National Cyber Security Centre
a part of GCHQ

Guidance (/)

10 Steps: Home and Mobile Working

Created: 29 Sep 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)
This section from within the NCSC's '10 Steps To Cyber Security' concerns Home and Mobile Working.

Summary

Mobile working and remote system access offers great business benefits but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers.

What is the risk?

Mobile working and remote access extends the transit and storage of information (or operation of systems) outside of the corporate infrastructure, typically over the Internet. Mobile devices will also typically be used in spaces that are subject to additional risks such as oversight of screens, or the theft/loss of devices. Organisations that do not establish sound mobile working and remote access practices might be vulnerable to the following risks:

- **Loss or theft of the device:** Mobile devices are highly vulnerable to being lost or stolen, potentially offering access to sensitive information or systems. They are often used in open view in locations that cannot offer the same level of physical security as your own premises.
- **Being overlooked:** Some users will have to work in public open spaces, such as on public transport, where they are vulnerable to being observed when working. This can potentially compromise sensitive information or authentication credentials.
- **Loss of credentials:** If user credentials (such as username, password, or token) are stored with a device used for remote working or remote access and it is lost or stolen, the attacker could use those credentials to compromise services or information stored on (or accessible from) that device.
- **Tampering:** An attacker may attempt to subvert the security controls on the device through the insertion of malicious software or hardware if the device is left unattended. This may allow them to monitor all user activity on the device, including authentication credentials.

How can the risk be managed?

Assess the risks and create a mobile working policy: Assess the risks associated with all types of mobile working and remote access. The resulting mobile security policy should determine aspects such as the processes for authorising users to work off-site, device provisioning and support, the type of information or services that can be accessed or stored on devices and the minimum procedural security controls. The risks to the corporate network or systems from mobile devices should be assessed and consideration given to an increased level of monitoring on all remote connections and the systems being accessed.

Educate users and maintain awareness: All users should be trained on the use of their mobile device for the locations they will be working in. Users should be supported to look after their mobile device and operate securely by following clear procedures. This should include direction on:

- secure storage and management of user credentials
- incident reporting
- environmental awareness (the risks from being overlooked, etc.)

Apply the secure baseline build: Develop and apply a secure baseline build and configuration for all types of mobile device used by the organisation. Consider integrating the security controls provided in the End User Device(/guidance/end-user-devices-security-guidance-introduction-0) guidance into the baseline build for mobile devices.

Protect data at rest: Minimise the amount of information stored on a mobile device to only that which is needed to fulfil the business activity that is being delivered outside the normal office environment. If the device supports it, encrypt the data at rest.

Protect data in transit: If the user is working remotely the connection back to the corporate network will probably use the Internet. All information exchanged should be appropriately encrypted. See Using IPsec to Protect Data(/guidance/using-ipsec-protect-data) and Using TLS to protect data(/guidance/tls-external-facing-services).

Review the corporate incident management plans: Mobile working attracts significant risks and security incidents will occur even when users follow the security procedures. The incident management plans should be sufficiently flexible to deal with the range of security incidents that could occur, including the loss or compromise of a device. Ideally, technical processes should be in place to remotely disable a device that has been lost or at least deny it access to the corporate network.

Further reading

Approaching enterprise technology with cyber security in mind(/guidance/approaching-enterprise-technology-cyber-security-mind)
End User Devices Security Guidance: Introduction(/guidance/end-user-devices-security-guidance-introduction-0)

Topics

Flexible working(/topics/flexible-working)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No