FRAUD FACTS

Fraud Advisory Panel

Issue 23 June 2014

INFORMATION FOR ORGANISATIONS

Bring your own device (BYOD) policies

Organisations are increasingly allowing staff to connect to their corporate network using their own personal devices. This factsheet highlights some of the security issues that should be considered and safeguarded against when adopting such an approach.

Introduction

Organisations are increasingly allowing staff to connect to their corporate network using their personally owned electronic devices. Such an approach can be advantageous, boosting productivity and enabling staff to work while travelling or away from their desk. However, businesses should be aware that there are important security issues around the use of personal devices for work purposes, and these need to be carefully considered and safeguarded against.

Some of the risks associated with allowing staff to use their personal devices for work purposes include (but are not limited to):

- loss or theft of staff-owned personal devices that contain business information;
- inadequate controls for unauthorised programs (such as apps, instant messaging, file sharing and 'paste bins') which may result in accidental data leakage and security vulnerabilities (malware);
- deliberate and/or malicious theft of business information and intellectual property;
- non-compliance or breaches of applicable laws, regulations and/or business policies (such as data protection and Payment Card Industry Data Security Standards); and
- insurance and IT security policies may become more complex and costly to manage.

In addition, it can be very difficult to tell staff what they can and cannot do with their own devices in their own time.

What is a BYOD policy?

A 'Bring Your Own Device' (BYOD) policy sets the standards, procedures and restrictions applicable to staff who use their personally owned devices to connect to the corporate network from home, at work or while travelling for business purposes. It aims to protect your business (and your staff) from accidental and deliberate information security breaches.

An effective BYOD policy should be simple, concise and easily understood. As a minimum it should explain:

- who the policy applies to (eg, staff, contractors/consultants/freelancers);
- which devices can be used (eg, laptops, tablets, smartphones);
- what services and/or information (data) can be accessed (eg, email, calendars, contacts);
- the responsibilities of the employer and staff member (including for security measures that need to be adopted);
- which applications (apps) can/cannot be installed (eg, for social media browsing, sharing or opening files etc);
- what help and support is available from IT staff; and
- the penalties for non-compliance (eg, privilege revocation and other disciplinary procedures).

Before staff are allowed to use their personal devices for work purposes they should agree to adhere to the requirements set out in the BYOD policy.

Whom should it cover?

Your policy should cover all full- and part-time staff who want to use their personal devices to access business systems and information. It should also cover consultants, contractors and freelancers.

Designating responsibility

Designate oversight for the policy to an individual and/or department with sufficient authority, such as a director or senior manager within the IT department.

Communicating your policy

All staff, contractors, consultants and freelancers should be made aware of your BYOD policy. Actively and regularly promote the policy to staff throughout the organisation – irrespective of grade, position or length of service.

Reviewing your policy

Technology changes rapidly. It is essential that you review your BYOD policy regularly to ensure that it remains relevant and effective.

Key security considerations

Before introducing a BYOD policy it is important that your business has well-managed and appropriate information security policies and procedures in place. Consider the legal risks and seek advice from an IT, data protection or other suitably qualified professional where appropriate.

Key issues to be considered are outlined below.

Help and support

Technical support may be required when staff connect to the network using their own device. This could involve activating desktop security settings (eg, screen lock), encryption and firewalls, installing remote desktop clients and a Virtual Private Network (VPN) connection.

Publish a list of supported devices and the security steps that staff must take for each device. All staff should access the network using a unique username and a strong password.

Sign-off procedure

Ensure each BYOD device is compliant with security policies before granting network access. Decide how this is done: either face to face or through the use of remote access technology. Ask staff to agree to various security provisions during the sign-off process (such as secure wipe settings).

Make it mandatory for staff to report lost or stolen personal devices and any suspected data breaches immediately to your IT/data protection department who can instigate actions to remotely wipe or protect the loss of business data.

Data classification

Categorise business information into public (eg, press releases), internal (eg, contact lists) and confidential data (eg, client or customer data). Use controls to limit the opportunities for confidential data loss by linking classification to your information and network security policies.

Information security

All staff should be asked to sign a security policy that prohibits the retention of confidential business data on personal devices (whether encrypted or decrypted). Limit staff access to data to a 'need to know' basis.

Link your BYOD policy to your Acceptable Use Policy (AUP) which asks staff not to connect to unacceptable, objectionable or illegal websites or engage in inappropriate behaviour through a VPN connection made accessible via a personal device (eg, using social media to post abusive content). Where possible, block access to high-risk websites via the VPN by using firewall accept and deny rules.

Consider including in employment contracts the disciplinary action that will be taken for policy breaches.

Always act on advice published by the Information Commissioner's Office (ICO) when reviewing security policies. Data protection must be taken seriously by all concerned. Remember: your business must never have access to any personal data stored on a BYOD device.

Network security

Ideally staff should access business resources through a virtual desktop that prohibits the download of any document to their personal hard drive. Personal devices should be considered 'untrusted' and given limited access to network resources. This can be done using Dynamic Host Configuration Protocol (DHCP). Access to limited network resources and data can be granted to untrusted devices through network separation and firewall rules.

Security management

Changes to network security policies may result in new vulnerabilities. Make sure that remote and virtual desktop applications are monitored and regularly patched. Critical security holes should be patched on a risk-sensitive basis (including a zero-day fix rule for emergency updates). All personal devices will need security management, vulnerability scanning and updates as required.

Leavers policy

Ensure your staff leavers policy allows your IT department to retain a copy of all business-related email communications and documents created by the leaver, whilst ensuring no copies are retained by any individual or personal device (eg, by performing an 'exit' wipe). Network access should be revoked immediately. Unless your business retains full control over security settings this may be challenging.

Hallmarks of an effective policy

DO:

- ✔ Make staff and consultants aware of your BYOD policy. Actively and regularly promote it throughout the organisation to staff – irrespective of grade, position or length of service.
- ✔ Require staff to set a strong PIN or password on the device. Passwords should contain a combination of letters, numbers and other characters, and be difficult to guess.
- ✔ Ensure that you have the right to wipe the content on devices that are lost or stolen. Provide guidance for staff on how to back up their personal content so that it can be restored to a new device.
- ✔ Designate responsibility for oversight of your BYOD policy to an individual and/or department with sufficient authority.
- ✔ Review the policy on a regular basis. Update it to reflect technological advances and changes to business activities.

DO NOT:

- ✗ Expect staff to be aware of the policy without telling them it exists.
- ✗ Introduce a BYOD policy and fail to follow up on it.
- ✗ Expect that the existence of a policy alone is enough to prevent fraud or loss of business information.

Further information

See our separate fraud factsheets on *Cloud Computing*, and *An Introduction to Fraud Risk Management* for more information.

Fraud Advisory Panel
www.fraudadvisorypanel.org

Get Safe Online
www.getsafeonline.org

Information Commissioner's Office
www.ico.org.uk

PCI Security Standards Council
www.pcisecuritystandards.org

The Fraud Advisory Panel gratefully acknowledges as the main contributor Seona Devaney (Frisk Online) in the preparation of this Fraud Facts.

Fraud Advisory Panel, Chartered Accountants' Hall, Moorgate Place, London EC2R 6EA.
Tel: 020 7920 8721, Fax: 020 7920 8545, Email: info@fraudadvisorypanel.org.
Company Limited by Guarantee Registered in England and Wales No. 04327390
Registered Charity No. 1108863

Distributed by