INFORMATION PACK

Remote Worker Security Information Pack – March 2020

Introduction

As more companies are moving to a “primarily working from home” model during the containment phase of the COVID-19 outbreak, we put together a reminder of teleworking security fundamentals to ensure the smooth running of your firm’s operations while keeping your assets protected from attackers.

Content

This information pack includes:

1. Risk Assessment Guidelines
2. Mobile Device and Teleworking Standard
3. Device Security Checklist
4. Security Awareness – Phishing Sticker
5. NIST SP 800-53 Control Mapping

Alongside this pack is also a further document, our Business Continuity Plan Template, to support organisations in establishing effective plans for ongoing service delivery.

Key Operational Best Practice

As a reminder of key operational best practice for organizations who already moved to a “WFH” model for the upcoming weeks:

1. Secure your premises’ physical access to avoid intrusion and physical access to your data
2. Alert your users on COVID-19-related active phishing campaigns
3. Remind your staff to not connect through public Wi-Fi and to change their default router password for personal Wi-Fi network
4. Enable Multi-Factor Authentication whenever possible
5. Ensure that your VPN provider has enough capacity for handling the rising traffic
6. Monitor and review your access logs for detection of abnormal behavior
7. Monitor and review your critical applications logs for off-baseline activities
8. Constantly monitor your data exfiltration points (including O365 and VPN sessions)
9. Monitor and investigate your DLP alerts
10. Limit the extension of your user’s rights and permissions with the principle of “need-to-know”.

Teleworking Risk Assessment Guidelines

Identification of Teleworking Risks

While allowing for a smooth run of operations during disruptive times, teleworking generates significant security risks which should be carefully assessed by enterprises to limit their exposure by implementing effective remediation strategies.

As users remotely access a wide range of systems, applications and files, an unsecure network or user's device vulnerabilities can lead to a data compromise. Risk owners and Executives need to consider the probability of occurrence of events such as:

- Data leak due to unsecure communications means (network, cryptography)
- Data leak due to end user computing (EUC) risks (i.e. BYOD, third parties)
- Unavailability of critical services (DDoS) due to inappropriate network capacity

Threats and Remediation Strategies

The following remote working threats should be considered as part of the enterprise Threat Modelling exercise:

1. **Unsecure Network (Man-in-the-middle Attack)**
   While remote, users will communicate and access organization's assets through the broadband or their own wireless network, both communication means being susceptible to eavesdropping if not properly secured. Organizations should protect themselves against communications interception by implementing VPN tunneling and strong cryptography.

2. **Compromised Devices (BYOD and third party devices)**
   The devices used to access organizational assets might not always be controlled by the organization itself, as it is the case for third party devices and BYOD devices. In such configuration, an infected / compromised device might go undetected and later spread malware through the internal network. Organizations can remediate this risk through the enforcement of an MDM as well as device hardening and the implementation of a strict network access control (NAC).

3. **Compromise of critical assets through external access**
   Critical information assets of the organization are traditionally kept within the network perimeter, which allows for a better control of its access. Remote access of those assets opens their availability to external hosts, increasing the risk of data leakage. Enabling Multi-Factor Authentication, limiting users' access rights through a strict Role-Based-Access-Control Model (RBAC) and constantly monitoring DLP solutions and systems/access logs are key contributors to the limitation of this risk.

Mobile Device and Teleworking Standard

Introduction

Background

Mobile devices (such as mobile phones, tablets and laptops) are a key part of the way staff complete their work. These devices allow employees to access the firm's information, systems and applications from a far greater range of locations than was the case previously.

A Mobile Device and Teleworking Standard defines the minimum security requirements that apply when our staff access company resources using mobile devices whilst not in the office (i.e., when teleworking) ,and to ensure company issued mobile devices are adequately protected at all times.

Purpose

This standard detail the requirements for the secure configuration, management, and use of all mobile devices which access our systems and/or networks, or which store, process, or transmit company information.

Scope

The requirements in this standard apply to all staff where mobile devices and teleworking options are used part of their day-to-day job functions.

All requirements for mobile devices and teleworking arrangements are in scope unless an exemption has been sought in accordance with the Cyber Security Policy.

Principles

The following principles provide the overarching requirements for the use of mobile devices.

Principle	Description
Secure configuration and management of mobile devices	Mobile Devices accessing the firm's applications, systems or information must be managed and configured securely
Secure Deletion	Devices storing or accessing corporate information or resources shall be configured to be remotely wiped by the IT Support personnel at any time. This may also result in personal data being wiped.
Privacy Expectations	All devices connected to the corporate network, applications or systems may be subject to monitoring by IT Security for the purpose of detecting security incidents.

Requirements

Mobile Devices

Requirement	Description
A mobile device management solution must be used to ensure mobile devices connecting to the corporate networks operate securely	A Mobile Device Management (MDM) solution must be used to manage the configuration and security of mobile devices used to access the corporate networks or systems by enforcing the following requirements: • All mobile devices storing or accessing corporate information and systems must have device encryption enabled • All corporate applications and data must be sandboxed from other applications through use of an encrypted container solution • Mobile devices must be configured to automatically update operating systems and installed applications within seven (7) days of update/patch publication • Bluetooth and Near-Field Communication (NFC) must not be used for transferring any corporate data • All devices must be configured to lock automatically after 10 minutes of inactivity • Automatic connection to open wi-fi networks must be disabled • Corporate data on devices that have been lost or stolen must be able to be remotely wiped • All mobile devices with access to the firm's networks must be protected by a secure access control method such as biometric authentication (e.g. fingerprint or face recognition) or the use of an alphanumeric password • "Jailbroken" or "rooted" devices must be prohibited from accessing the corporate networks, systems, and information.
Laptops connecting to corporate networks remotely must have security software installed	Laptops used by staff at any time to connect into corporate networks remotely must have security software installed that includes anti-malware and personal firewall functions that meet the firm's requirements in accordance with the *Malicious Code Standard.* The firm may at its discretion enforce this requirement through the use of a mobile device management solution.

Laptops

Requirement	Description
Laptops	Laptops must have anti-virus or anti-malware software installed where the operating system is known to be susceptible to malware.

Teleworking

The following requirements apply when staff are teleworking or working outside the corporate offices

Requirement	Description
Teleworking involving remote connections into corporate networks must be performed securely	All remote connections by staff to the corporate network or platforms or applications hosting corporate data for the purposes of teleworking must occur via a firm's approved TLS connection, SSH tunnel or IPsec virtual private network (VPN) solution.

Device Security Checklist

Introduction

This document has been developed to provide a specific set of security requirements for administrators, engineers, developers and others with privileged access to either organization or client information systems. It is intended to be used by staff on a periodic basis to assess and self-report their compliance posture. The collated results of these assessments may then be shared the organization's clients to aid in demonstrating our commitment to contemporary security practices.

Organizations recognize that company devices – and in some cases personally owned devices - often hold client data and we need to be confident that personnel with privileged access are managing them in a secure manner and in line with industry best practice.

Checklist

The below checklist of the most effective and recommended security controls can be used by personnel to:

- Quickly assess their current security posture; and
- Identify security areas that require strengthening.

Yes / No	Control
Passwords / Passphrases meet or exceed industry recommendations These controls refer to passwords used for client related accounts, organization's accounts, and local workstation accounts.	
Yes / No	Passwords or passphrases are a minimum of 13 alphabetic characters long, or a minimum of 10 characters with complexity – such as symbols and numbers
Yes / No	A unique password is used for each account / service
Multi-Factor Authentication (MFA) is used wherever possible Sometimes referred to as Two-Factor Authentication (2FA), MFA is an authentication strengthening method that requires an additional factor such as a token sent to your mobile phone, in addition to your username and password to authenticate.	
Yes / No	MFA is enabled for external logins on all corporate services that support MFA/2FA
Yes / No	Where MFA is not supported, additional care has been taken to ensure the account password is sufficiently complex and unique to the account
The workstation (including BYOD workstations) has been hardened Steps have been taken to harden the workstation used to handle sensitive client data.	

Yes / No	Control
Yes / No	An account with administrative privileges is **NOT** used for day-to-day use
Yes / No	Microsoft Office macros are not permitted to execute, or only whitelisted macros are permitted
Yes / No	The workstation is up to date with the latest operating system patches
Yes / No	The applications installed on the workstation are up to date and patched regularly
Yes / No	Antivirus is installed and operating on the workstation
Yes / No	The entire hard drive is encrypted (full-disk encryption), or the folder(s) that contain sensitive client data are encrypted
Yes / No	Java (produced by Oracle) or 'Adobe Flash' are **NOT** installed on the workstation or are only installed within a containerised environment – such as a virtual machine
BYOD Security has been considered Any personal device owned by a staff member that has the potential to contain sensitive client data, including devices where data has been sent via email in the case of a synchronised Inbox.	
Yes / No	Where possible, sensitive client data does not reside on BYOD devices
Yes / No	A BYOD policy exists and has been reviewed by the personnel
Yes / No	The device is the individual property of a staff member and not shared with others
Yes / No	The device is a well-known/reputable brand and a recent revision of the product line
Overseas travel Personnel are aware of their requirements to minimise client data on devices that they take with them overseas on business and to ensure additional protections are in place.	

Yes / No	Control
Yes / No	The organization's IT Staff are consulted before overseas travel to ensure devices containing client data have had additional hardening and data protection controls configured
Yes / No	Client data that is not directly related to the purpose of an overseas visit is removed from the device's disk drives prior to departure
Yes / No	Personnel are aware of the dangers of connecting to unknown or public Wi-Fi whilst travelling.
General Miscellaneous additional controls that are required.	
Yes / No	Application content controls are enabled on devices preventing unapproved/untrusted applications from executing
Yes / No	Application content controls are enabled on any BYOD device containing sensitive client data preventing unapproved/untrusted applications from executing
Yes / No	Only corporate email accounts and other <Company Name> approved mediums are used for communication
Yes / No	Only secure mediums approved by <Company Name> are used for the transfer of sensitive client data internally
Yes / No	Personnel have undertaken approved cyber security awareness training.

References

To develop this set of security requirements, the following publications produced by the Australian Signals Directorate (who provide guidance on cyber security matters for the Australian government) were reviewed as used as the primary inputs.

- Passphrase Requirements: https://www.asd.gov.au/publications/protect/Passphrase_Requirements.pdf
- Cyber Security for Contractors: https://www.asd.gov.au/publications/protect/Cyber_Security_for_Contractors.pdf
- Restricting Admin Privileges: https://www.asd.gov.au/publications/protect/Restricting_Admin_Privileges.pdf
- Hardening Windows 10: https://www.asd.gov.au/publications/protect/Hardening_Win10.pdf
- Multi-Factor Authentication: https://www.asd.gov.au/publications/protect/Multi_Factor_Authentication.pdf
- Overseas Travel: https://www.asd.gov.au/publications/protect/Electronic_Devices_OS_Travel.pdf
- Enterprise Mobility BYOD: https://www.asd.gov.au/publications/protect/Enterprise_Mobility_BYOD.pdf

Security Awareness – Phishing Sticker

NIST SP 800-53 Control Mapping

Source: NIST SP 800-46 Rev.2, Appendix A

NIST SP 800-53 Control	Telework/Remote Access/BYOD Implications
AC-2, Account Management	Single-factor or multi-factor authentication for remote access users, such as passwords, digital certificates, and/or hardware authentication tokens.
AC-17, Remote Access	Documentation of remote access requirements, authorizing remote access prior to allowing connections, monitoring and controlling remote access, encrypting remote access connections, etc.
AC-19, Access Control for Mobile Devices	Requirements for organization-controlled mobile devices and authorization to connect mobile devices to organizational systems, such as through remote access.
AC-20, Use of External Information Systems	Use of external information systems, such as personally owned client devices (BYOD) and third party-controlled client devices, that may process, store, or transmit organization-controlled data on behalf of the organization.
CA-9, Internal System Connections	Connections between a system and system components, including mobile devices and laptops
CP-9, Information System Backup	Teleworking Data has to be backed up either locally or remotely
IA-2, Identification and Authentication (Organizational Users)	Single-factor or multi-factor authentication for remote access users, such as passwords, digital certificates, and/or hardware authentication tokens.
IA-3, Device Identification and Authentication	Mutual authentication is recommended whenever feasible to verify the legitimacy of a remote access server before providing authentication credentials to it.
IA-11, Re-Authentication	Reauthentication periodically during long remote access sessions, such as after each eight hours of a session or after 30 minutes of idle time. This helps organizations confirm that the person using remote access is authorized to do so
RA-3, Risk Assessment	A risk assessment should be performed as part of selecting a remote access method (tunneling, application portals, remote desktop access, direct application access)
SC-7, Boundary Protection	Network segmentation (e.g., using subnetworks) to keep publicly accessible components off internal networks, and monitoring and controlling communications at key boundary points.
SC-8, Transmission Confidentiality and Integrity	The various remote access methods discussed in this publication protect the confidentiality and integrity of transmissions through use of cryptography.