential guide for ensuring systems and data availability without compromising security

## TIME OF CHANGE

During these unprecedented times, organisations around the world are either following government advice or being forced to minimise human contact through the adoption of home working for their employees. Depending on an organisation's IT environment, this could be reasonably straightforward to achieve, or present a challenge in terms of maintaining functionality, performance and information security requirements.

Companies use different approaches to allow staff to work with organisational systems, applications and data, including providing them with desktop personal computers (PCs) or thin-client systems (essentially a stripped-down device that accesses applications from servers over the network). In other cases, companies provide staff with mobile computing devices such as laptops or tablets.

Furthermore, some organisations have already adopted a "cloud first" approach to the provision of business applications including email, collaboration, file sharing, customer relationship management and other services accessible over the Internet. However, others have been more cautious and use on-premise servers and applications which are only accessible over the internal network, or remotely into it via a Virtual Private Network (VPN) connection.

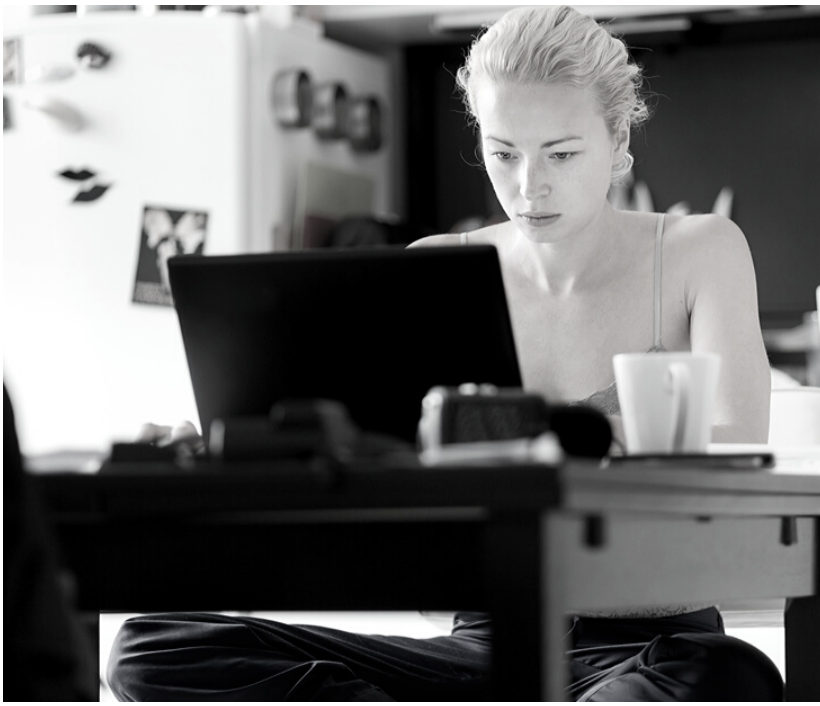
In anticipation of an upcoming requirement for rapid home working, Prism Infosec has already supported some organisations with deployment of secure builds for laptop devices, which have had to be quickly procured and distributed to key staff members. Additionally, given our extensive experience with delivering cutting edge security advice to organisations on internal networks, remote access and cloud services security, Prism Infosec would like to share some immediate considerations for any rapid change to remote working approach in this blog post. We plan to continue with further individual details associated with some of these areas in upcoming blog entries.

So, here are some immediate considerations and tips across technology, process and people from our team for ensuring a secure transition to remote working.

# 10 ESSENTIAL CHECKS

## 1) MAINTAIN SECURE BUILDS

A rapid transition from desktop PCs and thin client terminals to laptops should not circumvent existing security requirements and controls. Build and deploy a secure machine image as quickly as possible and prioritise the most important security options for the organisation, such as implementing full disk encryption, ensuring only user level access to the device, establishing a means to remotely manage and support it, (for example, using a Mobile Device Management and/or Remote Access Solution), restricting access to removable media and enabling automatic updates for the Operating System and applications;



## 2) HOME PC SECURITY

Although it may be tempting to allow remote access to company data from personal computers in employee's homes – there are many risks associated with this and it should be discouraged wherever possible.
The integrity and use of untrusted endpoints (home laptops/desktops and other devices) cannot be guaranteed and they may already be infected by malware which could compromise company data or lead to other issues such as a ransomware outbreak (particularly in the event that a VPN is used, or other services that allow a mapped network drive such as Microsoft Onedrive). If a presentational service (such as Citrix or Microsoft Terminal Services) is used for remote access to internal applications then this will reduce the risk considerably for the use of home PCs, however ensure a strong configuration is in place (see the next point)

## 3) REMOTE ACCESS CONFIGURATION

Ensure that any rapidly stood up VPN / Remote Access technology is configured with strong authentication and encryption. Where possible, use an additional factor of authentication such as a mobile device authenticator application or SMS codes and also ensure that the latest encryption technologies (IPSEC / TLS 1.2+) and cipher suites are used.

## 4) QUALITY OF SERVICE

A rapid change to remote working could lead to higher bandwidth and throughput on remote access technologies which in turn leads to performance issues associated with business-critical applications. Plan and implement user/client-based Quality of Service (QoS) limits on remote access endpoints. Where this is not possible consider implementing QoS policies on client Operating Systems to restrict network bandwidth.

## 5) CLOUD SERVICE CONFIGURATION

Review the configuration of cloud services and ensure that they are optimal. Many cloud service administration consoles (such as Microsoft Onedrive and Sharepoint and GSuite / Google Drive) allow the restriction of file sharing outside of the organisation. Additionally, log and audit settings may be off by default, make sure that these are enabled and that organisational cloud security settings are as secure as possible.

## Don't be tempted to implement quick solutions without fully exploring the risk to company data and acceptability to the organisation

### 6) CONTINUE TO ASSESS THE RISK

During urgent situations, particularly when the business is demanding rapid access to existing resources, it is tempting to implement quick solutions without fully exploring the risks to company data and whether they are acceptable to the organisation. Examples could include exposing a business- critical application to the Internet to allow immediate access to staff, or to bypass existing security controls to allow file sharing of company data. Implement a fast track risk assessment methodology (this should take no longer than ten minutes to complete) that covers some of the key information security controls and considerations that the organisation needs to maintain and ensure that IT team members planning those changes go through it and submit it to the management team.

## Implement user/client-based QoS limits on remote access endpoints.

### 7) MAINTAIN CHANGE CONTROL

Whilst the current climate may go on for sometime, remember it is unlikely to be permanent. As such, any emergency measures that have had to be taken will need to be rolled back safely and securely. Track all changes that are made either in an existing change management system, or use a simple spreadsheet or document template that tracks changes (e.g. date, time, resource responsible, systems affected, changes implemented, rollback procedure, reference to further documentation).

### 8) CYBER SECURITY AWARENESS

There has already been clear evidence of an increase in targeted and general phishing and other fraudulent attacks against people and organisations. Ensure regular communication and updates with employees on the importance of maintaining information and physical security in the home environment and regularly share information to the team. Remind staff not to expose company data over emails or unapproved resources (unauthorised file transfer portals or cloud storage areas)

# Ask staff to ensure devices are stored safely when not in use and make sure there are reporting guidelines if a device is lost or stolen

### 9) PHYSICAL SECURITY AWARENESS

With a higher number of corporate devices off-site than under normal conditions there may be a higher likelihood of loss or theft. Ensure staff understand the risks of leaving devices unattended, especially in public places. Ask staff to ensure devices are stored safely when not in use and make sure there are clear reporting guidelines if a device is lost or stolen.

### 10) BE AWARE OF GUIDANCE

Regular information security guidance is being published from national authorities such as the National Cyber Security Centre (NCSC) in the UK and the SANS Institute in the United States as well as security consultancies. Ensure that a resource within your organisation is assigned the responsibility of keeping up to date and briefing management on developments.

## ABOUT PRISM INFOSEC

Prism Infosec is based in Cheltenham and Liverpool, UK and was founded in 2006. The Company has delivered information security consultancy and assessment services to some of the world's largest organisations and has helped hundreds of companies to protect themselves from cyber-attacks. Prism Infosec is a CREST member company, a Cyber Essentials certifying body and is an 27001:2013 and ISO9001:2015 certified (UKAS-accredited) organisation.

To book an assessment call:
**+44 (0) 1242 652100**

To buy online visit:
**https://prisminfosec.com**

To send us an enquiry email:
**contact@prisminfosec.com**